Security and Privacy Features Supported by Different Overlay-based ICN/IP Coexistence Architectures

Mihhail Sokolov , Chhagan Lal , Mauro Conti
TU Delft

Abstract

Information-Centric Networking (ICN) is a common approach to the Internet of the future. However, transitioning to the new Internet architecture right away is impractical if not impossible. Hence, there will be some period of coexistence of ICN and IP. This paper investigates the support of security and privacy features in the three most popular overlay-based ICN/IP coexistence architectures - NDN, PURSUIT, NetInf. The aim is to find out which features are supported and which are not in order to determine which one is more secure and therefore more promising.

We analysed these three architectures for the support of availability, access control, data integrity, nonrepudiation, data authentication, anonymity, data confidentiality, and unlinkability. The analysis carried out by the in-depth review of relevant literature shows that NDN and PURSUIT support all eight security and privacy features while NetInf is missing nonrepudiation and does not fully support data authentication. Therefore, NDN and PURSUIT appear to be more secure and hence more promising as an architecture for the Internet of the future.

1 Introduction

Information-Centric Networking (ICN) is a common approach to future Internet architecturing as it is more suitable for modern Internet usage model than the current host-centric architecture. The main purpose of the ICN networks is retrieving the content regardless of where it is stored. In order to accomplish that the content itself is being addressed in the request instead of some specific host that stores it. In addition, the usage of pervasive caching on every network node allows for better scalability and efficiency [2].

Transitioning to the new architecture involves a period of coexistence between the two architectures. There is already some research being done in the area of developing ICN and Internet Protocol (IP) coexistence solutions. Conti et al provides a great overview of such solutions [6]. The three main types of these solutions are overlay-based, underlay-based, and hybrid. This research focuses on the overlay-based architectures for ICN/IP coexistence because of its popularity and ease of integration in the existing networks. Throughout this paper, IP and TCP/IP mean not just the protocols but have a more general meaning as a current host-centric architecture of the Internet.

In the overlay-based architectures, the IP is used for carrying the ICN packets without changing them from one network node to another thus creating a "tunnel" between two or more ICN networks [20]. Underlay-based architectures tend to change or augment the data packet to support coexistence, while hybrid-based architectures aim for supporting both ICN and IP with minimal changes to the current infrastructure [19].

Nevertheless, there still a lot of work to be done before such architectures are ready to be integrated into the real world. Especially important is the security of such solutions because nowadays privacy and security are a major concern for everyone. ***The purpose of this research is to investigate the security and privacy features supported by the different overlay-based ICN/IP coexistence architectures which is one of the types of coexistence solutions***. This research question can be further divided into several sub-questions which we aim to answer:

- How do ICN architectures and their inherent features such as forwarding, naming, caching, and security and privacy work?
- How do the three most popular overlay-based ICN/IP coexistence architectures work and how are they different?
- What security and privacy features do these three architectures support and which features are not supported? How can they achieve the support of missing features?

There has been some work done already regarding the security of ICN (e.g. [21]), however, more research should be put into the research of security of the ICN/IP coexistence solutions. Therefore, this paper aims to answer the question what are the security and privacy features supported by the three of the most popular overlay architectures - Publish-Subscribe Internet Technology (PURSUIT) [8], Network of Information (NetInf) [7], and Named Data Networks (NDN) [23].

The rest of the paper is laid out as follows: Section 2 provides an overview of the three chosen architectures (PURSUIT, NetInf, and NDN) and the work that has been done regarding the security and privacy features of the aforementioned architectures. Section 3 describes the contribution we have made by analysing these architectures focusing on security and privacy features. Next, section 4 discusses the results of the analysis, and section 5 reflects on the ethics and reproducibility of the paper. Following that is section 6 which discusses the results, and lastly, section 7 provides conclusions and discusses the future work.

2 Background and related works

In this section, we explain how the coexistence architectures we investigate (NDN, PURSUIT, NetInf) work - routing, forwarding, caching, etc.

