

SECURITY OF SELECTED FUTURE INTERNET ARCHITECTURES: A SURVEY

Rahamatullah Khondoker¹, Beny Nugraha², Ronald Marx¹, and Kpatcha Bayarou¹

¹Fraunhofer SIT, Rheinstr. 75, Darmstadt, Germany

²Department of Electrical Engineering, Mercu Buana University, Jakarta, Indonesia

ABSTRACT

The Internet faces many challenges in terms of flexibility (so called IP bottleneck) as well as host-centric addressing, mobility, self-configuration, self-monitoring, and security. Several Future Internet (FI) architectures have been proposed to address these challenges including eXpressive Internet Architecture (XIA), MobilityFirst, Named Data Networking (NDN), NEBULA, and Recursive InterNetwork Architecture (RINA). This paper surveys the security solutions of the FI architectures based on literatures, prototypes, and demonstrations. It has been found that none of the architectures can fulfill all of the security goals: confidentiality, authentication, integrity and availability. The results of the survey have been verified by the domain experts.

Index Terms— Future Internet (FI), Architecture, Security Analysis, Survey, XIA, RINA, NENA, SONATE, MobilityFirst, NDN, SONATE

1. INTRODUCTION

The Internet has many problems including host-based addressing (addressing a host rather than a content), static protocol stack, and security. Researchers choose one of the two design methods for developing a FI Architecture: “clean slate” or “evolutionary”. Whereas in the clean slate approach, the architecture is designed from the scratch, new design components are added to the existing architecture in the evolutionary approach.

This paper analyzes security of seven future network architectures, namely, eXpressive Internet Architecture (XIA) [1], Recursive InterNetwork Architecture (RINA) [2], Service Oriented Network Architecture (SONATE) [3], Netlet-based Node Architecture (NENA) [4], MobilityFirst [5], NEBULA [6], and Named Data Networking (NDN) [7]. We selected them as they are mature, and there exist either a demonstration or a prototype or both. Two of them, namely NENA and SONATE, are clean-slate. The rest five of them, namely XIA, RINA, MobilityFirst, NDN, and NEBULA, are evolutionary. To deploy an architecture in the Internet, it is a pre-requisite to know whether they fulfill the security requirements. In this paper, we consider the following security goals: confidentiality, integrity, availability, and authentication (defined in Section 2.1). The methodology of the research were 1, to specify the threats against each of the goal (discussed in Section 2.2) 2, to analyze each of the architectures based on it's

literatures, prototype, and demonstration to gather the available security mechanisms (described in Section 2.5) and 3, to decide on which of the threats can be overcome by which of the security mechanisms (depicted in Section 2.5).

The outline of the rest of paper is as follows: the result of the survey is presented and compared in Section 3 with a follow up conclusion in Section 4.

2. METHODOLOGY FOR THE SURVEY

The security of a system can be analyzed in one of the two ways: attack-centric and system-centric [8]. Whereas in the first way the attacks on a system (i.e., attack trees) are modeled, the system itself (i.e., STRIDE methodology) is modeled in the other way. Our approach is a combination of attack-centric and system-centric approach as it analyzes both the architectures and the attacks. Moreover, the combined approach provides a better view of the architectures vulnerability to attacks than to follow one of the methodologies. The combined methodology works as follows:

1. Defining the network security goals.
2. Specifying attacks that inhibit the network security goals and then analyzing the counter mechanisms for each attack (attack-centric).
3. Selection of future network architectures.
4. Analyzing the security solutions of each of the architectures (system-centric).
5. Matching the counter mechanisms for each attack and the security mechanisms of the future network architectures

The details of each item will be discussed as follows:

2.1. Defining Security Goals

The general goal of network security is to give people freedom to enjoy computer networks without fear of compromising their rights and interests [9].

To achieve the general goal, four specialized goals of network security have been identified as follows:

Confidentiality The message that is sent by the sender has to be intended for the receiver only, for the others, this message must be worthless.

Integrity The received message must be the same as the original message.

Availability The services that are accessible by the Internet (i.e., web services, remote machines, networks, etc.) must be available all the time for its authorized users.

Authentication Only the authorized user is able to send a message and the receiver is able to proof the sender's identity.

2.2. Specifying Threats Against Achieving The Goal

As following, several threats have been identified which work against achieving the goal.

2.2.1. Threats Against Confidentiality

Snooping and traffic analysis attacks are two of the possible threats against confidentiality. In snooping, the aim of the attacker is to get the database of an authorized user or the packets flowing in a network. Examples of this attack are: 1, using ping-type programs (ICMP ping, TCP ping) to identify active hosts on the network and to further locate potential targets and, 2, using TCP/UDP port scanning for detecting the target operating system [10]. Snooping attack can be prevented by having a data encryption mechanism to protect the packets.

In traffic analysis, the attacker intercepts and examines messages in order to extract information from the traffic patterns in a communication. The greater the number of packets that can be observed, the more the information that can be inferred from the traffic. A security mechanism to prevent this attack is to have a mechanism to conceal the identity of the users, therefore, an attacker cannot determine where he should watch for the traffic.

