# Down to Earth, Up to Space

## A Security Architecture Analysis of 5G Terrestrial and Non-Terrestrial Networks

Master Thesis

Jegor Zelenjak

Delft University of Technology

TU Delft

esa

# Down to Earth, Up to Space

## A Security Architecture Analysis of 5G Terrestrial and Non-Terrestrial Networks

by

Jegor Zelenjak

to obtain the degree of Master of Science

at the Delft University of Technology,

to be defended publicly on Friday December 12, 2025 at 16:00.


| | | |
|---|---|---|
| Student number: | 5216443 | |
| Project duration: | September 23, 2024 – December 12, 2025 | |
| Thesis committee: | Prof. dr. G. Smaragdakis, | TU Delft, thesis advisor |
| | Dr. A. Voulimeneas, | TU Delft, supervisor |
| | Dr. N. Mohan, | TU Delft, external committee member |
| | Dr. E. Bassetti, | European Space Agency / TU Delft, daily supervisor |
| | Dr. A. Atlasis, | European Space Agency, external advisor |


Style: TU Delft Report Style, with modifications by Daan Zwaneveld

An electronic version of this thesis is available at http://repository.tudelft.nl/.


# Preface

First of all, I would like to sincerely thank Dr. Antonios Atlasis for giving me the opportunity to do my Master thesis in collaboration with the European Space Agency (ESA), as well as for all the feedback and supervision you have given to me throughout the entire thesis. I would also like to thank Augusto Marziani and Giovanni Serafini from the ESA 5G/6G Telecom Lab for the provided lab setup, and other people I have met at ESA for a wonderful experience.

Next, I want to express my deepest gratitude to my daily supervisor, Dr. Enrico Bassetti, for all your help during the thesis, for answering all my questions, for our joint trips to ESTEC, and for all the things you have explained to me outside my thesis based on your enormous experience in the IT field.

I also want to thank my thesis advisor, Prof. dr. Georgios Smaragdakis, for your supervision and for your guidance, especially at the times when I was stuck. In addition, I want to give separate thanks to Dr. Alexios Voulimeneas for your feedback and advice during the thesis.

Last but not least, I am incredibly thankful to my family, friends, fellow students, everyone from the TU Delft Cybersecurity research group, as well as everyone else who has helped and/or supported me throughout this long journey.

*Jegor Zelenjak*
*Delft, December 2025*

# Abstract

5G non-terrestrial networks (NTN) are getting increasing attention as a complementary solution to the currently deployed 5G terrestrial networks (TN) to provide global connectivity and ensure service continuity, service ubiquity, and service scalability. However, little research has been done into the security architecture of 5G NTN. This thesis aims to close this gap by summarizing the security architecture of 5G terrestrial networks and extending it to 5G non-terrestrial networks. In our security analysis, we are the first to perform a head-to-head comparison of four different NTN architectures (Transparent payload, Full gNB on board, Split CU-DU, and UE-Satellite-UE communication) with the first of its kind head-to-head comparison of the security architecture of 5G terrestrial and non-terrestrial networks.

In the practical part of the thesis, we implement a flooding attack against a 5G base station using OpenAirInterface (OAI), one of the largest open-source 5G network implementations, and evaluate the attack in a terrestrial and a non-terrestrial setup. In the performed experiments using real SDR devices (TN) and simulated LEO and GEO satellites with a transparent payload (NTN), we managed to make the base station permanently allocate more contexts than the defined threshold on the active connections, allowing an attacker to completely exhaust the available memory resources in the long run. Furthermore, we were able to reach the maximum number of allowed connections in the base station in all experiments except those with a GEO satellite, leading to a DoS of a legitimate subscriber.

# Contents

**Preface** i

**Abstract** ii

**Abbreviations** v

**1 Introduction** 1

**2 Background** 4
2.1 5G terrestrial networks . . . 4
2.1.1 Usage scenarios . . . 4
2.1.2 Softwarization of networks . . . 4
2.1.3 Architecture . . . 5
2.1.4 Communication and message flows . . . 8
2.1.5 Mobility management . . . 12
2.1.6 Deployment modes . . . 14
2.2 Satellites and the space ecosystem . . . 16
2.2.1 Overview . . . 16
2.2.2 Earth orbits . . . 17
2.2.3 Satellite operation segments . . . 18
2.3 5G non-terrestrial networks . . . 19
2.3.1 Overview . . . 19
2.3.2 Transparent payload . . . 20
2.3.3 Regenerative payload: Full gNB on board . . . 21
2.3.4 Regenerative payload: Split CU-DU . . . 21
2.3.5 UE-Satellite-UE communication . . . 22
2.3.6 Store and Forward satellite operation . . . 24

**3 Related work** 25
3.1 Security of 5G terrestrial networks . . . 25
3.2 Security of 5G non-terrestrial networks . . . 27
3.3 3GPP standardization efforts . . . 28
3.4 CNSA Suite . . . 29
3.5 Open research questions . . . 30

**4 Methodology** 32
4.1 Research questions . . . 32
4.2 Research scope . . . 33
4.3 Research approach . . . 34

**5 Security analysis of 5G terrestrial networks** 36
5.1 Security protections . . . 36
5.2 Cryptographic profiles for NDS/IP networks . . . 43
5.2.1 IPsec . . . 43
5.2.2 IKEv2 . . . 47
5.2.3 (D)TLS . . . 52
5.2.4 Ambiguities . . . 59
5.3 AS/NAS security . . . 60
5.4 ECIES profiles for SUCI . . . 64
5.5 Analysis of the literature attacks on 5G terrestrial networks . . . 66
5.6 Reflections . . . 70
5.6.1 Ambiguities in the standards . . . 70

5.6.2 Crypto agility . . . 71
5.6.3 Discrepancies between the standards and deployments . . . 72
5.6.4 Quantum threat . . . 73

**6 Security analysis of 5G non-terrestrial networks 77**
6.1 Security architecture of NTN scenarios . . . 77
6.1.1 NTN scenario 1: Transparent payload . . . 77
6.1.2 NTN scenario 2: Full gNB on board . . . 78
6.1.3 NTN scenario 3: Split CU-DU . . . 79
6.1.4 NTN scenario 4: UE-Satellite-UE communication . . . 80
6.2 Comparison of NTN scenarios . . . 81
6.3 Analysis of TN literature attacks in NTN . . . 82
6.4 Comparison of TN and NTN security architectures . . . 85
6.5 Reflections . . . 87

**7 Flooding attack against 5G terrestrial and non-terrestrial networks 88**
7.1 Attack description . . . 88
7.2 Experimental setup . . . 89
7.3 Attack prototype (UERANSIM) . . . 90
7.3.1 Experimental setup . . . 90
7.3.2 Results . . . 90
7.3.3 Reflections . . . 95
7.4 Attack implementation (OpenAirInterface) . . . 96
7.4.1 Experimental setup . . . 96
7.4.2 Results . . . 96
7.4.3 Reflections . . . 105
7.5 Attack evaluation (OpenAirInterface) . . . 105
7.5.1 Terrestrial setup . . . 106
7.5.2 Non-terrestrial setup . . . 108
7.5.3 Reflections . . . 112
7.6 Conclusions and mitigations . . . 113

**8 Discussion 115**
8.1 Security challenges in terrestrial and non-terrestrial networks . . . 115
8.2 Attacks on terrestrial and non-terrestrial networks . . . 116
8.3 Recommendations for terrestrial and non-terrestrial networks . . . 117
8.4 Limitations . . . 117

**9 Conclusion 119**
9.1 Summary . . . 119
9.2 Future work . . . 121

**References 122**

**A Example update of 3GPP security documents 147**
A.1 Cryptographic Profiles . . . 147
A.1.1 TS 33.210 . . . 147
A.1.2 TS 33.310 . . . 148
A.2 Security Architecture . . . 149
A.2.1 TS 33.501 . . . 149
A.3 Security Assurance Specifications . . . 149
A.3.1 TR 33.926 . . . 149
A.3.2 TS 33.511 . . . 150

**B Studied literature attacks on 5G terrestrial networks 151**

# Abbreviations

| Abbreviation | Definition |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 5GC | 5G Core |
| 5GMM | 5GS Mobility Management |
| 5GS | 5G System |
| 5GSM | 5GS Session Management |
| AEAD | Authenticated Encryption with Associated Data |
| AES | Advanced Encryption Standard |
| AF | Application Function |
| AKA | Authentication and Key Agreement |
| AMF | Access and Mobility Management Function |
| AS | Access Stratum |
| AUSF | Authentication Server Function |
| CN | (5G) Core Network |
| CNSA | Commercial National Security Algorithm (Suite) |
| COTS | Commercial Off-The-Shelf |
| C-RNTI | Cell Radio Network Temporary Identifier |
| CRQC | Cryptographically Relevant Quantum Computer |
| CSI | Channel State Information |
| CU | Central Unit |
| CUPS | CP and UP Separation |
| DCI | Downlink Control Information |
| DL | Downlink |
| DN | Data Network |
| DNN | Data Network Name |
| DoS | Denial-of-Service |
| DRB | Data Radio Bearer |
| DTLS | Datagram Transport Layer Security |
| DU | Distributed Unit |
| ECIES | Elliptic Curve Integrated Encryption Scheme |
| eMBB | Enhanced Mobile Broadband |
| EPC | Evolved Packet Core |
| ESP | Encapsulating Security Payload |
| FBS | Fake Base Station |
| FIPS | Federal Information Processing Standard |
| GEO | Geostationary Earth Orbit |
| gNB-CU | gNB-Central Unit |
| gNB-DU | gNB-Distributed Unit |
| gNB | gNodeB |
| GPRS | General Packet Radio System |
| GSM | Global System for Mobile Communications (2G) |
| GTP-U | GPRS Tunnelling Protocol User Plane |
| GUTI | Globally Unique Temporary UE Identity |
| GW | Gateway |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |
| IKEv2 | Internet Key Exchange version 2 |
| IMEI | International Mobile station Equipment Identity |

| Abbreviation | Definition |
|---|---|
| IMSI | International Mobile Subscription Identity |
| IMS | IP Multimedia Subsystem |
| IoT | Internet of Things |
| IPsec | Internet Protocol Security |
| ISL | Inter-Satellite Link |
| ITU | International Telecommunication Union |
| LEO | Low Earth Orbit |
| LTE | Long Term Evolution (4G) |
| MAC | Media Access Control, Message Authentication Code |
| MCC | Mobile Country Code |
| ME | Mobile Equipment |
| MEO | Medium Earth Orbit |
| MIB | Master Information Block |
| mMTC | Massive Machine-type Communications |
| MNC | Mobile Network Code |
| MNO | Mobile Network Operator |
| MSIN | Mobile Subscriber Identification Number |
| NAS | Non-Access Stratum |
| NDS | Network Domain Security |
| NEF | Network Exposure Function |
| NF | Network Function |
| NFV | Network Function Virtualization |
| NGAP | NG Application Protocol |
| NG | Next Generation |
| NG-RAN | Next Generation Radio Access Network |
| NIST | National Institute of Standards and Technology |
| NRF | Network Repository Function |
| NR | New Radio |
| NSA | National Security Agency |
| NSA | Non-standalone (deployment) |
| NSS | National Security System |
| NTN | Non-Terrestrial Network |
| OAI | OpenAirInterface |
| O-RAN | Open RAN |
| PCF | Policy Control Function |
| PDCP | Packet Data Convergence Protocol |
| PDU | Protocol Data Unit |
| PEI | Permanent Equipment Identifier |
| PKI | Public Key Infrastructure |
| PLMN | Public Land Mobile Network |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RA | Random Access |
| RAR | Random Access Response |
| RAT | Radio Access Technology |
| RFC | Requests for Comments |
| RF | Radio Frequency |
| RLC | Radio Link Control |
| RLS | Radio Link Simulation |
| RNA | RAN-based Notification Area |
| RNTI | Radio Network Temporary Identifier |
| RRC | Radio Resource Control |
| SAD | Security Association Database |
| SA | Standalone (deployment) |

| Abbreviation | Definition |
|---|---|
| SBA | Service-Based Architecture |
| SBI | Service-Based Interface |
| SDAP | Service Data Adaptation Protocol |
| SDO | Standardization Development Organization |
| SDR | Software Defined Radio |
| SEPP | Security Edge Protection Proxy |
| SIB | System Information Block |
| SI | System Information |
| SMF | Session Management Function |
| SMS | Short Message Service |
| SPD | Security Policy Database |
| SP | Special Publication |
| SRB | Signalling Radio Bearer |
| SRI | Satellite Radio Interface |
| SR | Scheduling Request |
| SRS | Sounding Reference Signal |
| SUCI | Subscription Concealed Identifier |
| SUPI | Subscription Permanent Identifier |
| TAC | Tracking Area Code |
| TAL | Tracking Area List |
| TA | Tracking Area, Timing Advance |
| TLS | Transport Layer Security |
| TMSI | Temporary Mobile Subscriber Identity |
| TN | Terrestrial Network |
| TR | Technical Report |
| TS | Technical Specification |
| UAS | Unmanned Aircraft System |
| UAV | Unmanned Aerial Vehicle |
| UDM | Unified Data Management |
| UDP | User Datagram Protocol |
| UDR | Unified Data Repository |
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| UL | Uplink |
| UMTS | Universal Mobile Telecommunications System (3G) |
| UPF | User Plane Function |
| URLLC | Ultra-Reliable and Low Latency Communications |
| (U)SIM | (Universal) Subscriber Identity Module |
| USRP | Universal Software Radio Peripheral |

# 1

# Introduction

Recent technological advancements in cellular networks and mobile devices have massively increased and continue increasing our consumption of mobile data. In June 2024, Ericsson, a leading communications service provider, estimated that the total monthly global mobile network data traffic reached 145 exabytes (EB), or $10^{18}$ bytes, with the quarter-on-quarter growth of approximately 6% between Q4 2023 and Q1 2024 [144]. According to the report, such traffic growth is caused by two factors: an increasing number of smartphone subscriptions and increasing average data volume per subscription. The latter is driven mainly by increased consumption of video content, which accounted for 73% of all mobile data traffic at the end of 2023. In 2029, the total global mobile data traffic is estimated to increase by about three times, reaching 313 EB per month. If traffic generated by Fixed Wireless Access (FWA) is also included, then this estimate is 466 EB.

At the same time, deployment of 5G, or the fifth generation technology, is actively taking place. During the first quarter of 2024 alone, the number of 5G subscriptions increased by 160 million, exceeding a total of 1.7 billion [144]. In the same time period, subscriptions for 2G, 3G and 4G dropped by 41 million, 37 million and 26 million, respectively. In May 2024, it was estimated that about 300 service providers had started offering commercial 5G services. The leader in 5G subscription penetration is North America, covering 59% at the end of 2023, with the expectation of reaching 90% in 2029. The projections show that in 2028, 5G will be the dominant mobile access technology, with the estimate of 5.6 billion subscriptions in 2029, or 60% of all mobile subscriptions.

The earlier generations of cellular mobile technologies, from 1G in 1981, 2G in 1992 (Global System for Mobile Communications, or GSM), 3G in 2001 (Universal Mobile Telecommunications System, or UMTS) to 4G in 2009/2011 (Long Term Evolution (LTE)/LTE Advanced), aimed primarily at providing connectivity, with each generation being an improvement over the previous one and offering more connectivity than ever before [275, 333]. However, 5G, with its first deployments in 2019, is not only about serving consumer or enterprise subscribers with high-throughput connectivity and delivering peak data rates up to 20 Gbps (based on IMT-2020 requirements). It is able to meet the requirements for new enterprise use cases and offer new opportunities to operators and businesses. 5G opens four business horizons: improved services for existing use cases with Enhanced Mobile Broadband (eMBB), reduced operational costs and maximized capital expenditure using FWA, differentiated connectivity solutions for consumers or enterprises by leveraging public and private networks, and new value opportunities and ecosystem growth thanks to programmable networks [143]. Mobile ecosystem will expand to new industries, such as automotive industry, drones, healthcare, smart cities, and virtual reality [333, 388].

Despite new opportunities associated with 5G deployment, there are also new security challenges. Due to many interconnections with other systems, networks, and applications (e.g. third party service providers), a 5G mobile network is more likely to be attacked compared to 2G, 3G, and 4G networks, and its attack surface is much larger [225]. A successful attack on a 5G system may lead to more severe repercussions, as it is used by many different services, including those that involve human lives (e.g. connected vehicles, remote surgery). Furthermore, given the new requirements and use cases for

5G, the impact of some threats from previous 4G systems is higher [187]. For example, with massive Machine-to-Machine communications, the interaction with a human user is limited, hindering certain attack mitigation measures. New challenges have also been created by network function virtualizations (NFV) and cloud deployments, which assume certain trust relationships between the network operators and cloud service providers. Finally, to meet certain performance requirements, mobile network operators (MNO) may be tempted to disable some security mechanisms, such as user data encryption.

With the exponentially increasing number of mobile devices, the ever-increasing demand for new services, and desired Quality of Service (QoS) anytime and everywhere (including rural and highly dense areas, vessels, high-speed trains, and aeroplanes), there is a greater interest into 5G non-terrestrial networks (NTN) to complement terrestrial networks (TN) in serving uncovered or under-served geographical areas [344]. The recent technological advancements in satellite networks and NTN have addressed certain limitations related to aerial connectivity, which resulted in considerable performance improvements, lower deployment expenses, and more profitable business models relying on NTN-based connectivity solutions [174]. While TNs currently cover more than 95% of the global population, their coverage of the world's landmass is less than 45%. Aerial connectivity solutions can offer ubiquitous coverage across the entire globe, including maritime, remote and polar areas, where deploying traditional TNs is expensive and challenging, as well as during disasters and outages of TNs.

Next to all the benefits of global connectivity and resilience against natural disasters and physical attacks provided by NTN, integrating 5G networks with satellites also introduces additional security challenges. The space industry has been attacked by various types of adversaries with different motivations since its very beginning, with the attacks like jamming and eavesdropping of the communication channel, satellite hijacking, signal spoofing, buffer overflows, Denial-of-Service (DoS), and supply chain attacks [247, 62, 147]. An ongoing trend of using Commercial Off-the-Shelf (COTS) hardware and software components for satellites to decrease construction times and costs exposes them to all kinds of well-known cyberattacks [407]. Furthermore, our growing reliance on the services delivered by Satellite Communications (Satcoms) systems makes them a singular point of vulnerability, as their failure could result in disruption of many critical services and can have severe consequences, from communication loss to sensitive data disclosure [350]. As a result, space-based systems have turned into attractive targets for diverse types of adversaries, including commercial competitors, criminal groups seeking financial gain, terrorist organizations aiming to promote their causes, and nation-state military actors [243, 172], as seen from examples of real-world cyberattacks against the space infrastructure [172, 98, 401].

Despite the importance of cybersecurity in space-based systems, little research been done into the security architecture of 5G NTN, which motivates the need for further exploration of this field. In this thesis, we perform an extensive security analysis of the architecture of 5G terrestrial and non-terrestrial networks, as standardized by the 3rd Generation Partnership Project (3GPP), the major Standardization Development Organization (SDO) for 5G. In particular, our work aims to answer the following three research questions:

1. **"What is the current security architecture of 3GPP 5G terrestrial networks?"**
2. **"What is the current security architecture of 3GPP 5G non-terrestrial networks?"**
3. **"Can we successfully perform a flooding attack against gNB in 3GPP 5G terrestrial and non-terrestrial networks?"**

By extensively reviewing the security mechanisms proposed by 3GPP together with their usage requirement levels and cryptographic profiling, we summarized the security architecture of 5G terrestrial networks. Based on the identified protection measures, we extended this security architecture to 5G non-terrestrial networks and compared different NTN deployment scenarios with each other. We also analysed the impact of some TN literature attacks in an NTN setting, and performed a head-to-head comparison of terrestrial and non-terrestrial networks from the security perspective. Finally, we demonstrated a flooding attack using OpenAirInterface (OAI) in a TN and an NTN setup, successfully reaching the maximum allowed number of connections in all experiments except with a (simulated) GEO satellite, while also permanently allocating more RRC contexts in the gNB than the defined threshold.

Specifically, we make the following contributions into the research field of 5G TN and NTN security:

- We perform an extensive analysis of the 3GPP security architecture for 5G terrestrial networks, focusing on 10 non-SBI interfaces affected by the non-terrestrial deployments, and review the corresponding cryptographic profiles proposed by 3GPP.
- We summarize the identified security mechanisms and protection requirements into a single diagram representing the security architecture of 5G terrestrial networks.
- We compare the cryptographic profiles in the 3GPP specifications to the requirements and recommendations of NIST and NSA's CNSA 1.0 and 2.0 Suites.
- We summarize and analyse 30 literature attacks against 5G terrestrial networks, targeting weaknesses in the 3GPP specifications, and reflect on the impact and/or feasibility for each of them; we further discuss six selected attacks including the possible mitigations.
- We map the identified security mechanisms and protection requirements to four different 5G non-terrestrial deployment scenarios and summarize this information in the corresponding diagrams representing the security architecture of 5G non-terrestrial networks.
- We perform the first (to the best of our knowledge) head-to-head comparison of four different 5G non-terrestrial network architectures (Transparent payload, Full gNB on board, Split CU-DU, and UE-Satellite-UE communication) in terms of their security benefits and drawbacks.
- We analyse the impact of the six selected literature attacks against 5G terrestrial networks in the context of 5G non-terrestrial networks.
- We are the first (to the best of our knowledge) to present a head-to-head comparison between 5G terrestrial and non-terrestrial networks from the perspective of their security architecture.
- We implement a flooding attack against the gNB (based on a prior LTE attack [215]) using UERANSIM (for the attack prototype) and OpenAirInterface (for the actual attack), and evaluate it in a terrestrial setting using OAI with real SDR devices and in a non-terrestrial setting using the OAI RF simulator with the NTN-specific configuration to simulate GEO and LEO satellites with a transparent payload.

The rest of the thesis is structured as follows. First, chapter 2 provides the background information about the 3GPP 5G terrestrial networks, including the main entities and procedures, gives a general overview of the satellite ecosystem, and introduces the 3GPP 5G non-terrestrial networks. Next, chapter 3 discusses the relevant literature works on the security of 5G terrestrial and non-terrestrial networks, lists the main 3GPP standardization efforts, and identifies the research gaps. Then, chapter 4 describes the methodology of our work, including the research questions and subquestions, the scope, and the research approach. The core of our thesis is split into three chapters: the two theoretical parts in chapter 5 and chapter 6 present the security analysis of 5G terrestrial and non-terrestrial networks, while the practical part in chapter 7 presents the results of our flooding attack using UERANSIM (the attack prototype) and OpenAirInterface (the actual attack). Finally, chapter 8 reflects on the main findings and limitations of our work, while chapter 9 summarizes the answers to the stated research questions and proposes possible directions for future work.

# 2

# Background

This chapter presents the background information that can help the reader better understand 5G networks and make it easier to follow the rest of the thesis. In order to perform a security analysis of the 5G NTN architecture, we need to first understand the 5G TN architecture and the main network entities in a 5G system. Furthermore, we need to have a general understanding of the satellite ecosystem because it affects the architecture of NTN. Finally, we need to understand what NTNs are and what deployment scenarios have been proposed by 3GPP. In the following sections, we introduce all these new concepts. Note that physical layer security is outside the scope of this thesis, so we do not present the 5G enabling technologies such as mmWave, massive MIMO, and beamforming. Interested reader is invited to consult the corresponding papers, for example [63] by Agiwal et al.

## 2.1. 5G terrestrial networks

In this section, we give an overview of 3GPP 5G TN. We start by listing the main 5G usage scenarios and explaining the concept of softwarization and network slicing in 5G networks. Next, we present the architecture for 5G TN, describe the main network functions, show the main message flows, and explain some concepts for mobility management. Finally, we wrap up this section by discussing possible deployment modes of 5G networks.

### 2.1.1. Usage scenarios

The radiocommunication sector of International Telecommunication Union (ITU), or ITU-R, has defined three main usage scenarios for 5G [149]:

1. **Enhanced Mobile Broadband (eMBB)** aims to satisfy the requirements for hotspot scenarios given extremely high data rates, high user density, and very high traffic capacity, as well as to improve data rates and provide seamless coverage in high mobility scenarios.
2. **Massive Machine-type Communications (mMTC)** aims to satisfy the low power consumption requirements of a very large number of connected Internet of Things (IoT) devices.
3. **Ultra-Reliable and Low Latency Communications (URLLC)** aims to satisfy the strict latency and reliability requirements of safety-critical and mission-critical applications.

Figure 2.1 shows which aspects have higher importance for each of the three 5G usage scenarios [149]. For the requirements in NTN scenarios (specifically, for the satellite radio interface), see Figure 2.10.

### 2.1.2. Softwarization of networks

Telecommunication networks remain an indispensable part of any society that pursuits economic growth and social prosperity [60]. Millions of people rely upon telecommunication services on a daily basis. These networks have to evolve continuously in order to handle higher data loads and a wide range of services. With this evolution, the underlying technology also changes, resulting in a higher degree of programmability, higher configuration control and flexibility, and lower operational costs.

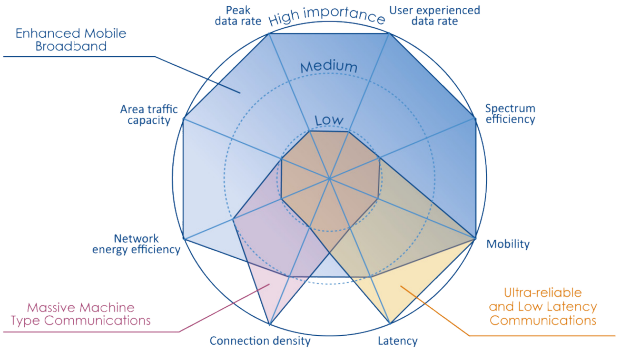



**Figure 2.1:** Three main 5G usage scenarios, as defined by ITU-R [149].

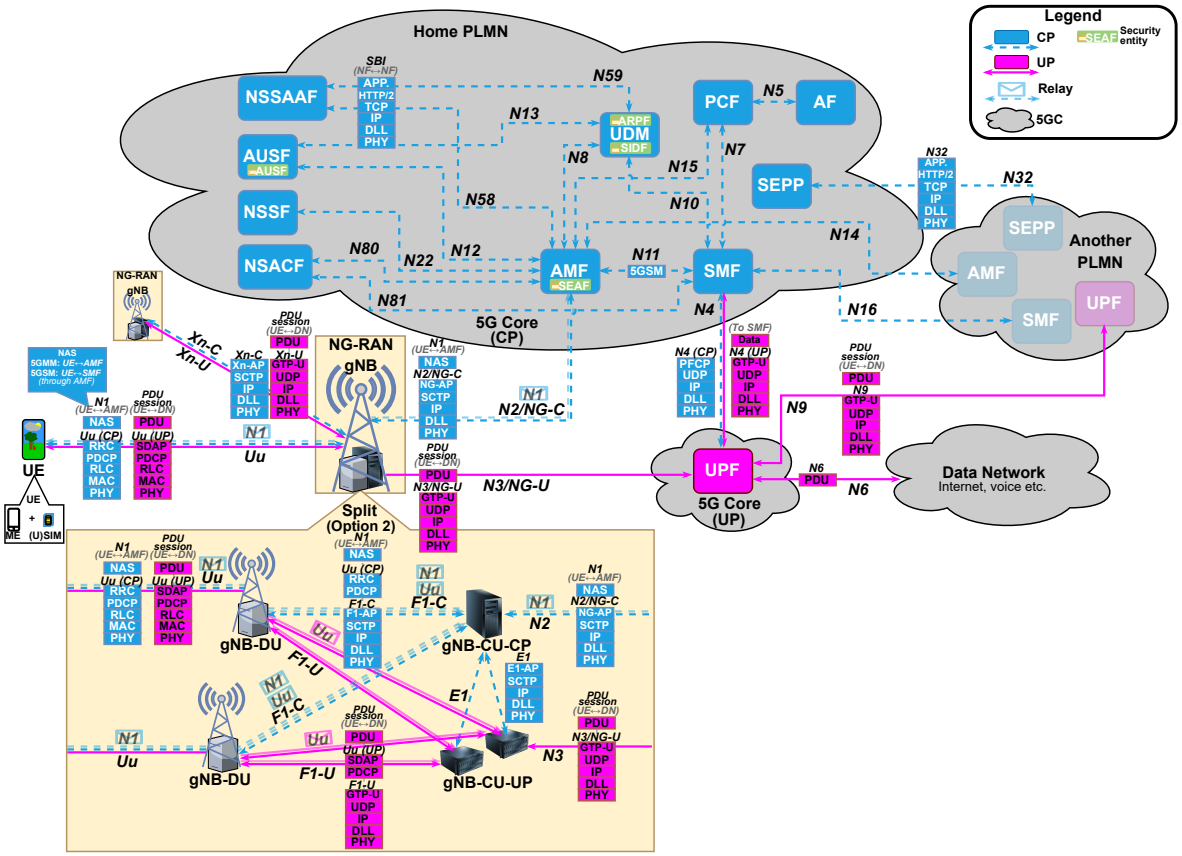
Apart from the evolution of mobile broadband network with the increased network speed and reliability, 5G transforms the network infrastructure and telecommunication technologies with Software Defined Networking (SDN) and Network Function Virtualization (NFV) [60]. SDN and NFV aim to decouple network functions (NFs) from proprietary hardware, offering them as virtualized software elements, and to decouple services from proprietary service platforms. Such softwarization helps to optimize operational processes, lower operational network costs and required infrastructure investments, as well as reduce the time to market for new services, resulting in a higher flexibility for network operators. Similar to the shift towards cloud computing in software and IT services, telecom architecture shifts from boxes to functions and from protocols to APIs.

As a result of SDN and NFV, network operators can split their network capacity and elements into virtual slices, which can then be utilized for various use cases [60]. This is called network slicing, and it is a key enabler for offering flexible, cost-efficient and customized services in 5G networks [395]. It is a way to create multiple independent logical networks over the same physical infrastructure with the required QoS guarantees based on the customer needs. This shift from a static and well-understood architecture towards a dynamic architecture based on multiple use cases is driven by business considerations of operators [59]. An operator can sell parts of their infrastructure to customers, such as industry verticals, factories, or even other operators. Not only does it help network operators reduce their costs as a result of maximized sharing of network resources, it also provides a lot of flexibility for creating dedicated logical networks in order to meet specific customer requirements [395]. The configurable QoS guarantees result in opportunities for new markets and various new use cases.

### 2.1.3. Architecture

Three main entities are involved in a 5G System (5GS) [19, 27, 58, 33, 187, 246, 363, 335, 377, 137]: User Equipment (UE), Next Generation Radio Access Network (NG-RAN), and 5G Core Network (5GC). The 5G architecture itself consists of NG-RAN and 5GC. Below, we present the involved entities and the architecture of a 5G terrestrial network (see Figure 2.2 for a visual overview).

**User Equipment (UE)**. UE consists of two parts: the Mobile Equipment (ME) and the Universal Integrated Circuit Card (UICC), which is a physically secure device that stores the (Universal) Subscriber Identity Module, or (U)SIM, either as a separate hardware element or embedded into the main chipset. The (U)SIM holds the subscription details of the user and the long-term root key used in the initial registration to the network to derive the subsequent integrity and confidentiality protection keys. On the network operator side, this key is stored in the UDM in the core network and is used for key derivations on the 5GC side. With the help of a UE, mobile subscribers can make use of the services offered by MNOs. However, a UE does not necessarily have to be a mobile device offering standard data or voice services to the subscribed user. It can also be a device used for Machine-to-Machine (M2M) communications or an IoT device. Depending on the UE type, it might have different characteristics, such as data rates or power supply, and different QoS requirements.




| 5G Abbreviations | | |
|---|---|---|
| 5GC: 5G Core | GTP: GRPS Tunneling Protocol | RRC: Radio Resource Control |
| 5GMM: 5GS (5G System) Mobility Management | HTTP: Hypertext Transfer Protocol | RU: Radio Unit |
| 5GSM: 5GS Session Management | IP: Internet Protocol | SBI: Service-Based Interface |
| AF: Application Function | ME: Mobile Equipment | SCTP: Stream Control Transmission Protocol |
| AP: Application Protocol (e.g. F1-AP, NG-AP, Xn-AP, E1-AP etc.) | NAS: Non-Access Stratum | SDAP: Service Data Adaptation Protocol |
| AMF: Access and Mobility Management Function | NG: Next Generation | SEPP: Security Edge Protection Proxy |
| ARPF: Authentication credential Repository and Processing Function | NSSAAF: Network Slice Specific Authentication and Authorization | SEAF: SEcurity Anchor Function |
| AS: Access Stratum | NSSF: Network Slicing Selection Function | SIDF: Subscription Identifier Deconcealing Function |
| AUSF: AUthentication Server Function | PCF: Policy Control Function | SMF: Session Management Function |
| CP: Control Plane | PDCP: Packet Data Convergence Protocol | TCP: Transmission Control Protocol |
| CU: Central Unit | PDU: Protocol Data Unit | TLS: Transport Layer Security |
| DLL: Data Link Layer | PFCP: Packet Forwarding Control Protocol | UDM: Unified Data Management |
| DN: Data Network | PHY: Physical Layer | UE: User Equipment |
| DU: Distributed Unit | PLMN: Public Land Mobile Network | UDP: User Datagram Protocol |
| gNB: gNodeB | RAN: Radio Access Network | UP(F): User Plane (Function) |
| GPRS: General Packet Radio Service | RLC: Radio Link Control | (U)SIM: (Universal) Subscriber Identity Module |

**Figure 2.2:** Architecture of a 5G terrestrial network (based on [27, 58, 187, 246, 363]).

**Next Generation Radio Access Network (NG-RAN)**. NG-RAN is based on gNodeB (gNB) and provides wireless connectivity for the UE to access the data network (DN) through the 5GC. The base stations (gNBs) in NG-RAN are separated into different Tracking Areas (TAs). The gNB implements the radio interface called Uu to communicate with the UE and the NG interface to communicate with the 5GC. It splits the data received from the UE into Control plane (CP) and User Plane (UP) segments and forwards them to the corresponding endpoints in the 5GC. In addition to the traditional monolithic gNB architecture, 3GPP has defined a split architecture, where the gNB can be split into two components (the so-called split option 2):

- **gNB-Distributed Unit (gNB-DU or DU)**. gNB-DU includes the physical radio interface and is responsible for serving the lower layers of the 5G New Radio (NR) protocol stack (namely, physical (PHY), Media Access Control (MAC), and Radio Link Control (RLC) layers) in order to handle the real-time scheduling functions. The gNB-DU is not supposed to have access to user communications, since it is likely to be deployed in unsupervised locations. One gNB-DU can support one or multiple cells, but one cell can be supported by only one gNB-DU.
- **gNB-Central Unit (gNB-CU or CU)**. gNB-CU is responsible for serving the upper layers of the 5G NR protocol stack (namely, Radio Resource Control (RRC), Packet Data Convergence Protocol (PDCP), and Service Data Adaptation Protocol (SDAP) layers) in order to handle non-real-time scheduling functions. Since the gNB-CU terminates the Access Stratum (AS) security, it should be deployed in a safeguarded location. The gNB-CU controls the operation of one or multiple gNB-DUs, and can be further split into gNB-CU-CP hosting the CP part of the PDCP protocol, and gNB-CU-UP hosting the UP part of the PDCP protocol (split option 2-2 [47, 52]).

**5G Core Network (5GC, CN)**. 5GC connects the UE to the DN, so that it can get the desired services, such as Internet or voice. It supports the CP and UP separation (CUPS), which is an enhancement to improve the scalability of the UP and increase the flexibility for the operators in managing their networks. The network architecture of 5GC is service-based (SBA): a service producer NF uses a service-based interface (SBI) based on an API connection to provide a service to an authorized service consumer NF. All CP communications over the SBI are transmitted via RESTful APIs in a JavaScript Object Notation (JSON) format, over HTTP/2 over TCP/IP. On non-SBI interfaces, the CP data is carried over SCTP (N2) or UDP (N4), and the UP data is sent over UDP (N3, N4, N9), encapsulated in the General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTP-U) protocol [13].

Figure 2.2 shows the 5G network architecture, with a selection of NFs shown in the 5GC. Note that the core network is presented using a reference architecture instead of SBA in order to better highlight the interfaces between the displayed NFs. In chapter 5 we revise this architecture diagram and include the security measures and the protection requirements on different interfaces (see Figure 5.1).

3GPP TS 23.501 [58] defines around 30 NFs for the core network of a 5G system. Below we present a selection of these NFs together with their main purposes [58, 187, 246, 363, 377, 382]:

- **Access and Mobility Management Function (AMF)**: AMF manages all signalling not specific to the user data (e.g. registration, authentication, mobility between tracking areas, and security). It is the first 5GC NF accessed by UE during registration and authentication. It also contains the Security Anchor Function (SEAF) which grants the UE access to the home network. AMF communicates with the UE on the logical N1 interface via NAS messages, and with the gNB (access network) on the N2 interface via NGAP messages. In 5GC, it acts as termination point for the NAS security.
- **Session Management Function (SMF)**: SMF handles control signalling associated with user data traffic, such as session establishment, management, and proper coordination. It selects the UPF to serve a UE, passes the required QoS parameters to the UPF, manages and supervises the interface between CP and UP, and assigns IP addresses to UEs when creating a PDU session. In addition, it interacts with PCF for policy decisions about QoS, and is responsible for downlink data notification.
- **User Plane Function (UPF)**: UPF handles user data and the QoS for the UP, buffers downlink data, as well as routes and forwards packets. Moreover, it connects a UE to the DN (e.g. voice, Internet or other services) for a PDU session, and serves as a UP collection point during a lawful intercept. UPF is the only NF in the UP in the 5GC.
- **Unified Data Management (UDM)**: UDM provides the subscriber details of a given UE during au-

thentication, roaming, and network access. It also stores the long-term keys and the related shared secrets used in authentication and key derivation. Furthermore, it stores the private key to derive the SUPI from a SUCI, and the identity of the NFs currently handling the UE.

- **Authentication Server Function (AUSF)**: AUSF is responsible for the UE authentication with the network. It fetches the long-term keys from the UDM, and transmits the derived keys and other input parameters to the AMF (namely, to its key derivation function). Upon successful authentication, it sends the SUPI associated to the authentication session to the AMF (SEAF).
- **Policy Control Function (PCF)**: PCF delivers policy controls for service data flows and PDU sessions, and performs dynamic policy decisions, depending on the network conditions, such as congestion, or subscriber location. It also manages service areas, i.e. a list of allowed and not allowed TAs. PCF can interact with the AMF and SMF, and it decides how a flow is charged.
- **Service Communication Proxy (SCP)**: SCP provides a means for indirect communications between CP NFs in the API-based interface.
- **Security Edge Protection Proxy (SEPP)**: SEPP filters and transmits messages between serving (visited) and home networks, and authenticates the other SEPP that it talks to. Importantly, it hides the internal network topology from other networks.
- **Unified Data Repository (UDR)**: UDR provides storage for subscription data used by the UDM and for policy data used by the PCF. UDR can consist of one or several instances.
- **Network Repository Function (NRF)**: NRF maintains a repository of NFs in the core network with their configuration data (e.g. their location and associated network slices). It offers a discovery service for NFs: it receives a discovery request for a NF and returns the IP addresses or domain names of the servers for that NF. It can also act as an authorization server based on the OAuth2 protocol and give access tokens to an authorized client. NRF is not used if the core network topology is static.
- **Application Function (AF)**: AF externally interacts with the core network (e.g. influencing the traffic routing, interacting with the PCF, or the IP Multimedia Subsystem (IMS) interactions with the 5GC).
- **Network Exposure Function (NEF)**: NEF exposes some information (e.g. capabilities and events) about 5GC NFs to an external (unauthorized) AF. It acts like a firewall: for the AFs outside the trust boundary of the 5GC, it only serves those requests that pass its rules.
- **Network Slice Selection Function (NSSF)**: NSSF provides the mapping of requested network slices to the supported ones. It is invoked when a UE requests a list of network slices (during the registration and possibly during PDU service requests). NSSF can also trigger a reselection of an AMF for a particular service by returning the network slice and the AMF for that service.
- **Network Slice Admission Control Function (NSACF)**: NSACF provides the monitoring and controlling of the number of registered UEs and the number of established PDU sessions per network slice. It also supports event-based network slice status notification and reports to a consumer NF.
- **Network Slice Specific Authentication and Authorization Function (NSSAAF)**: NSSAAF provides support for network slice-specific authentication and authorization with an Authentication, Authorization, and Accounting (AAA) server for particular network slice identified by an S-NSSAI, after a successful primary authentication of the UE.
- **Network Data Analytics Function (NWDAF)**: NWDAF collects data from NFs and AFs, and provides analytics information to NFs and AFs.

### 2.1.4. Communication and message flows

Whenever a UE wants to use the data services of a 5G network, it has to establish a Protocol Data Unit (PDU) session [382]. A PDU session is an association between the UE and an external DN that offers a PDU connectivity service, i.e. a service which allows the UE to be a member of the DN through a 5G network [58, 225]. A UE with an active PDU session has an identification address in the DN addressing scheme and can exchange data with the DN via a PDU transfer (where PDU indicates any block of data, e.g. IPv4, IPv6, IPv4v6, Ethernet, or Unstructured). A PDU session may consist of one or multiple QoS flows, e.g. for Internet and voice services [382]. After the UP communication channel has been set up by the gNB, the UE has an active PDU session and can send data to and receive data from the DN [363]. Subsequently, if desired, the UE can deregister from the 5G network.

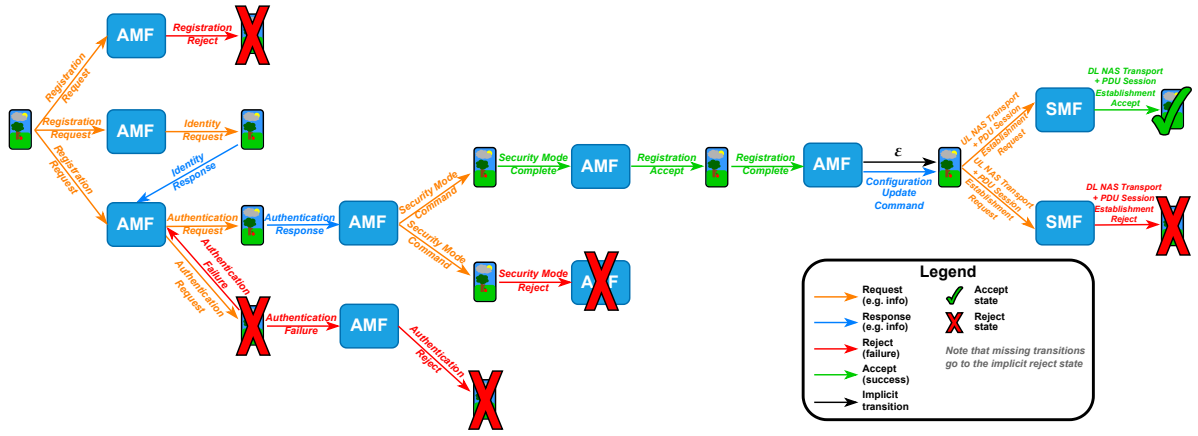



**Figure 2.3:** A non-deterministic finite automaton of the NAS message flows in a 5G system (based on [363]).

| Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 5.624 | gNB | UE | NR RRC | MIB |
| 5.624 | gNB | UE | NR RRC | SIB1 |
| 5.625 | UE | gNB | NR RRC | RRC Setup Request |
| 5.625 | gNB | UE | NR RRC | RRC Setup |
| 5.625 | UE | gNB | NR RRC/NAS-5GS | RRC Setup Complete, Registration request |
| 5.625 | gNB | AMF | NGAP/NAS-5GS | InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] |
| 5.671 | AMF | gNB | NGAP/NAS-5GS | SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request |
| 5.671 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Authentication request |
| 5.672 | UE | gNB | NR RRC/NAS-5GS | UL Information Transfer, Authentication response |
| 5.672 | gNB | AMF | NGAP/NAS-5GS | SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response |
| 5.701 | AMF | gNB | NGAP/NAS-5GS | SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command |
| 5.701 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Security mode command |
| 5.702 | UE | gNB | NR RRC/NAS-5GS/NAS-5GS | UL Information Transfer, Security mode complete, Registration request |
| 5.702 | gNB | AMF | NGAP/NAS-5GS/NAS-5GS | SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request |
| 5.833 | AMF | gNB | NGAP/NAS-5GS | SACK (Ack=2, Arwnd=106496) , InitialContextSetupRequest, Registration accept |
| 5.833 | gNB | AMF | NGAP | SACK (Ack=2, Arwnd=106496) , InitialContextSetupResponse |
| 5.833 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Registration accept |
| 5.834 | UE | gNB | NR RRC/NAS-5GS | UL Information Transfer, Registration complete |
| 5.834 | UE | gNB | NR RRC/NAS-5GS | UL Information Transfer, UL NAS transport, PDU session establishment request |
| 5.834 | UE | gNB | NR RRC/NAS-5GS | UL Information Transfer, UL NAS transport, PDU session establishment request |
| 6.040 | gNB | AMF | NGAP/NAS-5GS | UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request |
| 6.040 | AMF | gNB | NGAP/NAS-5GS | SACK (Ack=6, Arwnd=106294) , DownlinkNASTransport, Configuration update command |
| 6.041 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Configuration update command |
| 6.073 | AMF | SMF | HTTP2/JSON/NAS-5GS | DATA[1], JSON (application/json), PDU session establishment request |
| 6.154 | SMF | AMF | HTTP2/JSON/NAS-5GS/NGAP | DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer |
| 6.155 | AMF | gNB | NGAP/NAS-5GS | PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept |
| 6.159 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, DL NAS transport, PDU session establishment accept |
| 6.159 | gNB | AMF | NGAP | SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse |
| 6.181 | AMF | SMF | HTTP2/JSON/NAS-5GS | DATA[1], JSON (application/json), PDU session establishment request |
| 6.285 | AMF | SMF | HTTP2/JSON/NGAP | DATA[1], JSON (application/json), PDUSessionResourceSetupResponseTransfer |
| 6.291 | SMF | AMF | HTTP2/JSON/NAS-5GS/NGAP | DATA[1], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer |
| 6.292 | AMF | gNB | NGAP/NAS-5GS | SACK (Ack=7, Arwnd=106496) , PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept |
| 6.295 | gNB | AMF | NGAP | SACK (Ack=5, Arwnd=106496) , PDUSessionResourceSetupResponse |
| 6.295 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, DL NAS transport, PDU session establishment accept |
| 6.303 | AMF | SMF | HTTP2/JSON/NGAP | DATA[1], JSON (application/json), PDUSessionResourceSetupResponseTransfer |
| 13.880 | UE (PDU) | google.com | ICMP | Echo (ping) request id=0x0003, seq=1/256, ttl=64 (reply in 2717) |
| 13.880 | UPF | google.com | ICMP | Echo (ping) request id=0x0003, seq=1/256, ttl=63 (reply in 2715) |
| 13.884 | google.com | UPF | ICMP | Echo (ping) reply id=0x0003, seq=1/256, ttl=118 (request in 2714) |
| 13.884 | google.com | UE (PDU) | ICMP | Echo (ping) reply id=0x0003, seq=1/256, ttl=117 (request in 2712) |
| 14.272 | gNB | UE | NR RRC | MIB |
| 14.272 | gNB | UE | NR RRC | SIB1 |
| 16.551 | UE | gNB | NR RRC/NAS-5GS | UL Information Transfer, Deregistration request (UE originating) |
| 16.552 | gNB | AMF | NGAP/NAS-5GS | UplinkNASTransport, Deregistration request (UE originating) |

**Figure 2.4:** Wireshark capture with the message flows for UE registration, PDU session establishment, and UE deregistration (obtained using UERANSIM [178] with free5GC [241]).

Essential CP protocols for communications between the UE and the 5GC through the NG-RAN are Non-Access Stratum (NAS) [25] and NG Application Protocol (NGAP) [22] [363]. They are used during UE registration to the network, PDU session establishment, handover process, and UP configuration. Upon successful UE registration, they participate in QoS management, UP link creation, and UE mobility management. The two NAS protocols are the 5GS mobility management (5GMM) protocol between the UE and the AMF, and the 5GS session management (5GSM) protocol between the UE and the SMF through the AMF (specifically, 5GSM messages are piggybacked to specific 5GMM transport messages) [25]. 5GMM is responsible for controlling mobility when the UE is using the NG-RAN (or a non-3GPP access network, or both) and controlling security for the NAS protocols. The 5GSM is responsible for handling 5GS PDU sessions and controlling the UP resources together with the bearer control provided by the AS. NAS messages are carried by RRC between the UE and the gNB, with both RRC and NAS messages transmitted using Signalling Radio Bearers (SRBs) [30], and by NGAP between the gNB and the AMF. Figure 2.3 shows the possible NAS message flows (successful and unsuccessful) for the UE registration to a 5G network and the PDU session establishment [363]. A successful message flow, from the UE registration until its deregistration, is shown in a Wireshark capture in Figure 2.4 with the corresponding flow graph in Figure 2.5.


**Figure 2.5:** Wireshark flow graph for the message flows for UE registration, PDU session establishment, and UE deregistration (obtained using UERANSIM [178] with free5GC [241]).

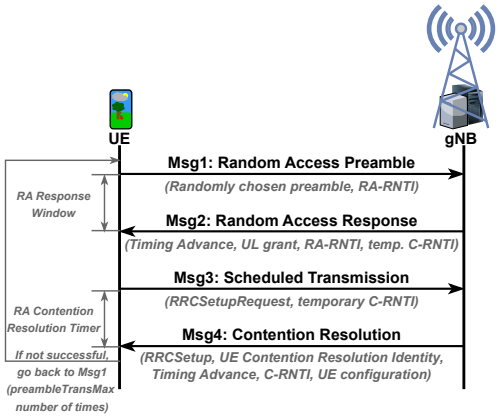



**Figure 2.6:** The 4-step contention-based Random Access procedure (based on [27, 26, 245]).

The gNB periodically broadcasts certain (RRC) information blocks required for the initial cell access, such as the Master Information Block (MIB) and the System Information Block (SIB) [245, 27]. The MIB contains cell status information, common physical layer parameters, and instructions on how to receive subsequent SIBs. The SIB1 defines the scheduling of other SIBs and has the necessary information for the initial cell access. During the initial cell attachment, the UE performs a 4-step (contention-based) Random Access (RA) procedure with the gNB (see Figure 2.6) [245, 27, 26]. Based on the RA parameters from the SIB, the UE transmits a randomly chosen preamble to the uplink (UL) RA channel (Msg1), and receives a RA Response (RAR, Msg2) in the downlink (DL) with some important information, such as Timing Advance (TA) to synchronize the UE UL transmission and an UL grant for the *RRCSetupRequest* (Msg3 in case of initial access). To resolve collisions between different UEs simultaneously initiating the RA procedure, the gNB attaches a “Contention Resolution” to the *RRCSetup* message (Msg 4) completing the RA. Upon successful completion of the RA procedure, the UE is assigned a Cell Radio Network Temporary Identifier (C-RNTI), so that it can be uniquely identified and addressed in the RAN. The C-RNTI is updated during the RRC connection re-establishment, e.g. after an inactivity period. Note that two types of RA procedures are possible: 4-step and 2-step, both either contention-based or contention-free (for more details, see the 3GPP specifications [26, 27]).

Once the RRC connection is established between the UE and the gNB, the UE sends a NAS *Registration Request* to the AMF, together with the *RRCSetupComplete* to the gNB acknowledging the *RRCsetup* [363, 137, 138]. The *Registration Request* contains the UE security capabilities and a subscriber identity for the UE identification in the form of a Subscription Concealed Identifier (SUCI), which is the encrypted version of the globally unique Subscription Permanent Identifier (SUPI), or the 5G Globally Unique Temporary Identifier (5G-GUTI). The SUPI can be of type International Mobile Subscription Identity (IMSI), which consists of Mobile Country Code (MCC), Mobile Network Code (MNC), and Mobile Subscriber Identification Number (MSIN), or it can have another type, such as Network Specific Identifier (NSI) in the form of a Network Access Identifier (NAI) [31]. The purpose of the 5G-GUTI is to unambiguously identify the UE without revealing its permanent identity in the 5GS. It consists of the Globally Unique AMF Identifier (GUAMI, constructed from MCC, MNC, and AMF Identifier) of the AMF that allocated the 5G-GUTI and the 5G Temporary Mobile Subscriber Identity (5G-TMSI) to uniquely identify the UE within that AMF. If the UE sends a 5G-GUTI and the CN cannot resolve it, then the AMF sends a NAS *Identity Request*, to which the UE replies with a NAS *Identity Response* including a SUCI [137, 363]. If the UE identity is unknown (or due to protocol errors or invalid values), the AMF sends a NAS *Registration Reject*, indicating the cause.

The encryption of SUPI is a privacy enhancement introduced in 5G networks to avoid the transmission of the sensitive subscription identifier over the network in clear text [187, 137]. Using elliptic curve cryptography (Elliptic Curve Integrated Encryption Scheme, or ECIES), the USIM card constructs a SUCI by encrypting the SUPI with the public key of the home network before it is sent in the NAS procedures (see section 5.4). On the 5GC side, the SUPI is deconcealed by the Subscription Identifier Deconcealing Function (SIDF) in the UDM of the subscriber's home network [33]. The SUPI concealment mitigates the problem of IMSI-catchers [327, 325, 239, 263, 126, 125]. These are eavesdropping devices which were used by attackers in previous mobile network generations to intercept the plaintext IMSI in order to track the location of the user [275]. Note that the Home Network Identifier part of SUCI (consisting of MCC and MNC) is sent unencrypted for routing purposes [33], which can give away some degree of personal information. This may be problematic when the home network is different from the serving network and is more identifiable (e.g. during a visit of a foreign delegation), allowing an eavesdropper to leak some information from the phones associated with the given home network [187].

Upon successful UE identification, the 5GC initiates the primary Authentication and Key Agreement (AKA) procedure (5G-AKA [33]) by sending a NAS *Authentication Request* with a random number (RAND) and an authentication token (AUTN) [363, 137, 138]. If the UE does not successfully verify the validity of RAND and the freshness of AUTN, it sends a NAS *Authentication Failure* with the cause "MAC failure" or "Sync failure", respectively. Otherwise, it sends a NAS *Authentication Response* with the response (RES) to the authentication challenge, generated using the RAND and the UE's permanent key. If the 5GC successfully verifies the validity of the RES, the primary authentication is considered successfully completed. The UE and the network can derive new keys for the confidentiality and integrity protection of the NAS signalling ($K_{NASenc}$, $K_{NASint}$), the RRC signalling ($K_{RRCenc}$, $K_{RRCint}$), and the UP traffic between the UE and the gNB ($K_{UPenc}$, $K_{UPint}$), as explained in 3GPP TS 33.501 [33].

Once the AKA procedure is completed, the AMF sends a NAS *Security Mode Command* with the selected ciphering and integrity protection algorithms for subsequent NAS messages [363, 137, 138, 33]. To protect against bidding-down attacks, the AMF replays the initial *Registration Request* with the UE security capabilities and includes a Message Authentication Code (MAC). If the UE successfully verifies the integrity of the *Security Mode Command* and the correctness of the replayed security capabilities, and if it supports the chosen algorithms, it replies with a ciphered and integrity-protected NAS *Security Mode Complete*, indicating that a secure NAS channel has been set up; otherwise, it sends a NAS *Security Mode Reject*. If requested by the AMF, the UE adds to the *Security Mode Complete* its Permanent Equipment Identifier (PEI) [31], e.g. an International Mobile station Equipment Identity (IMEI), an IMEI and Software Version number (IMEISV), or a MAC address [33]. An analogous Security Mode Command procedure establishes a secure channel for the RRC messages between the UE and the gNB (protected by PDCP), after which the UE can transmit its radio capabilities (e.g. supported frequency bands) to the network (in the previous generations, they were sent in clear) [137, 138].

After a successful Security Mode Command procedure, the UE has an active 5G NAS security context (and an AS security context for the messages between the UE and the gNB) [363, 33]. The AMF

sends a NAS *Registration Complete* to indicate that the 5GC accepts the initial UE registration. This NAS message contains information such as the UE registration area (the Tracking Area List, or TAL), the information about the Local Area Data Network (LADN), equivalent Public Land Mobile Networks (PLMNs), service area restrictions, allowed network slices, timers for periodic update registration, and the 5G-GUTI assigned by the AMF. The UE responds with a NAS *Registration Complete*, notifying that it has received the 5G-GUTI. At this point, the 5GC knows the location of the UE, its NAS connection, and the security information. The AMF can update the UE context using the NAS *Configuration Update Command*, e.g. to assign a new 5G-GUTI or update the TAL, service area list, LAND information etc.

To establish a PDU session, the UE sends a NAS (5GSM) *PDU Session Establishment Request* (encapsulated in the *UL NAS transport*), including information such as PDU session identification, PDU session type, the requested network slice, and the requested DN name (DNN) [363]. Based on these requirements, the 5GC can select the UPF and SMF for the requested PDU session. If the selected SMF supports this session, it sends a *PDU Session Establishment Accept* to the AMF, including the PDU address, QoS rules, session aggregate maximum bit rate, and other information. The AMF encapsulates the message in the *DL NAS transport* and sends it to the UE. If the SMF cannot provide the requested PDU session, it replies with a NAS (5GSM) *PDU Session Establishment Reject*, specifying the rejection cause. Together with the *PDU Session Establishment Accept*, the AMF also sends an NGAP *PDU Session Resource Setup Request* to the gNB, which forwards the AMF response to the UE together with the *RRCReconfiguration* message that includes the configuration of at least one Data Radio Bearer (DRB) [27]. This RRC message also activates the ciphering and integrity protection of the UP messages between the UE and the gNB (performed by PDCP) [137]. After the UE has established the DRB(s) and created the QoS Flow ID (QFI) to DRB mapping rules, it sends an *RRCReconfigurationComplete* to the gNB, which in turn sends an NGAP *PDU Session Resource Setup Response* to the AMF [27]. The UE can finally exchange the UP data with the gNB over the DRB(s) (according to the mapping rules), and the gNB exchanges this data with the UPF over a tunnel for this PDU session.

When the UE is switched off or if its USIM card has been removed, it initiates a (UE originated) deregistration procedure by sending a NAS *Deregistration Request* indicating “switch off” as deregistration type (this was the case in Figure 2.4 and Figure 2.5) [25, 32]. The AMF instructs the SMF to perform a local release of the PDU session(s). If the *Deregistration Request* is not due to the switch off, the AMF replies with a NAS *Deregistration Accept* before the procedure is (successfully) completed. The signalling connections with the NG-RAN are released as well. The deregistration procedure can also be initiated by the 5GC (UE terminated deregistration), e.g. to inform the UE to re-register to the network. In this case, the AMF sends a *Deregistration Request* and the UE responds with a *Deregistration Accept*. For more information about the message flows between UE, NG-RAN, and 5GC, refer to the corresponding 3GPP specifications [32, 27, 30, 25, 22, 33].

### 2.1.5. Mobility management

Mobility management is a complex topic, the details and specifics of which are well beyond the scope of this thesis. Therefore, in this subsection, we only introduce the main concepts. For more in-depth information on mobility management, refer to the relevant 3GPP specifications [27, 30, 32].

When the UE needs to be notified of the incoming data transmissions or a phone call, the network uses the paging mechanism [137, 138]. For incoming data or SMS, the paging procedure is started, telling all UEs within the cell to listen to the paging channel for paging messages (broadcast by the gNB) and react if their identity matches with the indicated recipient identity. For an incoming phone call, the same procedure is performed at a TA level. Paging allows the network to reach UEs in RRC_IDLE and RRC_INACTIVE states via RRC *Paging* messages, as well as to inform the UEs in RRC_IDLE, RRC_INACTIVE, and RRC_CONNECTED states about the system information change via RRC *Short Messages* (both message types are addressed with P-RNTI) [27]. The CN-initiated paging is performed using 5G-S-TMSI (constructed from the AMF Set ID, the AMF Pointer, and the 5G-TMSI), which is the shortened form of the 5G-GUTI and is used to allow more efficient radio signalling procedures, such as paging and Service Request [31]. The RAN-initiated paging is performed using full I-RNTI [30].

In a 5G network, the UE can be in one of the three RRC states (see Figure 2.7). If an RRC connection has been established between the UE and the gNB, the UE is either in RRC_CONNECTED or in RRC_INACTIVE; otherwise, it is in RRC_IDLE [30, 27]. The states have the following characteristics:

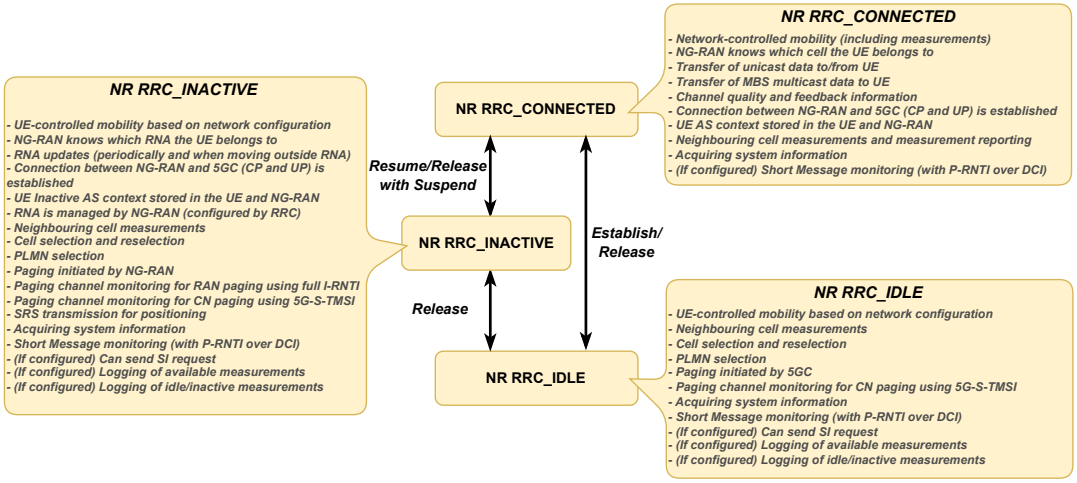



**Figure 2.7:** The three RRC states in 5G (NR) and the corresponding state transitions (based on [30, 27]).

- **RRC_IDLE**. The UE controls the mobility based on the network configuration. It performs measurements of the neighbouring cells, cell selection and reselection, as well as PLMN selection. The paging procedure for mobile terminated data is initiated by the CN (CN-initiated paging), and the UE monitors the paging channel for (RRC) *Paging* messages with the 5G-S-TMSI. The UE also listens to the broadcast of system information, and, if configured, can send a System Information (SI) request. In addition, the UE monitors RRC *Short Messages* with the P-RNTI sent over Downlink Control Information (DCI) for paging or system information change notification. If configured, the UE can perform logging of available measurements (with the location and time), and/or idle/inactive measurements.
- **RRC_INACTIVE**. The UE controls the mobility based on the network configuration. The NG-RAN knows the UE location on the level of a RAN-based notification area (RNA), which is managed by the NG-RAN. Periodically and when moving outside the RNA (configured by the RRC layer), the UE performs RNA updates. While the UE is in RRC_INACTIVE state, the connection between the NG-RAN and the 5GC (for both CP and UP) is established, and the UE Inactive AS context is stored in the UE and the NG-RAN. The UE performs measurements of the neighbouring cells, cell selection and reselection, as well as PLMN selection. The paging procedure is initiated by the NG-RAN, and the UE monitors the paging channel for the RAN-initiated paging with the full I-RNTI and for the CN-initiated paging with the 5G-S-TMSI. It also transmits the Sounding Reference Signal (SRS) for positioning. Similarly to the RRC_IDLE state, the UE listens to the broadcast of system information and can send an SI request (if configured). In addition, it monitors the Short Messages with P-RNTI in DCI, and, if configured, performs logging of available measurements and/or idle/inactive measurements.
- **RRC_CONNECTED**. The network controls the mobility within NR, as well as to/from lower generation RANs (e.g. LTE). The UE is actively transferring or receiving unicast data (or receiving multicast data) and provides channel quality and feedback information. The NG-RAN knows the UE location on the cell level. The connection between the NG-RAN and the 5GC (for both CP and UP) is established for the UE, and the UE AS context is stored in the UE and the NG-RAN. As in the other two states, the UE listens to the broadcast of system information, monitors the Short Messages over DCI (if configured), and performs neighbouring cell measurements and measurement reporting (if configured).

When the UE registers to the network (i.e. transitions from RM-DEREGISTERED to RM-REGISTERED, and from CM-IDLE to CM-CONNECTED), it moves from RRC_IDLE to RRC_CONNECTED [27, 225]. After the RRC inactivity timer expires, the UE moves to RRC_INACTIVE and its RRC connection with the gNB is released. The UE-associated NG-connection with the serving AMF and UPF is kept in the last serving gNB. In RRC_INACTIVE state, the UE remains connected (i.e. CM-CONNECTED) and can move within the RNA (as configured by the NG-RAN) without having to notify the NG-RAN. The RNA configuration can be provided to the UE by the last serving gNB in several ways, such as an explicit list of one or more cells that form the RNA, or as a list of RAN areas, where each RAN area is a subset of or equal to a 5GC Tracking Area and is identified by one RAN area ID, which consist of a Tracking Area Code (TAC) and optionally a RAN area code. The UE periodically sends an RNA update,

and is required to initiate the RNA update procedure when it moves outside the configured RNA due to its cell reselection procedure. When a new gNB receives the RNA update request from the UE, it retrieves the UE context from the last serving gNB via the Xn interface, and can decide whether to send the UE back to RRC_INACTIVE, send it to RRC_IDLE, or move it to RRC_CONNECTED state. For a periodic RNA update, the last serving gNB can choose not to relocate the UE context (by failing the UE context retrieve procedure) and send the UE back to RRC_INACTIVE or directly to RRC_IDLE with an encapsulated *RRCRelease* message.

Unlike RRC_INACTIVE and RRC_IDLE states, where the mobility is controlled by the UE (i.e. the UE chooses which gNB it listens to), the mobility in RRC_CONNECTED is controlled by the network (i.e. the network chooses which gNB the UE is connected to) [225]. In case of cell level mobility, explicit RRC signalling needs to be triggered, i.e. a handover, which can be performed within the same Radio Access Technology (RAT) and/or CN or can include a change of the RAT and/or CN [27]. The handover procedure is used to hand over a UE from a source NG-RAN node (gNB) to a target NG-RAN node (gNB) using the Xn or N2 interfaces (Xn handover and NG handover, respectively), and can be triggered due to new radio conditions, load balancing, or due to specific service [32]. The Xn-based inter-NG-RAN handovers (e.g. between two gNBs) can be performed with or without UPF reallocation, however Xn handovers are only supported for intra-AMF mobility (i.e. without changing the AMF). Inter NG-RAN node N2-based handover can be performed if there is no Xn connectivity to the target NG-RAN or in case of an unsuccessful Xn-based handover, and it may also be used for intra-NG-RAN node handover.

### 2.1.6. Deployment modes

Unlike 4G, 5G offers a lot of flexibility and many options when it comes to network deployment [275]. Network operators and service providers who have already done large investments in their network infrastructure in previous generation technologies can choose to reuse some parts of the LTE infrastructure when first deploying 5G. On the other hand, they can also choose to deploy a full-fledged 5G network right away. Thus, network operators can choose from the following two options [12, 275, 187]:

- **Non-standalone (NSA) deployment**: In an NSA deployment (see Figure 2.8a), multiple RATs are used, i.e. LTE and NR. In case of 5G, it means that NR gNBs are integrated into existing LTE system with the multi-radio E-UTRA-NR Dual Connectivity (EN-DC) implementation. The core network is an LTE Evolved Packet Core (EPC) and LTE eNBs are master nodes, providing the CP connection to the CN. NR gNBs act as secondary nodes with no CP connection to the CN, offering supplementary resources to the UE. UP traffic is split between master and secondary nodes. The 5G NSA mode allows for a faster deployment of 5G services and higher UP traffic speeds, reusing existing infrastructure and reducing the costs. However, it is not a full-fledged 5G deployment, meaning that new 5G features, such as network slicing, virtualization, and SUPI concealment (SUCI) are not available. Furthermore, the UE in DC needs to support LTE and NR radio interfaces at the same time, which increases its power consumption.
- **Standalone (SA) deployment**: In a SA deployment (see Figure 2.8b), only one RAT is used (LTE or NR). In case of 5G, it means that the network architecture consists of NR gNBs and 5GC. From the network operator's viewpoint, 5G SA deployment might result in higher capital expenditure and longer deployment time. However, a SA mode can provide all benefits that come with a 5G network, including eMBB, URLLC, mMTC, network slicing, SUPI concealment (SUCI), cleaner CUPS, 5GC SBA, NVF, and cloud deployments. Of course, NVF also means that the operator has to take care of proper isolation mechanisms between the virtual machines implementing virtualized NFs. In the rest of the thesis, we only consider 5G SA deployments as the long-term solution for network operators.

5G SA deployment offers many choices that network operators have to make depending on the industry vertical [275]. For example, smart manufacturing and other industry verticals requiring URLLC, high bandwidth, and integration with third-party applications might benefit from placing the UPF next to the edge computing platform and applications. On the other hand, if latency is not the main concern, then placing only the automation part with the UPF in the multi-access edge compute (MEC) is enough. If MEC is deployed next to gNB, it usually has limited hardware resources and site conditions, which requires having very low-footprint virtualization infrastructure, cooling, and limited power supply.

NFs in 5GC can also be deployed in different locations, such as [275]:

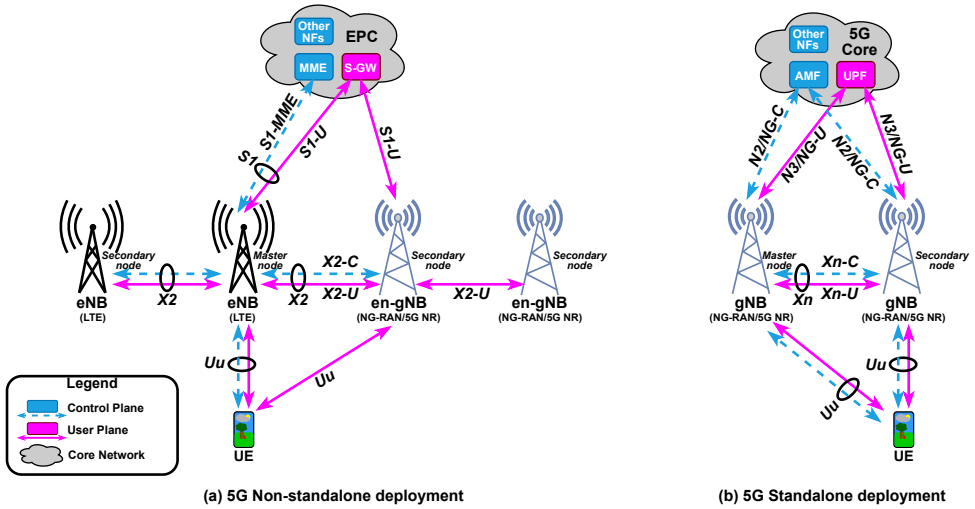



**Figure 2.8:** 5G Standalone (SA) and Non-standalone (NSA) deployment modes (based on [12, 275]).

- **On-premises**. NFs are deployed exclusively on private cloud, programmable routers, or low-footprint servers. This option gives the network operators a lot of flexibility with the infrastructure and higher data security, however it might also result in higher costs.
- **Multistack Public Cloud**. NFs are deployed exclusively on public cloud providers (e.g. Amazon Web Services, Microsoft Azure, Google Cloud) or public cloud managed by 5G equipment vendors. This option might be cheaper for the network operators, but may also pose security challenges depending on the country regulations on public cloud deployment.
- **Hybrid Cloud**. NFs are deployed both on-premises and on multistack public cloud. This option is a combination of the previous two, therefore the benefits and challenges are also a mix depending on the exact deployment.

Furthermore, NFs in 5GC can be deployed with a direct or indirect inter-NF communication model [275]:

- **Direct communication**. Two NFs interact with each other using an API. At the same time, the communication may take place with or without service discovery provided by NRF.
- **Indirect communication**. Two NFs communicate via SCP using an API, with or without NRF for service discovery. SCP aggregates HTTP links and monitors centralized signalling. Next to centralized monitoring, SCP can offer flexible network design by deploying SCP in distributed mode, load balancing through real-time congestion control, communication authorization and resilient integration with third-party vendors and application developers, and encrypted communications using cryptographic verification via TLS/mTLS as well as complete control over the distribution of keys and certificates.

RAN can also be deployed in different ways using the following deployment models [275]:

- **Virtualized RAN (VRAN)**. VRAN gives you virtualized NFs which can be deployed on any COTS hardware or on multistack public cloud.
- **Open RAN (O-RAN)**. O-RAN is specified by the O-RAN Alliance [67]. It allows you to use machine learning systems and AI backend modules to enhance network intelligence with the help of open and standardized interfaces. Requirements of open interface, flexible deployments, and reduction of the total cost of ownership is what drives O-RAN deployments. Moreover, O-RAN has a wider adoption than C-RAN because of its openness, cost-effectiveness, and deployment flexibility.
- **Centralized/Cloud RAN (C-RAN)**. C-RAN relies on open platforms and real-time virtualization technologies from cloud computing in order to be able to dynamically allocate CU and DU. C-RAN also has the Baseband Unit (BBU) at the centralized location, which allows for a lightweight deployment of Radio Unit (RU) and antenna at the cell location. BBU, located in the centralized core, is split into DU and CU and is connected to the RU at the cell cite using fronthaul interface. The benefits of C-RAN are better resource virtualization, joint processing, and the option for cooperative radio sharing.

Finally, 5G networks can be deployed either as public or private (non-public) networks [90]:

- **Public network**. A public 5G network is meant to be used by the public with a very high number of subscribers (e.g. tens of millions of subscribers on a nationwide network). The installation, service, and management of a public network is done by the MNO, who usually also owns the spectrum.
- **Private network**. A private 5G network is a dedicated network, intended to be used by a single enterprise or organization, e.g. college or university campuses, hospitals, manufacturing facilities, and places with critical infrastructure or mission-critical applications such as military bases. Private networks can be of two types:
  - **Independent network**. In an independent private network, the enterprise has to select the spectrum, set up the network infrastructure, manage the users, and deploy and maintain the network. While this option offers higher data security (because the data stays on site) and higher control over the network settings depending on the use case (e.g. URLLC or mMTC), it also means higher capital expenditure and challenges while selecting the spectrum.
  - **Dependent network**. In a dependent private network, the network itself is set up and maintained by an MNO who either dedicates the spectrum to the enterprise or uses network slicing. The MNO also manages user access, depending on the mutual agreement. While this option means less control over the network and data for the enterprise, the benefits include minimal capital expenditure (with ongoing monthly fees based on the number of users) and no need for special IT experience.

## 2.2. Satellites and the space ecosystem

In this section, we give an overview of the satellites and the space ecosystem, and describe the main satellite operation segments. This section is meant to be fairly generic, and it can help the reader better understand some concepts related to 3GPP NTN.

### 2.2.1. Overview

A satellite, or an artificial satellite, is an object orbiting another body like the Earth and is purposefully put in the outer space with the common applications such as providing communication services to the Earth, Earth observation, and research [402]. The first satellite sent to space and successfully placed in orbit around the Earth was Sputnik 1, launched from the Soviet Union in 1957 [276]. As of October 7, 2024, there are approximately 10,839 objects in different Earth orbits, according to a satellite tracking website *Orbiting Now* [323], while UNOOSA [389] shows even a higher number of 19,161 objects. In particular, 7,767 satellites are in Low Earth Orbit (LEO), 202 in Medium Earth Orbit (MEO), 101 in High Earth Orbit (HEO) or Graveyard, and 545 in Geosynchronous Earth Orbit (GEO) [323]. The majority of the satellites (7,019) belongs to Starlink [374] – a satellite-based Internet project from SpaceX [372]. Only in two years since the launch of the first batch, Starlink has sent to space 1,600 spacecrafts [223]. Eventually, SpaceX wants to operate a constellation of up to 40,000 satellites [399]. In the meantime, according to some forecasts, about 17,000 satellites are expected to be launched by 2030 [170].

Space privatization by big private companies like SpaceX and Rocket Lab, satellite miniaturization, and the emergence of novel services based on space data have led to what is knows as the New Space Era, offering quick and rather low-cost access to space [218]. New space services have emerged as a result of a shift from a product-oriented business model to a use-oriented model, similar to the terrestrial transition towards cloud computing, which gave rise to new applications [185]. The “servitization of space” created new types of service models, such as Payload-as-a-Service, Satellite-as-a-Service, Space Platform-as-a-Service, Constellation-as-a-Service, In-Space Mobility-as-a-Service, Ground station-as-a-Service, Mission-as-a-Service, Space-as-a-Service, and Space-Data-as-a-Service. In the past, getting access to ground stations was very expensive, so they were only limited to big satellite operators [402]. Nowadays, ground stations have become affordable to private users, especially due to the opportunity to use a ground station as a service, for example from Amazon Web Services [69] and Microsoft Azure [259] who only charge for the used actual antenna time (so called “pay-as-you-go” model”) and who claim to offer high security guarantees. The shift from conventional high capital expenditures coming from the development of space applications towards operating expenses will lead to a rise of in-space applications and further reduce the barrier for new entrants [185].

**Table 2.1:** The three classes of orbit, with GEO as a special case of HEO, their altitude and main use cases of satellites on these orbits [343, 371]. The quantity of satellite objects is based on *Orbiting Now* [323] (accessed October 7, 2024).

| Orbit | Altitude | Quantity | Main use cases |
|---|---|---|---|
| **Low Earth Orbit LEO** | 180–2,000 km | 7,767 | • Communication<br>• Remote sensing satellite systems<br>• International Space Station (ISS)<br>• Hubble Space Telescope |
| **Medium Earth Orbit MEO** | 2,000 - 35,780 km | 202 | • Navigation systems, including:<br>– US's GPS<br>– Europe's Galileo<br>– Russia's GLONASS |
| **High Earth Orbit (HEO)** | $\geq$ 35,780 km | 101 | • Solar activity monitoring<br>• Magnetic and radiation levels<br>• Other use cases for GEO |
| **Geostationary Earth Orbit (GEO)** | $\approx$ 36,000 km | 545 | • Telecommunications<br>• Phones, television, radio<br>• Earth observations<br>• Weather monitoring |

### 2.2.2. Earth orbits

Different Earth orbits offer different perspectives to the satellite, in the same way as different seats in theatre offer the viewer different angles on the performance [343]. The altitude from the Earth, eccentricity (the shape), and inclination (the angle relative to Earth's equator) of the orbit decide the path that the satellite will follow and the view of the Earth it will get. This makes each orbit more applicable for certain use cases. The three main orbit classes are LEO, MEO, and HEO (see Table 2.1).

When the satellite reaches the altitude of around 35,786 km above the Earth surface (thus, being in HEO), its Earth orbit period coincides with the Earth rotation period on its axis (i.e. around 24 hours), meaning that an observer from the Earth will see the satellite return to the same position in the sky after one sidereal day (23 hours, 56 minutes, 4 seconds) [323, 343, 148]. This orbit is called geosynchronous Earth orbit. As a special case, when this orbit is directly over the equator, the satellite does not move relative to the ground, i.e. it hovers over the same place above the Earth surface [343]. This is a geostationary Earth orbit (GEO), and it is very valuable for weather monitoring since the satellite offers a constant view of the same area. Furthermore, a GEO satellite covers a large range of the Earth, with only three equally-spaced satellites needed to provide almost global coverage [148]. However, this comes at the cost of latency: because the distance from the Earth is too large, the one-way time for a signal from the ground to a satellite is 120 ms and the round-trip time is 240 ms (i.e. one fourth of a second is only the signal propagation) [398]. This time is not acceptable for many real-time applications.

MEO orbits are between HEO (GEO) and LEO orbits, i.e. between 2,000 and 36,000 km above the ground [343]. Satellites in these orbits move faster relative to the Earth. For example, in the semi-synchronous MEO (around 20,200 km above the ground), a satellite completes the orbit in 12 hours, meaning that it passes over the same place on the equator two times per day. Another notable MEO orbit, the Molniya, is highly inclined and highly eccentric, making it useful for observing locations in the far north or south, which are not very visible for a GEO satellite. MEO orbits are often used for navigation satellites, like the European Galileo system, which provides navigation communications across Europe and uses a constellation of satellites to simultaneously cover large parts of the world [148].