2.1 NDN

According to Zhang et al, in order to receive data in the Named Data Networking (NDN), a consumer must send an Interest packet that contains the name of the desired data [23]. A router that receives this packet first checks if the requested data is already cached in the Content Store (CS). If it is, then the router responds with the Data packet which carries both the name and the content of the data, together with a signature by the producer's key. If the desired data is not cached in the router then it remembers the interface from which the request comes in by making a corresponding entry in the Pending Interest Table (PIT) and forwards the Interest packet by matching the name in its Forwarding Information Base (FIB). FIB is populated using a name-based routing protocol. This process continues until the Interest reaches a node that has the requested data. When this happens, a Data packet is sent back. This Data packet follows the reverse path of the Interest in order to reach the consumer.

Figure 1 below provides an overview of the NDN architecture. Data consumer sends an Interest packet to the NDN network. When the Interest is satisfied by some cached copy or reaches the producer, a Data packet is sent as response containing the requested content.

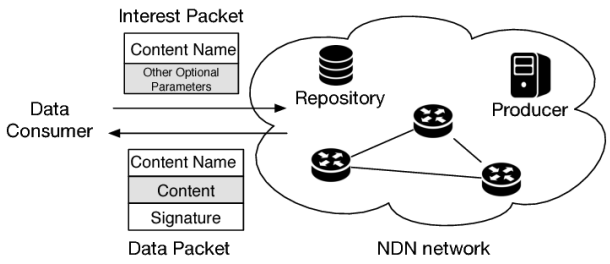

Figure 1: NDN architecture [1]

Both Interest and Data packets do not carry any information that can identify hosts or interfaces (such as IP addresses) because Interest packets are routed using the names specified in the packets, and Data packets are routed based on the information in the PIT at each router hop [23].

As Zhang et al states, NDN routers store Interest and Data packets for some period of time (close to packet round-trip time) [23]. When multiple Interests for the same data are received, only the first Interest is forwarded further. The router then inserts the Interest into the PIT. Each entry in the PIT maps the name of the Interest to the set of interfaces from which the Interest has arrived. When the Data packet is received, the router matches the name and sends the data to the interfaces listed in the according PIT entry. Then the router deletes that PIT entry and stores the Data in the CS.

Naming in the NDN follows a hierarchical structure. This hierarchical structure allows representing relationships between pieces of data and increases routing scalability [23].

As noted by Zhang et al, routing is done similar to how IP does routing [23]. Instead of announcing IP prefixes, NDN routers announce name prefixes of the data they are willing to serve. Then, when an Interest packet needs to be forwarded, the content name is matched in the FIB using the longest prefix match.

In addition, as explained by Zhang et al, NDN naturally supports multipath routing [23]. Interest packets cannot loop, because the name and a random nonce they contain can allow to easily identify duplicates which are then discarded. Data packets also cannot loop since they take the reverse path of Interests. Thus, routers can freely send Interest packets through multiple interfaces without worrying about loops.

According to Zhang et al, the security of NDN relies on public-key cryptography, which allows applications to accomplish data authenticity, confidentiality, and availability regardless of the underlying communication channels and where the data is situated. Data packets that can also carry certificates and trust schemas serve as a powerful foundation for developing security solutions. Furthermore, it is possible to establish naming conventions to define trust policies and enable name-based access control via encryption [24].

Padmanabhan et al explains that NDN-enabled nodes can communicate over IP tunnels, however, they first need to be able to discover each other [17]. In order to achieve that, they propose NDN Neighbor Discovery Protocol where a new entity called a rendezvous server with a defined DNS name is added to the network and manages the communication between isolated nodes. Each node is pre-configured with the rendezvous server's DNS name and can use standard DNS resolution to determine the server's IP address. The node can then send to the server its own IP address and NDN data names and receives the information about other NDN nodes.

2.2 PURSUIT

According to Buitenkamp et al, Publish-Subscribe Internet Technology (PURSUIT) is an architecture that works on a complete publish-subscribe protocol stack [4]. PURSUIT has three main components: a set of Rendezvous Nodes (RNs) known as Rendezvous Network (RENE), Topology Managers (TMs), and Forwarding Nodes (FNs). The naming scheme of data objects in the PURSUIT architecture is made of a unique pair of scope ID and rendezvous ID. The scope ID points to the grouping of contents, while the rendezvous ID is a unique identifier within that group.