2.2.2. Threats Against Integrity

Two threats against integrity are modification and repudiation attacks.

Modification attack involves deletion, insertion, or alteration of information in an unauthorized manner that is intended to appear genuine to the user [11]. The counter mechanisms for this attack are to hash the message or to have a digital signature, therefore, the receiver can check the correctness of the message.

Repudiation is a process in which the sender or the receiver cannot prove that a transaction has taken place between them, either one or both of them can deny that they are sending or receiving the data [11]. Repudiation attack can be prevented by having a digital signature in collaboration with a trusted third party to create a non-repudiation message.

2.2.3. Threats Against Availability

Denial of Service (DoS) attack is a threat against availability. This attack can deny access to information, applications, systems or communications. An example of DoS attack is to flood the traffic with bursts of packets [12]. DoS can be prevented by having a flow control or bandwidth allocation mechanism. Therefore, only the authorized packets that can flow in the traffic.

2.2.4. Threats Against Authentication

The attacks that are threats against authentication are: man-in-the-middle, reflection, masquerading, and replaying attack.

Staying in between the sender and the receiver, the attacker observes or modifies the traffic in the man-in-the-middle attack [13]. Man-in-the-middle attack can be mitigated by having a digital signature to authorize the real users.

The objective of the reflection attack is to pretend that the attacker is an authorized user by sending the response from the real authorized user to the target [14]. Reflection attack can also be mitigated by having a digital signature.

In masquerading, the attacker pretends to be an authorized user of a system in order to gain access to it [15]. Masquerading attack can be prevented by having an anonymous connection or a user authentication process.

Replaying attack occurs when an information is captured and then replayed later (in different session) in order, for example, to gain the trust of others [16]. Replaying attack can be prevented by having a marker (i.e., session key or random number) to bind one communication session. Therefore, the messages in one session are different than the messages in another session.

To conclude, there are nine attacks to be reviewed in this paper. Some attacks are present in today's Internet because the today's Internet is an address-based architecture. For example, an attacker can initiate a masquerading attack because he can obtain the IP address of his target. The future network architectures should be able to mitigate this type of attack intrinsically, which means the future network architectures should not be an address-based architecture. An example of another approach is a content-centric architecture, which is considered as a Future Internet by the Future Content Networks (FCN) Group [17].

2.3. Selection of FI Architectures

The selection of future network architectures is done by considering the maturity of the architecture, the availability of the demonstration, and the prototype as shown in Figure 1. We selected seven architectures to review, namely eXpressive Internet Architecture (XIA), Recursive Inter-Network Architecture (RINA), Service Oriented Network Architecture (SONATE), Netlet-based Node Architecture (NENA), MobilityFirst, NEBULA, and Named Data Networking (NDN) as they are mature (i.e., the projects started

Criteria	Future Internet Architectures						
	XIA	RINA	SONATE	NENA	MobilityFirst	NEBULA	NDN
Approach	Content-Centric	Content-Centric	Protocol Graph	Protocol Graph	Content-Centric	Supports Cloud Computing	Content-Centric
Project Started	In 2010	In 2010	In 2009	In 2009	In 2010	In 2010	In 2010
Demo	✓	✓	✓	✓	✓	✓	X
Prototype	✓	✓	✓	✓	✓	X	✓

Legend:
✓: Available
X: Not Available

Figure 1. FI Architectural approaches

in 2009 or 2010), they have either a prototype or a demonstration or both.

2.4. Asking and Receiving Expert’s Feedback

After surveying the literature, we got the result described in the following section 2.5. The result of each architecture has been sent to the pioneers of the architecture for review such as we asked the feedback for the XIA architecture only from the XIA inventors. Fortunately, we received feedback for all of the seven architectures.

2.5. Analyze The Security Solutions Of Every Architecture

At first the security of two clean slate approaches is analyzed: SONATE and NENA. The aim of both of these approaches is to use a customized protocol graph (similar to a TCP/IP or UDP/IP network stack) based on the requirements from the application. However, they differ in terms of “when” the composition is accomplished? Whereas in SONATE, the composition is done during runtime of communication association, the composition in NENA is accomplished during the design time of creating new protocols.

2.5.1. SONATE

In SONATE, the services provided by building blocks (the implementation of a protocol or a mechanism like CRC, retransmission etc.) are selected and composed by a composition algorithm to create a protocol graph during runtime based on the requirements from the application, constraints from the administrator, and networks [3].

The security mechanisms in SONATE [18] are:

1. SONATE is able to select building blocks that
 - (a) enable data encryption (i.e., data encryption micro protocol) [18],
 - (b) provide data authentication (i.e., digital signature, MAC) [18][19], and
 - (c) provide flow control service [19].
2. Each communication session is bound by one protocol graph [18].