Finally, LEO orbits are the closest to the Earth, typically less than 2,000 km above the ground [148]. While geostationary satellites have to follow a specific path along the Earth's equator, LEO satellites have more freedom with the routes they follow, which makes LEO quite popular. Depending on the precise altitude, the satellite circles the Earth in around two hours. This means that the satellite will not be connected to a ground station for long, making it less useful for telecommunications [398]. Nevertheless, a constellation of simultaneously working communication satellites in LEO can provide constant coverage for large areas [148]. Furthermore, LEO satellites offer certain benefits for communication: because the speed of light in space is 1.5 times higher than the speed of light in an optical fibre on the ground, then despite a small (15%) increase in the distance going over satellite links, the signal will travel 1.47 times faster, which is a net gain [398].

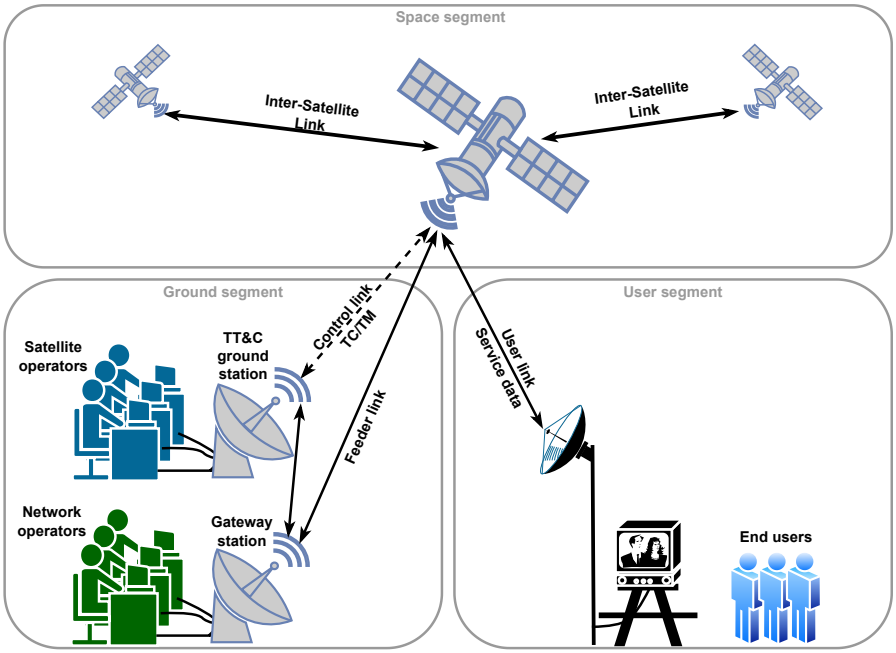



**Figure 2.9:** The three main segments involved in satellite operations (based on [402]).

### 2.2.3. Satellite operation segments

Satellite operations normally include three segments (see Figure 2.9) [218, 402]:

- **Ground Segment**. The ground segment is responsible for operating the satellite-based service throughout the entire lifetime of a satellite. It consists of ground stations, such as gateway (GW) station and Telemetry, Tracking and Control (TT&C) station, and big ground facilities for control, network operations, and backhauling. TT&C stations track the status of the satellites, run tests, and update configurations in order to maintain the satellites and keep them on the desired orbits. Hence, the operation of TT&C stations is managed by the satellite operators. They send commands to a satellite in the form of Telecommand (TC), and the satellite responds with the information about its status, errors, and other metrics in the form of Telemetry (TM). GW stations manage the network access and backhauling, thus they are run and maintained by the network operators.
- **Space Segment**. The space segment is responsible for providing the satellite-based service, e.g. communications or navigation. It consists of all spacecraft that is involved in satellite operations, either a single satellite or an entire constellation. In the latter case, the satellites communicate with each other using Inter-Satellite Links (ISLs). At the start of the operation, these satellites are sent to the intended orbit with the help of a launch vehicle (rocket), after which they go through the phase of orbital deployment in order to initiate communication with the ground station.
- **User Segment**. The user segment is responsible for receiving the service provided by the space segment and delivering it to the end users, e.g. determining positioning using received GPS signalling. Devices in the user segment are terminals, such as a Very Small Aperture Terminal (VSAT) or a GPS receiver. User terminals can be deployed both on fixed and mobile platforms (such as ships or planes). Depending on the application, the satellite might exclusively communicate with the ground segment, so there is no user segment, e.g. for Earth observation satellites.

TC/TM traffic between the ground and the space segments is transmitted over space protocols, developed by the Consultative Committee for Space Data Systems (CCSDS) [119], which is the main standardization organization proposing space standards and protocols [402]. CCSDS is a consortium of different space agencies who together agree on protocol standards for communicating with all components involved in space operations. These standards touch all layers of the OSI model, mostly with multiple options per layer [120]. Some examples are Space Data Link Security (SDLS) for the data link layer and Space Packet Protocol (SPP) for the network layer.

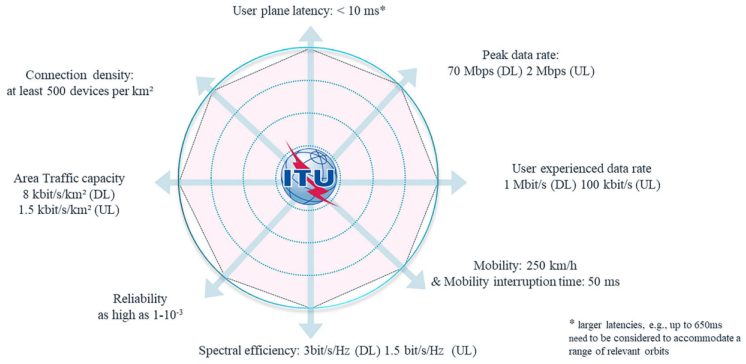



**Figure 2.10:** IMT-2020 requirements for the satellite radio interface. [136]

## 2.3. 5G non-terrestrial networks

This section will conclude the background chapter by explaining the concept of non-terrestrial networks (NTN) and the introducing the current deployment options proposed by the 3GPP community.

### 2.3.1. Overview

As defined by 3GPP, non-terrestrial or satellite networks are “networks, or segments of networks, using an airborne or space-borne vehicle to embark a transmission equipment relay node or base station” [37]. In other words, they use RF resources on board a satellite or an Unmanned Aircraft System (UAS) platform as part of the communication system. With their wide coverage and multicast capabilities, NTN can complement the already existing terrestrial infrastructure [218].

The 3GPP technical specification (TS) of service requirements for a 5G system states that “the 5G system shall be able to provide services using satellite access” [36]. A feasibility study has been conducted on using satellite access in 5G, where multiple use cases have been analysed, and the corresponding requirements have been proposed [56]. Three main (nonexclusive) categories have been defined for 5G NTN, based on their unique characteristics [56, 218]:

1. **Service continuity**. Deploying TNs in highly populated centres can result in geographical areas where it will not be possible to access 5G services through the radio coverage of a TN. In such cases, a combination of terrestrial and non-terrestrial networks can improve the reliability of the 5G network and give its users the opportunity to continuously access 5G services. This is especially the case for moving platforms (e.g. cars, trains, or planes) and mission-critical communications.
2. **Service ubiquity**. In some situations, deploying TNs may not possible due to economic considerations. 5G NTN can provide demanded services in unserved (e.g. deserts, oceans, forests) or underserved (e.g. urban areas) locations. Furthermore, the infrastructure of TNs may become temporarily or permanently unavailable due to natural disasters, such as earthquakes or floods.
3. **Service scalability**. Due to a large coverage achievable by NTN, they are more efficient in broadcasting and multicasting content over a very wide area. They can broadcast popular (heavy) content to the edge of the network or directly to the subscribers, offloading some traffic from TN during busy hours. Similarly, they can broadcast delay-tolerant data outside busy hours.

Figure 2.10 shows the main performance requirements for the satellite component, based on IMT-2020. When it comes to the architecture, an NTN typically has the following elements [36]:

- One or multiple satellite GWs (called NTN GW) connecting the NTN to a public data network.
  - GEO satellite is fed by one or multiple GWs deployed across the targeted coverage area of the satellite, providing continental, regional, or local service.
  - Non-GEO satellite is served consecutively by one or multiple GWs at a time. The system must ensure the continuity of the service and feeder links between the consecutive serving GWs and provide enough time for mobility anchoring and handover. A constellation of LEO and MEO satellites provides services in both Northern and Southern hemispheres, and in some cases even a global coverage including polar regions.

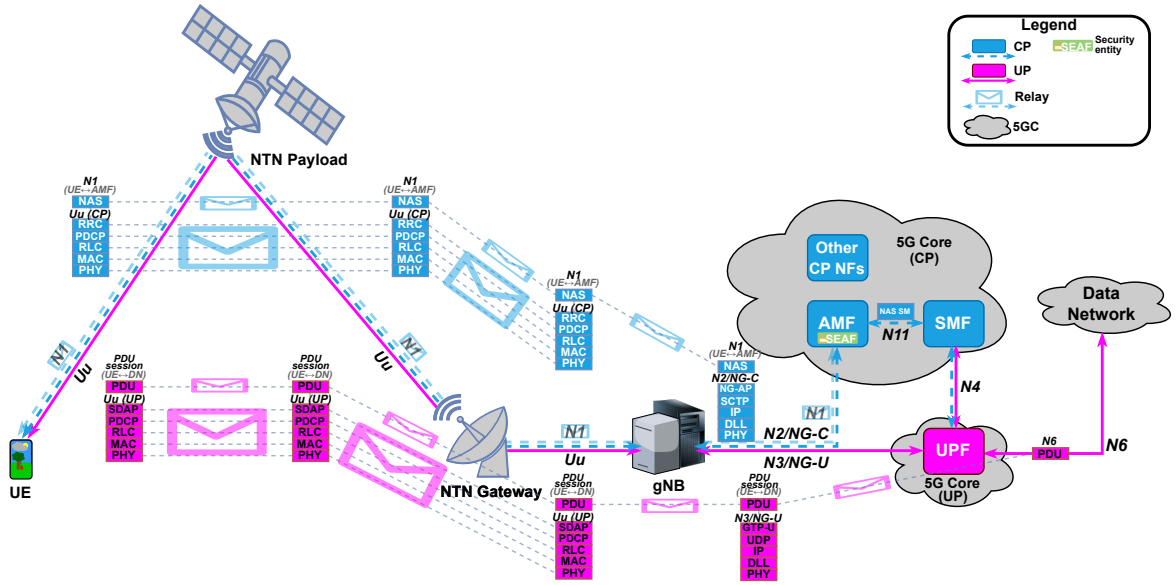



**Figure 2.11:** Architecture of the NTN Transparent payload scenario (based on [37]).

- Feeder link or radio link between the NTN GW and the satellite/UAS platform.
- Service link or radio link between the UE and the satellite/UAS platform.
- Satellite/UAS platform with a transparent or regenerative payload. It normally generates several beams (with elliptic-shaped footprints) over a given service area, which is restricted by its field of view. In this thesis, we focus on satellites, but UAS platforms might also be applicable.
- ISL can be used in case of a satellite constellation. However, this requires a regenerative payload.
- UE is served by the satellite/UAS platform which is within the given service area.

In Technical Report (TR) 38.821 [37], 3GPP has proposed three main architectures to integrate NTNs with TNs (with the assumption that mobile devices are able to directly connect to the satellites): transparent payload, regenerative payload with a full gNB on board, and regenerative payload with a CU-DU split (gNB-DU on board, gNB-CU on the ground) [398]. In these scenarios, the 5G architecture is used directly, with the satellite fully or partially replacing the base station, i.e. gNB (in case of a regenerative payload). Furthermore, TR 22.865 describes some enhancements of the 5G system over a satellite, such as Store and Forward (S&F) satellite operation for delay-tolerant communication service, and UE-Satellite-UE communication [53]. Below, we present these five NTN deployment modes.

### 2.3.2. Transparent payload

A satellite with a transparent payload (also called “bent-pipe payload” or “non-regenerative payload”) is a satellite that only relays the signal it receives [221, 398]. The satellite platform has no on-board processing capabilities, so no packet processing is performed. However, some signal processing takes place, such as altering the frequency carrier of the received UL radio frequency (RF) signal, RF filtering, frequency conversion, and amplification before sending the signal to the DL. Thus, the satellite acts as an analogue RF repeater, and the signal waveform repeated by the payload remains unchanged [37]. The functions of the gNB are performed on the ground behind the GW ground station. The advantage of this NTN mode is that the NG-RAN architecture and the CP and UP protocols do not need to be modified, although the system should adapt to longer roundtrip times on the Uu interface.

Figure 2.11 shows the architecture of the transparent payload scenario together with the protocol stacks. The architecture is used by the currently deployed LEO constellations like Starlink, with the satellite only relaying the signal between ground stations [398]. However, in 3GPP NTN, the 5G NR technology is used for the radio access instead of proprietary technology.

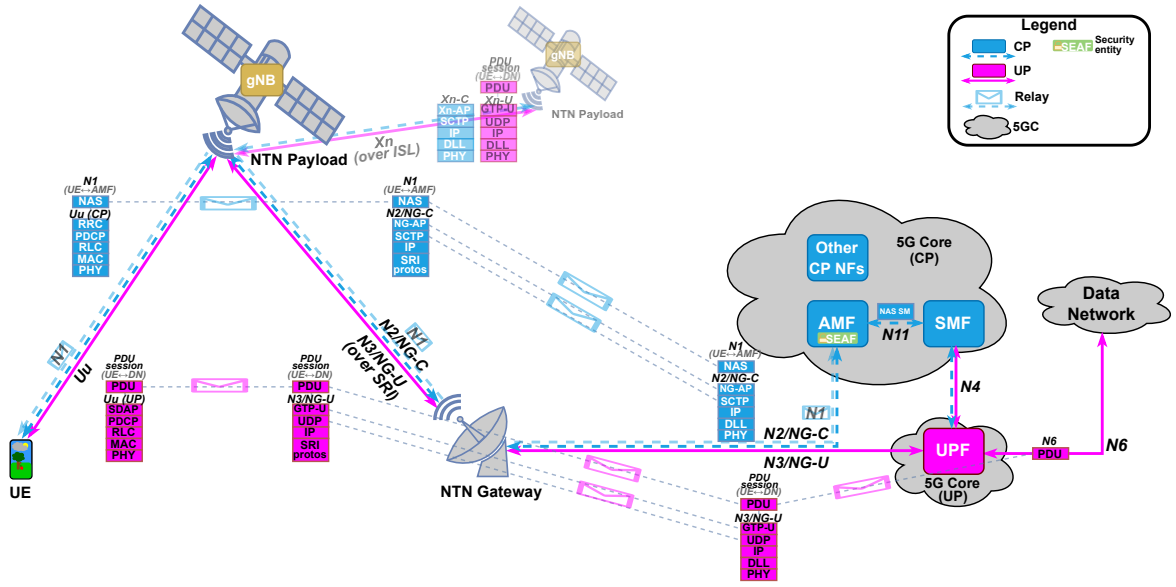



**Figure 2.12:** Architecture of the NTN Full gNB on board scenario, i.e. regenerative payload with the entire gNB functionality on board (based on [37]). The faded ISL represents the option to deploy multiple satellites.

### 2.3.3. Regenerative payload: Full gNB on board

A satellite with a regenerative payload (also called “non-transparent payload”) has, next to the signal processing functions, the on-board processing capabilities to provide demodulation (decoding), switching and/or routing, and modulation (coding) [221, 398, 37]. In case of a full gNB on board, the functions of the gNB are performed by the satellite, while the functions of the AMF and the UPF are provided by the devices on the ground. gNBs on different satellites can be connected to the same 5GC on the ground. On the service link between the UE and the on-board gNB, both CP and UP are sent over the 5G NR protocols. On the feeder link between the on-board gNB and the NTN GW, the PDUs, NGAP and NAS messages are transported as usual over the IP, but they are encapsulated in the protocol stack of the Satellite Radio Interface (SRI). As a Transport Network Layer node, the NTN GW supports all the required transport protocols, so that data exchange can take place between the 5GC and the on-board gNB (and between the 5GC and the UE). However, the implementation should address longer latencies on the NG (and Uu) interface, affecting both CP and UP.

Figure 2.12 shows the architecture and the protocol stacks of the 5G NTN architecture based on regenerative payload with a full gNB on board. This scenario represents a generic architecture for the integration of a satellite constellation with 5G and the Internet [398]. Each satellite in the constellation works as a flying base station, and the constellation together acts as a backhaul network. Connected by ISLs, it will become an IP network and will function as a carrier for the NG or Xn interfaces.

### 2.3.4. Regenerative payload: Split CU-DU

The NTN architecture based on regenerative payload with a CU-DU split is similar to the previous option, except that the satellite does not provide all functions of a base station [398, 221, 37]. In this case, the DU and CU of the gNB are separated, with the gNB-CU functionality provided by the devices on the ground and the gNB-DU functionality provided by the satellite. This means that the satellite only deals with the lower layers of the 5G NR protocol stack and regenerates the signals it receives from the ground. The gNB-DUs on different satellites can be connected to one ground gNB-CU. In this NTN scenario, all CP interfaces towards terrestrial NG-RAN nodes end on the ground. The protocol stack of the SRI is responsible for the transport of both CP and UP data over the F1 interface. The UP PDU and the NAS messages between the 5GC and the UE, the RRC messages between the UE and the gNB-CU, as well as the F1-C messages between the gNB-DU and the gNB-CU pass through the NTN GW, which is between the gNB-CU and the (on-board) gNB-DU. The NGAP messages between the 5GC and the gNB-CU are sent normally, since they are both on the ground. Note that the implementation

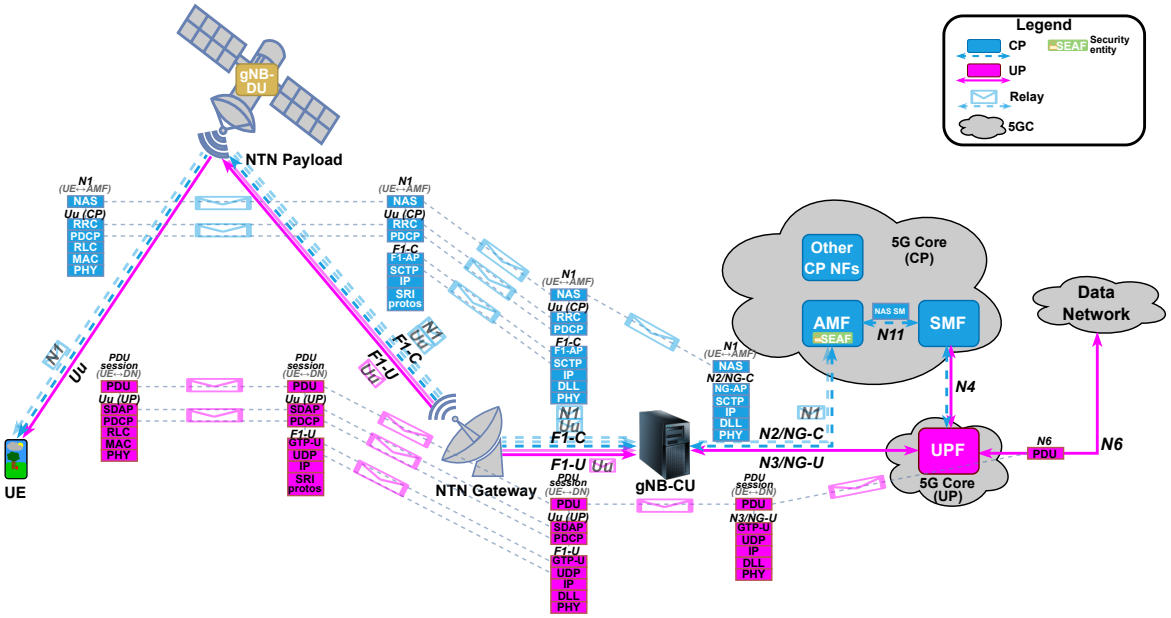



**Figure 2.13:** Architecture of the NTN Split CU-DU scenario, i.e. regenerative payload with gNB-DU on board (based on [37]).

should address longer latencies on the F1 interface, affecting both CP and UP. Figure 2.13 shows the architecture and the protocol stacks of the 5G NTN architecture based on regenerative payload with a CU-DU split (split option 2-1 [52]).

### 2.3.5. UE-Satellite-UE communication

In the UE-Satellite-UE communication, the 5G system is able to provide communication between UEs within the coverage area of one or more serving satellites without having to go through the ground segment, i.e. using only the satellite access [53, 221]. This is useful to prevent long delays and limited data rates, and it also helps to reduce the resource consumption for the backhaul network. For this mode, the gNB and the UPF must be deployed on a satellite [50]. In particular, the gNB-DU, the gNB-CU-UP, and the UPF are on board, while the gNB-CU-CP and the CP 5GC NFs are on the ground. This means that many interfaces are now transported by the SRI protocols on the feeder link, specifically, the F1-C interface between the gNB-DU and the gNB-CU-CP (carrying the Uu CP and N1 data), the E1 interface between the gNB-CU-CP and the gNB-CU-UP, the N4 interface between the SMF and the UPF (both CP and UP), and the N6 interface between the UPF and the DN. On the other hand, the F1-U interface between the gNB-DU and the gNB-CU-UP (carrying the Uu UP data), and the N3 interface between the gNB-CU-UP and the UPF are internal to the satellite. The architecture and the protocol stacks for the UE-Satellite-UE communication scenario are shown in Figure 2.13.

The use case of a UE-Satellite-UE communication can be illustrated with an example [53] (see Figure 2.15). In the Amazon rainforest, there is no modern communication infrastructure. While a satellite access network can provide connectivity, explorers and tourists are coming from different countries and may belong to different MNOs. Thus, they need mechanisms like roaming between mobile operator networks to access the same satellite. In this example, an explorer in the rainforest got injured and wants to call the rescue team. The explorer's mobile operator TerrA has a roaming agreement with the mobile operator TerrB of the rescue team, and TerrB has satellite access agreements with a satellite operator SatA, whose service area includes the rainforest. The explorer has signed up for a roaming plan of TerrA for accessing the mobile network of TerrB. Given all these subscriptions and agreements, when the injured explorer makes a call, SatA can determine the real-time position information of the explorer, and TerrB can determine the nearest rescuer. To decrease communication latency, the call is routed only through the satellite, without going through the ground networks that belong to TerrA and TerrB. Now the rescuer can find the injured explorer and help them.

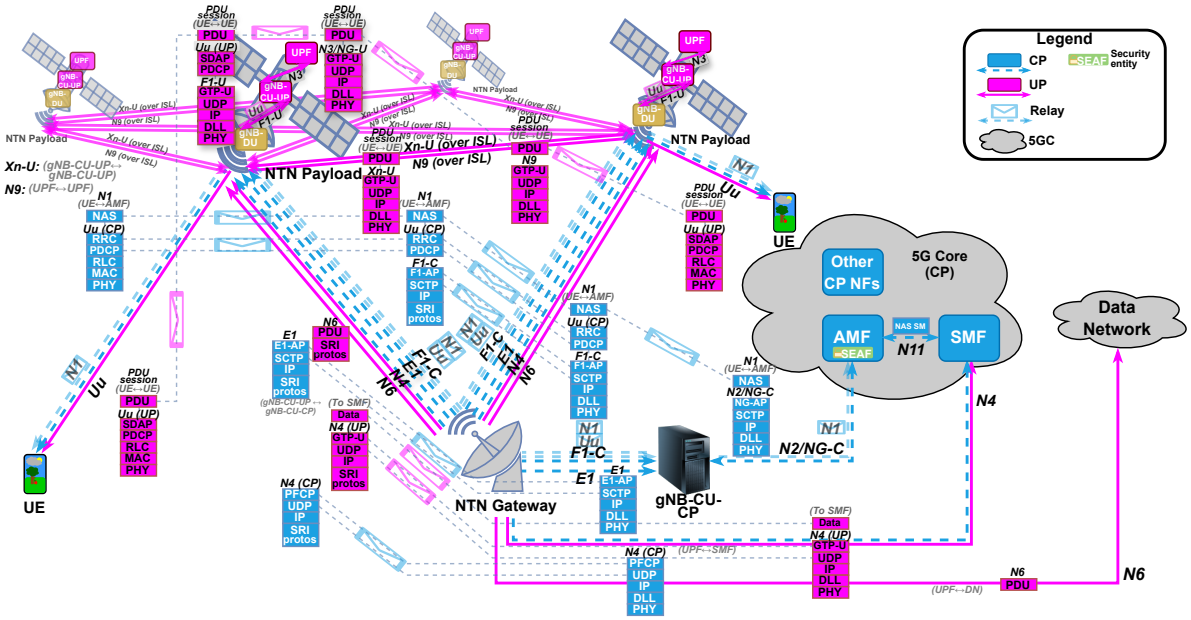



**Figure 2.14:** Architecture of the NTN UE-Satellite-UE communication scenario (based on [50]).

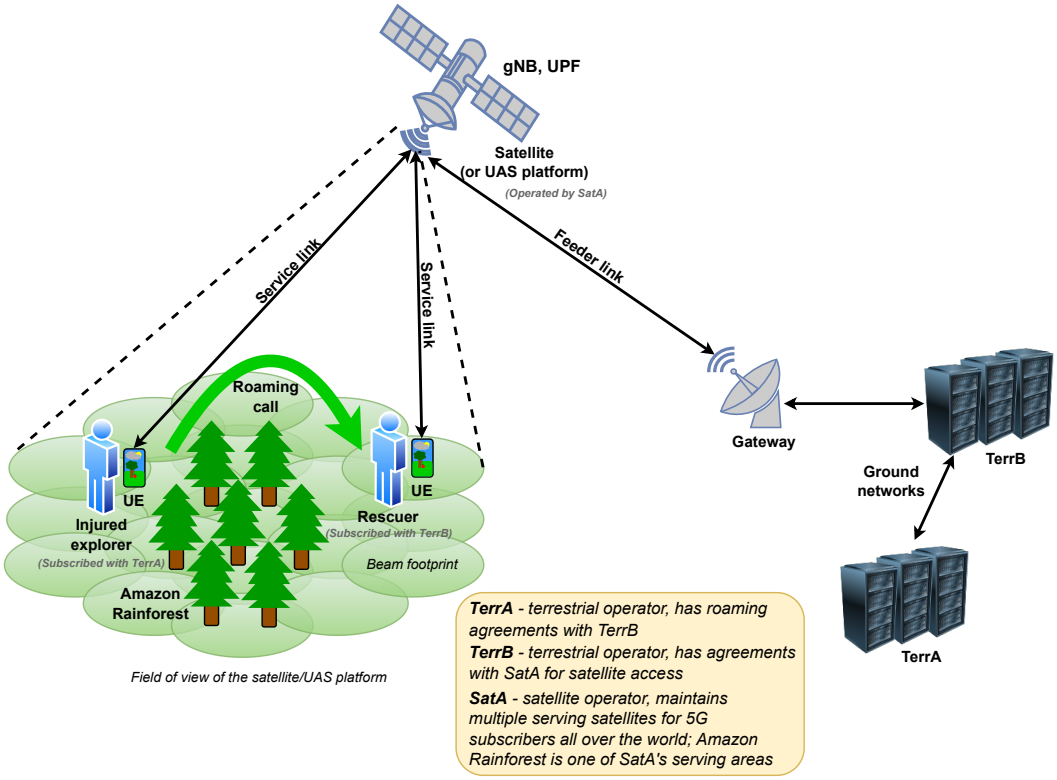



**Figure 2.15:** Possible use case for UE-Satellite-UE communication: an example of a phone call through one satellite without going through the ground network (based on [53]).

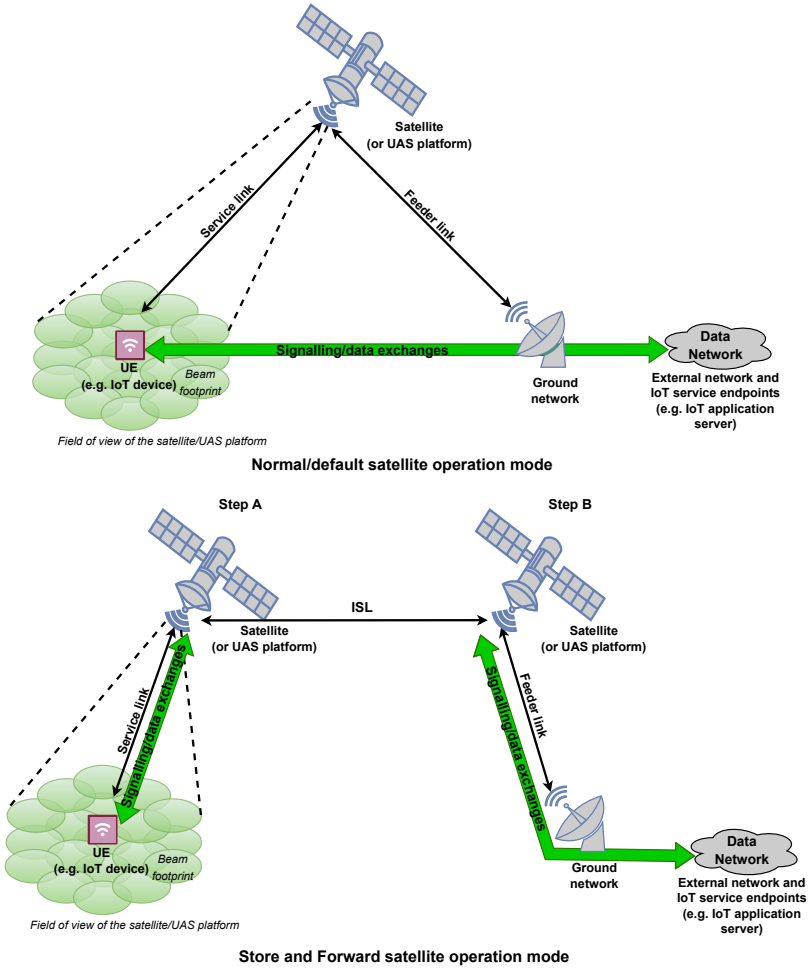



**Figure 2.16:** 5G NTN in a normal/default operation and S&F operation modes (based on [53]).

### 2.3.6. Store and Forward satellite operation

In the Store and Forward (S&F) satellite operation mode, the 5G system is able to provide some degree of service (in storing and forwarding the data) when the connection to the satellite is periodically or temporarily unavailable [53, 221]. For example, the system can offer communication service for UEs that are within the coverage area of a satellite but do not have a simultaneously active feeder link connection with the ground segment. This is especially important for delay-tolerant IoT services provided by satellites outside the GEO orbit (e.g. LEO or MEO). An example where S&F satellite operation mode can be used is Short Message Service (SMS), since it does not require an end-to-end connectivity between the endpoints (e.g. UE and an application server) but only between the endpoints and the SMS centre that functions as an intermediary node responsible for storing and relaying messages.

Under S&F satellite operation mode, the end-to-end exchange of signalling and data traffic is split into two steps that are not concurrent at a time (see Figure 2.16) [53]. In the first step, the UE and the satellite exchange signalling or data over an active service link connection. The satellite is not connected to the ground network, i.e. it does not have an active feeder link connection. In the second step, when the connectivity path between the satellite and the ground network is set up (i.e. the feeder link connection is active), communication between them can take place. Thus, the satellite transitions from being connected to the UE in the first step to being connected to the ground segment in the second step. This is different from the normal/default satellite operation mode that requires both service and feeder links to be active at the same time for the signalling or data exchange to take place, i.e. there must be a continuous end-to-end connectivity between the UE, the satellite, and the ground segment. Note that we do not cover the S&F scenario in our security analysis, leaving it for future work.

# 3

# Related work

This chapter presents a literature review which aims to identify which research has already been conducted into security of 5G terrestrial and non-terrestrial networks. First, we explore the existing knowledge of terrestrial networks, their security mechanisms, and attacks on them. Then, we investigate the literature on non-terrestrial networks, with the focus on their security. Next, we highlight the standardization efforts made by 3GPP into the architecture and security of both terrestrial and non-terrestrial networks. We also briefly discuss the NSA's CNSA Suite, which could provide directions for improvement for 3GPP cryptographic profiles. Finally, we raise some open research questions and gaps in the existing literature, pointing out the areas of further interest, which motivate the need for our study.

## 3.1. Security of 5G terrestrial networks

Mahyoub et al. [246] studied critical interfaces of a 5G system, i.e. interfaces that are connected to an external network and/or transmit sensitive (user) information: N1, Xn, F1, N2, N3, N4, SBI, N9, N32, and N6. They first summarized the mandatory and optional security recommendations proposed by the major Standardization Development Organizations (SDOs), such as 3GPP/ETSI, IETF, ITU, and GSMA. Then they identified threats to each of these interfaces when proper security measures are not implemented and classified these threats according to the STRIDE model [258].

Another study by Holtrup et al. [187] conducted a more generic risk analysis of 5G NSA and SA networks, identifying possible threats and threat vectors. They discussed 12 threat scenarios affecting the radio access and the core network and also classified them according to the STRIDE model. Finally, they proposed mitigations and security controls for the identified threat scenarios.

Two studies by Eleftherakis et al. [137, 138] analysed pre-5G attacks and the weaknesses that made them possible, such as transmission of IMSI in plain text, lack of RRC message ciphering, and transmission of UE measurement reports and UE radio capabilities before establishing a secure channel. They discovered that some pre-5G attacks have been defeated by mandatory (e.g. integrity protection of RRC and NAS messages, secured transmission of radio capabilities) or optional (e.g. UP integrity protection, concealment of SUPI) security measures. However, since network operators may decide not to use optional security mechanisms or may incorrectly implement mandatory measures, some weaknesses can still be exploitable. The authors also discussed some new attacks specific to 5G, e.g. targeting Integrated and Sensing based applications, satellite networks, and Ambient-IoT devices.

A holistic analysis of the first 3GPP release of the 5G security specifications has been conducted by Jover et al. [206], who discussed several insecure protocol edge cases, challenges, and limitations resulting from infeasible assumptions and requirements. At a high level, they analysed the security architecture of the 5G RAN, the main requirements, procedures, and deployment challenges in the context of the proposed security architecture (TS 33.501). The authors showed that 5G standards were still vulnerable to known LTE protocol attacks exploiting unprotected pre-authentication messages.

Non-Access Stratum (NAS) signalling security has been systematically analysed by Hu et al. [192] using TAMARIN [254], a tool for symbolic modelling and formal analysis of security protocols. Applying such a symbolic model analysis to the registration, identification, authentication, security mode command, service request, and deregistration procedures revealed 10 attacks exploiting vulnerabilities in the NAS signalling. The main reason for these attacks was the unconditional trust between UE and gNB, allowing an attacker to establish a connection with any victim UE, as well as lack of protection for the pre-authentication RRC and NAS messages. The authors verified the attacks on a testbed using Universal Software Radio Peripheral (USRP) devices, commercial mobile phones, and a precommercial 5G test network, and proposed a defence mechanism using the existing home network public-private key pair to give a new key pair to the gNB in order to provide authenticity to the NAS messages sent to the UE.

Security of NAS and RRC layers has also been studied by Hussain et al. [194] using the property-guided formal verification framework they developed, which follows the counterexample-guided abstraction-refinement principle (CEGAR) [114]. The constructed formal model included 5G procedures in the initial registration, deregistration, paging, configuration update, handover, and service request, and exposed 11 new attacks, exploiting protocol design weaknesses in the NAS layer, the RRC layer, and in both layers (cross-layer attacks). The authors also listed 5 attacks inherited from LTE [193, 358], which were still applicable to 5G networks. However, they did not verify the discovered attacks in a 5G commercial network or using an open-source 5G protocol stack, and did not propose any defences, as this would require modifying the protocol.

Sullivan et al. [376] investigated security issues in 5G networks from the perspective of the layers of the Open Systems Interconnection (OSI) model [197]. For each OSI layer, they described the present weaknesses, vulnerabilities, and threats, and listed existing security solutions and (open) challenges. They emphasized the need for ensuring security in all OSI layers, since no single layer can provide proper security to a 5G system.

Table 3.1 summarizes the listed studies. We build up on top of these works and perform a security analysis of 5G TN and 5G NTN architectures, including the review of the cryptographic profiles for the identified security measures. Other works on 5G TN security focus on bidding-down attacks [208], (D)DoS attacks or signalling storms [70, 183, 423], issues in the 5G-AKA protocol [83, 220, 414, 97, 124], issues in the SUCI mechanism [111, 212], base station authentication [195, 364, 415], fuzzing [86, 349, 384, 163, 365, 413], and unified policy control scheme [171]. Finally, ENISA has published multiple reports related to 5G security and its threat landscape [139, 140, 141, 142]. In section 5.5, we review six selected literature attacks (for all analysed attacks, see Appendix B).

**Table 3.1:** Summary of the relevant related work for 5G security in TNs and NTNs.

| Study | TN | NTN | Key contributions |
|---|---|---|---|
| **Mahyoub et al., 2024 [246]** | ✓ | ✗ | • Analysed the critical interfaces of a 5G system<br>• Summarized security measures proposed by the major SDOs (3GPP/ETSI, IETF, ITU, GSMA)<br>• Identified threats and classified them based on the STRIDE model |
| **Holtrup et al., 2021 [187]** | ✓ | ✗ | • Performed a generic risk analysis of 5G NSA and SA networks<br>• Identified and analysed 12 threat scenarios, classifying them based on the STRIDE model |
| **Eleftherakis et al., 2024 [137]** | ✓ | ✗ | • Discussed 12 existing pre-5G attacks violating User Identity Confidentiality and described the corresponding weaknesses<br>• Identified 10 mitigation mechanisms against these attacks proposed in 5G<br>• Described 7 recent 5G attacks with the corresponding weaknesses, and whether and how they are mitigated by the 5G mitigation mechanisms |
| **Eleftherakis et al., 2024 [138]** | ✓ | ✗ | • Compared real 5G NSA and SA networks and the emulated OpenAirInterface (OAI) 5G SA network against 8 pre-5G attacks and their level of compliance with the 5G security measures<br>• Found two new potential attacks against UE privacy |
| **Jover et al., 2019 [206]** | ✓ | ✗ | • Performed a holistic analysis of the first release of the 5G security specifications (3GPP TS 33.501), focusing on the NG-RAN<br>• Analysed the security architecture and the underlying security requirements, procedures, and assumptions, assessing them in the context of known (LTE) and new protocol attacks |

*Continued on the next page*

**Table 3.1** *(continued from the previous page)*

| Study | TN | NTN | Key contributions |
|---|---|---|---|
| **Hu et al., 2019 [192]** | ✓ | ✗ | • Formally analysed NAS signalling security using TAMARIN prover<br>• Proposed 10 attacks on the NAS signalling and a PKI defence mechanism to address the UE's unconditional trust to the gNB |
| **Hussain et al., 2019 [194]** | ✓ | ✗ | • Formally analysed security of NAS and RRC layers and their procedures<br>• Proposed 11 new attacks on 5G specifications and listed some attacks inherited from LTE that were still relevant in 5G |
| **Sullivan et al., 2021 [376]** | ✓ | ✗ | • Performed a security analysis of a 5G system for each of the seven layers of the OSI model |
| **Yan et al., 2021 [408]** | ✗ | ✓ | • Studied security requirements and key security technologies for 5G and satellite converged communication network, or SCCN (based on TR 38.811)<br>• Proposed the security architecture of the 5G SCCN |
| **Ahmad et al., 2022 [64]** | ✗ | ✓ | • Analysed the security landscape of the integrated satellite and terrestrial networks<br>• Discussed the key security challenges in satellite-to-satellite, satellite-to-ground stations, and satellite-to-UE communications |
| **Salim et al., 2024 [350]** | ✗ | ✓ | • Presented a comprehensive survey into Satcoms security<br>• Identified cyberattacks for the space, ground, and links segments<br>• Discussed the state-of-the-art cybersecurity strategies for the three segments of Satcoms systems<br>• Summarized the main lessons learned, proposed future research directions |
| **Tedeschi et al., 2022 [379]** | ✗ | ✓ | • Conducted a survey on link-layer SATCOM security<br>• Classified the existing literature into physical-layer security and cryptographic techniques, and discussed the offered security services<br>• Identified and proposed novel future research directions |
| **Lee et al., 2024 [230]** | ✗ | ✓ | • Summarized the latest trends in NR-NTN and IoT-NTN security<br>• Performed a general comparison of transparent and regenerative payload architectures<br>• Presented general and NTN-specific security requirements |
| **Li et al., 2022 [237]** | ✗ | ✓ | • Performed a high-level security analysis of the gNB-DU on board NTN architecture, summarizing the main cryptographic solutions to protect the exposed F1 interface |
| **Our work** | ✓ | ✓ | • Performed an extensive security analysis of 5G TN architecture, focusing on 10 non-SBI interfaces, including a review of the 3GPP cryptographic profiles, their comparison with the NSA's CNSA (2.0) Suite, and a review of 30 literature attacks on 5G TN (with 6 attacks analysed both in TN and NTN)<br>• Presented the first comparison of the security architectures of four different NTN deployment scenarios: Transparent payload, Full gNB on board, Split CU-DU, and UE-Satellite-UE communication<br>• Presented the first of its kind head-to-head comparison of 3GPP TN and NTN security architectures<br>• Implemented a flooding attack against the gNB using OpenAirInterface and evaluated the attack in TN and NTN settings |

## 3.2. Security of 5G non-terrestrial networks

While many studies have been conducted into the integration of satellites into the 5G system [177, 248, 136, 344, 218, 424, 240], little research has been done specifically into the security of 3GPP 5G NTNs. Below, we present some works analysing security of satellite communications systems and non-terrestrial or satellite networks.

Yan et al. [408] proposed security architecture of the 5G satellite converged communication network (SCCN). They listed security challenges caused by open network environment, dynamic changes in the network topology, heterogeneous interconnection, and low on-board processing capabilities of satellites, as well as security requirements, such as strict identity authentication, lightweight communication security, enhanced availability protection, and fine-grained resource sharing and isolation. For each technical requirement, they discussed possible solutions. For example, to protect user data communication, they proposed two mutually non-exclusive solutions: UE-DN's end-to-end security and UE-NR CU security (achievable with the CU-DU split architecture). They also advocated for the "forwarding on-satellite, processing off-satellite" principle to ensure lightweight communication security.

Security of satellite-terrestrial communications in NTNs was studied by Ahmad et al. [64]. They presented security challenges in the integrated environment of satellite and terrestrial networks from three different perspectives: satellite-to-satellite communications (within the same orbit, such as LEO-LEO, and between different orbits, such as LEO-MEO or GEO-MEO), satellite-to-ground stations communications (between satellites and base stations or gateways connecting satellites to UEs), and satellite-to-ground UE communications (between satellites and directly user devices on the ground). The authors pointed out that the main challenges originate from the mobility of the satellites, which makes the deployment of encryption technologies more challenging, primarily due to complexity in key distribution; higher bit error rate and longer link delays, as well as limited computing resources on satellites, hindering the deployment of efficient state-of-the-art security solutions. For each of the three analysed categories, the authors also discussed possible mitigations.

Salim et al. [350] conducted a comprehensive survey into Satellite Communications (Satcoms) security, identifying vulnerabilities and different types of cyberattacks for the three main segments of Satcoms systems: space segment, ground segment, and links segment. The authors also surveyed the state-of-the-art Satcoms cybersecurity strategies for the three segments, including encryption, authentication, anti-tamper mechanisms, access control, network segmentation, intrusion detection and prevention techniques, and development of secure protocols and standards. Finally, they summarized the main learned lessons, such as the need for a balance between security and cost-effectiveness, the importance of sharing threat intelligence and adopting Defence-in-Depth strategy, the significance of attack resilience planning, as well as the difficulty of securing legacy systems.

In another survey on SATCOM security, Tedeschi et al. [379] summarized the link-layer security threats, solutions, and mitigation techniques related to designing and deploying SATCOM systems. They classified the relevant literature on security solutions into physical-layer approaches (such as information-theoretic security schemes, anti-jamming strategies, and anti-spoofing schemes) and cryptography techniques (such as authentication, key agreement, and (quantum) key distribution), and analysed how the offered security services and schemes guarantee the desired security objectives. Finally, they identified new future research directions and additional challenges within each research domain.

A survey by Lee et al. [230] summarized the latest trends in the NTN security field, focusing on NR-NTN and IoT-NTN. They analysed and compared two payload architectures, namely transparent and regenerative payloads, and discussed security requirements for NTN, both general security requirements that apply to all NTN operations (such as data confidentiality, integrity, availability, authentication, and access control), and specific security requirements that aim to address problems inherent to NTN (such as handover security, energy-efficient security, adaptive security protocols, anti-jamming and anti-spoofing). Unlike the survey authors, we focus specifically on 3GPP 5G NTN architecture and also analyse other NTN architectures, such as Split CU-DU and UE-Satellite-UE communication, with a larger focus on security.

Li et al. [237] analysed the security of the gNB-DU processed payload, one of the NTN architectures with the on-board processing capabilities. The authors gave an overview of the main security protocols for protecting the exposed F1 link between the gNB-DU and gNB-CU, including IPsec, IKEv2, and DTLS, and emphasized the importance of migrating to quantum-resistant algorithms in the future. However, their analysis was relatively high-level and could be extended further to also analyse the specific cryptographic profiles, as well as their implementation and usage requirement levels.

Table 3.1 summarizes the key contributions of the above-mentioned works. We complement them by taking a different approach in our research. We compare the security architecture of 5G NTN with the security architecture of 5G TN, and we also compare different NTN deployment scenarios with each other. Furthermore, we focus directly on the measures proposed by 3GPP. The main contributions of our thesis, both for terrestrial and non-terrestrial 5G networks, are summarized at the end of Table 3.1.

## 3.3. 3GPP standardization efforts

Numerous 3GPP technical specifications (TS) and technical reports (TR) have to be considered in order to perform an in-depth security analysis of 5G NTN architecture. Below, we list some of the documents that are relevant to our study.

The 5G system architecture is defined in TS 23.501 [58], while TS 23.502 [32] defines the procedures and Network Function (NF) services. The overall description of NG-RAN is presented in TS 38.300 [27] and the architecture (including the gNB split into gNB-DU and gNB-CU) is described in TS 38.401 [19]. These documents give a comprehensive overview of how a 5G system (NG-RAN and CN) works, and can be used as a reference for the relevant procedures when analysing the security architecture.

TS 33.501 [33] specifies the security architecture of the 5G system, including security features and security mechanisms. TS 33.210 [17] contains cryptographic profiles for security above IP layer, and TS 33.310 [16] defines the authentication framework (e.g. certificate profiles). These documents are essential for analysing the security architecture of a 5G system, which will be done in chapter 5 for terrestrial networks with the focus on NG-RAN and non-SBI interfaces.

TR 38.811 [51] defines the NTN deployment scenarios (transparent payload and regenerative payload with gNB or gNB-DU on board) and related system parameters, whereas TR 38.821 [37] presents the protocol stacks for these deployment modes. TR 23.700-29 [50] studies generic regenerative payload architecture, Store and Forward (S&F) satellite operation, and UE-Satellite-UE communication enhancements for a 5G System. Finally, TR 33.700-29 [54] studies the security and privacy aspects of 5G satellite access for regenerative, S&F, and UE-satellite-UE communication enhancement architectures, although at the time of writing only solutions for S&F satellite are listed. These documents are important to consult when analysing the NTN architecture, which will be done in chapter 6.

## 3.4. CNSA Suite

The US National Security Agency (NSA) is responsible for approving cryptographic solutions to protect US National Security Systems (NSS), which are used to secure data with confidentiality requirements for years after system deployment and are thus planned over decade timescales [305]. With the recent progress in quantum computing research posing a threat in the future (see subsection 5.6.4), the protocols that are now using quantum-unsafe algorithms will eventually have to be addressed. Considering the long lifetime and unique nature of NSS, as well as the costs of migrating the current infrastructure to new quantum-resistant algorithms, it is crucial to develop a transitioning plan to ensure the confidentiality of the long-life data on the NSS.

In 2015, NSA published the Commercial National Security Algorithm Suite (CNSA) [116, 305] (see Table 3.2) – a revised set of cryptographic algorithms which can be used for NSS protection while the quantum-resistant algorithms are designed and standardized by the National Institute of Standards and Technology (NIST) [305, 306]. NSA's CNSA Suite is applicable for configuration, operation, and capabilities of all elements of US NSS, as well as other US Government systems processing highly valuable information [121]. The CNSA Suite aims to offer vendors and IT users short-term flexibility to meet their information assurance interoperability requirements by using current algorithms with increased security parameters. Such flexibility is intended to help vendors and customers avoid making two major transitions is a fairly short time while shifting to quantum-safe cryptography.

**Table 3.2:** Commercial National Security Algorithm (CNSA) Suite 1.0 and 2.0, based on [305, 311]

| Category | CNSA 1.0 | CNSA 2.0 |
|---|---|---|
| **Encryption** | • **AES with 256-bit keys** (FIPS 197 [277]) | • **AES with 256-bit keys** (FIPS 197 [277]) |
| **Key establishment** | • **ECDH using P-384 curve** (SP 800-56A [79])<br>• **DH with at least 3072-bit modulus** (RFC 3526 [219])<br>• **RSA with at least 3072-bit modulus** (SP 800-56B rev 1 [73]) | • **ML-KEM-1024** (FIPS 203 [291]) |
| **Digital signatures** | • **ECDSA using P-384 curve** (FIPS 186-4 [283])<br>• **RSA with at least 3072-bit modulus** (FIPS 186-4 [283]) | • **ML-DSA-87** (FIPS 204 [290]) |
| **Hashing** | • **SHA-384** (FIPS 180-4 [302]) | • **SHA-384** (FIPS 180-4 [302])<br>• **SHA-512** (FIPS 180-4 [302]) |

In September 2022, NSA released CNSA 2.0 Suite [117, 311] (see Table 3.2) containing quantum-resistant algorithms approved for the use in NSS [311, 310]. The algorithms listed in CNSA 2.0 are an update to the algorithms listed in the CNSA (1.0) and have been evaluated as secure against classical and quantum computers. Eventually, these quantum-resistant algorithms will be required for NSS.

Some Requests for Comments (RFCs) have been submitted to specify the profiles for Internet protocols for applications supporting the CNSA Suite. For example, RFC 9206 [122] specifies the conventions for using the CNSA Suite algorithms in IPsec, defines CNSA-based User Interface (UI) suites describing security configurations for IPsec ESP and IKEv2 protocols, and provides other constraints for algorithm selection and configuration. An Internet-Draft (I-D) (at the time of writing) in [180] specifies the IPsec/IKEv2 profile to comply with the CNSA 2.0 Suite. Another example is RFC 9151 [121], specifying the (D)TLS 1.2 and 1.3 profiles for use with the CNSA Suite, with an I-D in [84] for the CNSA 2.0 Suite. Finally, RFC 8603 [201] specifies a base profile for X.509 v3 Certificates and X.509 v2 Certificate Revocation Lists (CRLs) [95] for applications complying with the CNSA Suite, with an I-D in [200] for the CNSA 2.0 Suite. Note that these RFCs have been submitted on the Independent Submission stream and are not endorsed by the Internet Engineering Task Force (IETF) responsible for developing RFCs.

Although the CNSA (2.0) Suites are intended for the US NSS, the comparison between 3GPP and CNSA requirements can give a generic roadmap for the migration to post-quantum cryptography (see subsection 5.6.4). In addition, some NTN deployments may have governmental applications, which will require much stricter security requirements. In section 5.2, we will compare the algorithms allowed by 3GPP with the algorithms allowed by CNSA (2.0), based on RFC 9206 [122], RFC 9151 [121], and RFC 8603 [201], with the respective I-D's in [180], [84], and [200].

## 3.5. Open research questions

Extensive research has been done into security measures for 5G terrestrial networks, as discussed above. However, one open question is whether the cryptographic profiles adopted by 3GPP for the 5G interfaces are sufficient, as of the start of 2025. While Mahyoub et al. [246] described the protection measures for 5G critical interfaces, they did not mention which cryptographic profiles are used on these interfaces (e.g. which encryption and authentication transforms are mandated, recommended or prohibited for IPsec, or which cipher suites shall, should or shall not be supported for DTLS). The field of cryptography develops all the time: new algorithms are created, offering higher security guarantees, while existing algorithms are discovered to provide much lower security guarantees than was initially thought, or are badly broken, for instance, due to increased computation power of adversaries [405]. As a result, implementation requirements for cryptographic algorithms, as well as the guidelines for their usage, need to be periodically revised and updated to keep up with the reality. Flaws in specifications affect all network equipment following the specification [208]. Therefore, it is important that 3GPP standards do not leave room for insecure algorithms and modes.

Research into 5G non-terrestrial networks is much scarcer, as their architecture and deployment modes are still being designed and standardized. To the best of our knowledge, no previous works performed a head-to-head comparison of 5G terrestrial and non-terrestrial networks from the perspective of security architecture and exposed interfaces. The nature of NTN differs from that of TN, due to higher processing constraints in a satellite and the exposure of data exchange between a UE and satellite, which allows eavesdropping, tampering, and other attacks from a wider geographical scale than in TN. Furthermore, other security provisions might have to be introduced in the NTN context if the cryptographic solutions that worked in TN are not infeasible to deploy due to resource constraints.

Finally, we could not find any works comparing different NTN architectures with each other from the security perspective. Already defined scenarios Full gNB on board and CU-DU split [37], as well as currently under design UE-Satellite-UE communication [50], differ in terms of exposed interfaces and security threats. Therefore, the choice of which architecture scenario is best for a particular situation will depend on security considerations and the risk attitude of satellite and mobile network operators. The protection measures will also need to be implemented based on the chosen deployment scenario.

We believe that closing these gaps is crucial to enhance the security of 5G in the context of NTN. This motivates the need to review the cryptographic profiles proposed by 3GPP for 5G networks (both TN and NTN) and compare them to the CNSA (2.0) Suite, analyse the differences between 3GPP TN and NTN regarding the security architecture, and investigate how NTN architectures differ from each other in terms of security. Addressing these gaps is the main goal of our work.

# 4

# Methodology

Now that we have studied the relevant related work and identified the gaps in the existing state-of-the-art literature, we proceed with formulating the research questions and subquestions for our thesis. We then define the scope of our research in terms of the interfaces and scenarios that we consider in our security analysis. Finally, we present a step-by-step research plan that we will follow in order to answer the formulated research questions and subquestions.

## 4.1. Research questions

To address the identified research gaps, we focus on three different parts in our thesis. First, we investigate the security architecture and security measures for 5G TN, as these measures also apply for 5G NTN. Second, we map the identified security mechanisms to different NTN deployment scenarios and compare them with each other and with TN. Third, we implement and demonstrate one attack against an open-source 5G implementation in terrestrial and non-terrestrial setup. This brings us to the following research questions:

1. **"What is the current security architecture of 3GPP 5G terrestrial networks?"**
    a. *"What are the current security measures and protection requirements proposed by 3GPP?"*
    b. *"How do 3GPP cryptographic profiles compare to the requirements stated by NIST and CNSA (2.0) Suite?"*
    c. *"What are the relevant literature attacks on the security architecture of terrestrial networks?"*
    d. *"Can we find any new weaknesses in the security architecture of terrestrial networks?"*
2. **"What is the current security architecture of 3GPP 5G non-terrestrial networks?"**
    a. *"How do the current security measures proposed by 3GPP map to non-terrestrial networks?"*
    b. *"How are the proposed NTN deployment options different from each other in terms of security?"*
    c. *"What is the impact of the literature attacks for terrestrial networks on non-terrestrial networks?"*
    d. *"What are the differences in the security architecture of terrestrial and non-terrestrial networks?'*
3. **"Can we successfully perform a flooding attack against gNB in 3GPP 5G terrestrial and non-terrestrial networks?"**
    a. *"What is the impact of the attack in terrestrial networks?"*
    b. *"What is the impact of the attack in non-terrestrial networks?"*
    c. *"What are the necessary and sufficient conditions for the attack?"*
    d. *"What are the possible mitigations to protect against the attack?"*

Each research question builds on top of the previous questions. The first research question allows us to summarize the current 3GPP standardization efforts for 5G security and check if we can discover

any problems already in TN (e.g. insufficient protection mechanisms, space for vulnerable algorithm versions etc.). The second research question allows us to map the identified security mechanisms to NTN deployments to and compare the security architectures of 3GPP TN and NTN. The third research question allows us to assess the practical feasibility and impact of a specific attack in terrestrial and non-terrestrial networks, as well as analysing and comparing the observed results.

## 4.2. Research scope

Since the field of 5G networks is very broad, we need to define the scope of our thesis. First, we focus only on standalone (SA) mode as the long-term solution for 5G network deployments, leaving non-standalone (NSA) networks outside the scope. Second, we do not consider roaming scenarios and assume that the UE always communicates within its home network. While the roaming mode expands the possible attack surface, it is a separate topic on its own, which we leave as future work. Third, we focus on the following four NTN scenarios or deployment modes:

1. **Transparent payload** [37] – in this scenario, the satellite does not perform any decoding and simply forwards the traffic to the gNB(-DU) on the ground.
2. **Full gNB on board** [37] – in this scenario, the entire gNB functionality is on the satellite (i.e. both the DU and CU parts of a gNB are deployed on board a satellite).
3. **Split CU-DU** [37] – in this scenario, gNB-DU is on the satellite, while gNB-CU is on the ground (the gNB split corresponds to split option 2-1 [52], with PDCP and RRC terminating in gNB-CU).
4. **UE-Satellite-UE communication** [50] – in this scenario, part of the core network (UPF) together with gNB-DU and gNB-CU-UP are on the satellite, while gNB-CU-CP is on the ground (the gNB split corresponds to split option 2-2 [47, 52]). We consider the gNB and UPF to be deployed on every satellite, as this case covers all exposed interfaces; however, this does not have to be the case.

We focus only on the interfaces that are affected by NTN deployments, such as the interfaces that are exposed in at least one of the studied NTN scenarios. These are the non-SBI interfaces: Uu, N1, N2, N3, N4, N6, N9, Xn, F1, and E1. Thus, compared to Mahyoub et al. [246], we do not cover SBI (since it is not affected by the NTN deployment) and N32 (since we do not consider roaming), while we do cover the E1 interface. Table 4.1 shows each of the studied interfaces and the NTN scenarios by which they are affected.

**Table 4.1:** Studied interfaces and the corresponding NTN scenarios where they are affected.

| Interface | Plane | Endpoints | Exposed in NTN scenarios |
|---|---|---|---|
| **Uu (AS)** | CP + UP | UE ↔ gNB(-CU) | • Transparent payload<br>• Full gNB on board<br>• Split CU-DU<br>• UE-Satellite-UE communication |
| **N1 (NAS)** | CP | UE ↔ AMF | • Transparent payload<br>• Full gNB on board<br>• Split CU-DU<br>• UE-Satellite-UE communication |
| **N2 (NG-C)** | CP | gNB(-CU) ↔ AMF | • Full gNB on board<br>• UE-Satellite-UE communication |
| **N3 (NG-U)** | UP | gNB(-CU) ↔ UPF | • Full gNB on board<br>• UE-Satellite-UE communication |
| **N4** | CP + UP | SMF ↔ UPF | • UE-Satellite-UE communication |
| **N6** | UP | UPF ↔ DN | • UE-Satellite-UE communication |
| **N9** | UP | UPF ↔ UPF | • UE-Satellite-UE communication |
| **Xn** | CP + UP | gNB(-CU) ↔ gNB(-CU) | • Full gNB on board<br>• UE-Satellite-UE communication |
| **F1** | CP + UP | gNB-DU ↔ gNB-CU | • Split CU-DU<br>• UE-Satellite-UE communication |
| **E1** | CP | gNB-CU-CP ↔ gNB-CU-UP | • UE-Satellite-UE communication |

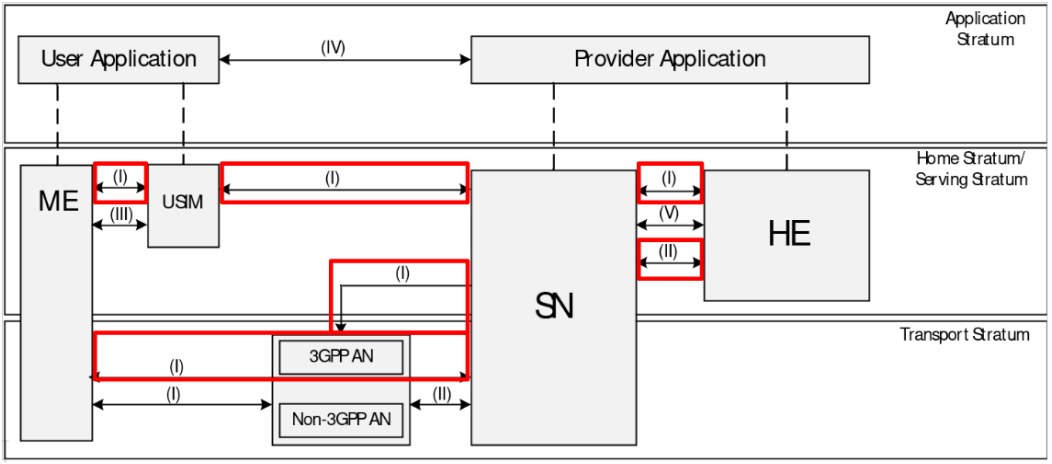



**Figure 4.1:** Overview of the 5G security architecture, as defined in 3GPP TS 33.501 [33], and the parts that we focus on.

From the perspective of the 3GPP security architecture [33] (see Figure 4.1), we focus on the network access security (I) and the network domain security (II). The former focuses on allowing a UE to securely authenticate and access services via the network, while the latter is responsible for secure exchange of CP and UP data between network nodes. Other security architecture parts, namely user domain security (III, secure user access to ME), application domain security (IV, secure message exchange between the applications in the user domain and in the provider domain), SBA domain security (V, secure communication of the SBA NFs within the serving network domain and with other network domains), and visibility and configurability of security (VI, informing the user if a security feature is operational), fall outside the scope of our work. Note that we only focus on the 3GPP access to the 5G network, leaving the non-3GPP access as future work.

## 4.3. Research approach

Having defined the research questions and the scope of our thesis, we now describe the three main steps of our methodology. Figure 4.2 provides a concise summary of these steps.

As the first step in our methodology, we perform an in-depth analysis of the security measures proposed by 3GPP for the 5G TN security architecture (as defined in TS 33.501 [33]). We identify what are the suggested protection mechanisms for the chosen 10 non-SBI interfaces, as well as what these interfaces protect. Furthermore, we investigate what are the requirements for the profiles of the cryptographic algorithms that are used on these interfaces (as specified in TS 33.210 [17] and TS 33.310 [16]), and which of them are mandatory, recommended, optional, or prohibited. We analyse which RFCs are referenced in the 3GPP documents and if some 3GPP provisions have been obsoleted by RFCs or other sources (e.g. NIST). We also search for any possible contradictions between the 3GPP specifications and the RFCs that they reference (e.g. if some algorithm or cipher suite is prohibited in the RFCs but is allowed by 3GPP). Moreover, we compare the algorithms allowed by 3GPP with the CNSA 1.0 and CNSA 2.0 Suite algorithms to get a general roadmap for transitioning to post-quantum cryptography. Finally, we summarize and analyse the relevant literature attacks and weaknesses against the 3GPP TN specifications. Even though we perform this methodology step for TN, it is also applicable for NTN. The security analysis for the TN part of our thesis is performed in chapter 5.

As the next step of our methodology, we perform a security analysis of the chosen four NTN scenarios. We map the identified security measures to the architecture of the studied NTN deployment modes and compare them head-to-head with each other in terms of their benefits and drawbacks regarding security. Next, we revisit the selected literature attacks against TN in the context of NTN to analyse which impact they have in the NTN deployments. Finally, we perform a head-to-head comparison of the TN and NTN architectures to see how they differ from each other from the security perspective (e.g. some threats may be more relevant in NTN deployments than in TN deployments and vice versa). The security analysis for the NTN part of our thesis is performed in chapter 6.

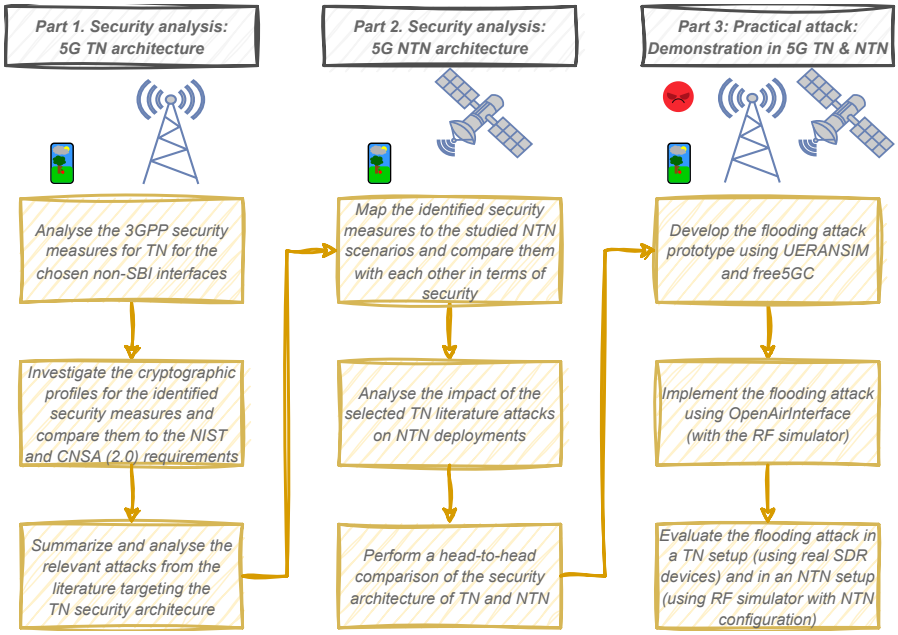



**Figure 4.2:** Summary of the three main steps in the methodology of our thesis.

As the last step of our methodology, we design and implement a flooding attack against the gNB in a TN and NTN setting using a real 5G implementation. The attack is based on the work by Kim et al. [215], who demonstrate an analogous attack against an LTE network. For this practical part of the thesis, there are multiple available 5G implementations that we could use. Among the existing open-source software, there are Open5GS [231] and free5GC [241] for the core network, UERANSIM [178] for simulating the UE and NG-RAN, srsRAN [369] for NG-RAN, and OpenAirInterface (OAI) [322] for 5GC, NG-RAN, and UE. From the proprietary closed-source software, there is Amarisoft [68], which is another 5G implementation that can be used for TN and NTN.

First, we develop the initial prototype of our flooding attack using UERANSIM with free5GC. Given that UERANSIM simulates the layers below RRC, we can abstract away the heavy radio part to investigate the impact of lightweight rogue UEs on the gNB. We can see whether the flooding rate is high enough to exhaust the maximum number of allowed RRC connections and to take down the base station. Next, we implement the actual attack using OAI, which allows us to perform the attack in a realistic setting. OAI provides the entire 5G NR stack and the core network together, offers a highly configurable RAN, and is getting increasingly more attention by a growing community [353]. It also has a more complete software stack than srsRAN [369] with respect to the 3GPP specifications. Finally, we evaluate our flooding attack in a TN setup using OAI with real Software Defined Radio (SDR) devices, and in an NTN setup using the OAI RF simulator with the NTN-specific configuration to simulate a GEO satellite and a LEO satellite [321]. The experimental setup and the results of the attack are presented in chapter 7.

All the code for the practical part of our thesis is available in the corresponding GitHub repositories for our UERANSIM fork [422] and our OAI fork [421]. The scripts and the configuration for the performed experiments are available in our thesis repository [420]. Finally, we also make available the source files for the diagrams used in this thesis [419], so that they can be consulted for better readability.

# 5

# Security analysis of 5G terrestrial networks

In order to perform a security analysis of non-terrestrial networks, it is important to first review the security of terrestrial networks, which the main focus of this chapter. We start by summarizing the security requirements and recommendations from 3GPP for each of 10 selected non-SBI interfaces, based on the security architecture standardized in TS 33.501 [33]. Next, we investigate the cryptographic profiles for IPsec, IKEv2, (D)TLS in the context of NDS/IP networks (i.e. 3GPP and fixed broadband networks) based on TS 33.210 [17], since they are applicable for some of our chosen interfaces (N2, N3, N4, N9, Xn, F1, and E1). We also compare these cryptographic profiles with the requirements from NIST and CNSA (2.0) Suite. Then, we check the requirements for ciphering and integrity protection of RRC/NAS signalling and UP data, i.e. Access Stratum (AS) and Non-Access Stratum (NAS) security (Uu and N1 interfaces), and the requirements for the Elliptic Curve Integrated Encryption Scheme (ECIES) profiles for SUCI (N1 interface), based on TS 33.501. Finally, we summarize and analyse some relevant literature attacks against the 5G TN security architecture.

## 5.1. Security protections

Table 5.1 lists the 3GPP security measures we have found for the studied non-SBI interfaces, together with their main functions. These provisions were taken from TS 33.501 [33], primarily from sections 5 (for AS/NAS security), 6.1 (for AKA), and 9 (for the other non-SBI interfaces). The idea of a security table was inspired by the work of Mahyoub et al. [246], however we combined all interfaces together in one table and included additional explanations for the encountered security measures (e.g. which measures are mandatory and optional to support and use). Note that, unlike Mahyoub et al., we did not find recommendations in TS 33.501 to protect the N4 interface using TLS and HTTPS. To give a better overview of what is protected on these interfaces and what are the possible attack vectors if they are not secured, we included the main functions and procedures of these interfaces. For example, N4 is involved in charging control through SMF that controls the functionality of UPF via various rules. If this interface is not integrity protected, an attacker could disable the traffic flow counting and use the mobile services for free. Similarly, if confidentiality of N3 or N9 carrying UP data is not protected, then an attacker would be able to sniff the user traffic.

While this table is not a comprehensive overview of the entire security architecture of 5G TN, it gives a good summary of the security measures, their protection levels, and the protected functions for these interfaces. Security engineers and mobile network operators should consult the actual 3GPP specifications for the security architecture when designing and implementing their networks. However, 5G researchers who want to get an overview of the security architecture of the non-SBI interfaces together with their main functions could save a lot of time by consulting our table instead of reviewing lengthy 3GPP documents. We have also separately listed the sources for the interface functions, so that interested readers could consult the relevant documents for more information.

