BARON

Base-Station Authentication Through Core Network for Mobility Management in 5G Networks

Lotto, Alessandro; Singh, Vaibhav; Ramasubramanian, Bhaskar; Brighente, Alessandro; Conti, Mauro; Poovendran, Radha

DOI
10.1145/3558482.3590187

Publication date
2023

Document Version
Final published version

Published in
WiSec 2023 - Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks

BARON: Base-Station Authentication Through Core Network for Mobility Management in 5G Networks

Alessandro Lotto
University of Padua
Padua, Italy
alessandro.lotto@studenti.unipd.it

Vaibhav Singh
University of Washington
Seattle, WA, USA
vaibhavs@uw.edu

Bhaskar Ramasubramanian
Western Washington University
Bellingham, WA, USA
ramasub@wwu.edu

Alessandro Brighente
University of Padua
Padua, Italy
alessandro.brighente@unipd.it

Mauro Conti
University of Padua
Padua, Italy
Delft University of Technology
Delft, Netherlands
mauro.conti@unipd.it

Radha Poovendran
University of Washington
Seattle, WA, USA
rp3@uw.edu

ABSTRACT

Fifth-generation (5G) cellular communication networks are being deployed on applications beyond mobile devices, including vehicular networks and industry automation. Despite their increasing popularity, 5G networks, as defined by the Third Generation Partnership Project (3GPP), have been shown to be vulnerable against *fake base station* (FBS) attacks. An adversary carrying out an FBS attack emulates a legitimate base station by setting up a *rogue base station*. This enables the adversary to control the connection of any user equipment that (inadvertently) connects with the rogue base station. Such an adversary can gather sensitive information belonging to the user. While there is a large body of work focused on the development of tools to detect FBSs, the user equipment will continue to remain vulnerable to an FBS attack.

In this paper, we propose BARON, a defense methodology to enable user equipment to determine whether a target base station that it is connecting to is legitimate or rogue. BARON accomplishes this by ensuring that the user receives an authentication token from the target base station which can be computed only by a legitimate and trusted entity. As a consequence, receiving such an authentication token from a base station ensures legitimacy of the base station. We evaluate BARON through extensive experiments on the *handover process* between base stations in 5G networks. Our experimental results show that BARON introduces an overhead of less than 1% during handover completion, which is 10000× lower than the overhead reported by a state-of-the-art method. BARON is also effective in thwarting an FBS attack and quickly recovering connection to a legitimate base station.

WiSec '23, May 29-June 1, 2023, Guildford, United Kingdom

ACM ISBN 978-1-4503-9859-6/23/05…$15.00
https://doi.org/10.1145/3558482.3590187

CCS CONCEPTS

• **Networks** → *Network protocol design*; • **Security and privacy** → **Mobile and wireless security**; **Authentication**.

KEYWORDS

5G Networks; 5G Security; Base-Station authentication.

ACM Reference Format:
Alessandro Lotto, Vaibhav Singh, Bhaskar Ramasubramanian, Alessandro Brighente, Mauro Conti, and Radha Poovendran. 2023. BARON: Base-Station Authentication Through Core Network for Mobility Management in 5G Networks. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29-June 1, 2023, Guildford, United Kingdom.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3558482.3590187

1 INTRODUCTION

The increased demand for services on mobile devices that require high throughput and low latency (e.g., video calling) has guided the rapid evolution of cellular networks. The current state-of-the-art in cellular communications is the *fifth generation* (5G) technology [17], which provides a significantly improved throughput over previous technologies such as fourth generation long-term evolution (4G-LTE). From the perspective of the physical layer, 5G uses also the millimeter-wave (mmWave) spectrum. While on one side this would increase the available bandwidth and reduce transmission latency, on the other mmWave has low penetration and, consequently, offers a lower transmission range. As a result, 5G networks require a dense base station (BS) deployment [13]. Many countries have already deployed functioning 5G networks, and the technology is under continuous development to meet higher standards for performance and security. Cellular communication technologies are also being increasingly adopted in other applications such as vehicular networks [30], real-time medical procedures [11] and industrial automation [7, 8]. However, these applications may create new attack surfaces that are vulnerable to exploitation by an adversary [25]. Thus, it is essential to develop solutions that can ensure high levels of security, confidentiality, and reliability in cellular communication before they become ubiquitous in other applications.

Mobility management is one of the most critical aspects of cellular communication [9]. Specifically, the handover procedure ensures

that users' mobile devices have the ability to switch between BSs with (almost) no interruption in connection and service [1]. Although dense BS deployment in 5G networks reduces transmission times between the BS and user, it also results in more frequent handovers compared to previous communication technologies, including 4G-LTE. These networks have been shown to be vulnerable to *fake base station* (FBS) attacks [10]. An adversary carrying out an FBS attack sets up a *rogue base station* (rBS) that emulates a legitimate BS. This can deceive a *user equipment* (UE) (*e.g.*, mobile phone) into connecting with the rBS, while believing it to be legitimate. Following connection with the rBS, the UE does not have the ability to restore connection to a genuine BS without rebooting the device or going out of range of the rBS. An adversary might use an FBS attack as a first-step towards carrying out more severe attacks, including denial-of-service (DoS) and man-in-the-middle (MitM) [10, 24] attacks, thus affecting network reliability [22].

Despite awareness of the vulnerability described above, defenses against FBS attacks have primarily focused on mechanisms and tools to detect FBSs [24]. These, however do not prevent an adversary from successfully carrying out an FBS attack. In a sequence of research papers, authors of [15, 24] propose two digital signature-based mechanisms to protect beacons broadcast by BSs. Results in [24], in particular, manage to reduce the introduced computation overhead up to 31% compared to other related works using asymmetric cryptography ([15, 18, 31]). However, both results in [15, 24] may be vulnerable to replay attacks, making them ineffective and preventing their deployment. Besides, they require to introduce a public key infrastructure (PKI) or similar entity in the core network for key management, resulting in possibly increased manufacturing and set-up costs.

Our Contribution: In this paper, we develop BARON[1], a framework for secure initial access and handover in 5G networks against FBS attacks. BARON enables the UE to (i) determine whether the BS it is connecting to is legitimate or not and (ii) efficiently recover a legitimate connection when subject to an FBS attack. We carry out extensive experiments to evaluate the performance of BARON in terms of the time overhead introduced during handover, and efficiency in recovering a legitimate connection in case of an FBS attack. Our experiments reveal that the additional overhead induced by BARON is less than 1% of the total time required for handover completion, and is 10000× lower than the additional overhead reported recently in [24]. Further, during an FBS attack, BARON is able to effectively recover connection to a legitimate base-station in a time that is of the same order of magnitude as the time required for handover completion.

The rest of the paper is organized as follows. Sec. 2 gives background on 5G. Sec. 3 defines the threat model and Sec. 4 describes the FBS attack. Sec. 5 introduces BARON, a defense against FBS attacks and Sec. 6 proposes a post-attack recovery mechanism. Sec. 7 presents results of our experiments, Sec. 8 discusses related work, and Sec. 9 concludes the paper. A complete list of abbreviations used in the paper and their full forms is provided in Appendix C.

[1]BARON: Base-station Authentication thRough cOre Network

2 PRELIMINARIES: 5G NETWORKS

In this section, we provide background on the architecture and main components of 5G networks. We also provide an overview of the handover process.