A simplified overview of PURSUIT architecture can be seen in the figure 2 below. A content provider publishes some content sending a PUBLISH message to the Rendezvous network and when a user send a SUBSCRIBE message to the network, the path between the content provider and the user is created and data is transferred.

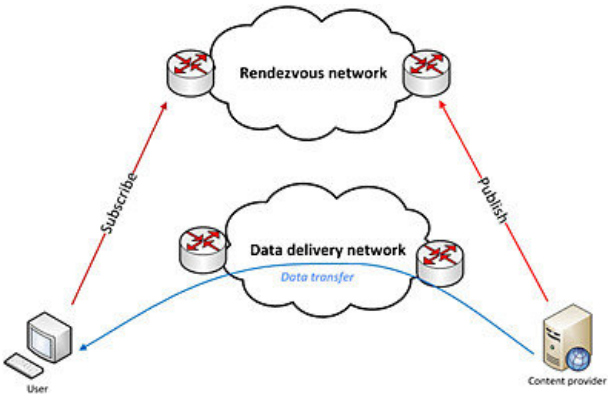

Figure 2: PURSUIT architecture [5]

PURSUIT has a hierarchical routing structure and uses the Distributed Hash Table (DHT) routing architecture. Buitenkamp et al describes the publish and subscribe process as follows [4]. When a publisher wants to make its content available to the network, it sends a Publish message to its local Rendezvous Node. The message is directed there based on the scope ID by the DHT. When a subscriber wants to get this content, it will send a Subscribe message to its local RN, which will use DHT to route the message to the publisher's local RN. The publisher's Rendezvous Node then sends a Delivery Path Request message to the Topology Manager, and the TM creates a route between the publisher and the subscriber. The TM creates a routing Bloom filter and adds it to the packet's header. The TM then sends a Start Publish message to the publisher with the route it created. The publisher then uses that route to send the data through a set of Forwarding Nodes back to the subscriber.

PURSUIT was developed as a continuation and improvement of the PSIRP project (http://www.psirp.org) [8]. Therefore, some of the features of PURSUIT are inherited from PSIRP. PSIRP utilizes elliptic curve cryptography to facilitate good security with shorter keys and smaller signature sizes. Smaller signature sizes allow to include the publisher's signature in every packet [12].

2.3 NetInf

According to Dannewitz et al, Network of Information (NetInf) is a "networking approach that provides access to named data objects (NDOs) as a first-order networking primitive". The main service is to forward requests to appropriate nodes and send requested objects back. Forwarding can be done using a hybrid combination of the routing on the object names (name-based routing) and with the help of name resolution services (NRS). NetInf employs a flat namespace for NDO names which means that there is no hierarchy in the names. Also, NetInf supports both on-path caching and off-path caching [7].

Dannewitz et al states that the protocol of NetInf must be implemented by all NetInf nodes and consists of 3 message types: GET, PUBLISH, SEARCH. The GET message requests an NDO from the NetInf network. A node responds to the GET message if it has an instance of the requested NDO. The PUBLISH message allows a node to push the name (for example, to an NRS) and, optionally, a copy of the object data and/or object metadata. The SEARCH message is used for discovering the names of NDOs that match query keywords [7].

Additionally, as noted by Dannewitz et al, NetInf supports both name resolution and name-based routing where at each step for a certain request, either name resolution or name-based routing can be employed. When responding to a GET request, any node can either return the requested object or a routing hint that helps to find the requested object. Routing hints can be lower-layer host identifiers (such as IP address of the next hop), some hints that are specific to the given protocol that can later be used to support name-based routing, or another NetInf name for indirection [7].

NetInf achieves lower-layer independence by using Convergence Layers (CLs). According to Dannewitz et al "CLs map the conceptual protocol to specific messages, transactions, or packet exchanges in the concrete protocol. A CL provides framing and message integrity for NetInf requests and responses for communication between two nodes as its main service. For example, NetInf-over-IP would require a CL that encapsulates, and potentially fragments and reassembles, NetInf message for transfer in IP packets and validates message integrity" [7].