**Table 5.1:** Security measures proposed by 3GPP for the studied non-SBI interfaces, based on 3GPP TS 33.501 [33].

| Int. | Endpoints | Security measures | Protected functions (attack vectors) |
|---|---|---|---|
| **Uu** *(CP + UP)* | **UE** ↔ **gNB(-CU)** | Confidentiality of RRC signalling and UP:<br>• **NEA0**, **128-NEA1**, **128-NEA2** (by PDCP) *(mandatory to support) (see Table 5.9)*<br>• **128-NEA3** (by PDCP) *(optional to support)*<br>• Optional to use *(but recommended whenever regulations permit)*<br>Authentication (integrity) and replay protection of RRC signalling and UP:<br>• **NIA0**, **128-NIA1**, **128-NIA2** (by PDCP) *(mandatory to support) (see Table 5.9)*<br>• **128-NIA3** (by PDCP) *(optional to support)*<br>• RRC: mandatory to use *(not NIA0)*, except for unauthenticated emergency calls and some exceptions *(see Table 5.9, which also lists RRC messages unauthenticated by design)*<br>• UP: optional to use *(larger packets and higher processing load)*; when not used, NIA0 shall not be used *(unnecessary overhead due to the empty 32-bit MAC with no security benefits)*<br>• *NIA0 must be disabled in gNB in the deployments where unauthenticated emergency session support is not required by regulations*<br>Replay protection (CP and UP):<br>• **PDCP COUNT** for DL and UL *(32 bits, starts with 0, bearer-specific)*: receiver must only accept each incoming PDCP COUNT value once within the same AS security context<br>• **PDCP COUNT check procedure for gNB** to detect maliciously inserted packets; redundant for integrity protected bearers *(optional to use)*<br>RRC UE capability transfer:<br>• The network should activate AS security before running the “RRC UE capability transfer” procedure | CP (RRC sublayer):<br>• **Broadcast of system information related to AS and NAS** *(e.g. NAS common information, information applicable for UEs in RRC_IDLE and RRC_INACTIVE states, information for UEs in RRC_CONNECTED state)*<br>• **Transport of dedicated NAS information** *(messages from NAS to UE and vice versa)*<br>• **Transfer of UE radio access capabilities**<br>• **Establishment/modification/suspension/ resumption/release of an RRC connection between the UE and NG-RAN** *(including assignment and modification of UE identity, e.g. C-RNTI, full I-RNTI)*<br>• **Establishment, configuration, maintenance, and release of Signalling Radio Bearers (SRB), Data Radio Bearers (DRB), MBS (Multicast/ Broadcast Services) Radio Bearers (MRB)**<br>• **Paging initiated by 5GC or NG-RAN**<br>• **Security functions** *(initial AS security activation, i.e. initial configuration of AS integrity protection (SRBs, DRBs) and AS ciphering (SRBs, DRBs); key management)*<br>• **Mobility functions** *(handover and context transfer, UE cell selection and reselection and control of cell selection and reselection)*<br>• **UE measurement reporting, reporting control**<br>UP:<br>• **(Non-guaranteed) delivery of UP PDUs**, i.e. user data, between UE and gNB *(in a PDU session between UE and DN)*<br>*(Sources: 3GPP TS 38.300 [27], TS 38.331 [30], TS 23.501 [58])* |

*Continued on the next page*

**Table 5.1** *(continued from the previous page)*

| Int. | Endpoints | Security measures (3GPP) | Protected functions (attack vectors) |
|---|---|---|---|
| **N1** *(CP)* | **UE** ↔ **AMF** | Confidentiality of NAS signalling:<br>• **NEA0**, **128-NEA1**, **128-NEA2** (by NAS) *(mandatory to support) (see Table 5.9)*<br>• **128-NEA3** (by NAS) *(optional to support)*<br>• Optional to use *(but recommended whenever regulations permit)*<br>Authentication (integrity) and replay protection of NAS signalling:<br>• **NIA0**, **128-NIA1**, **128-NIA2** (by NAS) *(mandatory to support) (see Table 5.9)*<br>• **128-NIA3** (by NAS) *(optional to support)*<br>• Mandatory to use *(not NIA0)*, except for unauthenticated emergency calls and some exceptions *(see Table 5.9, which also lists NAS messages unauthenticated by design)*<br>• *NIA0 must be disabled in AMF in the deployments where unauthenticated emergency session support is not required by regulations*<br>Replay protection:<br>• **NAS COUNT** for DL and UL *(24 bits, starts with 0, bearer-specific)*: receiver must only accept each incoming NAS COUNT value once within the same NAS security context<br>Protection of initial NAS message:<br>• UE includes the initial NAS message in a NAS Container in the ciphered and integrity protected *NAS Security Mode Complete*, when it has a NAS security context<br>Subscriber privacy:<br>• **5G-GUTI** once the registration is accepted *(mandatory to support, must be periodically reallocated)*<br>• **SUCI** *(optional to use, choice of the home network operator)*<br>– **SUCI null-scheme** when no protection is afforded *(mandatory to support)*<br>– SUPI should not be transmitted in plain text over NG-RAN *(except routing information: MNC, MCC)*<br>– SUPI protection is not required for unauthenticated emergency calls<br>• **PEI** must be transmitted only after NAS security context has been established *(except in emergency registrations)*<br>Authentication methods:<br>• **EAP-AKA'** and **5G AKA** *(mandatory to support; the home network operator decides which method to use)*<br>• **EAP-TLS** *(only intended for private networks or with IoT devices in isolated deployment scenarios)*<br>• **EAP-based secondary authentication** between UE and DN *(optional to use)* | • **Transport of NAS messages between UE and AMF** *(or another CN function via AMF, e.g. for session management signalling, SMS, UE policy, location services)*<br>• Single N1 NAS signalling connection is used for both **registration management** and **connection management (RM/CM)**, and for **session management (SM)** related messages and procedures for a given UE<br>• **UE mobility management (via NAS-MM protocol)** *(including authentication, identification, generic UE configuration update, and security mode control procedures)*<br>• **Session management (via NAS-SM protocol)** *(establishing and maintaining data connectivity between the UE and the DN)*<br>• **Transport of SMS, location services, UE policy container, and some other services**<br>*(Sources: 3GPP TS 23.501 [58], TS 24.501 [25])* |

*Continued on the next page*

**Table 5.1** *(continued from the previous page)*

| Int. | Endpoints | Security measures (3GPP) | Protected functions (attack vectors) |
|---|---|---|---|
| **N2** *(CP)* | **gNB(-CU)** ↔ **AMF** | • CP data on N2 shall be integrity, confidentiality and replay protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to implement)*<br>– **DTLS** over SCTP *(mandatory to support)*<br>• Mutual authentication over N2 between AMF and 5G-RAN:<br>– **DTLS** and/or **IKEv2** *(mandatory to support)*<br>– The identities specified in the end entity certificates shall be used for authentication and policy checks<br>• *On the CN side, a SEG may be used to terminate the IPsec tunnel*<br>• *Using transport layer security (DTLS), does not rule out the use of network layer protection (IPsec). IPsec also hides the network topology*<br>• *Using cryptographic solutions to protect N2 interface is an operator's decision* | • **NG interface management** *(start of NG interface operation, protocol errors etc.)*<br>• **UE context management** *(in AMF and gNB, e.g. to support user individual signalling)*<br>• **UE mobility management** *(for UEs in CM-CONNECTED state, intra-system handover within NG-RAN, and inter-system handover from/to EPS system)*<br>• **Transport of NAS messages** *(UE ↔ AMF)*<br>• **Paging procedure** *(sending paging requests with UE's 5G-S-TMSI to gNBs in the paging area, i.e. TA(s) where the UE is registered)*<br>• **PDU session management** *(NG-RAN part)*<br>• **Configuration transfer** *(request and transfer of RAN configuration information between two RAN nodes via CN)*<br>• **Location reporting** *(AMF can request a gNB to report the UE's current/last known location, or UE's presence in an area)*<br>• **AMF load balancing** *(AMF can indicate its relative capacity to gNB)*<br>*(Sources: 3GPP TS 38.300 [27], TS 38.410 [23], TS 38.413 [22])* |
| **N3** *(UP)* | **gNB(-CU)** ↔ **UPF** | • UP data on N3 shall be integrity, confidentiality and replay protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to implement)*<br>• *On the CN side, a SEG may be used to terminate the IPsec tunnel*<br>• *Using cryptographic solutions to protect N3 interface is an operator's decision* | • **(Non-guaranteed) delivery of UP PDUs**, i.e. user data, between gNB and the UPF, based on GTP-U tunnelling *(in a PDU session between UE and DN)*<br>*(Sources: 3GPP TS 38.300 [27], TS 23.501 [58])* |
| **N4** *(CP + UP)* | **SMF** ↔ **UPF** | • CP and UP data on N4 shall be integrity, confidentiality and replay protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to support, shall be used unless security is provided by other means, e.g. with physical security)*<br>• *A SEG may be used to terminate the IPsec tunnels*<br>• *Using cryptographic solutions to protect N4 interface is an operator's decision* | • **PDU and N4 session management** *(setting up an N4 SMF-UPF association for handling N4 sessions; creating, updating, and releasing N4 session context for a PDU session in UPF via Session ID (SEID))*<br>• **Controlling UPF functionality** *(via Packet Detection Rules (PDR), Forwarding Action Rules (FAR), Buffering Action Rules (BAR), Usage Reporting Rules (URR), QoS Enforcement Rules (QER) etc.)*<br>• **Reporting events by UPF to SMF** *(events related to an N4 session for an individual PDU session, e.g. Usage Report, DL Data Report (initiating Network Triggered Service Request to a UE in idle state), Session Report, UP Inactivity Report; general events, e.g. UP path failure)*<br>• **Policy charging and control** *(e.g. QoS control, gating control, UP traffic usage monitoring and reporting control, traffic redirection, packet rate enforcement, reporting start/stop of a solicited application by SMF to PCF; SMF "Pause of Charging" for better actual DL traffic accuracy)*<br>• **UP data forwarding between SMF and UPF** *(e.g. packets between UE and SMF, between SMF and DN, packets to be buffered in SMF)*<br>• **Lawful interception** *(SMF reports intercept related information (e.g. PDU session creation, modification, release) and triggers UPF to enable interception of target UP packets; UPF duplicates and reports UP packets from PDU sessions based on interception rules from SMF)*<br>*(Sources: 3GPP TS 29.244 [14], TS 23.502 [32], TS 33.127 [15], TS 23.501 [58]; [225], [345])* |

*Continued on the next page*

**Table 5.1** *(continued from the previous page)*

| Int. | Endpoints | Security measures (3GPP) | Protected functions (attack vectors) |
|---|---|---|---|
| **N6** *(UP)* | **UPF** ↔ **DN** | • Depends on the protocol used in the PDU session *(IP data, Ethernet data or unstructured data)* and network operator's decisions | • **Interworking between 5G PLMN and external DNs**, based on IP *(IPv4 and/or IPv6)*, but also Ethernet or unstructured PDU type data; a PDU is carried between the UE and the DN over the PDU session<br>*(Sources: 3GPP TS 29.561 [7], TS 23.501 [58])* |
| **N9** *(UP)* | **UPF** ↔ **UPF** | • UP data on N9 shall be integrity, confidentiality and replay protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to support, shall be used unless security is provided by other means, e.g. with physical security)*<br>• UPFs in the home routed scenario:<br>– **Inter-PLMN UP Security (IPUPS):** only forward GTP-U packets if they belong to an active PDU Session *(based on F-TEID)* and are not malformed *(optional to use)*<br>• *A SEG may be used to terminate the IPsec tunnels*<br>• *Using cryptographic solutions to protect N9 interface is an operator's decision* | • **(Non-guaranteed) delivery of UP PDUs**, i.e. user data, between different UPFs of the 5GC, based on GTP-U tunnelling *(in a PDU session between UE and DN)*<br>*(Sources: 3GPP TS 23.501 [58])* |
| **Xn** *(CP + UP)* | **gNB(-CU)** ↔ **gNB(-CU)** | • CP and UP data on Xn shall be integrity, confidentiality and replay-protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to implement)*<br>– **DTLS** *(over SCTP)* for CP on Xn-C *(mandatory to support)*<br>• Mutual authentication over Xn between gNBs:<br>– **DTLS** and/or **IKEv2** *(mandatory to support)*<br>– The identities specified in the end entity certificates shall be used for authentication and policy checks<br>• *Using transport layer security (DTLS), does not rule out the use of network layer protection (IPsec). IPsec also hides the network topology*<br>• *Using cryptographic solutions to protect Xn interface is an operator's decision* | CP (Xn-C interface):<br>• **Xn interface management** *(managing signalling associations between gNBs, surveying the Xn interface, recovering from errors)*<br>• **UE mobility management** *(handover via Xn, UE context transfer, data forwarding control; RAN paging with I-RNTI and change of RAN-based Notification Area (RNA) for UE in RRC_INACTIVE state)*<br>• **Dual connectivity** *(using additional resources in a secondary NG-RAN node)*<br>• **Energy saving** *(cell activation/deactivation)*<br>• **Load management** *(exchanging resource status and traffic load information between gNBs)*<br>UP (Xn-U interface):<br>• **Data transfer/forwarding between NG-RAN nodes** *(dual connectivity; mobility operation, during handover)*<br>• **Flow control** *(gNB receiving UP data can provide feedback about the data flow to the other gNB)*<br>• **Assistance information** *(gNB receiving UP data can provide assistance information, e.g. related to radio conditions, to the other gNB)*<br>*(Sources: 3GPP TS 38.300 [27], TS 38.420 [24]; [225])* |

*Continued on the next page*

**Table 5.1** *(continued from the previous page)*

| Int. | Endpoints | Security measures (3GPP) | Protected functions (attack vectors) |
|---|---|---|---|
| **F1** *(CP + UP)* | **gNB-DU** ↔ **gNB-CU** | • F1-C and F1-U shall support integrity, confidentiality and replay-protection:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to support)*<br>– **IPsec** *(mandatory to implement on the gNB-DU and on the gNB-CU)*<br>– **DTLS** *(over SCTP)* for CP on F1-C *(mandatory to support)*<br>• Mutual authentication over F1-C between gNB-CU and gNB-DU:<br>– **DTLS** and/or **IKEv2** *(mandatory to support)*<br>– The identities specified in the end entity certificates shall be used for authentication and policy checks<br>• *On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel*<br>• *All management traffic sent over F1 shall be integrity, confidentiality and replay protected*<br>• *F1-C and management traffic shall be protected independently of F1-U traffic (this allows F1-U to be protected differently from the F1-C in terms of using encryption and integrity protection)*<br>• *Using transport layer security (DTLS), does not rule out the use of network layer protection (IPsec). IPsec also hides the network topology*<br>• *Using cryptographic solutions to protect F1 interface is an operator's decision* | CP (F1-C interface):<br>• **F1 interface management** *(setup and removal, configuration update (may (de)-activate cells), resource coordination between DU and CU, network access rate reduction, TA information transfer between DU and CU)*<br>• **System information management** *(broadcast of System Information Blocks (SIBs))*<br>• **F1 UE context management** *(creation and modification of the necessary overall UE context, context release when UE enters RRC_IDLE or RRC_INACTIVE states; management of DRBs, SRBs and Sidelink (SL) DRBs)*<br>• **RRC message transfer between DU and CU** *(e.g. DU can report to CU if the downlink RRC message has been successfully delivered to UE; DU can duplicate downlink RRC message depending on the duplication configuration)*<br>• **Paging** *(paging procedure, Quality of Experience (QoE) information transfer control)*<br>• **Load management** *(reporting the load measurement results by the DU when requested by the CU)*<br>• **Positioning** *(transfer of location management messages, e.g. reporting Transmit/Receive Point information or positioning measurements when requested from the DU by the CU)*<br>UP (F1-U interface):<br>• **Transfer of user data between CU and DU** *(also PDU Set Information of a QoS flow, indication of End of Data Burst to the DU)*<br>• **Flow control** *(controlling the downlink user data flow to the DU)*<br>*(Sources: 3GPP TS 38.470 [21], TS 38.473 [20])* |
| **E1** *(CP)* | **gNB-CU-CP** ↔ **gNB-CU-UP** | • CP data on E1 shall be integrity, confidentiality and replay-protected:<br>– **IPsec ESP** and **IKEv2 certificates-based authentication** *(mandatory to support)*<br>– **DTLS** over SCTP *(mandatory to support)*<br>• Mutual authentication over E1 between gNB-CU-CP and gNB-CU-UP:<br>– **DTLS** and/or **IKEv2** *(mandatory to support)*<br>– The identities specified in the end entity certificates shall be used for authentication and policy checks<br>• *On both sides, a SEG may be used to terminate the IPsec tunnel*<br>• *Using transport layer security (DTLS), does not rule out the use of network layer protection (IPsec). IPsec also hides the network topology*<br>• *Using cryptographic solutions to protect E1 interface is an operator's decision* | • **E1 interface management** *(setup, removal, maintenance, configuration update, informing NR Cell Global Identifiers (CGI), Network-IDs (NID), S-NSSAI(s), PLMN-ID(s), QoS information supported by the CU-UP; sending capacity information and (non-)overloaded status by the CU-UP to the CU-CP)*<br>• **E1 bearer context management** *(setup, modification, and release; setup and update of QoS-flow to DRB mapping configuration; sending the alternative QoS Parameters Sets to the CU-UP when available for a QoS flow; sending security information to the CU-UP; sending transport layer information to the CU-UP to be used for data forwarding (e.g. during handovers); sending the parameters for header or uplink data compression to the CU-UP; notifying the CU-CP about DL data arrival to trigger paging procedure over F1 or Xn (for UE in RRC Inactive state); notifying the CU-CP about user inactivity (timer expiration) or user data reception for the expired timer, reporting data volume to the CU-CP)*<br>• **Load management** *(reporting the load measurement results by the CU-UP when requested by the CU-CP)*<br>• **Measurement results transfer** *(transfer of the measurement results received from the UE to the CU-UP, initiated by the CU-CP)*<br>*(Sources: 3GPP TS 37.480 [11], TS 37.483 [10])* |

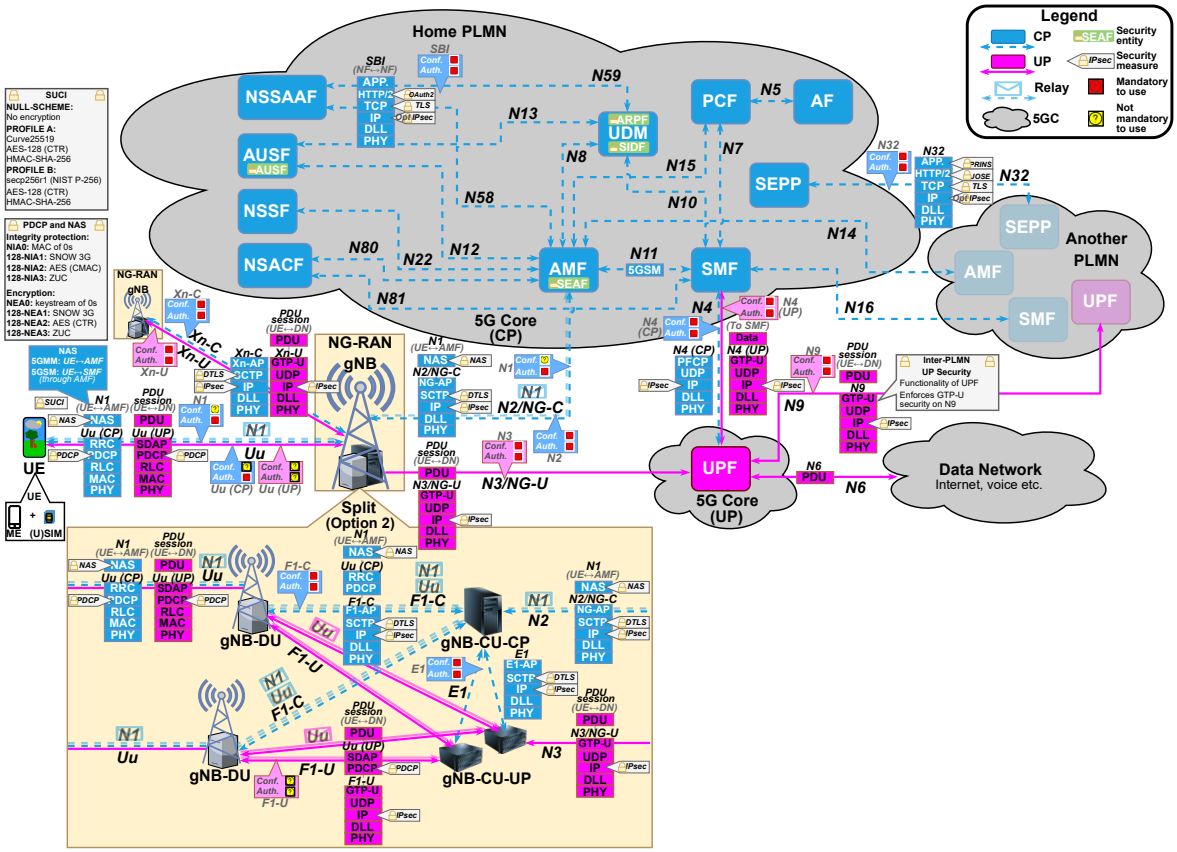



**Figure 5.1:** Security architecture of a 5G terrestrial network (based on [8, 9, 11, 14, 18, 21, 27, 28, 33, 58, 187, 246, 363]).

From Table 5.1 we can see that the AS and NAS interfaces (i.e. Uu and N1, respectively) are protected using ciphering and integrity protection algorithms (NEA and NIA). Integrity (and replay) protection is mandatory to use for the CP and optional for the UP, and confidentiality protection for both the CP and UP is optional to use but recommended whenever regulations allow. When it comes to the interfaces in the NDS/IP networks controlled by the network operator, then the CP interfaces (i.e. N2, N4, Xn-C, F1-C, and E1) are confidentiality, integrity, and replay protected using IPsec ESP, with IKEv2 for key exchange and certificates-based authentication. These interfaces (except for N4) are also required to support DTLS for mutual authentication, and integrity, replay, and confidentiality protection, as well as DTLS and/or IKEv2 for mutual authentication between the endpoints. On the other hand, the UP interfaces except N6 (i.e. N3, N9, Xn-U, and F1-U) are protected using only IPsec ESP (for confidentiality, integrity, and replay protection) and IKEv2 certificates-based authentication. Security of N6 depends on the type of data carried in the UP PDU (IP, Ethernet, or unstructured) and is not fully under the control of the operator (e.g. if the network is connected to the Internet). For all these NDS/IP interfaces, the use of cryptographic solutions to protect them is left to the operator to decide.

Table 5.2 summarizes the main security measures for each of the studied interfaces together with their security categories. In the following sections, we will consider each of these security categories and review the listed protection mechanisms in terms of the cryptographic profiles proposed by 3GPP.

Finally, in Figure 5.1, we extend the 5G TN architecture presented in chapter 2 (see Figure 2.2) with the 3GPP security measures that we have identified. This visual overview helps better understand which protocols and security mechanisms are used on which interfaces and can serve as a reference diagram for new researchers entering the field of 5G (security), as well as for more experienced researchers who want to recall the specifics of the 5G security architecture.

**Table 5.2:** Summary of the main security protections for the studied non-SBI interfaces.

| Interface | Security category | Main security protections |
|---|---|---|
| **Uu (AS)** | AS/NAS security | • RRC/UP ciphering algorithms<br>• RRC/UP integrity protection algorithms |
| **N1 (NAS)** | AS/NAS security<br>ECIES | • NAS ciphering algorithms<br>• NAS integrity protection algorithms<br>• SUCI |
| **N2 (NG-C)** | NDS/IP security | • IPsec + IKEv2<br>• DTLS |
| **N3 (NG-U)** | NDS/IP security | • IPsec + IKEv2 |
| **N4** | NDS/IP security | • IPsec + IKEv2 |
| **N6** | NDS/IP security | N/A |
| **N9** | NDS/IP security | • IPsec + IKEv2 |
| **Xn** | NDS/IP security | • IPsec + IKEv2<br>• DTLS *(for Xn-C)* |
| **F1** | NDS/IP security | • IPsec + IKEv2<br>• DTLS *(for F1-C)* |
| **E1** | NDS/IP security | • IPsec + IKEv2<br>• DTLS |

## 5.2. Cryptographic profiles for NDS/IP networks

Now that we have discussed the security protection measures for the non-SBI interfaces, we proceed with the investigation of their cryptographic profiles. While having a cryptographic solution in place is a good step towards security of the system, it is also important to implement this mechanism correctly, as otherwise it will not provide any meaningful extra security compared to not having it in the first place. For instance, the implementation of a security mechanism might have a bug which undermines the security it offers, or a vulnerable version might be supported or used, allowing an attacker to break or bypass the protection. Of course, assessing the security implementation of real 5G networks is not feasible without access to an actual 5G network. However, we could instead analyse what the 5G standards say about the cryptographic solutions for the studied non-SBI interfaces. If the standards are not periodically updated, or leave space for vulnerable versions, then 5G implementations will also be affected. This motivates the need to review the corresponding 3GPP specifications to see which cryptographic algorithms are mandated, recommended, allowed, and prohibited.

In this section, we investigate the cryptographic profiles for the NDS/IP networks, applicable for N2, N3, N4, N6, N9, Xn, F1, and E1 interfaces. We have seen that security of these interfaces primarily relies on IPsec, IKEv2, and DTLS. 3GPP TS 33.501 [33] section 9 states that *"The protection of IP based interfaces for 5GC and 5G-AN according to NDS/IP is specified in TS 33.210"* and that *"Traffic on interfaces carrying control plane signalling can be both integrity and confidentiality protected according to NDS/IP"*. Furthermore, the document says that IPsec profiling shall follow TS 33.210 [17], IKEv2 certificates-based authentication shall be implemented according to TS 33.310 [16], and IKEv2 profiling shall also conform to TS 33.310. Finally, DLTS security profiles shall follow the TLS profile in TS 33.210 (clause 6.2) and the certificate profile in TS 33.310 (clause 6.1.3a). In the following subsections, we review these two specifications.

### 5.2.1. IPsec

Internet Protocol Security (IPsec) is a security control at the network (IP) layer which is used to protect data exchange over public networks, encrypt IP traffic between communicating hosts, and set up virtual private networks (VPNs) [298]. It is a framework of open standards to provide private communications over IP networks [78]. The IPsec series of protocols relies on cryptographic algorithms to provide security services [319], which include access control, connectionless integrity, data origin authentication, replay detection and rejection (a form of partial sequence integrity), confidentiality, and limited traffic flow confidentiality (when encryption is used) [355]. It is designed to offer interoperable, cryptography-based security for IPv4 and IPv6, for all protocols carried over IP (including IP itself).

IPsec has two main components: 1) Encapsulating Security Payload (ESP) protocol [211], carrying the encrypted and authenticated traffic over the network; and 2) Internet Key Exchange (IKE) protocol [209] (see subsection 5.2.2) negotiating IPsec connection settings, security parameters and session keys; authenticating the IPsec peers to each other, and managing IPsec-protected communication channels [78]. Authentication Header (AH) [210], an older IPsec protocol for non-encrypted data, is no longer recommended for use, since ESP with NULL encryption can be used instead. Security Policy Database (SPD) specifies the policies determining disposition of all inbound and outbound IP traffic, what services are to be offered to IP packets and in what fashion (i.e. discard, bypass, protect) [355].

Table 5.3 summarizes the cryptographic profiling and usage requirements for IPsec, as standardized by 3GPP. IPsec support is based on RFC 4301 [355], and the ESP protocol shall be used as per RFC 4303 [211]. The tunnel mode, protecting the whole IP packet, is mandatory to support and shall be used between security gateways (SEGs, entities on the borders of the IP security domains). In contrast, the transport mode, protecting primarily the payload of the IP packet, i.e. the higher level protocols, is optional to support and is allowed to be used within a security domain (SD, networks managed by a single administrative authority) [17, 33]. Ciphers for (authenticated) encryption and authentication are specified in RFC 8221 [405] and in TS 33.210 [17] for explicit 3GPP requirements.

In Table 5.3 we also show the requirements for the NSA's CNSA 1.0 [305] and CNSA 2.0 [311] Suite algorithms (see section 3.4), based on RFC 9206 [122] and the I-D [180]. For brevity, we omit the requirements specific to the use of post-quantum cryptography in the IPsec/IKEv2 [207, 383] (for more information, see the I-D [180]). As can be seen from Table 5.3, the CNSA (2.0)-allowed set of algorithms is much more restricted than that of 3GPP/IETF and contains the algorithm versions with enhanced security parameters. This is something where 3GPP could improve in future releases, for example, by only allowing the use of Authenticated Encryption with Associated Data (AEAD) ciphers.

At the time of writing, RFC 8221 [405], which 3GPP requires to follow for the implementation conformance requirements for ESP (authenticated) encryption transforms and ESP authentication transforms, is the latest version proposed by the IETF in October 2017. Cryptographic algorithms known to be vulnerable and providing no meaningful security, such as DES and MD5, as well as deprecated algorithms, such as BLOWFISH, are prohibited to support. Most of the allowed transforms (mandatory, recommended, or optional) have been approved by NIST, i.e. specified in a Federal Information Processing Standards (FIPS) or a NIST Recommendation [78, 132, 279, 75, 76, 289, 286, 280, 281]. Exceptions are ChaCha20-Poly1305, AES-XCBC, and Triple-DES (3DES). ESP implicit IV (IIV) algorithms from RFC 8750 [260] are mentioned by NIST under work in progress in NIST Special Publication (SP) 800-77 Rev. 1 [78].

**Table 5.3:** Cryptographic profiles for IPsec, based on 3GPP TS 33.210 [17], TS 33.501 [33], and RFC 8221 [405]. CNSA requirements, based on RFC 9206 [122] and the I-D [180], are common for CNSA 1.0 and 2.0, unless specified otherwise.

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **Security protocols** | ! Requirements on support:<br>• **IPsec ESP** (RFC 4303 [211]) shall be supported and used when NDS/IP is applied<br>! Requirements on cryptographic algorithm implementation and usage:<br>• For encryption and authentication algorithms for ESP: RFC 8221 [405]<br>• For implicit IVs (IIVs, optional support): RFC 8750 [260]<br>? Optional to support features:<br>• **Extended sequence number**<br>*Differences in 3GPP compared to IETF RFCs are marked with "(!)"* | ! Mandatory to support:<br>• **IPsec ESP** protocol (RFC 4303 [211])<br>⊘ Prohibited to support:<br>• **IPsec AH** protocol (RFC 4302 [210]) |
| **Usage modes** | ! Requirements on support:<br>• **Tunnel mode** (RFC 4301 [355]) is mandatory to support, **transport mode** is optional<br>! Requirements on usage:<br>• **Tunnel mode** for inter-SD traffic *(SEGs shall be used between SDs)*<br>• **Transport mode** is allowed within an SD | N/A |

*Continued on the next page*

**Table 5.3** *(continued from the previous page)*

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **(Authenticated) Encryption transforms** (RFC 8221 [405], RFC 8750 [260]) | ! Mandatory to support ciphers:<br>• **ENCR_NULL** (RFC 2410 [167]) *(for ESP with only authentication - preferred over AH)*<br>• **ENCR_AES_CBC** (RFC 3602 [156]) *(128-bit and 256-bit keys; 192-bit is optional; expected to be replaced by AEAD ciphers in the future)*<br>• **ENCR_AES_GCM_16** (RFC 4106 [394]) *(AEAD cipher) (128-bit and 256-bit keys; 192-bit is optional; increased performance and key longevity compared to CBC)*<br>👍 Recommended to support ciphers:<br>• **ENCR_CHACHA20_POLY1305** (RFC 7634 [315]) *(AEAD cipher) (expected to become mandatory in the future)*<br>• **ENCR_AES_CCM_8** (RFC 4309 [190]) *(AEAD cipher) (for interoperability with IoT; 128-bit keys are recommended, 192-bit and 256-bit are optional)*<br>? Optional to support ciphers:<br>• **ENCR_AES_CTR** (RFC 3686 [191]) *(RFC 8221 mentions it at the MAY level)*<br>• **ENCR_AES_CCM_8_IIV**, **ENCR_AES_GCM_16_IIV**, **ENCR_CHACHA20_POLY1305_IIV** (RFC 8750 [260]) *(initiators may propose these implicit IV variant of algorithms, which saves 8 bytes per ESP packet)*<br>⚠ Not recommended to support:<br>• **ENCR_3DES** (RFC 2451 [328]) *(ENCR_CHACHA20_POLY1305 is a favourable alternative for ENCR_3DES, and is expected to replace it)*<br>🚫 Prohibited to support ciphers:<br>• **ENCR_DES** (RFC 2405 [131]) *(DES is vulnerable)*<br>• **ENCR_BLOWFISH** (RFC 2451 [328]) *(BLOWFISH is deprecated)*<br>• **ENCR_DES_IV32**, **ENCR_DES_IV64**, and **ENCR_3IDEA** *(unspecified by IETF)* | ! CNSA (2.0) requirements:<br>• **ENCR_AES_GCM_16** (FIPS 197 [277]) *(with key size 256 bits)*<br>? Optional to use features:<br>• **AES-GCM-SIV** (RFC 8452 [175]) (if a FIPS validated implementation is available) *(nonce construction using a misuse-resistant technique)* |
| **Authentication transforms** (RFC 8221 [405]) | ! Mandatory to support ciphers:<br>• **AUTH_HMAC_SHA1_96** (RFC 2404 [169], RFC 7296 [209]) *(trend to deprecate its usage)*<br>• **AUTH_AES_128_GMAC** (RFC 4543 [393]) **(!)** *(mandated by 3GPP, while IETF recommends using it only for AH, and not for ESP*)*<br>• **AUTH_HMAC_SHA2_256_128** (RFC 4868 [158]) *(to replace the SHA1_96 version)*<br>• **AUTH_NONE** (RFC 7296 [209], RFC 5282 [93]) *(NB! Only allowed with AEAD ciphers)*<br>👍 Recommended to support ciphers:<br>• **AUTH_HMAC_SHA2_512_256** (RFC 4868 [158]) *(a future replacement of the SHA2_256_128 version; preferred over the latter if implemented)*<br>• **AUTH_AES_XCBC_96** (RFC 3566 [157], RFC 7296 [209]) *(recommended only with IoT)*<br>? Optional to support ciphers:<br>• **AUTH_AES_192_GMAC** (RFC 4543 [393]) *(recommended only for AH, not for ESP*)*<br>• **AUTH_AES_256_GMAC** (RFC 4543 [393]) *(recommended only for AH, not for ESP*)*<br>• **AUTH_HMAC_SHA2_384_192** (RFC 4868 [158]) *(SHA2_512_256 is preferred)*<br>🚫 Prohibited to support ciphers:<br>• **AUTH_NONE** (RFC 7296 [209], RFC 5282 [93]) *( if not used with authenticated encryption algorithms)*<br>• **AUTH_HMAC_MD5_96** (RFC 2403 [168], RFC 7296 [209]) *(MD5 is vulnerable to collisions)*<br>• **AUTH_KPDK_MD5** *(MD5 is vulnerable to collisions)*<br>• **AUTH_DES_MAC** *(DES is vulnerable)*<br>** IETF recommends AUTH_HMAC_SHA2_256_128 for integrity when using ENCR_NULL, and ENCR_NULL_AUTH_AES_GMAC when using AES-GMAC in ESP without authentication* | ! CNSA (2.0) requirements:<br>• **AUTH_NONE** *(since AES-GCM is an AEAD cipher, either no integrity algorithm must be offered or the single integrity algorithm NONE is offered)* |

*Continued on the next page*

**Table 5.3** *(continued from the previous page)*

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **IV construction** | ! Requirements for CBC mode: [a]<br>• The IV (same size as the block size of the used cipher algorithm) shall be random and unpredictable to anyone other than the originator<br>• RFC 4086 [2] has guidelines for pseudorandom number generators<br>! Requirements for CTR, GCM, CCM, ChaCha20-Poly1305, GMAC modes:<br>• The IV (8 bytes) shall be constructed in a way that ensures uniqueness. The same IV and key pair shall not be used more than once<br>• Constructing an IV from the encrypted data of the preceding encryption process is *explicitly forbidden*<br>• Using a random IV is *explicitly forbidden*<br>[a] *These strengthening requirements take precedence over the description in RFC 2451 [328] and other descriptions allowing predictable IVs* | N/A |
| **Compression algorithms** (RFC 8221 [405]) | *Not mentioned in TS 33.210 [17], however IETF RFC 8221 mentions optional support for* ***IPCOMP_DEFLATE*** *(RFC 3173 [265]),* ***IPCOMP_LZS*** *(RFC 2395 [160]), and* ***IPCOMP_LZJH*** *(RFC 3051 [96]), and prohibits support for* ***IPCOMP_OUI*** | N/A |

ChaCha20-Poly1305 is an AEAD construction from a fast and secure stream cipher ChaCha20 (designed to provide 256-bit security) and the Poly1305 authenticator [315]. AEAD ciphers handle encryption/decryption and authentication in a single step and are the fastest and the most modern method to provide authenticated encryption, as opposed to combining a non-AEAD cipher with an authentication algorithm [405]. ChaCha20 is being increasingly adopted in the industry and has been recommended, among others, by the Crypto Forum Research Group (CFRG) as an alternative to AES-CBC and AES-GCM [405, 129]. Like other stream ciphers, it has not been approved by NIST. AES-XCBC is an AES CBC mode algorithm with a set of extensions to overcome the limitations of the classic CBC-MAC algorithm for messages of varying length [157]. It is recommended only in the context of IoT (which is not a general use case for VPNs), as they have a tendency to prefer AES-based HMAC functions to avoid implementing SHA2 algorithms [405]. Triple-DES is disallowed for encryption since January 1, 2024 and is allowed only for legacy decryption, key unwrapping, and Message Authentication Code (MAC) verification for data that is already protected [299, 74, 75]. RFC 8221 does not recommend supporting Triple-DES and expects to remove it [405].

AUTH_HMAC_SHA1_96, based on SHA-1, is still mandatory to support (at the “MUST-” level in RFC 8221) but is becoming deprecated in the industry [405]. In 2011, NIST deprecated the use of SHA-1 for generating digital signatures and time stamps, and other applications requiring collision resistance, disallowing the usage at the end of 2013 [286]. The algorithm was only allowed for keyed-hash MACs (HMACs), key derivation functions (KDFs), random number generators (RNGs), and for verifying old digital signatures and time stamps [294, 108]. By now, collision attacks against SHA-1 have become increasingly severe, significantly less complex, and affordable to academic researchers, resulting in SHA-1 becoming vulnerable to impersonation attacks and offering almost no security in practice [235, 234]. In December 2022, NIST has announced its plan to transition away from the limited usage of SHA-1 by December 31, 2030, in favour of the more secure SHA-2 and SHA-3 hash function groups [296, 297, 286]. Furthermore, hash functions with the output length of 224 bits are deprecated through December 31, 2030, and are expected to be disallowed after that time [385].

Next to having a good IPsec cryptographic profiling, it is also important to follow the recommendations and best practices for secure deployment of IPsec networks. Nation State Advanced Persistent Threat (APT) actors were previously found to have gained access to vulnerable VPN devices, allowing them to use remote code execution, intercept or hijack encrypted traffic sessions, and perform other unintended activities [309]. In order to secure VPNs and ensure protection of their confidentiality and integrity, US National Security Agency (NSA) recommends always using CNSSP 15-compliant and FIPS validated cryptography suites [117], removing unused or non-compliant cryptography algorithms (to mitigate downgrade attacks), not using the default vendor configurations (as they might allow for more cryptography suites than desired), implementing strict traffic filtering rules (to mitigate exposure

to network scanning and brute force attacks), and applying vendor-provided patches and updates [307]. Finally, NIST provides a practical guidance for implementing security services based on IPsec to reduce the risks related to sending sensitive data across networks [78].

### 5.2.2. IKEv2

Configuration of IPsec is generally performed using the Internet Key Exchange (IKE) protocol [78]. In essence, IKE is the command channel, while IPsec is the data channel. IKEv2, the current IKE version (with IKEv1 deprecated [404]), performs mutual authentication between two parties that want to set up secure IPsec connections (e.g. SEGs in NDS/IP networks), handles the key management and distribution between them, and negotiates, establishes, and maintains Security Associations (SA) between these peers [17, 209, 355]. All traffic of a SA is offered the same security processing. An IPsec SA is uniquely defined by the Security Parameters Index (SPI), destination IP address (i.e. the ESP SA endpoint), and a security protocol identifier (always ESP in NDS/IP networks). The state data and parameters for each active (keyed) IPsec SA are stored in the Security Association Database (SAD).

Initial IKE exchanges, i.e. IKE_SA_INIT and IKE_AUTH, are used to set up an IKE SA (Parent SA) and an associated IPsec SA (Child SA, or the created IPsec connection), both identified by the SPI [78]. Upon successful completion of these IKE exchanges, both entities have the IKE SA and one IPsec SA. The created IKE SA is then used to send and receive encrypted and authenticated management and configuration commands. For this purpose, other exchange types are used, e.g. CREATE_CHILD_SA is used to create additional IPsec SAs and rekey the existing IKE or IPsec SAs, and INFORMATIONAL allows to send notification messages (e.g. IPsec SA or IKE SA deletion, rekeying, dead peer detection, mobility update). Notify payloads can send extra information about supported algorithms and features.

A summary of the cryptographic profiles and usage requirements for IKEv2 is shown in Table 5.4, based on 3GPP TS 33.210 [17]. The IKEv2 implementation is based on RFC 7296 [209], with the update in RFC 8247 [319] for cryptographic algorithms and authentication methods (all parameters are listed in IANA IKEv2 registry [198]). IKEv2 certificates-based authentication is specified in TS 33.310 [16]. This specification also describes the certificate enrolment mechanism for base stations, which is recommended to be supported by gNBs, although its usage is left to the operator to decide [33].

**Table 5.4:** Cryptographic profiles for IKEv2, based on 3GPP TS 33.210 [17], TS 33.310 [16] and RFC 8247 [319]. CNSA requirements, based on RFC 9206 [122] and the I-D [180], are common for CNSA 1.0 and 2.0, unless specified otherwise.

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **General** | ! Requirements on support:<br>• **IKEv2** for negotiation of IPsec SAs (RFC 7296 [209] and the update in RFC 8247 [319])<br>! Requirements on usage:<br>• An ephemeral private key shall be used in precisely one key establishment transaction and then immediately destroyed (zeroed)<br>👍Recommended to support features:<br>• **IKEv2 Configuration Payload** (RFC 7296 [209])<br>• **Protocol support for High Availability** (RFC 6311 [202])<br>*Differences in 3GPP compared to IETF RFCs are marked with "(!)"* | ! Requirements on usage:<br>• **IKEv2** (RFC 7296 [209]) for IPsec implementations<br>• An ephemeral private key shall be used in precisely one key establishment transaction and then immediately destroyed (zeroed)<br>• After use, any derived shared secret shall be immediately destroyed (zeroed)<br>• For PSK: RFC 8784 [155] for CNSA 1.0; [366] for CNSA 2.0<br>👍CNSA recommendations on initiator proposal:<br>• **CNSA-GCM-256-ECDH-384**<br>• **CNSA-GCM-256-DH-3072**<br>• **CNSA-GCM-256-DH-4096**<br>• If no compliant proposal, the responder shall send NO_PROPOSAL_CHOSEN |

*Continued on the next page*

**Table 5.4** *(continued from the previous page)*

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **IKE_SA_INIT exchange: algorithm selection – transform type 1 (encryption algorithms)** (RFC 8247 [319]) | ! Mandatory to support ciphers:<br>• **ENCR_AES_CBC** (RFC 7296 [209]) *(128-bit and 256-bit keys; 192-bit is optional)*<br>• **ENCR_AES_GCM_16** (RFC 5282 [93]) *(AEAD cipher)* **(!)** *(IETF recommends this cipher with 128-bit and 256-bit keys, while 192-bit keys as well as 8- and 12-octet ICVs are optional; 3GPP mandates this cipher with 128-bit keys)*<br>👍 Recommended to support ciphers:<br>• **ENCR_CHACHA20_POLY1305** (RFC 7634 [315]) *(AEAD cipher)*<br>• **ENCR_AES_CCM_8** (RFC 5282 [93]) *(AEAD cipher) (for interoperability with IoT; 128-bit keys are recommended, 192-bit and 256-bit are optional)*<br>? Optional to support ciphers:<br>• **ENCR_AES_CTR** (RFC 5930 [274]) *(RFC 8247 mentions it at the MAY level)*<br>• **ENCR_3DES** (RFC 7296 [209]) *(much slower than ENCR_AES_CBC; furthermore, ENCR_CHACHA20_POLY1305 is a more modern alternative to AES(CBC))*<br>🚫 Prohibited to support ciphers:<br>• **ENCR_DES** (RFC 7296 [209]) *(provides no meaningful security)*<br>• **ENCR_NULL** *(provides no security)* | ! CNSA (2.0) requirements:<br>• **ENCR_AES_GCM_16** (FIPS 197 [277]) *(with key size 256 bits)*<br>? Optional to use features:<br>• **AES-GCM-SIV** (RFC 8452 [175]) (if a FIPS validated implementation is available) *(nonce construction using a misuse-resistant technique)* |
| **IKE_SA_INIT exchange: algorithm selection – transform type 2 (pseudorandom functions)** (RFC 8247 [319]) | ! Mandatory to support functions:<br>• **PRF_HMAC_SHA2_256** (RFC 4868 [158]) *(to replace PRF_HMAC_SHA1)*<br>• **PRF_HMAC_SHA1** (RFC 2104 [222]) *(trend to deprecate its usage)*<br>👍 Recommended to support functions:<br>• **PRF_HMAC_SHA2_384** (RFC 4868 [158]) **(!)** *(optional RFC 8247 [319], which prefers the SHA2_512 version over SHA2_384 due to negligible overhead)*<br>• **PRF_HMAC_SHA2_512** (RFC 4868 [158]) *(a future replacement for SHA2_256)*<br>• **PRF_AES128_XCBC** (RFC 4434 [186]) *(only with IoT, otherwise optional)*<br>🚫 Prohibited to support functions:<br>• **PRF_HMAC_MD5** (RFC 2104 [222]) *(industry-wide trend to remove MD5)* | ! CNSA (2.0) requirements:<br>• **PRF_HMAC_SHA2_512** (FIPS 180 [302])<br>• **PRF_HMAC_SHA2_384** (FIPS 180 [302]) (if available to both initiator and responder) |
| **IKE_SA_INIT exchange: algorithm selection – transform type 3 (integrity algorithms)** (RFC 8247 [319]) | ! Mandatory to support algorithms:<br>• **AUTH_HMAC_SHA1_96** (RFC 2404 [169], RFC 7296 [209]) *(trend to deprecate its usage)*<br>• **AUTH_HMAC_SHA2_256_128** (RFC 4868 [158]) *(to replace the SHA1_96 version)*<br>👍 Recommended to support functions:<br>• **AUTH_HMAC_SHA2_512_256** (RFC 4868 [158]) *(a future replacement for the SHA2_256_128 version; preferred over SHA2_384 due to negligible overhead)*<br>• **AUTH_AES_XCBC_96** (RFC 3566 [157], RFC 7296 [209]) *(only with IoT, otherwise optional)*<br>? Optional to support:<br>• **AUTH_HMAC_SHA2_384_192** (RFC 4868 [158]) *(SHA2_512_256 is preferred)*<br>🚫 Prohibited to support functions:<br>• **AUTH_HMAC_MD5_96** (RFC 2403 [168], RFC 7296 [209]) *(trend to remove MD5)*<br>• **AUTH_DES_MAC** *(an industry-wide trend to deprecate DES)*<br>• **AUTH_KPDK_MD5** *(an industry-wide trend to deprecate and remove MD5)* | ! CNSA (2.0) requirements:<br>• **AUTH_NONE** *(since AES-GCM is an AEAD cipher, either no integrity algorithm must be offered or the single integrity algorithm NONE is offered)* |

*Continued on the next page*

**Table 5.4** *(continued from the previous page)*

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **IKE_SA_INIT exchange: algorithm selection – transform type 4 (Diffie-Hellman groups)** (RFC 8247 [319]) | ! Mandatory to support groups:<br>• **14** (2048-bit MODP Group) (RFC 3526 [219]) *(to replace the 1024-bit MODP Group)*<br>• **19** (256-bit random ECP group) (RFC 5903 [370]) (!) *(IETF only recommends it)*<br>👍 Recommended to support groups:<br>• **20** (384-bit random ECP group) (RFC 5903 [370]) (!) *(not mentioned in RFC 8247 [319])*<br>• **31** (Curve25519) (RFC 8031 [316]) (!) *(not mentioned in RFC 8247 [319])*<br>⚠ Not recommended to support groups:<br>• **23** and **24** (2048-bit MODP groups with respectively 224-bit and 256-bit Prime Order Subgroups) (RFC 5114 [233]) *(not safe primes; small subgroups, so additional checks must be done (RFC 6989 [360] section 2.2); expected to become deprecated)*<br>🚫 Prohibited to support groups:<br>• Modular Exponential (MODP) groups less than 2048-bit (**1**, **2**, **5**, **22**) (!) *(explicit requirement by 3GPP)* | ! CNSA (2.0) requirements:<br>• **20** (384-bit random ECP group) (RFC 5903 [370])<br>• **15** (3072-bit MODP Group) (RFC 3526 [219])<br>• **16** (4096-bit MODP Group) (RFC 3526 [219])<br>! Additional CNSA 2.0 requirements:<br>• **ML-KEM-1024** (FIPS 203 [291]) *(may be proposed using a single Additional Key Exchange (Transform Type 6-12) in IKE_INTERMEDIATE; the Transform Type shall be ML-KEM-1024)* |
| **IKE_AUTH exchange: authentication methods** (RFC 8247 [319], TS 33.310 [16] clause 6.2) | ! Mandatory to support methods:<br>• **1** (RSA Digital Signature) (RFC 7296 [209]) *(widely deployed, kept for interoperability)* (!) *(3GPP recommends not using this method, as it uses PKCS#1v1.5 padding)*<br>– ! Mandatory to support key lengths: **2048**<br>– 👍 Recommended to support key lengths: **3072** and **4096**<br>– ? Optional to support key lengths: **between 2049 and 4095**<br>– ⚠ Not recommended to support key lengths: **smaller than 2048** *(the signatures only have value in real time and do not need future protection)*<br>• **2** (Shared Key Message Integrity Code) (RFC 7296 [209])<br>• **14** (Digital Signature) (RFC 7427 [217]) *(provides hash function, signature format, and algorithm agility; expected to replace RSA/ECDSA Digital Signature methods)* (!) *(IETF only recommends this method)*<br>– ! Mandatory to support: **ecdsa-with-sha256** (!) *(recommended by IETF)*<br>– 👍 Recommended to support: **ecdsa-with-sha384** (!) *(not mentioned in RFC 8247 [319])*, **RSASSA-PSS with SHA-256** (!) *(mandated by IETF)*<br>– ? Optional to support: **RSASSA-PKCS1-v1.5**<br>– 🚫 Prohibited to support: **sha1WithRSAEncryption**, **dsa-with-sha1**, **ecdsa-with-sha1**, **RSASSA-PSS with Empty/Default Parameters** *(SHA1)*<br>👍 Recommended to support methods:<br>• **ECDSA Digital Signature** [a] *(do not provide hash function agility, expected to be downgraded; ECDSA can be performed using generic Digital Signature method)*<br>– **9** (ECDSA-256 - ECDSA with SHA-256 on the P-256 curve) (RFC 4754 [161])<br>– **10** (ECDSA-384 - ECDSA with SHA-384 on the P-384 curve) (RFC 4754 [161])<br>– **11** (ECDSA-521 - ECDSA with SHA-512 on the P-521 curve) (RFC 4754 [161])<br>⚠ Not recommended to support methods:<br>• **3** (DSS Digital Signature) (RFC 7296 [209]) *(signatures are bound to SHA-1 and offer the same security level as 1024-bit RSA; support expected to be removed)* | ! CNSA 1.0 requirements on signature generation:<br>• **SHA-384** (RFC 8017 [267]) with **ECDSA-384** (RFC 4754 [161]) or **RSA** with ≥ **3072**-bit modulus<br>! CNSA 1.0 requirements on signature verification:<br>• **ECDSA-384** signatures<br>• **RSA** with **3072**-bit or **4096**-bit modulus and **SHA-384** signatures<br>• Any other authentication method shall not be accepted *(must return an AUTHENTICATION_FAILED Notify payload and stop message processing)*<br>! CNSA 2.0 requirements on digital signatures:<br>• **ML-DSA-87** (FIPS 204 [290]) *(non-deterministic signatures)*<br>• Any other authentication method shall not be accepted *(must return an AUTHENTICATION_FAILED Notify payload and stop message processing)* |

[a] *3GPP mandates support for methods 9, 10, and 11 (ECDSA Digital Signature), but the corresponding hash functions/curves are only recommended*

*Continued on the next page*

**Table 5.4** *(continued from the previous page)*

| | 3GPP/IETF | CNSA (2.0) |
|---|---|---|
| **IKE_AUTH exchange: other features** | ! Mandatory to support features:<br>• **IP addresses** and **Fully Qualified Domain Names** for identification<br>• **Rekeying of IPsec SAs and IKE SAs** (RFC 7296 [209]); shall not lead to a noticeable service degradation<br>• **Hash Algorithm Notification** (RFC 7427 [217]) *(for the Digital Signature algorithm method; indicated with a Notify payload sent inside the IKE_SA_INIT exchange)*<br>– ! Mandatory to support hash functions: **SHA2-256**<br>– 👍 Recommended to support hash functions: **SHA2-384 (!)** *(optional in RFC 8247 [319])*, **SHA2-512**<br>– 🚫 Prohibited to support hash functions: **SHA1**<br>– 👍 Recommended default hash function: **SHA-256 (!)** *(requirement by 3GPP)*<br>🚫 Prohibited to use features:<br>• **Identification Payloads (IDi, IDr)** *(but may be used for policy lookup)* | ! Requirements on peer authentication decisions:<br>• **Subject** or **Subject Alternative Name** from the certificate containing the key for validating the signature in the Authentication Payload *(for peer authentication decisions)*<br>🚫 Prohibited to use features:<br>• **Identification Payloads (IDi, IDr)** *(but may be used for policy lookup)* |
| **CREATE_CHILD_SA exchange** | 👍 Recommendations on usage:<br>• **A DH key exchange** *(giving Perfect Forward Secrecy)*<br>• **Frequent change of the session keys** | ! Mandatory to support:<br>• **Rekeying** of CREATE_CHILD_SA *(by both parties)*<br>? Optional to use:<br>• **A DH key exchange** *(the DH group (of KEi or a new DH key) shall be the same as used in IKE_INIT_SA)* |
| **Reauthentication** | ! Requirements on support:<br>• **Reauthentication of IKE SAs** (RFC 7296 [209] section 2.8.3)<br>! Requirements on usage:<br>• IKE SA reauthentication shall be proactively initiated by NE (with the creation of Child SAs); the new SAs shall be created before the old ones expire<br>• IKE SA with its Child SAs shall be destroyed once the IKE SA's authentication lifetime expires<br>• Reauthentication shall not lead to a noticeable service degradation | N/A |
| **Certificate based IKEv2 authentication (additional requirements)** (TS 33.310 [16] clause 6.2) | ! Requirements on usage:<br>• CERT payload identity (and end entity certificate) shall be used for policy checks<br>• Initiating end entities shall send certificate requests in the IKE_INIT_SA exchange, and responding end entities - in the IKE_AUTH exchange<br>• Peer end entity shall not send cross-certificates *(they are pre-configured in end entity)*<br>• Certificate payload certificates shall be encoded as type 4 *(i.e. "X.509 Certificate - Signature")*<br>• If any used end entity certificate expires, an end entity shall re-key the IKE SA<br>• If DNS is available, *subjectAltName* and IKEv2 policy should both contain FQDN (otherwise - IP address) | ! Requirements on public key certificates:<br>• X.509 certificates that comply with RFC 8603 [201] shall be used *(CNSA Suite certificate and CRL profile)*<br>• End-entity certificate of the authenticating party shall be used<br>! Additional CNSA 2.0 requirements:<br>• IKE_AUTH messages shall include CERT payloads complying with [200]<br>• CERT payloads shall be encoded as type 4 *(i.e. "X.509 Certificate - Signature")*<br>• CERT payloads may also use other Cert Encodings, s.a. CRL (7), as needed<br>• Other public key formats shall not be used<br>• CERTREQ payload is mandatory to use |

RFC 8247 [319], referenced by 3GPP for implementation requirements and usage guidance for IKEv2, is currently the latest version, published in September 2017. From the four transform types, listed in cryptographic proposals sent by the IKE_SA_INIT exchange to establish the encrypted IKE SA [78], encryption and integrity transforms have the same allowed algorithms as the IPsec transforms (as discussed in subsection 5.2.1). A small difference is that AUTH_AES_128_GMAC (and the 192- and 256-bit versions) is not explicitly mentioned in RFC 8247; ENCR_3DES is still at the "MAY" level, and ENCR_NULL is prohibited (while ESP can be used with only authentication, which is preferred over AH due to NAT traversal [405]). The negotiated pseudorandom function (PRF) transform is used to derive all encryption and authentication keys from the secret value (SKEYSEED), generated upon successful completion of the IKE_SA_INIT when both entities have performed the (Elliptic Curve, EC) Diffie-Hellman (DH) key exchange [78]. Generally, the negotiated integrity algorithm and the PRF are the same cryptographic algorithm, although when an AEAD cipher is used without a separate integrity algorithm (omitted or NONE), then the PRF is a different algorithm (typically, SHA-2 family hash function). The allowed algorithms for PRF transforms are the same as the ones for integrity transforms and are approved by NIST, except for AES-XCBC [109, 75, 78].

When it comes to the (EC)DH transforms, used for the key exchange during IKE_SA_INIT, then the 3GPP-allowed groups are all NIST-approved, namely groups with the security strength of at least 112 bits, i.e. at least 2048-bit DH groups and at least 224-bit ECDH groups [75]. Note that the key-agreement transactions using MODP-2048 safe-prime group [219] and ffdhe2048 safe-prime group [166] (not mentioned in RFC 8247), providing 112 bits of security strength [79], will be deprecated after December 31, 2030, in favour of MODP [219] and ffdhe [166] safe-prime groups with 3072, 4096, 6144, or 8192 bits, offering at least 128 bits of security [76]. Key-agreement transactions using elliptic curves P-256, P-384, and P-521 (256-Bit, 384-Bit, and 521-Bit Random ECP Groups, respectively [370]), providing at least 128-bit security strength [284, 110], are acceptable for use (with no indication of future deprecation at the time of writing). Curve25519, with 128-bit security strength, is also approved by NIST [110]. Finally, MODP groups less than 2048 bits are prohibited by 3GPP, similar to NIST [75], and 2048-bit MODP groups from RFC 5114 [233] (23 and 24) are expected to be removed.

From the authentication methods, used during IKE_AUTH exchange by the peers to verify each other's identities and authenticate the previous IKE_SA_INIT exchange [78], 3GPP and RFC 8247 allow RSA Digital Signature, Shared Key Message with Integrity Code, Digital Signature and ECDSA Digital Signature [319, 17, 16]. NIST approves three techniques to generate and verify digital signatures: RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), and Edwards Curve DSA (EdDSA), with DSA (method 3) only allowed to verify existing signatures [284, 285]. For RSA signatures (PKCS #1 v1.5 and PSS), NIST requires the modulus length to be at least 2048 bits [75, 284], similar to 3GPP. Note that RSA signature generation using moduli larger than 2048 but smaller than 3072 bits (i.e. with the security strength of at least 112 bits but less than 128 bits) is intended to be deprecated after December 31, 2030, in favour of key lengths at least 3072 bits, providing at least 128-bit security [76]. NIST-approved ECDSA curves for digital signature generation must be at least 224 bits to satisfy the minimum security-strength requirement of 112 bits, and after December 31, 2030, $<$ 256-bit curves will be deprecated in favour of $\geq$ 256-bit curves to meet the minimum security requirement of 128 bits [75, 76]. This is the case for the ECDSA curves in Table 5.4. Allowed hash functions are also approved by NIST [286, 76].

Digital Signature, not mentioned by NIST, is a new IKEv2 authentication method, designed to support digital signature methods in a more general way [217]. This replaces the cumbersome design of handling current signature-based IKEv2 authentication methods per algorithm (one for RSA, one for DSS (using SHA-1), and three for different ECDSA curves, each tied to exactly one hash function). The new method is designed to be flexible enough to include all currently supported signature methods (e.g. RSA, ECDSA, RSASSA-PSS) and introduce new methods in the future (e.g. ECGDSA, ElGamal).

Finally, Shared Key Message Integrity Code is widely deployed and is mandatory to implement per RFC 8247 and TS 33.210 [319, 17]. With this method, the hosts authenticate one another by each signing (or computing a MAC using padded shared secret as the key) a block of data [209]. The integrity code is computed using the negotiated PRF and the shared key associated with the identity in the ID payload. NIST requires that pre-shared keys (PSK) are highly random (with at least 112-bit security) and are not based on simple words or phrases (to resist against dictionary attacks) [78]. Using group PSKs is strongly discouraged, as all parties knowing the PSK may impersonate other hosts in the group.

Since IKEv2 is used together with IPsec in VPNs or, in the context of 3GPP, in NDS/IP-networks, suggestions listed in the previous subsection for IPsec networks (see subsection 5.2.1) are also applicable to IKEv2. In particular, network operators should follow recommendations and best practices for secure deployment of IPsec networks and secure configuration and usage of IKE [307]. Furthermore, the "Guide to IPsec VPNs" by NIST [78] can assist the operators in enhancing the security of their networks. As was also the case for IPsec (see subsection 5.2.1), the CNSA (2.0) Suite is much more restricted than the 3GPP/IETF IKEv2 profile (see Table 5.4), which could be addressed in future 3GPP releases.

### 5.2.3. (D)TLS

Transport Layer Security (TLS) is a protocol that establishes a protected channel for data exchange between two applications (a server and a client) [253, 339]. It is based on its predecessor protocol Secure Sockets Layer (SSL) 3.0 [159], being an improvement over the latter. The protocol provides data confidentiality, data integrity and replay protection, and authentication between the two entities and protects against eavesdropping, message tampering, and message forgery. TLS is application protocol independent and can be used in many environments to secure traffic between various applications communicating over a network using an application protocol, such as Hypertext Transfer Protocol (HTTP). Being a layered protocol, TLS runs on top of a reliable in-order data stream transport protocol, which is usually the Transmission Control Protocol (TCP).

TLS consists of two main components: TLS handshake protocol and TLS record protocol [337, 339]. The handshake protocol authenticates communicating peers, securely negotiates cryptographic parameters and modes, and creates the material for the shared keying before the application layer protocol sends or receives any data. The identity of the peer is authenticated using asymmetric (public key) cryptography (such as RSA or ECDSA [284]), or a symmetric pre-shared key (PSK). The authentication is generally required for the server side, while for the client side it can be made optional. The record protocol relies on the parameters established by the handshake to protect data exchange using symmetric encryption (such as AES [277]). For each connection, unique symmetric keys are generated, based on the negotiated secret. Furthermore, messages include a keyed MAC for integrity check.

TLS assumptions about reliable transport make it unusable as is for datagram protocols like User Datagram Protocol (UDP), where packets can be lost or reordered [341, 342]. Such unreliability breaks TLS implementations in datagram environments, since the protocol does not have internal mechanisms to deal with unreliable transport. Simply using IPsec instead is not suitable for some applications [85], and developing a custom security protocol for the application layer requires a lot of time and efforts. To fix this problem while making minimal changes to TLS, a Datagram TLS (DTLS) has been created based on TLS to provide communication privacy for datagram protocols. It intentionally designed to be as similar to TLS as possible to minimize new security invention and maximise code and infrastructure reuse. The resulting protocol is mostly identical to TLS and provides equivalent security guarantees.

Table 5.5 presents version requirements for (D)TLS, additional requirements, and TLS certificate profile; TLS profiles also apply for DTLS [17]. For N2, Xn-C, F1-C, and E1, DTLS over SCTP [387] shall be supported for mutual authentication, and confidentiality, integrity, and replay protection [33]. As expected, the 3GPP certificate profile is less strict than a CNSA (2.0)-compliant profile.

**Table 5.5:** Cryptographic profiles for (D)TLS, based on 3GPP TS 33.210 [17] and TS 33.310 [16]. CNSA (2.0) requirements, based on RFC 8603 [201] and the I-D [200], are common for CNSA 1.0 and 2.0, unless specified otherwise.

| | 3GPP | CNSA (2.0) |
|---|---|---|
| **Prohibited versions** | **SSL 1.0**, **SSL 2.0**, **SSL 3.0**,**TLS 1.0**, **TLS 1.1** and **DTLS 1.0**. | CNSA 1.0: **prior to (D)TLS 1.2**.<br>CNSA 2.0: **prior to (D)TLS 1.3**. |
| **Mandatory versions** | **TLS 1.2** (RFC 5246 [339]), **TLS 1.3** (RFC 8446 [337]); if DTLS is supported, then **DTLS 1.2** (RFC 6347 [341]) is mandatory to support and **DTLS 1.3** (RFC 9147 [342]) is recommended to support. | CNSA 1.0: **(D)TLS 1.2** (RFC 5246 [339], RFC 6347 [341]) or **(D)TLS 1.3** (RFC 8446 [337], RFC 9147 [342]).<br>CNSA 2.0: **(D)TLS 1.3** (per [84]). |
| **Secure use of (D)TLS** | Recommendations are given in RFC 9325 [361], RFC 9113 [380]. | N/A |
| **HTTP/2 over TLS** | Additional requirements are given in RFC 9113 [380]. | N/A |

*Continued on the next page*

**Table 5.5** *(continued from the previous page)*

| | 3GPP | CNSA (2.0) |
|---|---|---|
| **HTTP over TLS** (as in RFC 9110 [153]) | The client shall not set up a connection *"upgraded to TLS Within HTTP/1.1"* (RFC 9110 [153], RFC 9112 [154]), but shall only create the tunnel over a raw TCP connection. | N/A |
| **Common rules to all certificates (including TLS)** (TS 33.310 [16] clause 6.1.1) | Requirements on certificates:<br>• **X.509 version 3 certificate** according to RFC 5280 [95]<br>• TLS entities *(also Network Entities (NEs) and Security Gateways (SEGs))* shall verify the certificate compliance with the NDS/AF profiles (TS 33.310) and only accept compliant certificates<br>• Receiving TLS *(and SEG)* entities shall be able to process "critical" extensions<br><br>Hash algorithms (prior to signing certificate):<br>• ❗ Mandatory to support: **SHA-256**<br>• 👍 Recommended to support: **SHA-384**<br>• 🚫 Prohibited to support: **MD5**, **MD2**, **SHA-1**<br><br>Signature algorithms:<br>• ❗ Mandatory to support: **RSAEncryption** *(not recommended, since it uses PKCS#1v1.5 padding)*, **ecdsa**<br><br>Public key algorithms:<br>• ❗ Mandatory to support: **rsaEncryption**, **id-ecPublicKey**<br><br>Parameters for ecdsa and id-ecPublicKey:<br>• ❗ Mandatory to support: **secp256r1**<br>• 👍 Recommended to support: **secp384r1**<br><br>RSA certificates:<br>• ❗ Requirements on public key length: **at least 2048 bits**<br>• ❗ Mandatory to support public key length: **at least 4096 bits**<br>• 🚫 Prohibited to support public key length: **less than 2048 bits**<br>• ⚠ Not recommended to use parameters: key lengths **less than 3072 bits**, **PKCS#1v1.5 padding** *(should not be used in certificates expiring after 2030)*[a]<br>• ❗ Requirements on public exponent: **no less than 65537**<br><br>[a] *By 2030, several organizations plan to prohibit the usage of RSA with key lengths less than 3072 bits and with PKCS#1v1.5 padding*<br><br>ECDSA certificates:<br>• 🚫 Prohibited to support elliptic curve groups: **less than 256 bits** *(except curve25519, ed25519, and W-25519)*<br>• ❗ Mandatory to support public key length: **at least 384 bits**<br>• ❓ Optional to use algorithms: **deterministic ECDSA** (RFC 6979 [331])<br>• 👍 **ECDSA** is recommended for newly created certificates<br><br>Security level of public keys:<br>• The public key signing the certificate shall have at least the same security level as the public keys in the certificate<br><br>Subject and issuer name format:<br>• `(C=<country>), O=<Organization Name>, CN=<Some distinguishing name>` *(O and CN shall have UTF8 format, C is optional)*<br>• `cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>` *(ou is optional)* | Requirements on certificates:<br>• **X.509 version 3 certificate** (RFC 5280 [95])<br>• Shall be compliant with the CNSA Suite Certificate and CRL profile (CNSA 1.0: RFC 8603 [201], CNSA 2.0: [200])<br><br>Hash algorithms (prior to signing certificate):<br>• CNSA 1.0: **SHA-384**<br>• CNSA 2.0: **internal hashing of ML-DSA or ML-KEM**; otherwise **SHA-384** should be used or **SHA-512** may be used<br><br>Signature algorithms:<br>• CNSA 1.0: **RSAEncryption**, **ecdsa**<br>• CNSA 2.0: **id-ML-DSA-87**<br><br>Public key algorithms:<br>• CNSA 1.0: **rsaEncryption**, **id-ecPublicKey**<br>• CNSA 2.0: **id-ML-DSA-87** *(for signature verification keys)*, **id-alg-ml-kem-1024** *(for key management keys)*<br><br>Parameters for ecdsa and id-ecPublicKey (CNSA 1.0):<br>• **secp384r1**<br><br>RSA certificates (CNSA 1.0):<br>• Public key length: **3072** or **4096 bits**<br>• Public exponent: shall satisfy $2^{16} < e < 2^{256}$ and be **odd** (DSS [284])<br>• **RSASSA-PKCS1-v1_5**<br>• If RSASSA-PSS is supported: **rsaEncryption**, **SHA-384**, **MGF1** (RFC 8017 [267]), **48-octet salt**<br><br>ECDSA certificates (CNSA 1.0):<br>• **secp384r1** uncompressed form (RFC 5480 [330]) *(compressed form is optional)* |

*Continued on the next page*

**Table 5.5** *(continued from the previous page)*

| | 3GPP | CNSA (2.0) |
|---|---|---|
| | Certificate revocation verification:<br>• ❗ Mandatory to support methods: **CRLs** (TS 33.310, 6.1a)<br>• 👍Recommended to support methods: **OCSP** (TS 33.310, 6.1b)<br>Certificate extensions:<br>• Extensions mentioned in RFC 5280 [95] but not mandated by TS 33.310 are optional to implement *(shall be marked as "non critical" if present)* | Certificate extensions:<br>• Per RFC 8603 [201] ([200]) for different certificate types; not mentioned extensions remain at the requirement level of RFC 5280 [95]. |
| **TLS entity certificate profile** (TS 33.310 [16] clause 6.1.3a) | Additional requirements:<br>• TLS client and server certificates shall be directly signed by the corresponding TLS client and server CAs in the operator domain they belong to<br>• Recommendations for SIP domain certificates: RFC 5922 [224] and RFC 5924 [229]<br>• The issuer name in the TLS CA certificate is the same as the subject name<br>Extensions:<br>• ❗ Mandatory critical extensions: **Key Usage** *(at least **digitalSignature** shall be set)*<br>• ❗ Mandatory non-critical extensions: **CRL Distribution Points**<br>• ❓Optional non-critical extensions: **Authority Key Identifier**, **Subject Key Identifier**, **Extended Key Usage** *(if present, then at least **id-kp-serverAuth** and **id-kp-clientAuth** shall be set for TLS server and client certificates respectively)* | Extensions:<br>• Self-signed: critical: **Key Usage**, **Basic Constraints**; non-critical: **Subject Key Identifier**<br>• Non-self-signed: critical: **Key Usage**, **Basic Constraints**; non-critical: **Authority Key Identifier**, **Certificate Policies** *(if a policy is asserted)*<br>• End-entity: critical: **Key Usage**; non-critical: **Authority Key Identifier**, **Certificate Policies** *(if a policy is asserted)*; **Subject Key Identifier** *(recommended)*<br>• *For further requirements see RFC 8603 [201] ([200])* |

3GPP allows support only for (D)TLS versions 1.2 and 1.3. Other versions, namely SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and DTLS 1.0 have been deprecated by IETF [329, 82, 266] and are obsolete [308]. Support for TLS 1.3 is required by NIST for agencies since January 1, 2024, with a recommendation to also support TLS 1.2 next to TLS 1.3, unless TLS 1.3 servers do not need TLS 1.2 for interoperability [253]. NIST also prohibits using servers that incorrectly implement TLS version negotiation.

Compared to the guidelines for TLS implementations in NIST SP 800-52 [253], 3GPP requirements for the TLS entity certificate profile in TS 33.310 [16] align with the ones specified by NIST. Similar to 3GPP, NIST requires TLS certificates to be the version 3 of an X.509 certificate. The public key in the certificate and the signature must have at least 112 bits of security (i.e. RSA modulus length at least 2048 bits and ECDSA length at least 224 bits [76]). RSA or ECDSA signature certificates (using SHA-256) are required for TLS servers, with ECDSA signature certificates using curve P-256 or curve P-384 for the public key (secp256r1 and secp384r1, respectively in SECG [317]). Furthermore, NIST requires that server certificates are issued by a Certificate Authority (CA) which publishes the certificate revocation information in Online Certificate Status Protocol (OCSP) responses and, optionally, in a Certificate Revocation List (CRL), similar to 3GPP. For extensions, TS 33.310 agrees with NIST, except that NIST requires Authority Information Access non-critical extension, which is not mandated by 3GPP.

Profiling for TLS 1.3 is summarized in Table 5.6, as per TS 33.210 [17]. TLS 1.3 (specified in RFC 8446 [337]) is an improvement over TLS 1.2 (specified in RFC 5246 [339]), with a new handshake protocol and a new key derivation process using HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [253]. It removes all symmetric encryption algorithms considered legacy and the CBC mode of operation for block ciphers (e.g. AES), leaving only AEAD algorithms [249, 253]. Furthermore, it removes the cipher suites using static RSA key transport and DH key exchange, limiting the supported public-key based key exchange algorithms to only those providing perfect forward secrecy (PFS, i.e. a compromise of a long-term private key does not result in the compromise of a session key established using the long-term key [253]). RSA padding has been changed to use the RSA Probabilistic Signature Scheme (RSASSA-PSS). New signature algorithms such as EdDSA have been added, and point format negotiation, the DSA, and custom Ephemeral DH (DHE) groups have been removed. SHA-1

has also been removed, which, together with MD5, has been deprecated for TLS 1.2 and TLS 1.3 by IETF [391]. Many TLS 1.2 (and earlier) extensions cannot be used with TLS 1.3 [253]. Finally, handshake messages after the ServerHello are encrypted in TLS 1.3 [337]. The new EncryptedExtensions message allows some extensions that were previously sent unencrypted in the ServerHello message to be sent with confidentiality protection.

**Table 5.6:** Cryptographic profiles for (D)TLS 1.3, based on 3GPP TS 33.210 [17] and RFC 8446 [337]. CNSA (2.0) requirements, based on RFC 9151 [121] and the I-D [84], are common for CNSA 1.0 and 2.0, unless specified otherwise.

| | 3GPP | CNSA (2.0) |
|---|---|---|
| **General** | ! Requirements on support:<br>• For TLS 1.3 cipher suites: RFC 8446 [337] section 9.1<br>• For TLS 1.3 extensions: RFC 8446 [337] sections 4.2 and 9.2, and RFC 9325 [361]<br>• For HTTP/2 over TLS 1.3: RFC 9113 [380] section 9.2.3<br>*Differences in 3GPP compared to IETF RFCs are marked with "(!)"* | ? Optional to support features:<br>• (D)TLS server may send a **NewSessionTicket** message to a (D)TLS client to enable resumption<br>! CNSA 2.0 requirements on PSKs:<br>• **PSK-based authentication** may be used next to certificate-based authentication (RFC 8773 [189])<br>• PSKs shall be **at least 256 bits**, generated from a **NIST-approved random bit generator** supporting **256-bit entropy** (SP 800-90C [81]) |
| **TLS cipher suites** | ! Mandatory to support cipher suites:<br>• **TLS_AES_128_GCM_SHA256** (GCM [133], RFC 5116 [251], SHS [302]) *(AEAD cipher)*<br>👍 Recommended to support cipher suites:<br>• **TLS_AES_256_GCM_SHA384** (GCM [133], RFC 5116 [251], SHS [302]) *(AEAD cipher)*<br>• **TLS_CHACHA20_POLY1305_SHA256** (RFC 8439 [318], SHS [302]) *(AEAD cipher)*<br>🚫 Prohibited to support cipher suites:<br>• **TLS_SHA256_SHA256** (RFC 9150 [105]) **(!)** *(not mentioned in RFC 8446 section 9.1)*<br>• **TLS_SHA384_SHA384** (RFC 9150 [105]) **(!)** *(not mentioned in RFC 8446 section 9.1)* | ! CNSA (2.0) requirements:<br>• **TLS_AES_256_GCM_SHA384**<br>• This cipher suite shall be the first (most preferred) cipher suite in ClientHello and extensions |
| **TLS signature schemes** | ! Mandatory to support signature schemes:<br>• **rsa_pkcs1_sha256** *(for certificates)*<br>• **rsa_pss_rsae_sha256** *(for CertificateVerify and certificates)*<br>• **ecdsa_secp256r1_sha256**<br>👍 Recommended to support signature schemes:<br>• **ecdsa_secp384r1_sha384** **(!)** *(not mentioned in RFC 8446 section 9.1)* | ! CNSA 1.0 requirements for "signature_algorithms":<br>• **ecdsa_secp384r1_sha384**<br>• **rsa_pss_pss_sha384**<br>• **rsa_pss_rsae_sha384**<br>• Clients allowing negotiation of TLS 1.2 may offer **rsa_pkcs1_sha384** with TLS 1.2<br>! CNSA 1.0 requirements for "signature_algorithms_cert":<br>• **ecdsa_secp384r1_sha384**<br>• **rsa_pkcs1_sha384**<br>• If supported, **rsa_pss_pss_sha384** and **rsa_pss_rsae_sha384** should be offered<br>! CNSA 2.0 requirements (for "signature_algorithms" and "signature_algorithms_cert"):<br>• **ML-DSA-87** (FIPS 204 [290]) |

*Continued on the next page*

**Table 5.6** *(continued from the previous page)*

| | 3GPP | CNSA (2.0) |
|---|---|---|
| **TLS key exchange modes and DH groups** | ! Mandatory to support key exchange modes:<br>• **secp256r1** (NIST P-256)<br>👍 Recommended to support key exchange modes:<br>• **x25519** (RFC 7748 [227])<br>• **secp384r1** (NIST P-384) **(!)** *(not mentioned in RFC 8446 section 9.1)*<br>🚫 Prohibited to support key exchange modes:<br>• **ffdhe2048 (!)** *(not mentioned in RFC 8446 section 9.1)* | ! CNSA 1.0 requirements:<br>• ECDHE: **secp384r1**, using **uncompressed form** (RFC 8422 [317], RFC 8446 [337], SP 800-56A Rev. 3 sec. 5.6.1.2 [79])<br>• DHE: **ffdhe3072**, **ffdhe4096** (RFC 7919 [166], SP 800-56A Rev. 3 sec. 5.6.1.1.1 [79])<br>! CNSA 2.0 requirements:<br>• **ML-KEM-1024** (FIPS 203 [291]) |
| **TLS PSK key exchange modes** | 🚫 Prohibited to support PSK key exchange modes:<br>• **psk_ke (!)** *(not mentioned in RFC 8446 section 9.1) (no forward secrecy)* | ! CNSA (2.0) requirements:<br>• **psk_dhe_ke** shall be requested by the client **to resume a session**<br>! CNSA 2.0 requirements:<br>• 🚫 Prohibited: **psk_ke**<br>• ! Mandatory: **psk_dhe_key** using **ML-KEM-1024** *(if PSK is used)* |
| **TLS extensions** | ! Mandatory to support extensions:<br>• **Supported Versions** (RFC 8446 [337]) *(required for all ClientHello, ServerHello, and HelloRetryRequest messages)*<br>• **Cookie** (RFC 8446 [337])<br>• **Signature Algorithms** (RFC 8446 [337]) *(required for certificate authentication)*<br>• **Signature Algorithms Certificate** (RFC 8446 [337])<br>• **Supported Groups** (RFC 8446 [337]) *(required for ClientHello messages using DHE/ECDHE key exchange)*<br>• **Key Share** (RFC 8446 [337]) *(required for DHE/ECDHE key exchange)*<br>• **Server Name Indication** (RFC 6066 [1]) *(with applications capable of using it)*<br>👍 Recommended to support extensions:<br>• **Certificate Status Request**, i.e. “OCSP stapling” (RFC 6066 [1], RFC 8446 [337]) **(!)** *(not mentioned in RFC 8446 section 9.2)*<br>! Requirements for HTTP/2 over TLS 1.3:<br>• HTTP/2 servers shall not send post-handshake TLS 1.3 CertificateRequest messages *(it shall be treated by HTTP/2 clients as a connection error of type PROTOCOL_ERROR)*; post-handshake authentication is not allowed even if the client has offered the “post_handshake_auth” TLS extension<br>• TLS early data may be used to send requests if RFC 8470 [381] is followed; clients assume initial values for all server settings | ! Mandatory to include:<br>• **Signature Algorithms** (RFC 8446 [337])<br>👍 Recommended to include:<br>• **Signature Algorithms Certificate** (RFC 8446 [337]) (not required by CNSA 2.0, as only ML-DSA-87 is allowed)<br>🚫 Prohibited to include:<br>• **Early Data** *(no inherent replay protections for early data [337])*<br>! CNSA 2.0 additional requirements:<br>• To facilitate using KEM, the ML-KEM-1024 public key and ciphertext are sent via the **Key Share** extension *(in ClientHello and ServerHello, respectively [118])*<br>• **Certificate with External PSK** shall be included if external PSK is used (per RFC 8773 [189])<br>! Certificate status requirements:<br>• Certificate revocation status information shall be provided via a **CRL distribution point** or using **OCSP** *(should be requested per RFC 8446 sec. 4.4.2.1 [337])*<br>• If OCSP is supported, OCSP responses should be provided in **CertificateEntry** message |

The specified cipher suites for TLS 1.3 rely on the same cryptographic algorithms as IPsec (see subsection 5.2.1) and are all NIST-approved, except ChaCha20-Poly1305 [253]. The same holds for the TLS signature schemes, key exchange modes and (EC)DH groups, which are based on the same cryptographic primitives as IKEv2 (see subsection 5.2.2) and satisfy the minimum NIST-required security strength of 112 bits (both for TLS 1.3 and TLS 1.2) [253]. PSKs, used for session resumption in TLS 1.3, are allowed by NIST for all TLS 1.3 cipher suites, assuming the additional guidelines are followed. This is not mentioned by 3GPP in TS 33.210. As for TLS 1.3 extensions, the ones mandated or recommended by 3GPP (see Table 5.6) are also mandated by NIST if TLS 1.3 is supported. In addition, NIST requires support for Pre-Shared Key Exchange Modes if the optional Pre-Shared Key extension is sup-

ported, and discourages support for Early Data Indication. 3GPP is less clear about these extensions (see subsection 5.2.4). Finally, NIST requires system administrators to carefully assess the risks of supporting non-mandatory extensions and advises against supporting extensions that are not required by the application and do not enhance security. Otherwise, this can have unexpected security implications due to increased chance of implementation flaws (e.g. Heartbleed [282] was an implementation bug for the heartbeat extension [403]).

Table 5.7 shows the profiles for TLS 1.2 from TS 33.210 [17]. 3GPP allows support only for cipher suites with AEAD and PFS. This requirement makes TLS 1.2 cipher suite profile similar to TLS 1.3. Furthermore, support for the finite field DH groups has also been removed (see Appendix A).

**Table 5.7:** Cryptographic profiles for (D)TLS 1.2, based on 3GPP TS 33.210 [17] and RFC 5246 [339]. CNSA 1.0 requirements are based on RFC 9151 [121]. As per the I-D [84], connections with TLS 1.2 or lower cannot be CNSA 2.0-compliant.

| | 3GPP | CNSA (1.0) |
|---|---|---|
| **TLS cipher suites** | ! Requirements on support:<br>• The rules on allowed cipher suites are given in RFC 5246 [339]<br>• Only **cipher suites with AEAD** *(e.g. GCM)* and **PFS** *(i.e. ECDHE)* shall be supported<br>! Mandatory to support and recommended to use cipher suites:<br>• **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** (RFC 5289 [338])<br>• **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** (RFC 5289 [338])<br>👍 Recommended to support cipher suites:<br>• **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** (RFC 5289 [338])<br>• **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (RFC 5289 [338])<br>🚫 Prohibited to support ciphers:<br>• Cipher suites **without AEAD** *(e.g. CBC, CTR)*<br>• Cipher suites **without PFS** *(e.g. DH, ECDH)*<br>• Cipher suites **using DHE** *(as specified in requirements for DH groups)* | ! General requirements:<br>• RFC 5246 [339] shall be used<br>• Updates in RFC 8446 [337] (sec. 1.3) should be applied<br>! CNSA requirements:<br>• **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** (RFC 5289 [338], RFC 8422 [317])<br>• **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** (RFC 5289 [338], RFC 8422 [317])<br>• **TLS_RSA_WITH_AES_256_GCM_SHA384** (RFC 5288 [351])<br>• **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384** (RFC 5288 [351], RFC 7919 [166])<br>• The above cipher suites shall be the first (most preferred) cipher suites in ClientHello<br>• For RSA key transport, **RSAES-PKCS1-v1_5** (RFC 8017 [267]) shall be supported |
| **PSK cipher suites** | ! Requirements on support:<br>• If psk cipher suites are implemented in TLS, RFC 5489 [182] applies<br>! Mandatory to support and recommended to use cipher suites:<br>• **TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256** (RFC 8442 [249])<br>! Recommended to support cipher suites:<br>• **TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384** (RFC 8442 [249]) | N/A |
| **Diffie-Hellman groups** | ! Mandatory to support groups:<br>• **secp256r1** (NIST P-256) (RFC 8422 [317], SECG-SEC2 [100])<br>👍 Recommended to support groups:<br>• **secp384r1** (NIST P-384) (RFC 8422 [317], SECG-SEC2 [100])<br>🚫 Prohibited to support groups:<br>• **Elliptic curve groups of less than 256 bits** (except x25519)<br>• **Finite field Diffie-Hellman** (i.e. DHE) | ! CNSA requirements:<br>• ECDHE: **secp384r1**, using **uncompressed form** (RFC 8422 [317], RFC 8446 [337], SP 800-56A Rev. 3 sec. 5.6.1.2 [79])<br>• DHE: **ffdhe3072**, **ffdhe4096** (RFC 7919 [166], SP 800-56A Rev. 3 sec. 5.6.1.1.1 [79]) |

*Continued on the next page*

**Table 5.7** *(continued from the previous page)*

| | 3GPP | CNSA (1.0) |
|---|---|---|
| **Hash functions** | ! Mandatory to support functions:<br>• **SHA-256**<br>👍 Recommended to support functions:<br>• **SHA-384**<br>🚫 Prohibited to support functions:<br>• **SHA-1**<br>• **MD5** | ! CNSA requirements:<br>• **SHA-384** (SHS [302]) |
| **Signature algorithms** | ! Mandatory to support algorithms:<br>• **ecdsa**<br>• **rsa_pss_rsae**<br>• **rsa_pkcs1** *(usage not recommended by 3GPP)*<br>👍 Recommended to support algorithms:<br>• **ecdsa_secp384r1_sha384** | ! CNSA requirements (for "signature_algorithms" and "signature_algorithms_cert"):<br>• **ecdsa_secp384r1_sha384**<br>• **rsa_pkcs1_sha384**<br>• If supported, **rsa_pss_pss_sha384** and **rsa_pss_rsae_sha384** should be offered |
| **TLS compression** | ! Mandatory to support methods:<br>• **"null" compression method** (RFC 5246 [339])<br>🚫 Prohibited to support methods:<br>• All other compression methods | N/A |
| **TLS extensions** | ! Requirements on support:<br>• If TLS extensions are used with TLS, RFC 6066 [1] applies<br>! Mandatory to support extensions:<br>• **Server Name Indication** (RFC 6066 [1])<br>• **Renegotiation Indication** (RFC 5746 [397]) *(for TLS servers and clients; the server shall accept client-initiated renegotiation only if secured based on RFC 5746 [397])*<br>• **Extended Master Secret** (RFC 7627 [89])<br>• **Signature Algorithms** (RFC 5246 [339])<br>• **Supported Groups** (RFC 8422 [317], RFC 7919 [166])<br>👍 Recommended to support extensions:<br>• **TLS Session Resumption** (RFC 5246 [339] or RFC 5077 [146])<br>• **Certificate Status Request** (OCSP Status) (RFC 6066 [1])<br>🚫 Prohibited to support extensions:<br>• **Truncated HMAC** (RFC 6066 [1]) | ! Mandatory to include:<br>• **Signature Algorithms** (RFC 8446 [337])<br>👍 Recommended to include:<br>• **Extended Master Secret** (RFC 7627 [89])<br>👍 Optional to include:<br>• **Signature Algorithms Certificate** (RFC 8446 [337])<br>! Certificate status requirements:<br>• Certificate revocation status information shall be provided via a **CRL distribution point** or using **OCSP** *(should be requested per RFC 8446 sec. 4.4.2.1 [337])*<br>• If OCSP is supported, OCSP responses should be provided in **CertificateStatus** message |

Similarly to TLS 1.3, profiling for TLS 1.2 specifies the cipher suites, DH groups, hash functions and signature algorithms that are approved by NIST [253]. While NIST does not mention the PSK cipher suites from Table 5.7, RFC 8442 [249] where they are defined was published at around the same time as the NIST SP [253]. Nevertheless, NIST requires PSKs to provide at least 112 bits of security and to be distributed securely. In general, NIST does not recommend PSK usage in TLS versions before TLS 1.3 and for initial session setup in TLS 1.3, however, it suggests considering PSK cipher suites in infrastructure applications, especially if network entities are required to be frequently authenticated, but only if both client and server belong to the same organization. Regarding extensions for TLS 1.2, the mandated and recommended extensions from Table 5.7 are also mandated by the NIST SP 800-52. The Certificate Signature Algorithms extension is recommended for TLS 1.2, but it is not mentioned by 3GPP. Furthermore, NIST requires support for the Supported Point Formats and Supported Elliptic Curves extensions from RFC 8422 [317] if the EC cipher suites are supported, and discourages support for Client Certificate URL (due to potential DoS attacks), while 3GPP does not mention these extensions (see subsection 5.2.4). Lastly, NIST emphasizes the importance to understand the security impact of TLS session resumption if long-term or shared keys are compromised, and suggests frequent key replacement and short lifetimes for resumption information if the feature is supported. Note that TLS session resumption can reduce the protection provided by the forward secrecy [373].