2.1 5G Network Architecture

The 5G core network consists of multiple entities. A simplified representation of the architecture is shown in Fig. 1. We identify and briefly describe functions of four major entities below [2, 6]:

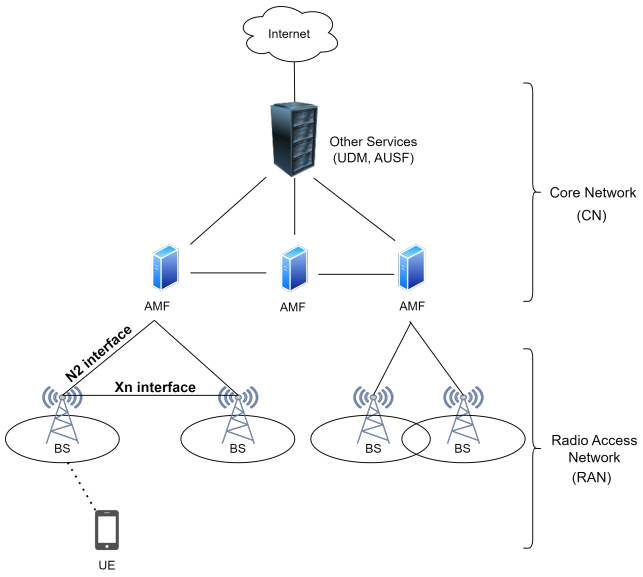

Figure 1: Example of simplified architecture of a 3GPP 5G network.

- *User Equipment (UE)*: The UE refers to an integrated module consisting of the universal subscriber identity module (USIM) and the mobile equipment. The UE may be a smartphone or an Internet-of-Things (IoT) device with a mobile broadband chip conforming to the 5G Standard. The USIM stores a 15-digit unique subscriber permanent identifier and associated cryptographic keys. This identifier is used for authentication of the UE when it initiates a connection with the core network.
- *Base Station* (BS): A BS is responsible for establishing and maintaining wireless communications with the UEs. Together with the UEs, BSs compose the radio access network (RAN). As shown in Fig. 1, a BS communicates with entities in the core network through a secure channel using the *N2 interface*. BSs may also directly communicate each other using a secure *Xn interface*. The BS broadcasts master information block (MIB) and secondary information block (SIB) messages multiple times a second, which contain information required to facilitate the access to the BS itself.
- *Access and Mobility Function (AMF)*: The AMF is primarily responsible for mobility, connection, and security context management. Although the AMF forms a part of the core

network, we prefer to abstract it as a separate entity due to its central role in our solution.

- *Core Network (CN)*: The CN comprises all entities excluding the RAN, and it is responsible for data and connection management. As Fig. 1 shows, the CN connects the RAN to the broader internet. Within the CN, the unified data management (UDM) entity is responsible for user initial registration, while the authentication server function (AUSF) provides authentication support for 5G services.

2.2 Securing Communications in 5G Networks

We can use encryption and authentication mechanisms to protect messages exchanged between entities in the 5G network in order to accomplish secure communication [6]. The 3GPP standard for 5G networks defines the *Authentication and Key Agreement* (AKA) protocol. This protocol defines a set of security procedures to provide (i) mutual authentication between the UE and 5G network, (ii) message integrity and confidentiality, and (iii) security parameters that can be used for subsequent procedures [6]. Starting from a (symmetric) master key shared between the UDM and the USIM, the UE goes through a set of challenge-response authentication and hierarchical key derivation processes. Upon completion of the AKA protocol, the UE builds a chain of trust with the serving network, and derives one or more keys for each entity in the CN and for the current serving base station (sBS). The set of secret keys, security parameters, and employed encryption and authentication algorithms define the *UE security context*. At the end of the AKA procedure, the CN, the BS, and UE share the necessary security parameters and keys for secure communication [20]. The following symmetric keys are established before initiating a handover process:

- K_{SEAF}: (long term) key shared between UE and CN.
- K_{AMF}: (long term) key shared between UE and AMF. It is obtained from K_{SEAF} through a key derivation process [6].
- K_{gNB}: (short term) session key shared between UE and sBS. This can be derived either from K_{AMF} or from a previous K_{gNB} [6].

Once handover is triggered, the UE derives a new session key K_{gNB} to establish secure communication with the target base station (tBS). We assume that most communication between any pair of entities in the network is secure. The exceptions are the random access channel (RACH) procedure and the `Radio Resource Control (RRC) Reconfiguration` message. These exceptions occur due to the fact that according to 3GPP specifications, the UE security context is activated only after the RRC connection is established [1].

2.3 Cellular Handover

The process by which the transfer of user information from the sBS to a new tBS is termed a *handover*. Handover is critical to ensuring continuity of cellular services, and is typically triggered when the UE senses stronger reception from a BS other than the sBS. This is likely to happen when the UE is approaching the limit of the range of the sBS.

Consider a scenario in which the UE is connected to sBS and is approaching a tBS that has a greater signal strength. Assume

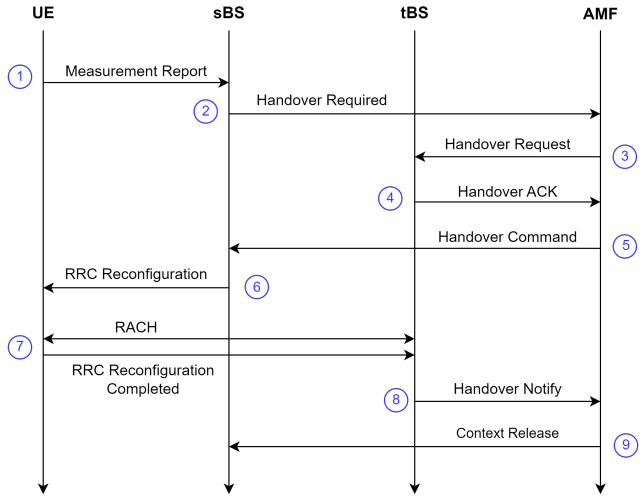

Figure 2: Example of a 3GPP N2-handover with sBS and tBS under control of the same AMF. If sBS and tBS were under control of different AMFs, then the AMF controlling sBS would forward the `Handover Request` message to the AMF controlling the tBS.

that the sBS and tBS are both under the control of the same AMF. The handover procedure from sBS to tBS develops according to the following steps [2, 26] (Fig. 2):

① The UE periodically senses MIB and SIB messages broadcast from neighbouring BSs, and transmits a `Measurement Report (MR)` message. This message contains information about the strength of the received signal from the sBS as well as signals from surrounding BSs.

② Based on the content of the `MR`, the sBS decides whether there is a need to hand over the UE to another BS. In the case where a handover is deemed necessary, the sBS selects the tBS. The handover decision is generally threshold based: if the signal strength from another BS exceeds a certain threshold compared to the signal from sBS, then handover is triggered. At handover decision, sBS transmits the `Handover Required` message to the AMF that contains information about the choice of tBS and the protocol data unit sessions that need to be handed over.

③ The AMF identifies the tBS and forwards a `Handover Request` message, providing information such as UE security context, capabilities and session information.

④ Based on the information received and available resources, the tBS decides whether to admit the UE. In the case of handover acceptance, the tBS replies to the AMF with a `Handover Acknowledge (ACK)` message, which specifies which session it can accept.

⑤ Upon receipt of handover confirmation from the tBS, the AMF sends a `Handover Command` message to the sBS. This message contains information included in `Handover ACK` that the UE needs in order to obtain access to the target.

⑥ The sBS triggers the handover procedure by forwarding information received with a `RRC Reconfiguration` message to the UE.
⑦ The UE interrupts the connection with sBS and performs a RACH procedure with the tBS [1]. After successful RACH, the UE considers the handover as complete, and transmits a `RRC Reconfiguration Completed` message to the tBS.
⑧ The tBS considers the handover complete and sends a `Handover Notify` message to the AMF to inform it about the change of connection handler for the UE.
⑨ The AMF transmits a `UE Context Release` message to sBS, instructing it to release resources that were dedicated to the UE.