An overview of NetInf architecture's network stack that includes CLs can be seen in the figure 3 below. It shows how CLs are placed in the network stack to transform a lower-layer data to be used by the NetInf protocol on the next layer.

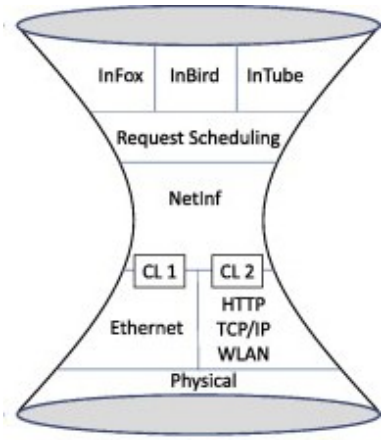

Figure 3: NetInf network stack [7]

2.4 Security and Privacy features

In this section, we provide definitions of the security and privacy features that are analyzed later, and how these features relate to the ICN paradigm. These features have been chosen because they are most widely used for analysis of the possible architectures of the future Internet, for example in Ambrosin et al [3].

Security

Availability means that "an authorized party should not be prevented from accessing objects to which he, she, or it has legitimate access" [15], i.e. the information should always be *available* to an authorized user. ICN architectures generally provide better availability than the current host-centric architecture, because the data itself is being addressed regardless of its location and if one host that serves this data is down, it can be easily served from another due to the pervasive use of in-network caching.

Access control means that the owner/author of the information object is able to control who or entities with which rights can access the published information object [16]. Access control in ICN appears to be simpler to implement because only the access to the data itself must be controlled and the connection to the host that serves this data.

Data integrity means that the data is accurate, relevant, timely, reputable, and complete [14]. Integrity can be achieved by making sure that the data is not tampered with or any alterations to the data can easily be detected by the consumer. Data integrity in information-centric networks is quite similar to host-centric networks - only the integrity of arrived packages must be validated.

Nonrepudiation means the provision of "an assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data" [22]. Nonrepudiation in ICN architectures is also simpler due to the data-centric nature - only packages' origin must be verifiable so that the participants would not be able to repudiate sending those packages.

Data authentication can be broken down to *data integrity* (see definition above) and *data origin authentication*, which means that the recipient can be sure that the data was not changed and it originated from the stated sender [10]. In ICN architectures, data authentication comes down to verifying that the data is intact and verifying that the received data originated from a valid producer. This can be achieved by supporting data integrity checks and supporting data origin verification by, for example, attaching a signature of the producer's private key.

Privacy

Anonymity prevents the association of the requests to the users that made them [9], so if two users send the same request, they should get the same response and there should be no way of distinguishing them. The data-centric nature of ICN architectures allows for better anonymity as the actual hosts are never addressed, only the requested data is.

Data confidentiality relates to "limiting the availability of information to unauthorized entities", essentially preventing information from falling into the hands of those the information provider would like to prevent accessing it [13]. Data confidentiality in ICN implies that access to the data is controlled and unauthorized parties cannot read this data. This can be achieved through access control (see definition above).

Unlinkability means that an attacker cannot sufficiently distinguish whether two or more messages or transactions are related or not [18]. Because of improved anonymity in ICN and data-centric nature, the requests and responses are harder to link together than in the host-centric architectures.

3 Security and Privacy Analysis of Overlay Architectures

This section provides an analysis of each of the chosen architectures to determine what security and privacy (S&P) features they implement.

3.1 Security

Availability

NDN NDN has strong support for availability. Due to the Forwarding Information Base, all interest packets sooner or later reach the node that has the requested data if the packet has a valid name for the data. Nodes on the path of the response can cache the data in the Content Store, thus allowing for even greater availability in case of big network latency or if the original producer is not available at the moment. Additionally, Denial of Service attacks such as Interest Flooding which hinder availability the most can be mitigated by monitoring the Pending Interest Table as explained in Tourani et al [21].