For both (D)TLS 1.3 and 1.2 profiles (see Table 5.6 and Table 5.7, respectively), it can be seen that 3GPP is more lenient with the allowed cryptographic algorithms than CNSA 1.0 and CNSA 2.0. This is to be expected, given the nature of NSS, which are the target audience for both CNSA Suites. Since CNSA 2.0 requires two new post-quantum algorithms (ML-KEM and ML-DSA), their inclusion into 3GPP standardization will take time (as discussed in subsection 5.6.4). On the other hand, the main difference between 3GPP and CNSA 1.0 profiles is that the latter allows only SHA-384, 256-bit keys for AES, and P-384 curve, while 3GPP also allows less secure versions of the corresponding algorithms. This is something that could be addressed in the next 3GPP releases, for as much as it is possible.

As it is always the case, having a secure cryptographic profiling does not guarantee that the system is secure. It is also crucial for organizations and agencies to use appropriate network security protections [204], follow the guidelines for storage media sanitization [216], and keep their servers and the associated platforms up-to-date for security patches [253]. Furthermore, system administrators and site operators should understand the tradeoffs between optimizing the performance of TLS and offering high security levels [373]. Since cryptographic security guarantees are bound by the weakest cipher suite allowed by the configuration, the system administrators should understand all consequences when choosing cipher suites and configuring the system to support only those profiles [253]. Throughout the time, certain TLS cipher suites have become vulnerable to specific attacks (e.g. timing attacks against CBC cipher suites [65, 106], other timing attacks [268, 255, 103, 101], CBC padding attacks [264, 226], collision attacks [88], hash function attacks [336], and attacks on smaller DH groups [61]). This requires implementing the relevant mitigation measures, such as (near) constant-time decryption, correct decoding of padding bytes, usage of AEAD ciphers (to prevent CBC-based attacks), and correct deployment of DH [253, 176]. Secure random number generation (with $\geq$112 bits of security) is also crucial, as the server and client random numbers affect the randomness of the session keys [253, 301].

### 5.2.4. Ambiguities

When analysing cryptographic profiles for IPsec, IKEv2, and (D)TLS in TS 33.210 [17], we encountered some ambiguous places (see Table 5.8). The document often references RFCs specifying requirements for cryptographic profiles or protocol implementations (e.g. RFC 8221 [405] for IPsec, RFC 7296 [209] and RFC 8247 [319] for IKEv2, RFC 8446 [337] for TLS 1.3, and RFC 5246 [339] for TLS 1.2). In case of conflicts, TS 33.210 takes precedence over the referenced RFC. However, an ambiguity occurs when the referenced RFC defines an algorithm that is not mentioned in TS 33.210. Such places can be interpreted differently. For example, an NDS/IP network operator may interpret such an algorithm as “optional to support”, since it is not explicitly prohibited by 3GPP, and may decide to implement it due to available hardware features, even if it was not the intention of 3GPP. This could lead to vulnerabilities [236] or downgrade attacks if the algorithm is weak or gets broken. In general, any silence in specifications is considered by the implementers as a “design freedom” [332]. We advise 3GPP to resolve such ambiguities by either explicitly prohibiting all algorithms other than the ones specified, or by mentioning that their support is the operator’s decision.

**Table 5.8:** Ambiguities between 3GPP TS 33.210 [17] and RFCs.

| | |
|---|---|
| **IPsec** (RFC 8221 [405]) | Encryption and authentication transforms:<br>RFC 8221, referenced by TS 33.210 for the implementation conformance requirements for ESP encryption and authentication transforms, says that *“any algorithm listed at the IPsec IANA registry [198] that is not mentioned in this document MAY be implemented”*. 3GPP does not mention this in TS 33.210. |
| **IKEv2** (RFC 8247 [319]) | Algorithm selection - transform types 1, 2, 3, 4:<br>RFC 8247, referenced by TS 33.210 for the implementation requirements and usage guidance, says that *“any algorithm listed at the IKEv2 IANA registry [198] not mentioned in this document MAY be implemented”*. 3GPP does not mention this in TS 33.210. Note, however, that 3GPP explicitly says that *“the use of Diffie-Hellman MODP groups less than 2048-bit shall not be supported”*, which prohibits the support of such groups in the IKEv2 IANA registry. |

*Continued on the next page*

**Table 5.8** *(continued from the previous page)*

| | |
|---|---|
| **(D)TLS 1.3** (RFC 8446 [337]) | Cipher suites:<br>RFC 8446, which TS 33.210 references as the required RFC for TLS 1.3 support, also defines **TLS_AES_128_CCM_SHA256** (RFC 5116 [251], SHS [302]) and **TLS_AES_128_CCM_8_SHA256** (RFC 6655 [252], SHS [302]), which are not mentioned in RFC 8446 section 9.1. 3GPP does not mention these cipher suites in TS 33.210.<br>Signature schemes:<br>RFC 8446 also lists the following schemes that are not mentioned by 3GPP in TS 33.210, nor in the requirements from TLS 1.3 RFC 8446 section 9.1:<br>• RSASSA-PKCS1-v1_5 algorithms: **rsa_pkcs1_sha384**, **rsa_pkcs1_sha512**<br>• RSASSA-PSS algorithms with public key OID rsaEncryption: **rsa_pss_rsae_sha384**, **rsa_pss_rsae_sha512**<br>• RSASSA-PSS algorithms with public key OID RSASSA-PSS: **rsa_pss_pss_sha256**, **rsa_pss_pss_sha384**, **rsa_pss_pss_sha512**<br>• ECDSA algorithms: **ecdsa_secp521r1_sha512**<br>• EdDSA algorithms: **ed25519**, **ed448**<br>• Legacy algorithms: **rsa_pkcs1_sha1**, **ecdsa_sha1** *(refer only to signatures that appear in certificates, and are not defined for usage in signed TLS handshake messages; should not be negotiated, unless for backward compatibility; shall be listed as the lowest priority by the clients offering them; servers shall not offer a SHA-1 signed certificate, unless no valid certificate chain can be produced without it)*<br>Key exchange groups/curves:<br>RFC 8446 also defines **secp521r1**, **x448** and finite field DHE groups **ffdhe3072**, **ffdhe4096**, **ffdhe6144**, **ffdhe8192**, which are not mentioned in RFC 8446 section 9.1. 3GPP does not mention them in TS 33.210.<br>Pre Shared Key (PSK) key exchange modes:<br>RFC 8446 also defines **psk_dhe_ke**. 3GPP does not mention it in TS 33.210.<br>TLS extensions:<br>RFC 8446 requires support of **Pre-Shared Key** and **Pre-Shared Key Exchange Modes** for PSK key agreement if the implementation offers this feature, but they are not mentioned as mandatory or recommended. Furthermore, in RFC 8446 section 4.2, other extensions are defined (**Certificate Authorities**, **OID Filters**, **Post-Handshake Client Authentication** *(not HTTP/2)*, **Early Data Indication**) or referenced (e.g. **Server Name**, **Maximum Fragment Length Negotiation** from RFC 6066 [1]). 3GPP does not mention these extensions in TS 33.210. |
| **(D)TLS 1.2** (RFC 5246 [339]) | PSK cipher suites:<br>RFC 8442 [249], which TS 33.210 only references for the two (GCM) PSK cipher suites, also defines **TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256** and **TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256**. 3GPP does not mention these cipher suites in TS 33.210.<br>Key exchange groups/curves:<br>RFC 8422 [317], which TS 33.210 only references for the explicitly supported curves, also defines **secp521r1** (P-521) (RFC 8422 [317], SECG-SEC2 [100]), **x25519** (RFC 7748 [227]) and **x448** (RFC 7748 [227]) (and only allows support for “uncompressed” point format). 3GPP does not mention these curves in TS 33.210.<br>Hash functions:<br>RFC 5246, which TS 33.210 references as the required RFC for TLS 1.2 support, also defines **SHA-224** and **SHA-512** (and “none” or “unhashed data” if a signature algorithm does not require hashing before signing). 3GPP does not mention these hash functions in TS 33.210.<br>Signature algorithms:<br>RFC 5246 also defines **dsa** and **anonymous** signatures (i.e. in case of anonymous negotiation). Furthermore, RFC 8422 [317] defines **eddsa**, **ed25519**, and **ed448** (which are not mentioned in TLS 1.2 RFC 5246). 3GPP does not mention these signature algorithms in TS 33.210.<br>TLS extensions:<br>RFC 6066 [1], which TS 33.210 says *“shall apply”* if TLS Extensions are used in conjunction with TLS, also defines **Maximum Fragment Length Negotiation**, **Client Certificate URLs**, and **Trusted CA Indication**. Furthermore, **Supported Elliptic Curves** and **Supported Point Formats** are required for ECC cipher suites by RFC 8422 [317]. 3GPP does not mention these extensions in TS 33.210. |

## 5.3. AS/NAS security

Access-Stratum (AS) between UE and gNB(-CU) and Non-Access Stratum (NAS) between UE and AMF correspond to the Uu and N1 interfaces, respectively. Protection of NAS signalling is provided by the NAS protocol, while protection of RRC signalling (CP) and user data (UP) are provided by PDCP (see Figure 5.2 for a schematic overview). Both protections rely on three non-NULL algorithms: 128-N(E/I)A1, 128-N(E/I)A2, and 128-N(E/I)A3 (see Table 5.9). The NULL algorithm (NEA0/NIA0) provides no security. As seen earlier in Table 5.1, RRC and NAS integrity protection (with a non-NULL algorithm) is mandatory to use (see Table 5.9 for exceptions), while RRC, NAS, and UP ciphering and UP integrity protection are optional to use (although ciphering is recommended to use whenever regulations permit).

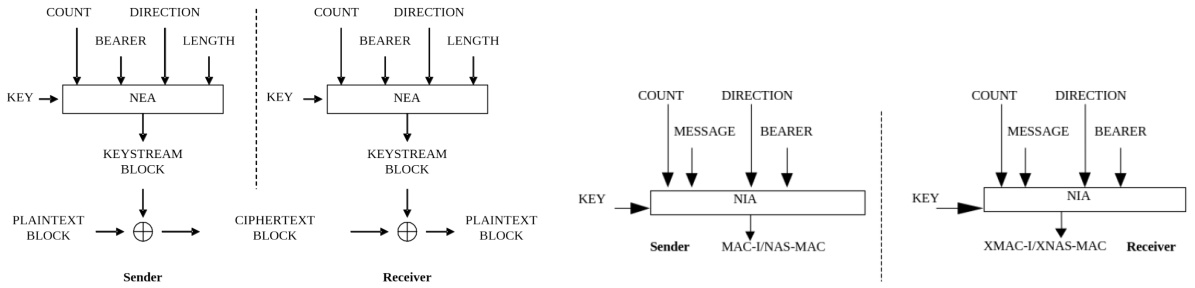



**Figure 5.2:** Schematic overview of the security mechanisms for AS and NAS, as defined in TS 33.501 [33]: (a) ciphering and (b) integrity protection.

**Table 5.9:** Ciphering and integrity protection for AS and NAS, based on 3GPP TS 33.501 [33], TS 33.401 [57], TS 38.323 [28] (PDCP), TS 24.501 [25] (NAS), TS 38.331 [30] (RRC).

| | |
|---|---|
| **AS/NAS ciphering and deciphering** (TS 33.501 [33], TS 33.401 [57], TS 38.323 [28], TS 38.331 [30], TS 24.501 [25]) | AS/NAS ciphering algorithms:<br>• **NEA0:** a KEYSTREAM of all zeroes<br>• **128-NEA1:** based on SNOW 3G (TS 35.215 [42])<br>• **128-NEA2:** based on 128-bit AES in CTR mode (FIPS 197 [277], SP 800-38A [132])<br>• **128-NEA3:** based on ZUC (TS 35.221 [38])<br>AS ciphering (done by PDCP) appiles to the following data units:<br>• **MAC-I** *(i.e. PDCP follows MAC-then-Encrypt principle)*<br>• **Data part of the PDCP Data PDU** *(except SDAP header and SDAP Control PDU if present)*<br>• NB! Not applicable to PDCP Control PDUs, MRBs and sidelink SRB4<br>NAS ciphering (done by NAS) applies to the following Information Elements (IEs):<br>• **Plain 5GS NAS message** *(when a NAS message needs to be both ciphered and integrity protected, it is first ciphered and then the ciphered message and the NAS sequence number (SN) are integrity protected by computing a MAC, i.e. NAS follows Encrypt-then-MAC principle; otherwise, the unciphered NAS message and the NAS SN are integrity protected with a MAC)*<br>The required inputs to the ciphering function:<br>• $\boldsymbol{COUNT}$ *(32 bits)*<br>• $\boldsymbol{DIRECTION}$ *(direction of the transmission, 1 bit: UL = 0, DL = 1)*<br>• $\boldsymbol{BEARER}$ *(radio bearer identifier, 5 bits)*<br>• $\boldsymbol{LENGTH}$ *(length of the keystream required, only affects the length of the KEYSTREAM BLOCK)*<br>• $\boldsymbol{KEY}$ *(*$\boldsymbol{K_{RRCenc}}$ *for RRC (CP),* $\boldsymbol{K_{UPenc}}$ *for UP,* $\boldsymbol{K_{NASenc}}$ *for NAS (CP); 128 bits)* |
| **AS/NAS integrity protection and verification** (TS 33.501 [33], TS 33.401 [57], TS 38.323 [28], TS 38.331 [30], TS 24.501 [25]) | AS/NAS integrity protection algorithms:<br>• **NIA0:** shall generate a 32 bit (X)MAC-I of all 0s<br>• **128-NIA1:** based on SNOW 3G (TS 35.215 [42])<br>• **128-NIA2:** based on 128-bit AES in CMAC mode (FIPS 197 [277], SP 800-38B [134])<br>• **128-NIA3:** based on ZUC (TS 35.221 [38])<br>AS integrity protection (done by PDCP) applies to the following data units:<br>• **PDCP header**<br>• **Data part of the PDCP** before ciphering<br>• NB! Not applicable to PDCP Control PDUs, MRBs and sidelink SRB4<br>• Integrity protection is always applied to PDCP Data PDUs of SRBs, i.e. CP *(padding of "0"s if not configured, e.g. in unauthenticated emergencies)*<br>NAS integrity protection (done by NAS) applies to the following Information Elements (IEs):<br>• **Sequence number**<br>• **Plain 5GS NAS message** *(ciphered or unciphered)*<br>The required inputs to the integrity function include:<br>• $\boldsymbol{COUNT}$ *(32 bits)*<br>• $\boldsymbol{DIRECTION}$ *(direction of the transmission, 1 bit: UL = 0, DL = 1)*<br>• $\boldsymbol{BEARER}$ *(radio bearer identifier, 5 bits)*<br>• $\boldsymbol{MESSAGE}$ *(the message itself; bit length is* $LENGTH$*)*<br>• $\boldsymbol{KEY}$ *(*$\boldsymbol{K_{RRCint}}$ *for RRC (CP),* $\boldsymbol{K_{UPint}}$ *for UP,* $\boldsymbol{K_{NASint}}$ *for NAS (CP), 128 bits)* |

*Continued on the next page*

**Table 5.9** *(continued from the previous page)*

| | |
|---|---|
| **NULL integrity protection for NAS** (TS 24.501 [25]) *(for more information and comments, see clause 4.4.4.1 of TS 24.501)* | Using the NULL integrity protection algorithm *(5G-IA0 in TS 24.501 and NIA0 in TS 33.501)* in the current 5G NAS security context is allowed only in the following cases:<br>1. **for an unauthenticated UE for which establishment of emergency services is allowed**<br>2. **for a W-AGF[a] acting on behalf of an FN-RG**<br>3. **for a W-AGF acting on behalf of an N5GC device**<br>4. **for a 5G-RG acting on behalf of an Authenticable Non-3GPP (AUN3) device**<br>[a] *Wireline Access Gateway Function (W-AGF) acting on behalf of the Non-5G Capable (N5GC) device is a W-AGF that enables an N5GC device behind a 5G-CRG (5G Cable Residential Gateway) or an FN-CRG (Fixed Network Cable RG) to connect to the 5G Core (definition from TS 24.501)* |
| **Integrity checking of NAS signalling messages in the UE** (TS 24.501 [25]) *(for more information and comments, see clause 4.4.4.2 of TS 24.501)* | The following NAS messages are accepted by the UE without integrity protection, as in certain situations they are sent by the network before security can be activated:<br>1. **IDENTITY REQUEST** *(if requested identification parameter is SUCI)*<br>2. **AUTHENTICATION REQUEST**<br>3. **AUTHENTICATION RESULT**<br>4. **AUTHENTICATION REJECT**<br>5. **REGISTRATION REJECT** *(if the 5GMM cause is not #76, #78, #81 or #82)*[a]<br>6. **DEREGISTRATION ACCEPT** *(for non switch off)*<br>7. **SERVICE REJECT** *(if the 5GMM cause is not #76 or #78)*<br>• All other NAS signalling messages shall not be processed by the receiving UE unless the network has set up secure NAS message exchange for the NAS signalling connection.<br>• Once the secure NAS message exchange has been established, the UE shall not process any NAS messages that have not passed the integrity check and shall discard such messages. The same applies to NAS messages received without integrity protection, despite the establishment of the secure exchange of NAS messages by the network.<br>[a] *#76 = "Not authorized for this CAG or authorized for CAG cells only" (CAG being Closed Access Group), #78 = "PLMN not allowed to operate at the present UE location", #81 = "Selected N3IWF is not compatible with the allowed NSSAI" (N3IWF being Non-3GPP Inter-Working Function), #82 = "Selected TNGF is not compatible with the allowed NSSAI" (TNGF being Trusted Non-3GPP Gateway Function)* |
| **Integrity checking of NAS signalling messages in the AMF** (TS 24.501 [25]) *(for more information and comments, see clause 4.4.4.3 of TS 24.501)* | The following NAS messages are processed by the AMF even when the MAC fails the integrity check or cannot be verified, as in certain situations they can be sent by the UE protected with a 5G NAS security context which is no longer available in the AMF (see TS 24.501 clause 4.4.4.3 for the required actions):<br>1. **REGISTRATION REQUEST**<br>2. **IDENTITY RESPONSE** *(if requested identification parameter is SUCI)*<br>3. **AUTHENTICATION RESPONSE**<br>4. **AUTHENTICATION FAILURE**<br>5. **SECURITY MODE REJECT**<br>6. **DEREGISTRATION REQUEST**<br>7. **DEREGISTRATION ACCEPT**<br>8. **SERVICE REQUEST** *(once a current NAS security context exists, until the secure NAS message exchange has been set up)*<br>9. **CONTROL PLANE SERVICE REQUEST** *(once a current NAS security context exists, until the secure NAS message exchange has been set up)*<br>• Integrity-unprotected REGISTRATION REQUEST is sent by the UE in case the registration procedure is started because of an inter-system change in 5GMM-IDLE mode and the UE has no current 5G NAS security context. The other messages above (except 8 and 9) are accepted without integrity protection, because in certain situations they can be sent by the UE before security can be activated<br>• Integrity-unprotected DEREGISTRATION REQUEST can be sent by the UE, for instance, if the UE is registered for emergency services and has no valid 5G NAS security context, or if a registration procedure is cancelled due to user interaction before secure NAS message exchange has been set up.<br>• All other NAS signalling messages shall not be processed by the receiving AMF *(or forwarded to the SMF)* unless secure NAS message exchange has been set up for the NAS connection.<br>• Once the secure NAS message exchange has been established, the AMF shall not process any NAS messages that have not passed the integrity check and shall discard such messages. The same applies to NAS messages received without integrity protection, despite the establishment of the secure exchange of NAS messages by the network. |
| **AS ciphering and integrity protection** (TS 38.331 [30]) *(for more information and comments, see clause 5.3.1.2 of TS 38.331)* | • AS security provides ciphering/integrity protection for RRC signalling *(SRBs)* and user data *(DRBs)*.<br>• After AS security has been activated, PDCP applies protection to all RRC messages on SRB1, SRB2, and, if configured, SRB3, SRB4, SRB5 and DRBs. This includes RRC messages carrying NAS messages *(which are also independently protected by the NAS layer)*. However, ciphering and integrity protection do not apply for SRB0 *(i.e. paging and broadcast system information)*.<br>• Both protections are always activated together *(i.e. in one message or procedure)*, and are never deactivated for SRBs *(although, switching to NEA0 is possible)*.<br>• NIA0 is used only for SRBs and for UE in limited service mode. When used for SRBs, integrity protection for DRBs is disabled. If NIA0 is used, then NEA0 is also used. |

*Continued on the next page*

**Table 5.9** *(continued from the previous page)*

| | |
|---|---|
| **Unprotected RRC messages** (TS 38.331 [30]) *(for more information and comments, see Annex B of TS 38.331)* | • Messages that can be sent (unprotected) prior to AS security activation: **DedicatedSIBRequest**, **DLInformationTransfer**, **MBSBroadcastConfiguration**, **MBSMulticastConfiguration**, **MIB**, **Paging**, **RRCReconfiguration**, **RRCReconfigurationComplete**, **RRCReject**, **RRCRelease**, **RRCSetup**, **RRCSetupComplete**, **RRCSetupRequest**, **RRCSystemInfoRequest**, **SIB1**, **SecurityModeCommand**[a], **SecurityModeFailure**, **SidelinkUEInformationNR**, **SystemInformation**, **UECapabilityEnquiry**, **UECapabilityInformation**, **ULInformationTransfer** *(22 messages)*<br>• Messages that can be sent without integrity protection after AS security activation: **MBSBroadcastConfiguration**, **MBSMulticastConfiguration**, **MIB**, **Paging**, **RRCReject**, **RRCSetup**, **RRCSystemInfoRequest**, **SIB1**, **SystemInformation** *(9 messages)*<br>• Messages that can be sent unciphered after AS security activation: **MBSBroadcastConfiguration**, **MBSMulticastConfiguration**, **MIB**, **Paging**, **RRCReestablishment**, **RRCReestablishmentRequest**[b], **RRCReject**, **RRCResumeRequest**[c], **RRCResumeRequest1**[d], **RRCSetup**, **RRCSystemInfoRequest**, **SIB1**, **SecurityModeComplete**, **SystemInformation** *(14 messages)*<br>[a] Integrity protected, but not ciphered<br>[b] Not protected by PDCP, but includes *shortMAC-I*<br>[c] Not protected by PDCP, but includes *resumeMAC-I*<br>[d] Not protected by PDCP, but includes *resumeMAC-I* |

5G AS and NAS reuse the strong, well-proven security algorithms from 4G systems [320]. Specifically, the 5G encryption algorithms 128-NEA1, 128-NEA2, and 128-NEA3 are identical to the 4G encryption algorithms 128-EEA1, 128-EEA2, and 128-EEA3, respectively, and the 5G integrity protection algorithms 128-NIA1, 128-NIA2, and 128-NIA3 are identical to the 4G integrity protection algorithms 128-EIA1, 128-EIA2, and 128-EIA3, respectively [33, 57]. As can be seen in Figure 5.2, all NEA algorithms perform the eXclusive-OR (XOR) operation (bitwise binary addition) on the plaintext and the generated keystream for encryption, and on the ciphertext and the same keystream for decryption [33]. All NIA algorithms output a 32-bit MAC: the sender computes the MAC of the message to send (MAC-I/NAS-MAC) and appends it to the message, while the receiver computes the expected MAC of the received message (XMAC-I/XNAS-MAC) and compares it to the received MAC (MAC-I/NAS-MAC).

128-EEA1 (128-NEA1) and 128-EIA1 (128-NIA1) algorithms [42, 43, 44, 45, 46], which are not distributed by ETSI, are identical to the UEA2 and UIA2 algorithms from the Universal Mobile Telecommunications System (UMTS, 3G), which are distributed by ETSI, and have a defined way to map the LTE parameters onto the UMTS parameters [150, 57]. The algorithm set is based on the SNOW 3G cipher (version 1.1) [43], chosen for UMTS since it met the 3GPP requirements for time and memory resources (it has a linear time complexity, guaranteeing efficiency during encryption/decryption, and a constant space complexity, suitable for systems with limited working memory) [324]. SNOW 3G is the successor of SNOW 2.0 of the SNOW family of ciphers, which consist of a Linear Feedback Shift Register (LFSR) part and a non-linear finite state machine part [412]. The algorithm has been thoroughly evaluated before its adoption and has been concluded to fit well for the intended use, due to the sound design principles and absence of practical attacks [151]. On the other hand, some timing and fault attacks on specific implementations have been found [102, 128], as well as some attacks on the initialization phase of the reduced round versions of the algorithm [91, 92]. Further cryptoanalysis of SNOW 3G under 256-bit keys revealed that it is not able to offer the full 256-bit security level because of the two found linear attacks with complexities $2^{172}$ and $2^{177}$, although their costs exceed the practical capabilities of current attackers who are also not likely to get enough data to perform such attacks [410, 412]. Two new ciphers, SNOW-V and the extreme performance version SNOW-Vi, have been proposed to the ETSI Security Algorithms Group of Experts (SAGE) to be considered for 5G. These algorithms have much stronger security (providing 256-bit security level) and higher speeds.

128-EEA2 (128-NEA2) and 128-EIA2 (128-NIA2), for which ETSI is not the custodian, are based on AES as specified in FIPS 197 [277], in particular AES-CTR [132] and AES-CMAC [134], respectively [150]. Both are NIST-approved algorithms [277, 272, 134], and are used as follows [57]:

- 128-NEA2 constructs the initial counter block (ICB) for AES-CTR by setting the most significant 64 bits to $COUNT[0]..COUNT[31]||BEARER[0]..BEARER[4]||DIRECTION||0^{26}$ (where $0^{26}$ is 26

consecutive zeros) and the least significant 64 bits to all zeros. The following counter blocks are constructed by incrementing ( $\mod 2^{64}$) the least significant 64 bits of the previous counter block.

- 128-NIA2 constructs the input bit string for AES-CMAC by setting the most significant 64 bits to $COUNT[0]..COUNT[31]||BEARER[0]..BEARER[4]||DIRECTION||0^{26}$ and the following bits to the actual message bits (i.e. $MESSAGE[0]..MESSAGE[BLENGTH-1]$, where $BLENGTH$ is the bit length of the message, with the total input length for AES-CMAC being $BLENGTH+64$). With these inputs, a MAC of length 32 bits is obtained and used directly as the output of 128-NIA2.

NIST states that the MAC length of at least 64 bits should suffice for protection against guessing attacks, and that smaller lengths should not be used unless the amount of times the verification process can return INVALID with any given key across all implementations is sufficiently restricted (e.g. using short session duration, or due to the low bandwidth of the communication channel) [134]. It could be that the 32-bit MAC length was chosen for performance reasons and that 3GPP has considered the risks.

128-EEA3 (128-NEA3) and 128-EIA3 (128-NIA3) algorithms [38, 39, 40, 41] are based on the ZUC stream cipher that was initially designed by the Data Assurance and Communication Security Research Centre (DACAS) at the Chinese Academy of Science, which also holds the essential patents on the cipher [150, 273]. 3GPP Systems and Architecture Group (SA3) agreed to accept ZUC as the basis for the new (third) encryption and integrity algorithm set [273]. A possible reason was that the Chinese authorities would allow its use in China. However, one stated design goal was that new algorithms are considerably different from the other two LTE algorithm sets, so that an attack on one algorithm set would not be likely to cause an attack on any of the other two. Even though there are some architectural similarities between ZUC and SNOW 3G, there are also important differences, thus, the two algorithms will not "stand or fall together". Similar to most stream ciphers, ZUC consists of a linear part (LFSR) and a non-linear part to disrupt the linearity from the LFSR contribution [411]. Over time, the cipher has undergone several international public evaluations, and some weaknesses have been found in the previous versions [273, 406, 261, 425, 354]. The current ZUC version 1.6 [39] is so far not known to have any weaknesses, nor is it known to have obvious trap-doors, and thus is believed to be secure [273]. However, a distinguishing attack against ZUC-256, the 256-bit ZUC version, with complexity $2^{236}$ has been proposed, which, while not very strong, is faster than the exhaustive key search, indicating that ZUC-256 does not achieve the full 256-security level [411, 410]. Nevertheless, 3GPP keeps the ZUC implementation requirements at the optional level (see Table 5.1) [33].

As can be seen in Table 5.9, some NAS and RRC messages can be sent without integrity protection in certain situations. The lack of authentication in these messages can lead to several attacks [415], which will be discussed in section 5.5 together with other attacks from the literature. We believe that 3GPP is aware of the risks associated with sending these NAS and RRC messages unauthenticated.

## 5.4. ECIES profiles for SUCI

Even though SUCI does not protect any of the non-SBI interfaces we focus on, it protects SUPI, which is transmitted via the N1 interface. Therefore, we include it in the protection measures for completeness. There are two non-null ECIES [99, 100] profiles for SUCI: profile A (based on Curve25519 [227] with 256-bit public keys) and profile B (based on secp256r1 [100] with 264-bit public keys), both implemented by the ME (for encryption) and SIDF in UDM (for decryption) [33]. The null-scheme offers no privacy protection. Below, we discuss both ECIES profiles and the cryptographic algorithms they rely on.

SUPI is a globally unique permanent identifier for a 5G subscription and is assigned to each subscriber in the 5G system [31]. It can be of type International Mobile Subscription Identity (IMSI, at most 15 digits), consisting of Mobile Country Code (MCC, 3 digits), Mobile Network Code (MNC, 2-3 digits), and Mobile Subscriber Identification Number (MSIN), but it can also have other formats, such as Network Specific Identifier (NSI), Global Line Identifier (GLI), and Global Cable Identifier (GCI). For IMSI-type SUPI, the subscription identifier part of IMSI (i.e., MSIN) is used as the scheme input for encryption, while MCC and MNC, comprising the SUCI field Home Network Identifier, as well as other SUCI fields are sent in clear [33, 31]. The details about the SUCI fields can be found in TS 23.003 clause 2.2B [31].

Figure 5.3 shows the SUCI structure with the scheme output for the null-scheme and the ECIES profiles. The scheme output for the ECIES profiles consists of the 256-bit (profile A) or 264-bit (profile B) ECC ephemeral public key, the encrypted scheme input, and the 64-bit MAC [33]. The largest allowed size

of the scheme output for proprietary protection schemes is a total of 3000 bytes and the input size, chosen to allow quantum-resistant protection schemes to be introduced in the future. SUCIs larger than the scheme output size limit shall not be sent by the UE and may be rejected by the network.

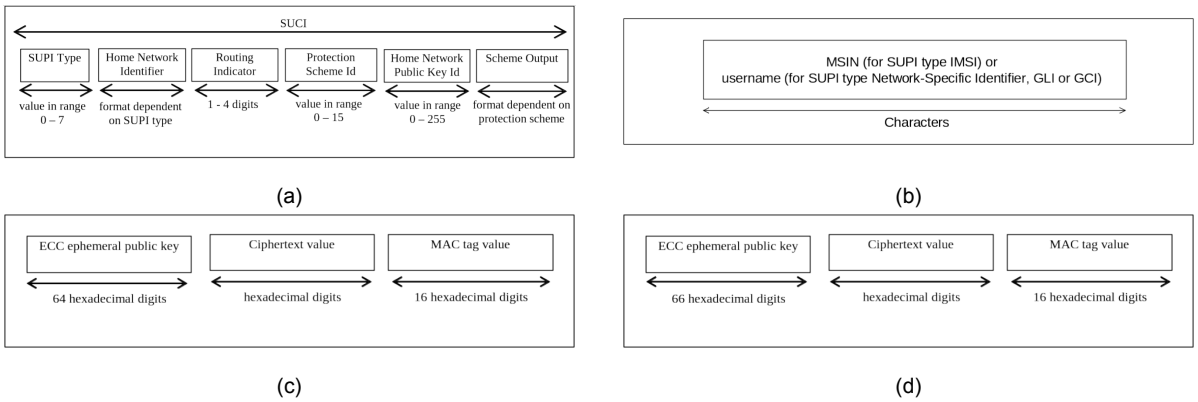



**Figure 5.3:** The structure of SUCI, as defined in TS 23.003 [31]: (a) the SUCI fields, (b) the scheme output for the null-scheme, (c) the scheme output for the ECIES profile A, and (d) the scheme output for the ECIES profile B.

The SUPI encryption and decryption process, as performed by the UE and SIDF, respectively, is shown in Figure 5.4. To protect against replay attacks, the UE computes a fresh SUCI every time [33]. It uses the provisioned home network public key and a freshly generated ECC ephemeral public and private key pair based on the ECIES parameters provided by the home network. To deconceal a SUCI, the home network uses its private key and the received UE ephemeral public key. Note that the home network does not have to generate a fresh ephemeral key pair for every decryption, and TS 33.501 does not specify how often a new key pair is created and how the key is supplied to the UE.

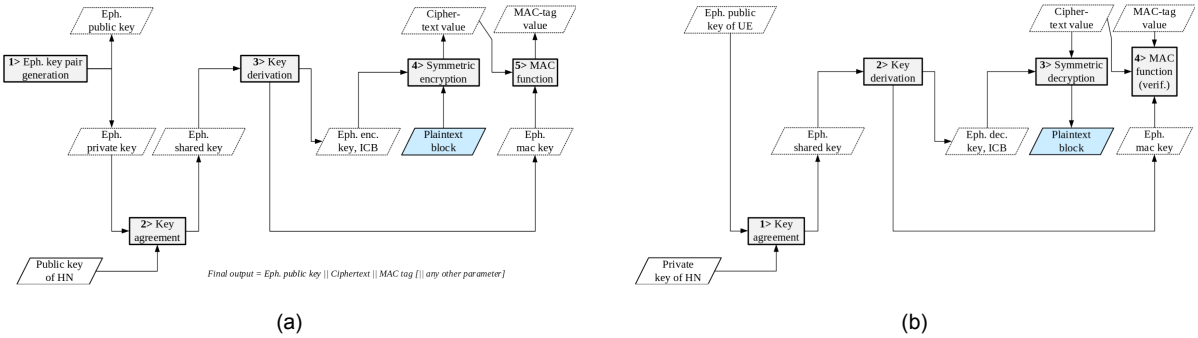



**Figure 5.4:** The use of ECIES for SUPI concealment and the corresponding processing, as defined in TS 33.501 [33]: (a) at the UE for encryption and (b) at the home network (SIDF) for decryption.

Table 5.10 shows the cryptographic profiling for the ECIES profiles A and B. The profiling differs only in the elliptic curves and their associated parameters. Both curves are NIST-approved [79, 110], and other parameters, namely AES-128 CTR and SHA-256/HMAC-SHA-256 are also approved by NIST [132, 286, 302, 289, 385], as discussed earlier (see section 5.2). On the other hand, these parameters are not CNSA 1.0-approved, which requires the secp384r1 curve, the SHA-384 hash function, and AES with 256-bit keys [305]. Furthermore, truncating the output of a cryptographic hash function (to 64 bits for the ECIES profiles) reduces its expected collision resistance strength to half the truncated output length (32 bits), reduces the expected preimage resistance to the truncated output length (64 bits), and also reduces the expected second preimage resistance strength, which sometimes depends on the length of the message [127]. It could be that truncating the MAC is done for performance reasons and that 3GPP has considered the potential risks.

**Table 5.10:** ECIES cryptographic profiles for SUCI, based on 3GPP TS 33.501 [33] Annex C.3.4; terminology and processing are specified in SECG version 2 [99].

| | **Profile A** | **Profile B** |
|---|---|---|
| **Elliptic curve** | **Curve25519** (RFC 7748 [227])<br>EC Diffie-Hellman primitive: X25519 (RFC 7748 [227])<br>Point compression: N/A<br>KDF: ANSI-X9.63-KDF [99] | **secp256r1** (SECG SEC 2 [100])<br>EC Diffie-Hellman primitive: Elliptic Curve Cofactor Diffie-Hellman Primitive [99]<br>Point compression: True<br>KDF: ANSI-X9.63-KDF [99] |
| **Encryption** | **AES–128 in CTR mode**<br>Key length: 128 bits<br>ICB length: 128 bits | **AES–128 in CTR mode**<br>Key length: 128 bits<br>ICB length: 128 bits |
| **Hash** | **SHA-256** | **SHA-256** |
| **MAC** | **HMAC-SHA-256**<br>MAC key length: 256 bits<br>MAC length: 64 bits<br>MAC tag: 64 most significant bits of the HMAC function output | **HMAC–SHA-256**<br>MAC key length: 256 bits<br>MAC length: 64 bits<br>MAC tag: 64 most significant bits of the HMAC function output |
| **Shared info** | $\text{SharedInfo}_1$: $\bar{R}$ *(ephemeral public key byte string – SECG SEC 1 [99] section 5.1.3)*<br>$\text{SharedInfo}_2$: **empty string** | $\text{SharedInfo}_1$: $\bar{R}$ *(ephemeral public key byte string – SECG SEC 1 [99] section 5.1.3)*<br>$\text{SharedInfo}_2$: **empty string** |
| **Backwards compatibility mode** | **False**<br>*(thus, incompatible with SECG version 1)* | **False**<br>*(thus, incompatible with SECG version 1)* |

When it comes to the performance of the used elliptic curves, then Curve25519 is very efficient and has extremely high speeds, absence of time variability, short private and public keys, and short code [87], making it a good choice for resource-constrained environments [378]. On the other hand, secp256r1 (NIST P-256), despite being widely adopted, shows slower execution times and has increased computational overhead due to larger key size and more complex arithmetic operations [378]. Cryptographic operations with NIST curves can have several times slower performance than those with Curve25519 [378], and more than a hundred times slower than encryption using AES [199]. Furthermore, the NIST curves have larger memory footprints than Curve25519 [378]. It is not clear to what extent a SUCI-based DoS attack against a UDM (similar to the attacks described by Hammouchi [183] and Hu et al. [192]) can create an amplification and stress the UDM, and is left for future work.

Finally, we note that a proof-of-concept SUCI-Catcher attack has been implemented by Chlosta et al. [111] in a 5G SA network, exploiting the AKA-linkability issue. By capturing encrypted SUCIs and linking encrypted identities between sessions, it is possible to answer whether the user X is present in the network. Even though the attack scales worse than IMSI-Catchers in pre-5G networks, especially with mitigation measures like rate-limiting in place, it allows targeted tracking of specific users. The authors propose mitigations such as linkability prevention, abnormal behaviour detection by networks and UEs, and throttling at both sides to reduce the scalability of the attack.

## 5.5. Analysis of the literature attacks on 5G terrestrial networks

Having reviewed the 3GPP security measures for the studied non-SBI interfaces, we now proceed with the analysis of the previously discovered attacks on 5G TN. We focus primarily on the weaknesses found in the 3GPP standards (including earlier releases), leaving aside generic threats that are clearly mitigated by the 3GPP security mechanisms, threats from the 3GPP SCAS documents [35, 34, 4, 6, 3, 5]), and vulnerabilities due to obvious implementation mistakes. Moreover, we focus mainly on the AS/NAS security and the radio interface, where in some situations the UE does not (yet) have a security context. We do not cover NDS/IP networks, as they are secured using traditional Internet security solutions like IPsec, IKEv2, and (D)TLS, and are fully controlled by the network operator. While some attacks [179, 246] have been proposed on the NDS/IP network interfaces, they can be mitigated if the appropriate security measures are in place.

For each of the studied attacks, we specify the weakness (the root cause) and the category (e.g. the layer it exploits, and whether it applies before or after RRC/NAS authentication); we summarize the attack steps and include our analysis of the impact and/or feasibility based on our knowledge (i.e.

without performing lab experiments). While some attacks appear to be theoretical or too optimistic, we still include them, as they can indicate likely places for implementation errors. Table B.1 in Appendix B lists 30 attacks on 5G networks that we found in the literature, while Table 5.11 lists six attacks that we consider the most interesting. These selected attacks will be further analysed in the NTN context in section 6.3, and the feasibility and practical impact of one of these attacks ("DoS by gNB resource depletion") will be demonstrated in chapter 7.

**Table 5.11:** Summary and analysis of the selected attacks on 5G networks from the literature.

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS using NAS Registration Reject** [192, 187, 246] *Root cause: By design, NAS Registration Reject is accepted by the UE without authentication before security can be activated.* | AS/NAS security *(NAS layer, pre-auth.)* | NAS *Registration Reject* message is sent unprotected before security activation, which can be exploited by an attacker, using a rogue gNB, by impersonating the AMF. Specifically, when a UE attempts to connect to the rogue gNB after the cell (re-)selection procedure (with the rogue gNB having higher signal strength than that of a legitimate gNB), the attacker responds with a *Registration Reject*, denying the service and triggering a new registration procedure. In addition, if the gNB sets the 5GMM cause to *"Illegal UE"*, then the UE is forced to update the connectivity status to *"Roaming Not Allowed"* and will not retry the registration procedure until it is rebooted, or its SIM card is reinstalled. This can permanently disconnect the communication interface (e.g. for mobile IoT devices). | The attack exploits the implicit trust between the UE and the (core) network before (NAS) security is activated and allows blocking cell access for the victim UE (which is harder to detect than a with a signal jamming). Depending on the parameters in the *Registration Reject*, the attacker can keep the UE being denied of the service from the network. Possible mitigation: Earlier (core) network authentication (e.g. using certificates). |
| **DoS using RRCReject** [194] *Root cause: By design, the UE accepts RRCReject messages without authentication (prior to AS security activation, but also after that, since this message can be sent in SRB0, i.e. using the common control channel (CCCH), in RRC_INACTIVE state).* | AS/NAS security *(RRC layer, pre-auth.)* | The victim UE connects to the fake base station with an *RRCSetupRequest*. The latter replies with an unauthenticated *RRCReject*, which the UE accepts, since it is in RRC_IDLE state (i.e. not connected). As a result, the UE is denied of the connection. In addition, the attacker can set the *"mobility backoff timer"* in *RRCReject* for the UE to wait in the idle mode before reconnecting to the gNB. By repeatedly sending such unauthenticated *RRCReject* messages, the attacker can keep the UE in this connection setup loop and prevent it from getting services from the network. | The attack exploits the implicit trust between the UE and the gNB before (AS) security is activated and, similarly to the NAS *Registration Reject* attack, allows blocking cell access for the victim UE. Depending on the parameters in the *RRCReject*, the attacker can keep the UE being denied of the service from the network. In addition, by setting the wait time to its maximum value (16 seconds), the attacker can keep the UE out of service for longer. Possible mitigation: Earlier gNB authentication (e.g. using certificates). |
| **DoS by gNB resource depletion** [215, 192, 187, 246] *Root cause: By design, the RRC connection setup procedure does not authenticate the sender.* | AS/NAS security *(RRC layer, pre-auth.)* | The RRC connection setup procedure does not hide the message content and does not authenticate the sender (the authentication procedure is left to the AMF). Therefore, during the initial registration, a rogue UE can establish an RRC connection. Due to an invalid authentication response, the authentication procedure fails and the UE is not able to connect to the core network. While the UE cannot keep this connection for long, it can still connect to the operator's gNB. Thus, an attacker can repeatedly perform the Random Access procedure, ignoring the NAS *Authentication Request* from the AMF, to exhaust the capacity of the active RRC connections in the gNB. This can prevent legitimate subscribers from connecting to the base station and the core network. | Unless the implementation has a fixed limit on allowed RRC connections (other than the allocated memory), it may be infeasible to exhaust the capacity of active connections. However, establishing many fake connections can have an impact on the gNB resources, depending on how fast new contexts are created, and the old contexts are released (which depends on the implementation). Possible mitigation: proper release of stale RRC contexts; rate limiting of the total failed registration attempts; reducing the inactivity timer, so that fake RRC connections expire earlier; sender authentication. |

*Continued on the next page*

**Table 5.11** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS by spoofing uplink grants** [245] Root cause: *By design, DCI messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | An attacker can spoof the UL Downlink Control Information (DCI), i.e. uplink grants, to perform a fake allocation of UL resources. By injecting spoofed UL grants to the connected UEs in every time slot, the attacker can force multiple benign UEs to constantly transmit on the same UL resources (chosen by the attacker) even when they do not have any pending data to send (due to required padding to fill all allocated resources). Furthermore, modifying the *Transmission Power Control* field in the same DCI will instruct the UEs to transmit at the maximum power. This effectively creates a jammer for legitimate UEs, disrupting their communication and decreasing the throughput, while possibly also draining the battery of the jamming UEs. | The attack can create a heavy congestion in the cell if many UEs start transmitting at the same time at a high power, making the cell unusable in the worst case. In addition, such a jamming is not easily detectable, since it comes from many legitimate UEs and not from a single source (as in traditional signal jamming). Possible mitigation: Authentication (possibly with encryption) of the lower layers (DCI messages). |
| **DoS by blocking initial cell access** [245] Root cause: *By design, the RA procedure is not protected. In addition, SIB and PO messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | The Random Access (RA) procedure is performed by the UE during network attachment. The RA parameters are broadcast by the gNB in the unprotected *System Information Block (SIB)* message, which the attacker can modify to change the RA configuration at the UE, e.g.:<br>• Minimize the *RA Response (RAR)* reception window (*ra-ResponseWindowSize*) to make the RA fail due to *RAR* timer expiration;<br>• Maximize the number of retries after RA failure (*preambleTransMax*) to increase congestion;<br>• Maximize the power ramp-up after each RA failure (*powerRampingStep*) to increase battery usage.<br>As a result, all UEs connecting to the network will keep failing the RA procedure and will not be able to attach to the cell. In order to target already connected UEs (which do not monitor the *SIB* messages), the attacker can send them a *SIB* paging, asking to monitor the *SIB* for updates. Then, the attacker can force the target UE(s) to run the RA procedure by injecting a special DCI called *PDCCH Order (PO)*. This message instructs a connected UE to start a RA procedure to re-establish synchronization in the UL (e.g. updating the *Timing Advance (TA)* value). Such a stealthy way of triggering a RA procedure allows draining resources (due to collisions in the limited RA resources) or disconnecting the users to perform further localization or traffic analysis attacks. | Manipulating RA parameters in broadcast *SIB* messages can create a high congestion if many UEs are present in the cell (either already connected or trying to connect). In the worst case, this attack can prevent all UEs in the cell from connecting to the gNB and the core network and getting the desired services. Furthermore, the attack is harder to detect than a traditional signal jamming, since the *SIB* messages could also come from a legitimate gNB (there is no authentication). Possible mitigation: Earlier gNB authentication (e.g. using certificates); authentication (possibly with encryption) of the lower layers (*SIB* messages, RA procedure, *PO* messages). |
| **Location tracking with a SUCI-Catcher** [111, 83, 192] Root cause: *AKA linkability in the design: the target UE responds differently to the NAS Authentication Request than a regular UE (accept and reject, respectively).* | AS/NAS security *(NAS layer, pre-auth.)* ECIES | An attacker obtains the victim's SUCI, e.g. using a fake base station (discovery phase), asks the network for an authentication challenge associated with the wanted subscriber's identity, and forwards the *Authentication Request* to all connected UEs (linking SUCIs phase). Only the UE accepting the *Authentication Request* (or responding with an *Authentication Failure* with the cause *"Synch Failure"*) is the searched-for-subscriber (other UEs send an *Authentication Failure* with the cause *"MAC Failure"*). Thus, when an unknown UE connects to the fake cell, a SUCI-Catcher can check if it belongs to the wanted subscriber (who can even be a national leader or ambassador), which allows verifying if a person of interest is in the current location or not. | The attack allows verifying if the person of interest is present in the cell by capturing SUCIs and linking encrypted identities between the sessions. While mitigation measures such as rate-limiting or throttling of the user authentication can reduce the scalability of the attack, it is still possible to perform targeted tracking of specific victims. Possible mitigation: Earlier (core) network authentication (e.g. using certificates); throttling or rate-limiting of user authentication; UE-based anomaly detection. |

For three of the selected attacks in Table 5.11 (the two DoS attacks using NAS and RRC reject messages and the SUCI-Catcher attack), as well as for many of the attacks in Appendix B, the attacker

can make use of a fake/false base station (FBS) [193, 347, 195, 357] to force the victim UE to connect to the attacker-controlled gNB. The rogue base station sends initial broadcast messages, i.e. System Information Blocks SIB1 and SIB2, with a higher signal strength than a legitimate gNB, which lures the UE and allows for further attacks [194, 195]. These attacks do not aim at eavesdropping or changing the traffic between the CN and the UE, which would fail due to the AKA procedure and security protections like ciphering and integrity protection for RRC/NAS, and IPsec and DTLS for NDS/IP networks. Instead, they exploit unauthenticated or unencrypted RRC messages between the UE and gNB(-CU), and NAS messages between the UE and AMF (forwarded by the gNB without processing).

The reason such attacks are possible is that the gNB is implicitly trusted by the UE, and the authentication procedure takes place later between the UE and the AMF, after the RRC connection has already been established and the UE identity has been verified by the UDM. In addition, some RRC and NAS messages are by design sent before AS/NAS security can be established and therefore lack confidentiality protection and authentication (see Table 5.9 in section 5.3). Since a rogue gNB can overshadow the signal from a legitimate gNB [244, 409, 145], the UE does not know if these messages come from a real or fake base station. Therefore, it is important to apply mechanisms for detecting rogue gNBs and protecting RRC/NAS messages sent before security activation.

Currently, 3GPP TS 33.501 [33] Annex E includes a general informative detection framework for UE-assisted network-based FBS detection. Depending on the measurement configuration given by the network, the UE in RRC_CONNECTED state sends to the network the measurement reports including received-signal strength, location information, cell identifier, or frequency information. These are used to detect FBSs or SUPI/5G-GUTI catchers and mitigate the attacks they perform. In addition, a separate technical report TR 33.809 [48] studies potential threats and privacy issues related to FBS scenarios based on the attacks identified in the literature [194, 112, 347, 409], and proposes possible solutions to mitigate the corresponding risks. The document aims to improve the FSB detection framework in future 3GPP releases. For instance, some solutions propose to enrich UE measurement reports, e.g. by sending additional information about camped and neighbouring cells, such as hashes of MIBs and SIBs and information about reject messages that the UE has received earlier, to help in detection of DoS attempts. Other solutions rely on public key based digital signatures, symmetric key based MACs, or message hash consistency checks without a digital signature or a MAC.

Next to the 3GPP solutions, some mitigations for FBS and unprotected RRC/NAS messages have been proposed in academic works [195, 364, 415, 238, 126, 130, 125]. For example, Hussain et al. [195] suggested a PKI-based base station authentication mechanism during connection bootstrapping, providing integrity protection to MIB and SIB broadcast messages. Their solution uses a custom lightweight certificate encoding with only the relevant fields (such as identity, public key, and expiration time) to overcome the constraints on the packet size. Furthermore, it optimizes for the signature size and the signature generation time, while sacrificing on the signature verification time at the UE, which happens less frequently than the scheduled signature generation by the gNB. To raise the bar for replay/relay attacks, the mechanism adds a location-dependent parameter $\Delta t$, so that the message is only considered valid if it is received within this time ($\Delta t$) since the message generation.

To overcome the challenges of the certificate-based solution by Hussain et al. (e.g. communication and computation overhead, as well as long delay at the UE to verify signatures and certificate chains), Singla et al. [364] designed a hierarchical identity-based signature scheme based on Schnorr signatures [162] (Schnorr-HIBS). The authentication protocol they propose introduces a new entity to the AUSF, called core-Private Key Generator (core-PKG), which generates public-private key pairs for the AMF, which in turn generates the public-private key pairs for the gNBs under its control. As a result, the UE, with the knowledge of the master public key of the PKG, can verify the authenticity of the broadcast messages (most importantly, *SIB1*) received from the gNB in the cell that it tries to connect to.

Yu et al. [415] build on the work by Singla et al. to also protect individual RRC and NAS messages, next to authenticating the gNB. They design and analyse a two-level HIBS scheme, involving UE, gNB, AMF (second-level PKG), and UDM (root PKG). The solution consists of three main phases: initial setup (HIBS system parameters are generated at the PKG, and the public parameters are passed to the UE through secure out-of-band/in-band ways), key generation and distribution (PKG generates the secret key for the AMF, and the AMF generates the secret key for the gNB), and sign and verify (the UE can verify the authenticity of the NAS messages from the CN and the RRC messages from the gNB).

The two attacks at the lower layers from Table 5.11 (DoS by spoofing uplink grants and DoS by blocking initial cell access) exploit the lack of integrity and confidentiality protection in the layers below PDCP in the 5G NR protocol stack. The absence of authentication in the design makes these attacks difficult to detect, because the receiving end cannot verify if these messages come from a legitimate UE/gNB or from the attacker. Therefore, to mitigate these attacks, encryption and integrity protection should be extended to the lower layers of the radio stack [245], while other attacks relying on initial broadcast messages can be prevented with the base station authentication solutions discussed above.

Finally, DoS by gNB resource depletion exploits the lack of sender authentication in the RRC connection establishment procedure, which allows any UE to connect to the gNB and create a (fake) RRC context. Since introducing sender authentication to the lower layers can be a complex task, other mitigations also need to be considered. For example, rate limiting could be used to either block the direction where the fake connections are coming from or (temporarily) not accepting new RRC connections if there are too many failed registrations in the network (likely indicating an attack). This might not be desired, but it is better than having the entire gNB taken down. Otherwise, the inactivity timer could be adjusted to make the fake RRC connections expire quicker, which, however, risks removing legitimate RRC connections if they cannot be served due to the flooding. For further discussion on the practical impact and mitigations, see chapter 7.

## 5.6. Reflections

Having performed an extensive analysis of the security measures for the 10 chosen non-SBI interfaces, we could not find any new serious issues in the 3GPP standards defining these protection mechanisms. The security specifications we investigated mandate and recommend cryptographic algorithms that are currently considered secure enough to be used. The standards reference RFCs that are not obsoleted and do not leave space for vulnerable versions. Furthermore, 3GPP security profiles are updated at every release based on IETF standardization efforts, government requirements, and academic research to keep them up-to-date [250]. An example of such an update as part of Release 19 can be found in Appendix A. Below, we discuss some important reflection points.

One possible direction for improvement would be to further restrict the allowed versions for the used cryptographic algorithms. As seen in section 5.2, CNSA 1.0 profiling, intended to be an intermediate step towards migration to post-quantum cryptography, provides stricter profiling, both in terms of the number of allowed algorithms and their security parameters. While 3GPP and CNSA generally target different audiences, 3GPP can still, where possible, improve its allowed algorithm suite to further enhance security. For example, allowing only AEAD algorithms for IPsec and IKEv2 is one recommendation. Furthermore, restricting the allowed algorithms to the more secure versions required by CNSA 1.0 is a feasible step, as many of these algorithm versions are already allowed by 3GPP (i.e. marked as mandatory, recommended or optional). Compared to CNSA 2.0, which requires implementing new post-quantum cryptographic algorithms, using CNSA 1.0 as a guidance for 3GPP cryptographic profiling, especially for new systems and devices, should be possible in a relatively short term.

Another suggestion would be to mandate the confidentiality and authentication for the F1-U interface. According to TS 33.501 [33] (see Table 5.1 and Figure 5.1), confidentiality, integrity, and replay protection are only mandatory to use for the management traffic sent over F1, while the F1-U interface is only required to support confidentiality, integrity, and replay protection and shall be protected independently of F1-C. Such a requirement might come from the fact that F1-U traffic between gNB-DU and gNB-CU is already protected by PDCP. However, confidentiality and integrity protection of UP data on the Uu interface is also not mandated. Therefore, we believe that F1-U should be required to be confidentiality, integrity, and replay protected (e.g. using IPsec), similarly to F1-C.

### 5.6.1. Ambiguities in the standards

We believe that 3GPP documents should be more explicit about their intentions and avoid ambiguities (see subsection 5.2.4). Places that can be interpreted differently by different implementers can lead to interoperability problems among different implementations of the same system or protocol, and design uncertainties can even lead to vulnerabilities [236]. The freedom to choose to support unintended or weak cryptographic algorithms can open the system to downgrade attacks. Simply put, ambiguous language in standards leads to ambiguous implementation, which results in security flaws in proto-

cols [400]. Problems and usability issues with 3GPP technical specifications have been identified both for their consumers and producers [392]. Specification consumers find the documents difficult to read due to vague language, lack of background information, and decentralized nature of information, next to the complicated technical descriptions. The vague language is sometimes intentional to give telecommunication companies the freedom to introduce implementation differences in order to get a competitive advantage in the market. Unfortunately, this comes at the cost of making the specifications less clear.

Ambiguities have also been previously found in RFCs [236, 332], despite the existence of several special RFCs [352, 340, 135] providing guidance and instructions to RFC writers. One study has shown that ambiguous keywords "SHOULD" and "MAY" (as compared to unambiguous keywords MUST (NOT), SHALL (NOT), and REQUIRED) had the second-highest frequency across all analysed RFCs [236]. In addition, the RFCs related to the Session Initiation Protocol (SIP) relied the most on ambiguous keywords and also had the most implementation flaws, as follows from the SIP-related CVEs. This indicates that some degree of correlation may be present between the ambiguity level of RFCs and the following security flaws in implementations. The most effective way to lower the frequency of network security incidents is by fixing the RFCs, removing the freedom for sloppy interpretations, and ensuring that implementers have no other option but to write exploit-robust implementations, regardless of their knowledge and expertise in the security domain [332].

When analysing 3GPP TS 33.210 (version 19.0.0) [17], we have found an inconsistency in the document. For the TLS 1.2 profiling, while the support for finite field DH has been removed (*"Finite field Diffie-Hellman (i.e. DHE) shall not be supported"*, see Appendix A), **TLS_DHE_RSA_WITH_AES_128_GCM_SHA256** cipher suite was still present in the list of cipher suites that are mandatory to support and recommended to use, even though the referenced RFC for it has been removed (i.e. made "void"). We have contacted our colleagues at Ericsson, and they have confirmed that it was indeed a mistake, which could be brought as a contribution in the next 3GPP meeting, and that 3GPP was aware of it. While this is not a serious mistake and the cipher suite is not known to be insecure, it shows that 3GPP standards can contain mistakes and should ideally be more carefully reviewed to spot such inconsistencies.

### 5.6.2. Crypto agility

The next point we want to emphasize is that new systems and devices should not use cryptographic algorithms that are expected to be deprecated in the future, even if they are acceptable for use now. For instance, on January 1, 2031, NIST plans to transition from the 112-bit security strength provided by current public-key schemes to 128-bit security strength, as an intermediate transition to facilitate the transitioning to the post-quantum cryptography [76, 77]. Therefore, as discussed earlier (see section 5.2), after December 31, 2030, the usage of multiple cryptographic algorithms will be deprecated in favour of more secure alternatives. In particular:

- applying cryptographic protection using SHA-1 (for non-digital signature applications, such as MACs) and hash functions with 224-bit output length will be disallowed and replaced with the more secure SHA-2 and SHA-3 hash function families;
- key-agreement transactions with MODP-2048 [219] and ffdhe2048 [166] safe-prime groups (providing 112-bit security strength [79]) will be deprecated and replaced with MODP and ffdhe safe-prime groups with 3072, 4096, 6144, or 8192 bits (providing at least 128-bit security strength [79]);
- key-agreement transactions using elliptic curves less than 256 bits, such as P-224 curve [110] (providing less than 128-bit security strength [79]) will be deprecated and replaced with the curves at least 256 bits (providing at least 128-bit security strength [79]);
- signature generation using RSA with the modulus (key) lengths smaller than 3072 but larger than 2048 bits (providing at least 112-bit but less than 128-bit security strength [76]) will be deprecated and replaced with modulus lengths at least 3072 bits (providing at least 128-bit security strength [76]);
- signature generation using ECDSA curves with less than 256 bits (providing less than 128-bit security strength [110]) will be deprecated and replaced with the curves at least 256 bits (providing at least 128-bit security strength [110]).

This decision affects certain cryptographic profiles for NDS/IP networks. For example, IPsec and IKEv2 profiles still have AUTH_HMAC_SHA1_96 authentication transform at the "MUST" level, and according to the IKEv2 profile, 2048-bit MODP group and RSA digital signature key lengths of 2048 bits are still

mandatory to support. While these algorithms are secure enough at the moment, new systems and devices should not rely on them, and instead use the algorithms with higher security guarantees. This is because a device that is not designed to transition to a more secure algorithm version (e.g. to RSA with a larger key/modulus size) during its lifetime will have to be replaced [77]. Since many devices have a long lifespan, design for such transitions from the start is usually more cost-effective.

Transitioning to new cryptographic algorithms creates many challenges, such as backward compatibility, interoperability issues, and disruption of operation, which cause the transition period to be extremely long, often taking longer than was initially planned [77]. For example, while AES was standardized in 2001 [277] in order to replace Triple-DES [74], the latter was disallowed only in January 2024. Similarly, despite the discovered collision search attacks on SHA-1 in 2005 [396] and the subsequent deprecation of SHA-1 for digital signature generation in 2011 [286], many existing secure protocols relied on this hash algorithm for signature generation in entity authentication, which created problems for interoperability and backward compatibility [77]. As a result, a complete shift away from any usage of SHA-1 is planned to take place only by the end of 2030 [76].

This illustrates the need for cryptographic (crypto) agility, i.e. the ability to adapt and replace cryptographic algorithms used in protocols, applications, software, hardware, and infrastructures without having to interrupt the flow of a running system, with the aim to achieve resilience [77]. Crypto agility is a future-proofing strategy to handle changes, and it makes the transitioning between cryptographic algorithms much easier. It means that introducing new algorithms to a system, an application, or a protocol and preventing the use of weak algorithms does not require major changes and does not break interoperability. Without crypto agility and the ability to perform timely migrations, the support for a weak algorithm has to be allowed longer than necessary for the sake of backward compatibility.

In order to achieve cryptographic agility, collaboration between cryptographers, implementers, security policymakers, and IT administrators is needed to manage the risks associated with cryptographic data protection [77]. Security analysis and assessment of protocols, applications, and system configurations must also specify transitioning mechanisms. SDOs must introduce new algorithms and deprecate or disallow the weak ones in a timely manner, before the current algorithms reach their breaking point. Implementations of security protocols need to be modular to facilitate insertion of new algorithms or cipher suites and removal of the old ones. Moreover, a tradeoff has to be considered between relying on cryptographic algorithms in hardware, which provides performance, portability, and private key protection, or in software, which facilitates the provisioning of multiple algorithms.

SDOs must also revise the list of mandatory-to-implement cryptographic algorithms and cipher suites (reflecting the state-of-the-art cryptography and ensuring basic interoperability) without changing the base security protocol specifications [77]. For example, NIST increases agility by not mandating support for any of the allowed TLS cipher suites in order to give freedom to administrators to consider the needs of their systems, and to allow them to instantly disable cipher suites as soon as attacks are discovered while still maintaining compliance with the standards [253]. Furthermore, crypto agility is increased when a security protocol supports multiple key-establishment methods [77]. However, if a protocol offers negotiation and selection of cryptographic algorithms, then it must do so in an integrity-protected way to prevent downgrade attacks. This requires transition mechanisms to consider which algorithm(s) shall be used to provide integrity protection of algorithm negotiation.

### 5.6.3. Discrepancies between the standards and deployments

The level of security ensured by the 5G standards does not matter if real 5G deployments do not implement the corresponding security mechanisms. Unfortunately, security improvements introduced in 3GPP specifications for 5G do not always make their way to the real 5G networks [313, 228, 138, 184, 256]. The optional level of many security provisions gives network operators the choice to ignore their deployment. Furthermore, even some mandatory measures might be dropped for performance, cost, compatibility, and other practical considerations. Indeed, measurements of real commercial 5G networks suggest that 3GPP security enhancements for UP data protection, user identity protection, refreshing of temporal subscriber identifiers, and initial NAS message protection are not fully deployed, exposing subscribers to threats like leakage of user data, location tracking, breach of identity privacy, and DoS attacks [313, 228]. This illustrates the gap between the 3GPP security specifications for 5G networks and real-world commercial 5G deployments.

Another study revealed the noncompliance of Mobile Network Operators (MNOs) with 3GPP specifications for the cryptographic profiles [165]. Many MNOs still supported and announced DH groups less than 2048 bits, which are prohibited by the standards: a great majority supported the 1024-bit MODP group, 40% supported the 768-bit MODP group, and only one private operator supported EC groups. This is despite the previous estimations that breaking 768-bit prime is feasible for an academic team, and breaking 1024-bit prime is plausible for state-level actors [61]. At least 41% of the MNOs accepted weak client (UE) preferences over stronger supported groups, and only 42% requested an upgrade to a stronger key exchange method if a common stronger group was available [165]. Mediatek devices allowed a downgrade to any DH group (e.g. 768-bit MODP), including those that were not proposed by the client in the handshake. On the client side, there was also a large share of deprecated IKEv2 algorithms among all operator-specific settings, with the 1024-bit DH group being the most popular. Finally, at least 13 operators on three continents, serving 140 million customers, used the same global set of 10 static private keys. The number of vulnerable operators might be even higher, as many use geoblocking at Voice over Wi-Fi (VoWiFi) for customers staying abroad [164].

While implementers and administrators might want to enhance security by selecting the strongest supported algorithm during the negotiation process, they also want to maintain interoperability [77]. This limits their actions, because implementers are often not willing to remove deprecated algorithms from the software, and administrators are not willing to disable them. Unfortunately, 3GPP does not have a defined depreciation path for weak cryptographic algorithms: removing them from the standards does not actually remove them from the affected devices, and if the target device (silently) supports weak algorithms, then a downgrade attack can be performed [165]. Therefore, it is important that 3GPP defines an upgrade timeline for the minimum supported security parameters (e.g. key length). Operator and device manufacturers must remove unsupported cryptographic algorithms not only from the handshake advertisement, but also from the code base. It is also better to use client autoconfiguration mechanisms instead of irregularly updated preloaded configurations. Finally, UEs can detect intra-operator key reusage using mechanisms such as local key freshness tests.

### 5.6.4. Quantum threat

In the last decades, extensive research has been done into quantum computing [152, 314] and quantum computers - machines that exploit the phenomena of quantum mechanics and rely on qubits or quantum bits [107, 312]. Such machines can solve mathematical problems that are difficult for classical computers and perform certain algorithms exponentially faster. While increases in computational power are very desirable for some applications, such as optimization and search problems, it is definitely not desirable for cryptography which relies on the computational complexity of certain mathematical operations to protect information in computer systems and secure communications on the Internet [188].

A cryptographically relevant quantum computer (CRQC) is able to attack real-world cryptosystems [312]. It can undermine the widely deployed public-key infrastructures (PKI) which rely on mathematical problems believed to be practically unsolvable for conventional computers [270]. For example, the RSA integer factorization and ECC discrete log problem can be broken using Shor's algorithm [362] within hours (see Table 5.12). Furthermore, Grover's quantum mechanical algorithm [173] can search through a solution space of $2^n$ values in about $2^{\frac{n}{2}}$ steps, (i.e. $O(\sqrt{N})$ instead of $O(N)$), which would also reduce the security of symmetric cryptography (e.g. AES with 128-bit keys would provide the security strength equivalent to only 64 bits for current non-quantum computers, as seen in Table 5.12). As a result, security of several NIST-approved public-key cryptosystems, such as digital signature schemes, key exchanges using (EC)DH and Menezes-Qu-Vanstone (MQV), and key agreements and key transport using RSA, will be threatened by large-scale quantum computers [76]. This would be disastrous for many real-world systems, either due to direct attacks or by disrupting trust in them [270].

**Table 5.12:** Estimates of quantum resilience for currently deployed cryptosystems (integer factorization cryptography, elliptic curve cryptography, finite field cryptography, symmetric cryptography, hash functions), based on [188, 107, 72, 80, 284, 286]

| Cryptosystem | Category | Key size (bits) | Security (bits) | Attack | Time to break | Impact |
|---|---|---|---|---|---|---|
| **IFC** *(RSA)* | Public key *(signatures, key exchange)* | 1024<br>2048<br>3072<br>4096<br>7680 | $\leq$80<br>112<br>128<br>152<br>192 | Shor's algorithm [362] | 3.58 hours<br>28.63 hours<br>N/A<br>229 hours<br>N/A | No longer secure |
| **ECC** *(ECDSA, ECDH)* | Public key *(signatures, key exchange)* | 224 *(P-224)*<br>256 *(P-256)*<br>384 *(P-384)*<br>521 *(P-521)* | 112<br>128<br>192<br>256 | Shor's algorithm [362] | N/A<br>10.5 hours<br>37.67 hours<br>55 hours | No longer secure |
| **FFC** *(DSA, DH, MQV)* | Public key *(signatures, key exchange)* | (1024,160)<br>(2048,224)<br>(3072,256)<br>(7680,384) | $\leq$80<br>112<br>128<br>192 | Shor's algorithm [362] | N/A | No longer secure |
| **Symmetric cryptography** *(AES)* | Symmetric key | 128<br>192<br>256 | 128<br>192<br>256 | Grover's algorithm [173] | $2^{64}$ time *($2.61 \cdot 10^{12}$ years)*<br>$2^{96}$ time *($1.97 \cdot 10^{22}$ years)*<br>$2^{128}$ time *($2.29 \cdot 10^{32}$ years)*<br>*(for AES-GCM)* | Larger key sizes needed |
| **Hash functions** *(SHA-2, SHA-3)* | Hashing *(signatures; HMAC, KMAC, key derivation functions, random bit generation)* | N/A | collision,preimage<br>112,224 *(for SHA(3)-224)*<br>128,256 *(for SHA(3)-256)*<br>192,384 *(for SHA(3)-384)*<br>256,512 *(for SHA(3)-512)* | Grover's algorithm [173] | $1.8 \cdot 10^4$ years *(for SHA-256)* | Larger output needed |

While small examples of quantum computers have already been built, it is not known when a CSQCs will be available [312]. Whether it is still possible to delay taking action depends on three parameters [269]:

- **Security shelf life**, or how long the cryptographic keys need to stay secure; generally depends on a personal, business, or policy decision (e.g. 0 years for just real-time security requirements; a certain number of years to protect personal health data, trade secrets, national security information etc.)
- **Migration time**, or how long it takes to deploy quantum-resistant mechanisms; it can be 0 years if the transitioning only requires an auto-update (e.g. switching from 128-bit AES keys to 256-bit keys), but it can also be many years if the transitioning involves a new public-key algorithm, which needs to be tested and adapted to a specific environment, and a complicated standardization process
- **Collapse time**, or how long it takes before a (cryptographically relevant) quantum computer (or another method) breaks the currently deployed public-key cryptosystems

If **security shelf life** $+$ **migration time** $>$ **collapse time**, then it signals a serious problem now, as the data secured by quantum-unsafe methods at the end of the migration period will not stay protected for the required amount of time once the quantum threat becomes the reality [269, 270, 271]. Organizations need to evaluate required security shelf life and collapse time. The difference (collapse time $-$ security shelf life) shows the maximum available migration time they have for a safe transitioning.

Despite the fact that building a CRQC is an extremely challenging task, expert opinions generally accept that a CRQC will be developed sooner or later, as there are no known specific fundamental obstacles and because there has been a stable (and sometimes even fast) progress [271]. Even a "pessimistic" interpretation of the surveyed experts' responses leads to a $\sim$19% average likelihood estimate that a disruptive quantum threat becomes the reality within the next 10 years. Depending on the security needs and risk tolerance level of companies and institutions, it means that many of them might, without even knowing it, already be facing an unacceptable risk level demanding immediate actions. Attackers can already intercept and collect encrypted data to decrypt it later with a CRQC (an attack called

"harvest now, decrypt later"). Considering that the deployment of our modern public key cryptography infrastructure has taken almost 20 years, it means that whether or not we can precisely estimate the arrival time of a CRQC, we must start now to prepare our systems to resist the quantum threat [107].

Transitioning from the current widely deployed cryptosystems to their secure quantum-resistant counterparts will require considerable efforts in order to ensure that it is done in a smooth and secure way [107]. In general, there are two complementary solution families that can be employed [269, 107, 304]:

- **Post-quantum cryptography (PQC)** (or quantum-resistant cryptography) uses conventional cryptographic algorithms that are based on (possibly very old) mathematical problems thought to be secure against both quantum and classical attacks, and are able to interoperate with existing protocols and networks. While PQC solutions can work on traditional hardware, the computational security is still based on the hypothesized difficulty of some problem.
- **Quantum cryptography** (or quantum-key distribution) relies on the counterintuitive properties of quantum mechanics to set up a secure communication channel (i.e. establish symmetric keys). It is also expected to resist against quantum attacks, but in a different way. While this solution does not rely on computational assumptions, it requires a quantum channel, or a means to transmit qubits between different locations. In the short run, such channels will be available over fairly short distances (from point to point), however in the long run, global quantum key distribution will be made possible with satellite quantum communication and quantum repeaters.

In 2016, NIST started a PQC project, involving an open collaboration with the public, which could submit their algorithms in a competition for new standards and evaluate other submissions [293, 292]. In August 2024, the institute released the first three finalized PQC FIPS standards, specifying quantum-resistant key establishment and digital signature schemes [278, 295]:

- **Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)** [291], derived from CRYSTALS-Kyber, is intended to be the main algorithm for general encryption.
- **Module-Lattice-Based Digital Signature Algorithm (ML-DSA)** [290], from CRYSTALS-Dilithium, is intended to be the main algorithm for securing digital signatures.
- **Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)** [303], from Sphincs+, is intended to be a backup algorithm for securing digital signatures if ML-DSA proves insecure.

The fourth PQC FIPS is being designed for a new algorithm called Fast-Fourier Transform (FFT) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), derived from FALCON [295]. NIST encourages system administrators to start migrating to the new standardized solutions without delay, as these are the primary methods, and any subsequent PQC standards would serve as backups to the three approved algorithms [295]. For instance, in March 2025, NIST selected another algorithm for standardization to expand its key-establishment portfolio: Hamming Quasi-Cyclic (HQC), or a KEM that is based on quasi-cyclic codes with no hidden trapdoor in the code [66, 300].

At the moment, NIST is designing a schedule for transitioning to the quantum-secure algorithms [76]. For symmetric key cryptosystems, doubling the key lengths can compensate for the quadratic speedup coming from the Grover's algorithm [107]. However, most post-quantum replacements for the current public key cryptosystems have much larger public keys and signatures, directly affecting the size of the certificates containing them, and larger key-encapsulation ciphertext [77]. This can challenge network capacity, increase the transmission time for messages carrying signatures or ciphertexts, and may require changing some Internet protocols, such as TLS or IKE [107]. For example, some difficulties arise when unencrypted IKEv2 messages exceed a certain number of bytes, meaning that ML-KEM with its larger public key cannot directly replace the current algorithms without introducing dramatic changes to this part of IKEv2 [312]. In the near future, a solution drafted within IETF [207] could be used, which first performs a smaller key establishment with the currently approved schemes, followed by a larger but encrypted key establishment with ML-KEM. Alternatively, an IKEv2 extension using PSKs [155] allows it to resist a CRQC. Such hybrid methods combine the well-tested traditional algorithms with the new quantum-resistant schemes, while research into PQC continues and implementations are being developed [77]. This emphasizes the importance of crypto agility for security protocol designers and implementers to ease the migration to the PQC algorithms [76, 77].

The problems and challenges discussed above directly affect 5G networks, which make use of PKI in many places. As seen in section 5.1, the studied non-SBI interfaces heavily rely on IPsec, IKEv2, and DTLS for confidentiality, integrity, and replay protection, as well as mutual certificate-based authentication. SUPI concealment is also done using quantum-unsafe ECC. Furthermore, NFs in 5GC use their own public-key certificates to authenticate, authorize, and secure transactions [113]. On the other hand, the symmetric 128-bit algorithms used for AS and NAS security (SNOW 3G, AES, and ZUC) are not believed to be seriously threatened by the Grover's algorithm [203]. Still, it is important to verify that these algorithms can perform well with their 256-bit versions in a 5G system [320].

3GPP is well-aware of the threats posed by CRQCs and has conducted a study on the support of 256-bit algorithms in a 5G system, in the form of TR 33.841 [55]. The study analyses the threats, possible countermeasures, and the timeline for introducing countermeasures, particularly the increased key sizes. In many cases, 256 bits of classical security can already be applied to UP traffic, e.g. using 256-bit block ciphers in IPsec and TLS traffic sent over NG-RAN. Algorithms for AS/NAS security can be updated to use 256-bit keys, however, more evaluation is needs to be done. The majority of asymmetric algorithms in a 5G system (e.g. for network domain security, identity privacy, and untrusted non-3GPP access) are not used as part of a 3GPP protocol but are used widely (e.g. IPsec and TLS). These algorithms should be updated to support quantum-safe alternatives when they are available, and potential challenges should be addressed (e.g. due to increased key and ciphertext sizes).

Considering that 5G mobile networks are critical infrastructure creating high economic and societal value, they must be protected against future quantum attacks [250]. In section 5.2, we presented a head-to-head comparison of the 3GPP cryptographic profiles for NDS/IP-networks with NSA's fully post-quantum CNSA 2.0 Suite. This can serve as a generic roadmap for transitioning to PQC. Another set of recommendations is given in [262] with a simple multiphase approach to transition to quantum-secure systems. Since 5G standards target very long-term deployment scenarios (well beyond 2030), it is important that quantum-resistant counterparts are included in the current specifications [212]. This is especially relevant in NTN deployments, which will be further discussed in chapter 6. 3GPP has been actively monitoring the standardization process by NIST and IETF and plans to introduce quantum-resilient algorithms in the next releases, so that the next generation of mobile networks, or 6G, is fully quantum-secure from the start [250].

# 6

# Security analysis of 5G non-terrestrial networks

In the previous chapter, we analysed the 3GPP security architecture for 5G terrestrial networks, focusing primarily on the non-SBI interfaces that are affected by non-terrestrial deployments. In this chapter, we build on top of our previous work and investigate the 3GPP security architecture for non-terrestrial networks (NTN). We map the identified security measures to the architectures of the chosen NTN deployment scenarios (Transparent payload, Full gNB on board, Split CU-DU, and UE-Satellite-UE communication) and compare them with each other. Next, we revisit the selected literature attacks from section 5.5 and discuss their potential impact in NTN deployments. Finally, we compare terrestrial and non-terrestrial networks from the perspective of security.

## 6.1. Security architecture of NTN scenarios

3GPP Release 17 introduced support of NTNs and at the time of writing, the standardized architecture assumes transparent (i.e. bent-pipe) payload [390]. While regenerative payload architectures have also been studied [37, 50], they have not been standardized yet. Similarly, the UE-Satellite-UE communication enhancement for NTNs is only discussed in a technical report (see 3GPP TR 23.700-29 [50]). In this section, we analyse the architecture of these NTN scenarios and compare them based on the advantages and disadvantages that each scenario has from the security perspective.

### 6.1.1. NTN scenario 1: Transparent payload

Satellite with a transparent payload is the most basic NTN scenario and does not require any modifications for security. The NTN payload transparently forwards the radio protocols from the UE to the NTN gateway (and vice versa) and does not perform any processing other than filtering, frequency conversion, and power amplification [390]. Since the satellite does not perform any decoding, no security measures have to be implemented on the satellite and no extra processing is involved. This makes meaningful resource depletion attacks more difficult to perform than with regenerative payloads. On the other hand, since lower layers (i.e. MAC, RLC) terminate in the gNB on the ground, the satellite has no way of detecting tampering or spoofing at these layers and has to forward malformed or malicious packets further. This can also be abused by more skilled attackers, who can communicate using such a satellite that blindly reflects packets, even the ones not matching the 3GPP specifications.

Figure 6.1 shows the security architecture of the NTN Transparent payload scenario. The exposed interface is only Uu (CP and UP) on both the service and feeder links, protected with AS ciphering and integrity protection using PDCP. While CP authentication is mandatory to use, CP confidentiality protection, as well as UP authentication and confidentiality protection, are not mandatory to use. In the NTN context, choosing not to use these protections allows attackers to eavesdrop the CP and UP data and tamper the UP data from a much larger geographical area than in TN. Thus, it is important that network operators understand this threat and apply the corresponding protection measures.