According to the 3GPP specifications [5], we can classify cellular handovers based on whether: (i) the serving and target cells belong to the same or to different BSs; (ii) the sBS and tBS belong to the same or different AMF; (iii) the sBS and tBS belong to the same or different Radio Access Technologies (RAT). For 5G networks, we distinguish between two handover scenarios. An *N2-handover* occurs when the CN, and therefore the serving AMF (sAMF), is involved (shown in Fig. 2), and an *Xn-handover* occurs when there is a dedicated and direct communication channel between the sBS and tBS [2, 27]. In the latter case, the time required for handover completion is lower since there are fewer delays associated with network entities.

Generally, once received the `RRC Reconfiguration` message, the UE interrupts the connection with sBS. However, 3GPP allows also the possibility for a special case of handover called as *Dual Active Protocol Stack* (DAPS) handover [2]. According to DAPS handover, the UE maintains the downlink with the sBS until it receives instruction from the tBS to release the connection. Also, in DAPS handover case, the UE maintains the uplink until successful RACH with tBS. Whether to use standard or DAPS handover generally depends on the UE capabilities [2]. All the aforementioned cellular handover procedures consist of three phases [10, 28]:

- *Preparation* (Steps 1 - 5): decision of handover and resource allocation on the tBS side,
- *Execution* (Steps 6-7): instruction to proceed for handover and connection to the tBS, and
- *Completion* (Steps 7-9): update of the new serving base station and release of old resources.

3 THREAT MODEL

An adversary carrying out an FBS attack aims to stealthily make the UE connect to a rogue base station (rBS) instead of a legitimate BS. Such an attack enables the adversary to gain control over the UE connection, possibly leading to other types of attacks, such as DoS, MitM or bidding-down attacks [33]. We adopt a threat model similar to [10] and [24]. Our threat model makes the following assumptions:

- The attacker can drop, modify, inject and eavesdrop messages exchanged between legitimate parties. Specifically, the attacker is able to collect MIB and SIB messages broadcast by BSs.
- The attacker can set up a rBS that has the same capabilities as a legitimate BS.
- The attacker cannot tamper with the USIM card, BSs, and CN. Specifically, they cannot learn keys derived during the AKA protocol other than by exploiting vulnerabilities of the AKA protocol itself.
- The attacker can successfully complete a standard RACH procedure with the victim UE [3, 4].

4 THE FAKE BASE STATION ATTACK

In this section we provide an overview of the FBS attack and briefly describe its flow. We observe that an FBS attack is feasible during the handover process and during initial access (IA). We direct the reader to [10] for a more detailed description of the FBS attack.

4.1 Attack Flow

Consider a scenario where an attacker sets up a rBS to imitate a tBS. First, the attacker sniffs the SIB and MIB messages broadcast by the tBS, and replays them without modification. The general principle that 5G networks follow for selecting the best BS is based on the power of the received signal. The BS providing the highest signal strength is (commonly) chosen as the best BS, and thus as the tBS for handover [10, 24]. As a consequence, the attacker transmits the replayed messages with a higher transmission power compared to the surrounding BSs (Fig. 3, ①). Once a UE falls within the transmission range of the rBS, it reads the replayed messages and transmits the `MR` message containing information about surrounding BSs. After receiving the `MR`, the sBS triggers handover to the legitimate tBS (Fig. 3 ②). However, upon receiving the `Handover Command`, the UE connects to the rBS instead of the tBS, and the FBS attack is successful (Fig. 3 ③). Finally, since the tBS does not receive any connection from the UE, it does not send the `Handover Notify` to the AMF, which in turn does not send the `Context Release` command to sBS (Fig. 3 ④,⑤).

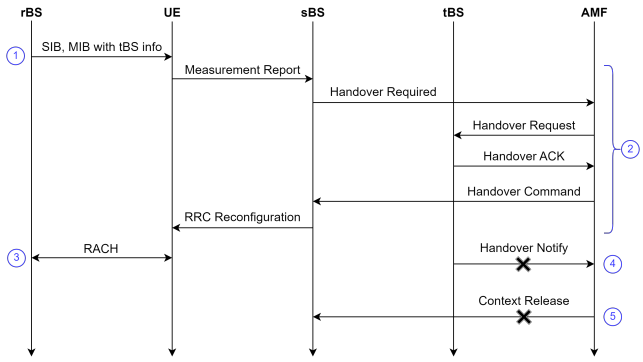

Figure 3: Example of call flow of a *Fake Base Station* attack. The UE receives replayed messages from the rBS. When instructed for handover, the UE performs RACH with the rBS, believing it to be the legitimate tBS, resulting in attack success. The × symbol indicates that the corresponding message is not transmitted.

4.2 Attack Consequences

An FBS attack has an impact on both, the user, as well as the CN [10, 22, 24].

Impact on the network.

- *Resource wastage*: If the handover fails, then all resources used during handover preparation are wasted. However, this issue is not limited to handover preparation only. From the perspective of the CN, the UE has disappeared, and the AMF initiates a *paging* procedure to locate the UE [2] which results in additional resource utilization.
- *BS disconnection*: A BS that has a handover success rate below a desired threshold (95% in [22]) may be removed from the list of possible targets until it is recovered.

Impact on UE.

- *DoS attacks*: The attacker can reject all incoming messages resulting in complete DoS to the UE.
- *Bidding-down attacks*: The attacker forces the UE into adopting older cellular standards (*e.g.*, 2G or 3G). Older standards usually provide lower service quality and security. Therefore, the attacker may exploit these protocols' vulnerabilities to carry out subsequent attacks.
- *Location tracking*: In the case of 4G networks, the attacker can exploit the lack of authentication and integrity protection of the `Identity Request` message. This forces the UE to transmit its permanent or temporal subscriber identifier in plain-text. As a result, the attacker can track UE movements by exploiting vulnerabilities in the paging protocol [14]. The 5G standard overcomes this vulnerability by requiring the UE to encrypt its identifiers, and to periodically refresh the temporal identifier. However, an adversary may still be able to perform location tracking by carrying out a bidding-down attack.

5 BARON

In this section, we describe the working of BARON and detail how it mitigates the impact of an FBS attack. The adversary is assumed to be as defined in Section 3. All exchanged messages, except for those between the UE and tBS (or rBS) are assumed to be authenticated and encrypted (Sec. 2.2).

5.1 FBS Attack: Reasons for Vulnerability

As identified in [10], there are three major reasons that make 5G networks vulnerable to an FBS attack:

- *Insecure transmission of broadcast messages*: The UE completely trusts the content and provenance of MIB / SIB messages that are transmitted and accepted without any authentication;
- *Unverified measurement reports*: The sBS completely trusts the content of the `MR` message without verification;
- *Missing cross-validation*: There is no cross-verification to check if the content of the `MR` message reports data values that correspond to those expected for the real tBS.

In works [15, 24], authors identify the *insecure transmission of broadcast messages* as the primary cause for 5G networks being vulnerable to FBS attacks. In order to mitigate this vulnerability, the authors developed a sequence of digital signature schemes to authenticate MIB and/or SIB messages. Such an approach, however, might be vulnerable to replay attacks [15, 24].

The broadcast nature of the MIB / SIB messages allows users to gather information about the BS. As a result, all users, including those that are not yet in the *RRC_Connected* [1] status, need to be able to verify the authenticity of MIB / SIB messages. In the absence of a pre-distributed public key, the BS itself must provide the public key together with the authenticated message.

In order to design a completely secure defense mechanism against the threat model described in Sec. 3, we analyze the vulnerability to FBS attacks from a different perspective. Consider the handover procedure presented in Sec. 2.3. According to the 3GPP specifications [2], the UE considers a handover to be complete at the conclusion of the RACH procedure. We observe that the success condition is "UE successfully concludes RACH", and not "UE successfully concludes RACH with the tBS". As a consequence, in the absence of an active adversary, the UE connects to the tBS correctly; however, when subject to an FBS attack, the UE will connect to the rBS while believing the handover to be completed successfully. We also observe that the UE is "left alone" during handover execution: once the UE receives instruction to proceed for handover, there is no feedback from the CN to verify whether a legitimate tBS has actually been reached or not. In our analysis, we observe that the UE will then have no means to corroborate whether the RACH procedure has been executed with the legitimate tBS. BARON, by design, addresses this vulnerable aspect of the handover procedure.