PURSUIT Given a valid content name - a pair of scope ID and rendezvous ID, Rendezvous Nodes, Forwarding Nodes, and Topology Manager always find a way to deliver the requested content if such a way exists. Therefore, availability is supported by the PURSUIT.

NetInf As explained earlier, NetInf allows for hybrid forwarding - supporting both Name Resolution Service and name-based routing. This allows for better flexibility for GET request forwarding. Also, NetInf can use both on-path and off-path caching, thus improving data availability even more. Given all that, NetInf has good support for availability.

Access Control

NDN As stated earlier and explained by Zhang et al, NDN supports name-based access control through encryption [24]. NDN employs a model similar to Simple Distributed Security Infrastructure (SDSI/SPKI) for managing keys. It uses hierarchical namespaces and predefined key name generation procedures so that both consumers and producers can easily reach the same name for the data that holds the key. Thus, it is easy to encrypt the data and provide the decryption keys only to the authorized consumers.

PURSUIT Data in the response packets can be encrypted, restricting access to the data to only those users who have the encryption key. Thus, PURSUIT supports access control.

NetInf Similar to NDN and PURSUIT, NetInf can employ symmetric encryption in order to provide access control for requested data.

Data Integrity

NDN NDN does not have explicit support for data integrity, however, it can be achieved by attaching a digest of the message to the message itself. This way upon receiving a message client can recompute its digest and compare it with the received digest. If they match, then the message has not been tampered with.

PURSUIT PURSUIT inherits Packet Level Authentication (PLA) with per-packet signatures from its predecessor PSIRP (http://www.psirp.org). In addition to other features, these signatures provide data integrity verification [12]. Hence, PURSUIT supports data integrity.

NetInf The CLs of NetInf provide message integrity and validate the integrity of all received messages before possibly assembling the whole message and sending it to the higher layer in the network stack. This is achieved by providing a SHA-256 hash in the application-specific metadata inside the NDO [7]. Therefore, NetInf supports message integrity.

Nonrepudiation

NDN As stated earlier, the Interest packets in NDN carry the signature constructed from the producer's private key. It can be found in the Data packet field called *publisher ID*. Thus, the producer cannot later repudiate that he/she produced this data.

PURSUIT Per packet signatures in PLA provided by PURSUIT allow for nonrepudiation on the network layer by using elliptic curve cryptography [12]. Hence, PURSUIT supports nonrepudiation.

NetInf NetInf does not have built-in support for nonrepudiation, but it can be achieved by attaching a signature of the producer's private key or providing a signature in a separate data packet. Similar to hash stored in the application-specific metadata inside the NDO, signature can also be provided in a similar manner.

Data authentication

NDN NDN supports both data integrity and data origin validations, therefore data authentication is supported. A signature of the producer's private key and digest of the produced data are enough to verify that the data was produced by the expected producer and has not been tampered with. Signature and publisher ID along with needed metadata such as digest algorithm are all provided in every Data packet [23]. Hence, NDN supports data authentication.

PURSUIT As stated by Lagutin et al, PURSUIT's per packet cryptographic signatures provide data authentication on the network layer using elliptic curve cryptography (ECC). ECC provides a good security with small key sizes which means that the key can easily be included in every packet [12]. Thus, data authentication is supported in PURSUIT.

NetInf NetInf has built-in support for data integrity, but it does not explicitly support the data origin authentication. It can support data origin authentication by attaching a signature of the producer's private key. Thus, NetInf does not have full support for data authentication, but it can if data origin authentication is supported.

3.2 Privacy

Anonymity

NDN Data packets carry only the name of the desired data and response packets carry only data and a signature of the producer's private key. Therefore, there is no information about who requests the data and who provides it (except for the producer's key which is needed for data origin authentication and nonrepudiation), and anonymity is supported. Additionally, there is no way to tell if received data was sent from the actual producer or it was a data copy that was cached previously.

PURSUIT PURSUIT architecture supports anonymity because the packets do not carry information (such as IP addresses) that could identify specific producers and consumers. Therefore, both producers and consumers are anonymous.