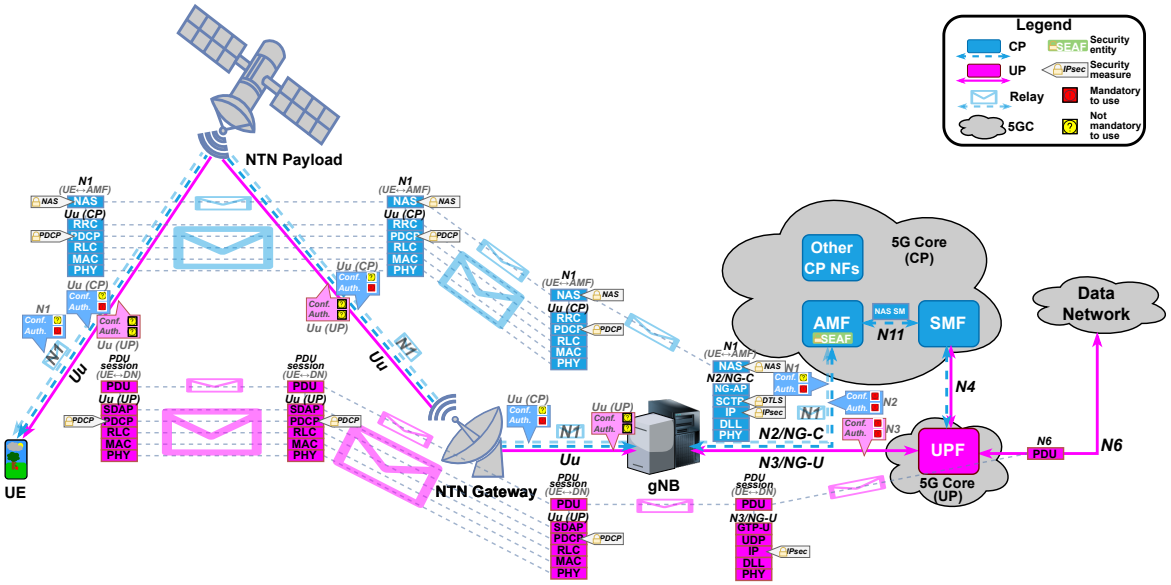



**Figure 6.1:** Security architecture of the NTN Transparent payload scenario (based on [37]).

### 6.1.2. NTN scenario 2: Full gNB on board

As the name indicates, in the Full gNB on board scenario the entire gNB radio stack is implemented in the NTN payload, which has an on-board processor capable of performing more advanced operations (e.g. modulation and demodulation, forward error correction) [390]. From the security perspective, the NTN payload has to implement all PDCP processing related to confidentiality and integrity protection, together with IPsec, IKEv2 and DTLS functionality. In addition, all UE security contexts, cryptographic material, IPsec SPDs and SADs and other security-related information needs to be present on board. In practice, this might be difficult to realize due to high processing constraints of a satellite, such as physical and weight/size constraints, which poses restrictions on the available computational and memory resources. To address these challenges, it may be tempting for network and/or satellite operators to sacrifice security and not use some protections. This will further increase the attack surface and allow for data tampering or eavesdropping, depending on which security measures are disabled.

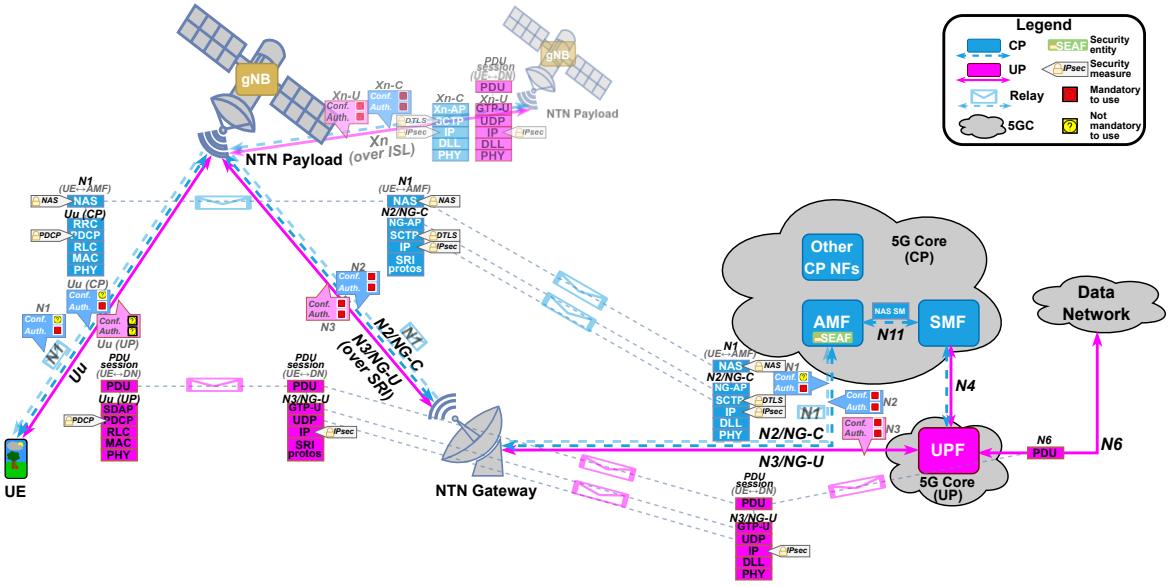



**Figure 6.2:** Security architecture of the NTN Full gNB on board scenario (based on [37]).

The security architecture of the NTN Full gNB on board scenario is shown in Figure 6.2. The exposed interfaces are Uu (CP and UP) on the service link and N2 (CP) and N3 (UP) on the feeder link. While the Uu interface has the same issues as for transparent payload (i.e. only CP authentication is mandatory to use), the feeder link protection is mandatory to use for both CP and UP. Since ensuring secure physical environment is not possible for a feeder link, the use of cryptographic algorithms to protect N2 and N3 should be mandatory in the context of NTNs (currently, using cryptographic solutions to protect N2 and N3 interfaces is an operator's decision). Furthermore, the data (except for NAS PDU) is not protected inside the satellite, as the security protection is terminated on board. This may be a problem if the satellite operator is not trusted by the mobile user, in which case using end-to-end encryption and authentication could be considered. The advantage of extra security functionality on board is that tampering and spoofing at the PDCP layer are detected by the satellite and do not propagate further on the ground. However, this extra processing next to the radio stack implementation and system processing makes it easier to perform resource depletion attacks on a resource-constrained satellite.

### 6.1.3. NTN scenario 3: Split CU-DU

To reduce the complexity of the NTN payload resulting from hosting the entire gNB, including termination of all its network interfaces, the operator may choose to host only a subset of gNB functionality on board, while keeping the rest on the ground [390]. One such option is the standardized CU-DU split (the so-called option 2 [19]), although other split options [52] are also possible, including the lower layer split [49]; in our thesis, however, we only consider the standardized split option 2 (RRC and PDCP in gNB-CU, RLC, MAC, PHY and RF in gNB-DU), leaving other options as future work. Despite a simpler payload implementation, the split architectures were not designed with the NTN scenario in mind, which creates additional challenges [390]. For example, the F1 interface was designed to be "persistent" between the same gNB-DU and gNB-CU pair without being torn down and established again (especially from the same gNB-DU to a different gNB-CU). Since F1 cannot relocate UE contexts "on demand" to a different pair of gNB-CU and gNB-DU, its teardown will release all handled UE contexts and drop the corresponding connections. Hence, this architecture cannot natively support LEO satellites changing NTN GWs without addressing this limitation (e.g. by hosting two gNB-DUs on board, which are simultaneously connected to different ground gNB-CUs).

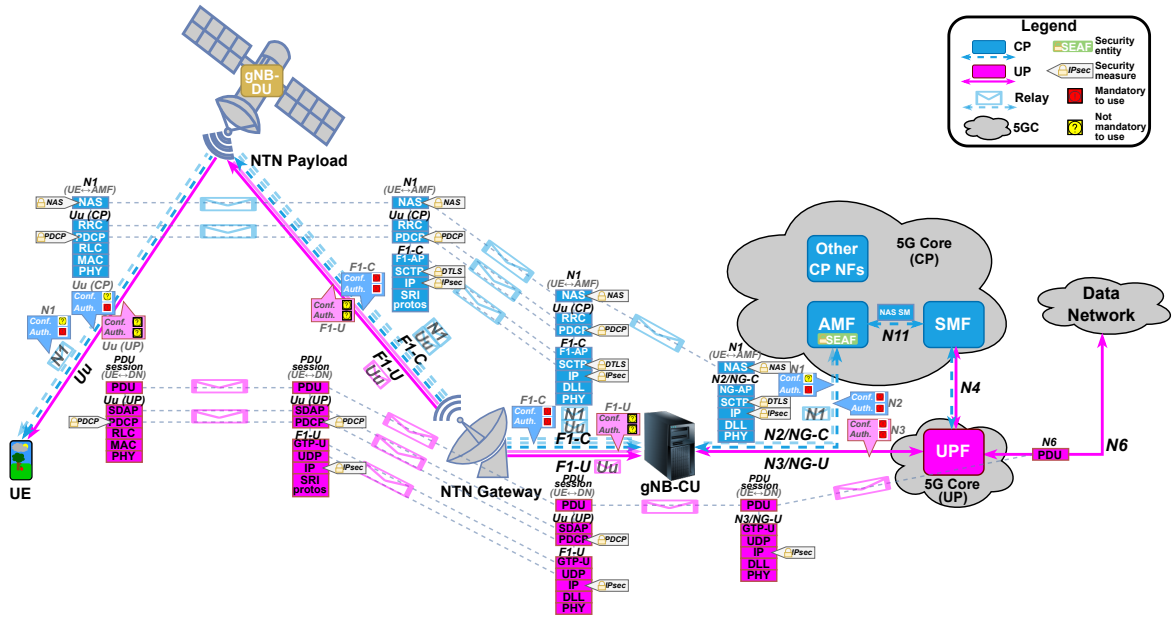



**Figure 6.3:** Security architecture of the NTN Split CU-DU scenario (based on [37]).

Figure 6.3 presents the security architecture for the Split CU-DU scenario. The exposed interfaces on the feeder link are F1-C (CP) and F1-U (UP), which carry PDCP-protected RRC and SDAP layers, respectively, terminating in gNB-CU on the ground. The F1 interface uses traditional cryptographic

protections: IPsec and DTLS for F1-C and IPsec for F1-U. While confidentiality protection and authentication of F1-C is mandatory to use, the 3GPP specification [33] requires F1-C and management traffic to be protected independently of F1-U traffic, which allows F1-U to be protected differently from F1-C regarding the use of encryption and integrity protection. This implementation freedom, however, is not justified in the NTN deployment where F1-U cannot be placed in a physically secure environment and PDCP is not mandatory to use for the UP traffic. Choosing not to use cryptographic protections for this link directly compromises all user data confidentiality and authentication. This is especially detrimental in governmental scenarios where countries with conflicting interests may be able to sniff each other's traffic (unless end-to-end encryption and authentication is used). We therefore think it is important that 3GPP mandates the use of cryptographic solutions for the F1 interface (both CP and UP).

In other security aspects, Split CU-DU is a mix of the two previously discussed scenarios: Transparent payload and Full gNB on board. The NTN payload is capable of adding extra cryptographic protection for F1 next to PDCP. Similarly to Transparent payload, PDCP terminates on the ground, which prevents the satellite from accessing plaintext data, even though it cannot detect PDCP tampering and spoofing. While the resource depletion attacks are more difficult to perform than for the Full gNB on board scenario due to less on-board processing, it is easier than for Transparent payload, since the NTN payload in the split architecture performs the decoding and processing of the lower layers of the radio protocol stack (PHY, MAC, RLC, and RRC for MIB/SIB). Finally, similar to the transparent payload architecture, UE AS security contexts (such as keys and sequence numbers) are not stored on the satellite, while IPsec and DTLS related data and parameters must be on board, as in the case of full gNB on board.

### 6.1.4. NTN scenario 4: UE-Satellite-UE communication

One of the features that can be provided by a satellite is "direct-to-device" ("direct-to-cell", "D2D"), offered by Starlink [334, 375] and Apple [181]. The latest iPhones use satellite services for emergency communication, road-side assistance, location sharing with friends, but also iMessage and SMS [115]. The feature allows for ubiquitous access to messaging, calling, and browsing from any location on the Earth, including areas with no cellular connectivity, such as lakes and oceans.

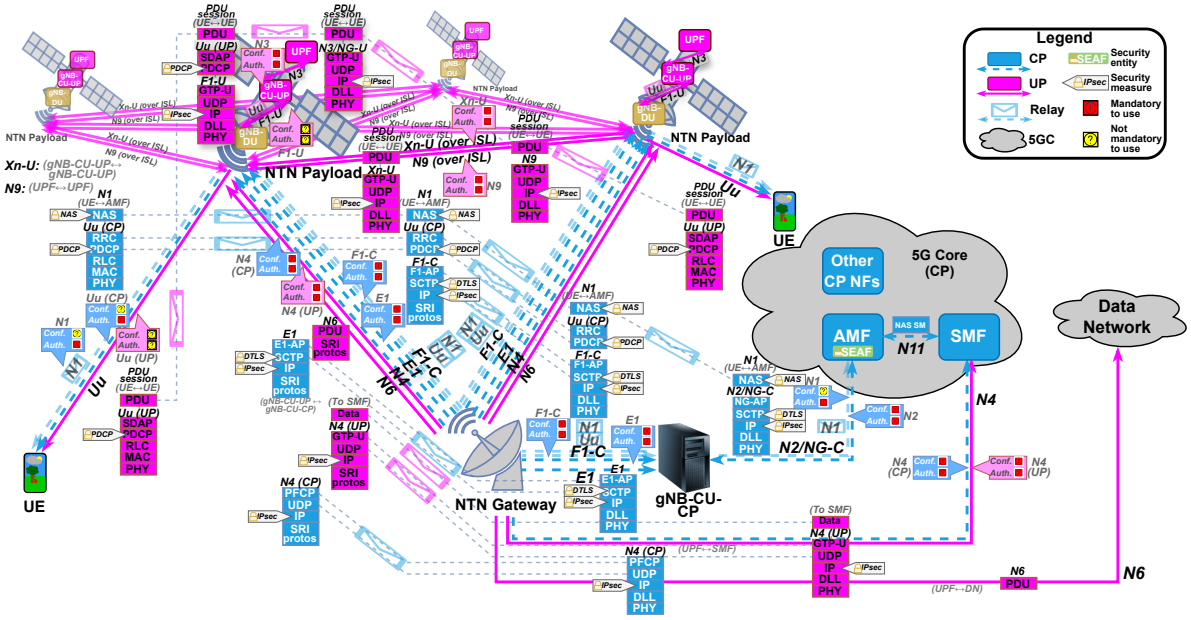



**Figure 6.4:** Security architecture of the NTN UE-Satellite-UE communication scenario (based on [50]).

D2D has the potential to allow standard smartphones to access the network, thus increasing the traffic flow. To reduce the saturation on feeder links and achieve higher resilience, operators may consider a UE-Satellite-UE deployment, in which routing is local to one or more satellites. In order to do that, the UPF needs to be placed on board to perform local routing. This makes the architecture different from and more complex than the previous three scenarios, as shown in Figure 6.4.

The presented architecture has UPF, gNB-DU and gNB-CU-UP on board every satellite (note that UPF does not have to be deployed on every satellite). As a result, N4 (CP and UP), F1-C, E1, and N6 interfaces correspond to the exposed feeder link, while N9 and Xn-U are exposed as an ISL. N4, N9, Xn-U, and E1 include mandatory to use confidentiality and integrity protection: IPsec shall be supported for N4, N9, and Xn-U; IPsec and DTLS shall be supported for E1. Protection of N6 depends on the PDU type. Similar to the Split CU-DU scenario discussed in subsection 6.1.3, F1-C on the feeder link has mandatory to use protection (IPsec and DTLS), with the PDCP protection terminated in gNB-CU-CP on the ground. The interfaces F1-U and N3 are not directly exposed, but are implemented inside the NTN payload. Protection of F1-U (using IPsec) is not mandatory to use, while protection of N3 (using IPsec) is mandatory to use. Even though these interfaces are not exposed over the air, their security protection is still important, since a compromised application in the satellite payload could eavesdrop and tamper with the traffic between the corresponding endpoints.

## 6.2. Comparison of NTN scenarios

As we have seen in section 6.1, each NTN deployment architecture has its own advantages and disadvantages in terms of security. Table 6.1 summarizes the strong and weak points of the first three NTN scenarios: Transparent payload, Full gNB on board, and Split CU-DU. It compares them in terms of exposed interfaces and the corresponding protection levels (mandatory or not mandatory to use), security implementation requirements for the NTN payload, processing requirements, and other aspects. In short, from the security perspective, we could summarize the three NTN scenarios as follows:

1. **Transparent payload.** The short-term deployment solution that can be directly used with an NTN-compatible payload. However, the NTN payload does not provide advanced features of a regenerative payload (e.g. packet switching directly in the payload) and cannot detect attacks against the satellite (e.g. at the PDCP layer).
2. **Full gNB on board.** The long-term deployment solution that can support more advanced features and detect some attacks on board (e.g. at the PDCP layer). However, the NTN payload needs to implement a lot of security functionality (next to the entire radio protocol stack), requires significant processing power, and a large storage for all UE security contexts (PDCP, IPsec, IKEv2, DTLS).
3. **Split CU-DU.** A combination of the above two deployment solutions that provides more features than Transparent payload and needs to implement some security functionality on board (next to the lower layers of the radio protocol stack). It requires less processing power and less storage space than Full gNB on board. However, it cannot detect PDCP layer attacks against the satellite.

**Table 6.1:** Comparison between three NTN deployment scenarios: Transparent payload, Full gNB on board, and Split CU-DU.

| | Transparent payload | Full gNB on board | Split CU-DU |
|---|---|---|---|
| **Plaintext data** | Satellite cannot access plaintext (unprotected) data | Satellite can access plaintext (unprotected) data | Satellite cannot access plaintext (unprotected) data |
| **Security implementation** | Satellite does not need to implement security | Satellite has to implement security (IPsec, DTLS, PDCP) | Satellite has to implement security (IPsec and DTLS) |
| **Service link protection** | Only service link (Uu) CP authentication is mandatory to use (CP/UP confidentiality protection and UP authentication are not mandatory to use) (with PDCP and NAS) | Only service link (Uu) CP authentication is mandatory to use (CP/UP confidentiality protection and UP authentication are not mandatory to use) (with PDCP and NAS) | Only service link (Uu) CP authentication is mandatory to use (CP/UP confidentiality protection and UP authentication are not mandatory to use) (with PDCP and NAS) |
| **Feeder link protection** | Feeder link (Uu) is only protected with PDCP (and NAS) | Feeder link (N2/N3) is only protected (next to NAS) with IPsec and DTLS (IPsec and DTLS for CP; IPsec for UP) | Feeder link (F1) is extra protected next to PDCP (and NAS) (IPsec and DTLS for CP; IPsec for UP) |
| **Feeder link CP authentication** | Feeder link (Uu) CP authentication is mandatory to use | Feeder link (N2) CP authentication is mandatory to use | Feeder link (F1-C) CP authentication is mandatory to use |
| **Feeder link CP confidentiality protection** | Feeder link (Uu) CP confidentiality protection is not mandatory to use | Feeder link (N2) CP confidentiality protection is mandatory to use | Feeder link (F1-C) CP confidentiality protection is mandatory to use |

*Continued on the next page*

**Table 6.1** *(continued from the previous page)*

| | Transparent payload | Full gNB on board | Split CU-DU |
|---|---|---|---|
| **Feeder link UP authentication** | Feeder link (Uu) UP authentication is not mandatory to use | Feeder link (N3) UP authentication is mandatory to use | Feeder link (F1-U) UP authentication is not mandatory to use |
| **Feeder link UP confidentiality protection** | Feeder link (Uu) UP confidentiality protection is not mandatory to use | Feeder link (N3) UP confidentiality protection is mandatory to use | Feeder link (F1-U) UP confidentiality protection is not mandatory to use |
| **Tampering at PDCP layer** | Tampering at PDCP layer is not detected by the satellite and propagates all the way to the ground gNB | Tampering at PDCP layer is detected by the satellite and does not propagate further | Tampering at PDCP layer is not detected by the satellite and propagates all the way to the ground gNB |
| **UE spoofing at PDCP layer** | UE spoofing at PDCP layer is not detected by the satellite and propagates all the way to the ground gNB | UE spoofing at PDCP layer is detected by the satellite and does not propagate further | UE spoofing at PDCP layer is not detected by the satellite and propagates all the way to the ground gNB |
| **Processing on satellite** | Satellite needs to do minimum processing (no decoding) | Satellite needs to do all the processing (encoding and decoding of the entire radio stack + PDCP ciphering and integrity protection + IPsec and DTLS + handovers) | Satellite needs to do relatively large amount of processing (encoding and decoding of the radio part, i.e. PHY, MAC, RLC, and RRC for MIB/SIB) |
| **Handovers** | No need for gNB handovers | gNB handovers may be needed for the feeder link (for non-GEO satellites) and keys have to be transferred to the target gNB | No need for gNB handovers |
| **(D)DoS attacks on satellite** | Difficult to perform due to minimum processing on the satellite | Easiest to perform due to very high processing on the satellite | Fairly easy to perform due to relatively high processing on the satellite |
| **UE AS security context** | UE AS security context (e.g. keys, SNs) is not stored on the satellite | UE AS security context (e.g. keys, SNs) is stored on the satellite and may need to be shared between multiple satellites | UE AS security context (e.g. keys, SNs) is not stored on the satellite |
| **Impact of satellite compromise** | Low impact, since the satellite does not store any sensitive data | Critical impact, since the satellite stores IPsec/DTLS keys and certificates for the feeder link protection as well as AS security context (e.g. PDCP keys and SNs) for the service link protection | High impact, since the satellite stores IPsec/DLTS keys and certificates for the feeder link protection |

The UE-Satellite-UE communication, relying on regenerative payload architecture, has similar strengths and weaknesses as Full gNB on board and Split CU-DU scenarios. The satellite can access plaintext (unprotected) UP data, but not CP data, and needs to implement IPsec, DTLS, and PDCP. On-board gNB-CU-UP, terminating the UP part of PDCP, allows detecting tampering and spoofing of UP data, while CP data manipulation propagates to the gNB-CU-CP on the ground. The satellite has to perform a lot of processing: the entire UP radio stack, the lower layers of the CP radio stack, UPF functionality (including packet forwarding and communication with SMF on the ground), PDCP ciphering and integrity protection for UP, IPsec and DTLS for the feeder link, and handovers (for non-GEO satellites). Because of this, resource exhaustion attacks against the NTN payload are much easier to perform than in the Transparent payload scenario. Moreover, satellite compromise has extremely high impact, since IPsec/DTLS keys and certificates, as well as UE security contexts for UP are stored on board.

## 6.3. Analysis of TN literature attacks in NTN

In section 5.5, we presented our analysis of the selected attacks against TN found in the literature. In this section, we revisit those attacks, but discuss them in the context of NTNs. Table 6.2 lists a brief summary of each attack and its potential impact on NTN. For a more detailed description and our analysis of the general impact, together with (proposed) mitigations, see Table 5.11 in section 5.5. Furthermore, the practical impact of the “DoS by resource depletion” attack is further analysed in subsection 7.5.2.

In our discussion, we assume that a rogue gNB (FBS) can be implemented using a drone or an UAV, controlled by the attacker. Such an aerial vehicle could overshadow the signal coming from the satellite to the UE or vice versa. The abused interface is still Uu, but unlike TNs where this interface is between the UE and a terrestrial gNB, it is now between the UE and the satellite (with a transparent or regenerative payload). Note, however, that such a setup is very complex and expensive to implement, especially if the FBS has to be in the orbit to overshadow the signal from the UE. Therefore, the cost of performing these attacks increases compared to a TN setting, where the attacker could use a relatively cheap COTS equipment for a rogue gNB.

**Table 6.2:** Selected TN literature attacks from Table 5.11 revisited in the context of NTNs.

| Attack (Weakness) | Categ. | Attack summary | Potential impact on NTNs |
|---|---|---|---|
| **DoS using NAS Registration Reject** [192, 187, 246] *Root cause: By design, NAS Registration Reject is accepted by the UE without authentication before security can be activated.* | AS/NAS security *(NAS layer, pre-auth.)* | Since the UE accepts NAS *Registration Reject* messages without authentication before NAS security activation, the attacker can use an FBS to reply to the NAS *Registration Request* with a spoofed NAS *Registration Reject*, pretending to be the AMF. This will deny the victim UE of the network access and can keep it out of service for some time, which can be permanent in some cases (e.g. with IoT devices). | The impact on the UE is the same as in TNs. The volume of the attack is larger: more UEs could be targeted, since more UEs can be served by the satellite due to a larger coverage area. However, the attack complexity and cost are higher, since the signal from the satellite needs to be overshadowed. |
| **DoS using RRCReject** [194] *Root cause: By design, the UE accepts RRCReject messages without authentication (prior to AS security activation, but also after that, since this message can be sent in SRB0, i.e. using the common control channel, in RRC_INACTIVE state).* | AS/NAS security *(RRC layer, pre-auth.)* | Since the UE in RRC_IDLE (i.e. not connected) state accepts unauthenticated *RRCReject* messages, which are sent before AS security activation, the attacker can use an FBS to reply to the *RRCSetupRequest* with a spoofed *RRCReject*, pretending to be the gNB, and possibly ask the UE to wait in the idle mode before reconnecting to the gNB (for a maximum of 16 seconds). This will deny the victim UE of the cell access and can keep it in the idle state for some time, which means that the UE will not get the services from the network. | The impact on the UE is the same as in TNs. The volume of the attack is larger: more UEs could be targeted, since more UEs can be served by the satellite due to a larger coverage area. However, the attack complexity and cost are higher, since the signal from the satellite needs to be overshadowed. |
| **DoS by gNB resource depletion** [215, 192, 187, 246] *Root cause: By design, the RRC connection setup procedure does not authenticate the sender.* | AS/NAS security *(RRC layer, pre-auth.)* | Because the sender is not authenticated during the RRC connection setup procedure, the attacker can establish many fake RRC connections, each time ignoring the NAS *Authentication Request* from the AMF, with the goal of exhausting the capacity of the allowed active RRC connections in the gNB. If the attacker manages to overload the gNB, then the legitimate UEs will not be able to connect to the base station and the core network and get the desired services. | With a transparent payload, the impact is comparable to the TN, however higher latencies reduce the flooding rate. With a regenerative payload, the satellite can experience a higher load due to constraints on processing and memory resources. However, the practical impact of the attack depends on how the gNB implementation handles UE contexts (e.g. expiration timeout, maximum count, release both at MAC and RRC layers). The attack complexity and cost are comparable to the TN. |
| **DoS by spoofing uplink grants** [245] *Root cause: By design, DCI messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | Due to the lack of authentication in Downlink Control Information (DCI) messages, an attacker can spoof the uplink grants (UL DCI) and perform a fake allocation of UL resources. If continuously done for all connected UEs and in every time slot, these benign UEs can be forced to transmit on the same UL resources (possibly at the maximum power), creating interference and congestion in the cell. The legitimate UEs become jammers that disrupt the communication in the cell and lower the throughput. | The impact on a single UE is the same as in TNs. The volume of the attack is larger: more UEs can be reached due to a larger coverage area of the satellite. However, the attack complexity and cost are higher, since the signal from the satellite needs to be overshadowed. |

*Continued on the next page*

**Table 6.2** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Attack summary | Potential impact on NTNs |
|---|---|---|---|
| **DoS by blocking initial cell access** [245] *Root cause: By design, the RA procedure is not protected. In addition, SIB and PO messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | Since the Random Access (RA) procedure is not protected by design and *System Information Block (SIB)* messages are accepted by the UE without authentication, the attacker can modify the RA parameters in the broadcast *SIB* messages from the gNB (e.g. by minimizing the *RA Response (RAR)* reception window, maximizing the number of retries, and maximizing the power ramp-up after each failure) to make all UEs connecting to the network keep failing the RA procedure and not getting access to the cell. The attack can also target already connected UEs by injecting a special *PDCCH Order (PO)* DCI message, telling these UEs to start a RA procedure to re-establish synchronization in the UL. As a result, the attacker can drain resources and disconnect the UEs to launch subsequent localization attacks. | The impact on a single UE is the same as in TNs. The volume of the attack is larger: more UEs can be reached due to a larger coverage area of the satellite. However, the attack complexity and cost are higher, since the signal from the satellite needs to be overshadowed. |
| **Location tracking with a SUCI-Catcher** [111, 83, 192] *Root cause: AKA linkability in the design: the target UE responds differently to the NAS Authentication Request than a regular UE (accept and reject, respectively).* | AS/NAS security *(NAS layer, pre-auth.)* ECIES | Due to the AKA linkability issue, the attacker, having obtained the victim's SUCI (e.g. using a fake base station), can differentiate between the searched-for-subscriber and a regular subscriber based on their reply to the NAS *Authentication Request* message from the (impersonated) AMF. Specifically, the target UE replies with *Authentication Response* (or *Authentication Failure* with *"Synch Failure"* as the cause), while a non-target UE sends *Authentication Failure* with *"MAC Failure"* as the cause. This allows the attacker to verify the presence of a particular person of interest in the current location. | The impact on the UE is the same as in TNs. The volume of the attack is larger: more UEs could be tracked, since more UEs can be served by the satellite due to a larger coverage area. However, the attack complexity and cost are higher, since the signal from the satellite needs to be overshadowed. |

From Table 6.2, we can see that the analysed attacks targeting the UE generally have the following differences between a terrestrial and a non-terrestrial environment:

- **From the perspective of a single targeted UE, the impact is the same in NTN and in TN.** In both terrestrial and a non-terrestrial networks, the victim UE is still on the ground in a typical scenario. If the attacker can successfully perform a DoS or a location tracking attack, then it does not matter whether the attack is performed with the gNB on the ground or in space.
- **The attack volume is larger in NTN than in TN.** Since a satellite has a larger coverage area than a terrestrial gNB, more UEs can be served by a single satellite (with a transparent or regenerative payload) and across a larger geographical area. This also means that more UEs can become possible targets of an attack (whether a DoS, jamming, or location tracking).
- **The attack complexity and cost are higher in NTN than in TN.** For the attacks involving a rogue gNB, the attacker needs to overshadow the signal from the serving satellite. This could be done if the attacker device is close to the victim (which is not always possible) or somewhere between the satellite and the victim. In the latter case, a more complex and expensive setup is needed (compared to a simple COTS device) and the satellite location might also have to be known. This can be a limitation of these attacks and would restrict them to higher-skilled attackers (such as state-sponsored actors).

As for the attacks targeting the on board gNB, while in theory they could have a higher impact in NTN than in TN due to higher constraints on satellite resources, this is not necessarily the case in practice. If the gNB implementation properly releases stale UE contexts and the expiration timeout is low enough (but not too low to avoid disconnecting legitimate UEs), then only the computational resources would be affected. However, the rate of flooding attacks would be lower due to higher latencies, especially with higher altitudes. In addition, the impact on the satellite processing resources would depend on the amount of computational resources available to the attacker.

## 6.4. Comparison of TN and NTN security architectures

Now that we have analysed different NTN deployment scenarios and the impact of TN attacks on NTN, we can reflect on the differences between terrestrial and non-terrestrial networks from the security perspective. Table 6.3 gives a head-to-head comparison of TN and NTN. More generally, we can highlight the following differences:

- **Satellite has a much larger coverage area.** Eavesdropping and tampering are possible from a larger geographical area than in terrestrial networks. In addition, larger coverage area increases the volume of attacks due to more possible targets. However, the complexity and cost of these attacks can also become higher, especially if the signal from the satellite needs to be overshadowed.
- **Satellite has much stricter requirements on processing and memory.** Keeping track of all identifiers and (security) contexts becomes challenging with strict memory constraints, especially for regenerative payloads. Moreover, unlike in TN, adding more resources may not be possible as a countermeasure against resource exhaustion attacks, due to physical constraints. Resource limitations may also result in deployments without (sufficiently) implemented security protections.
- **Satellite can be moving, which may require context transfers.** For non-GEO satellites, the feeder and service links change when the satellite moves out of sight. With a transparent payload, all security contexts (e.g. PDCP, IPsec, DTLS) are stored on the ground, so no context transfer is needed. With the gNB-DU on board, a new F1 interface needs to be established between the gNB-CU on the ground and the next gNB-DU. With a full gNB on board, the UE context needs to be securely transferred between the old and new serving satellites, or a new security context has to be established between the UE and the next serving satellite. The latter would require connection (re-)establishment, which may include unprotected RRC messages that are sent before security activation.
- **Satellite is not physically accessible.** Once launched, the satellite remains in space for its entire lifetime. It cannot be reached physically in the same way a base station on the ground can be accessed. This makes key management more difficult, since a compromised key cannot be physically replaced. Moreover, (post-quantum) cryptographic algorithms and other security solutions need to be carefully planned before the satellite is launched. On the other hand, a satellite is less vulnerable to physical attacks (such as disruption or key extraction) compared to a terrestrial gNB.

**Table 6.3:** Head-to-head comparison of the security of terrestrial and non-terrestrial networks.

| | Terrestrial networks | Non-terrestrial networks |
|---|---|---|
| **Uu interface** | • The distance between the UE and the gNB is relatively small<br>• The Uu interface is always available and is fixed<br>• Eavesdropping, spoofing, and tampering are only possible from a close distance to the UE and/or gNB | • The distance between the UE and the gNB is much larger (but also depends on the orbit)<br>• The Uu interface corresponds to the service link and may be changed with a different serving satellite (in case of non-GEO satellites)<br>• Eavesdropping, spoofing, and tampering are possible from a larger distance to the UE and/or gNB (with the gNB on board) |
| **N2 and N3 interfaces** | • The N2 and N3 interfaces are always connected to a single gNB<br>• The interfaces may be placed in a physically secure location | • The N2 and N3 interfaces may be connected to different gNBs at different times (in case of non-GEO satellites)<br>• The interfaces are fully exposed in case of a feeder link (with a full gNB on board) |
| **F1 interface (CU-DU split)** | • gNB-DU and gNB-CU are relatively close to each other<br>• The F1 interface is always connected to a single gNB-DU<br>• The interface may be placed in a physically secure location<br>• Exploiting the absence of F1-U protections (confidentiality and authentication) is possible only within a limited distance from the gNB-DU and/or gNB-CU | • gNB-DU and gNB-CU are far from each other (which also depends on the orbit)<br>• The F1 interface may be connected to different gNB-DUs at different times (in case of non-GEO satellites)<br>• The interface is fully exposed as a feeder link<br>• Exploiting the absence of F1-U protections (confidentiality and authentication) is possible from a much larger geographical area |

*Continued on the next page*

**Table 6.3** *(continued from the previous page)*

| | Terrestrial networks | Non-terrestrial networks |
|---|---|---|
| **Xn interface** | • The Xn interface is always between the same two gNBs and is fixed<br>• The key transfer is relatively simple for the network side (both gNBs are fixed) | • The Xn interface may be between different gNBs (in case of non-GEO satellites)<br>• The key transfer is more complex for the network side in case of a full gNB on board (gNBs are moving, and many keys are involved) |
| **Cryptographic protections on NDS/IP network interfaces** | • Cryptographic protections are fully controlled by the network operator<br>• Physically secure location may be possible<br>• Cryptographic protections may be not needed (in case of a physically secure location) | • Cryptographic protections may be subject to agreements with the satellite operator<br>• Physically secure location is not possible in case of a feeder link<br>• Cryptographic protections are always needed for exposed feeder and service links |
| **Handovers** | • The gNB location is always fixed<br>• Handovers occur only when the UE changes the cell (due to mobility)<br>• Cell sizes are smaller, so handovers due to UE mobility can be more frequent<br>• Only one serving gNB needs to have the UE security context (e.g. keys, SNs etc.) | • The gNB location may be non-fixed (in case of non-GEO satellites)<br>• Handovers occur when the UE changes the cell (due to mobility) and when service and/or feeder links are not available<br>• Cell sizes are larger, so handovers due to UE mobility can be less frequent<br>• Multiple serving gNBs might need to have the UE security context (e.g. keys, SNs etc.), so it has to be securely transferred, or a new context needs to be established (with regenerative payloads) |
| **Constraints on the UE** | • The UE has to be close to the gNB to connect to the network (i.e. within the coverage area of the mobile network operator)<br>• Lower transmission power is needed to reach the ground gNB | • The UE can connect to the network from a much larger area (including places with no terrestrial connectivity)<br>• Larger transmission power is needed to reach the on-board gNB, which could be abused by an attacker |
| **Constraints on the gNB (satellite)** | • Lower or no processing constraints (due to the absence of physical restrictions, such as energy and weight)<br>• Storing security contexts for many UEs for every session can be addressed by adding more resources (e.g. CPU, RAM)<br>• Flooding attacks and signalling storms can be mitigated by adding more resources | • Higher processing constraints (due to physical restrictions, such as energy and weight)<br>• Storing security contexts for many UEs for every session may not be feasible with a full gNB on board (CPU cycles and RAM size may be limited due to physical restrictions)<br>• Flooding attacks and signalling storms cannot be mitigated by adding more resources |
| **Plaintext data exposure** | • Plaintext data is only exposed to the network operator | • Plaintext data may also be exposed to a third party satellite operator (with full gNB on board) |
| **Impact of unprotected RRC/NAS messages** | • Tampering pre-authentication RRC/NAS messages affects a smaller number of UEs (due to smaller cell sizes)<br>• Tampering with SIB1/SIB2 messages can create destructive interference [245] affecting less UEs (since generally less UEs will be connected to a terrestrial gNB) | • Tampering pre-authentication RRC/NAS messages can affect a larger number of UEs (due to larger cell sizes)<br>• Tampering with SIB1/SIB2 messages can create destructive interference [245] affecting more UEs (since more UEs can be connected to a non-terrestial gNB) |
| **Attacks involving an FBS** | • An attacker has to be physically close to the UE or the gNB<br>• FBSs are easier to detect due to a smaller geographical area<br>• Attacks involving an FBS are generally easier and cheaper to perform (possible with a COTS device) | • An attacker can be physically far from the UE or the gNB<br>• FBSs are more difficult to detect due to a larger geographical area<br>• Attacks involving an FBS can be more difficult and more costly to perform (a more complex and expensive setup may be needed to overshadow the signal from the satellite) |
| **Physical security** | • An attacker can get physically close to the base station, as it is often located in a fairly accessible area (e.g. on top of a building)<br>• Physically extracting cryptographic keys can be much easier<br>• In case of secret sharing between gNBs, the risk of physically compromising one gNB is higher | • An attacker cannot easily get physically close to the satellite<br>• Physically extracting cryptographic keys is very difficult and expensive<br>• Some degree of secret sharing between satellites could be tolerated, as the risk of physically compromising one satellite is lower |
| **Impact of the environment** | • No specific security challenges related to the terrestrial environment | • High radiation levels can flip bits in the memory (e.g. for keys or security contexts), therefore some redundancy is needed |

## 6.5. Reflections

The exposed nature of feeder and service links makes the corresponding interfaces open for eavesdropping and tampering attacks from a larger distance than in terrestrial deployments. In case of NTN, communication may be exposed to another country, possibly with conflicting interests. This is especially important for governmental NTN implementations, where national security may be at stake. Since it is not possible to ensure a physically secure environment for the exposed interfaces, we suggest that 3GPP explicitly mandates the use of cryptographic solutions for confidentiality, integrity, and replay protection on these interfaces. In addition, as already discussed in chapter 5 for TNs, it is important to ensure correct implementation of cryptographic algorithms as well as maintaining cryptographic agility.

Due to processing restrictions of an NTN payload, the network and/or satellite operators might be tempted to not implement some security mechanisms proposed by 3GPP. One such example is the use of IPsec and DLTS on F1-C and N2 interfaces. IPsec is implemented by the host operating system and is usually OS-specific. It can be used for mutual authentication, but only between hosts. On the other hand, (D)TLS is application-to-application, providing mutual authentication between functions and applications running on the same host, e.g. using virtualization. If DTLS is not implemented (e.g. due to processing and memory constraints of the satellite), then there is a gap between the host OS and the running applications. In this case, a compromised application on the same NTN payload would be able to read the traffic between another application and the kernel, for instance, using system calls. To address this problem, a zero trust network model should be used between applications.

Traditional cryptographic solutions can be difficult to implement on an NTN payload due to processing and memory constraints. Host-to-host IPsec VPNs, providing protection for data during transit, may be resource-heavy to implement and maintain in terms of configuration management (e.g. cryptographic algorithms, SPDs, SADs, long keys) [78]. Due to the limited storage capacity and processing restrictions, it may be infeasible to provide fine-grained protection by separately keying each connection with different cryptographic material. As a possible solution, using more lightweight cryptography could be considered. For instance, RFC 8221 [405] and RFC 8247 [319] list ENCR_AES_CCM_8 (AEAD), AUTH_AES_XCBC_96, and PRF_AES128_XCBC algorithms for use in IoT scenarios. Furthermore, NIST has recently selected the Ascon family to be standardized for lightweight cryptography applications [287, 288]. The new Ascon-based family of symmetric-key cryptographic primitives has been developed to provide AEAD, hash, and Extendable Output Function (XOF) capabilities (Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128, and Ascon-CXOF128) [386]. Due to its lightweight permutation-based primitives, the Ascon family offers robust security, efficiency, and flexibility, which makes it perfect for resource-constrained environments, e.g. IoT devices, embedded systems, and low-power sensors, and in cases when AES may not perform optimally.

As discussed in subsection 5.6.4, the increasing threat of cryptographically relevant quantum computers creates the need to transition to the post-quantum cryptography as soon as possible. With NTN deployments, early migration to quantum-resistant solutions is especially important due to long lifetimes of NTN payloads. A satellite that is launched into the orbit may remain there even after quantum computers emerge. Since replacing all satellites relying on quantum-unsafe cryptography is not feasible due to the associated costs and unavailability periods, it is important to deploy new payloads already with quantum-secure cryptographic algorithms. Of course, using post-quantum cryptography in space creates its own challenges, such as large key sizes and certificate management, however addressing these problems is beyond the scope of our thesis.

# 7

# Flooding attack against 5G terrestrial and non-terrestrial networks

In the previous two sections, we performed a security analysis of 3GPP 5G terrestrial and non-terrestrial networks. We investigated the proposed security mechanisms and their usage requirement levels, compared different NTN scenarios with each other, discussed some relevant literature attacks, and highlighted the differences between terrestrial and non-terrestrial networks. However, our analysis, while in-depth, was done at a theoretical level. In this section, we perform the practical part of our thesis, which is the implementation and evaluation of a flooding attack against the gNB. We develop the attack prototype using UERANSIM with free5GC and the actual attack using OpenAirInterface (OAI). Then, we evaluate our attack against OAI gNB in a TN setting (using real SDR devices) and in an NTN setting (using RF simulator and NTN configuration).

## 7.1. Attack description

The flooding attack that we present in this section was initially proposed and demonstrated by Kim et al. [215] against an LTE network, under the name “BTS resource depletion attack” (with BTS for Base Transceiver Station). It has also been discussed in Table 5.11 and Table 6.2 under the name “DoS by gNB resource depletion”. While similar attacks have also been described in the literature for 5G networks [192, 187, 246], they have only been discussed at a theoretical level. In this chapter, we design and demonstrate this attack against OAI gNB in terrestrial and non-terrestrial settings.

The original attack aims at depleting the capacity of active RRC connections in the gNB, which would prevent other (legitimate) UEs from connecting to the base station. The attacker continuously performs the Random Access (RA) procedure, establishing a new RRC connection with the gNB, and sends a NAS *Registration Request* with an arbitrary user IMSI. However, upon receiving a NAS *Authentication Request*, the attacker ignores the message and instead restarts the RA procedure to set up a new RRC connection. While the AMF is waiting for a NAS *Authentication Response* from the UE, the established RRC connection with the associated context is kept in the gNB. The authors point out that for the attack to be successful, the number of newly created connections must be greater than the number of already existing connections that are released.

For implementation and validation, Kim et al. used a Universal Software Radio Peripheral (USRP) B210 device for a software radio transceiver and srsUE [368] for the rogue UE. They performed the attack against a COTS femtocell connected to the testbed EPC network running OpenAirInterface. Using an Airscope analyser [367] to decode the communication channels in the physical layer, they tried to estimate the number of fake RRC connections that one USRP device could establish. The results showed that the malicious UE was able to create 16 RRC connections in 0.762 seconds, after which the femtocell started rejecting all further connection requests, both valid and invalid. The authors were able to establish 20 RRC connections per second, which would allow the attacker to create 200 connections if the base station was to wait for 10 seconds before releasing inactive RRC connections.

We build on top of the proposed attack, but with a different experimental setup (see section 7.2). First, the authors used an arbitrary user IMSI to establish an RRC connection. While it may be feasible to collect some valid IMSIs in an LTE network using an IMSI catcher, we do not make such an assumption for a 5G network. Instead, we either use one registered IMSI or generate invalid (not registered) IMSIs to represent a more realistic scenario. Furthermore, we also investigate the impact that the flooding attack has on the CPU and memory usage of the target gNB, as well as on the resources of the AMF and the rogue UE. Finally, while a related attack by Hammouchi [183] aimed at stressing the UDM, we cannot meaningfully test this, because at the time of writing, OpenAirInterface does not implement the ECIES profiles for SUCI, making a sufficient amplification infeasible. Therefore, our attack focuses primarily on exhausting the number of RRC connections and also on overloading the gNB.

## 7.2. Experimental setup

As a first step, we design the attack prototype using UERANSIM [178], with free5GC as the core network. While this is not a realistic setup (since all layers below RRC are simulated), it allows us to quickly implement the attack and investigate its impact. Next, we implement the actual attack using OpenAirInterface [322], representing a more realistic scenario. We use the OAI RF simulator, which behaves like a real RF board, but simulates the RF by forwarding samples between the endpoints instead of transmitting them over the air. Since all layers above physical work in exactly the same way, the UE can use the actual RA procedure in the MAC layer during the attack. Finally, we evaluate our attack in a TN setup using real SDR devices for the UE and the gNB/gNB-DU, and in an NTN setup using the OAI RF simulator with the relevant configuration parameters for NTN.

While the exact experimental details depend on the used implementation, in all our tests we differentiate between the two types of experiments:

- **Experiment 1:** The UE is known to the network (i.e. has a valid IMSI). In this experiment, we use one registered IMSI and repeatedly connect the UE to the network using the same IMSI.
- **Experiment 2:** The UE is not known to the network (i.e. has no valid IMSI). In this experiment, we generate incrementing IMSIs and connect the UE to the network using a generated IMSI.

The two experiments represent two different types of attacker trying to abuse the network. In the first experiment, the attacker can be a legitimate subscriber, while in the second experiment, the attacker is an illegitimate user. In each case, the network will react differently to the *Registration Request* from the UE. Registration requests with a legitimate IMSI will be processed by the AMF, which will send a NAS *Authentication Request* back to the UE. While such a continuous flooding using the same IMSI is very easily detectable, we do not expect the detection mechanisms to be present in the implementation under test. On the other hand, registration requests with an invalid IMSI will be rejected by the AMF with a NAS *Registration Reject*. Even if the connection is immediately deleted, sending many registration requests like that could possibly have an impact on the gNB. Figure 7.1 shows the Wireshark captures with the message flows for each experiment, and Figure 7.2 shows the respective flow graphs.

| No. | Time | Delta | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|---|
| 33 | 4.780 | 0.000 | gNB | UE | NR RRC | MIB |
| 34 | 4.780 | 0.000 | gNB | UE | NR RRC | SIB1 |
| 35 | 4.781 | 0.000 | UE | gNB | NR RRC | RRC Setup Request |
| 36 | 4.781 | 0.000 | gNB | UE | NR RRC | RRC Setup |
| 37 | 4.781 | 0.000 | UE | gNB | NR RRC/NAS-5GS | RRC Setup Complete, Registration request |
| 198 | 4.829 | 0.047 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Authentication request |
| 200 | 4.829 | 0.000 | UE | gNB | ICMP | Destination unreachable (Port unreachable) |

(a)

| No. | Time | Delta | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|---|
| 55 | 8.864 | 0.000 | gNB | UE | NR RRC | MIB |
| 56 | 8.864 | 0.000 | gNB | UE | NR RRC | SIB1 |
| 57 | 8.865 | 0.000 | UE | gNB | NR RRC | RRC Setup Request |
| 58 | 8.865 | 0.000 | gNB | UE | NR RRC | RRC Setup |
| 59 | 8.865 | 0.000 | UE | gNB | NR RRC/NAS-5GS | RRC Setup Complete, Registration request |
| 210 | 8.911 | 0.045 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Registration reject (Congestion) |
| 211 | 8.911 | 0.000 | UE | gNB | ICMP | Destination unreachable (Port unreachable) |
| 221 | 9.016 | 0.105 | gNB | UE | NR RRC/NAS-5GS | DL Information Transfer, Registration reject (Tracking area not allowed) |
| 222 | 9.016 | 0.000 | UE | gNB | ICMP | Destination unreachable (Port unreachable) |

(b)

**Figure 7.1:** Wireshark capture with the RRC setup procedure, NAS Registration Request, and response from the network (obtained using UERANSIM and free5GC): (a) for a known UE (valid IMSI) and (b) for an unknown UE (invalid IMSI).

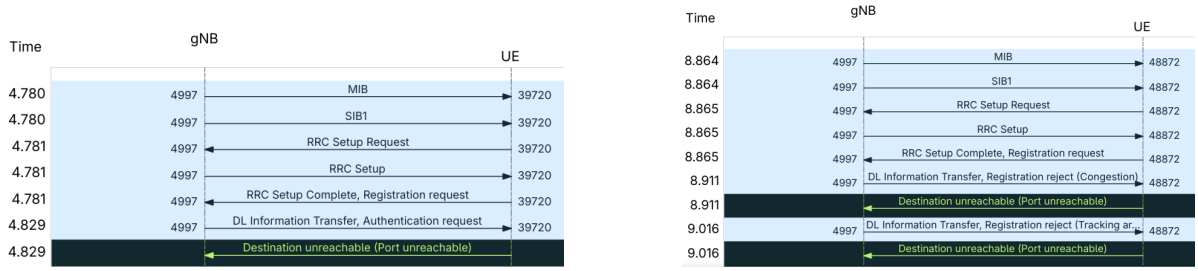



**Figure 7.2:** Wireshark flow graph for the RRC setup procedure, NAS Registration Request, and response from the network (obtained using UERANSIM and free5GC): (a) for a known UE (valid IMSI) and (b) for an unknown UE (invalid IMSI).

For the experiments using UERANSIM and OAI RF simulator, we use a Lenovo laptop with a 24-core Intel i7-12800HX CPU and 32 GB of RAM, running Linux kernel version 6.17. We use Docker for all network entities and allocate a certain amount of CPU and memory resources for the UE, gNB, and AMF containers, keeping track of their CPU and memory utilization during the attack, as well as monitoring the number of UE connections stored in the gNB. For the OAI experiments involving SDRs, we use an Intel NUC machine and two USRP B210 devices for the UE and the gNB. In these experiments, we focus on the number of RRC connections established by the UE. In the following sections, we discuss the specific experimental setup for UERANSIM (see section 7.3) and OpenAirInterface (see section 7.4 and section 7.5), and present the results of our flooding attack.

## 7.3. Attack prototype (UERANSIM)

In this section, we develop the prototype of our flooding attack and test it using UERANSIM [178] and free5GC [241]. Given that UERANSIM does not implement the 5G NR layers below RRC, the lower part of the radio stack is bypassed in our attack prototype. We describe the experimental setup specific to UERANSIM and free5GC, and then present the results for each experiment.

### 7.3.1. Experimental setup

For the 5G core network, we rely on free5GC-compose [242], which is the Docker Compose version of free5GC. For the UE and the gNB, we build our own Docker image based on the modified UERANSIM source code, which is available in our GitHub fork [422]. In particular, we modify the UE program to exit right after it sends the *RRCSetupComplete* message with the NAS *Registration Request*, as any further waiting is not necessary if the UE does not respond to the following message anyway. Inside a loop, we start a new UE as a background process, specifying the same registered IMSI in Experiment 1 and an incrementally generated IMSI in Experiment 2. While running many UE processes simultaneously is not a very realistic scenario, starting a new UERANSIM UE instance requires little resources, given that all layers below RRC are simulated. Furthermore, such an approach allows for parallelization, which can generate a higher load on the gNB.

We restrict the CPU and memory resources that are available to the UE, gNB, and AMF containers. Specifically, we allocate:

- 15.0 CPU cores and 4 GB of memory for the UE (attacker) container
- 2.0 CPU cores and 2 GB of memory for the gNB container
- 1.0 CPU core and 1 GB of memory for the AMF container

Other details specific to the experimental setup together with a step-by-step guide on how to run the experiments and generate plots can be found in our GitHub repository [420].

### 7.3.2. Results

Figure 7.3 and Figure 7.4 show the CPU and memory utilization of the targeted gNB and AMF containers during both experiments. The corresponding resource consumption of the (attacker) UE container is shown in Figure 7.5. To give an indication of the baseline resource usage, we waited around 10 seconds

before running the attack script. The presented statistics have been obtained from the Docker stats, which have been continuously fetched for the entire duration of the attack.

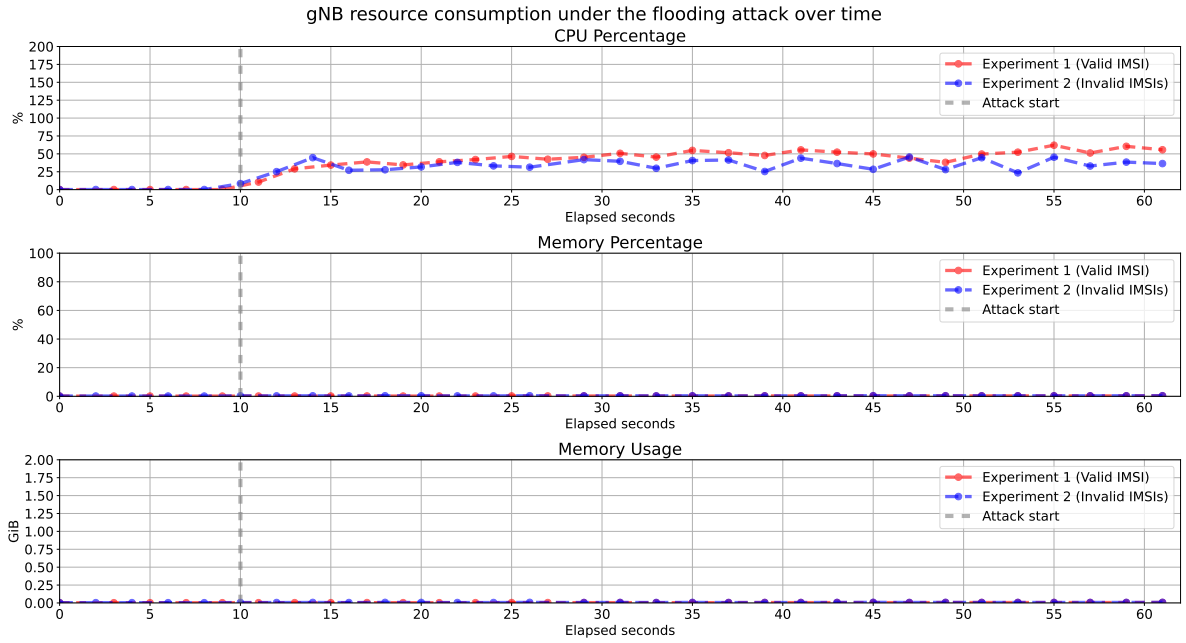



**Figure 7.3:** CPU and memory usage of the gNB container during the flooding attack (UERANSIM).

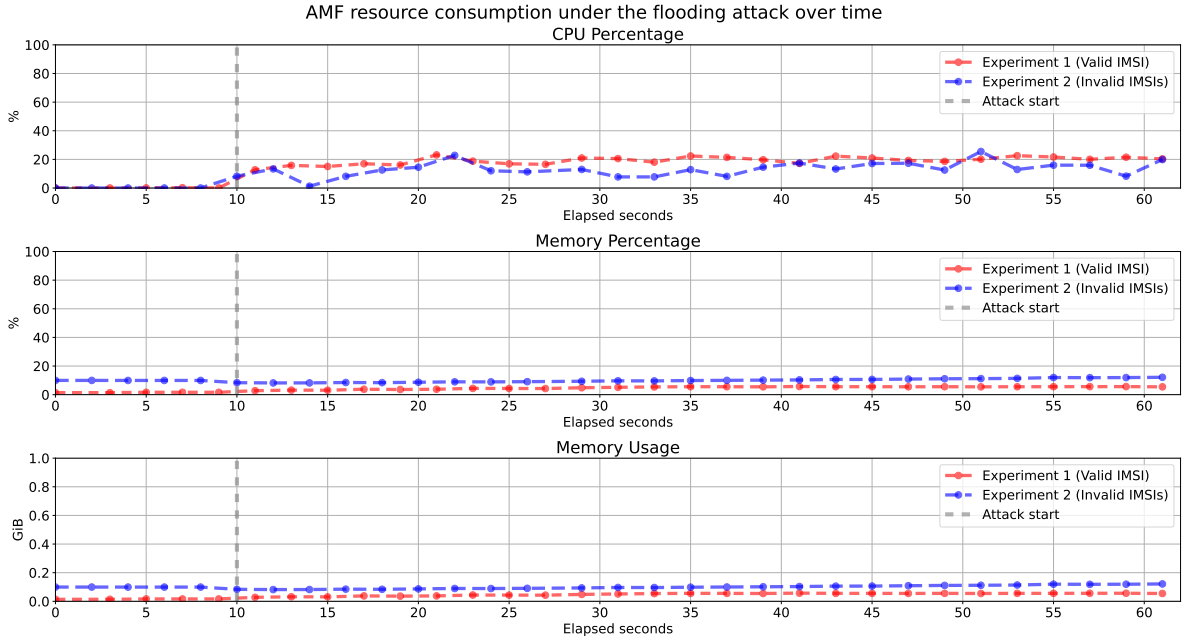



**Figure 7.4:** CPU and memory usage of the AMF container during the flooding attack (UERANSIM).

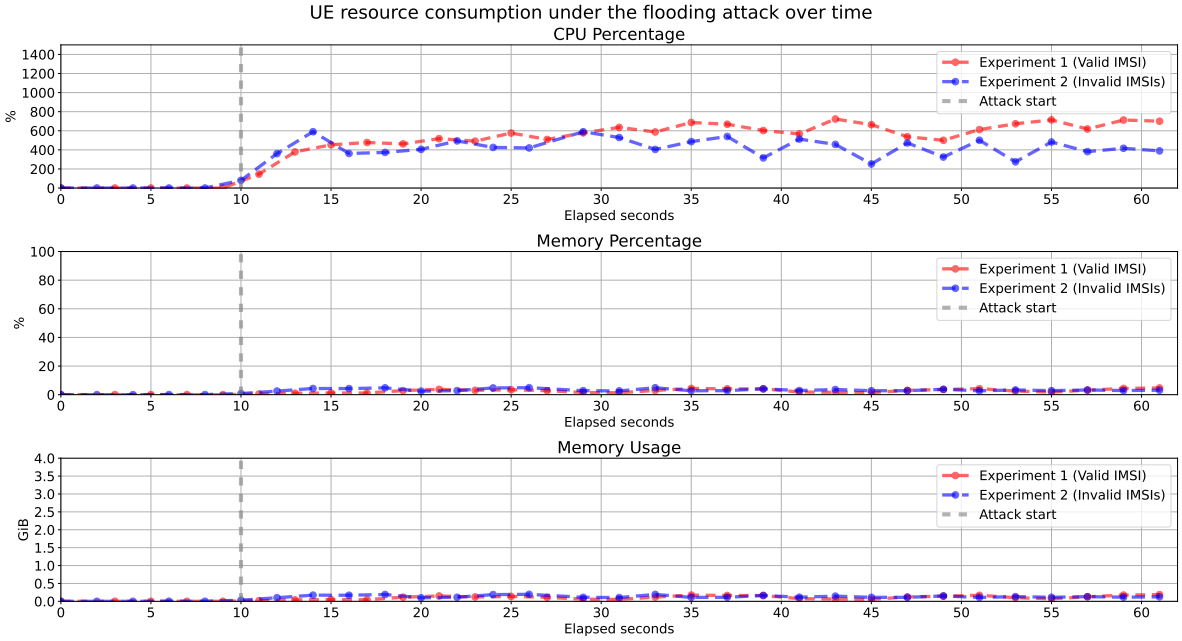



**Figure 7.5:** CPU and memory usage of the UE container during the flooding attack (UERANSIM).

From the figures, we can observe that the resource utilization remains similar between the two experiments. The memory usage of the targeted components (gNB and AMF) is not noticeably affected during the attack. This is also the case for the UE container, whose memory consumption is negligible. For the gNB, this indicates that the fake RRC connections created by the rogue UE do not use enough memory to allow the attacker to overload the base station. As for the CPU utilization, the effects of the flooding attack are more noticeable, even though none of the containers reaches critical levels. We can generally see the CPU consumption of around 30-50% for the gNB (which is less than one of the two allocated cores) and 10-20% for the AMF. The attacker container, which continuously creates new background UE processes, ends up using much more than one CPU core (represented by 100%), while not going over 8 cores (800%), which is less than the allocated 15 cores.

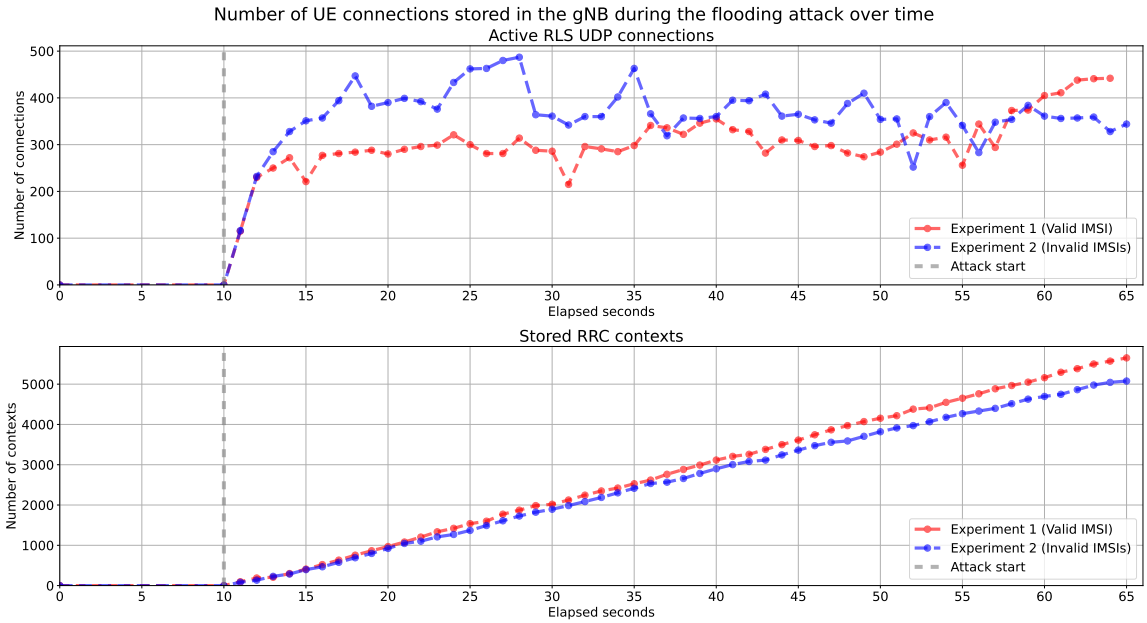



**Figure 7.6:** Active connections and stored RRC contexts in the gNB over time during the flooding attack (UERANSIM).

An important parameter in our flooding attack prototype against UERANSIM is the flooding rate, or how quickly new UEs are created. In the UERANSIM implementation, RRC messages are encapsulated in a specific Radio Link Simulation (RLS) protocol. For each connected UE, next to an RRC context, the gNB creates an RLS UDP connection which represents the actual UE connection. These entries are deleted when the UE has not been ”seen” by the gNB for longer than the heartbeat threshold (defined as 2 seconds), while the stored RRC contexts are not erased. This is illustrated in Figure 7.6, which shows both the fluctuating number of active RLS UDP connections and the linearly increasing number of the total stored RRC contexts in the gNB during the attack, with the numbers that are not very different between the two experiments. We have observed that if UE connections are created too fast, the gNB simply cannot process all the incoming requests, so new RLS UDP connections are continuously being added and deleted due to timeouts. As a result, for the vast majority of new UEs, the RRC connection setup procedure is not completed and no *Registration Request* messages reach the AMF.

While keeping the gNB busy in such a way might sound like a success, it depends on the goals of the attack. Even though the gNB is constantly busy creating and deleting UE connections, almost no NAS *Registration Request* messages are received by the AMF, leaving the core network unaffected by the attack. Furthermore, while new RRC contexts are created in the gNB, which happens when it receives an *RRCSetupRequest*, their number is much lower than the number of RLS UDP connections that are being created and deleted. Therefore, this can be seen as gNB distraction, which is, however, specific to the UERANSIM implementation. On the other hand, to make sure that the UE messages are processed properly, we can also give the gNB a bit more time and create new UEs in batches. For instance, we can create a batch of around 100-150 UEs and wait for one second (which is less than the two-second heartbeat threshold). This batch size, which we call the flooding rate, can be adjusted depending on the goals of the attack (the graphs presented above use the flooding rate of 115 UEs).

Another reason to introduce the flooding rate parameter is that the gNB sometimes crashes due to a segmentation fault. With some debugging, we discovered that the crashes happen due to accessing an invalid memory address. In some cases, it happens in the `std::equal_to<int>::operator()` function when checking the presence of a `ueId` in the unordered map with RLS UDP connections (see Figure 7.7a). In other cases, it happens in a for-loop iterating over the same unordered map when sending a broadcast SIB1 message to all connected UEs (see Figure 7.7b). We believe that these crashes are caused by a race condition or use-after-free, when the UE entry that is being accessed has already been deleted by another part of the program. This definitely does not happen due to successful exhaustion of the number of connections or resources at the gNB, since its memory utilization is extremely low, as seen in Figure 7.3. Moreover, the gNB code uses C++ unordered maps for both RRC contexts and RLS UDP connections, which can grow enormously large. Adjusting the flooding rate can make such crashes happen less frequently when running experiments.

```
17 void RlsUdpTask::send(int ueId, const rls::RlsMessage &msg)
16 {
15     if (ueId == 0)
14     {
13         for (auto &ue : m_ueMap)
12             send(ue.first, msg);
11         return;
10     }
9
8      if (!m_ueMap.count(ueId))
7      {
6          // ignore the message
5          return;
4      }
3
2      sendRlsPdu(m_ueMap[ueId].address, msg);
1  }
```

(a)

```
17 void RlsUdpTask::send(int ueId, const rls::RlsMessage &msg)
16 {
15     if (ueId == 0)
14     {
13         for (auto &ue : m_ueMap)
12             send(ue.first, msg);
11         return;
10     }
9
8      if (!m_ueMap.count(ueId))
7      {
6          // ignore the message
5          return;
4      }
3
2      sendRlsPdu(m_ueMap[ueId].address, msg);
1  }
```

(b)

**Figure 7.7:** Lines in the UERANSIM gNB source code where the segmentation fault happens: (a) while checking if a UE connection exists and (b) while sending a SIB1 message to all UEs.

For Experiment 1, it is interesting to note a couple of observations regarding UE connections, which all use the same IMSI. First, each *RRCSetupRequest* contains a different random value for the UE identity. This is to be expected, because the RRC layer is not aware that the IMSIs are the same, as they are transported by the NAS layer. However, since each UE gets a different *’ueIdentity’* (of type

*'randomValue'*), a new RRC context is created each time, even though the used IMSI represents the same subscriber. Furthermore, the NGAP tunnel between the gNB and the AMF is also different for each NAS *Registration Request* (initial UE message), since the gNB has no way of verifying that it is serving the same user. For each *Registration Request*, the AMF sends a separate *Authentication Request*, essentially treating them as different requests despite the same IMSI. While this is not desired, it is the intended behaviour given the lack of authentication for the *Registration Request* message in the 5G standards. If only one message was processed by the AMF, the attacker would be able to perform a DoS against a legitimate subscriber by spoofing their IMSI. Lastly, based on the default free5GC configuration, the AMF retransmits the *Authentication Request* for a maximum of 4 times, with the expiration time of 6 seconds, even though no response will follow from the UE. All these factors allow the attacker to use a single registered IMSI to perform the flooding attack.

Finally, given that our flooding attack keeps the gNB busy processing fake connections, it could be used as a way to distract the base station and prevent legitimate UEs from connecting to the network. To test this, we registered a new subscriber to the free5GC core network with a different IMSI from the one used for the attack. In both experiments, we connected this UE to the network in normal conditions. As can be seen in Figure 7.8, the UE successfully completed the registration procedure, established the PDU session, and got connectivity to the Internet. Next, we started the attack, waited for a couple of seconds, and tried connecting the victim UE again. This time, as seen in Figure 7.9, the UE was not able to successfully complete the registration and get the PDU session, and was continuously retrying the registration procedure due to timeouts. Overall, even though the attack prototype resulted in a successful DoS with UERANSIM, it needs to be further tested with a more complete 5G implementation including the full 5G NR radio stack, which will be done in the next section using OpenAirInterface.

```
root@c5d093ef45d0:/ueransim# ./nr-ue -c config/uecfg.yaml
UERANSIM v3.2.7
[2025-09-12 18:43:26.421] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2025-09-12 18:43:26.422] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2025-09-12 18:43:26.422] [nas] [info] Selected plmn[208/93]
[2025-09-12 18:43:26.422] [rrc] [info] Selected cell plmn[208/93] tac[1] category[SUITABLE]
[2025-09-12 18:43:26.422] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2025-09-12 18:43:26.422] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2025-09-12 18:43:26.422] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2025-09-12 18:43:26.423] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:43:26.423] [nas] [debug] Sending Initial Registration
[2025-09-12 18:43:26.423] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2025-09-12 18:43:26.423] [rrc] [debug] Sending RRC Setup Request
[2025-09-12 18:43:26.423] [rrc] [info] RRC connection established
[2025-09-12 18:43:26.423] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2025-09-12 18:43:26.423] [nas] [info] UE switches to state [CM-CONNECTED]
[2025-09-12 18:43:26.469] [nas] [debug] Authentication Request received
[2025-09-12 18:43:26.469] [nas] [debug] Received SQN [000000000027]
[2025-09-12 18:43:26.469] [nas] [debug] SQN-MS [000000000000]
[2025-09-12 18:43:26.499] [nas] [debug] Security Mode Command received
[2025-09-12 18:43:26.499] [nas] [debug] Selected integrity[2] ciphering[0]
[2025-09-12 18:43:26.626] [nas] [debug] Registration accept received
[2025-09-12 18:43:26.626] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2025-09-12 18:43:26.626] [nas] [debug] Sending Registration Complete
[2025-09-12 18:43:26.626] [nas] [info] Initial Registration is successful
[2025-09-12 18:43:26.626] [nas] [debug] Sending PDU Session Establishment Request
[2025-09-12 18:43:26.626] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:43:26.626] [nas] [debug] Sending PDU Session Establishment Request
[2025-09-12 18:43:26.626] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:43:26.832] [nas] [debug] Configuration Update Command received
[2025-09-12 18:43:27.037] [nas] [debug] PDU Session Establishment Accept received
[2025-09-12 18:43:27.037] [nas] [info] PDU Session establishment is successful PSI[1]
[2025-09-12 18:43:27.057] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.60.0.2] is up.
[2025-09-12 18:43:43.438] [nas] [warning] Retransmitting PDU Session Establishment Request due to T3580 expiry
[2025-09-12 18:43:43.438] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:43:43.570] [nas] [debug] PDU Session Establishment Accept received
[2025-09-12 18:43:43.570] [nas] [info] PDU Session establishment is successful PSI[2]
[2025-09-12 18:43:43.583] [app] [info] Connection setup for PDU session[2] is successful, TUN interface[uesimtun1, 10.61.0.3] is up.
```

(a)

```
root@c5d093ef45d0:/ueransim# ping -I uesimtun0 -c 5 google.com
PING google.com (142.250.179.142) from 10.60.0.2 uesimtun0: 56(84) bytes of data.
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=1 ttl=112 time=6.24 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=2 ttl=112 time=6.60 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=3 ttl=112 time=8.62 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=4 ttl=112 time=8.88 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=5 ttl=112 time=8.76 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.237/7.820/8.876/1.152 ms
```

(b)

**Figure 7.8:** A legitimate UE successfully connects to the network and has Internet connectivity before the attack: (a) the UE logs and (b) the result of a ping command (UERANSIM).

```
root@c5d093ef45d0:/ueransim# ./nr-ue -c config/uecfg.yaml
UERANSIM v3.2.7
[2025-09-12 18:46:56.688] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2025-09-12 18:46:56.689] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2025-09-12 18:46:56.694] [nas] [info] Selected plmn[208/93]
[2025-09-12 18:46:56.694] [rrc] [info] Selected cell plmn[208/93] tac[1] category[SUITABLE]
[2025-09-12 18:46:56.694] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2025-09-12 18:46:56.694] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2025-09-12 18:46:56.694] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2025-09-12 18:46:56.694] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:46:56.694] [nas] [debug] Sending Initial Registration
[2025-09-12 18:46:56.694] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2025-09-12 18:46:56.694] [rrc] [debug] Sending RRC Setup Request
[2025-09-12 18:46:56.699] [rrc] [info] RRC connection established
[2025-09-12 18:46:56.699] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2025-09-12 18:46:56.699] [nas] [info] UE switches to state [CM-CONNECTED]
[2025-09-12 18:47:11.703] [nas] [debug] NAS timer[3510] expired [1]
[2025-09-12 18:47:11.703] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2025-09-12 18:47:11.703] [nas] [info] UE switches to state [5U2-NOT-UPDATED]
[2025-09-12 18:47:11.703] [nas] [info] Performing local release of NAS connection
[2025-09-12 18:47:11.703] [nas] [info] UE switches to state [MM-DEREGISTERED/ATTEMPTING-REGISTRATION]
[2025-09-12 18:47:11.703] [rrc] [info] UE switches to state [RRC-IDLE]
[2025-09-12 18:47:11.703] [nas] [info] UE switches to state [CM-IDLE]
[2025-09-12 18:47:21.713] [nas] [debug] NAS timer[3511] expired [1]
[2025-09-12 18:47:21.713] [nas] [debug] Initial registration required due to [T3511-EXPIRY-IN-ATT-REG]
[2025-09-12 18:47:21.713] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2025-09-12 18:47:21.713] [nas] [debug] Sending Initial Registration
[2025-09-12 18:47:21.713] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2025-09-12 18:47:21.713] [rrc] [debug] Sending RRC Setup Request
[2025-09-12 18:47:21.713] [rrc] [info] RRC connection established
[2025-09-12 18:47:21.713] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2025-09-12 18:47:21.713] [nas] [info] UE switches to state [CM-CONNECTED]
[2025-09-12 18:47:36.728] [nas] [debug] NAS timer[3510] expired [1]
[2025-09-12 18:47:36.728] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2025-09-12 18:47:36.728] [nas] [info] Performing local release of NAS connection
[2025-09-12 18:47:36.728] [nas] [info] UE switches to state [MM-DEREGISTERED/ATTEMPTING-REGISTRATION]
[2025-09-12 18:47:36.728] [rrc] [info] UE switches to state [RRC-IDLE]
[2025-09-12 18:47:36.728] [nas] [info] UE switches to state [CM-IDLE]
```

(a)

```
root@c5d093ef45d0:/ueransim# ping -I uesimtun0 google.com
ping: SO_BINDTODEVICE uesimtun0: No such device
```

(b)

**Figure 7.9:** A legitimate UE cannot connect to the network and has no Internet connectivity during the attack: (a) the UE logs and (b) the result of a ping command (UERANSIM).

### 7.3.3. Reflections

The results of our flooding attack prototype using UERANSIM and free5GC can be interpreted differently depending on the goal of the attack. In terms of resource utilization, we did not manage to meaningfully overload the network, with the memory consumption being negligible for the gNB and the AMF, and the CPU usage of the gNB, despite being noticeable, not reaching critical levels. Furthermore, with the implementation using dynamic unordered maps, there is no clear maximum number of RRC connections other than the maximum size of a C++ unordered map or the limit based on the allocated RAM, both of which are not feasible to reach in our experimental setting. Regarding the gNB crash, while it would be a desirable outcome for an attacker in a real-world 5G network, we see it as an implementation bug rather than a successful attack outcome. As it turns out, a similar issue[1] was already submitted in the UERANSIM repository in 2022, which, at the time of writing, still remains open and unanswered.

On the other hand, if the primary goal of the attack is to distract the gNB and cause a DoS for legitimate UEs trying to connect to the network, then the attack prototype can be considered successful. If distracting the gNB is the only goal and neither the number of stored RRC contexts nor the amount of NAS *Registration Request* messages reaching the AMF matter for the attack, then new UE processes can be created non-stop without waiting between batches (in other words, using a `while true` loop without the flooding rate parameter). This can further increase the CPU utilization of the gNB, although it also makes it much more likely to crash. It is not fully clear, however, if such gNB distraction and a DoS of a legitimate UE can also be performed if the lower layers of the radio stack are not simulated. This motivates the need to further develop and test our flooding attack using OpenAirInterface, which implements the entire 5G NR stack.

[1] `https://github.com/aligungr/UERANSIM/issues/575`

## 7.4. Attack implementation (OpenAirInterface)

In this section, we build on top of our attack prototype and implement the actual flooding attack using OpenAirInterface (OAI) [322] in the RF simulation mode. Unlike UERANSIM, OAI implements the entire radio protocol stack, which is a more realistic scenario, allowing us to test the attack using real SDR devices (see subsection 7.5.1). Furthermore, OAI supports the gNB split option 2-1 [52, 19], where PDCP and RRC terminate in the gNB-CU and the lower layers terminate in the gNB-DU. Therefore, we can test two different deployment modes for each experiment. Below, we describe the experimental setup specific to OAI and then present the results for each of the two experiments for each of the two deployment options (i.e. with and without the gNB split).

### 7.4.1. Experimental setup

For the 5G core network, we rely on the official Docker images from the OpenAirInterface Software Alliance [322]. For the UE and the gNB, we build our own image based on the modified OAI source code, which can be found in our GitHub fork [421]. However, there are some differences in the attack implementation compared to UERANSIM. First, each OAI UE software modem starts an SDR and has a high memory consumption (taking around 400 MB of RAM in a Docker container). As a result, starting new UEs as background processes like we did with UERANSIM is neither feasible nor practical in a real-world setting. Therefore, we run a single UE softmodem and reuse the allocated radio resources. This way, despite losing parallelization, the setup for our flooding attack becomes realistic.

Furthermore, unlike with UERANSIM, all UL messages are dynamically scheduled at the MAC layer by a generic UL scheduler running in a separate thread. Longer RRC and NAS messages are segmented by the RLC layer and may be transmitted separately. These segments also need to be acknowledged if running in RLC Acknowledged Mode (AM), which is the case for all CP messages starting from *RRCSetupComplete*. Thus, to make sure that the gNB receives the *RRCSetupComplete* with the *Registration Request*, the UE restarts the RA procedure as soon as the first RRC *DLInformationTransfer* message is received, containing either *Authentication Request* or *Registration Reject*, depending on the experiment (the message itself is discarded without processing). This is similar to the approach used in the original attack by Kim et al. [215]. The RRC connection is dropped by the RRC layer, which instructs the MAC layer to reset the configuration and restart the RA procedure, and releases the established RLC/PDCP radio bearers. In addition, the UE ignores any *RRCReject* messages with the wait timer and instead restarts the RA procedure, as if a *DLInformationTransfer* message was received.

Similar to UERANSIM, we also limit the CPU and memory resources for the UE, gNB, and AMF containers. In particular, we allocate:

- 15.0 CPU cores and 4 GB of RAM to the UE (attacker) container
- 3.0 CPU cores and 2 GB of RAM to the gNB container, to accommodate for the extra processing in the radio stack (in case of a split, these are the resources for the gNB-DU container, while the gNB-CU container gets 1.0 CPU core and 1 GB of RAM)
- 1.0 CPU core and 1 GB of memory to the AMF container

For other details regarding the experimental setup for OAI, as well as the instructions on how to run the experiments and create plots, see our thesis repository [420].