5.2 BARON: Overview

BARON defence methodology relies on the chain of trust built by the UE through the AKA protocol [6]. We introduce the notion of a *Closest Trusted Entity* (CTE), which acts as a guarantor for the authenticity of the tBS with which the UE is establishing a connection.

Definition 5.1 (Closest Trusted Entity (CTE)). *The Closest Trusted Entity in a 5G network is the closest node to the UE that can ensure trust and security on behalf of the core network, and for which the UE has a valid security context. During a handover, these two conditions must hold for both, serving and target base stations.*

We provide two examples to illustrate the CTE.

Example 5.1. *Consider an N2-handover in Fig. 2 where both the sBS and tBS are under the control of the same AMF. In this case, the AMF acts as the CTE since it is the last node of the network (the closest to UE) that is common to both sBS and tBS, for which the UE has a valid security context. In the case when sBS and tBS do not belong to the same AMF, the serving AMF (sAMF) will act as the CTE. This is because the sAMF can reach the target AMF (tAMF), which in turn reaches the tBS.*

Example 5.2. *Consider an Xn-handover. Since sBS and tBS can directly communicate, the sBS is the CTE.*

The objective of BARON is to allow a UE to be cognizant of whether a reached BS is legitimate or not. We can accomplish this objective by requiring the tBS to prove that is has communicated

with the CTE. At the completion of the RACH procedure, the UE expects to receive (within a certain time-interval) an *Authentication Token (AT)* that could have been computed only by the CTE.

The rBS is not able to establish a connection with the CTE since it is not legitimate. Moreover, encryption of the AT with the key of the CTE (described in Sec. 5.3) ensures that an attacker sniffing a message during wireless transmission will not be able to use that before decrypting it. In such a scenario, the attacker has two options: (i) not transmit anything, or (ii) randomly guess the AT. For (i), the absence of a transmitted message will ensure that the UE considers the handover as failed and initiates a reconnection procedure. In the case of (ii), if n bits are used for AT, the probability that a guess is correct is 2^{-n}, which decreases to 0 as n increases. As a result, the UE will reject the connection with high probability (for large values of n) and initiate a reconnection procedure.

BARON leverages the above insight and uses reception of the correct AT from the tBS as proof of communication with the CTE, thereby guaranteeing the legitimacy of the tBS with high probability. We note, however, that BARON does not prevent the UE from connecting to the rBS. Rather, it provides a means to verify if a reached BS is legitimate. We propose two ways in which BARON can be implemented.

5.3 BARON: Defense Mechanism 1

The first approach we propose is a *challenge-response* mechanism, wherein the UE challenges the tBS by transmitting a random value, and expects to receive a response that could have been correctly computed only by the CTE. Such a mechanism is suitable for both IA and handover, with minor differences between the two cases. We assume that the UE has already performed *Initial Registration* to the CN, implying it already has a valid security context.

Let the sAMF be the CTE. Together with the `MR` message, the UE transmits the AT, which is the encryption of a random number R. The encryption is performed using the symmetric key K_{CTE}, shared between the UE and CTE. The sBS then forwards the AT to the sAMF which retrieves R and computes $R' = H(R)$. The function $H(\cdot)$ can be any deterministic or randomized function. The sAMF encrypts R' to obtain the AT' value, and forwards it to the tBS with the `Handover Required` message. After completing the RACH procedure, the UE starts an internal timer for both handover and IA. If the timer expires, the UE considers the connection attempt as failed. In the meantime, the UE also computes AT' and expects to receive a message from the tBS containing $\tilde{AT'}$. In case of reception, the UE suspends the timer and verifies whether $AT' = \tilde{AT'}$. If the two values match, the UE deems the tBS to be legitimate. Otherwise, it initiates a connection recovery procedure in case of handover, or selects a new tBS in case of IA. The underlying working principle in the case of IA is similar to that for handover, with the main difference being that there is no sBS. Therefore, the UE transmits the AT to tBS. For example, the N2-handover (Fig. 4) and IA (Fig. 5) procedures with BARON develops according to the following steps:

N2-Handover with BARON (Fig. 4):

① UE → sBS: (MR, AT)
- MR = Measurement Report
- $AT = E_{K_{CTE}}(R)$ | R = random number, $E_K(\cdot)$ = encryption, key K

② sBS → AMF: (`Handover Required`, AT)

③ AMF → tBS: (`Handover Request`, AT')
- $R = D_{K_{CTE}}(AT)$ | $D_K(\cdot)$ = decryption, key K
- $R' = H(R)$ | $H(\cdot)$ = any algorithm
- $AT' = E_{K_{CTE}}(R')$

④ tBS → AMF: `Handover ACK`

⑤ AMF → sBS: `Handover Command`

⑥ sBS → UE: `RRC Reconfiguration`

⑦ UE ↔ tBS: RACH procedure

⑧ tBS → UE: $\tilde{AT'}$

⑨ UE: verifies whether $AT' = \tilde{AT'}$

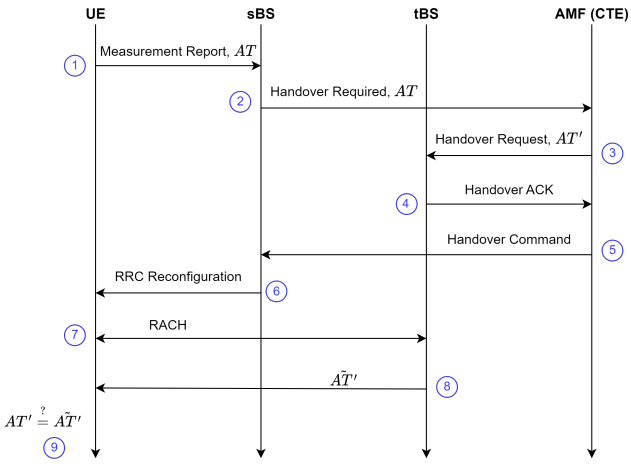

Figure 4: Example of an N2-handover using BARON with *Defense Mechanism 1*. Receipt of the correct AT' from the tBS proves it has communicated with the CTE, thereby establishing its legitimacy.

Initial Access with BARON (Fig. 5):

① UE → tBS: $msg = \left(UE_{info}, ID_{CTE}, AT, MAC_{UE}\right)$
- UE_{info} = user information
- ID_{CTE} = identifier of the CTE
- $AT = E_{K_{CTE}}(R)$ | R = random number, $E_K(\cdot)$ = encryption, key K
- MAC_{UE} = Message Authentication Code of the UE, computed using K_{CTE}

② tBS → AMF: msg

③ AMF: verifies the MAC_{UE} and computes AT'
- $R = D_{K_{CTE}}(AT)$ | $D_K(\cdot)$ = decryption, key K
- $R' = H(R)$ | $H(\cdot)$ = any algorithm
- $AT' = E_{K_{CTE}}(R')$

④ AMF → tBS: $(VerificationOK, AT')$

⑤ tBS → UE: $\left(VerificationOK, \tilde{AT'}\right)$

⑥ UE: verifies for $AT' = \tilde{AT'}$

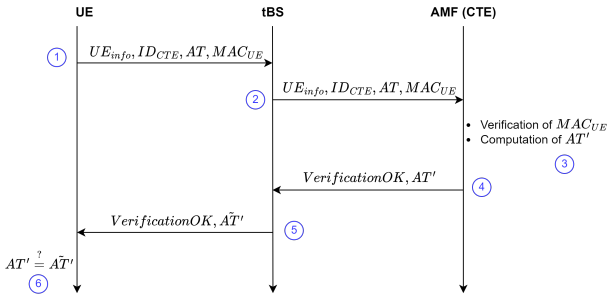

Figure 5: Example of initial access procedure using BARON with *Defense Mechanism 1*. Receipt of the correct MAC_{UE} establishes legitimacy of the UE to the AMF. Receipt of the correct AT' from the tBS proves that it has communicated with the CTE, thereby establishing its legitimacy.