NetInf NetInf also supports anonymity since the packets do not carry any identifying information. NRS and name-based routing only point to the next node in the network and there is no way to tell if this node is a producer or not. Therefore, all participants stay anonymous. Also, since NetInf supports both on-path and off-path caching, there is no way to tell if received data was sent from the actual producer or it was a cached copy of the data. However, as explained in [11], the responders to SEARCH requests might not want to always send a response as this way they expose their cached contents which decreases anonymity.

Data Confidentiality

NDN Data confidentiality can be achieved through access control and anonymity. As stated earlier, NDN supports both these features, therefore it also supports data confidentiality.

PURSUIT PURSUIT supports data confidentiality since it can employ encryption to allow for access control to keep the published data confidential and supports anonymity to keep the data about the participants confidential.

NetInf Similar to NDN and PURSUIT, NetInf architecture supports both access control and anonymity, and therefore supports data confidentiality. However, it is worth mentioning that only the content is encrypted while the affiliated data is not. Therefore, it is concluded data confidentiality is only partially supported.

Unlinkability

NDN Since NDN supports anonymity and each Interest packet carries a random nonce, it is impossible to link the requests together. Therefore NDN supports unlinkability.

PURSUIT PURSUIT supports unlinkability because all participants are anonymous, so it is hard to link the requests together.

NetInf In the NetInf request forwarding process, only the next hop is identified at once, and it is impossible to know what was the previous hop and what hop will be after that. Additionally, all participants are anonymous. Therefore, it is impossible to link the requests together which means that NetInf supports unlinkability.

3.3 Results summary

Table 1 below summarizes and provides an overview of the results of the analysis of security and privacy features for NDN, PURSUIT, and NetInf.

S&P feature	NDN	PURSUIT	NetInf
Availability	+	+	+
Access Control	+	+	+
Data Integrity	+	+	+
Nonrepudiation	+	+	-
Data Authentication	+	+	+-
Anonymity	+	+	+
Data Confidentiality	+	+	+
Unlinkability	+	+	+

Table 1: Support of security and privacy features in different overlay ICN architectures (*"+" - supported, "-" - not supported, "+-" - partially supported*)

As can be concluded from table 1, only NDN and PURSUIT support all eight security and privacy features. Meanwhile, NetInf is lacking nonrepudiation and hence cannot also fully supports data authentication. In order for NetInf to support all eight features, it should implement data origin authentication and nonrepudiation. Both can be achieved if the content is augmented with the producer's private key.

The analysis shows that there is still work and research to be done in this area before new architecture can be deployed globally, however, the results are already quite promising. All three investigated architectures support the features that are inherent to ICN, such as availability and anonymity. NDN and PURSUIT have better support of S&P features than NetInf. Therefore, they are more secure as an overlay-based ICN/IP coexistence architecture.

4 Responsible Research

This section provides an overview of the methodology that has been used in order to achieve the presented results. A clear description of the methodology allows for better reproducibility as when attempted to reproduce, one would know which literature databases, which search engines, and which keywords were used. Additionally, this section reflects on the ethical aspects of the research.

4.1 Methodology

The main methodology employed in this research is the in-depth analysis of the relevant literature. The literature was found on such databases as *Elsevier*, *ScienceDirect*, *IEEE Xplore*, *ACM Digital Library*, and *ResearchGate*. Search engines that were used are *Google Scholar* and *Google Search*. The papers were picked by the relevance to the topic - if the abstract of the paper presents relevant information then the paper was read further, otherwise, the search continued. Some additional literature was taken from the list of publications of the websites of the projects that developed PURSUIT and NDN. The websites are *https://cordis.europa.eu/project/id/257217* for PURSUIT and *https://named-data.net* for NDN (accessed both on 07.06.2021).