### 7.4.2. Results

The resource utilization of the gNB, AMF, and UE containers during the flooding attack is shown in Figure 7.10, Figure 7.11, and Figure 7.12, respectively. The same statistics for the gNB split are presented in Figure 7.13 (gNB-DU), Figure 7.14 (gNB-CU), Figure 7.15 (AMF), and Figure 7.16 (UE). Similar to the UERANSIM experiments, we started the attack after around 10 seconds of fetching Docker statistics in order to show the baseline usage before the attack.

The results for the memory utilization are similar to the results for the attack prototype using UERANSIM. For both experiments and regardless of whether the gNB is deployed fully or as a split, the flooding attack shows no noticeable effects on the memory consumption of the targeted components within the tested time period, even though the baseline is already very high for the gNB and gNB-DU (around 69% or 1.39 GiB). While it might seem that the created RRC contexts use little memory and are insufficient

to overload the base station, this is not the case, as OAI sets a limit on the maximum number of allowed UEs that are served by a single gNB (this will be discussed in more detail later in this subsection). As for the UE container, its memory usage remains stable at around 430 MiB (which is around 10% of the allocated 4 GiB) for the entire duration of the attack (with and without the gNB split). This is because only one UE software modem is used to flood the gNB.

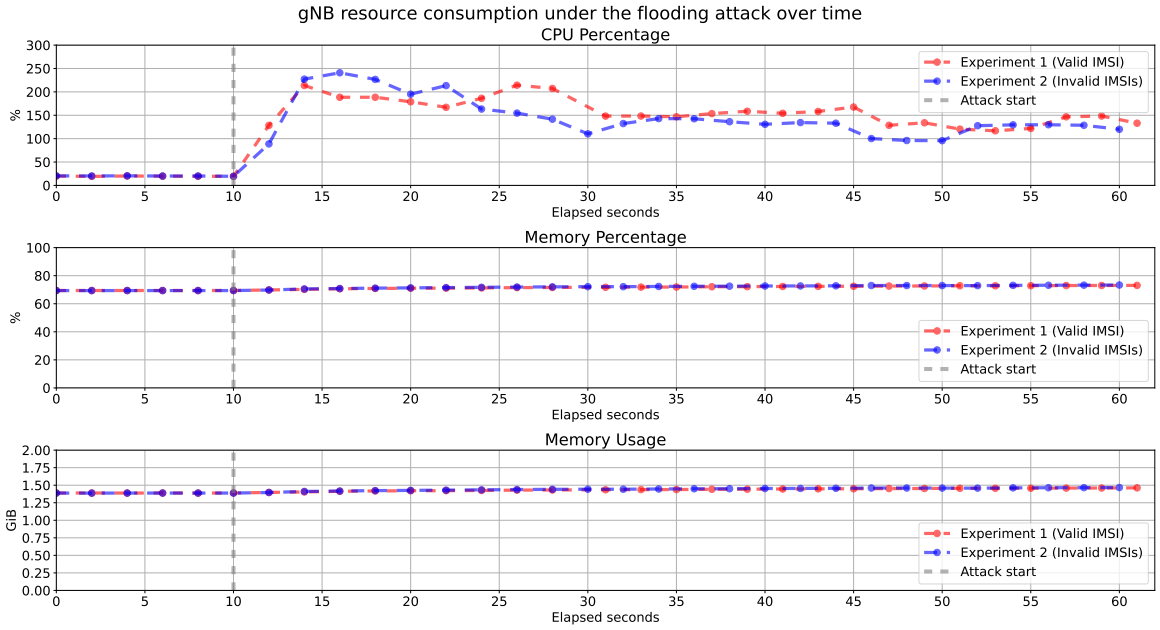



**Figure 7.10:** CPU and memory usage of the gNB container during the flooding attack (OAI, full gNB).

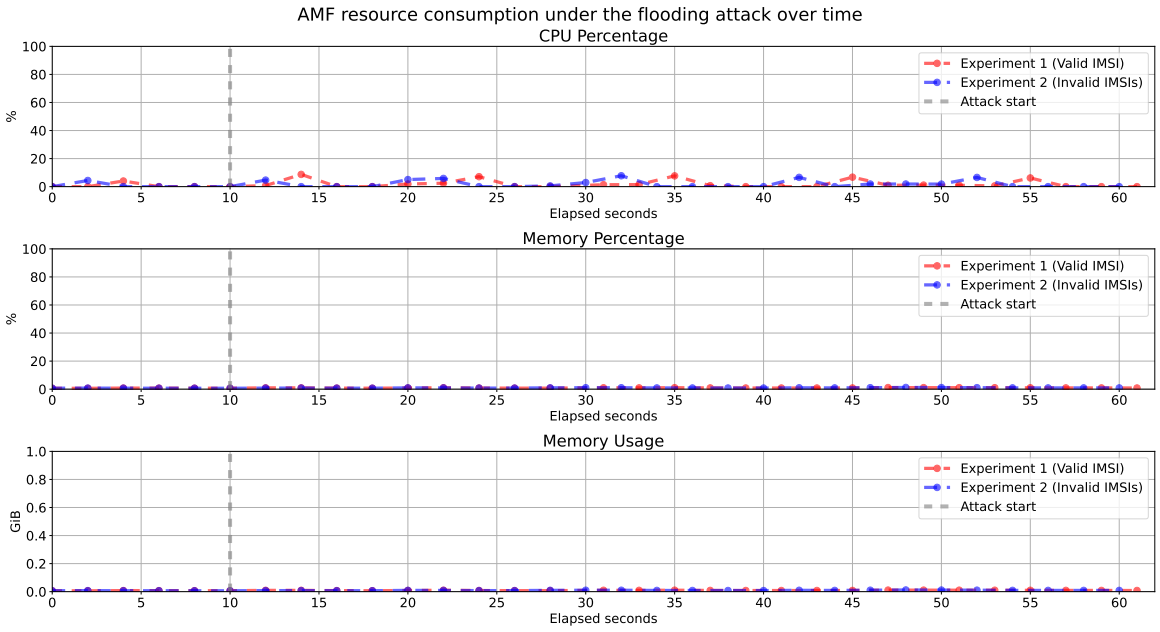



**Figure 7.11:** CPU and memory usage of the AMF container during the flooding attack (OAI, full gNB).

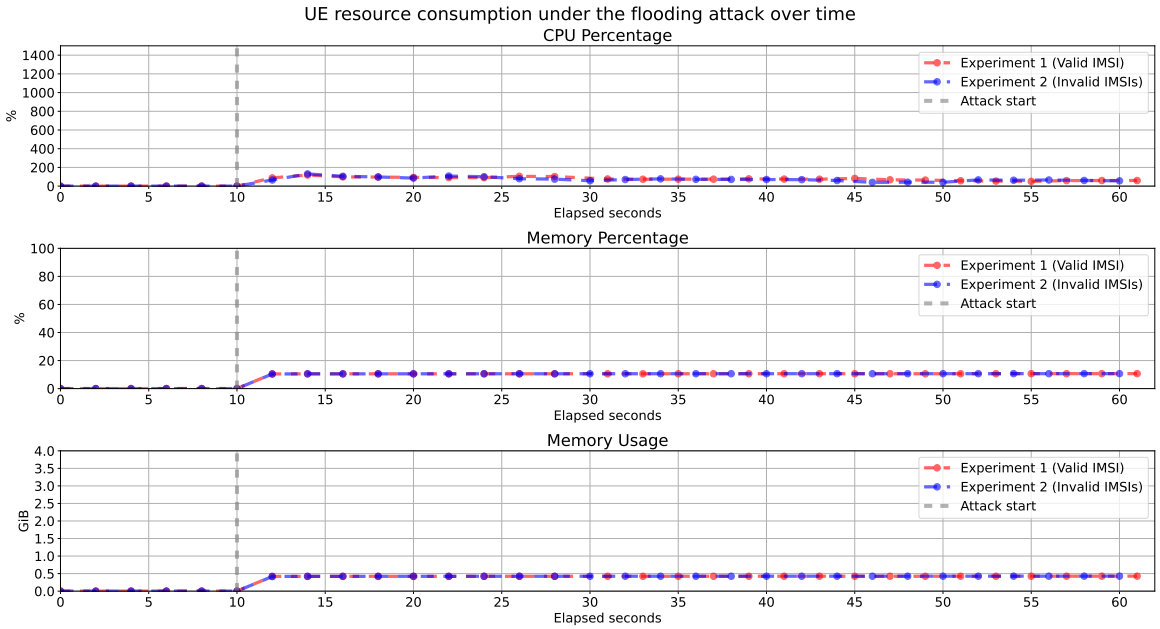



**Figure 7.12:** CPU and memory usage of the UE container during the flooding attack (OAI, full gNB).

As was the case with UERANSIM, the impact on the CPU utilization of the targeted containers is more noticeable, with similar results for both experiments. Given that most of the heavy radio processing (such as encoding, decoding, and scheduling) happens in the lower layers, the gNB-CU is idle most of the time (with < 5% CPU usage). On the other hand, full gNB and gNB-DU have around 20% utilization before the attack starts, going over 100% and at times getting close to or even above 200% during the attack (i.e. 2 of the 3 allocated cores). Since the UE keeps performing the RA procedure even when the limit on the allowed UEs is reached, the gNB(-DU) is constantly busy accepting new UEs that are then rejected using *RRCReject* (which is ignored by our UE). The CPU usage of the AMF remains very low during the entire attack (< 5%). This is not surprising, as it is not the main target of our attack, and because the UEs rejected with an *RRCReject* due to the limit in the gNB do not reach the AMF.

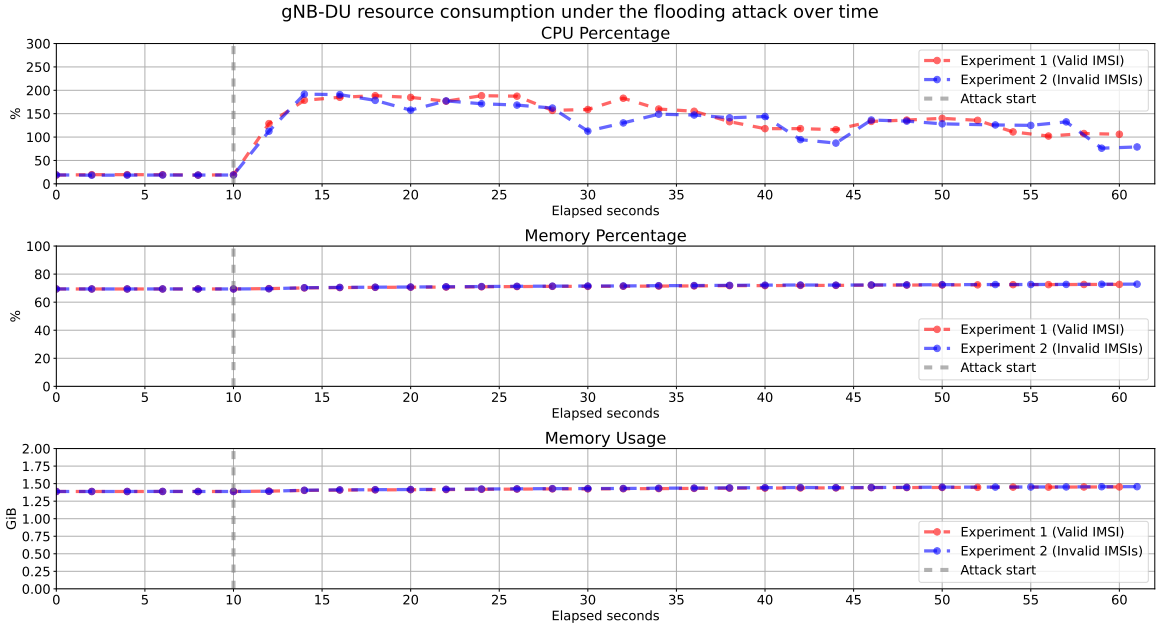



**Figure 7.13:** CPU and memory usage of the gNB-DU container during the flooding attack (OAI, gNB split).

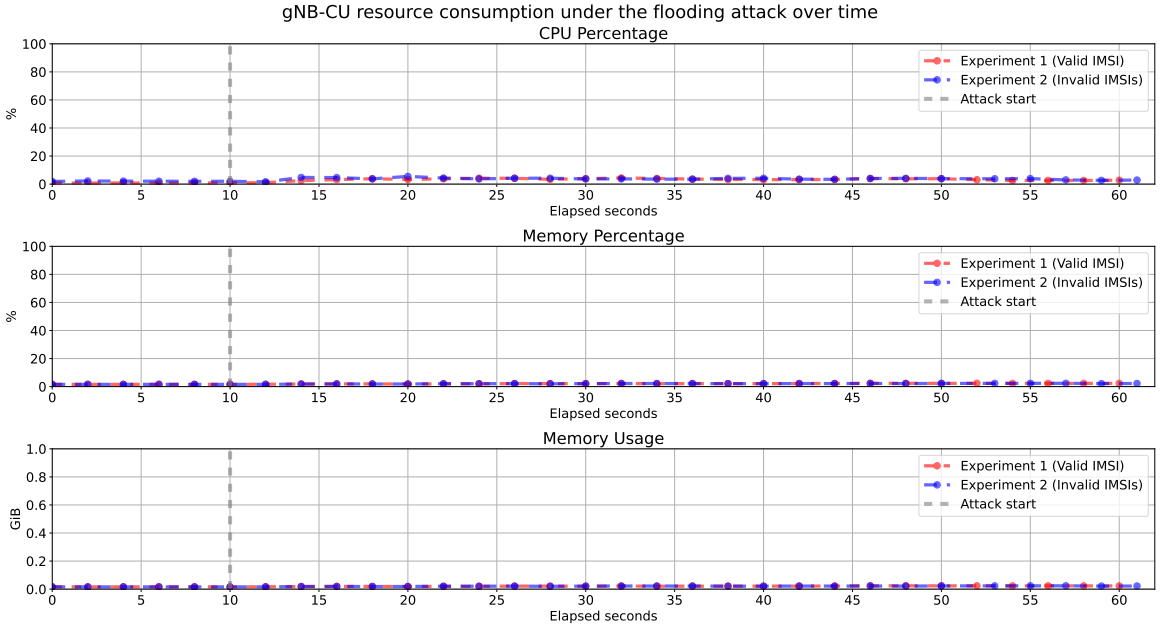



**Figure 7.14:** CPU and memory usage of the gNB-CU container during the flooding attack (OAI, gNB split).

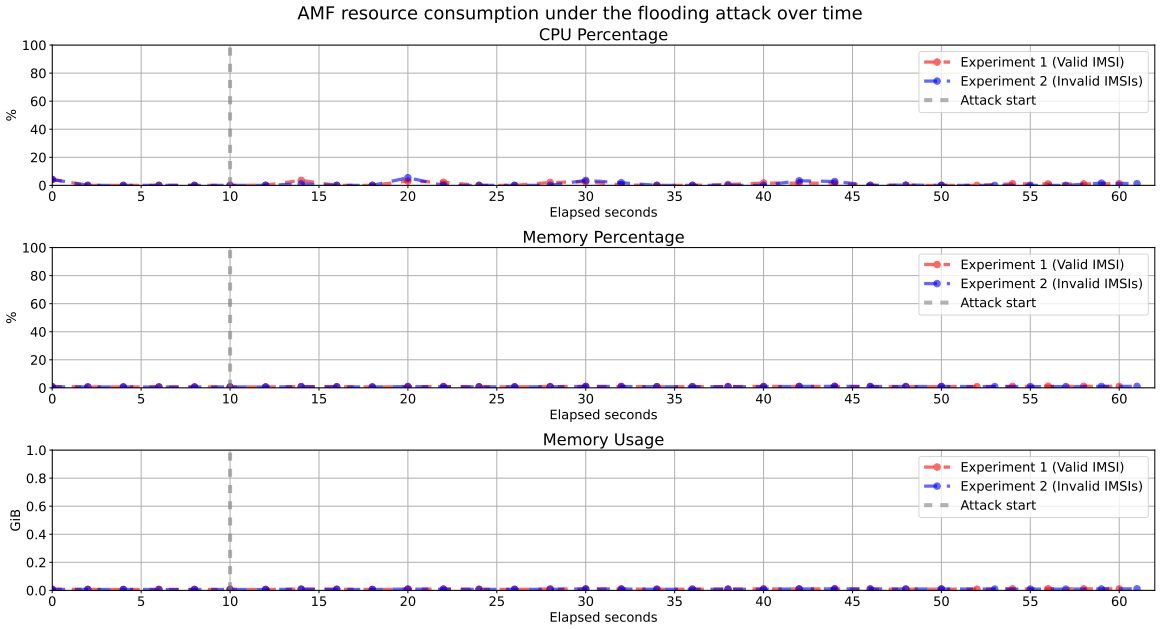



**Figure 7.15:** CPU and memory usage of the AMF container during the flooding attack (OAI, gNB split).

Unlike with UERANSIM, however, the CPU consumption of the UE remains very low, mostly between 60% and 120% throughout the entire attack, which is considerably less than the 15 cores allocated to the container. This can be attributed to the fact that we only run one UE softmodem due to the considerations discussed in the experimental setup (see subsection 7.4.1), whereas many lightweight UERANSIM UEs run as independent background processes, allowing for parallelization. As a result, the OAI UE did not need as many CPU resources as it was allocated, and it could have reached the same results if it was given only 2-3 cores.

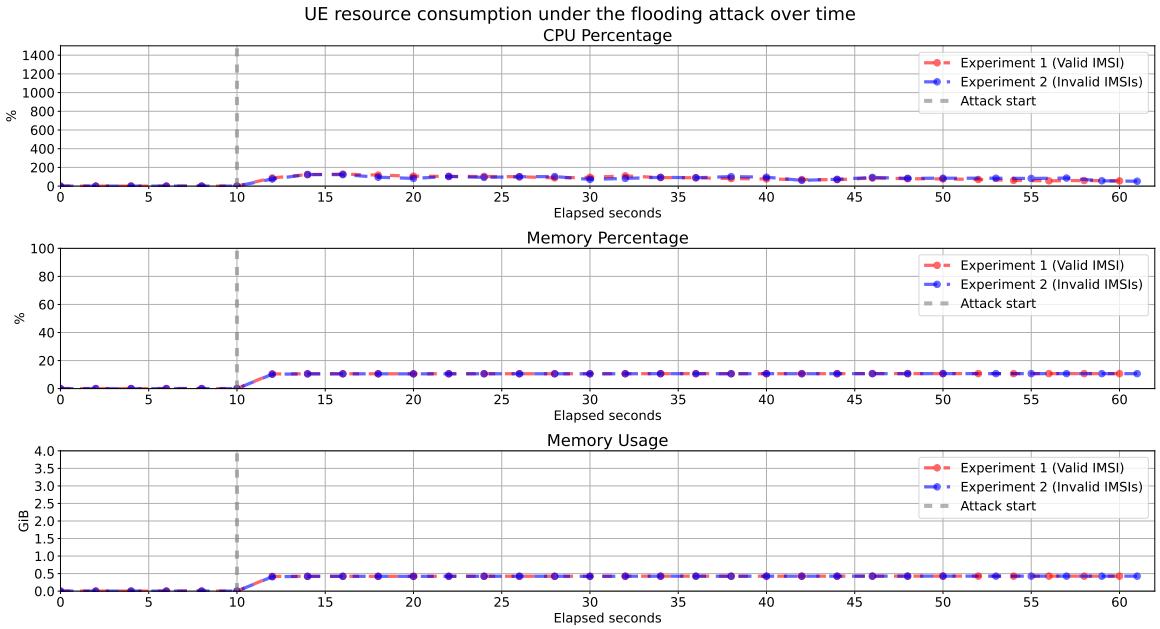



**Figure 7.16:** CPU and memory usage of the UE container during the flooding attack (OAI, gNB split).

When it comes to RRC connections stored in the gNB during the attack, there are a couple of observations we can make. First, OAI defines a limit on the number of UEs that can be served by a single gNB, which is set to 16 by default, but can be increased to 64 if using at least 40 MHz bandwidth (which is the case for our experiments). However, this is the maximum supported number that was set by the OAI developers, and we could not increase it further. As a result, we are not able to test a real-world impact of our attack with the OAI gNB implementation. To approximate the number of RRC connections that the UE could establish if there was no threshold, we also count the cumulative number of RRC contexts, including those that are deleted when the UE is rejected with an *RRCReject* once the limit has been reached. Figure 7.17 and Figure 7.18 show the number of active RRC contexts together with their cumulative count during the flooding attack (for full and split gNB, respectively).

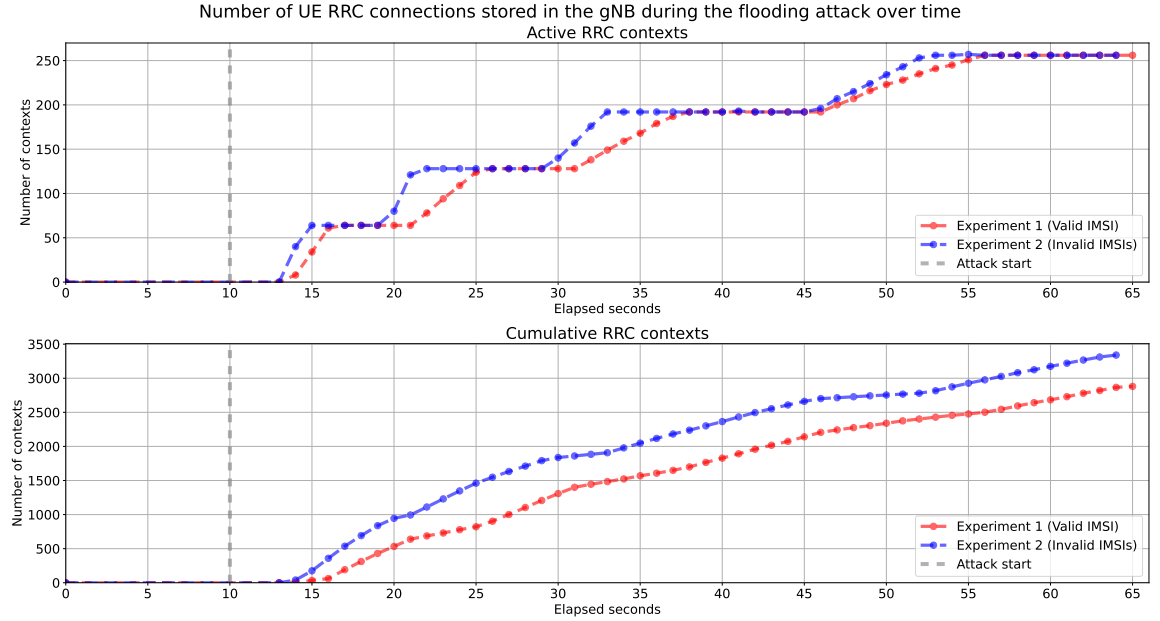



**Figure 7.17:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, full gNB).

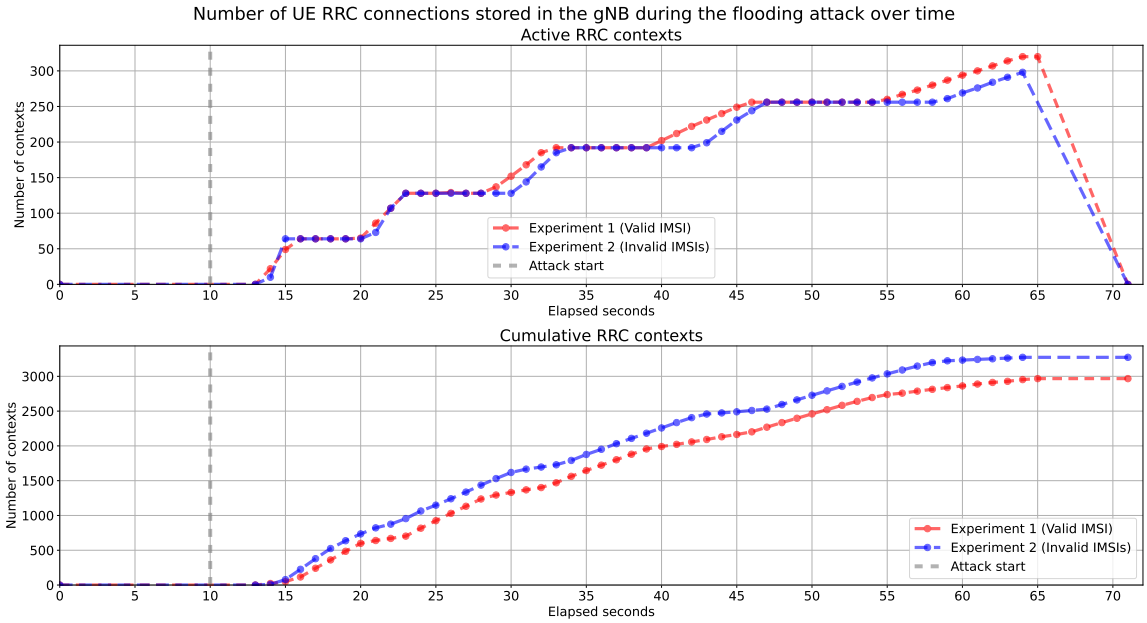



**Figure 7.18:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, gNB split).

Another observation is that successfully established connections are not fully released. As can be seen in Figure 7.17 and Figure 7.18, the line for the active RRC contexts follows a stair-wise pattern. When the number of connections reaches its maximum (which is 64, both at MAC and RRC layers), new UEs are rejected with an *RRCReject* and their corresponding RRC context is released. For the already connected (fake) UEs, after the UL failure timeout expires (which is triggered because the UE is not transmitting anything even if it is expected), the DU part (the MAC layer) requests the CU part (the RRC layer) to start an F1AP UE Context Release procedure [20]. The stale connections are released at the MAC layer and new UEs are accepted, however the respective stale RRC contexts remain at the CU part, so the number of active contexts increases to 128 and further with new batches of connected UEs. Note that the rapid decrease to zero in Figure 7.18 for the gNB split happens because all RRC contexts in the gNB-CU are immediately released when the gNB-DU gets disconnected, which is the case when we shut down the containers at the end of the experiment.

The reason for the observed behaviour is that OAI gNB only releases RRC contexts during internal F1 UE Context Release procedure if requested by the core network, as it could also be that the CU requested the connection release at the DU during normal operation, such as handover. This check was introduced as part of F1 handover implementation[2], while the original functionality for internal F1 UE Context Release[3] was always deleting the RRC connection. In case of our attack, given that the fake UEs will never send any data, there is no need to store their RRC contexts at the CU part. However, the fact that they are not released gives an attacker a way to exhaust gNB resources and possibly cause a DoS, especially in memory-constrained environments (e.g. on board a satellite).

To illustrate this, we performed the flooding attack against a (full) gNB for a longer period of time. In 10 minutes, our rogue UE was able to create around 800 RRC contexts in the gNB, despite the limit of 64 UE connections, with the cumulative number of contexts close to 10,000 (see Figure 7.19). Furthermore, as can be seen in the resource utilization plots in Figure 7.20, the memory usage of the gNB container has also increased by around 200 MB, from 70% to 80%. If such a flooding attack is performed for an even longer amount of time, it could eventually cause the gNB to run out of memory and crash. We have contacted the OAI developers and notified them about this behaviour, but received no response by the time of thesis publication.

[2] `https://gitlab.eurecom.fr/oai/openairinterface5g/-/commit/b01810a8580baec28736d5e7fd89ef6370713b16`
[3] `https://gitlab.eurecom.fr/oai/openairinterface5g/-/merge_requests/2101`

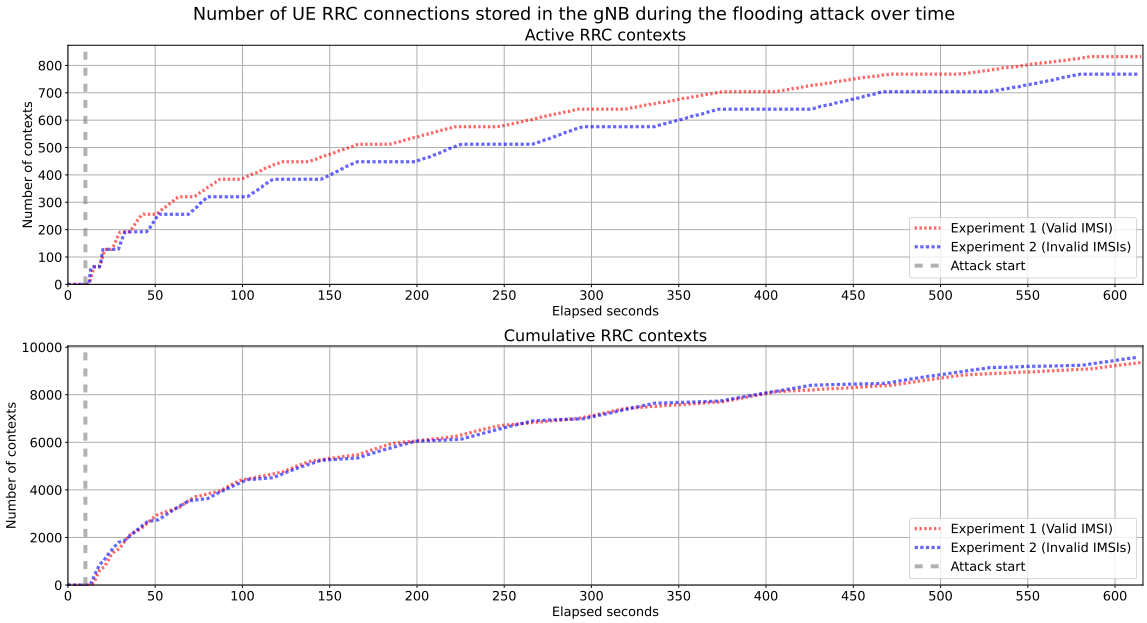



**Figure 7.19:** Active and cumulative RRC connections in the gNB over a longer time during the flooding attack (OAI, full gNB).

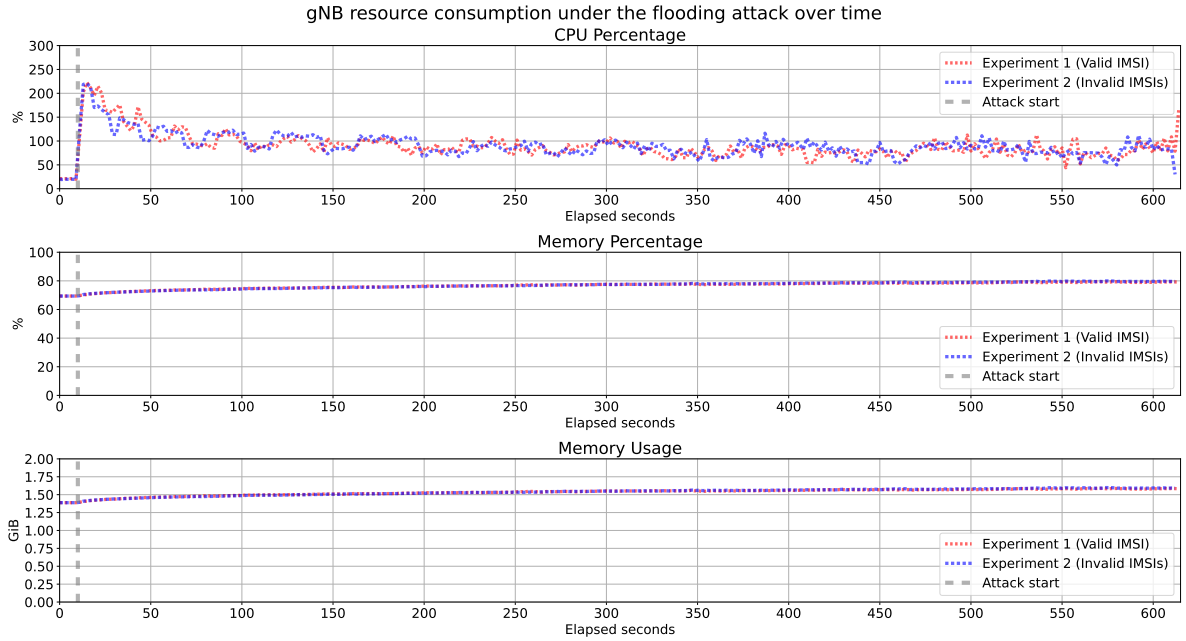



**Figure 7.20:** CPU and memory usage of the gNB container during the flooding attack over a longer time (OAI, full gNB).

Next, we also plot the number of established RRC connections as logged by the UE, which is presented in Figure 7.21 and Figure 7.22 for full gNB and gNB split, respectively. Specifically, a connection is considered established when the UE is done processing the *RRCSetup* and passes the *RRCSetupComplete* with the *Registration Request* to the lower layers to be scheduled for transmission. In addition, we also count the iterations, which correspond to the number of RA restarts triggered by RRC. This happens in two cases: when the UE receives a *DLInformationTransfer* message (with an *Authentication Request* or a *Registration Reject*) or when it receives an *RRCReject* indicating that the gNB cannot establish the connection. The latter is the case when the maximum number of allowed UEs has been reached. We can see that the numbers are consistent with the counts obtained from the gNB logs.

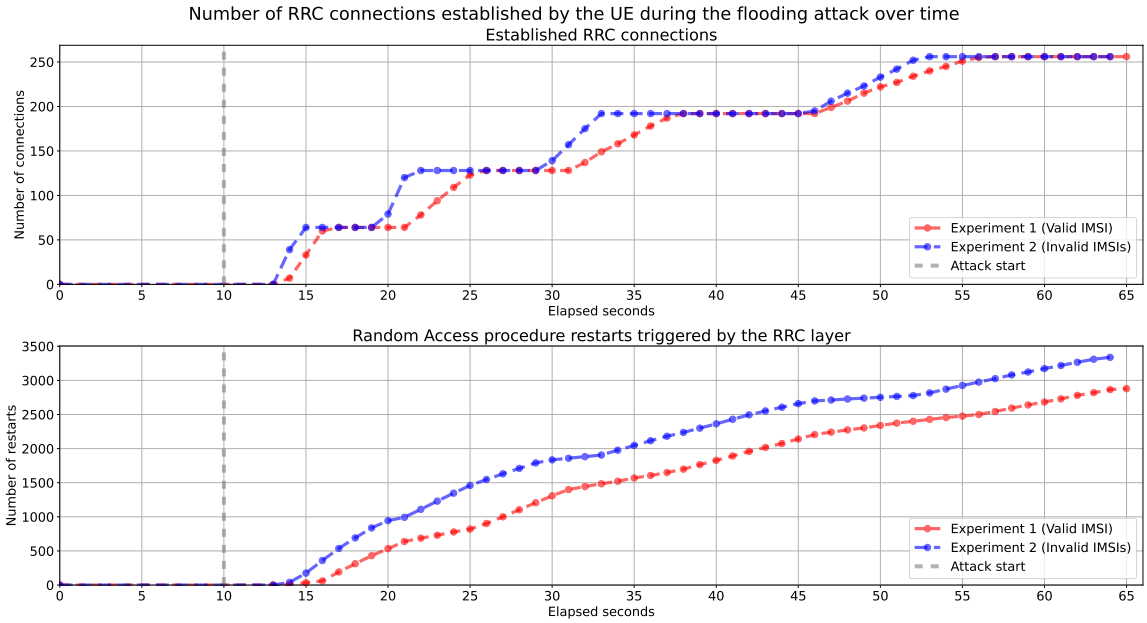



**Figure 7.21:** Established RRC connections and RA restarts by the UE over time during the flooding attack (OAI, full gNB).

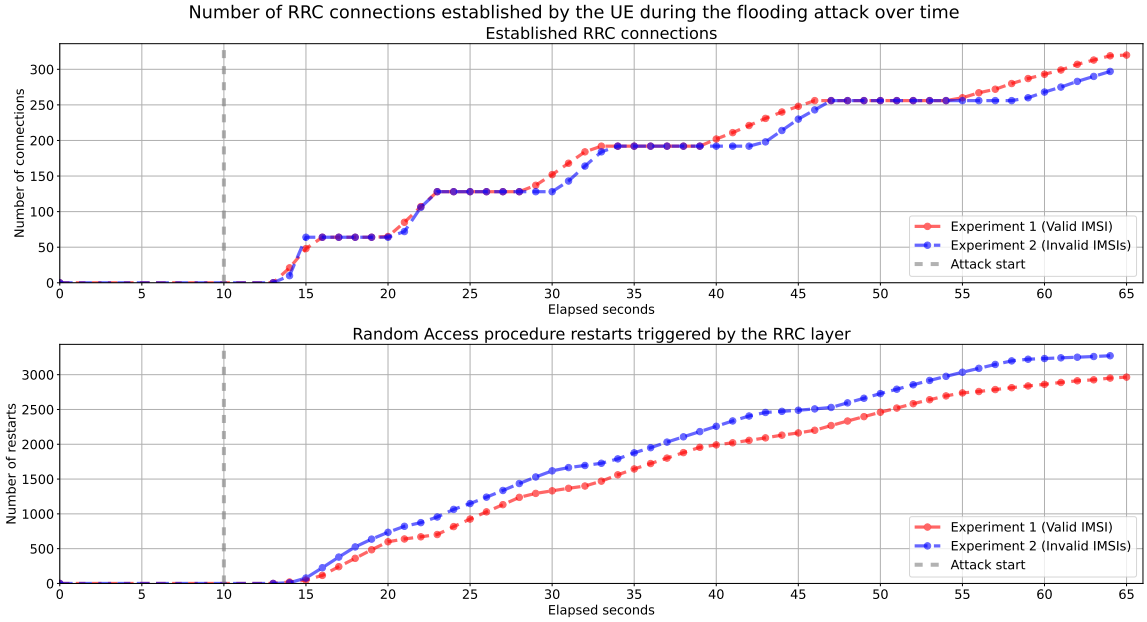



**Figure 7.22:** Established RRC connections and RA restarts by the UE over time during the flooding attack (OAI, gNB split).

To wrap up this section, we perform the same experiment with connecting a legitimate UE to the network during the flooding attack as we did in our attack prototype using UERANSIM. First, we connect a UE to the network during normal conditions (see Figure 7.23). The UE successfully completes the registration procedure, establishes the PDU session, and gets connectivity to the Internet, as indicated by the successful ping command. Next, we start the attack and connect the UE to the network before the limit of 64 UEs is reached (see Figure 7.24). Again, the UE is able to establish the PDU session and reach the Internet. This is different from UERANSIM, where there is no threshold on the allowed UEs, but the victim UE was still not able to connect (likely because UERANSIM does not implement the actual scheduling at the MAC layer). However, the victim UE is not able to connect to the gNB once the limit on the UEs is reached, instead receiving an *RRCReject*, as shown in Figure 7.25.

```
[PHY]   [RRC]UE NR Capability encoded, 10 bytes (86 bits)
[NR_RRC]   UECapabilityInformation Encoded 106 bits (14 bytes)
[NAS]   [UE 0] Received NAS_DOWNLINK_DATA_IND type FGS_REGISTRATION_ACCEPT with length 53
[NAS]   Received Registration Accept with result 3GPP
[NAS]   SMS not allowed in 5GS Registration Result
[NR_RRC]   5G-GUTI: AMF pointer 1, AMF Set ID 1, 5G-TMSI 3450089504
mac a8 d6 16 b
[NAS]   Send NAS_UPLINK_DATA_REQ message(RegistrationComplete)
mac 62 d1 2d d4
[NAS]   Send NAS_UPLINK_DATA_REQ message(PduSessionEstablishRequest)
[RLC]   Added srb 2 to UE 0
[RLC]   Added drb 1 to UE 0
[RLC]   Added DRB to UE 0
[NR_RRC]   RRCReconfiguration includes radio Bearer Configuration
[MAC]   [UE 0] Applying CellGroupConfig from gNodeB
[SDAP]   Default DRB for the created SDAP entity: DRB 1
[PDCP]   Added DRB 1 to UE ID 0
[NR_RRC]   State = NR_RRC_CONNECTED
[NR_RRC]   RRCReconfiguration includes Measurement Configuration
[NR_RRC]   Measurement gaps not yet supported!
[NAS]   [UE 0] Received NAS_CONN_ESTABLI_CNF: errCode 1, length 98
[NR_RRC]   rrcReconfigurationComplete Encoded 10 bits (2 bytes)
[NR_RRC]    Logical Channel UL-DCCH (SRB1), Generating RRCReconfigurationComplete (bytes 2)
[NAS]   Received PDU Session Establishment Accept, UE IPv4: 10.0.0.2
Unknown IEI 129
[OIP]   Interface oaitun_ue1 successfully configured, IPv4 10.0.0.2, IPv6 (null)
[UTIL]   threadCreate() for ue_tun_read_0_p10: creating thread with affinity ffffffff, priority 1
[NR_MAC]   UE 0 RNTI 3593 stats sfn: 896.8, cumulated bad DCI 0
    DL harq: 16/0
    UL harq: 46/0 avg code rate 0.1, avg bit/symbol 2.0, avg per TB: (nb RBs 29.0, nb symbols 5.4)
```

(a)

```
root@cfa2bc6ce8da:/opt/oai-nr-ue# ping -I oaitun_ue1 -c 5 google.com
PING google.com (172.217.23.206) from 10.0.0.2 oaitun_ue1: 56(84) bytes of data.
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=1 ttl=111 time=21.1 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=2 ttl=111 time=22.1 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=3 ttl=111 time=20.5 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=4 ttl=111 time=21.4 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=5 ttl=111 time=20.4 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 20.441/21.087/22.056/0.610 ms
```

(b)

**Figure 7.23:** A legitimate UE successfully connects to the network and has Internet connectivity before the attack: (a) the UE logs and (b) the result of a ping command (OAI).

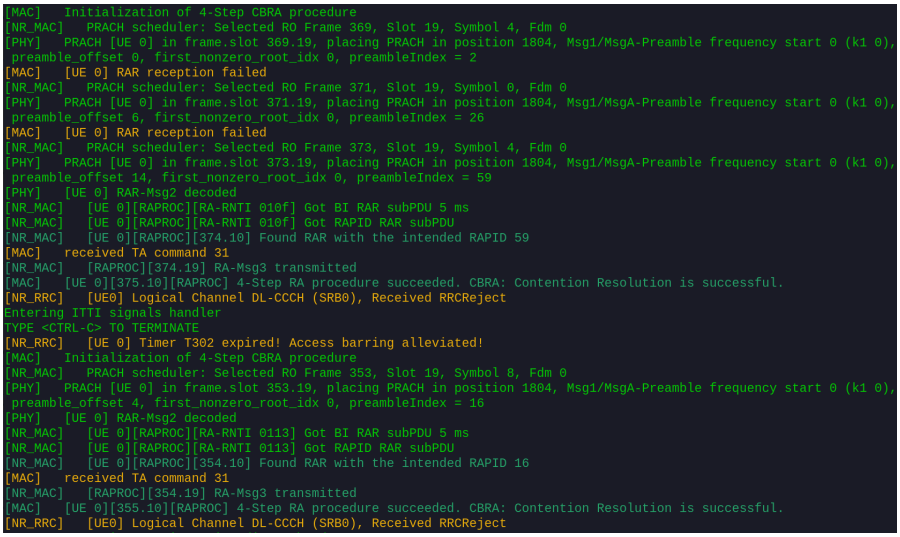
```
[PHY]   [RRC]UE NR Capability encoded, 10 bytes (86 bits)
[NR_RRC]   UECapabilityInformation Encoded 106 bits (14 bytes)
[NAS]   [UE 0] Received NAS_DOWNLINK_DATA_IND type FGS_REGISTRATION_ACCEPT with length 53
[NAS]   Received Registration Accept with result 3GPP
[NAS]   SMS not allowed in 5GS Registration Result
[NR_RRC]   5G-GUTI: AMF pointer 1, AMF Set ID 1, 5G-TMSI 2704003761
mac ed 79 0 f
[NAS]   Send NAS_UPLINK_DATA_REQ message(RegistrationComplete)
mac 67 57 91 e
[NAS]   Send NAS_UPLINK_DATA_REQ message(PduSessionEstablishRequest)
[RLC]   Added srb 2 to UE 0
[RLC]   Added drb 1 to UE 0
[RLC]   Added DRB to UE 0
[NR_RRC]   RRCReconfiguration includes radio Bearer Configuration
[MAC]   [UE 0] Applying CellGroupConfig from gNodeB
[SDAP]   Default DRB for the created SDAP entity: DRB 1
[PDCP]   Added DRB 1 to UE ID 0
[NR_RRC]   State = NR_RRC_CONNECTED
[NR_RRC]   RRCReconfiguration includes Measurement Configuration
[NR_RRC]   Measurement gaps not yet supported!
[NAS]   [UE 0] Received NAS_CONN_ESTABLI_CNF: errCode 1, length 98
[NR_RRC]   rrcReconfigurationComplete Encoded 10 bits (2 bytes)
[NR_RRC]    Logical Channel UL-DCCH (SRB1), Generating RRCReconfigurationComplete (bytes 2)
[NAS]   Received PDU Session Establishment Accept, UE IPv4: 10.0.0.2
Unknown IEI 129
[OIP]   Interface oaitun_ue1 successfully configured, IPv4 10.0.0.2, IPv6 (null)
[UTIL]   threadCreate() for ue_tun_read_0_p10: creating thread with affinity ffffffff, priority 1
[NR_MAC]   UE 0 RNTI 89d3 stats sfn: 512.8, cumulated bad DCI 0
    DL harq: 16/0
    UL harq: 46/0 avg code rate 0.1, avg bit/symbol 2.0, avg per TB: (nb RBs 20.1, nb symbols 8.0)
```

(a)

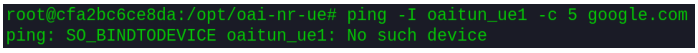
```
root@cfa2bc6ce8da:/opt/oai-nr-ue# ping -I oaitun_ue1 -c 5 google.com
PING google.com (172.217.23.206) from 10.0.0.2 oaitun_ue1: 56(84) bytes of data.
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=1 ttl=111 time=22.2 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=2 ttl=111 time=54.4 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=3 ttl=111 time=57.7 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=4 ttl=111 time=61.9 ms
64 bytes from prg03s05-in-f14.1e100.net (172.217.23.206): icmp_seq=5 ttl=111 time=56.8 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 22.218/50.599/61.921/14.399 ms
```

(b)

**Figure 7.24:** A legitimate UE successfully connects to the network and has Internet connectivity during the attack before the limit on UEs is reached: (a) the UE logs and (b) the result of a ping command (OAI).




(a)




(b)

**Figure 7.25:** A legitimate UE cannot connect to the network and has no Internet connectivity during the attack after the limit on UEs is reached: (a) the UE logs and (b) the result of a ping command (OAI).

### 7.4.3. Reflections

The actual implemented attack was able to achieve its primary objective: the rogue UE was able to quickly reach the maximum number of RRC connections, which aligns with the results obtained by Kim et al. [215] for the original attack on LTE. As a result, we were able to perform a successful Denial-of-Service (DoS) attack against a legitimate subscriber, who was rejected by the gNB and could not get Internet connectivity once the limit on the allowed UEs has been reached.

While 64 UE connections (or 16 connections in the original paper) is not a realistic number for a real-world cellular network, we showed that we were also able to establish much more RRC contexts in the gNB(-CU) than the maximum number of allowed connections, due to a potential vulnerability in the OAI implementation. The fact that UE contexts are released at the MAC layer but not at the RRC layer allows an attacker to eventually exhaust the gNB resources if the attack is performed over a long enough period (in which case the increase in the memory consumption becomes more noticeable, as we have demonstrated in one of our experiments). Given that the attacker can permanently create an RRC context in the gNB, even if the threshold on the allowed UE connections was higher, it would still be possible to reach this limit and create more connections in the gNB, which would not be possible if these contexts were released both in the DU part and in the CU part.

As for the resource utilization, the (low) threshold on the UE connections also restricted the impact on the gNB memory usage, since new contexts were not be allocated until the old connections were released, resulting in a slower increase in memory consumption. The impact on the CPU utilization of the gNB(-DU) was noticeable, although it was not reaching critical levels. For the attacker UE, the resource consumption remained fairly low, since only one software modem was used. Even if the attack was parallelized within the same softmodem, the impact on the OAI gNB resource consumption would likely still be limited, as extra connections would be rejected until the old ones time out.

## 7.5. Attack evaluation (OpenAirInterface)

In this section, we perform an evaluation of our flooding attack, which we have implemented using OAI. We follow a similar approach and experimental setup as in the previous section (see subsection 7.4.1), focusing primarily on the number of UE connections established at the gNB. For a TN setting, we use two USRP B210 devices, one for the UE and one for the gNB(-DU). For an NTN setting, we use the

OAI RF simulator, similar to section 7.4, and configure the relevant NTN parameters and NTN channel simulation to simulate a satellite in a geostationary orbit (GEO) and in a low earth orbit (LEO), both with transparent payload. While GEO satellites are not very likely to be used for 5G networks due to large latencies, we are able to test the impact of higher delays on our flooding attack.

### 7.5.1. Terrestrial setup

The results of the flooding attack against the gNB in a terrestrial setting are shown in Figure 7.26 and Figure 7.27 for the number of UE RRC contexts at the gNB(-CU), and in Figure 7.28 and Figure 7.29 for the number of established RRC connections as logged by the UE.

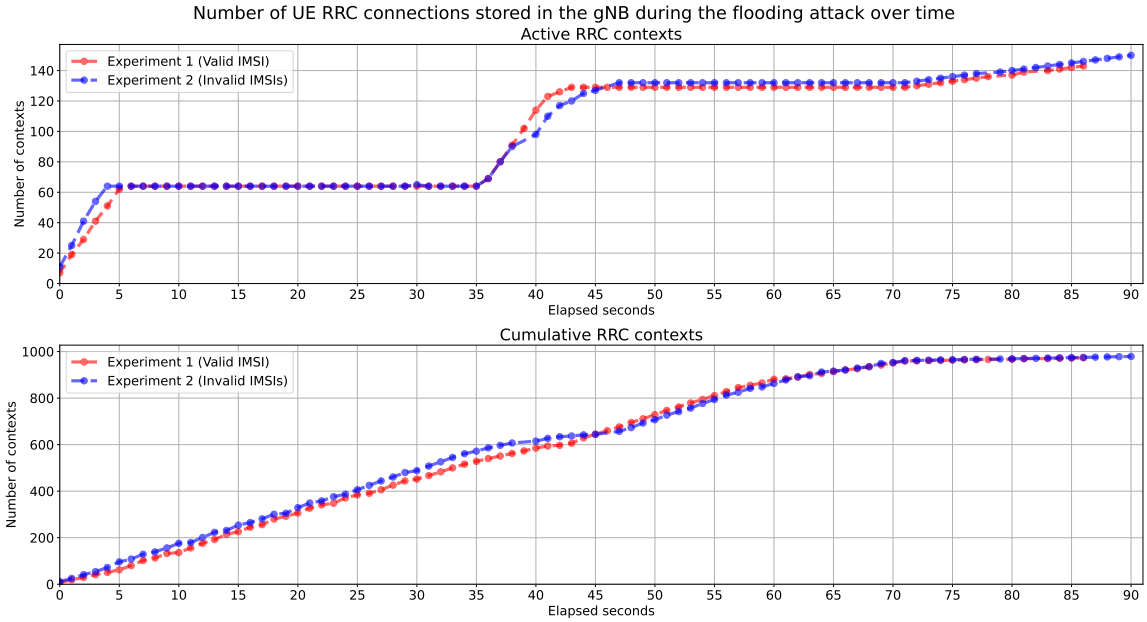



**Figure 7.26:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, SDRs, full gNB).

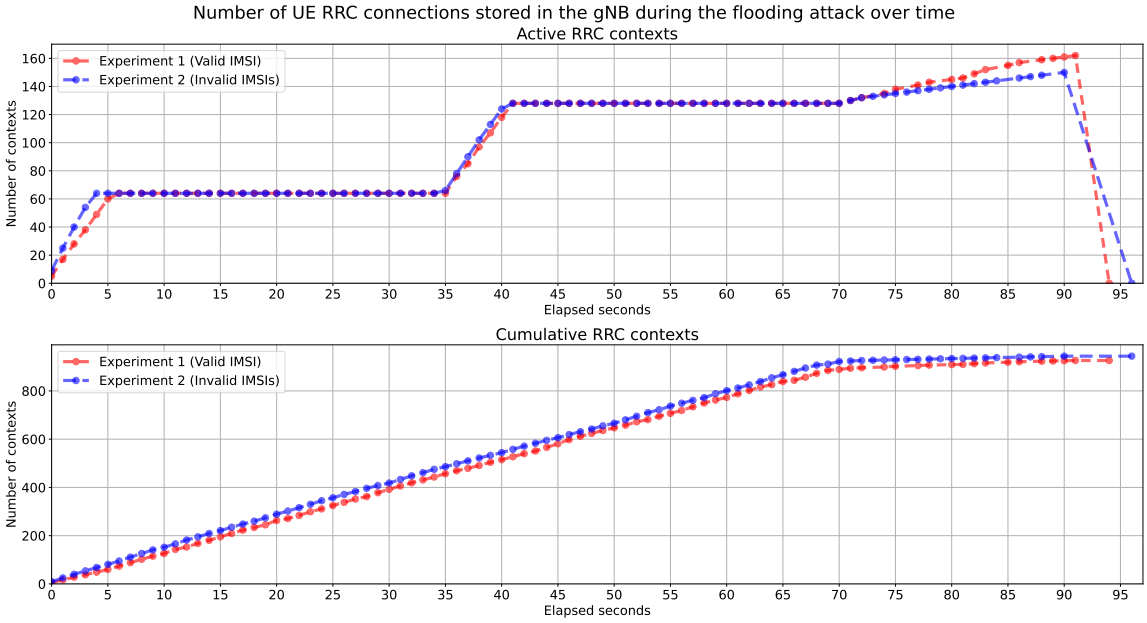



**Figure 7.27:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, SDRs, gNB split).

The results show similar trends to what we observed with the OAI RF simulator (see section 7.4). The UE was able to reach the limit on the maximum number of connections at the gNB, causing the subsequent RRC connection setup requests to be rejected, until the stale connections time out. Overall, the numbers are lower for both active and cumulative contexts at the gNB, because (initial) UE connections are established slower than when RF simulation is used. As a result, the created connections take longer to time out, blocking new connections in the meantime. Similar to OAI RF simulator, we can observe all active RRC contexts being deleted at the gNB-CU at the end of the monitored time period (see Figure 7.27), since we shut down the gNB-DU before stopping gNB-CU.

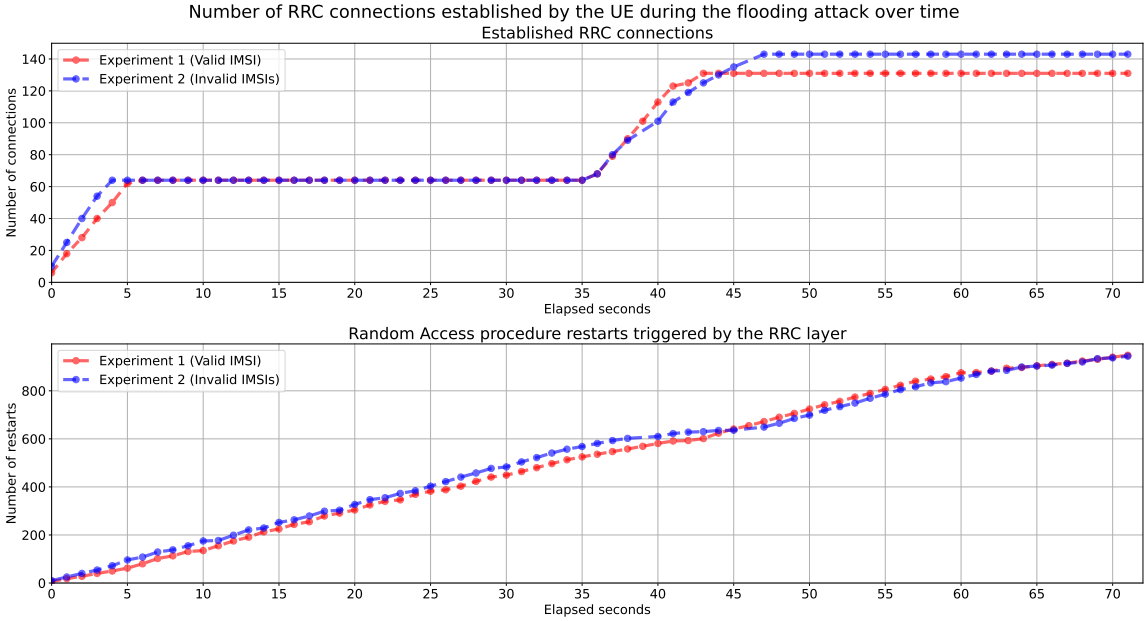



**Figure 7.28:** Established RRC connections and RA restarts by the UE over time during the flooding attack (OAI, SDRs, full gNB).

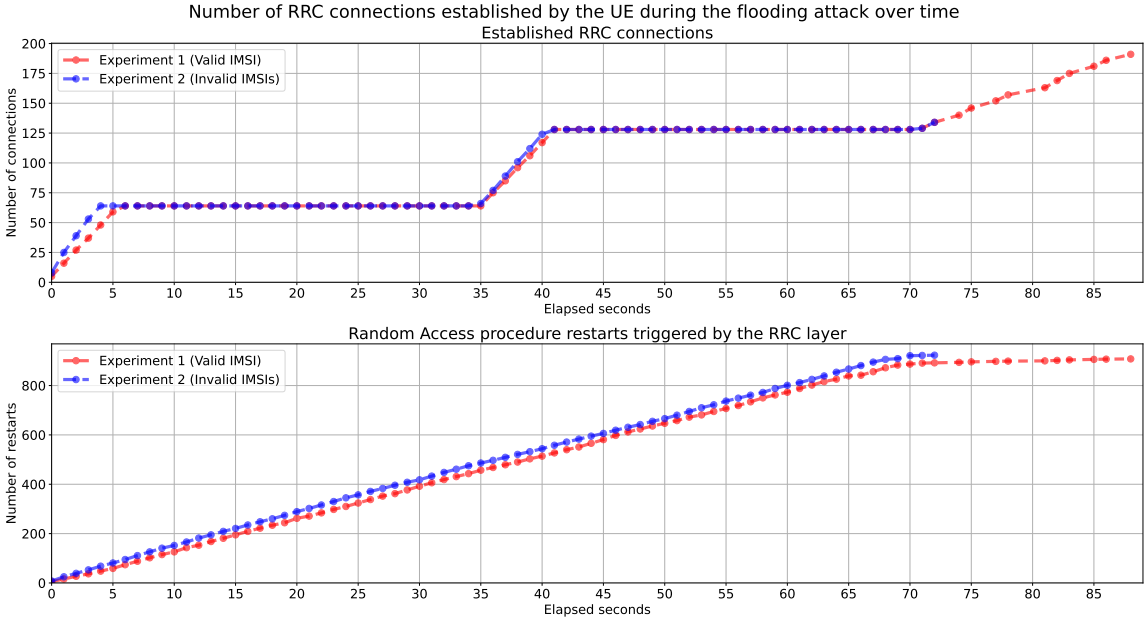



**Figure 7.29:** Established RRC connections and RA restarts by the UE over time during the flooding attack (OAI, SDRs, gNB split).

Unlike with RF simulation, the performance of the attack using real USRP devices decreases after around one minute since the start, which happens due to the issues at the lower layers. The UE starts experiencing problems in the transmission channels, such as RAR reception failure, contention resolution failure, PBCH decoding errors, and reaching the maximum number of transmissions for a Scheduling Request (which triggers the RA procedure restart). In the worst case, the synchronization fails and the UE cannot connect to the gNB any more. This is also reflected in the differences between the counts in the gNB plots (see Figure 7.26 and Figure 7.27) and in the UE plots (see Figure 7.28 and Figure 7.27) at the end of the monitored time period. Given that the UE logs the established RRC connections and RA restarts only when receiving either *RRCReject* or *DLInformationTransfer*, some connections might not be logged if the UE had to restart the RA procedure in the lower layers (e.g. due to SR failures) after the RRC connection has been established.

However, the observed decrease in the attack performance happens primarily due to the physical layer and the MAC layer, and not because of a problem in the methodology of our attack. We believe that these issues can be addressed with some tweaks at the physical and MAC layers, better synchronization parameters, and with more powerful SDR devices.

### 7.5.2. Non-terrestrial setup

For NTN experiments, we use the configuration files provided by OAI. Since these files use 5 MHz bandwidth (compared to 40 MHz bandwidth in all previous experiments), we have to decrease the maximum number of UEs per gNB to 16 to make the gNB work. The NTN configuration adds some parameters to cope with larger NTN propagation delays, such as *cellSpecificKoffset*, *ta-Common*, and *ta-CommonDrift*, as well as ephemeris data (satellite position and velocity vectors) [321]. For a GEO satellite, a propagation delay of 238.74 ms is added to the RF simulator. For a LEO satellite, a channel model in the RF simulator simulates the delay and Doppler shift for a circular orbit located at 600 km height using a Matlab function. In both cases, a satellite with transparent payload is assumed, so the gNB (full or split) remains on the ground. Therefore, the main focus of our NTN experiments is the impact of latencies and other NTN-related parameters on the attack.

The results for a GEO satellite are presented in Figure 7.30 for full gNB and Figure 7.31 for gNB split, with both figures showing the number of RRC contexts stored in the base station. The corresponding resource utilization plots for the gNB and gNB-DU are shown in Figure 7.32 and Figure 7.33, respectively. Note that the drop to zero at the end of the monitored period in Figure 7.31 happens because all RRC contexts are released in the gNB-CU when the gNB-DU disconnects on shutdown.

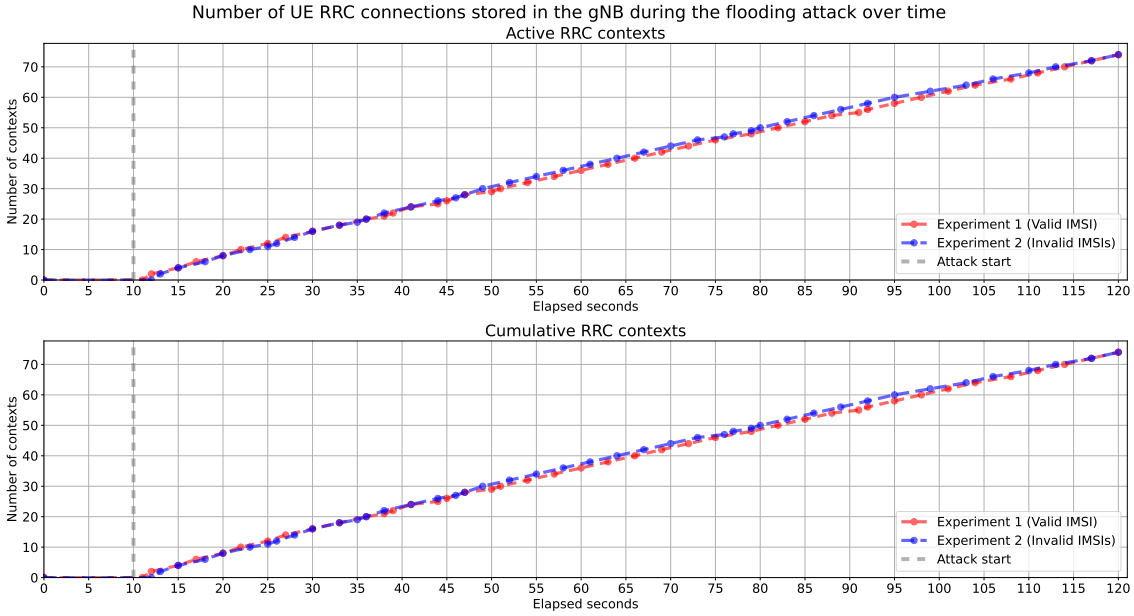



**Figure 7.30:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, GEO, full gNB).

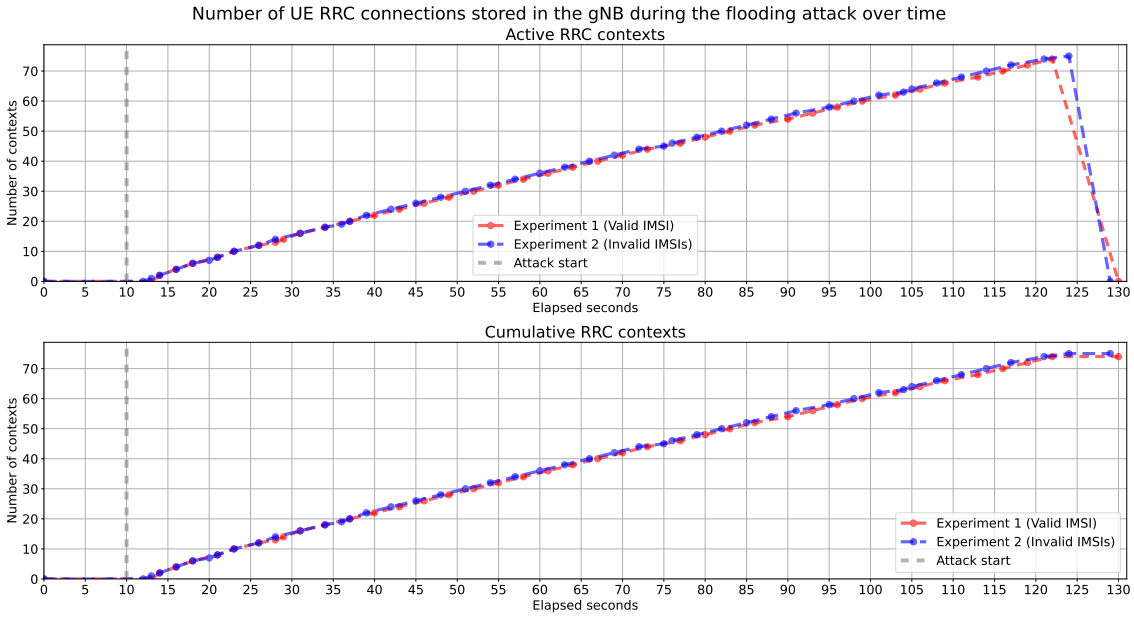



**Figure 7.31:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, GEO, gNB split).

As can be seen in Figure 7.30 and Figure 7.31, the cumulative count of RRC contexts coincides with the number of active RRC contexts in the gNB. This is different from all the experiments performed so far, where the number of cumulative contexts was always higher. Furthermore, both counts grow linearly, rather than in a step-wise pattern. Due to the high propagation delay from the UE to the GEO satellite to the gNB on the ground, the rogue UE needs more time to reach the threshold of 16 connected UEs. As a result, by the time this limit is reached, some stale UE connections have already timed out, allowing new contexts to be established. Normally, if old UE connections were released both in MAC and RRC layers, it would greatly reduce the practical impact of the attack. However, with the current OAI behaviour, every RRC connection that the attacker establishes gets stored in the gNB, and the total number of established RRC connections goes over the maximum allowed number of UEs.

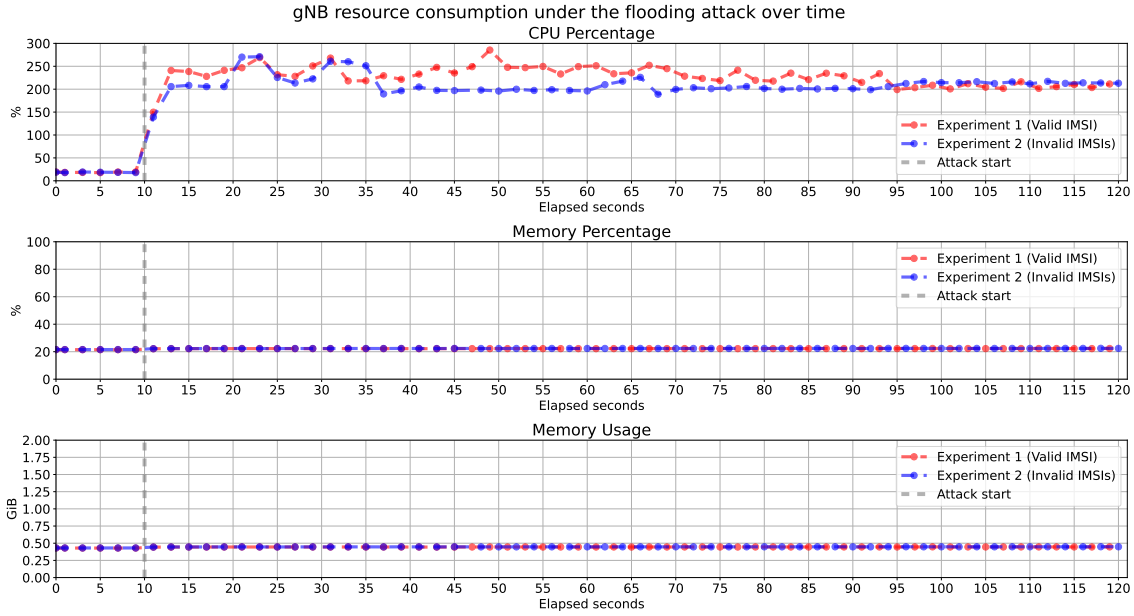



**Figure 7.32:** CPU and memory usage of the gNB container during the flooding attack (OAI, GEO, full gNB).

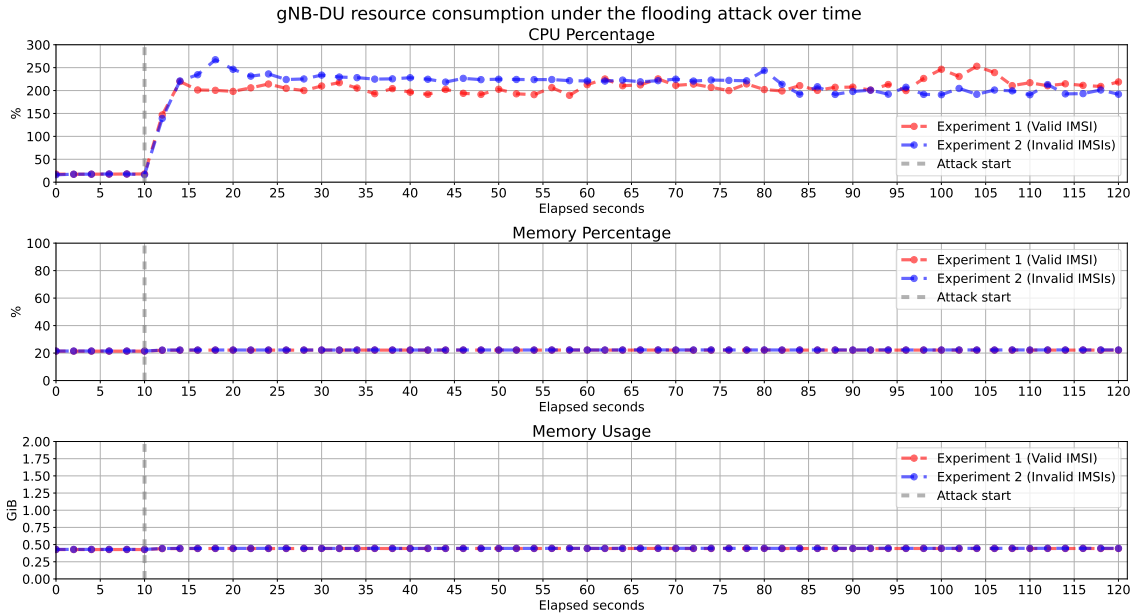



**Figure 7.33:** CPU and memory usage of the gNB-DU container during the flooding attack (OAI, GEO, gNB split).

Figure 7.32 and Figure 7.33 show the resource utilization of the on-ground gNB and gNB-DU when a GEO satellite is simulated. Since other components like the gNB-CU and the AMF were not meaningfully affected in terms of resource usage in the previous TN experiments (see subsection 7.4.2), we did not measure their performance. Regardless if the gNB split is used or not, given that fake UE connections take longer to be established, the impact on the memory consumption is not noticeable within the monitored time frame. In addition, since the gNB can serve at most 16 UEs (compared to 64 UEs in all previous experiments), the baseline memory usage is already very low (around 21% or 440 MiB, compared to 69% or 1.39 GiB for the experiments in subsection 7.4.2). As for the CPU utilization, it is initially low (< 20%) but stays over 200% and sometimes even goes above 250% during the attack, which is higher than for the previous experiments. We believe this can be attributed to the physical layer and different configuration parameters, as new UE connections are established very slowly.

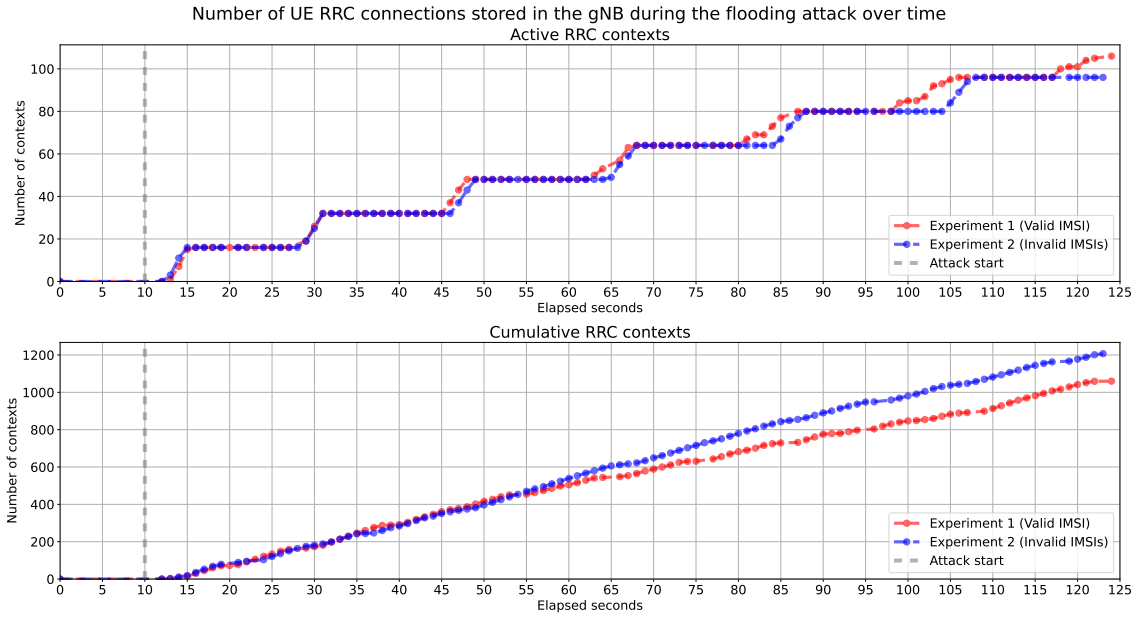



**Figure 7.34:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, LEO, full gNB).

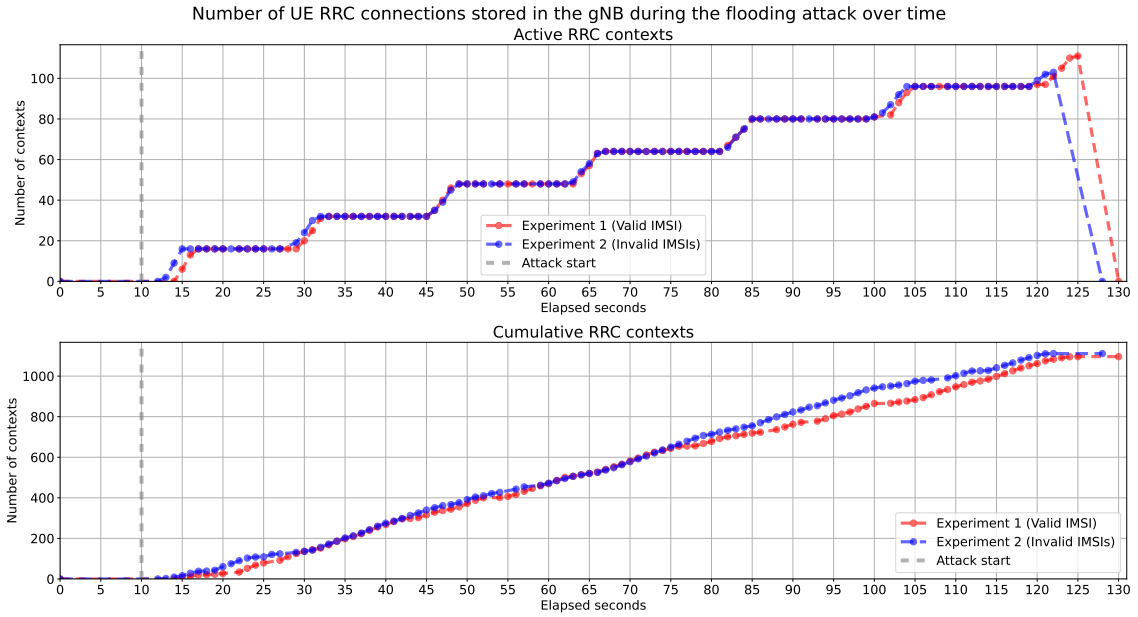



**Figure 7.35:** Active and cumulative RRC contexts in the gNB over time during the flooding attack (OAI, LEO, gNB split).

The results for a simulated LEO satellite, as presented in Figure 7.34 and Figure 7.35, show similar trends to the TN experiments, following a step-wise pattern for the active RRC contexts in the gNB. Since the threshold on the allowed UEs is lower (16 UEs compared to 64 UEs), this limit is reached quicker than in TN experiments. Furthermore, given that the propagation delay for the LEO satellite is much lower than for the GEO satellite (around 20 ms compared to 238.74 ms), the UE actually manages to reach the limit, with subsequent UEs being rejected until stale connections time out. Still, the latency to reach the gNB is higher than in a normal TN setting, so the numbers for both active and cumulative RRC contexts in the gNB established within one minute is lower than in TN experiments using real SDR devices (see subsection 7.5.1) and much lower than in TN experiments using the OAI RF simulator (see subsection 7.4.2).