We make the following remarks about this mechanism:

- It is always true that the sAMF is the CTE for N2-handover. However, this may not hold for IA. Thus, the ID_{CTE} and K_{CTE} need be properly selected. We provide additional details on CTE selection at IA in Appendix A.
- During the IA procedure, UE_{info} is the set of all information that the UE transmits according to standard 3GPP for IA [1], and the MAC_{UE} is used to provide UE authentication to the CTE. Although we want to challenge the tBS, at the same time, we want the AMF and tBS to respond if and only if the challenge comes from a legitimate user.
- We leave implementations of $E(\cdot)$, $D(\cdot)$ and $H(\cdot)$ algorithms to the service provider, based on their needs and constraints, as long as these are reasonably fast algorithms. The same applies to the MAC_{UE}.

Fig. 6 shows the flow for the case of an Xn-handover. The underlying procedure is the same as that for the N2-handover, with the only difference being that the sBS is the CTE for the Xn-handover.

5.4 BARON: Defense Mechanism 2

We can apply this second defense mechanism to implement BARON only to handover because it requires that the UE already has an ongoing trusted connection. In this case, the UE does not challenge the tBS but receives the AT along with the `RRC Reconfiguration` message from sBS (which is a trusted node). The AT is computed by the CTE (sAMF for the N2-handover, and sBS for Xn-handover). Following this, similar to *Defense Mechanism 1* (Sec. 5.3), the UE expects to receive the $\tilde{AT}$ from tBS, and compares it with the previously received AT. If the two values match, the UE can conclude that the tBS is legitimate. Here, the AT can take any arbitrary value; the only condition that needs to be satisfied is $AT = \tilde{AT}$.

The *Defense Mechanism 2* is better suited for resource-constrained devices (*e.g.*, IoT devices), since the UE does not need to compute any cryptographic value. Fig. 7 shows the steps for an N2-handover using *Defense Mechanism 2*.

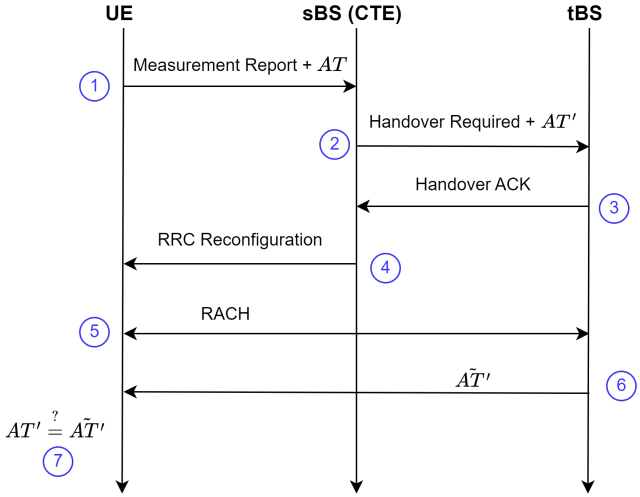

Figure 6: Example of Xn-handover using BARON with *Defense Mechanism 1*. Here, the sBS is the CTE due to the direct communication between sBS and tBS. Receipt of the correct value of AT' from the tBS is proof that the tBS has communicated with the CTE, thereby establishing its legitimacy.

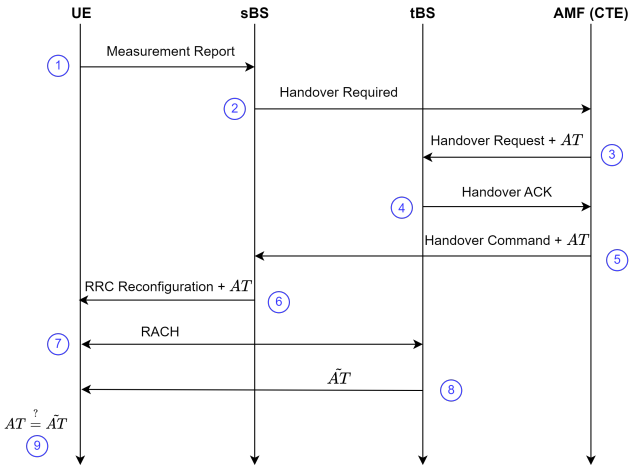

Figure 7: Example of an Xn-handover using BARON with *Defense Mechanism 2*. Here, the UE does not challenge the network but receives the AT from the sBS, which is trusted. Receipt of the correct AT from the tBS proves it has communicated with the CTE, thereby establishing its legitimacy.

6 BARON: RECOVERING CONNECTION TO A LEGITIMATE BASE STATION

The BARON Defense Mechanisms described in Sec. 5 allows the UE to determine if a tBS with which it has established a connection is legitimate. However, since BARON does not prevent the UE from connecting with a rBS, it will be important to provide a fast and efficient mechanism to recover connection to a legitimate BS.

Table 1: Comparison of advantages and drawbacks for *Reconnection Token* (RT) computation (i) by sBS and (ii) by AMF.

RT computation method	Advantages (✓) and Disadvantages (×)
sBS computes RT	✓ Faster reconnection since there is no need to pass through the AMF ✓ No transmission overhead introduced between sBS and AMF × Can reconnect only to sBS if no direct communication between BSs (Xn-configuration)
AMF computes RT	✓ Can reconnect to any reachable BS under that AMF × Introduces transmission overhead between sBS and AMF × Longer reconnection time

The recovery mechanism that we propose follows similarly to the BARON Defense Mechanisms. The objective is to allow a UE that is the victim of an FBS attack to efficiently and securely recover connection with a legitimate BS. When instructed to proceed for handover, the UE receives an additional token termed the *Recovery Token* (*RT*). This token is used to quickly recover a connection in case of handover failure, while at the same time, ensuring legitimacy of the new tBS. If a handover fails, the UE initiates the recovery procedure by selecting the tBS (excluding the previous tBS) with the highest signal strength. It then transmits a `Connection Recovery` message containing UE_{info}, ID_{CTE} and RT' (computed from RT). Three scenarios are possible:

(1) The new tBS coincides with the previous sBS. In this case, the sBS is the CTE.
(2) The new tBS does not coincide with previous sBS, but belongs to the sAMF. Here, the sAMF is the CTE.
(3) The new tBS does not belong to the sAMF. In this case also, the sAMF is the CTE.