The following keywords and their combinations were used during the search: *ICN, overlay-based ICN, ICN over IP, Named Data Networking, NDN, Publish-Subscribe Internet Technology, PURSUIT, PSIRP, Network of Information, NetInf, security, privacy, overlay NDN, overlay PURSUIT, overlay NetInf, NDN over IP, PURSUIT over IP, NetInf over IP, security of NDN, security of PURSUIT, security of NetInf.*

4.2 Ethical aspects

Developing, researching, and deploying a new Internet architecture has many implications and effects on everyone. While we are still in the research and development stage, we should make sure to pay as much attention as possible to privacy and security aspects and what effect it will have on the users. Every decision and solution has its pros and cons and it is crucial to critically weigh and assess all the advantages and disadvantages. Take for example anonymity. Anonymity is good for users, it facilitates user's privacy and freedom of speech. However, in the current, less anonymous Internet, law enforcement uses IP addresses to track and catch criminals. On the anonymous Internet, evildoers will also be anonymous, which makes it harder to find them.

5 Discussion

This section discusses and compares the results of this research.

All three architectures - NDN, PURSUIT, NetInf - have a common idea of making the data a centerpiece of the system instead of the hosts where the data is located. However, they all reach this in different ways. NDN uses Interest packets that are circulated in the network until they are satisfied either by a cached copy of the content or by the provider of the content and a response with a Data packet is sent following the reverse path of the Interest. PURSUIT employs a publish/subscribe ideology. Producer publishes his/her content to the network by sending the PUBLISH message. When a user wants to receive this content, the GET message is sent to the network, Topology Manager creates a route from producer to consumer, and requested data sent through this route. NetInf uses Convergence Layers to augment the network stack to allow communication between NetInf protocol and other protocols such as TCP/IP. At each hop in the network, either name-based resolution or a separate name resolution service can be employed to find the next hop that leads towards the requested data. An interesting feature that only NetInf has but NDN and PURSUIT don't is the search feature. It works like a small search engine to find the names of data based on certain keywords, but these keywords are also like a kind of identifier of the data and can disclose what exact data is there. Therefore, data providers should be careful not to disclose sensitive information. As can be seen, the architectures differ a lot, but the idea of focusing on the data instead of hosts remains the same.

All investigated architectures implement the features that are inherent to all ICN architectures like anonymity and availability. However, our focus is on the security and privacy (S&P) features. Both NDN and PURSUIT support all eight S&P features we analysed, while NetInf is missing nonrepudiation and full data authentication. This can be seen as a

point for improvement and future work. The support of these missing features can be achieved by, for example, attaching a producer's signature to the requested data or by allowing to retrieve this signature separately as other architectures do this. In any case, this is something that should be kept in mind and addressed in order to make it more secure and reliable as this might be the architecture of the future Internet.

6 Conclusions

This research aimed to answer the question of what security and privacy (S&P) features are supported by overlay-based ICN/IP coexistence architectures. The three most popular overlay architectures were chosen for this - NDN, PURSUIT, and NetInf. These architectures were analysed to find whether or not they support availability, access control, data integrity, nonrepudiation, data authentication, anonymity, data confidentiality, and unlinkability. The analysis was carried out by the means of a deep review of the relevant literature on the topic. We have reached the conclusion that NDN and PURSUIT support all these eight S&P features, while NetInf is missing the support for nonrepudiation and has only partial support for data authentication. Nevertheless, NetInf has the ability to support the missing features if the data is signed by its producer and is made verifiable for data consumers.

This shows that these architectures have good support for security and privacy and in the modern Internet security and privacy are one of the most crucial aspects. However, there is still some work to be done and there are still points for improvement before these architectures can be used for the Internet of the future.

References

[1] A. Afanasyev, J. Burke, T. Refaei, L. Wang, B. Zhang, and L. Zhang. A brief introduction to named data networking. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pages 1–6, 2018.

[2] Bengt Ahlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, and Börje Ohlman. A survey of information-centric networking. *IEEE Communications Magazine - IEEE Commun. Mag.*, 50:26–36, 07 2012.

[3] Moreno Ambrosin, Alberto Compagno, Mauro Conti, Cesar Ghali, and Gene Tsudik. Security and privacy analysis of nsf future internet architectures. 10 2016.

[4] Dyon Buitenkamp and Raj Jain. *A Survey of Information-Centric Networking Approaches*. 2019.

[5] Tomaso Cola, Daniele Tarchi, and Alessandro Vanelli-Coralli. Future trends in broadband satellite communications: Information centric networks and enabling technologies. *International Journal of Satellite Communications and Networking*, 33, 03 2015.