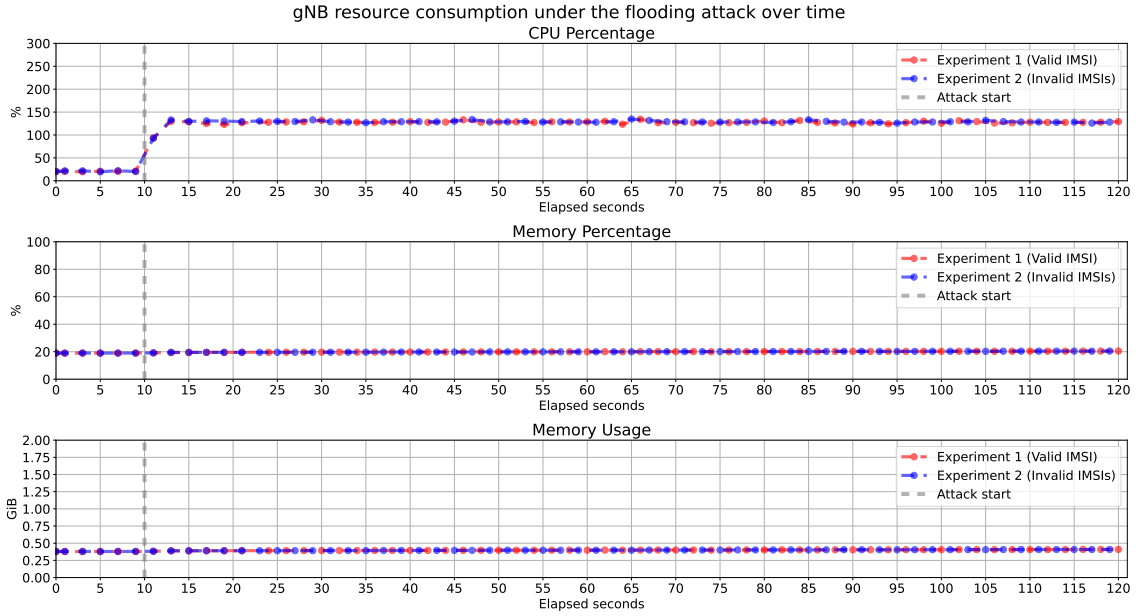



**Figure 7.36:** CPU and memory usage of the gNB container during the flooding attack (OAI, LEO, full gNB).

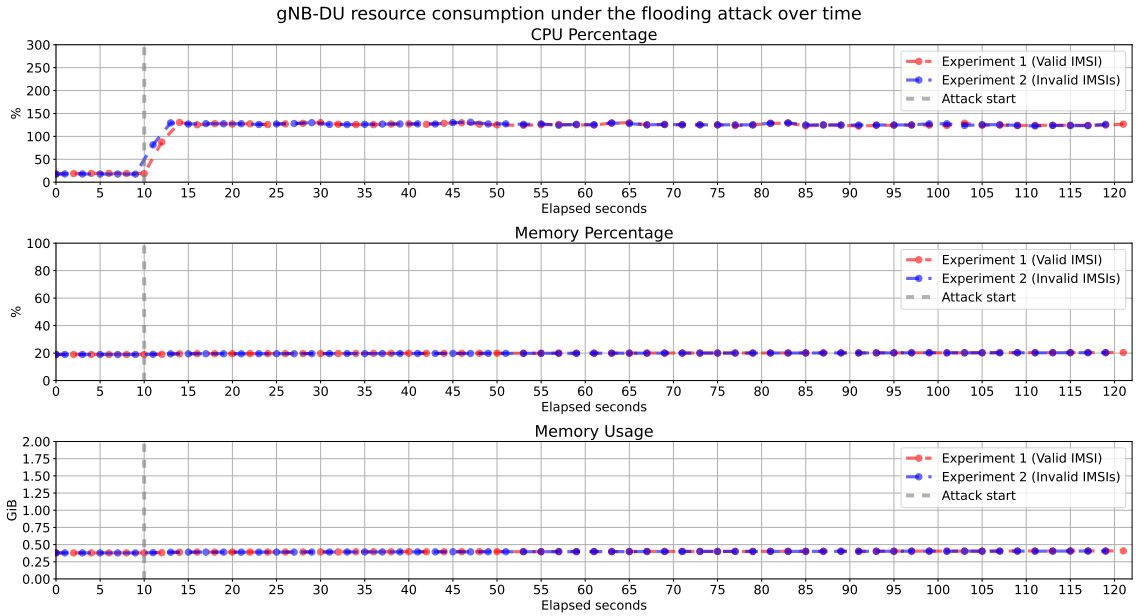



**Figure 7.37:** CPU and memory usage of the gNB-DU container during the flooding attack (OAI, LEO, gNB split).

Finally, the resource utilization for the on-ground gNB and gNB-DU when using a simulated LEO satellite (see Figure 7.36 and Figure 7.37) is also comparable to the corresponding results obtained for the TN experiments using the OAI RF simulator (see subsection 7.4.2). Similar to the GEO satellite, the resource consumption remains very low for the baseline due to the lower number of supported UEs at the gNB, with the memory utilization not having a noticeable impact within the monitored time period. On the other hand, the CPU usage remains below 150%, which is lower than for the experiments involving a GEO satellite, and slightly lower (but more stable) than for the experiments with the OAI RF simulator. We do note that some differences might be related to the configuration parameters, however a clear increase in the CPU utilization is visible during the attack.

### 7.5.3. Reflections

The results that we obtained for the TN experiments using real SDR devices and for the NTN experiments using the OAI RF simulator with NTN-specific configuration are consistent with what we have observed during the attack implementation in section 7.4, even though the counts for the active and cumulative RRC contexts in the gNB (representing the flooding rate) were lower. In all experiments, the UE was able to create more RRC contexts in the gNB than the defined limit on the number of UEs, which happens because the OAI implementation of the gNB does not release the timed out connections at the RRC layer. As for resource utilization, despite some differences, which we believe are caused by the physical layer and different configuration parameters, a noticeable increase in the CPU usage was also observed for the NTN experiments, with the memory consumption remaining fairly stable within the entire monitored time period.

For the TN experiments, the physical layer configuration can be improved and the functionality of the physical and MAC layers at the UE can be tweaked to overcome the experienced decrease in the attack performance after around one minute since the start. In addition, having more powerful devices can also address the issues related to synchronization and improve the performance of the attack. For the NTN experiments, higher propagation delays compared to a usual TN setup do have an impact on the attack, especially with a GEO satellite, where the attack would be mitigated if the OAI gNB also releases the stale RRC contexts at the CU part. With a LEO satellite, higher latency than in TN does not impact the attack as much as with a GEO satellite, even though new RRC connections are created slower than in the TN experiments.

## 7.6. Conclusions and mitigations

The results of our flooding attack align with the results obtained by Kim et al. [215] for the original "BTS resource depletion attack" on LTE. We were also able to reach the maximum number of allowed UE connections at the gNB. However, we covered many more aspects of the attack with our experiments.

Initially, we implemented and tested our attack prototype using UERANSIM and free5GC. Since all layers below RRC were simulated (which includes the scheduling and the Random Access procedure at the MAC layer), the rogue UE was able to keep the gNB busy and prevent a legitimate UE from successfully connecting to the network, despite the absence of the maximum number of allowed RRC connections. Our approach with spawning lightweight UEs as background processes, while not practical in a real setting, allowed utilizing much of the allocated resources and have a noticeable impact on the CPU utilization of the gNB. However, the memory consumption remained very low, even though the created RRC contexts were not deleted after the corresponding RLS UDP connections were released. Finally, we experienced crashes in the gNB, which we believe happened due to concurrency. While such a crash could be desirable for an attacker in a real network, for our experiments we consider it as an implementation bug, rather than a success of the attack.

Next, we implemented our attack using the OAI NR UE, where we could make use of the Random Access procedure and resource scheduling at the MAC layer to perform a more realistic version of the attack. This came at the cost of less efficient resource utilization from the attacker's perspective and lack of parallelization, since only one software modem was used. We still observed a noticeable increase in the CPU usage of the gNB(-DU) during the attack, with the increase in the memory consumption only visible over a longer time period. The impact on other targets, such as the AMF and the gNB-CU, was negligible. Nevertheless, similar to the attack prototype using UERANSIM, we were able to cause a DoS for a legitimate UE, which happened once the limit on the maximum allowed UEs at the gNB was reached by the attacker.

We also discovered that the OAI gNB only released timed out UE connections at the MAC layer (in the DU part), while the corresponding contexts were not deleted at the RRC layer (in the CU part) during our attack, since the context release was not requested by the core network. This allowed the attacker to create more RRC contexts in the gNB than the maximum allowed number of UEs that are served by a single gNB (64 UEs). If the attack is performed over a longer period of time, the impact on the gNB memory consumption becomes more noticeable, although the growth is still relatively slow, as the established fake connections need to time out before new contexts can be created. Given that it is possible to permanently create an RRC context in the gNB, the attacker can eventually exhaust the memory resources of the base station, even though the time to achieve this depends on the exact deployment. For example, it would take much longer with the gNB split, because the RRC contexts are stored in the gNB-CU, which remains relatively idle during the attack.

Finally, we evaluated our attack in a TN setting using OAI with real USRP devices and in an NTN setting using the OAI RF simulator. With the USRP devices, the attacker was able to create more connections than the defined threshold, even though the performance of the attack started to decrease after around one minute of flooding, likely because the devices lost the synchronization. Nonetheless, this is a physical and/or MAC layer issue, rather than a problem in the attack methodology, and we believe it can be addressed with better configuration, fine-tuning functionality, and more powerful SDR devices. As for the NTN experiments, we observed that the higher propagation delay with a GEO satellite could mitigate the attack if the RRC contexts were properly released, while the impact of latency on the attack with a LEO satellite was much lower. In both cases, the attacker was still able to create more RRC contexts than the threshold on the UEs, although the flooding rate was lower than in a terrestrial setting.

Based on the obtained results, we can see that there is no noticeable difference on the attack performance when using the same registered IMSI or different incrementally generated IMSIs. This is because the main target of the attack is the RRC layer at the gNB, which is not aware of the IMSI that is transferred by the NAS layer. Whether the IMSI is registered or not would affect the behaviour of the AMF if the corresponding Registration Request messages reach the core network. However, even in this case, we did not observe a noticeable difference between the two experiments. Furthermore, we also saw similar results for both the full gNB and the gNB split. With the split, the RRC contexts were stored in the gNB-CU, which had dedicated resources for higher-layer processing and was decoupled

from the gNB-DU, which performed the more computationally-expensive lower-layer processing (e.g. encoding, decoding, and scheduling). In addition, the OAI gNB-CU released all active RRC contexts when the gNB-DU got disconnected, which happened when we stopped it at the end of the experiments.

Given the OAI behaviour that we observed during our experiments, both having a threshold on the number of UEs or not having it can be beneficial for the attacker, depending on their goals. If there is a limit, the attacker can cause a DoS against a legitimate UE once this threshold is reached, as we have seen in subsection 7.4.2. However, having a (low) limit also restricts the impact on the gNB resource consumption, especially the memory usage, because new contexts will not be allocated until the stale UE connections time out. On the other hand, if there is no limit on the allowed UEs, the attacker will not be able to prevent a legitimate UE from connecting to the base station, as it will still get the radio resources for transmission from the gNB. However, the attacker will be able to allocate more contexts at the RRC layer, therefore having a larger impact on the gNB memory utilization. Nevertheless, this will only have a meaningful effect if the UE contexts are not released at the RRC layer, which is the case with the (current) OAI implementation of the gNB.

We also note that the performance of the attack could be improved with further modifications at the physical and MAC layers. An example of such modifications would be some retransmission parameters, which can be decreased at the UE if it experiences issues with the transmission channels. For instance, the maximum number of Scheduling Requests and *preambleTransMax* could be reduced, so that the UE restarts the RA procedure sooner, instead of waiting until the corresponding thresholds are reached. Furthermore, better tweaking of the physical layer, especially the parts related to synchronization and transmission channels, can also help with performance. Alternatively, using a different, more robust UE implementation instead of OAI could also help the attacker. In the best case, a UE that allows sending arbitrary packets using the entire 5G NR stack (including the RF part) would be the most flexible option for the attacker, although building such a software is also a very complex task.

As for the countermeasures, the attack against the OAI gNB can be fairly easily mitigated by releasing the stale UE contexts both at the MAC layer and at the RRC layer. This would greatly limit the impact on the memory resources, even if the attack is performed over a longer time period. In addition, fine-tuning the value for the UL failure timeout can also ensure that the stale UE connections will be released sooner and reduce the flooding rate, although the best timeout value would depend on the specific environment. In real-world networks, having an IDS functionality can detect the attack, regardless if the same IMSI, an incrementally generated IMSI, or a randomly generated IMSI is used (the latter is more difficult to detect, but it is still noticeable based on a large number of failed or uncompleted registration requests). Finally, fine-tuning the physical and MAC layer configuration at the gNB (e.g. setting higher values for failure thresholds) could also make the attack more difficult to implement, unless the attacker is aware of these changes and addresses them.

# 8

# Discussion

In this chapter, we discuss the findings of our security analysis of 3GPP terrestrial and non-terrestrial networks, reflecting on the challenges and the attacks in both environments. We also provide recommendations to the 3GPP community and mobile network operators, and reflect on the limitations of our work, including the methodology and the experimental setup of our flooding attack.

## 8.1. Security challenges in terrestrial and non-terrestrial networks

Security of terrestrial networks has been extensively analysed in the research community. However, as discussed in subsection 5.6.3, some MNOs choose not to use the non-mandatory protection measures (e.g. confidentiality protection of RRC and NAS signalling, or encryption and authentication of the UP data). What is more, even the mandatory protection mechanisms may be not implemented or implemented incorrectly. This becomes a bigger issue in NTN deployments, where the operators are more likely to neglect security protections due to higher constraints on satellite resources. For instance, they can decide to use only IPsec protection on the feeder link and not implement DTLS. In the worst case, they can even choose to disable security altogether if it becomes too expensive for them to implement and maintain. As a result, this allows malicious actors to perform various attacks, including eavesdropping, spoofing, and tampering the data between the satellite and the ground.

As discussed in section 6.4, new challenges emerge in NTN that were not present in TN. Different NTN deployments expose certain interfaces as service or feeder links, making them accessible over a larger geographical area. This also means that an attacker does not need to be physically close to the UE or the gNB to perform an attack. In addition, the exposed operator-controlled interfaces cannot be placed in a physically secure environment, meaning that cryptographic solutions need to be used to provide confidentiality, integrity, and replay protection. However, some countermeasures from the network might need to be different, since computation-based mitigations (e.g. hashes or SYN-cookies) may not always be easily provisioned by simply adding more resources. While already known attacks could be mitigated in other ways, this can be a problem for future attacks. Other challenges arise for moving (i.e. non-GEO) satellites with a regenerative payload, where some contexts may need to be securely transferred between the serving satellites. This is especially challenging with a full gNB on board, where storing all (security) contexts for every served UEs, together with all the cryptographic material (e.g. IPsec databases, DTLS certificates etc.) may be infeasible due to the physical constraints.

On the other hand, NTN deployments can also offer certain benefits. Since a satellite is not physically accessible, physical attacks have a much lower risk than in TN, where the gNB may be located on a building and can be accessed by attackers who can extract the cryptographic secrets. This can give a certain degree of freedom in sharing secrets between the satellites, if having independent secrets for every communicating pair is not feasible. Of course, if the keys in a satellite get compromised by some other means (e.g. by exploiting a software vulnerability), they cannot be easily replaced as in TN. Finally, some attacks (e.g. involving signal overshadowing from the gNB) become more difficult to perform, requiring a more expensive setup and higher level of skills than in a typical terrestrial setup.

## 8.2. Attacks on terrestrial and non-terrestrial networks

Many attacks against 5G TN have been discussed in the literature, some of them exploiting implementation vulnerabilities and others relying on weaknesses in the 3GPP specifications. While attacks against implementations affect only specific devices having the vulnerability, weaknesses in the 3GPP specifications affect all devices following the standard. Therefore, in our security analysis, we focused on the attacks against the 3GPP specifications, particularly the attacks on the radio interface (e.g. targeting unprotected pre-authentication RRC and NAS messages or unprotected lower layer protocols). Having analysed 30 such attacks (see Appendix B), we have seen that many of them are too optimistic or even theoretical, with little or no meaningful practical impact, while some are only applicable in very specific situations. We have selected 6 attacks, which we have further analysed both in TN and in NTN (see section 5.5 and section 6.3), and demonstrated one of them against a real 5G implementation (see chapter 7).

The attacks we have analysed can be performed in both terrestrial and non-terrestrial deployments, however there are some differences. For the attacks that target the UE (e.g. DoS attacks or location tracking attacks), while their impact on a single UE is the same in TN and NTN, the volume of these attacks becomes larger. This is because a satellite has a much larger coverage area than a terrestrial base station, resulting in larger cell sizes. With a larger number of UEs that can be served by a satellite, an attacker has more possible targets within a single cell. On the other hand, the complexity and cost of the attacks in an NTN environment can significantly increase, especially for the attacks that use a fake base station (FBS) to overshadow the signal from a legitimate gNB (e.g. attacks exploiting unauthenticated RRC and NAS reject messages or lower-layer messages, such as DCI). If the attacker device needs to be placed in the orbit, it would require a very expensive setup together with advanced skills to actually perform the attack. Therefore, we expect the threat model to shift towards highly-skilled attackers, such as state-sponsored threat actors. As for the attacks against a non-terrestrial gNB, we have seen in subsection 7.5.2 that the impact can depend on a specific implementation, and that higher latencies reduce the flooding rate, especially with satellites in higher orbits.

In our analysis of the 3GPP security specifications (see chapter 6), we were not able to find any new attacks or weaknesses that have not already been discovered in the previous research. Our security analysis showed that 3GPP mandates confidentiality, integrity, and replay protection on all NDS/IP network interfaces (N2, N3, N4, N9, Xn, F1, E1), even though not necessarily using cryptographic solutions (which is left to the operator to decide). The only exception is the F1-U interface, where confidentiality, integrity, and replay protection is not explicitly mandated. The reason may be that the PDCP protection for the UP data is terminated in the gNB-CU, providing protections for the layers above PDCP. However, the use of PDCP for confidentiality protection and authentication of UP data is also not mandated. This means that in the absence of both PDCP and IPsec protections on the F1-U interface, the user data passing through this link is open to the eavesdropping and tampering attacks. Furthermore, while the CP data on the Uu and N1 interfaces (i.e. RRC and NAS messages) is mandatory to be authenticated, this does not apply to the use of confidentiality protection for these messages, which is left to the operator to decide. Similarly, both confidentiality and integrity protection of UP data on the Uu interface is not mandatory to use. Next to summarizing the security architecture of 5G networks, we provided additional value by mapping the 3GPP protection measures for the studied interfaces into the four chosen NTN scenarios (see section 6.1), which has not been done by the previous research.

We have also seen that the 3GPP cryptographic profiling does not leave space for vulnerable versions (see section 5.2). While there were a couple of cases where the protocols in the linked RFCs were considered weak, their usage is becoming deprecated and is expected to be removed. On the other hand, we have seen that NIST intends to deprecate the usage of cryptographic algorithms providing security strength less than 128 bits, such as RSA modulus length lower than 3072, 2048-bit MODP groups, and elliptic curves with less than 256 bits, by December 31, 2030. Some of these algorithms were present in the 3GPP profiling, meaning that they should not be used in new systems. Furthermore, we have seen that 3GPP allows algorithms that are not allowed by the CNSA 1.0 and/or CNSA 2.0 Suites. While 3GPP targets a different audience than the CNSA Suite, following the CNSA (2.0) profiling can be helpful in transitioning towards post-quantum cryptography to address the emerging threat of cryptographically-relevant quantum computers.

## 8.3. Recommendations for terrestrial and non-terrestrial networks

Considering the challenges and the attacks discussed above and throughout our security analysis, we can provide the following recommendations to the 3GPP community and/or MNOs:

- The 3GPP specifications should be non-ambiguous when it comes to the support and usage of a certain cryptographic protocol. It is best if they clearly state whether only the explicitly listed protocols are allowed to be used, or whether the usage of all other protocols is up to the operator to decide. In addition, the standards should clearly specify which cryptographic algorithms are mandatory to support and which algorithms are mandatory to use.
- The 3GPP specifications should take into account the future deprecation of cryptographic algorithms planned by NIST, e.g. the algorithms providing less than 128-bit security strength which will be deprecated by December 31, 2030. The MNOs should not use these algorithms on new devices that are expected to be operational after the deprecation deadline.
- The MNOs and vendors should strive for crypto agility, so that the used cryptographic algorithms can be changed without having to interrupt the system operation. This is also important when transitioning to the post-quantum algorithms, which may also be broken.
- The 3GPP specifications and MNOs should take into account the CNSA 1.0 and CNSA 2.0 profiling wherever possible in order to facilitate the transitioning to the post-quantum cryptography. Given that this migration takes time, it needs to start as soon as possible.
- The 3GPP specifications should introduce mandatory protection mechanisms for fake base station detection and base station authentication, in order to mitigate the attacks exploiting the unprotected RRC and NAS messages sent before the AS/NAS security activation or the unprotected lower-layer messages (for example, based on the solutions already proposed by 3GPP TR 33.809 [48] or solutions from academic works, such as [195, 364, 415])
- The MNOs should implement all mandatory protection measures specified in the 3GPP standards. In addition, they should also implement the non-mandatory security mechanisms wherever possible. It is essential to have protections at different levels of the protocol stacks, so that a compromise of one layer does not compromise the entire system.
- The 3GPP specifications should mandate the use of cryptographic algorithms or alternative mechanisms for confidentiality, integrity, and replay protection on the exposed interfaces in NTN deployments, where a physically secure environment is impossible to ensure. This includes the service link (Uu and N1) and the feeder link (N2, N3, N4, N6, F1, and E1 depending on the deployment scenario).
- The 3GPP specifications should consider introducing lightweight cryptography solutions (such as the Ascon family [386] which is being standardized by NIST) for NTN due to the processing and memory constraints for satellite payloads. Resource limitations make satellite operators more likely to neglect cryptographic protections.
- The developers of 5G implementations should properly implement the release of stale UE connections (such as RRC contexts) to mitigate the impact of flooding attacks against the gNB that aim to create fake connections. The MNOs should carefully choose the values for failure timeouts and failure thresholds, such that fake connections are released sooner and legitimate UEs are not disconnected (this configuration is likely to be network-specific).

## 8.4. Limitations

In our security analysis of terrestrial and non-terrestrial networks (performed in chapter 5 and chapter 6), we followed a manual approach to review the 3GPP specifications. While our analysis was focused around the chosen non-SBI interfaces affected by NTN deployments, the 3GPP documents are long and complex, often cross-referencing other specifications. Therefore, more structured approaches such as fuzzing [86, 349, 384, 163, 365, 413] and/or formal model-based methods [194, 193, 192] can be used to complement our analysis with an automated way of finding inconsistencies and discovering unexpected crashes and transitions in the protocols.

In the practical part of our thesis (performed in chapter 7), we evaluated our flooding attack using UERANSIM (as the attack prototype) and OpenAirInterface (as the actual attack). With the OAI imple-

mentation of the gNB, we had to stick to the defined threshold on the maximum supported number of UEs served by a single gNB (at most 64 UEs at the time of writing). While reaching this limit allowed us to successfully perform a DoS attack against a legitimate UE, it did not allow us to create new RRC contexts in the gNB until the old connections timed out. Therefore, the impact on the gNB memory resources was only visible when running the attack over a longer period of time. It is possible that the memory consumption would be higher during the attack if there was no threshold on the number of UEs. Furthermore, a possible vulnerability in OAI allowed us to create more RRC contexts in the gNB than the maximum supported number of UEs, because the stale contexts were only released at the MAC layer but not at the RRC layer. Other 5G implementations might not have this behaviour, which would affect some of our results (e.g. active UE connections in the gNB and its memory utilization). Thus, further evaluation using other (possibly closed-source) gNB implementations can be performed to get a more accurate estimation of the attack performance.

In addition, our implementation of the flooding attack against the gNB was affected by the choice of using OpenAirInterface as the UE implementation. The OAI NR UE was designed to function in accordance with the 3GPP specifications, while the rogue UE in our attack was supposed to not follow some standard procedures and behave differently. As a result, when developing the attack, we were restricted by the inner workings of OAI. Therefore, using a different, more flexible implementation for a rogue UE may result in a better attack performance with a higher flooding rate.

# 9 Conclusion

In this chapter, we summarise the main findings of our work, including the security analysis of terrestrial and non-terrestrial networks, as well as the implementation and evaluation of a flooding attack in a terrestrial and non-terrestrial setting. We also provide directions for future research.

## 9.1. Summary

The active deployment of 5G networks creates new use cases for various industry verticals, with the main usage scenarios being Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communications (URLLC), and Massive Machine-type Communications (mMTC). Operators and enterprises get new opportunities and revenue sources, while network operators have a lot of flexibility with virtualization, cloud deployments, CUPS, and programmable networks. At the same time, non-terrestrial 5G networks (NTN) are getting increasing attention as a complementary solution to the terrestrial infrastructure, offering service continuity, service ubiquity, and service scalability, aiming to achieve the global connectivity. Despite all the benefits provided by 5G terrestrial and non-terrestrial deployments, new security challenges are introduced, especially in the field of NTN security, which has been only scarcely analysed by the previous research.

In this thesis, we aimed to answer three main research questions. Below, we summarize our findings for each of these questions.

**1. "What is the current security architecture of 3GPP 5G terrestrial networks?"**

We performed an in-depth analysis of the 3GPP specifications, focusing on the selected ten non-SBI interfaces that are affected by NTN deployments (Uu, N1, N2, N3, N4, N6, N9, Xn, F1, and E1). We summarized the security architecture of terrestrial networks, including the proposed protection mechanisms together with their usage requirement levels. In addition, we also reviewed the cryptographic profiling for the identified security measures, comparing them with the cryptographic algorithms allowed by NIST and NSA's CNSA 1.0 and CNSA 2.0 Suites. While the 3GPP specifications did not leave space for vulnerable algorithm versions, a better compliance with the CNSA (2.0) Suite could further enhance the security and help in the transitioning to the post-quantum cryptography in order to address the emerging threat of cryptographically relevant quantum computers.

We also summarized and analysed 30 literature attacks against weaknesses in the 3GPP security specifications for terrestrial networks. Many of these attacks seemed too optimistic, and we could not see a meaningful impact in a real setting. From the reviewed attacks, we selected six which we found most interesting for further analysis. These attacks exploited the lack of authentication in the RRC and NAS messages that are sent before security activation, or the general absence of authentication in the lower layers of the 5G NR stack (such as the MAC layer). While we did not find any new weaknesses or attacks against the 3GPP specifications, we believe that our analysis is useful for both the academic community and the industry, providing a good overview of the 3GPP security architecture and serving as a reference for various aspects of 5G security.

**2. "What is the current security architecture of 3GPP 5G non-terrestrial networks?"**

Building on top of our work on TN security, we mapped the identified protections mechanisms into the four studied NTN scenarios: Transparent payload, Full gNB on board, Split CU-DU, and UE-Satellite-UE communication. Based on the summarised NTN security architecture, we performed, to the best of our knowledge, the first head-to-head comparison of these deployment options. With no on-board security provisions, Transparent payload is the simplest scenario, which is only capable of reflecting the received signal, regardless of the actual message structure and content. While Full gNB on board and UE-Satellite-UE communication can offer the most features (including detection of unauthenticated or malformed messages), they also face more challenges due to large amounts of (security) contexts and cryptographic material that need to be stored on board a satellite with processing and memory constraints. Split CU-DU combines some advantages of the other scenarios, offering more features than Transparent payload (e.g. detection of malformed messages), while also requiring less processing power and less storage space than Full gNB on board and UE-Satellite-UE communication.

We have also analysed the impact of the selected six TN literature attacks in the context of NTN. We showed that the volume of the attacks targeting the UE (e.g. DoS or location tracking attacks) increases, with more possible targets available to an attacker due to a larger coverage area of a single serving satellite. On the other hand, the cost and complexity of these attacks also increase, requiring a more expensive setup and more advanced skills to actually perform the attack. For instance, to implement a fake base station, the attacker may need a drone or a satellite in the orbit, while a cheap COTS device can be sufficient in TN. The attacks targeting the non-terrestrial gNB (e.g. flooding attacks) could in theory be more feasible to perform than in TN, as satellite processing and memory resources are limited by the physical constraints, even though higher latencies can reduce the flooding rate compared to TN. However, the exact practical impact will depend on the gNB implementation and on the computational resources available to the attacker.

Finally, based on our comparison of NTN scenarios and our analysis of the selected literature attacks in NTN, we performed the first of its kind head-to-head comparison of 5G terrestrial and non-terrestrial networks. We discussed the new challenges introduced in NTN deployments, such as stricter requirements on processing and memory, which makes the implementation of the 3GPP security protections and other computation-based countermeasures more difficult than in TN deployments. The exposed operator-controlled interfaces cannot be placed in a physically secure environment, meaning that the required confidentiality, integrity, and replay protection need to be provided using cryptographic solutions. Additional challenges are faced by moving satellites with regenerative payloads, where (security) contexts may need to be transferred between the serving satellites and where storing all the contexts for all served UEs together with all the cryptographic materials may be infeasible due to memory restrictions. On the other hand, some advantages are also offered by the NTN deployments, such as a much lower risk of physical attacks (e.g. physical extraction of secrets) and generally higher cost and complexity of performing attacks, shifting the threat model towards higher-skilled attackers.

**3. "Can we successfully perform a flooding attack against gNB in 3GPP 5G terrestrial and non-terrestrial networks?"**

In the practical part of our thesis, we demonstrated a flooding attack, originally proposed by Kim et al. [215] for LTE networks. In the initial attack prototype using UERANSIM, we managed to prevent a legitimate subscriber from connecting to the network even with the absence of a limit on the RRC connections. However, we did not observe a noticeable memory increase in the gNB during the attack. With the actual attack implementation using OpenAirInterface (OAI) with the RF simulator, we managed to reach the defined maximum number of allowed RRC connections, resulting in a DoS of a legitimate UE who was rejected by the gNB once the limit has been reached. This aligns with the results obtained by Kim et al. for the original attack. Furthermore, we were able to create more RRC contexts in the gNB than the maximum supported number of UE connections, because the OAI gNB only released the timed out stale connections at the MAC layer but not at the RRC layer. On the other hand, the threshold on the UE connections did not allow us to create new RRC contexts non-stop, so the increase in the memory consumption was only visible when the attack was performed over a longer time.

The results of our attack evaluation in TN and NTN settings were consistent with the results obtained using the OAI RF simulator during the attack implementation. Our rogue UE was able to reach the

threshold on the UE connections and allocate more RRC contexts in the gNB than defined by the limit. In the TN setup using real SDR devices, we observed some performance decrease after some time. However, this is a problem at the physical and MAC layers, which can be addressed with a better parameter configuration, some tweaks, and more powerful devices. In the NTN setup, we used the OAI RF simulator and the NTN configuration, simulating LEO and GEO satellites with a transparent payload. Due to higher latencies, we observed a lower flooding rate than in TN experiments. With a GEO satellite, this would fully mitigate the attack if the OAI gNB released the stale RRC contexts.

For the flooding attack to be successful, new UE connections need to be created faster than the old ones are released. We were able to achieve this in all experiments, except with the simulated GEO satellite, where old connections were deleted faster due to higher latencies that slowed down the new connections. With the observed behaviour in the OAI implementation of the gNB, we were able to permanently create an RRC context in the gNB, allowing us to allocate even more contexts once the old fake connections were released at the MAC layer. Therefore, the main mitigation against our attack is a proper release of RRC contexts at the gNB (both at the lower and the higher layers), together with a configurable value of the uplink failure timeout, which could release stale UE contexts sooner.

## 9.2. Future work

In our security analysis, we focused on the standard scenario of a non-roaming mode and 3GPP access. Our work can be further extended to also include roaming scenarios and non-3GPP access, which introduce new attack vectors. As we have seen in our review of the literature attacks, the lower layers of the 5G NR protocol stack lack protection mechanisms, which makes them vulnerable to various attacks, such as spoofing, tampering, and eavesdropping. These lower layers can be more extensively analysed for security issues, especially in the NTN setting, where they become exposed from a larger geographical area. Our analysis of the NTN deployments can also be extended to include the Store-and-Forward satellite operation scenario. Finally, from the selected six literature attacks, we assessed the practical feasibility and impact of one of them, but this can also be done for the other attacks.

The flooding attack that we developed using OAI can be further evaluated against other gNB implementations, such as srsRAN [369] or Amarisoft [68]. This can give an even better estimation of the attack impact. While our NTN experiments used the OAI RF simulator with NTN channel simulation, the same experiments can be performed with an NTN channel emulator. Although the main target of our attack is the RRC layer and not the physical layer, the results obtained with an NTN channel emulator can even better reflect the real-world impact of the attack against NTN deployments. Furthermore, a different implementation of the UE can also be used, considering the difficulties experienced by us and others when trying to connect the OAI NR UE to a different gNB software[1].

Another possible direction for future work is automated Security Assurance Specification (SCAS) conformance testing, based on the 3GPP SCAS documents [35, 34, 5, 4, 6, 3]. One such (Python-based) framework to automate the 3GPP SCAS tests is pySCASso [104], developed by the German Federal Office for Information Security (BSI). At the time of writing, the tool has many tests that are defined but not implemented. As an experiment, we wrote a test checking integrity protection of RRC signalling between the UE and the gNB(-CU), which has been successfully merged[2] into the tool by the maintainer. Other tests can also be implemented to make the tool more complete. This would allow for automated SCAS testing of existing 5G implementations, such as OpenAirInterface, free5GC, and open5GS, and possibly even commercial software like Amarisoft based on the logs they provide.

[1] https://github.com/srsran/srsRAN_Project/discussions/395
[2] https://github.com/BSI-Bund/pySCASso/pull/2

# References


[1] Donald E. Eastlake 3rd. *Transport Layer Security (TLS) Extensions: Extension Definitions*. RFC 6066. Jan. 2011. DOI: 10.17487/RFC6066. URL: https://www.rfc-editor.org/info/rfc6066.

[2] Donald E. Eastlake 3rd, Steve Crocker, and Jeffrey I. Schiller. *Randomness Requirements for Security*. RFC 4086. June 2005. DOI: 10.17487/RFC4086. URL: https://www.rfc-editor.org/info/rfc4086.

[3] 3rd Generation Partnership Project (3GPP). *5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class*. Technical Specification (TS) 33.515. Version 18.1.0. Release 18. 3GPP, Dec. 2023. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3448.

[4] 3rd Generation Partnership Project (3GPP). *5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)*. Technical Specification (TS) 33.512. Version 18.2.0. Release 18. 3GPP, June 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445.

[5] 3rd Generation Partnership Project (3GPP). *5G Security Assurance Specification (SCAS); Split gNB product classes*. Technical Specification (TS) 33.523. Version 19.1.0. Release 19. 3GPP, Mar. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4147.

[6] 3rd Generation Partnership Project (3GPP). *5G Security Assurance Specification (SCAS); User Plane Function (UPF)*. Technical Specification (TS) 33.513. Version 18.1.0. Release 18. 3GPP, Dec. 2023. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3446.

[7] 3rd Generation Partnership Project (3GPP). *5G System; Interworking between 5G Network and external Data Networks; Stage 3*. Technical Specification (TS) 29.561. Version 19.0.0. Release 19. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3390.

[8] 3rd Generation Partnership Project (3GPP). *5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3*. Technical Specification (TS) 29.573. Version 19.0.0. Release 19. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3530.

[9] 3rd Generation Partnership Project (3GPP). *5G System; Technical Realization of Service Based Architecture; Stage 3*. Technical Specification (TS) 29.500. Version 19.0.0. Release 19. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3338.

[10] 3rd Generation Partnership Project (3GPP). *E1 Application Protocol (E1AP)*. Technical Specification (TS) 37.483. Version 18.3.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3957.

[11] 3rd Generation Partnership Project (3GPP). *E1 general aspects and principles*. Technical Specification (TS) 37.480. Version 18.1.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3954.

[12] 3rd Generation Partnership Project (3GPP). *Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Overall Description; Stage 2*. Technical Specification (TS) 37.340. Version 18.3.0. Release 18. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3198.

[13] 3rd Generation Partnership Project (3GPP). *General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)*. Technical Specification (TS) 29.281. Version 19.1.0. Release 19. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1699.

[14] 3rd Generation Partnership Project (3GPP). *Interface between the Control Plane and the User Plane nodes*. Technical Specification (TS) 29.244. Version 19.0.0. Release 19. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3111.

[15] 3rd Generation Partnership Project (3GPP). *Lawful Interception (LI) architecture and functions*. Technical Specification (TS) 33.127. Version 19.1.0. Release 19. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3182.

[16] 3rd Generation Partnership Project (3GPP). *Network Domain Security (NDS); Authentication Framework (AF)*. Technical Specification (TS) 33.310. Version 19.3.0. Release 19. 3GPP, Jan. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2293.

[17] 3rd Generation Partnership Project (3GPP). *Network Domain Security (NDS); IP network layer security*. Technical Specification (TS) 33.210. Version 19.0.0. Release 19. 3GPP, Jan. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279.

[18] 3rd Generation Partnership Project (3GPP). *NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN*. Technical Specification (TS) 38.305. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3310.

[19] 3rd Generation Partnership Project (3GPP). *NG-RAN; Architecture description*. Technical Specification (TS) 38.401. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3219.

[20] 3rd Generation Partnership Project (3GPP). *NG-RAN; F1 Application Protocol (F1AP)*. Technical Specification (TS) 38.473. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3260.

[21] 3rd Generation Partnership Project (3GPP). *NG-RAN; F1 general aspects and principles*. Technical Specification (TS) 38.470. Version 18.3.0. Release 18. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3257.

[22] 3rd Generation Partnership Project (3GPP). *NG-RAN; NG Application Protocol (NGAP)*. Technical Specification (TS) 38.413. Version 18.3.0. Release 18. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3223.

[23] 3rd Generation Partnership Project (3GPP). *NG-RAN; NG general aspects and principles*. Technical Specification (TS) 38.410. Version 18.2.0. Release 18. 3GPP, June 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3220.

[24] 3rd Generation Partnership Project (3GPP). *NG-RAN; Xn general aspects and principles*. Technical Specification (TS) 38.420. Version 18.1.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3225.

[25] 3rd Generation Partnership Project (3GPP). *Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3*. Technical Specification (TS) 24.501. Version 19.0.0. Release 19. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3370.

[26] 3rd Generation Partnership Project (3GPP). *NR; Medium Access Control (MAC) protocol specification*. Technical Specification (TS) 38.321. Version V18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3194.

[27] 3rd Generation Partnership Project (3GPP). *NR; NR and NG-RAN Overall Description; Stage 2*. Technical Specification (TS) 38.300. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3191.

[28] 3rd Generation Partnership Project (3GPP). *NR; Packet Data Convergence Protocol (PDCP) specification*. Technical Specification (TS) 38.323. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3196.

[29] 3rd Generation Partnership Project (3GPP). *NR; Physical layer procedures for control*. Technical Specification (TS) 38.213. Version V18.5.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3215.

[30] 3rd Generation Partnership Project (3GPP). *NR; Radio Resource Control (RRC); Protocol specification*. Technical Specification (TS) 38.331. Version 18.4.0. Release 18. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197.

[31] 3rd Generation Partnership Project (3GPP). *Numbering, addressing and identification*. Technical Specification (TS) 23.003. Version 19.2.0. Release 19. 3GPP, Mar. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729.

[32] 3rd Generation Partnership Project (3GPP). *Procedures for the 5G System (5GS)*. Technical Specification (TS) 23.502. Version 19.2.0. Release 19. 3GPP, Dec. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3145.

[33] 3rd Generation Partnership Project (3GPP). *Security architecture and procedures for 5G system*. Technical Specification (TS) 33.501. Version 19.1.0. Release 19. 3GPP, Nov. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169.

[34] 3rd Generation Partnership Project (3GPP). *Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class*. Technical Specification (TS) 33.511. Version 19.0.0. Release 19. 3GPP, Jan. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3444.

[35] 3rd Generation Partnership Project (3GPP). *Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes*. Technical Report (TR) 33.926. Version 19.3.0. Release 19. 3GPP, Jan. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3002.

[36] 3rd Generation Partnership Project (3GPP). *Service requirements for the 5G system; Stage 1*. Technical Specification (TS) 22.261. Version 20.0.0, Release 20, 3GPP. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107.

[37] 3rd Generation Partnership Project (3GPP). *Solutions for NR to support Non-Terrestrial Networks (NTN)*. Technical Report (TR) 38.821. Version 16.2.0. Release 16. 3GPP, Mar. 2023. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3525.

[38] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications*. Technical Specification (TS) 35.221. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2399.

[39] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 2: ZUC specification*. Technical Specification (TS) 35.222. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2400.

[40] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data*. Technical Specification (TS) 35.223. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2401.

[41] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 4: Design and Evaluation Report*. Technical Report (TR) 35.924. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2407.

[42] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications*. Technical Specification (TS) 35.215. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2395.

[43] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification*. Technical Specification (TS) 35.216. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2396.

[44] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data*. Technical Specification (TS) 35.217. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2397.

[45] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 4: Design conformance test data*. Technical Specification (TS) 35.218. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2398.

[46] 3rd Generation Partnership Project (3GPP). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 5: Design and evaluation report*. Technical Report (TR) 35.919. Version 18.0.0. Release 18. 3GPP, Mar. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2406.

[47] 3rd Generation Partnership Project (3GPP). *Study of separation of NR Control Plane (CP) and User Plane (UP) for split option 2*. Technical Report (TR) 38.806. Version 15.0.0. Release 15. 3GPP, Dec. 2017. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3307.

[48] 3rd Generation Partnership Project (3GPP). *Study on 5G security enhancements against False Base Stations (FBS)*. Technical Report (TR) 33.809. Version V18.1.0. Release 18. 3GPP, Sept. 2023. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539.

[49] 3rd Generation Partnership Project (3GPP). *Study on Central Unit (CU) - Distributed Unit (DU) lower layer split for NR*. Technical Report (TR) 38.816. Version 15.0.0. Release 15. 3GPP, Dec. 2017. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3364.

[50] 3rd Generation Partnership Project (3GPP). *Study on integration of satellite components in the 5G architecture; Phase 3*. Technical Report (TR) 23.700-29. Version 19.0.0. Release 19. 3GPP, June 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4212.

[51] 3rd Generation Partnership Project (3GPP). *Study on New Radio (NR) to support non-terrestrial networks*. Technical Report (TR) 38.811. Version 15.4.0. Release 15. 3GPP, Sept. 2020. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234.

[52] 3rd Generation Partnership Project (3GPP). *Study on new radio access technology: Radio access architecture and interfaces*. Technical Report (TR) 38.801. Version 14.0.0. Release 14. 3GPP, Mar. 2017. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3056.

[53] 3rd Generation Partnership Project (3GPP). *Study on satellite access Phase 3*. Technical Report (TR) 22.865. Version 19.2.0. Release 19. 3GPP, Dec. 2023. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4089.

[54] 3rd Generation Partnership Project (3GPP). *Study on Security Aspects of 5G Satellite Access in the 5G architecture; Phase 3*. Technical Report (TR) 33.700-29. Version 19.0.0. Release 19. 3GPP, Mar. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4241.

[55] 3rd Generation Partnership Project (3GPP). *Study on the support of 256-bit algorithms for 5G*. Technical Report (TR) 33.841. Version 16.1.0. Release 16. 3GPP, Mar. 2019. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3422.

[56] 3rd Generation Partnership Project (3GPP). *Study on using Satellite Access in 5G; Stage 1*. Technical Report (TR) 22.822. Version 16.0.0. Release 16. 3GPP, June 2018. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3372.

[57] 3rd Generation Partnership Project (3GPP). *System Architecture Evolution (SAE); Security architecture*. Technical Specification (TS) 33.401. Version 18.2.0. Release 18. 3GPP, Sept. 2024. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296.

[58] 3rd Generation Partnership Project (3GPP). *System architecture for the 5G System (5GS); Stage 2*. Technical Specification (TS) 23.501. Version 19.2.1. Release 19. 3GPP, Jan. 2025. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[59] 5G Public Private Partnership (5G PPP). *View on 5G Architecture*. White Paper. Version 2.0. 5G PPP, Dec. 2017. URL: https://www.5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf.

[60] 5G Public Private Partnership (5G PPP). *Vision on Software Networks and 5G*. White Paper. Version 2.0. 5G PPP, Jan. 2017. URL: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_SoftNets_WG_whitepaper_v20.pdf.

[61] David Adrian et al. “Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice”. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015, pp. 5–17.

[62] Aerospace Corporation. *Space Attack Research & Tactic Analysis (SPARTA)*. URL: https://sparta.aerospace.org/ (visited on July 25, 2025).

[63] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. “Next Generation 5G Wireless Networks: A Comprehensive Survey”. In: *IEEE communications surveys & tutorials* 18.3 (2016), pp. 1617–1655.

[64] Ijaz Ahmad et al. “Security of Satellite-Terrestrial Communications: Challenges and Potential Solutions”. In: *IEEE Access* 10 (2022), pp. 96038–96052.

[65] Nadhem J Al Fardan and Kenneth G Paterson. “Lucky Thirteen: Breaking the TLS and DTLS Record Protocols”. In: *2013 IEEE symposium on security and privacy*. IEEE. 2013, pp. 526–540.

[66] Gorjan Alagic et al. *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/Internal Report (NISTIR) 8545. U.S. Department of Commerce, Mar. 2025. DOI: 10.6028/NIST.IR.8545. URL: https://csrc.nist.gov/pubs/ir/8545/final.

[67] O-RAN Alliance. URL: https://www.o-ran.org/.

[68] Amarisoft. *Amarisoft 4G-5G from the lab to the field*. URL: https://www.amarisoft.com/.

[69] Amazon Web Services. *AWS Ground Station*. URL: https://aws.amazon.com/ground-station/ (visited on Oct. 10, 2024).

[70] George Amponis et al. "Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications". In: *EURASIP Journal on Wireless Communications and Networking* 2022.1 (2022), p. 124.

[71] Mohamad Badra. *Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode*. RFC 5487. Mar. 2009. DOI: 10.17487/RFC5487. URL: https://www.rfc-editor.org/info/rfc5487.

[72] Elaine Barker. *Recommendation for Key Management: Part 1 – General*. NIST Special Publication (SP) 800-57 Part 1 Revision 5. U.S. Department of Commerce, May 2020. DOI: 10.6028/NIST.SP.800-57pt1r5. URL: https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final.

[73] Elaine Barker, Lily Chen, and Dustin Moody. *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*. NIST Special Publication (SP) 800-56B Revision 1. U.S. Department of Commerce, Sept. 2014. DOI: 10.6028/NIST.SP.800-56Br1. URL: https://csrc.nist.gov/pubs/sp/800/56/b/r1/final.

[74] Elaine Barker and Nicky Mouha. *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. NIST Special Publication (SP) 800-67 Revision 2. U.S. Department of Commerce, Nov. 2017. DOI: 10.6028/NIST.SP.800-67r2. URL: https://csrc.nist.gov/pubs/sp/800/67/r2/final.

[75] Elaine Barker and Allen Roginsky. *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST Special Publication (SP) 800-131A Revision 2. U.S. Department of Commerce, Mar. 2019. DOI: 10.6028/NIST.SP.800-131Ar2. URL: https://csrc.nist.gov/pubs/sp/800/131/a/r2/final.

[76] Elaine Barker and Allen Roginsky. *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. NIST Special Publication (SP) 800-131A Revision 3 (Initial Public Draft). U.S. Department of Commerce, Oct. 2024. DOI: doi.org/10.6028/NIST.SP.800-131Ar3.ipd. URL: https://csrc.nist.gov/pubs/sp/800/131/a/r3/ipd.

[77] Elaine Barker et al. *Considerations for Achieving Cryptographic Agility: Strategies and Practices*. NIST Cybersecurity White Paper (CSWP) 39 (Initial Public Draft). U.S. Department of Commerce, Mar. 2025. DOI: 10.6028/NIST.CSWP.39.ipd. URL: https://csrc.nist.gov/pubs/cswp/39/considerations-for-achieving-cryptographic-agility/ipd.

[78] Elaine Barker et al. *Guide to IPsec VPNs*. NIST Special Publication (SP) 800-77 Revision 1. U.S. Department of Commerce, June 2020. DOI: 10.6028/NIST.SP.800-77r1. URL: https://csrc.nist.gov/pubs/sp/800/77/r1/final.

[79] Elaine Barker et al. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. NIST Special Publication (SP) 800-56A Revision 3. U.S. Department of Commerce, Apr. 2018. DOI: 10.6028/NIST.SP.800-56Ar3. URL: https://csrc.nist.gov/pubs/sp/800/56/a/r3/final.

[80] Elaine Barker et al. *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*. NIST Special Publication (SP) 800-56B Revision 2. U.S. Department of Commerce, Mar. 2019. DOI: 10.6028/NIST.SP.800-56Br2. URL: https://csrc.nist.gov/pubs/sp/800/56/b/r2/final.

[81] Elaine Barker et al. *Recommendation for Random Bit Generator (RBG) Constructions*. NIST Special Publication (SP) 800-90C Fourth Public Draft. U.S. Department of Commerce, July 2024. DOI: 10.6028/NIST.SP.800-90C.4pd. URL: https://csrc.nist.gov/pubs/sp/800/90/c/4pd.

[82] Richard Barnes et al. *Deprecating Secure Sockets Layer Version 3.0*. RFC 7568. June 2015. DOI: 10.17487/RFC7568. URL: https://www.rfc-editor.org/info/rfc7568.

[83] David Basin et al. “A Formal Analysis of 5G Authentication”. In: *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*. 2018, pp. 1383–1396.

[84] Alison Becker. *Commercial National Security Algorithm (CNSA) Suite Profile for TLS 1.3*. Internet-Draft draft-becker-cnsa2-tls-profile-01. Work in Progress. Internet Engineering Task Force, Mar. 2025. 13 pp. URL: https://datatracker.ietf.org/doc/draft-becker-cnsa2-tls-profile/01/.

[85] Steven Bellovin. *Guidelines for Specifying the Use of IPsec Version 2*. RFC 5406. Feb. 2009. DOI: 10.17487/RFC5406. URL: https://www.rfc-editor.org/info/rfc5406.

[86] Nathaniel Bennett et al. “RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces”. In: *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*. 2024, pp. 2027–2041.

[87] Daniel J Bernstein. “Curve25519: New Diffie-Hellman Speed Records”. In: *Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings 9*. Springer. 2006, pp. 207–228.

[88] Karthikeyan Bhargavan and Gaëtan Leurent. “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pp. 456–467.

[89] Karthikeyan Bhargavan et al. *Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension*. RFC 7627. Sept. 2015. DOI: 10.17487/RFC7627. URL: https://www.rfc-editor.org/info/rfc7627.

[90] Ashish Bhatia. *How is a Private 5G Network Different from a Public 5G Network?* May 2021. URL: https://www.samsung.com/global/business/networks/insights/blog/0503-how-is-a-private-5g-network-different-from-a-public-5g-network/ (visited on Oct. 1, 2024).

[91] Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. “Differential Resynchronization Attacks on Reduced Round SNOW 3G⊕”. In: *International Conference on E-Business and Telecommunications*. Springer. 2010, pp. 147–157.

[92] Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. “Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3G⊕”. In: *Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010. Proceedings 8*. Springer. 2010, pp. 139–153.

[93] David L. Black and David McGrew. *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*. RFC 5282. Aug. 2008. DOI: 10.17487/RFC5282. URL: https://www.rfc-editor.org/info/rfc5282.

[94] Alejandro Blanco et al. “Performance Evaluation of Single Base Station ToA-AoA Localization in an LTE Testbed”. In: *2019 IEEE 30th annual international symposium on personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE. 2019, pp. 1–6.

[95] Sharon Boeyen et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. May 2008. DOI: 10.17487/RFC5280. URL: https://www.rfc-editor.org/info/rfc5280.

[96] John Border and Jeff Heath. *IP Payload Compression Using ITU-T V.44 Packet Method*. RFC 3051. Jan. 2001. DOI: 10.17487/RFC3051. URL: https://www.rfc-editor.org/info/rfc3051.

[97] Ravishankar Borgaonkar et al. “New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols”. In: *Cryptology ePrint Archive* (2018).

[98] Nicolò Boschetti, Nathaniel G Gordon, and Gregory Falco. “Space Cybersecurity Lessons Learned from the ViaSat Cyberattack”. In: *ASCEND 2022*. American Institute of Aeronautics and Astronautics, 2022, p. 4380.

[99] Daniel R. L. Brown. *SEC 1: Elliptic Curve Cryptography*. Standards for Efficient Cryptography 1 (SEC 1). Certicom Research, May 2009. URL: https://www.secg.org/sec1-v2.pdf.

[100] Daniel R. L. Brown. *SEC 2: Recommended Elliptic Curve Domain Parameters*. Standards for Efficient Cryptography 2 (SEC 2). Certicom Research, Jan. 2010. URL: https://www.secg.org/sec2-v2.pdf.

[101] Billy Bob Brumley and Nicola Tuveri. "Remote Timing Attacks Are Still Practical". In: *European Symposium on Research in Computer Security*. Springer. 2011, pp. 355–371.

[102] Billy Bob Brumley et al. "Consecutive S-box Lookups: A Timing Attack on SNOW 3G". In: *Information and Communications Security: 12th International Conference, ICICS 2010, Barcelona, Spain, December 15-17, 2010. Proceedings 12*. Springer. 2010, pp. 171–185.

[103] David Brumley and Dan Boneh. "Remote timing attacks are practical". In: *Computer Networks* 48.5 (2005), pp. 701–716.

[104] Bundesamt für Sicherheit in der Informationstechnik (BSI). *pySCASso*. URL: https://github.com/BSI-Bund/pySCASso.

[105] Nancy Cam-Winget and Jack Visoky. *TLS 1.3 Authentication and Integrity-Only Cipher Suites*. RFC 9150. Apr. 2022. DOI: 10.17487/RFC9150. URL: https://www.rfc-editor.org/info/rfc9150.

[106] Brice Canvel et al. "Password Interception in a SSL/TLS Channel". In: *Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23*. Springer. 2003, pp. 583–599.

[107] Lidong Chen et al. *Report on Post-Quantum Cryptography*. NIST Interagency/Internal Report (NISTIR) 8105. U.S. Department of Commerce, Apr. 2016. DOI: https://doi.org/10.6028/NIST.IR.8105. URL: https://www.nist.gov/publications/report-post-quantum-cryptography.

[108] Lily Chen. *NIST Policy on Hash Functions*. NIST. Dec. 2022. URL: https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1 (visited on Mar. 15, 2025).

[109] Lily Chen. *Recommendation for Key Derivation Using Pseudorandom Functions*. NIST Special Publication (SP) 800-108 Revision 1. U.S. Department of Commerce, Feb. 2024. DOI: 10.6028/NIST.SP.800-108r1-upd1. URL: https://csrc.nist.gov/pubs/sp/800/108/r1/upd1/final.

[110] Lily Chen et al. *Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters*. NIST Special Publication (SP) 800-186. U.S. Department of Commerce, Feb. 2023. DOI: 10.6028/NIST.SP.800-186. URL: https://csrc.nist.gov/pubs/sp/800/186/final.

[111] Merlin Chlosta et al. "5G SUCI-Catchers: Still catching them all?" In: *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2021, pp. 359–364.

[112] Merlin Chlosta et al. "LTE security disabled: misconfiguration in commercial networks". In: *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*. 2019, pp. 261–266.

[113] Charles Clancy, Robert McGwier, and Lidong Chen. "Post-quantum cryptography and 5G security: Tutorial". In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 2019, pp. 285–285.

[114] Edmund Clarke et al. "Counterexample-Guided Abstraction Refinement". In: *Computer Aided Verification: 12th International Conference, CAV 2000, Chicago, IL, USA, July 15-19, 2000. Proceedings 12*. Springer. 2000, pp. 154–169.

[115] Jiska Classen et al. "Starshields for iOS: Navigating the Security Cosmos in Satellite Communication". In: *Network and Distributed Systems Security (NDSS) Symposium 2025* (2025).

[116] Committee on National Security Systems (CNSSP). *CNSSP 15 - Use of Public Standards for Secure Information Sharing*. Committee on National Security Systems (CNSSP). Oct. 2016. URL: https://www.cnss.gov/CNSS/issuances/Policies.cfm (visited on June 1, 2025).

[117] Committee on National Security Systems (CNSSP). *CNSSP 15 - Use of Public Standards for Secure Information Sharing*. Committee on National Security Systems (CNSSP). Dec. 2024. URL: https://www.cnss.gov/CNSS/issuances/Policies.cfm (visited on Mar. 16, 2025).

[118] Deirdre Connolly. *ML-KEM Post-Quantum Key Agreement for TLS 1.3*. Internet-Draft draft-ietf-tls-mlkem-00. Work in Progress. Internet Engineering Task Force, Apr. 2025. 11 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-mlkem/00/.

[119] Consultative Committee for Space Data Systems (CCSDS). URL: https://public.ccsds.org/default.aspx (visited on Oct. 12, 2024).

[120] Consultative Committee for Space Data Systems (CCSDS). *Overview of Space Communication Protocols*. Apr. 2023. URL: https://public.ccsds.org/Pubs/130x0g4e1.pdf (visited on Oct. 12, 2024).

[121] Deb Cooley. *Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3*. RFC 9151. Apr. 2022. DOI: 10.17487/RFC9151. URL: https://www.rfc-editor.org/info/rfc9151.

[122] Laura Corcoran and Michael J. Jenkins. *Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)*. RFC 9206. Mar. 2022. DOI: 10.17487/RFC9206. URL: https://www.rfc-editor.org/info/rfc9206.

[123] Andy Coulbeck et al. *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*. RFC 2252. Dec. 1997. DOI: 10.17487/RFC2252. URL: https://www.rfc-editor.org/info/rfc2252.

[124] Cas Cremers and Martin Dehnel-Wild. "Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion". In: *Network and Distributed System Security Symposium (NDSS)*. Internet Society. 2019.

[125] Adrian Dabrowski, Georg Petzl, and Edgar R Weippl. "The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection". In: *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19*. Springer. 2016, pp. 279–302.

[126] Adrian Dabrowski et al. "IMSI-catch me if you can: IMSI-catcher-catchers". In: *Proceedings of the 30th annual computer security applications Conference*. 2014, pp. 246–255.

[127] Quynh Dang. *Recommendation for Applications Using Approved Hash Algorithms*. NIST Special Publication (SP) 800-107 Revision 1. U.S. Department of Commerce, Aug. 2012. DOI: 10.6028/NIST.SP.800-107r1. URL: https://csrc.nist.gov/pubs/sp/800/107/r1/final.

[128] Blandine Debraize and Irene Marquez Corbella. "Fault Analysis of the Stream Cipher Snow 3G". In: *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE. 2009, pp. 103–110.

[129] Jean Paul Degabriele et al. "The Security of ChaCha20-Poly1305 in the Multi-User Setting". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021, pp. 1981–2003.

[130] Van Thuan Do et al. "Strengthening Mobile Network Security Using Machine Learning". In: *Mobile Web and Intelligent Information Systems: 13th International Conference, MobiWIS 2016, Vienna, Austria, August 22-24, 2016, Proceedings 13*. Springer. 2016, pp. 173–183.

[131] Naganand Doraswamy and Cheryl R. Madson. *The ESP DES-CBC Cipher Algorithm With Explicit IV*. RFC 2405. Nov. 1998. DOI: 10.17487/RFC2405. URL: https://www.rfc-editor.org/info/rfc2405.

[132] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation*. NIST Special Publication (SP) 800-38A. U.S. Department of Commerce, Dec. 2001. DOI: 10.6028/NIST.SP.800-38A. URL: https://csrc.nist.gov/pubs/sp/800/38/a/final.

[133] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication (SP) 800-38D. U.S. Department of Commerce, Nov. 2007. DOI: 10.6028/NIST.SP.800-38D. URL: https://csrc.nist.gov/pubs/sp/800/38/d/final.

[134] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication*. NIST Special Publication (SP) 800-38B. U.S. Department of Commerce, May 2005. DOI: 10.6028/NIST.SP.800-38B. URL: https://csrc.nist.gov/pubs/sp/800/38/b/upd1/final.

[135] RFC Editor and Heather Flanagan. *RFC Style Guide*. RFC 7322. Sept. 2014. DOI: 10.17487/RFC7322. URL: https://www.rfc-editor.org/info/rfc7322.

[136] Mohamed El Jaafari et al. “Introduction to the 3GPP-defined NTN standard: A comprehensive view on the 3GPP work on NTN”. In: *International Journal of Satellite Communications and Networking* 41.3 (2023), pp. 220–238.

[137] Stavros Eleftherakis, Domenico Giustiniano, and Nicolas Kourtellis. “SoK: Evaluating 5G Protocols Against Legacy and Emerging Privacy and Security Attacks”. In: *arXiv preprint arXiv:2409.06360* (2024).

[138] Stavros Eleftherakis et al. “Demystifying Privacy in 5G Stand Alone Networks”. In: *arXiv preprint arXiv:2409.17700* (2024).

[139] ENISA. *ENISA Threat Landscape for 5G Networks Report*. Report. ENISA, Dec. 2020. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks.

[140] ENISA. *Security in 5G Specifications - Controls in 3GPP*. Report. ENISA, Feb. 2021. URL: https://www.enisa.europa.eu/publications/security-in-5g-specifications.

[141] ENISA. *Signalling Security in Telecom SS7/Diameter/5G*. Report. ENISA, Mar. 2018. URL: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g.

[142] ENISA. *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*. Report. ENISA, Jan. 2016. URL: https://www.enisa.europa.eu/publications/sdn-threat-landscape.

[143] Ericsson. *Ericsson Mobility Report Business Review 2024*. Report. Ericsson, 2024. URL: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/business-review.

[144] Ericsson. *Ericsson Mobility Report June 2024*. Tech. rep. Ericsson, 2024. URL: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2024.

[145] Simon Erni et al. “AdaptOver: adaptive overshadowing attacks in cellular networks”. In: *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*. 2022, pp. 743–755.

[146] Pasi Eronen et al. *Transport Layer Security (TLS) Session Resumption without Server-Side State*. RFC 5077. Jan. 2008. DOI: 10.17487/RFC5077. URL: https://www.rfc-editor.org/info/rfc5077.

[147] European Space Agency (ESA). *Space Attacks and Countermeasures Engineering Shield (SPACE-SHIELD)*. URL: https://spaceshield.esa.int/ (visited on July 25, 2025).

[148] European Space Agency (ESA). *Types of orbits*. Mar. 2020. URL: https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits (visited on Oct. 11, 2024).

[149] European Telecommunications Standards Institute (ETSI). *5G*. 2020. URL: https://www.etsi.org/technologies/5g (visited on Sept. 23, 2024).

[150] European Telecommunications Standards Institute (ETSI). *Algorithms & Codes*. URL: https://www.etsi.org/security-algorithms-and-codes (visited on Mar. 25, 2025).

[151] European Telecommunications Standards Institute (ETSI). *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 5: Design and evaluation report*. ETSI/SAGE Technical Report. Version 1.1. ETSI, Sept. 2006. URL: https://www.gsma.com/about-us/wp-content/uploads/2014/12/uea2designevaluation.pdf.

[152] Richard P Feynman. “Simulating Physics with Computers”. In: *Feynman and computation*. cRc Press, 2018, pp. 133–153.

[153] Roy T. Fielding, Mark Nottingham, and Julian Reschke. *HTTP Semantics*. RFC 9110. June 2022. DOI: 10.17487/RFC9110. URL: https://www.rfc-editor.org/info/rfc9110.

[154] Roy T. Fielding, Mark Nottingham, and Julian Reschke. *HTTP/1.1*. RFC 9112. June 2022. DOI: 10.17487/RFC9112. URL: https://www.rfc-editor.org/info/rfc9112.

[155] Scott Fluhrer et al. *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*. RFC 8784. June 2020. DOI: 10.17487/RFC8784. URL: https://www.rfc-editor.org/info/rfc8784.

[156] Sheila Frankel, K. Robert Glenn, and Scott G. Kelly. *The AES-CBC Cipher Algorithm and Its Use with IPsec*. RFC 3602. Sept. 2003. DOI: 10.17487/RFC3602. URL: https://www.rfc-editor.org/info/rfc3602.

[157] Sheila Frankel and Howard C. Herbert. *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*. RFC 3566. Sept. 2003. DOI: 10.17487/RFC3566. URL: https://www.rfc-editor.org/info/rfc3566.

[158] Sheila Frankel and Scott G. Kelly. *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*. RFC 4868. May 2007. DOI: 10.17487/RFC4868. URL: https://www.rfc-editor.org/info/rfc4868.

[159] Alan O. Freier, Philip Karlton, and Paul C. Kocher. *The Secure Sockets Layer (SSL) Protocol Version 3.0*. RFC 6101. Aug. 2011. DOI: 10.17487/RFC6101. URL: https://www.rfc-editor.org/info/rfc6101.

[160] Robert C. Friend and Robert Monsour. *IP Payload Compression Using LZS*. RFC 2395. Dec. 1998. DOI: 10.17487/RFC2395. URL: https://www.rfc-editor.org/info/rfc2395.

[161] David E. Fu and Jerome Solinas. *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. RFC 4754. Jan. 2007. DOI: 10.17487/RFC4754. URL: https://www.rfc-editor.org/info/rfc4754.

[162] David Galindo and Flavio D Garcia. "A Schnorr-like lightweight identity-based signature scheme". In: *Progress in Cryptology–AFRICACRYPT 2009: Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21-25, 2009. Proceedings 2*. Springer. 2009, pp. 135–148.

[163] Matheus E Garbelini et al. "Towards Automated Fuzzing of 4G/5G Protocol Implementations Over the Air". In: *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE. 2022, pp. 86–92.

[164] Gabriel K Gegenhuber, Philipp É Frenzel, and Edgar Weippl. "Why ET Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi". In: *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services*. 2024, pp. 183–195.

[165] Gabriel K Gegenhuber et al. "Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments". In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 451–468.

[166] Daniel Kahn Gillmor. *Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)*. RFC 7919. Aug. 2016. DOI: 10.17487/RFC7919. URL: https://www.rfc-editor.org/info/rfc7919.

[167] K. Robert Glenn and Stephen Kent. *The NULL Encryption Algorithm and Its Use With IPsec*. RFC 2410. Nov. 1998. DOI: 10.17487/RFC2410. URL: https://www.rfc-editor.org/info/rfc2410.

[168] K. Robert Glenn and Cheryl R. Madson. *The Use of HMAC-MD5-96 within ESP and AH*. RFC 2403. Nov. 1998. DOI: 10.17487/RFC2403. URL: https://www.rfc-editor.org/info/rfc2403.

[169] K. Robert Glenn and Cheryl R. Madson. *The Use of HMAC-SHA-1-96 within ESP and AH*. RFC 2404. Nov. 1998. DOI: 10.17487/RFC2404. URL: https://www.rfc-editor.org/info/rfc2404.

[170] *Global Satellite Launch Forecast (2024-2030)*. Apr. 2024. URL: https://space-inventor.com/news/how-will-the-satellite-market-evolve-in-the-coming-years (visited on Oct. 7, 2024).

[171] German Peinado Gomez et al. “Security policies definition and enforcement utilizing policy control function framework in 5G”. In: *Computer Communications* 172 (2021), pp. 226–237.

[172] Rafal Graczyk, Paulo Esteves-Verissimo, and Marcus Voelp. “Sanctuary lost: a cyber-physical warfare in space”. In: *arXiv preprint arXiv:2110.05878* (2021).

[173] Lov K Grover. “A fast quantum mechanical algorithm for database search”. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 212–219.

[174] GSM Association (GSMA). *The Mobile Economy Europe 2025*. Report. GSMA, 2025. URL: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/europe/.

[175] Shay Gueron, Adam Langley, and Yehuda Lindell. *AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption*. RFC 8452. Apr. 2019. DOI: 10.17487/RFC8452. URL: https://www.rfc-editor.org/info/rfc8452.

[176] *Guide to Deploying Diffie-Hellman for TLS*. May 2015. URL: https://weakdh.org/sysadmin.html (visited on Mar. 23, 2025).

[177] Alessandro Guidotti et al. “Architectures and Key Technical Challenges for 5G Systems Incorporating Satellites”. In: *IEEE Transactions on Vehicular Technology* 68.3 (2019), pp. 2624–2639.

[178] Ali Güngör. *GitHub - free5gc/free5gc: Open source 5G core network based on 3GPP R15*. URL: https://github.com/aligungr/UERANSIM.

[179] Shubham Gupta, Balu L Parne, and Narendra S Chaudhari. “Security Vulnerabilities in Handover Authentication Mechanism of 5G Network”. In: *2018 First international conference on secure cyber computing and communication (ICSCCC)*. IEEE. 2018, pp. 369–374.

[180] Rebecca Guthrie. *Commercial National Security Algorithm (CNSA) Suite 2.0 Profile for IPsec*. Internet-Draft draft-guthrie-cnsa2-ipsec-profile-00. Work in Progress. Internet Engineering Task Force, Mar. 2025. 18 pp. URL: https://datatracker.ietf.org/doc/draft-guthrie-cnsa2-ipsec-profile/00/.

[181] Jack Haddon. *Apple expands satellite messaging beyond emergency calls*. June 2024. URL: https://www.capacitymedia.com/article/2dd1f76g4ah04c1qnglj4/news/apple-expands-satellite-messaging-beyond-emergency-calls (visited on July 2, 2025).

[182] Ibrahim Hajjeh and Mohamad Badra. *ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)*. RFC 5489. Mar. 2009. DOI: 10.17487/RFC5489. URL: https://www.rfc-editor.org/info/rfc5489.

[183] Taha Hammouchi, D Rupprecht, and KS Kohls. “Intrusion Detection System for 5G Core Systems”. MA thesis. Radboud University Nijmegen, 2023.

[184] Thijs Heijligenberg et al. “BigMac: Performance Overhead of User Plane Integrity Protection in 5G Networks”. In: *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2023, pp. 145–150.

[185] Andreas Hein and Citlali Bruce Rosete. “Space-as-a-Service: A Framework and Taxonomy of-as-a-Service Concepts for Space”. In: *International Astronautical Congress 2022*. 2022.

[186] Paul E. Hoffman. *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*. RFC 4434. Feb. 2006. DOI: 10.17487/RFC4434. URL: https://www.rfc-editor.org/info/rfc4434.

[187] Gerrit Holtrup et al. “5G System Security Analysis”. In: *arXiv preprint arXiv:2108.08700* (2021).

[188] Mark Horowitz and Emily Grumbling. *Quantum Computing: Progress and Prospects*. National Academies Press, 2019.

[189] Russ Housley. *TLS 1.3 Extension for Certificate-Based Authentication with an External Pre-Shared Key*. RFC 8773. Mar. 2020. DOI: 10.17487/RFC8773. URL: https://www.rfc-editor.org/info/rfc8773.

[190] Russ Housley. *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*. RFC 4309. Dec. 2005. DOI: 10.17487/RFC4309. URL: https://www.rfc-editor.org/info/rfc4309.

[191] Russ Housley. *Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)*. RFC 3686. Jan. 2004. DOI: 10.17487/RFC3686. URL: https://www.rfc-editor.org/info/rfc3686.

[192] Xinxin Hu et al. "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security". In: *IEEE Access* 7 (2019), pp. 125424–125441.

[193] Syed Hussain et al. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE". In: *Network and Distributed Systems Security (NDSS) Symposium 2018*. 2018.

[194] Syed Rafiul Hussain et al. "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019, pp. 669–684.

[195] Syed Rafiul Hussain et al. "Insecure connection bootstrapping in cellular networks: the root of all evil". In: *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*. 2019, pp. 1–11.

[196] Syed Rafiul Hussain et al. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information". In: *Network and distributed systems security (NDSS) symposium2019* (2019).

[197] International Organization for Standardization (ISO). *ISO - 35.100 - Open systems interconnection (OSI)*. URL: https://www.iso.org/ics/35.100/x/ (visited on Dec. 23, 2024).

[198] Internet Assigned Numbers Authority (IANA). *Internet Key Exchange Version 2 (IKEv2) Parameters*. IANA, Jan. 2005. URL: https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml (visited on Feb. 15, 2025).

[199] Onur İşler. "Implementation and Performance Evaluation of Elliptic Curve Cryptography over SECP256R1 on STM32 Microprocessor". In: *Cryptology ePrint Archive* (2024).

[200] Michael J. Jenkins and Alison Becker. *Commercial National Security Algorithm Suite Certificate and Certificate Revocation List Profile*. Internet-Draft draft-jenkins-cnsa2-pkix-profile-02. Work in Progress. Internet Engineering Task Force, Apr. 2025. 10 pp. URL: https://datatracker.ietf.org/doc/draft-jenkins-cnsa2-pkix-profile/02/.

[201] Michael J. Jenkins and Lydia Zieglar. *Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile*. RFC 8603. May 2019. DOI: 10.17487/RFC8603. URL: https://www.rfc-editor.org/info/rfc8603.

[202] Rajeshwar Jenwar et al. *Protocol Support for High Availability of IKEv2/IPsec*. RFC 6311. July 2011. DOI: 10.17487/RFC6311. URL: https://www.rfc-editor.org/info/rfc6311.

[203] Erik Thormarker John Preuß Mattsson Ben Smeets. *Quantum technology and its impact on security in mobile networks*. 2021. URL: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum (visited on Apr. 1, 2025).

[204] Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication (SP) 800-53 Revision 5. U.S. Department of Commerce, Dec. 2020. DOI: 10.6028/NIST.SP.800-53r5. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[205] Roger Piqueras Jover. "LTE security, protocol exploits and location tracking experimentation with low-cost software radio". In: *arXiv preprint arXiv:1607.05171* (2016).

[206] Roger Piqueras Jover and Vuk Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications". In: *IEEE Access* 7 (2019), pp. 24956–24963.

[207] Panos Kampanakis and Gerardo Ravago. *Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)*. Internet-Draft draft-kampanakis-ml-kem-ikev2-09. Work in Progress. Internet Engineering Task Force, Nov. 2024. 10 pp. URL: https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/09/.

[208] Bedran Karakoc et al. “Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G”. In: *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2023, pp. 97–108.

[209] Charlie Kaufman et al. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 7296. Oct. 2014. DOI: 10.17487/RFC7296. URL: https://www.rfc-editor.org/info/rfc7296.

[210] Stephen Kent. *IP Authentication Header*. RFC 4302. Dec. 2005. DOI: 10.17487/RFC4302. URL: https://www.rfc-editor.org/info/rfc4302.

[211] Stephen Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Dec. 2005. DOI: 10.17487/RFC4303. URL: https://www.rfc-editor.org/info/rfc4303.

[212] Haibat Khan, Benjamin Dowling, and Keith M Martin. “Identity Confidentiality in 5G Mobile Telephony Systems”. In: *International Conference on Research in Security Standardisation*. Springer. 2018, pp. 120–142.

[213] Rohit Khare and Scott Lawrence. *Upgrading to TLS Within HTTP/1.1*. RFC 2817. May 2000. DOI: 10.17487/RFC2817. URL: https://www.rfc-editor.org/info/rfc2817.

[214] Hongil Kim et al. “Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations”. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 2015, pp. 328–339.

[215] Hongil Kim et al. “Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane”. In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 1153–1168.

[216] Richard Kissel et al. *Guidelines for Media Sanitization*. NIST Special Publication (SP) 800-88 Revision 1. U.S. Department of Commerce, Dec. 2014. DOI: 10.6028/NIST.SP.800-88r1. URL: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

[217] Tero Kivinen and Joel Snyder. *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*. RFC 7427. Jan. 2015. DOI: 10.17487/RFC7427. URL: https://www.rfc-editor.org/info/rfc7427.

[218] Oltjon Kodheli et al. “Satellite Communications in the New Space Era: A Survey and Future Challenges”. In: *IEEE Communications Surveys & Tutorials* 23.1 (2020), pp. 70–109.

[219] Mika Kojo and Tero Kivinen. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. RFC 3526. May 2003. DOI: 10.17487/RFC3526. URL: https://www.rfc-editor.org/info/rfc3526.

[220] Adrien Koutsos. “The 5G-AKA Authentication Protocol Privacy”. In: *2019 IEEE European symposium on security and privacy (EuroS&P)*. IEEE. 2019, pp. 464–479.

[221] Joern Krause. *Non-Terrestrial Networks (NTN)*. May 2024. URL: https://www.3gpp.org/technologies/ntn-overview (visited on Oct. 21, 2024).

[222] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. *HMAC: Keyed-Hashing for Message Authentication*. RFC 2104. Feb. 1997. DOI: 10.17487/RFC2104. URL: https://www.rfc-editor.org/info/rfc2104.

[223] Erik Kulu. “Satellite Constellations - 2021 Industry Survey and Trends”. In: *35th Annual Small Satellite Conference* (2021).

[224] Bell Laboratories, Scott Lawrence, and Vijay K. Gurbani. *Domain Certificates in the Session Initiation Protocol (SIP)*. RFC 5922. June 2010. DOI: 10.17487/RFC5922. URL: https://www.rfc-editor.org/info/rfc5922.

[225] Xavier Lagrange. *5G Network Fundamentals*. Nov. 2022. URL: https://www.coursera.org/learn/5g-network-fundamentals (visited on Jan. 6, 2025).

[226] Adam Langley. *The POODLE bites again*. ImperialViolet. Dec. 2014. URL: https://www.imperialviolet.org/2014/12/08/poodleagain.html (visited on Mar. 23, 2025).

[227] Adam Langley, Mike Hamburg, and Sean Turner. *Elliptic Curves for Security*. RFC 7748. Jan. 2016. DOI: 10.17487/RFC7748. URL: https://www.rfc-editor.org/info/rfc7748.

[228] Oscar Lasierra et al. “European 5G Security in the Wild: Reality versus Expectations”. In: *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2023, pp. 13–18.

[229] Scott Lawrence and Vijay K. Gurbani. *Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates*. RFC 5924. June 2010. DOI: 10.17487/RFC5924. URL: https://www.rfc-editor.org/info/rfc5924.

[230] Seungbin Lee and Jiyoon Kim. “Survey on Security for Non-Terrestrial Networks”. In: *Research Briefs on Information & Communication Technology Evolution (ReBICTE)* 10.7 (2024), pp. 111–123.

[231] Sukchan Lee. *Open5GS*. URL: https://github.com/open5gs.

[232] Dr. Steven Legg. *Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules*. RFC 4517. June 2006. DOI: 10.17487/RFC4517. URL: https://www.rfc-editor.org/info/rfc4517.

[233] Matt Lepinski and Stephen Kent. *Additional Diffie-Hellman Groups for Use with IETF Standards*. RFC 5114. Jan. 2008. DOI: 10.17487/RFC5114. URL: https://www.rfc-editor.org/info/rfc5114.

[234] Gaëtan Leurent and Thomas Peyrin. “From Collisions to Chosen-Prefix Collisions Application to Full SHA-1”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 527–555.

[235] Gaëtan Leurent and Thomas Peyrin. “SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust”. In: *29th USENIX Security Symposium (USENIX Security 20)*. 2020, pp. 1839–1856.

[236] Matt Lewis. *Investigating Potential Security Vulnerability Manifestation through Various Analyses & Inferences Regarding Internet RFCs, and how RFC Security might be Improved*. Jan. 2021. URL: https://www.nccgroup.com/us/research-blog/investigating-potential-security-vulnerability-manifestation-through-various-analyses-inferences-regarding-internet-rfcs-and-how-rfc-security-might-be-improved/ (visited on Mar. 26, 2025).

[237] Mu Li et al. “A 5G NTN-RAN Implementation Architecture with Security”. In: *2022 4th International Conference on Communications, Information System and Computer Engineering (CISCE)*. IEEE. 2022, pp. 42–45.

[238] Zhenhua Li et al. “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild”. In: *NDSS*. 2017.

[239] Andy Lilly. “IMSI catchers: hacking mobile communications”. In: *Network Security* 2017.2 (2017), pp. 5–7.

[240] Xingqin Lin et al. “5G from Space: An Overview of 3GPP Non-Terrestrial Networks”. In: *IEEE Communications Standards Magazine* 5.4 (2021), pp. 147–153.

[241] Linux Foundation Projects. *free5gc*. URL: https://github.com/free5gc/free5gc.

[242] Linux Foundation Projects. *free5GC compose*. URL: https://github.com/free5gc/free5gc-compose.

[243] David Livingstone and Patricia Lewis. *Space, the Final Frontier for Cybersecurity?* Chatham House. The Royal Institute of International Affairs, 2016.

[244] Norbert Ludant and Guevara Noubir. “SigUnder: A stealthy 5G low power attack and defenses”. In: *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2021, pp. 250–260.

[245] Norbert Ludant, Marinos Vomvas, and Guevara Noubir. “Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous”. In: *arXiv preprint arXiv:2403.06717* (2024).

[246] Mohammed Mahyoub et al. “Security Analysis of Critical 5G Interfaces”. In: *IEEE Communications Surveys & Tutorials* (2024).

[247] Mark Manulis et al. “Cyber security in New Space: Analysis of threats, key enabling technologies and challenges”. In: *International Journal of Information Security* 20.3 (2021), pp. 287–311.

[248] Gino Masini et al. “5G meets satellite: Non-terrestrial network architecture and 3GPP”. In: *International Journal of Satellite Communications and Networking* 41.3 (2023), pp. 249–261.

[249] John Preuß Mattsson and Daniel Migault. *ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2*. RFC 8442. Sept. 2018. DOI: 10.17487/RFC8442. URL: https://www.rfc-editor.org/info/rfc8442.

[250] John Preuß Mattsson, Erik Thormarker, and Ben Smeets. *Migration to quantum-resistant algorithms in mobile networks*. Feb. 2023. URL: https://www.ericsson.com/en/blog/2023/2/quantum-resistant-algorithms-mobile-networks (visited on Apr. 1, 2025).

[251] David McGrew. *An Interface and Algorithms for Authenticated Encryption*. RFC 5116. Jan. 2008. DOI: 10.17487/RFC5116. URL: https://www.rfc-editor.org/info/rfc5116.

[252] David McGrew and Daniel Bailey. *AES-CCM Cipher Suites for Transport Layer Security (TLS)*. RFC 6655. July 2012. DOI: 10.17487/RFC6655. URL: https://www.rfc-editor.org/info/rfc6655.

[253] Kerry McKay and David Cooper. *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. NIST Special Publication (SP) 800-52 Revision 2. U.S. Department of Commerce, Aug. 2019. DOI: 10.6028/NIST.SP.800-52r2. URL: https://csrc.nist.gov/pubs/sp/800/52/r2/final.