The above procedure reduces the recovery of a legitimate connection to that of IA, where RT' simultaneously serves as the AT and MAC_{UE}. Consider an N2-handover using BARON *Defense Mechanism 1*, where the UE is a the victim of an FBS attack. Further, assume that the UE reconnects to the sBS. The recovery mechanism develops as follows (Fig.8):

Legitimate Connection Recovery (Fig. 8):

① AMF → sBS: `Handover Command`
② sBS → UE: (`RRC Reconfiguration`, RT)
- $RT = E_{K_{CTE}}(M)$ | M = random number, $E_K(\cdot)$ = encryption, key K

③ After RACH, rBS → UE: $\tilde{AT'}$
④ UE: verifies for $AT' = \tilde{AT'}$.
For an n-bit message, with probability $1 - 2^{-n}$: $\tilde{AT'} \neq AT'$
⑤ UE → sBS: (`Connection Recovering`, UE_{info}, ID_{CTE}, $\tilde{RT'}$)
- UE_{info} = user information
- ID_{CTE} = identifier of the CTE
- $M = D_{K_{CTE}}(RT)$ | $D_K(\cdot)$ = decryption, key K
- $M' = H(M)$ | $H(\cdot)$ = any algorithm
- $\tilde{RT'} = E_{K_{CTE}}(M')$

⑥ sBS: verifies for $\tilde{RT'} = RT'$
⑦ sBS → UE: (`Reconnection Accepted`, $\tilde{RT''}$)
- $M'' = H(M')$
- $\tilde{RT''} = E_{K_{CTE}}(M'')$

⑧ UE: verifies for $\tilde{RT''} = RT''$

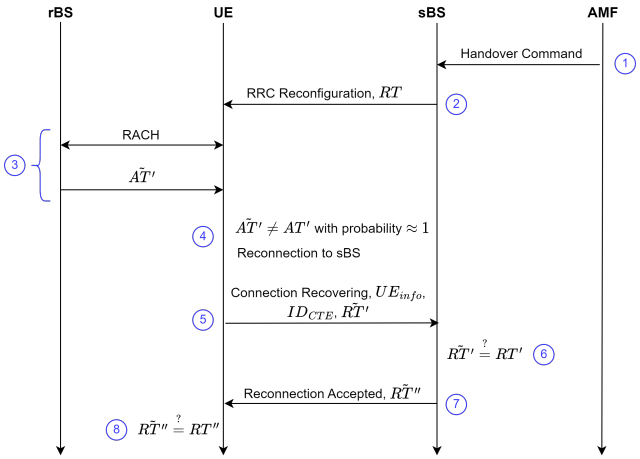

Figure 8: Example of BARON legitimate connection recovery procedure after an FBS attack. At the end of the procedure, the UE reconnects with the sBS.

We need to define which entity should compute the RT value - the sBS or sAMF. Table 1 lists the advantages and disadvantages in each case. We propose to adopt a hybrid strategy to overcome limitations of each solution. The sAMF initially generates RT. However, if the UE tries to reconnect with the sBS, the RT value is treated as if it was the random number M, thus $RT' = H(RT)$. This will allow an immediate reconnection to the sBS, without requiring an intervention from the sAMF. If instead, the new tBS is not the same as sBS, we will need to pass through the sAMF. Such a hybrid solution allows selection of the best reconnection strategy depending on the specific scenario.

In the case of connection recovery with the sBS when a deterministic algorithm $H(\cdot)$ is used, an attacker sniffing the communication channel will be able to easily compute the value of RT' (= $H(RT)$) and thus increasing the probability of success for a FBS attack. To prevent this possibility, we shall transform the value of RT before passing it as an input to $H(\cdot)$. One way to carry out this transformation, while also encrypting RT, is through an XOR operation between RT and (a portion of) the key K_{gNB} that was previously shared between the UE and sBS. This process will ensure that only the legitimate UE could have computed the correct value of RT'.

We observe that such a recovery mechanism is required only for handover, since it will be sufficient to change the tBS in the case of IA. The DAPS handover scenario [1] also does not require a

dedicated connection recovery mechanism. In this setting, since the UE does not drop connection with the sBS, when a tBS is identified as not legitimate, the UE can fall back to the connection with the sBS. In the case the handover fails, the UE also transmits the *Radio Link Failure* (RLF) report to notify the unsuccessful handover [1].

7 BARON PERFORMANCE EVALUATION

We carry out extensive experiments to evaluate the performance of BARON by simulating an N2-handover. We observe that the additional overhead induced by BARON is 10000× lower than a state-of-the-art method from [24]. All numbers we report are computed as the average over 10 turns (each of 1000 runs) of a self-contained software simulation. Our code is written in C++; we provide details in Appendix B, and make the source code publicly available[2]. The performance of BARON is quantified in terms of two metrics:

(1) overhead induced due to the computation, transmission, and evaluation of the AT and RT values, and
(2) time required for connection recovery after an FBS attack.

We summarize our main findings in Table 2, which indicates that the induced overhead when using BARON is minimal. Table 2 also shows that the time required for reconnection following an FBS attack is a fraction of the time required for handover completion.

We use 32-bit random numbers R, M in our implementation to represent a balanced trade-off between security and memory overhead. The length of the random numbers can be suitably adjusted, based on the needs of service providers. We use the following functions in our experiments:

- $E(\cdot), D(\cdot)$: For encryption and decryption, we use a custom implementation of $AES-128$.
- $H(x)$: We use a simple, but effective deterministic function $H(x) = x + 1$ in order to process the response for AT. This choice of $H(\cdot)$ introduces minimal overhead. At the same time, the security of BARON is not compromised since AT will be encrypted at a subsequent stage.
- $H'(x) := x \oplus K_{gNB}$, where $\oplus$ is the binary XOR operation. This function is applied to RT during reconnection with sBS in order to compute the value of RT' in the `Connection Recovery` message (Fig. 8 ④).

7.1 BARON: Induced Overhead

We evaluate the time overhead induced by BARON by comparing the time required for a handover using a standard 3GPP procedure with the time required to complete a handover when using BARON. In this case, we assume that there is no FBS attack. This allows us to examine the additional time that will be required to manage and transmit values of AT and RT when using BARON. We separately evaluate the cases wherein the tBS is under the control of the sAMF and when it is not in the sAMF. Fig. 9 compares the actual times taken to complete a handover using the standard 3GPP procedure (orange bars) and when using BARON (blue bars). We observe that the time taken to complete the handover when using BARON is almost equal to the time taken when following the standard 3GPP procedure. **The overhead induced by BARON is** $\sim 43\ ns$**, which is about** 10000× **lower** than the overhead reported in [24] (0.53 ms).

[2]https://github.com/aleLtt/BARON_simulation.git

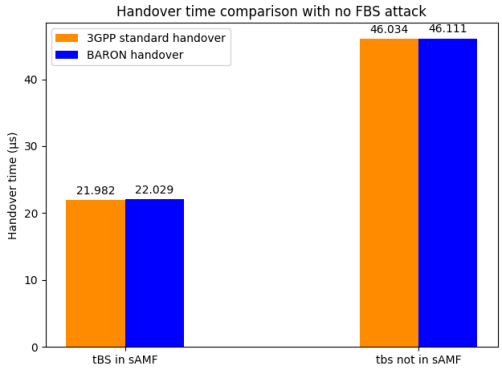

Figure 9: Comparison of times for handover completion between the standard 3GPP procedure and BARON with *Defense Mechanism 1* when there is no FBS attack. The additional overhead introduced by BARON in both cases is negligible.

7.2 BARON: Connection Recovery Time

To evaluate the connection recovery time, we consider a scenario where an adversary is carrying out an FBS attack. In this setting, we measure the time required to recover connection to a legitimate BS when using BARON. Since the absolute value of the time needed for connection recovery strictly depends on the specific network topology, we present results as a fraction of the time required for BARON handover completion in the case of no FBS attack. Let:

- T_1: time for handover completion using BARON when tBS is under the control of the same AMF as sBS (sAMF).
- T_2: time for handover completion using BARON when tBS in not under the same AMF as sBS.

We evaluate the time required for reconnection when the tBS is (i) the same as the sBS, (ii) in the sAMF as the sBS, and (iii) not in the sAMF as the sBS. Further, we implement an active attacker that randomly guesses the value of AT'. Fig. 10 compares the time for handover completion when using BARON in the absence of an FBS attack (orange bars) and the (total) time for handover completion and connection recovery when using BARON in the presence of an FBS attack (blue bars) for the scenarios (i) - (iii). We observe that the additional time for connection recovery is of a similar order of magnitude as the time required for handover completion. Based on our results from Sec. 7.1, we can conclude that the additional time required to re-establish connection to a legitimate BS is almost entirely associated with transmission delays rather than computation and verification of values of RT. A further reduction in reconnection time might be possible by using the hybrid strategy defined in Sec. 6. Our results in this section reveal that **the total time for handover completion and reconnection to a legitimate BS using BARON is still lower than the** 0.53 ms **overhead** presented in [24]. Reporting the reconnection time as a fraction of the time required for handover completion will also allow our experiments to be extended for arbitrary network topology and UE location.