[6] Mauro Conti, Ankit Gangwal, Muhammad Hassan, Chhagan Lal, and Eleonora Losiouk. The road ahead for networking: A survey on icn-ip coexistence solutions. *IEEE Communications Surveys Tutorials*, PP, 04 2020.

[7] Christian Dannewitz, Dirk Kutscher, Börje Ohlman, Stephen Farrell, Bengt Ahlgren, and Holger Karl. Network of information (netinf) – an information-centric networking architecture. *Computer Communications*, 36:721–735, 04 2013.

[8] Nikos Fotiou, Pekka Nikander, Dirk Trossen, and George C. Polyzos. Developing information networking further: From psirp to pursuit. In Ioannis Tomkos, Christos J. Bouras, Georgios Ellinas, Panagiotis Demestichas, and Prasun Sinha, editors, *Broadband Communications, Networks, and Systems*, pages 1–13, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[9] Manish J. Gajjar. Chapter 9 - sensor security and location privacy. In Manish J. Gajjar, editor, *Mobile Sensors and Context-Aware Computing*, pages 223–265. Morgan Kaufmann, 2017.

[10] Vijay K. Garg. Chapter 13 - security in wireless systems. In Vijay K. Garg, editor, *Wireless Communications Networking*, The Morgan Kaufmann Series in Networking, pages 397–433. Morgan Kaufmann, Burlington, 2007.

[11] D. Kutcher, NEC, S. Farrell, and E. Davies. *The NetInf Protocol*. 2013.

[12] Dmitrij Lagutin, Kari Visala, and Sasu Tarkoma. *Publish/Subscribe for Internet: PSIRP Perspective*. IOS Press, 2010.

[13] Claire Laybats and Luke Tredinnick. Information security. *Business Information Review*, 33:76–80, 06 2016.

[14] Yang Lee, Leo Pipino, Diane Strong, and Richard Wang. Process-embedded data integrity. *J. Database Manag.*, 15:87–103, 01 2004.

[15] Suhail Mir and Syed Quadri. Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, 07:185–194, 01 2016.

[16] Tawfik Mudarri, Samer Al-Rabeei, and Samer Abdo. Security fundamentals: Access control models. *Interdisciplinarity in theory and practice*, 08 2015.

[17] Arthi Padmanabhan, Lan Wang, and Lixia Zhang. Automated tunneling over ip land: Run ndn anywhere. In *Proceedings of the 5th ACM Conference on Information-Centric Networking*, ICN '18, page 188–189, New York, NY, USA, 2018. Association for Computing Machinery.

[18] Andreas Pfitzmann and Marit Hansen. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management–a consolidated proposal for terminology. *Version v0*, 31, 01 2007.

[19] Akbar Rahman, Dirk Trossen, Dirk Kutscher, and Ravi Ravindran. Deployment Considerations for Information-Centric Networking (ICN). RFC 8763, April 2020.

[20] Eduardo Rosa and Flávio Silva. Enabling native coexistence between icn and tcp/ip architectures over the same domain. pages 13–19, 12 2020.

[21] R. Tourani, S. Misra, T. Mick, and G. Panwar. Security, privacy, and access control in information-centric networking: A survey. *IEEE Communications Surveys Tutorials*, 20(1):566–600, 2018.

[22] Evan Wheeler. Chapter 7 - security controls and services. In Evan Wheeler, editor, *Security Risk Management*, pages 127–146. Syngress, Boston, 2011.

[23] Lixia Zhang, Deborah Estrin, Jeffrey Burke, Van Jacobson, James D. Thornton, Diana K. Smetters, Beichuan Zhang, Gene Tsudik, kc claffy, and Dan et al. Massey. *Named Data Networking (NDN) Project*. 2010.

[24] Zhiyi Zhang, Yingdi Yu, Haitao Zhang, Eric Newberry, Spyridon Mastorakis, Yanbiao Li, Alexander Afanasyev, and Lixia Zhang. An overview of security support in named data networking. *IEEE Communications Magazine*, 56(11):62–68, 2018.