[254] Simon Meier et al. “The TAMARIN Prover for the Symbolic Analysis of Security Protocols”. In: *International conference on computer aided verification*. Springer. 2013, pp. 696–701.

[255] Robert Merget et al. “Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)”. In: *30th USENIX Security Symposium (USENIX Security 21)*. 2021, pp. 213–230.

[256] Sotiris Michaelides et al. “Secure integration of 5G in industrial networks: State of the art, challenges and opportunities”. In: *Future Generation Computer Systems* (2024), p. 107645.

[257] Benoit Michau and Christophe Devine. “How to not break LTE crypto”. In: *ANSSI Symposium sur la sécurité des technologies de l’information et des communications (SSTIC)*. 2016.

[258] Microsoft. *Microsoft Threat Modeling Tool threats*. Aug. 2022. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model (visited on Dec. 8, 2024).

[259] Microsoft Azure. *Azure Orbital Ground Station*. URL: https://azure.microsoft.com/en-us/products/orbital/ (visited on Oct. 10, 2024).

[260] Daniel Migault, Tobias Guggemos, and Yoav Nir. *Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)*. RFC 8750. Mar. 2020. DOI: 10.17487/RFC8750. URL: https://www.rfc-editor.org/info/rfc8750.

[261] TANG Ming, CHENG PingPan, and QIU ZhenLong. “Differential Power Analysis on ZUC Algorithm”. In: *Cryptology ePrint Archive* (2012).

[262] Chris J Mitchell. “The impact of quantum computing on real-world security: A 5G case study”. In: *Computers & Security* 93 (2020), p. 101825.

[263] Stig F Mjølsnes and Ruxandra F Olimid. “Easy 4G/LTE IMSI Catchers for Non-Programmers”. In: *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7*. Springer. 2017, pp. 235–246.

[264] Bodo Möller, Thai Duong, and Krzysztof Kotowicz. “This POODLE Bites: Exploiting The SSL 3.0 Fallback”. In: *Security Advisory* 21 (2014), pp. 34–58.

[265] Bob Monsour et al. *IP Payload Compression Protocol (IPComp)*. RFC 3173. Sept. 2001. DOI: 10.17487/RFC3173. URL: https://www.rfc-editor.org/info/rfc3173.

[266] Kathleen Moriarty and Stephen Farrell. *Deprecating TLS 1.0 and TLS 1.1*. RFC 8996. Mar. 2021. DOI: 10.17487/RFC8996. URL: https://www.rfc-editor.org/info/rfc8996.

[267] Kathleen Moriarty et al. *PKCS #1: RSA Cryptography Specifications Version 2.2*. RFC 8017. Nov. 2016. DOI: 10.17487/RFC8017. URL: https://www.rfc-editor.org/info/rfc8017.

[268] Bruce Morton. *TLS Protocol 1.2 Vulnerable to Raccoon Attack*. Entrust. Sept. 2020. URL: https://www.entrust.com/blog/2020/09/tls-protocol-1-2-vulnerable-to-raccoon-attack (visited on Mar. 23, 2025).

[269] Michele Mosca. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" In: *IEEE Security & Privacy* 16.5 (2018), pp. 38–41.

[270] Michele Mosca and Marco Piani. *2021 Quantum Threat Timeline Report*. Report. Global Risk Institute, 2022.

[271] Michele Mosca and Marco Piani. *Quantum Threat Timeline Report 2024*. Report. Global Risk Institute, Dec. 2024.

[272] Nicky Mouha and Morris Dworkin. *Report on the Block Cipher Modes of Operation in the NIST SP 800-38 Series*. NIST Interagency/Internal Report (NISTIR) 8459. U.S. Department of Commerce, Sept. 2024. DOI: doi.org/10.6028/NIST.IR.8459. URL: https://csrc.nist.gov/pubs/ir/8459/final.

[273] Chandra Sekhar Mukherjee, Dibyendu Roy, and Subhamoy Maitra. *Design and Cryptanalysis of ZUC: A Stream Cipher in Mobile Telephony*. Springer, 2021.

[274] S murthy, Sean Shen, and Yu Mao. *Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol*. RFC 5930. July 2010. DOI: 10.17487/RFC5930. URL: https://www.rfc-editor.org/info/rfc5930.

[275] Pramod Nair. *Securing 5G and Evolving Architectures*. Addison-Wesley Professional, 2021.

[276] National Aeronautics and Space Administration (NASA). *Sputnik 1*. NASA. URL: https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1957-001B (visited on Oct. 8, 2024).

[277] National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publications (FIPS) 197. U.S. Department of Commerce, Nov. 2001. DOI: 10.6028/NIST.FIPS.197-upd1. URL: https://csrc.nist.gov/pubs/fips/197/final.

[278] National Institute of Standards and Technology (NIST). *Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*. NIST. Aug. 2024. URL: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved (visited on Mar. 31, 2025).

[279] National Institute of Standards and Technology (NIST). *Block Cipher Techniques*. NIST. Feb. 2025. URL: https://csrc.nist.gov/projects/block-cipher-techniques (visited on Mar. 15, 2025).

[280] National Institute of Standards and Technology (NIST). *Cryptographic Algorithm Validation Program*. NIST. Feb. 2025. URL: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program (visited on Mar. 15, 2025).

[281] National Institute of Standards and Technology (NIST). *Cryptographic Module Validation Program*. NIST. Mar. 2025. URL: https://csrc.nist.gov/projects/cmvp/sp800-140c (visited on Mar. 15, 2025).

[282] National Institute of Standards and Technology (NIST). *CVE-2014-0160 Detail*. NIST. Feb. 2025. URL: https://nvd.nist.gov/vuln/detail/CVE-2014-0160 (visited on Mar. 23, 2025).

[283] National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication (FIPS) 186-4. U.S. Department of Commerce, July 2013. DOI: 10.6028/NIST.FIPS.186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[284] National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication (FIPS) 186-5. U.S. Department of Commerce, Feb. 2023. DOI: 10.6028/NIST.FIPS.186-5. URL: https://csrc.nist.gov/pubs/fips/186-5/final.

[285] National Institute of Standards and Technology (NIST). *Digital Signatures*. NIST. Nov. 2024. URL: https://csrc.nist.gov/projects/digital-signatures (visited on Mar. 16, 2025).

[286] National Institute of Standards and Technology (NIST). *Hash Functions*. NIST. Sept. 2024. URL: https://csrc.nist.gov/projects/hash-functions (visited on Mar. 15, 2025).

[287] National Institute of Standards and Technology (NIST). *Lightweight Cryptography*. NIST. Apr. 2025. URL: https://csrc.nist.gov/projects/lightweight-cryptography (visited on July 1, 2025).

[288] National Institute of Standards and Technology (NIST). *Lightweight Cryptography Standardization Process: NIST Selects Ascon*. NIST. Feb. 2023. URL: https://csrc.nist.gov/news/2023/lightweight-cryptography-nist-selects-ascon (visited on July 1, 2025).

[289] National Institute of Standards and Technology (NIST). *Message Authentication Codes*. NIST. Sept. 2024. URL: https://csrc.nist.gov/projects/message-authentication-codes (visited on Mar. 15, 2025).

[290] National Institute of Standards and Technology (NIST). *Module-Lattice-Based Digital Signature Standard*. Federal Information Processing Standards Publication (FIPS) 204. U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.204. URL: https://csrc.nist.gov/pubs/fips/204/final.

[291] National Institute of Standards and Technology (NIST). *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Federal Information Processing Standards Publication (FIPS) 203. U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.203. URL: https://csrc.nist.gov/pubs/fips/203/final.

[292] National Institute of Standards and Technology (NIST). *NIST Asks Public to Help Future-Proof Electronic Information*. NIST. Feb. 2025. URL: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information (visited on Mar. 31, 2025).

[293] National Institute of Standards and Technology (NIST). *NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat*. NIST. Feb. 2025. URL: https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat (visited on Mar. 31, 2025).

[294] National Institute of Standards and Technology (NIST). *NIST Policy on Hash Functions*. NIST. Sept. 2024. URL: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions (visited on Mar. 15, 2025).

[295] National Institute of Standards and Technology (NIST). *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. NIST. Feb. 2025. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (visited on Mar. 31, 2025).

[296] National Institute of Standards and Technology (NIST). *NIST Retires SHA-1 Cryptographic Algorithm*. NIST. Dec. 2022. URL: https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps (visited on Mar. 15, 2025).

[297] National Institute of Standards and Technology (NIST). *NIST Retires SHA-1 Cryptographic Algorithm*. NIST. Feb. 2025. URL: https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm (visited on Mar. 15, 2025).

[298] National Institute of Standards and Technology (NIST). *NIST Revises Guide to IPsec VPNs: SP 800-77 Revision 1*. NIST. Feb. 2025. URL: https://www.nist.gov/news-events/news/2020/06/nist-revises-guide-ipsec-vpns-sp-800-77-revision-1 (visited on Mar. 15, 2025).

[299] National Institute of Standards and Technology (NIST). *NIST to Withdraw Special Publication 800-67 Revision 2*. NIST. July 2023. URL: https://csrc.nist.gov/news/2023/nist-to-withdraw-sp-800-67-rev-2 (visited on Mar. 15, 2025).

[300] National Institute of Standards and Technology (NIST). *Post-Quantum Cryptography*. NIST. Mar. 2025. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (visited on Apr. 1, 2025).

[301] National Institute of Standards and Technology (NIST). *Random Bit Generation*. NIST. Mar. 2025. URL: https://csrc.nist.gov/projects/random-bit-generation (visited on Mar. 23, 2025).

[302] National Institute of Standards and Technology (NIST). *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publications (FIPS) 180-4. U.S. Department of Commerce, Aug. 2015. DOI: 10.6028/NIST.FIPS.180-4. URL: https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[303] National Institute of Standards and Technology (NIST). *Stateless Hash-Based Digital Signature Standard*. Federal Information Processing Standards Publication (FIPS) 205. U.S. Department of Commerce, Aug. 2024. DOI: 10.6028/NIST.FIPS.205. URL: https://csrc.nist.gov/pubs/fips/205/final.

[304] National Institute of Standards and Technology (NIST). *What Is Post-Quantum Cryptography?* NIST. Dec. 2024. URL: https://www.nist.gov/cybersecurity/what-post-quantum-cryptography (visited on Mar. 31, 2025).

[305] National Security Agency (NSA). *Commercial National Security Algorithm (CNSA) Suite*. Oct. 2021. URL: https://media.defense.gov/2021/Oct/15/2002874275/-1/-1/0/CNSA_WORKSHEET_20211015.PDF (visited on May 30, 2025).

[306] National Security Agency (NSA). *Commercial National Security Algorithm Suite*. Aug. 2015. URL: https://web.archive.org/web/20220218193742/https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm (visited on June 1, 2025).

[307] National Security Agency (NSA). *Configuring IPSec Virtual Private Networks (VPNs)*. NSA. July 2020. URL: https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2002855928/ (visited on Mar. 16, 2025).

[308] National Security Agency (NSA). *Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations*. NSA. Jan. 2021. URL: https://media.defense.gov/2021/Jan/05/2002560140/-1/-1/0/ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF (visited on June 1, 2025).

[309] National Security Agency (NSA). *Mitigating Recent VPN Vulnerabilities*. NSA. Oct. 2019. URL: https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2002855926/ (visited on Mar. 16, 2025).

[310] National Security Agency (NSA). *NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems*. Sept. 2022. URL: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/ (visited on June 1, 2025).

[311] National Security Agency (NSA). *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*. Sept. 2022. URL: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF (visited on May 30, 2025).

[312] National Security Agency (NSA). *The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ*. NSA. Dec. 2024. URL: https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF (visited on Mar. 30, 2025).

[313] Shiyue Nie et al. “Measuring the Deployment of 5G Security Enhancement”. In: *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2022, pp. 169–174.

[314] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[315] Yoav Nir. *ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec*. RFC 7634. Aug. 2015. DOI: 10.17487/RFC7634. URL: https://www.rfc-editor.org/info/rfc7634.

[316] Yoav Nir and Simon Josefsson. *Curve25519 and Curve448 for the Internet Key Exchange Protocol Version 2 (IKEv2) Key Agreement*. RFC 8031. Dec. 2016. DOI: 10.17487/RFC8031. URL: https://www.rfc-editor.org/info/rfc8031.

[317] Yoav Nir, Simon Josefsson, and Manuel Pégourié-Gonnard. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier*. RFC 8422. Aug. 2018. DOI: 10.17487/RFC8422. URL: https://www.rfc-editor.org/info/rfc8422.

[318] Yoav Nir and Adam Langley. *ChaCha20 and Poly1305 for IETF Protocols*. RFC 8439. June 2018. DOI: 10.17487/RFC8439. URL: https://www.rfc-editor.org/info/rfc8439.

[319] Yoav Nir et al. *Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 8247. Sept. 2017. DOI: 10.17487/RFC8247. URL: https://www.rfc-editor.org/info/rfc8247.

[320] Karl Norrman, Prajwol Kumar Nakarmi, and Eva Fogelström. *5G security - enabling a trustworthy 5G system*. White Paper. Ericsson, Mar. 2021. URL: https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system.

[321] OpenAirInterface Software Alliance. *How to run a NTN configuration*. URL: https://gitlab.eurecom.fr/oai/openairinterface5g/-/blob/develop/doc/RUNMODEM.md#how-to-run-a-ntn-configuration (visited on Dec. 2, 2025).

[322] OpenAirInterface Software Alliance. *OpenAirInterface (OAI)*. URL: https://gitlab.eurecom.fr/oai.

[323] *ORBITING NOW | active satellite orbit data*. URL: https://orbit.ing-now.com/ (visited on Oct. 7, 2024).

[324] Ghizlane Orhanou, Said El Hajji, and Youssef Bentaleb. "SNOW 3G Stream Cipher Operation and Complexity Study". In: *Contemporary Engineering Sciences-Hikari Ltd* 3.3 (2010), pp. 97–111.

[325] Ivan Palamà et al. "IMSI Catchers in the wild: A real world 4G/5G assessment". In: *Computer Networks* 194 (2021), p. 108137.

[326] CheolJun Park et al. "DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices". In: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, pp. 1325–1342.

[327] Shinjo Park et al. "Anatomy of Commercial IMSI Catchers and Detectors". In: *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*. 2019, pp. 74–86.

[328] Roy Pereira and Robert L. Adams. *The ESP CBC-Mode Cipher Algorithms*. RFC 2451. Nov. 1998. DOI: 10.17487/RFC2451. URL: https://www.rfc-editor.org/info/rfc2451.

[329] Tim Polk and Sean Turner. *Prohibiting Secure Sockets Layer (SSL) Version 2.0*. RFC 6176. Mar. 2011. DOI: 10.17487/RFC6176. URL: https://www.rfc-editor.org/info/rfc6176.

[330] Tim Polk et al. *Elliptic Curve Cryptography Subject Public Key Information*. RFC 5480. Mar. 2009. DOI: 10.17487/RFC5480. URL: https://www.rfc-editor.org/info/rfc5480.

[331] Thomas Pornin. *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*. RFC 6979. Aug. 2013. DOI: 10.17487/RFC6979. URL: https://www.rfc-editor.org/info/rfc6979.

[332] Venkat Pothamsetty and Prabhaker Mateti. "A case for exploit-robust and attack-aware protocol RFCs". In: *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium*. IEEE. 2006, 8–pp.

[333] Qualcomm. *Everything You Need to Know About 5G*. Qualcomm. 2024. URL: https://www.qualcomm.com/5g/what-is-5g (visited on Sept. 23, 2024).

[334] Jason Rainbow. *SpaceX gets conditional approval for direct-to-smartphone service*. Nov. 2024. URL: https://spacenews.com/spacex-gets-conditional-approval-for-direct-to-smartphone-service/ (visited on July 2, 2025).

[335] RCR Wireless News. *Exploring functional splits in 5G RAN: Tradeoffs and use cases (Reader Forum)*. Mar. 2021. URL: https://www.rcrwireless.com/20210317/5g/exploring-functional-splits-in-5g-ran-tradeoffs-and-use-cases-reader-forum (visited on Oct. 1, 2024).

[336] Red Hat. *SLOTH: TLS 1.2 vulnerability (CVE-2015-7575)*. Red Hat. Jan. 2016. URL: https://access.redhat.com/articles/2112261 (visited on Mar. 23, 2025).

[337] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug. 2018. DOI: 10.17487/RFC8446. URL: https://www.rfc-editor.org/info/rfc8446.

[338] Eric Rescorla. *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*. RFC 5289. Aug. 2008. DOI: 10.17487/RFC5289. URL: https://www.rfc-editor.org/info/rfc5289.

[339] Eric Rescorla and Tim Dierks. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. Aug. 2008. DOI: 10.17487/RFC5246. URL: https://www.rfc-editor.org/info/rfc5246.

[340] Eric Rescorla and Brian Korver. *Guidelines for Writing RFC Text on Security Considerations*. RFC 3552. July 2003. DOI: 10.17487/RFC3552. URL: https://www.rfc-editor.org/info/rfc3552.

[341] Eric Rescorla and Nagendra Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347. Jan. 2012. DOI: 10.17487/RFC6347. URL: https://www.rfc-editor.org/info/rfc6347.

[342] Eric Rescorla, Hannes Tschofenig, and Nagendra Modadugu. *The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*. RFC 9147. Apr. 2022. DOI: 10.17487/RFC9147. URL: https://www.rfc-editor.org/info/rfc9147.

[343] Holli Riebeek. *Catalog of Earth Satellite orbits*. URL: https://earthobservatory.nasa.gov/features/OrbitsCatalog/page1.php (visited on Oct. 7, 2024).

[344] Federica Rinaldi et al. “Non-Terrestrial Networks in 5G & Beyond: A Survey”. In: *IEEE access* 8 (2020), pp. 165178–165200.

[345] Carmine Rizzo. *Lawful Interception in mobile networks*. Aug. 2022. URL: https://www.3gpp.org/technologies/li (visited on Mar. 5, 2025).

[346] David Rupprecht, Kai Jansen, and Christina Pöpper. “Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness”. In: *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. 2016.

[347] David Rupprecht et al. “Breaking LTE on Layer Two”. In: *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2019, pp. 1121–1136.

[348] David Rupprecht et al. “On Security Research Towards Future Mobile Network Generations”. In: *IEEE Communications Surveys & Tutorials* 20.3 (2018), pp. 2518–2542.

[349] Zujany Salazar et al. “5Greplay: a 5G Network Traffic Fuzzer - Application to Attack Injection”. In: *Proceedings of the 16th International Conference on Availability, Reliability and Security*. 2021, pp. 1–8.

[350] Sara Salim, Nour Moustafa, and Martin Reisslein. “Cybersecurity of Satellite Communications Systems: A Comprehensive Survey of the Space, Ground, and Links Segments”. In: *IEEE Communications Surveys & Tutorials* 27.1 (2024), pp. 372–425.

[351] Joseph A. Salowey, David McGrew, and Abhijit Choudhury. *AES Galois Counter Mode (GCM) Cipher Suites for TLS*. RFC 5288. Aug. 2008. DOI: 10.17487/RFC5288. URL: https://www.rfc-editor.org/info/rfc5288.

[352] Gregor D. Scott. *Guide for Internet Standards Writers*. RFC 2360. June 1998. DOI: 10.17487/RFC2360. URL: https://www.rfc-editor.org/info/rfc2360.

[353] Mauri Seidel et al. “How to Get Away with OpenAirInterface: A practical Guide to 5G RAN Configuration”. In: *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*. IEEE. 2023, pp. 1–6.

[354] Gautham Sekar. “The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3: Timing Attacks and Countermeasures”. In: *International Conference on Information Security and Cryptology*. Springer. 2011, pp. 269–288.

[355] Karen Seo and Stephen Kent. *Security Architecture for the Internet Protocol*. RFC 4301. Dec. 2005. DOI: 10.17487/RFC4301. URL: https://www.rfc-editor.org/info/rfc4301.

[356] Altaf Shaik et al. “New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities”. In: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 2019, pp. 221–231.

[357] Altaf Shaik et al. “On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks”. In: *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 2018, pp. 75–86.

[358] Altaf Shaik et al. “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”. In: *arXiv preprint arXiv:1510.07563* (2015).

[359] ShareTechnote. *5G/NR – HARQ*. URL: https://www.sharetechnote.com/html/5G/5G_HARQ.html (visited on May 25, 2025).

[360] Yaron Sheffer and Scott Fluhrer. *Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 6989. July 2013. DOI: 10.17487/RFC6989. URL: https://www.rfc-editor.org/info/rfc6989.

[361] Yaron Sheffer, Peter Saint-Andre, and Thomas Fossati. *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. RFC 9325. Nov. 2022. DOI: 10.17487/RFC9325. URL: https://www.rfc-editor.org/info/rfc9325.

[362] Peter W Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM review* 41.2 (1999), pp. 303–332.

[363] Lucas BD Silveira et al. “Tutorial on communication between access networks and the 5G core”. In: *Computer Networks* 216 (2022), p. 109301.

[364] Ankush Singla et al. “Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations”. In: *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*. 2021, pp. 501–515.

[365] Ilja Siroš, Dave Singelée, and Bart Preneel. “CovFUZZ: Coverage-based fuzzer for 4G&5G protocols”. In: *arXiv preprint arXiv:2410.20958* (2024).

[366] Valery Smyslov. *Mixing Preshared Keys in the IKE_INTERMEDIATE and in the CREATE_CHILD_SA Exchanges of IKEv2 for Post-quantum Security*. Internet-Draft draft-ietf-ipsecme-ikev2-qr-alt-10. Work in Progress. Internet Engineering Task Force, May 2025. 14 pp. URL: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-qr-alt/10/.

[367] Software Radio Systems (SRS). *AirScope*. URL: https://www.softwareradiosystems.com/tag/airscope/.

[368] Software Radio Systems (SRS). *srsRAN*. URL: https://github.com/srsran/srsRAN_4G.

[369] Software Radio Systems (SRS). *SRSRAN Project - Open Source RAN*. URL: https://www.srsran.com/.

[370] Jerome Solinas and David E. Fu. *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*. RFC 5903. June 2010. DOI: 10.17487/RFC5903. URL: https://www.rfc-editor.org/info/rfc5903.

[371] Space Foundation Editorial Team. *Types of Orbits*. URL: https://www.spacefoundation.org/space_brief/types-of-orbits/ (visited on Oct. 7, 2024).

[372] SpaceX. URL: https://www.spacex.com/ (visited on Oct. 7, 2024).

[373] Drew Springall, Zakir Durumeric, and J Alex Halderman. “Measuring the Security Harm of TLS Crypto Shortcuts”. In: *Proceedings of the 2016 Internet Measurement Conference*. 2016, pp. 33–47.

[374] Starlink. URL: https://www.starlink.com/ (visited on Oct. 7, 2024).

[375] Starlink. *STARLINK DIRECT TO CELL*. URL: https://www.starlink.com/business/direct-to-cell (visited on July 2, 2025).

[376] S Sullivan et al. “5G Security Challenges and Solutions: A Review by OSI Layers”. In: *Ieee Access* 9 (2021), pp. 116294–116314.

[377] Qiang Tang et al. “A Systematic Analysis of 5G Networks With a Focus on 5G Core Security”. In: *IEEE Access* 10 (2022), pp. 18298–18319.

[378] Vinayak Tanksale. “Efficient Elliptic Curve Diffie–Hellman Key Exchange for Resource-Constrained IoT Devices”. In: *Electronics* 13.18 (2024), p. 3631.

[379] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. “Satellite-based communications security: A survey of threats, solutions, and research challenges”. In: *Computer Networks* 216 (2022), p. 109246.

[380] Martin Thomson and Cory Benfield. *HTTP/2*. RFC 9113. June 2022. DOI: 10.17487/RFC9113. URL: https://www.rfc-editor.org/info/rfc9113.

[381] Martin Thomson, Mark Nottingham, and Willy Tarreau. *Using Early Data in HTTP*. RFC 8470. Sept. 2018. DOI: 10.17487/RFC8470. URL: https://www.rfc-editor.org/info/rfc8470.

[382] Moazzam Tiwana. *5G: Technologies, Architecture And Protocols*. Feb. 2020. URL: https://www.udemy.com/course/5g-network-training-key-technologies-architecture-and-protocols/ (visited on Sept. 30, 2024).

[383] C. Tjhai et al. *Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 9370. May 2023. DOI: 10.17487/RFC9370. URL: https://www.rfc-editor.org/info/rfc9370.

[384] Kai Tu et al. “Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands”. In: *33rd USENIX Security Symposium (USENIX Security 24)*. 2024, pp. 3063–3080.

[385] Meltem Sönmez Turan and Luís T. A. N. Brandão. *Keyed-Hash Message Authentication Code (HMAC): Specification of HMAC and Recommendations for Message Authentication*. NIST Special Publication (SP) 800-224 (Initial Public Draft). U.S. Department of Commerce, June 2024. DOI: 10.6028/NIST.SP.800-224.ipd. URL: https://csrc.nist.gov/pubs/sp/800/224/ipd.

[386] Meltem Sönmez Turan et al. *Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions*. NIST Special Publication (SP) 800-232 (Initial Public Draft). U.S. Department of Commerce, Nov. 2024. DOI: 10.6028/NIST.SP.800-232.ipd. URL: https://csrc.nist.gov/pubs/sp/800/232/ipd.

[387] Michael Tüxen, Eric Rescorla, and Robin Seggelmann. *Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)*. RFC 6083. Jan. 2011. DOI: 10.17487/RFC6083. URL: https://www.rfc-editor.org/info/rfc6083.

[388] Hanif Ullah et al. “5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases”. In: *Ieee Access* 7 (2019), pp. 37251–37268.

[389] United Nations Office for Outer Space Affairs. *Online index of objects launched into outer space*. URL: https://www.unoosa.org/oosa/osoindex/ (visited on Oct. 8, 2024).

[390] Alessandro Vanelli-Coralli et al. *5G Non-Terrestrial Networks: Technologies, Standards, and System Design*. John Wiley & Sons, 2024.

[391] Loganaden Velvindron, Kathleen Moriarty, and Alessandro Ghedini. *Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2*. RFC 9155. Dec. 2021. DOI: 10.17487/RFC9155. URL: https://www.rfc-editor.org/info/rfc9155.

[392] Flavia-Denisa Veres. “A study into the usability of 3GPP technical specifications”. MA thesis. University of Twente, 2022.

[393] John Viega and David McGrew. *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*. RFC 4543. May 2006. DOI: 10.17487/RFC4543. URL: https://www.rfc-editor.org/info/rfc4543.

[394] John Viega and David McGrew. *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*. RFC 4106. June 2005. DOI: 10.17487/RFC4106. URL: https://www.rfc-editor.org/info/rfc4106.

[395] Qi Wang et al. “SliceNet: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks”. In: *2018 IEEE international symposium on broadband multimedia systems and broadcasting (BMSB)*. IEEE. 2018, pp. 1–5.

[396] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. “Finding Collisions in the Full SHA-1”. In: *Advances in Cryptology–CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings 25*. Springer. 2005, pp. 17–36.

[397] One Way et al. *Transport Layer Security (TLS) Renegotiation Indication Extension*. RFC 5746. Feb. 2010. DOI: 10.17487/RFC5746. URL: https://www.rfc-editor.org/info/rfc5746.

[398] Cedric Westphal, Lin Han, and Richard Li. “LEO Satellite Networking Relaunched: Survey and Current Research Challenges”. In: *arXiv preprint arXiv:2310.07646* (2023).

[399] *What is Starlink? Everything there is to know in 2024*. Feb. 2024. URL: https://starlinkinsider.com/what-is-starlink/ (visited on Oct. 7, 2024).

[400] Russ White. *The Insecurity of Ambiguous Standards*. Mar. 2021. URL: https://circleid.com/posts/20210330-the-insecurity-of-ambiguous-standards/ (visited on Mar. 26, 2025).

[401] Johannes Willbold et al. “Satellite Cybersecurity Reconnaissance: Strategies and their Real-world Evaluation”. In: *2024 IEEE Aerospace Conference*. IEEE. 2024, pp. 1–13.

[402] Johannes Willbold et al. “Space Odyssey: An Experimental Software Security Analysis of Satellites”. In: *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2023, pp. 1–19.

[403] Michael Williams, Michael Tüxen, and Robin Seggelmann. *Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension*. RFC 6520. Feb. 2012. DOI: 10.17487/RFC6520. URL: https://www.rfc-editor.org/info/rfc6520.

[404] Paul Wouters. *Deprecation of the Internet Key Exchange Version 1 (IKEv1) Protocol and Obsoleted Algorithms*. RFC 9395. Apr. 2023. DOI: 10.17487/RFC9395. URL: https://www.rfc-editor.org/info/rfc9395.

[405] Paul Wouters et al. *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*. RFC 8221. Oct. 2017. DOI: 10.17487/RFC8221. URL: https://www.rfc-editor.org/info/rfc8221.

[406] Hongjun Wu et al. “Differential Attacks against Stream Cipher ZUC”. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2012, pp. 262–277.

[407] Nikita Yadav et al. “Orbital Shield: Rethinking Satellite Security in the Commercial Off-the-Shelf Era”. In: *2024 Security for Space Systems (3S)*. IEEE. 2024, pp. 1–11.

[408] Xincheng YAN et al. “Study on Security of 5G and Satellite Converged Communication Network”. In: *ZTE communications* 19.4 (2021), p. 79.

[409] Hojoon Yang et al. “Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE”. In: *28th USENIX Security Symposium (USENIX Security 19)*. 2019, pp. 55–72.

[410] Jing Yang. “Contributions to Confidentiality and Integrity Algorithms for 5G”. PhD thesis. Lund University, 2021.

[411] Jing Yang, Thomas Johansson, and Alexander Maximov. “Spectral analysis of ZUC-256”. In: *IACR transactions on symmetric cryptology* (2020), pp. 266–288.

[412] Jing Yang, Thomas Johansson, and Alexander Maximov. “Vectorized linear approximations for attacks on SNOW 3G”. In: *IACR Transactions on Symmetric Cryptology* (2019), pp. 249–271.

[413] Jingda Yang et al. “5G RRC Protocol and Stack Vulnerabilities Detection via Listen-and-Learn”. In: *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE. 2023, pp. 236–241.

[414] Ilsun You et al. “5G-AKA-FS: A 5G Authentication and Key Agreement Protocol for Forward Secrecy”. In: *Sensors* 24.1 (2023), p. 159.

[415] Chuan Yu et al. “Protecting unauthenticated messages in LTE/5G mobile networks: A two-level Hierarchical Identity-Based Signature (HIBS) solution”. In: *Computer Networks* 254 (2024), p. 110814.

[416] Kurt Zeilenga. *Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates*. RFC 4523. June 2006. DOI: 10.17487/RFC4523. URL: https://www.rfc-editor.org/info/rfc4523.

[417] Kurt Zeilenga. *Lightweight Directory Access Protocol (LDAP): Directory Information Models*. RFC 4512. June 2006. DOI: 10.17487/RFC4512. URL: https://www.rfc-editor.org/info/rfc4512.

[418] Kurt Zeilenga. *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*. RFC 4510. June 2006. DOI: 10.17487/RFC4510. URL: https://www.rfc-editor.org/info/rfc4510.

[419] Jegor Zelenjak. *Master Thesis Diagrams*. URL: https://github.com/jzelenjak/master-thesis-diagrams.

[420] Jegor Zelenjak. *Master Thesis Repository*. URL: https://github.com/jzelenjak/master-thesis-repository.

[421] Jegor Zelenjak. *OpenAirInterface Fork*. URL: https://github.com/jzelenjak/openairinterface5g.

[422] Jegor Zelenjak. *UERANSIM Fork*. URL: https://github.com/jzelenjak/UERANSIM.

[423] Bohan Zhang. "Mitigating Signalling Storms in 5G". In: *University of Waterloo* (2024).

[424] Shunliang Zhang, Dali Zhu, and Yongming Wang. "A survey on space-aerial-terrestrial integrated 5G networks". In: *Computer Networks* 174 (2020), p. 107212.

[425] Chunfang Zhou, Xiutao Feng, and Dongdai Lin. "The Initialization Stage Analysis of ZUC v1.5". In: *International Conference on Cryptology and Network Security*. Springer. 2011, pp. 40–53.

# A

# Example update of 3GPP security documents

During the thesis project, we discovered that 3GPP updated some of the security documents that we were working with. In this appendix, we show an example of such an update (January 2025) to the Network Domain Security and the cryptographic profiles (TS 33.210 and TS 33.310), the security architecture (TS 33.501) and the Security Assurance Specifications (TR 33.926 and TS 33.511).

## A.1. Cryptographic Profiles

### A.1.1. TS 33.210

Table A.1 summarizes the update introduced to TS 33.210 *"Network Domain Security (NDS); IP network layer security"* [17] during the time of writing. Full diff is available on the website of the Diffchecker tool[1].

**Table A.1:** Changes made to TS 33.210 [17] in January 2025.

| | |
|---|---|
| **Profiling of IPsec** *(clause 5.3)* | Support of ESP encryption transforms (clause 5.3.3):<br>• Add support for RFC 8750 [260] (*"Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)"*) to the used ESP encryption algorithms<br>Requirements on the construction of the IV (clause 5.3.5):<br>• Add ChaCha20-Poly1305 to the list with CTR, GCM, CCM and GMAC modes for which the same requirements on IV construction apply<br>• Mention that *"It is explicitly not allowed to use a random IV"* for CTR, GCM, CCM, ChaCha20-Poly1305 and GMAC mode |
| **Profiling of IKEv2** *(clause 5.4)* | General (in clause 5.4.2):<br>• Mention that *"An ephemeral private key shall be used in exactly one key establishment transaction and shall be destroyed (zeroized) as soon as possible"*<br>For IKE_SA_INIT exchange (in clause 5.4.2):<br>• Remove AUTH_HMAC_SHA256_128 for integrity from the algorithms that shall be supported<br>IKE_AUTH exchange (in clause 5.4.2):<br>• Mention that *"Identification Payloads (IDi and IDr) shall not be used for the IKEv2 authentication, but may be used for policy lookup"* |

*Continued on the next page*

[1] `https://www.diffchecker.com/Qxcn2aik/`

**Table A.1** *(continued from the previous page)*

| | |
|---|---|
| **TLS protocol profiles - General** *(clause 6.2.1)* | General:<br>• Add RFC 9325 [361] and RFC 9113 [380] for recommendations for secure use of TLS and DTLS<br>TLS versions:<br>• Add a recommendation to support DTLS 1.3 (based on TLS 1.3) as specified in RFC 9147 [342] (*"DTLS 1.3 as specified in RFC 9147 [75] should be supported"*)<br>Other:<br>• Link RFC 9113 [380] with the additional requirements in case the TLS connection is used to transport HTTP/2 over TLS<br>• Link RFC 9110 [153] and RFC 9112 [154] (instead of RFC 2817 [213]) in case the TLS connection is used to transport HTTP over TLS as specified in RFC 9110 [153] |
| **Profiling for TLS 1.3** *(clause 6.2.2)* | TLS cipher suites and Diffie-Hellman groups:<br>• Remove support for ffdhe2048 (*"Ffdhe2048 shall not be supported"*)<br>• Link RFC 9113 [380] with the additional requirements for HTTP/2 over TLS 1.3<br>TLS PSK key exchange modes:<br>• Remove support for psk_ke (*"psk_ke shall not be supported"*)<br>TLS cipher suites:<br>• Remove support for TLS_SHA256_SHA256 and TLS_SHA384_SHA384 (*"TLS_SHA256_SHA256 and TLS_SHA384_SHA384 shall not be supported"*)<br>TLS extensions:<br>• Add RFC 9325 [361] and section 4.2 of RFC 8446 [337] to the requirements for TLS extensions<br>• Add RFC 9113 [380] with the additional requirements for HTTP/2 over TLS 1.3 (*"Specifically, HTTP/2 servers shall not send post-handshake TLS 1.3 CertificateRequest messages and the prohibition on post-handshake authentication applies even if the client offered the "post_handshake_auth" TLS extension"*) |
| **Profiling for TLS 1.2** *(clause 6.2.3)* | TLS cipher suites:<br>• Add TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 [338] to the cipher suites that are mandatory to support and recommended to use<br>• Remove DHE from the examples of allowed to support cipher suites providing PFS (it now says *"Only cipher suites with AEAD (e.g. GCM) and PFS (i.e., ECDHE, ~~DHE~~) shall be supported"*)<br>Diffie-Hellman groups:<br>• Remove support for DHE (*"Finite field Diffie-Hellman (i.e. DHE) shall not be supported"*); however TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 is still present in the cipher suites that are mandatory to support and recommended to use (a mistake, since the reference for it has been made "void")<br>• For ECDHE, change *"Except curve25519, ed25519, and W-25519, elliptic curve groups of less than 256 bits shall not be supported"* into *"Except x25519, elliptic curve groups of less than 256 bits shall not be supported"*<br>PSK cipher suites:<br>• Remove TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 (RFC 5487 [71]) from the cipher suites that are mandatory to support and recommended to use |

## A.1.2. TS 33.310

Table A.2 presents a summary of the update that 3GPP has introduced to TS 33.310 *"Network Domain Security (NDS); Authentication Framework (AF)"* [16]. The full diff can be found on Diffchecker's website[2].

**Table A.2:** Changes made to TS 33.310 [16] in January 2025.

| | |
|---|---|
| **Architecture and use cases of the NDS/AF - Use cases** *(clause 5.2)* | Operator Registration: Creation of interconnect agreement (clause 5.2.1):<br>• Update LDAP RFC from RFC 2252 [123] to RFC 4510 [418], RFC 4517 [232], RFC 4523 [416] and RFC 4512 [417] |

*Continued on the next page*

[2] `https://www.diffchecker.com/QU88JJPi/`

**Table A.2** *(continued from the previous page)*

| | |
|---|---|
| **Certificate profiles** *(clause 6.1)* | CRL profile (clause 6.1a):<br>• Update LDAPv3 RFC from RFC 2252 [123] to RFC 4510 [418], RFC 4517 [232], RFC 4523 [416] and RFC 4512 [417] |
| **IKE negotiation and profiling** *(clause 6.2)* | IKEv2 profile (clause 6.2.1b):<br>• Add *"Authentication: Method 9/10/11 - ECDSA Digital Signature"* (RFC 4754 [161]) with recommendations to support ECDSA with SHA-256 on the P-256 curve, ECDSA with SHA-384 on the P-384 curve, and ECDSA with SHA-512 on the P-521 curve (for IKE_INIT_SA and IKE_AUTH exchanges) |
| **Certificate enrolment and renewal for 5GC NFs** *(clause 10.3)* | CMPv2 Profiling - Profile for PKIBody Field - Initialization Request (clause 10.3.1.4.2):<br>• Add a note that *"the NF is required to authenticate the origin of the "ir" message to the operator CA/RA"* during the initial trust set-up procedure, and describe the corresponding process if the selected mechanism for initial trust is an OAM certificate, an IAK, or a signature of certain NF profile selected parameters (see TS 33.310 clause 10.3.1.4.2 for the full note) |

# A.2. Security Architecture

## A.2.1. TS 33.501

In TS 33.501 *"Security architecture and procedures for 5G system"* [33], 3GPP has added a note for *N2*, *Xn*, *F1-C* and *E1*, that *"DTLS over SCTP as described in RFC 6083 [53] has message size limitations"* (section 9 *"Security procedures for non-service based interfaces"*). Other changes have also been made (e.g. to the core network), however, they are not relevant for the scope of our thesis. For reasons of brevity, we do not include these changes here (see the diff on Diffchecker's website[3] for all changes to TS 33.501).

# A.3. Security Assurance Specifications

## A.3.1. TR 33.926

For TR 33.926 *"Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes"* [35] 3GPP has added two new threats for gNB, gNB-CU, gNB-CU-CP, gNB-CU-UP, gNB-DU:

1. **"Peer certificate validity checking"**
   - Threat category: Information Disclosure, Tampering data, Denial of Service
   - Threatened asset: User Plane Data, Control Plane Data, Sufficient Processing Capability
   - Threat description: *"If the gNB* [gNB-CU/gNB-CU-CP/gNB-CU-UP/gNB-DU] *does not have the capability to check the validity of peer certificate, the gNB* [gNB-CU/gNB-CU-CP/gNB-CU-UP/gNB-DU] *may mislead to establish a connection with any peer potentially with malicious intent and using invalid certificates that could have been already revoked or expired, etc"*
   - Clauses: D.2.2.10 for gNB, R.2.2.10 for gNB-CU, S.2.2.8 for gNB-CU-CP, T.2.2.5 for gNB-CU-UP, and U.2.2.5 for gNB-DU
2. **"Certificate expiry checking"**
   - Threat category: Denial of Service
   - Threatened asset: Sufficient Processing Capability
   - Threat description: *"If the gNB* [gNB-CU/gNB-CU-CP/gNB-CU-UP/gNB-DU] *does not have the capability to check for certificate expiry and to expose such issue (for example by raising an alarm or logging) should the certificate be about to expire, then this may result in the peer (for example, the UPF or the AMF* [or gNB-CU for gNB-DU]*) rejecting the connection with the gNB* [gNB-CU/gNB-CU-CP/gNB-CU-UP/gNB-DU]*. Such a failure will mean the gNB* [gNB-CU/gNB-CU-CP/gNB-CU-UP/gNB-DU] *will be unable to provide the expected service due to a lack of connectivity with other network nodes. Furthermore, such issue could remain unnoticed."*

[3] `https://www.diffchecker.com/E5S6O7j2/`

- Clauses: D.2.2.11 for gNB, R.2.2.11 for gNB-CU, S.2.2.9 for gNB-CU-CP, T.2.2.6 for gNB-CU-UP, and U.2.2.6 for gNB-DU

The full diff is available on the website of the Diffchecker tool[4].

### A.3.2. TS 33.511

Finally, based on the new threats described above, two new requirements (and the corresponding test cases with the pre-conditions, execution steps, expected results, expected format of evidence) have been added to TS 33.511 *"Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class"* [34]:

1. **"Expired Certificate checking at base station"** and the test **TC_EXPIR_CERT_CHCK** to *"verify that the gNB can check whether its certificate issued by operator CA is about to expire and to act accordingly"* (see clause 4.2.2.1.22)
2. **"Peer certificate checking at base station"** and the test **TC_PEER_CERT_CHCK** to *"verify that the gNB has the ability to check the peer certificate is valid or not"* (see clause 4.2.2.1.23)

The full version of the diff can be seen on Diffchecker's website[5].

[4] https://www.diffchecker.com/NksNU6u7/
[5] https://www.diffchecker.com/7OuMNHe1/

# B

# Studied literature attacks on 5G terrestrial networks

**Table B.1:** Summary and analysis of the attacks on 5G networks from the literature.

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS using NAS reject messages** [192, 193, 187, 246] *Root cause: By design, NAS Registration Reject, Authentication Reject, and Service Reject are accepted by the UE without authentication before security can be activated.* | AS/NAS security *(NAS layer, pre-auth.)* | NAS *Registration Reject*, *Authentication Reject*, and *Service Reject* messages are sent unprotected before security activation, which can be exploited by an attacker, using a rogue gNB, by impersonating the AMF:<br>• If a UE attempts to connect to the rogue gNB after the cell (re-)selection procedure, the attacker responds with a *Registration Reject*, denying the service and triggering a new registration procedure. In addition, if the gNB sets the 5GMM cause to *"Illegal UE"*, then the UE is forced to update the connectivity status to *"Roaming Not Allowed"* and will not retry the registration procedure until it is rebooted, or its SIM card is reinstalled. This can permanently disconnect the communication interface (e.g. for mobile IoT devices).<br>• If a victim UE connects to a rogue gNB, the latter can directly send an *Authentication Reject* to the UE, making it automatically disconnect the RRC connection and become out of service for some time.<br>• If an attacker connects the victim UE and a legitimate gNB through their own gNB and UE (i.e. victim UE $\rightarrow$ rogue gNB $\rightarrow$ rogue UE $\rightarrow$ legitimate gNB), then all NAS signalling and UP traffic will go through the network controlled by the attacker. When the UE asks for a service (e.g. a call, SMS, receiving paging messages) with a *Service Request*, the rogue gNB can respond with *Service Reject*, causing a local DoS. | Out of the three variations, using *Registration Reject* makes the most sense to exploit the implicit trust between the UE and the (core) network before security is activated and deny the UE of the network service.<br>*Authentication Reject* is normally sent by the AMF to the UE to indicate the that the authentication procedure has failed, so it does not add any extra benefits compared to sending a *Registration Reject*.<br>It is not clear how to exploit the *Service Reject* message, since it can only be sent unauthenticated before the secure exchange of NAS messages has been established. |
| **Downgrade to EPC using Registration Reject** [275, 208] *Root cause: By design, NAS Registration Reject is accepted by the UE without authentication before security can be activated.* | AS/NAS security *(NAS layer, pre-auth., NSA)* | NAS *Registration Reject* messages are used for optimization of the system availability to the connected UEs (even in RRC_INACTIVE state) and can take a UE out of service. An attacker can modify an unprotected *Registration Reject* from the AMF to the UE and force the latter from the 5G network to the EPC network (e.g. using the cause *"N1 Mode Not Allowed"*, *"5GS Services Not Allowed"* or *"PLMN Not Allowed"*), where existing vulnerabilities [112, 193, 196, 205, 214, 215, 257, 326, 346, 347, 348, 358] can be exploited (e.g. IMSI catching, MitM attacks). | While the attack can be performed in 5G NSA deployments, it will be automatically mitigated in the long term when all MNOs will use only 5G SA deployments (i.e. there will be no LTE networks to downgrade to). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS using deregistration procedure** [192] *Root cause: By design, the UE can send unauthenticated NAS Deregistration Request in certain situations, such as during emergency services and when the UE has no valid 5G NAS security context (yet). In addition, a fake base station can have a stronger signal and lure the victim UE to connect to it.* | AS/NAS security *(NAS layer, pre- or post-auth.)* | In certain situations, an attacker can exploit the deregistration procedure:<br>1. A rogue UE can send a spoofed NAS *Deregistration Request* (for UE originating deregistration) with the victim's 5G-GUTI to ensure that the latter receives the corresponding *Deregistration Accept* and deregisters from the network. Setting the *"re-registration required"* field in *Deregistration Request* to 0 can make the UE remain out of service for some time, while setting it to 1 allows for other attacks after re-registration. Note that in general, a *Deregistration Request* from a UE must be integrity-protected, but there are some exceptions such as emergency services and when the UE does not (yet) have a valid NAS security context (see Table 5.9).<br>2. Using a malicious gNB with a stronger signal power, the attacker can connect all nearby UEs to this gNB and deregister them with a *Deregistration Request* (for UE terminated deregistration). This makes the UEs in the cell have no access to the communication service. In addition, setting the *"re-registration required"* field in *Deregistration Request* to 1 can cause a signalling storm, since all UEs in the cell will try to simultaneously register to the network. | While deregistering a UE that uses emergency services can have severe consequences, many other attacks (such as spoofing, eavesdropping, and tampering) are possible if no security context can be established for the UE requesting emergency services. Otherwise, it is not clear how to perform the attack in a meaningful way before NAS security context is established. The second attack variation does not have any meaningful impact, as the rogue gNB cannot connect UEs to the core network and complete the registration procedure (due to IPsec and other NDS/IP security mechanisms). |
| **DoS by resetting NAS COUNT** [194] *Root cause: The specifications do not say what to do when the received NAS message has a lower sequence number than in the last accepted message.* | AS/NAS security *(NAS layer, post-auth.)* | NAS COUNT is used for replay protection: a given COUNT value is accepted at most once and only if the message passes the integrity check [25]. UL NAS COUNT at AMF is the largest value in a successfully authenticated NAS message, and DL NAS COUNT at AMF is the value to be used in the next message. The 24-bit COUNT consists of a 16-bit overflow counter (*oc*, not sent) and an 8-bit sequence number (*seq*, sent). After each new or retransmitted security-protected NAS message, the sender increments the NAS COUNT by one (incrementing *oc* if *seq* wraps around). The receiver uses the received *seq* to compute the sender's COUNT, which is used as input to the integrity verification algorithm. If the received NAS message has a smaller *seq* than the *seq* of the last accepted message, the receiver can handle its DL *oc* in two ways:<br>1. The *oc* is not incremented when neither the received *seq* nor the locally stored *seq* is close to $2^8$.<br>2. The *oc* is incremented, assuming that the messages between the received (sender's) *seq* and the locally stored (receiver's) *seq* have been lost.<br>Both interpretations can lead to two different attacks:<br>1. The attacker can replay *Security Mode Command* and *Security Mode Complete* messages captured during the initial registration and both having *seq* of 0 (the security mode control procedure can be initiated by the network to change the security algorithms or to change the value of UL NAS COUNT used in the latest *Security Mode Complete* message). This resets the AMF's UL *seq* and UE's DL *seq*, desynchronizing the UL COUNT values between the victim UE and the legitimate AMF. The derived $K_{gNB}$ will also be different at the UE and the AMF, forcing the UE to perform a new registration procedure to re-establish the connection.<br>2. The attacker can silently drop an arbitrary number of messages, as the message is accepted by the receiver even if the received *seq* is smaller than the stored *seq*. | The means for the receiver to determine if a NAS message is a replay of an earlier NAS message are implementation-dependent, making the attack impact depend on a specific implementation. An attacker can always drop messages to disrupt communication, making the sender and receiver eventually reestablish the connection (regardless of counter values).<br>For the first interpretation (*oc* is not incremented), it is not clear to us if this attack could be performed successfully in a practical setting. Future work should test this attack in a real setting against a 3GPP-compliant 5G implementation. |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS by desynchronizing uplink NAS COUNT** [194] *Root cause: The maximum number of allowed consecutive failed attempts for the NAS Security Mode Command procedure (due to integrity check failure) is not specified.* | AS/NAS security *(NAS layer, post-auth.)* | An attacker uses a fake base station to connect to the victim UE and sends NAS *Security Mode Command* messages with arbitrary MAC values. The UE discards these messages (sending *Security Mode Reject*) and increments its UL *seq*. The attacker repeats this until the UE's UL *seq* wraps around (i.e. reaches $2^8$), incrementing the locally maintained *oc* by 1. As a result, the UL COUNTs between the victim UE and the legitimate AMF are desynchronized. While the UE can successfully verify the DL messages from the AMF, the AMF itself cannot verify and will discard any UL messages from the UE (including *Security Mode Complete* used for the UL NAS COUNT resynchronization). To resynchronize, the UE has to establish a new connection or the AMF has to initiate the Tracking Area Update procedure. The attack can lead to a prolonged DoS and service disruption. | The impact of the attack depends on a specific implementation. For example, if the UE (or AMF) immediately aborts the security mode control procedure and restarts the registration, the attack becomes theoretical. If the attacker wants to disrupt communication, they can simply drop the messages between the UE and the 5GC, regardless of the NAS COUNT values. |
| **UE cellular activity monitoring using NAS COUNT** [194] *Root cause: NAS sequence numbers (SNs) are sent in clear (although, the ciphered NAS message and NAS SN are authenticated).* | AS/NAS security *(NAS layer, post-auth.)* | With the knowledge of the victim's C-RNTI, an attacker can eavesdrop the UL and DL NAS messages, learning the NAS sequence numbers (*seq*) and the corresponding NAS COUNT values. This information can leak victim UE's cellular activity, such as the number of AKA runs or the cipher suite changes, or indicate the engagement level (service consumption) at different time intervals. | The leaked information does not give away any sensitive or important details about the subscriber, and therefore does not need extra protection. |
| **Traffic analysis by neutralizing 5G-TMSI refreshment** [194, 138] *Root cause: By design, the AMF needs to explicitly include "Configuration update indication" Information Element (IE) if it needs to request an acknowledgement for NAS Configuration Update Command (or a registration procedure) from the UE. The presence of this IE is optional.* | AS/NAS security *(NAS layer, post-auth.)* | The AMF initiates the configuration update procedure by transmitting a ciphered and integrity protected NAS *Configuration Update Command* to the UE. This message contains the new 5G-TMSI (5G-GUTI) and may indicate if an ACK from the UE (i.e. *Configuration Update Complete*) is required (by setting the Acknowledgement bit of the *"Configuration update indication"* IE). If an ACK is not requested, an attacker can drop the *Configuration Update Command* and disrupt the refreshing mechanism, so that the UE uses the same 5G-TMSI. When there are incoming services for the UE (e.g. phone call, SMS), the paging is first done using the new 5G-TMSI for some number of attempts and then retried with the old 5G-TMSI. Knowing the victim's old 5G-TMSI, the attacker can compute the paging occasion and hijack the paging channel, ensuring the UE does not receive subsequent paging messages. After some number of tries, the network aborts the paging and configuration update. This allows the attacker to force the usage of the same 5G-TMSI, allowing for further tracking. | A proper implementation requiring an ACK from the UE for the *Configuration Update Command* makes this attack theoretical. If the ACK is not requested for some reason, the impact of the attack depends on the 5G-TMSI refreshment frequency (the less frequent it is, the lower the impact of the attack). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **Traffic analysis due to infrequent update, reuse or predictable generation of 5G-GUTI** [246, 137, 138]<br>*Root cause:*<br>*The specifications leave the frequency of additional 5G-GUTI reassignments up to the implementation to decide. Moreover, the recommendation for 5G-TMSI generation is fairly vague.* | AS/NAS security *(NAS layer, post-auth.)* | 3GPP TS 33.501 [33] explicitly defines when the AMF shall send a new 5G-GUTI to the UE:<br>• *"Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE"*<br>• *"Upon receiving Registration Request message of type "periodic registration update" from a UE"*<br>• *"Upon receiving Service Request message sent by the UE in response to a Paging message"*<br>• *"Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM-IDLE mode with suspend indication in response to a Paging message"*<br>However, it also notes that *"It is left to implementation to re-assign 5G-GUTI more frequently than in cases mentioned above"* and simply states that *"5G-TMSI generation should be following the best practices of unpredictable identifier generation"*. If the 5G-GUTI is not updated frequently enough (or is predictable), an attacker may be able to track the UE. The impact can be even worse if the AMF does not assign a new 5G-GUTI and the UE keeps using the old identifier during initial registration, mobility update and paging update. | A proper implementation of the 5G-GUTI generation and update mechanisms (i.e. unpredictable and frequent) makes this attack theoretical.<br>Even if the implementation only updates 5G-GUTI in the explicitly defined cases, we do not believe that this gives away any sensitive or important information about the subscriber. |
| **DoS by paging channel hijacking** [194, 193]<br>*Root cause:*<br>*By design, (RRC) Paging messages are sent by the network without authentication prior to and after AS security activation.* | AS/NAS security *(NAS + RRC layers, pre- and post-auth.)* | The attacker sets up a fake base station operating in the same frequency band as the legitimate gNB and the same paging occasion (when a UE listens to the paging channel) as the victim UE. The malicious gNB then broadcasts fake empty paging messages in the shared paging channel with a higher signal power than the legitimate gNB. As a result of such paging channel hijacking, the victim UE does not receive any legitimate paging messages from the core network and does not receive any service notifications (e.g. for incoming phone calls or SMS messages), since they are silently dropped by the attacker. Such a DoS attack can cause customer dissatisfaction and the operator's reputation damage. Hijacking the paging channel also allows creating artificial emergencies by broadcasting fake emergency paging messages (with empty records but with fake emergency warnings) to many UEs for all paging occasions of a legitimate gNB. | An attacker can always perform jamming of the paging channel to ensure that no UE receives paging messages (including the target UE), even if paging was authenticated. Therefore, the impact of this attack is not higher than during a traditional jamming.<br>We believe that broadcasting fake emergency paging messages would not have a significant impact in a real setting. |
| **Traffic analysis by exposing 5G-TMSI and paging occasion** [194]<br>*Root cause:*<br>*By design, the RRC connection release procedure does not include an ACK for the RRCRelease message sent by the network to the UE. In addition, paging retransmission requests use the same 5G-TMSI.* | AS/NAS security *(NAS + RRC layers, post-auth.)* | With a fake base station, the attacker drops the *RRCRelease* message from a legitimate gNB to the victim UE, forcing it to stay in the RRC_CONNECTED state. The CN thinks that the UE has released the RRC connection and is in the RRC_IDLE mode. The attacker makes multiple phone calls (i.e. service notifications) to UE's phone number, and for every call, the CN asks the gNB to broadcast paging messages with UE's 5G-TMSI. The UE will not receive the paging message, because the paging occasion is different for idle and connected modes. Nevertheless, the attacker can sniff the paging channel and leak the victim's 5G-TMSI (and the paging occasion), which appears in multiple paging messages triggered by previous phone calls. Knowing the 5G-TMSI and the paging occasion (when the network transmits paging messages to a UE), the attacker could track the victim (depending on the 5G-TMSI update policy), or broadcast fake emergency alerts on the paging channel to launch other attacks [409]. | The attack could leak the 5G-TMSI of the victim UE, but otherwise has no impact by itself.<br>Considering mandatory 5G-TMSI update when (re-)connecting to the network, we believe that the traffic analysis using the learned 5G-TMSI would not reveal any important or sensitive information about the subscriber.<br>Note that if the UE needs to send data, then it will reconnect to the gNB after a timeout caused by the first unacknowledged data (at the RRC, NAS, or PDU layers). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS by I-RNTI exposure** [194] *Root cause: By design, the RRC connection release procedure does not include an ACK for the RRCRelease message sent by the network to the UE. In addition, paging retransmission requests use the same I-RNTI.* | AS/NAS security *(NAS + RRC layers, post-auth.)* | With a fake base station, the attacker drops the *RRCRelease* message (indicating RRC suspend) from a legitimate gNB to the victim UE, forcing it to stay in the RRC_CONNECTED state instead of going to RRC_INACTIVE. The gNB thinks that the UE is in the inactive mode. The attacker then makes multiple phone calls to UE's phone number, and for every call, the gNB broadcasts paging messages with UE's I-RNTI. This allows the attacker to learn the I-RNTI and the paging occasion of the victim. With this knowledge, the attacker could subsequently hijack the paging channel and launch (silent) DoS attacks. | The attack could leak the I-RNTI of the victim UE, but otherwise has no impact by itself. The subsequent paging channel hijacking is comparable to a traditional signal jamming. Note that if the UE needs to send data, then it will reconnect to the gNB after a timeout caused by the first unacknowledged data (at the RRC, NAS, or PDU layers). |
| **DoS by gNB resource depletion** [215, 192, 187, 246] *Root cause: By design, the RRC connection setup procedure does not authenticate the sender.* | AS/NAS security *(RRC layer, pre-auth.)* | The RRC connection setup procedure does not hide the message content and does not authenticate the sender (the authentication procedure is left to the AMF). Therefore, during the initial registration, a rogue UE can establish an RRC connection. Due to an invalid authentication response, the authentication procedure fails and the UE is not able to connect to the core network. While the UE cannot keep this connection for long, it can still connect to the operator's gNB. Thus, an attacker can repeatedly perform the Random Access procedure, ignoring the NAS *Authentication Request* from the AMF, to exhaust the capacity of the active RRC connections in the gNB. This can prevent legitimate subscribers from connecting to the base station and the core network. | Unless the implementation has a fixed maximum number of allowed RRC connections, it may be infeasible to exhaust the capacity of active connections. However, establishing many fake connections can have an impact on the gNB resources, depending on how fast new contexts are created, and the old contexts are released (which depends on the implementation). |
| **DoS by RRC connection deletion** [215, 194] *Root cause: By design, the RRC connection setup procedure does not authenticate the sender.* | AS/NAS security *(RRC layer, pre-auth.)* | An attacker sends a spoofed *RRCSetupRequest* message with the victim's 5G-TMSI (as *ueIdentity*) to the gNB that the victim UE is connected to. This causes the gNB to implicitly release the existing connection with the victim UE (which was in the RRC_CONNECTED state), and connect to the attacker's UE. As a result, this will disconnect and deny the victim UE from the network (until it attempts to establish a new RRC connection). | A proper implementation should not delete existing RRC contexts if a spoofed *RRCSetupRequest* is received by the gNB. We therefore consider this attack theoretical or an implementation error. |
| **DoS by forcing UE into RRC_IDLE** [194] *Root cause: By design, the UE releases the RRC connection upon unsuccessful integrity verification of RRCReconfiguration, RRCReestablishment and RRCResume messages.* | AS/NAS security *(RRC layer, post-auth.)* | To reconfigure the RRC connection with the UE, the gNB sends a ciphered and integrity-protected *RRCReconfiguration* message to the UE. If the UE is not able to verify the integrity protection, it releases the RRC connection and goes to the RRC_IDLE state. With the help of a fake base station, an attacker can impersonate the gNB and send an *RRCReconfiguration* with an arbitrary MAC. Since the victim UE is not able to successfully verify the message integrity, it will go to the RRC_IDLE state, implicitly (locally) releasing the connection and deleting its security context. The UE will establish a new connection with the RRC security context if it has any outgoing or incoming messages. Repeating this attack frequently causes a DoS and drains the UE's battery. Similar attacks can also be performed using *RRCReestablishment* or *RRCResume* messages. | We were not able to find the release of the RRC connection by the UE for a failed integrity check of an *RRCReconfiguration* in TS 38.331 [30], making this attack theoretical or an implementation error. For *RRCReestablishment* and *RRCResume*, the UE indeed goes to or stays in RRC_IDLE, which is to be expected as the procedure to resume or reestablish the RRC connection fails. However, the attacker can also just drop or corrupt these RRC messages to achieve the same effect (i.e. keep or move the UE to the idle state). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **Bidding down using RRC Security Mode Failure** [194] *Root cause: By design, RRC SecurityModeFailure is not authenticated by the UE and is accepted by the gNB without authentication (as it is sent before AS security activation).* | AS/NAS security *(RRC layer, pre-auth.)* | When the gNB wants to establish or refresh the RRC (PDCP) layer security context, it initiates the RRC security mode procedure. An attacker can impersonate the victim UE by sending an unauthenticated *SecurityModeFailure* in response to a *SecurityModeCommand* from a legitimate gNB (assuming the C-RNTI of the victim is known). As a result, the UE and the gNB continue using the security configuration used before receiving the *SecurityModeCommand*, i.e. neither integrity protection nor ciphering are applied at the RRC/PDCP layer (NEA0/NIA0 are used). A UE in such limited service mode may still be allowed to send an emergency registration message to establish an emergency session. In that case, the attacker could send a NAS *Identity Request* to leak the UE's SUCI, and with the "NULL" integrity and ciphering algorithms, the attacker is able to inspect or inject CP packets. | This attack does not have any meaningful impact, as the UE does not send subsequent (post-auth.) RRC messages without protection (unless there is an implementation error). Moreover, TS 38.331 [30] (clause 5.3.4.3) says that the UE continues using prior (NULL) configuration if *SecurityModeCommand* fails the integrity check for the initial AS security activation, but it does not mention how the gNB handles the received *SecurityModeFailure*. |
| **DoS using RRCReject** [194] *Root cause: By design, the UE in RRC_IDLE state accepts RRCReject messages without authentication (prior to AS security activation and after AS security activation if sent in SRB0 in RRC_INACTIVE state).* | AS/NAS security *(RRC layer, pre-auth.)* | The victim UE connects to the fake base station with an *RRCSetupRequest*. The latter replies with an unauthenticated *RRCReject*, which the UE accepts, since it is in RRC_IDLE state (i.e. not connected). As a result, the UE is denied of the connection. In addition, the attacker can set the *"mobility backoff timer"* in *RRCReject* for the UE to wait in the idle mode before reconnecting to the gNB. By repeatedly sending such unauthenticated *RRCReject* messages, the attacker can keep the UE in this connection setup loop and prevent it from getting services from the network. To prevent the UE's connection establishment fail counter on the same cell from reaching its limit, the attacker can also periodically send *RRCRelease* messages. By setting the *"redirected carrier information"* field of the *RRCRelease* message, the UE can be tricked to connect to another attacker-controlled fake base station operating on the redirected frequency. | Using (unauthenticated) *RRCReject* messages, it is possible to prevent the UE from connecting to the gNB. However, TS 38.331 [30] now states that *"RRCRelease message sent before AS security activation cannot include deprioritisationReq, suspendConfig, redirectedCarrierInfo, cellReselectionPriorities information fields"* (must be ignored by the UE), thus mitigating the second part of the attack. |
| **Downgrade of UE radio capabilities** [275, 356] *Root cause: By design, RRC UECapabilityEnquiry and UECapabilityInformation messages are sent unprotected prior to AS security activation.* | AS/NAS security *(RRC layer, pre-auth.)* | A MitM attacker can force the UE to operate with limited or restricted radio capabilities (or downgrade them to a lower generation network) by intercepting the RRC *UECapabilityInformation* from the UE, lowering the capability level, and forwarding the modified message to the gNB. The UE capabilities can also reveal device characteristics (e.g. model, manufacturer, version, running applications etc.). The attack is possible because *UECapabilityEnquiry* and *UECapabilityInformation* messages are by design sent unprotected prior to AS security activation to improve service or connectivity for the user (e.g. by providing early optimization). | TS 38.331 [30] now states that *"The network should retrieve UE capabilities only after AS security activation"*, which would mitigate this attack. Downgrading the UE to lower generation network is only possible in 5G NSA deployments and will be automatically mitigated after full migration to 5G SA deployments only. |
| **DoS by manipulating resumeCause in RRCResumeRequest** [275] *Root cause: By design, the resumeCause field in RRCResumeRequest is not authenticated by the UE (it is not included in resumeMAC-I).* | AS/NAS security *(RRC layer, pre- or post-auth.)* | *RRCResumeRequest* is not protected by PDCP, but includes a *resumeMAC-I* (16 LSBs of the MAC-I computed over *VarResumeMAC-Input*, which includes *sourcePhysCellId*, *targetCellIdentity*, and *source-c-RNTI*). However, the *resumeCause* field (together with *resumeIdentity*) is not authenticated. Furthermore, TS 38.331 states that *"The network is not expected to reject an RRCResumeRequest due to unknown cause value being used by the UE"*. As a result, an attacker can change the *resumeCause* value in the *RRCResumeRequest*. For instance, changing *"emergency"* to *"rna-Update"* makes a big difference in the requested and delivered service, as this may keep the UE in RRC_INACTIVE state instead of providing emergency service. This can be especially dangerous for critical services. | Changing *resumeCause* from *"emergency"* to *"rna-Update"* (or similar) can have severe consequences for the subscriber. In other situations, manipulating the value of the *resumeCause* field might not even have significant impact (depending on the actual field value and the way the network handles this field). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **DoS by spoofing RRCResumeRequest validating the wait timer** [275] *Root cause: It is possible to replay RRCResumeRequest when the wait timer expires.* | AS/NAS security *(RRC layer, pre- or post-auth.)* | When the UE starts the *RRCResumeRequest* procedure and the gNB is busy, the gNB responds with the *RRCReject* containing a wait timer. When this timer expires, the UE attempts to set up a connection using the same *resumeMAC-I* with the same I-RNTI and $K_{RRCint}$ as in the initial request (per TS 38.331 [30] clause 5.3.13.3, the keys $K_{gNB}$ and $K_{RRCint}$ are used from the stored UE Inactive AS context, and all input bits for COUNT, BEARER and DIRECTION are set to binary ones). The attacker can spoof the previously intercepted *RRCResumeRequest* and validate it before the wait timer expires, causing the resume procedure for the victim UE to fail, resulting in a DoS. | This attack does not have any significant impact, since the UE can subsequently reconnect to the gNB and establish a new RRC connection with a new AS context. |
| **DoS by spoofing uplink grants** [245] *Root cause: By design, DCI messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | An attacker can spoof the UL Downlink Control Information (DCI), i.e. uplink grants, to perform a fake allocation of UL resources (spoofing DL DCI, i.e. downlink allocations, is also possible but is only useful for spoofing data to a UE at layers above physical). By injecting spoofed UL grants to the connected UEs in every time slot, the attacker can force multiple benign UEs to constantly transmit on the same UL resources (chosen by the attacker) even when they do not have any pending data to send (due to required padding to fill all allocated resources). Furthermore, modifying the *Transmission Power Control* field in the same DCI will instruct the UEs to transmit at the maximum power. This effectively creates a jammer for legitimate UEs, disrupting their communication and decreasing the throughput, while draining the battery of the jamming UEs. | The attack can create a heavy congestion in the cell if many UEs start transmitting at the same time at a high power. Even worse, such a jamming is not easily detectable, since it comes from many legitimate UEs and not from a single source (as in traditional signal jamming). |
| **DoS by blocking initial cell access** [245] *Root cause: By design, the RA procedure is not protected. In addition, SIB and PO messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | The Random Access (RA) procedure is performed by the UE during network attachment. The RA parameters are broadcast by the gNB in the unprotected *System Information Block (SIB)* message, which the attacker can modify to change the RA configuration at the UE, e.g.:<br>• Minimize the *RA Response (RAR)* reception window (*ra-ResponseWindowSize*) to make the RA fail due to *RAR* timer expiration;<br>• Maximize the number of retries after RA failure (*preambleTransMax*) to increase congestion;<br>• Maximize the power ramp-up after each RA failure (*powerRampingStep*) to increase battery usage.<br>As a result, all UEs connecting to the network will keep failing the RA procedure and will not be able to attach to the cell. In order to target already connected UEs (which do not monitor the *SIB* messages), the attacker can send them a *SIB* paging, asking to monitor the *SIB* for updates. Then, the attacker can force the target UE(s) to run the RA procedure by injecting a special DCI called *PDCCH Order (PO)*. This message instructs a connected UE to start a RA procedure to re-establish synchronization in the UL (e.g. updating the *Timing Advance (TA)* value). Such a stealthy way of triggering a RA procedure allows draining resources (due to collisions in the limited RA resources) or disconnecting the users to perform further localization or traffic analysis attacks. | Manipulating RA parameters in broadcast *SIB* messages can create a high congestion if many UEs are present in the cell. In the worst case, this attack can prevent all UEs in the cell from connecting to the gNB and the core network. Furthermore, the attack is harder to detect than a traditional signal jamming, since the *SIB* messages could also come from a legitimate gNB (there is no authentication). |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **Spoofing resource scheduling request** [245] *Root cause: By design, Scheduling Request messages are not authenticated by the UE and are accepted by the gNB without authentication.* | AS/NAS security *(lower layers)* | To request UL resources, the UE sends a *Scheduling Request (SR)* message to the gNB, which will allocate these resources. The attacker can spoof *SR*s to:<br>• Keep the victim's connection active for long time, circumventing the RRC inactivity timer, which allows for prolonged location tracking with the same RNTI;<br>• Ask for radio resources on behalf of multiple UEs with no pending UL data, which allows increasing network congestion. Spoofed UL transmissions are also more difficult to detect than for DL;<br>• Ask for an UL DCI for a specific UE and steal the allocated UL grant, which allows spoofing or injecting higher-layer data (e.g. MAC) impersonating the user. | The impact of scheduling request spoofing depends on the further attack steps and the goal of the attack (if used as an intermediary step).<br>Creating cell congestion can have a high impact if many UEs are connected to the cell. It can also be hard to detect, since scheduling requests might come from legitimate UEs. |
| **Disrupting communication using HARQ procedure** [245] *Root cause: By design, the HARQ procedure is not protected. In addition, the DCI messages are not authenticated by the gNB and are accepted by the UE without authentication.* | AS/NAS security *(lower layers)* | Hybrid Automatic Repeat reQuest (HARQ) [26, 29] is a combination of Forward Error Correction (FEC) and ARQ, i.e. retransmission using acknowledgments (ACKs) [359]. Downlink ACKs are omitted in 5G; the UE is implicitly notified of lost packets by requesting retransmissions. Uplink ACKs are dynamically scheduled and can be aggregated in the same Uplink Control Information (UCI). A *Downlink Assignment Index (DAI)* counter is included in the DL DCI, so that the UE can learn if there were any lost transmissions and adjust its bitmap size (with 1 bit for each aggregated ACK). The attacker can spoof a DCI with a different *DAI* counter, which will desynchronize the transmitted and received packets at the UE side. As a result, the gNB will not be able to infer which packets correspond to the ACKs in the received bitmap, causing a HARQ failure. This can disrupt the communication of a legitimate victim UE. | The impact of the attack can be high if such a desynchronization of transmitted and received frames can be performed constantly, fully disrupting the communication. Such an attack will also be more difficult to detect than a traditional signal jamming. However, the practical feasibility and impact of this attack should be tested in a real setting. |
| **User localization using SSB and RA procedure** [245] *Root cause: By design, the RA procedure is not protected. In addition, there is a one-to-one mapping of RA occasions and the beam with the strongest measured signal.* | AS/NAS security *(lower layers)* | The gNB broadcasts *Synchronization Signal Block (SSB)* and *SIB*s over different beams, each having a unique index within the cell. By measuring the received power for each *SSB*, the UE learns the strongest beam. Each *SSB* beam index is uniquely mapped to a RA occasion, allowing the gNB to choose the optimal beam for the UE based on the used RA occasion. In order to localize a user, the attacker creates a fingerprint of the beam configuration of a given cell and a map with exact locations of the gNB and every beam in the cell. By sniffing the RA channel, the attacker infers the beam chosen by the UE from the RA occasion and gets the *TA* value from the *RAR* of the gNB. Using these values, it is possible to estimate the UE's azimuth and the distance from the gNB, which reveals the location of the UE. Note that this attack can also be performed against already connected users by spoofing a *PO* message to force the RA procedure. | The attack can be useful to localize a specific target individual, but it does not reveal much useful information about arbitrary users. Not only can it confirm the presence of the user in the cell, but it can pinpoint the approximate location of the victim.<br>However, the practical feasibility and impact of this attack should be tested in a real setting. |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **User localization using CSI reports** [245, 137] *Root cause: By design, CSI reports containing C-RNTI and the strongest beam index identifier are not encrypted by the UE.* | AS/NAS security *(lower layers)* | The gNB periodically sends the Channel State Information (CSI) reference signal (RS) in the downlink. The UE measures the downlink channel quality and reports the CSI to the gNB, which uses these parameters in resource scheduling. These reports are sent in UCI, but can be scheduled by the MAC layer. The CSI report is transmitted in clear and includes important information, which may allow a passive attacker to track the movement of users in the cell. In particular, it contains the C-RNTI of the UE and the index identifier and the measured signal strength of the strongest beam of the CSI RS, which are essential for UE positioning. The attack has three steps:<br>1. Build a fingerprint database with the signal strength of the strongest beam in the area of a gNB (i.e. learn the static cell beam configuration by measuring the physical area covered by each beam index).<br>2. Decode the CSI reports containing the C-RNTI of the target UE (e.g. obtained using silent messages) and the index of the strongest beam.<br>3. Use the decoded beam value and the entries in the beam database to estimate the GPS coordinates describing the UE path from the beams reported by the target UE, which leaks its position. | The attack can be useful to localize a specific target individual, but it does not reveal much useful information about arbitrary users. Not only can it confirm the presence of the user in the cell, but it can pinpoint the approximate location of the victim.<br>However, the practical feasibility and impact of this attack should be tested in a real setting. |
| **User localization and communication disruption using SRS** [244] *Root cause: By design, the SRSs are sent by the UE without protection.* | AS/NAS security *(lower layers)* | The Sounding Reference Signal (SRS) is used to estimate the channel across the entire uplink band and may be interesting for an attacker [94]:<br>• As an UL transmission that is not expected by the gNB, it will interfere with other transmissions in the uplink scheduled by the gNB. Thus, it will either jam the data sent by other UEs or pollute their SRSs, disrupting the measured CSI.<br>• Disabling the transmission of semi-persistent SRSs (i.e. sent with a fixed period) for the victim UE using the corresponding MAC Control Element (CE) will disrupt the channel estimation at the gNB, greatly decreasing the throughput (especially in beamforming scenarios)<br>• Since SRS is a predefined wideband signal (Zadoff-Chu signal) it can provide cross-correlation properties to the attacker, who can localize a certain user by measuring the difference in the arrival time. | Communication disruption can have a high impact if done constantly; it is also more difficult to detect than a traditional signal jamming.<br>The impact of localizing a specific target individual depends on how precise the location can be estimated.<br>However, the practical feasibility and impact of this attack should be tested in a real setting. |
| **Location tracking using normal radio link interception** [187] *Root cause: By design, the home network identifier in a SUCI is not encrypted. In addition, knowledge of the targeted user's vector of positions can allow for further location tracking.* | AS/NAS security *(NAS layer + lower layers)* ECIES | If NAS signalling messages are not ciphered, then the PEI is sent in clear in the NAS *Security Mode Complete* message. However, even when ciphering is applied, an attacker can leak some information from the unencrypted home network identifier in the SUCI. If the home network can be more uniquely identified (e.g. during the visit of a foreign delegation), all UEs associated with this network can be tracked.<br>In addition, using a sufficiently dense network of (possibly low-cost) radio sensors, the attacker may be able to track the location of given UEs at all times. Knowing the targeted user's vector of positions and using big data analysis may allow matching the known position vector to a 5G-GUTI without knowing SUPI or PEI and completing the location pattern outside the already known locations. If the target's location is known at the start of the tracking session, then there is no need to physically follow the victim. | The home network identifier has to be sent in clear for routing purposes (unless encrypted by the encapsulating PDCP/NAS layers). However, it does not directly reveal the subscriber's identity, only the presence of a user with a foreign home network in the cell.<br>The location tracking can only have a meaningful impact if estimated accurately (requiring enough data for the vector of positions). The practical feasibility of this approach should be tested in a real setting. |

*Continued on the next page*

**Table B.1** *(continued from the previous page)*

| Attack (Weakness) | Categ. | Description | Analysis |
|---|---|---|---|
| **Resource exhaustion by NAS Identity Request flooding** [192, 246] *Root cause: By design, the UE accepts NAS Identity Request from the gNB without authentication before security can be activated.* | AS/NAS security *(NAS layer, pre-auth.)* ECIES | A malicious gNB can start the identification procedure by repeatedly sending NAS *Identity Request* messages (unauthenticated by design) to the UE with "SUCI" as *"Identity type".* Per TS 24.501 [25], *"A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode."* When sending *Identity Response*, the UE shall generate a fresh SUCI (for replay protection) if timer T3519 is not running (and then start the T3519 timer and store the generated SUCI), or use the stored SUCI if T3519 timer is running. An attacker can make the victim UE repeatedly generate an ECC ephemeral public key and encrypt its SUPI, which can eventually exhaust UE's resources. | We consider this attack theoretical, since the T3519 timer and security activation (if properly implemented) degrade the attack scalability to the point that the impact can be considered negligible. |
| **(D)DoS by SUCI flooding** [183] *Root cause: By design, NAS Registration Request messages with SUCI must be forwarded and processed all the way at the UDM.* | AS/NAS security *(NAS layer, pre-auth.)* ECIES | An attacker sends valid and invalid NAS *Registration Request* messages to the network (invalid requests have a SUCI/SUPI that is not in the UDM). This abuses the normal functionality of the network entities participating in the registration procedure (including the UDM). The UDM itself is attacked only through communication with the 5GC internal entities, and has to decrypt SUCIs that might not even correspond to real subscribers. Since the UDM contains critical subscription information, a DoS attack on the UDM leads to a DoS attack on the core network. | The impact of the attack depends on the speed with which the UDM can decrypt the received SUCIs and validate the subscriber (if done fast enough, then the impact will be negligible). Note that this attack can be performed together with *"DoS by gNB resource depletion"*, which focuses on overloading the gNB using the same process. |
| **Location tracking with a SUCI-Catcher** [111, 83, 192] *Root cause: AKA linkability in the design: the target UE responds differently to the NAS Authentication Request than a regular UE (accept and reject, respectively).* | AS/NAS security *(NAS layer, pre-auth.)* ECIES | An attacker obtains the victim's SUCI, e.g. using a fake base station (discovery phase), asks the network for an authentication challenge associated with the wanted subscriber's identity, and forwards the *Authentication Request* to all connected UEs (linking SUCIs phase). Only the UE accepting the *Authentication Request* (or responding with an *Authentication Failure* with the cause *"Synch Failure"*) is the searched-for-subscriber (other UEs send an *Authentication Failure* with the cause *"MAC Failure"*). Thus, when an unknown UE connects to the fake cell, a SUCI-Catcher can check if it belongs to the wanted subscriber (who can even be a national leader or ambassador), which allows verifying if a person of interest is in the current location or not. | The attack allows verifying if the person of interest is present in the cell by capturing SUCIs and linking encrypted identities between the sessions. While mitigation measures such as rate-limiting or throttling of the user authentication can reduce the scalability of the attack, it is still possible to perform targeted tracking of specific victims. |