Table 2: Performance of BARON in terms of the induced overhead, and time required for reconnection following an FBS attack.

	tBS is sBS	tBS in sAMF	tBS not in sAMF
BARON overhead*	N.A.	$< 1\%$	$< 1\%$
BARON reconnection time	0.25-0.30 T_1^{**}	0.65-0.70 T_1	0.25-0.30 T_2^{**}

*Overhead is given comparing the BARON handover time and 3GPP standard handover time in case of no FBS attack.
**T_1 = BARON handover time with tBS in sAMF; T_2 = BARON handover time with tBS not in sAMF.

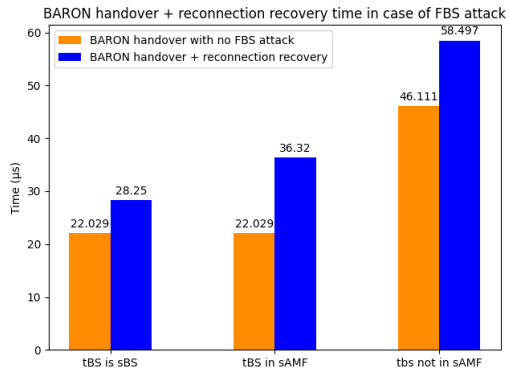

Figure 10: Comparison of times between handover completion using BARON with *Defense Mechanism 1* in absence of an FBS attack, and total time for handover and connection recovery completion in case of an FBS attack.

8 RELATED WORKS

A large part of the existing research in the security of 4G and 5G cellular networks focuses on the identification of weaknesses and the design of countermeasures to overcome these weaknesses [15]. For example, methods to overcome vulnerabilities in privacy in wireless networks are proposed in [21, 32]. These solutions, however, are not adequate to defend against an FBS attack. Another approach investigated is to add an integrity protection mechanism to messages that are broadcast [4, 22, 23]. However, an attacker might be able to deceive such a defense mechanism by carrying out a bidding-down attack, as noted in [24]. Detection mechanisms have also been designed to identify inconsistencies in the content of MR messages and deployment information (e.g., BS identifier, operation frequency) of a legitimate BS [6, 19, 34]. Machine learning techniques for FBS detection are becoming increasingly popular [12, 16]. However, recent work [22, 29] has demonstrated that such solutions can be ineffective. Digital signature schemes to authenticate broadcast messages, either using a PKI infrastructure or a certificate authority, have been proposed in [15, 18, 24, 31]. In [15] authors propose an optimized PKI infrastructure-based solution to authenticate SIB1 and SIB2 messages. Challenges that were identified in [15] related to the management of a PKI infrastructure included the size of the certificate, vulnerabilities to replay attacks, and public key revocation. These challenges were faced by the use of a custom encoding to limit the size of the certificate, a location-dependent parameter to mitigate replay attacks, and a time-based expiration mechanism for public keys respectively. Several schemes are evaluated, with the smallest overhead reported in [15] was $\sim 176ms$. However, this solution was not fully secure against replay attacks [15]. The same research group propose in [24] a Schnorr-HIBS digital signature-based scheme with hierarchical key derivation. This work does not rely on a PKI, but rather, it introduces a private key generator (PKG) node to generate private keys from a master secret. The PKG is embedded within the CN and distributes the generated keys to participating entities. These entities then generate private keys for lower-layer entities. The hierarchical key derivation proceeds up to the AMF generating private keys for the BSs. The BSs authenticate the SIB1 messages with their private key and attach to it the corresponding public key for verification. The security of this mechanism is guaranteed by the hierarchical key derivation process, which binds the BSs' private and public keys to those of the CN entities. The proposed scheme, thanks to optimizations, managed to reduce communication overhead by 31% compared to [15, 18, 31], and incurred a fixed end-to-end delay of $0.53ms$ [24]. However, this solution may still be vulnerable to replay attacks. Comparing with the above methods, BARON introduces negligible ($< 1\%$) overhead while being able to successfully determine legitimacy of a BS and restore connection to a legitimate BS when subject to an FBS attack.

9 CONCLUSION

In this paper, we developed BARON, a framework for secure initial access and handover in 5G networks against FBS attacks. BARON introduces the concept of *closed trusted entity*, thanks to which it enables the UE to (i) determine whether a BS it is connecting to is legitimate or not and (ii) efficiently recover a legitimate connection when subject to an FBS attack. Our experiments evaluated the performance of BARON in terms of the time overhead introduced during handover, and effectiveness in recovering a legitimate connection in case of an FBS attack. Our experimental results revealed that BARON introduces an overhead of less than 1% of the time required for standard 3GPP handover completion. In case of being victim of an FBS attack, the time taken by a UE to recover connection to a legitimate base station using BARON is of the same order of magnitude as the time required for handover completion in the absence of an FBS attack.

ACKNOWLEDGMENTS

This work was supported by the US National Science Foundation, the Office of Naval Research, European Commission under the Horizon Europe Program, as part of the project LAZARUS, via grants CNS-2153136, N00014-20-1-2636 and 101070303 respectively. The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

REFERENCES

[1] 3GPP. 2019. *5G; NR; Radio Resource control (RCC); Protocol specification.* Technical Specification (TS) 38.331. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/ChangeRequests.aspx?q=1&specnumber=38.331 Version 15.6.0.

[2] 3GPP. 2020. *5G; NR; NR and NG-RAN Overall description; Stage-2.* Technical Specification (TS) 38.300. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/ChangeRequests.aspx?q=1&specnumber=38.300 Version 16.2.0.

[3] 3GPP. 2020. *Physical layer procedures for control.* Technical Specification (TS) 38.213. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/ChangeRequests.aspx?q=1&specnumber=38.213 Version 16.2.0.

[4] 3GPP. 2020. *Technical Specification Group Services and System Aspects Study on 5G Security Enhancement against False Base Stations (FBS) (Release 17).* Technical Specification (TS) 33.809. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539 Version 0.12.1.

[5] 3GPP. 2021. *5G; Procedures for the 5G System (5GS).* Technical Specification (TS) 33.809. 3rd Generation Partnership Project (3GPP). https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/16.07.00_60/ts_123502v160700p.pdf Version 16.7.0.

[6] 3GPP. 2022. *Security architecture and procedures for 5G system.* Technical Specification (TS) 33.501. 3rd Generation Partnership Project (3GPP). https://portal.3gpp.org/ChangeRequests.aspx?q=1&specnumber=33.501 Version 17.7.0.

[7] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. 2019. Security for 5G and beyond. *IEEE Communications Surveys & Tutorials* 21, 4 (2019), 3682–3722.

[8] Adnan Aijaz. 2020. Private 5G: The future of industrial wireless. *IEEE Industrial Electronics Magazine* 14, 4 (2020), 136–145.

[9] Nadine Akkari and Nikos Dimitriou. 2020. Mobility management solutions for 5G networks: Architecture and services. *Computer Networks* 169 (2020), 107082.

[10] Evangelos Bitsikas and Christina Pöpper. 2021. Don't Hand It Over: Vulnerabilities in the Handover Procedure of Cellular Telecommunications. In *Annual Computer Security Applications Conference*. 900–915.

[11] Sathian Dananjayan and Gerard Marshall Raj. 2021. 5G in healthcare: how fast will be the transformation? *Irish Journal of Medical Science (1971-)* 190, 2 (2021), 497–501.

[12] Van Thuan Do, Paal Engelstad, Boning Feng, and Thanh van Do. 2016. Strengthening mobile network security using machine learning. In *International Conference on Mobile Web and Information Systems*. Springer, 173–183.

[13] Akhil Gupta and Rakesh Kumar Jha. 2015. A survey of 5G network: Architecture and emerging technologies. *IEEE access* 3 (2015), 1206–1232.

[14] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. *Network and Distributed Systems Security (NDSS) Symposium2019* (2019).

[15] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. 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*. 1–11.

[16] Jian Jin, ChangLiang Lian, and Ming Xu. 2019. Rogue base station detection using a machine learning approach. In *2019 28th Wireless and Optical Communications Conference (WOCC)*. IEEE, 1–5.

[17] Damigou Kombate et al. 2016. The Internet of vehicles based on 5G communications. In *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 445–448.

[18] Cheng-Chi Lee, I-En Liao, and Min-Shiang Hwang. 2009. An extended certificate-based authentication and security protocol for mobile networks. *Information Technology and Control* 38, 1 (2009).

[19] Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu. 2017. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild.. In *NDSS*.

[20] Aleksi Peltonen, Ralf Sasse, and David Basin. 2021. A comprehensive formal analysis of 5G handover. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 1–12.

[21] Yue Qiu, Maode Ma, and Xilei Wang. 2017. A proxy signature-based handover authentication scheme for LTE wireless networks. *Journal of Network and Computer Applications* 83 (2017), 63–71.

[22] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2018. 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*. 75–86.

[23] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. 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*. 221–231.

[24] Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, Attila Yavuz, and Elisa Bertino. 2021. 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*. 501–515.

[25] S. Sullivan, Alessandro Brighente, S. A. P. Kumar, and M. Conti. 2021. 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access* 9 (2021), 116294–116314. https://doi.org/10.1109/ACCESS.2021.3105396

[26] Techplayton.com. 2021. 5G SA Inter gNB Handover – N2 Handover. Retrieved Febbruary 10, 2023 from https://www.techplayon.com/5g-sa-inter-gnb-handover-n2-or-ngap-handover/

[27] Techplayton.com. 2021. 5G SA Inter gNB Handover – Xn Handover. Retrieved Febbruary 10, 2023 from https://www.techplayon.com/5g-sa-inter-gnb-hanodver-xn-handover/

[28] Techplayton.com. 2022. 5G Mobility Scenarios – Handovers. Retrieved Febbruary 10, 2023 from https://www.techplayon.com/5g-mobility-scenarios-handovers/

[29] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE.. In *USENIX Security Symposium*. 55–72.

[30] Yang Yang and Kun Hua. 2019. Emerging technologies for 5G-enabled vehicular networks. *IEEE Access* 7 (2019), 181117–181141.

[31] Xun Yi, Eiji Okamoto, and Kwok Yan Lam. 1998. An optimized protocol for mobile network authentication and security. *ACM SIGMOBILE Mobile Computing and Communications Review* 2, 3 (1998), 37–39.

[32] Yongbin Zeng, Hui Guang, and Guangsong Li. 2018. Attribute-based anonymous handover authentication protocol for wireless networks. *Security and Communication Networks* 2018 (2018).

[33] Dongsheng Zhao, Zheng Yan, Mingjun Wang, Peng Zhang, and Bin Song. 2021. Is 5G handover secure and private? A survey. *IEEE Internet of Things Journal* 8, 16 (2021), 12855–12879.

[34] Zhou Zhuang, Xiaoyu Ji, Taimin Zhang, Juchuan Zhang, Wenyuan Xu, Zhenhua Li, and Yunhao Liu. 2018. Fbsleuth: Fake base station forensics via radio frequency fingerprinting. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 261–272.

A CTE SELECTION DURING INITIAL ACCESS

The most important aspect of the BARON *Defense Mechanism 1* presented in Sec. 5.3 in the initial access scenario is the selection of the CTE. In practice, it is not always guaranteed that the tBS will belong to the same AMF cluster with which the UE was most recently connected. Further, it might be the case that the encryption key K_{AMF} is no longer valid. We propose two possible methods for CTE selection for initial access: (i) the UE simply reports the identity of the AMF stored, and the task of resolving the AMF is left to the CN, or (ii) the UE is notified that the reported AMF is not a valid CTE for the tBS in question. In (ii), the CTE is changed to an entity of the network in a higher layer than the AMF (as long as this is a valid choice). Both these methods results in additional effort for the CN, and consequently, increased resource consumption and connection delays. The increased connection delay in the initial access scenario might be acceptable in order to accomplish improved security. On the other hand, increased resource utilization might impact the performance of the CN. Analyzing tradeoffs between performance and resource utilization is an interesting avenue for future research.

B SIMULATION IMPLEMENTATION - ADDITIONAL INFORMATION

This appendix provides additional details about our simulation setup for experiments in Sec. 7.

B.1 Simulation Setup

We consider a 2-dimensional plane with coordinates (x, y) and located two AMFs, with each controlling 6 BSs. The UE is randomly placed in the 2-dimensional plane at the start of each simulation, and we assume that it has a connection to a legitimate BS at the start of the run. We choose the sBS to be the second-nearest BS to the UE. As a result, the nearest BS will be selected as the tBS for

handover. The received signal power (PR) from base station i (BS_i) is modelled according to standard signal power propagation:

$$PR_i = \frac{PT_i}{d\,(UE, BS_i)^2}, \tag{1}$$

where $d\,(x, y)$ is the distance between x and y, and PT_i is the transmission power of BS_i.

In the presence of an attacker carrying out a FBS attack, we place the rBS within a range of 150 m from the UE's position. The rBS uses a BS identifier assigned at random, but different from that of the sBS. We additionally ensure that the rBS has a higher transmission power in order to maximize the probability of coming under an FBS attack scenario.

B.2 Handover Completion Time Computation

In our experiments, we assumed that all communications between the UE and BSs are wireless. On the other hand, communication between BSs and AMF, and between two AMFs were wired. The wireless and wired media have different speeds of light: $3\times10^8\ ms^{-1}$ and $2\times10^8\ ms^{-1}$, respectively. The total time required to complete a handover will depend on times associated with transmission delays and message handling. The former represents the time required for a message to reach the destination, while the latter quantifies the time required to generate a response message after receiving an incoming message. We compute the transmission delay (TD) between x and y as:

$$TD = \frac{d(x, y)}{c}, \tag{2}$$

where c is the speed of light, set according to the transmission medium. For computing the handling time we used the `C++` standard "*chrono*" library.

B.3 Experiments: Details of Computations

We use the following procedure to evaluate BARON:

(1) Run the simulation to obtain 1000 samples for each scenario considered;
(2) Determine the median of the 1000 samples;
(3) Repeat steps (1)-(2) 10 times;
(4) Compute the arithmetic mean (average) over the collected values (the median values).

The median is used to eliminate outlier samples. In our experiments, we observed that the magnitude of a very small number of outliers was very large. In such a scenario, using the average would have resulted in misleading values of overhead and connection recovery times.

C INDEX OF TERMS

This appendix gives a complete list of abbreviations used in the paper and their full forms.

Abbreviation	Full form
3GPP	Third Generation Partnership Project
4G-LTE	Fourth generation long term evolution
5G	Fifth generation
ACK	Acknowledgement
AKA	Authentication and key agreement
AMF	Access and mobility function
AT	Authentication token
AUSF	Authentication server function
BS	Base station
CN	Core network
DoS	Denial of service
DAPS	Dual active protocol stack
FBS	Fake base station
IA	Initial access
MIB	Master information block
MitM	Man in the middle
mmWave	Millimeter wave
MR	Measurement report
PKI	Public key infrastructure
RACH	Radio access channel
RAN	Radio access network
RAT	Radio access technology
rBS	Rogue base station
RLF	Radio link failure
RRC	Radio resource control
RT	Reconnection token
sBS	Serving base station
SIB	Secondary information block
tBS	Target base station
UE	User equipment
UDM	Unified data management
USIM	Universal subscriber identity module