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	Data Encryption BB
	Traffic Analysis	NONE: SONATE does not provide anonymous communication
Integrity	Modification	Digital Signature BB
	Repudiation	NONE: SONATE does not have a trusted third party to provide non-repudiation message
Availability	Denial of Service	Flow Control BB
Authentication	Man-In-The-Middle	Digital Signature BB
	Reflection Attack	Digital Signature BB
	Masquerading	NONE: SONATE does not provide anonymous communication
	Replaying	One Protocol Graph Per-Session

Figure 2. Handling attacks in SONATE

SONATE is not able to mitigate the traffic analysis attack and the masquerading attack since SONATE does not provide anonymous communication and an attacker only needs to know the port and the address of the target to initiate both attacks. SONATE also cannot mitigate the repudiation attack because it does not have a trusted third party to prove a communication between two users has been finished, thus, cannot create a non-repudiation message.

The advantage of SONATE is that it is able to mitigate the other attacks by selecting an appropriate BB to counter the attacks. Example of BB that can be used for counter the threats are data encryption (to prevent the snooping attack), digital signature (to mitigate the modification, man-in-the-middle, and reflection attacks), and flow control (to counter DoS attack).

2.5.2. NENA

In NENA [4], the services provided by building blocks (the implementation of a protocol or a mechanism like CRC, Retransmission etc.) are selected and composed by a composition algorithm to create a protocol graph (called netlet) during design time (by a developer or assisted by a software) assuming the requirements from an application, constraints from the administrator and networks. However, the selection of the most appropriate netlet is accomplished during runtime.

The security mechanisms of NENA are:

1. NENA uses secure deployment of protocols. Each protocol has a unique protocol ID [20].
2. NENA has a collaborative attack detection mechanism [21].
3. Similar to SONATE, NENA is able to select a protocol that offers
 - (a) data encryption (i.e., data encryption BB) [4].
 - (b) data authentication (i.e., digital signature, MAC) [4].

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	Data Encryption Netlet
	Traffic Analysis	NONE: NENA does not provide anonymous communication
Integrity	Modification	Digital Signature Netlet and Protocol Signing
	Repudiation	NONE: NENA does not have a trusted third party
Availability	Denial of Service	Collaborative Attack Detection
Authentication	Man-In-The-Middle	Digital Signature Netlet
	Reflection Attack	Digital Signature Netlet
	Masquerading	NONE: NENA does not provide anonymous communication
	Replaying	Timestamp Netlet

Figure 3. Handling attacks in NENA

NENA is not able to prevent the traffic analysis and masquerading attacks since NENA does not provide anonymous connection and an attacker only need to know the port and the address of the target to pretend to be the target. Furthermore, NENA cannot prevent the repudiation attack since it does not have a trusted third party server.

NENA is able to prevent the other attacks by using the secure deployments of protocols, collaborative attack detection, or by selecting an appropriate netlet to counter the attacks. Examples of netlets that can be used for counter the attacks are data encryption and digital signature netlets. Meanwhile, in order to mitigate denial-of-service attack, NENA utilizes the service of collaborative attack detection.

2.5.3. XIA

Whereas in the Internet, an IP address is used to address both the host and the content, XIA uses three principle types of identifiers to retrieve the content: Content ID, Host ID, and Service ID [1]. The content ID, the hash of the content, is used to retrieve the content without needing to know its location. The host ID, the hash of the host's public key, is used to contact the host that provides the content. The service ID, the hash of the service's public key, is used to get the service that provides the content.

The security mechanisms in XIA are:

1. The architecture uses Content / Host / Service ID (CID / HID / SID) to retrieve the content. CID is the hash of the content, HID is the hash of the Public Key of the Host, and SID is the hash of the Public Key of the service [1].
2. The LAP (Lightweight Anonymity and Privacy) defense mechanism enables anonymous communication to prevent remote tracking [22].
3. The STRIDE defense mechanism allocates the available bandwidth in a tree-based topology [23].
4. The AKI (Accountable Key Infrastructure) defense mechanism provides data authentication process [24].

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	Public key of the service (used in SID) can also be used for encryption mechanism
	Traffic Analysis	LAP mechanism
Integrity	Modification	Hashed Principals (CID/HID/SID)
	Repudiation	Hashed Principals (CID/HID/SID) and AKI mechanism
Availability	Denial of Service	STRIDE mechanism
Authentication	Man-In-The-Middle	AKI mechanism
	Reflection Attack	AKI mechanism
	Masquerading	LAP and AKI mechanisms
	Replaying	NONE: XIA does not have any mechanisms to bind one communication session

Figure 4. Handling attacks in XIA

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	SDU Protection Module (Data encryption)
	Traffic Analysis	SDU Protection Module and Member authentication process
Integrity	Modification	SDU Protection Module (Hash function)
	Repudiation	NONE: RINA does not have a trusted third party
Availability	Denial of Service	NONE: The attack from inside cannot be mitigated
Authentication	Man-In-The-Middle	Member authentication process
	Reflection Attack	Member authentication process
	Masquerading	Member authentication process
	Replaying	Unique CEP-Id in every session

Figure 5. Handling attacks in RINA

XIA is able to mitigate all of the reviewed attacks except the replaying attack, because XIA does not have any mechanism to bind one communication session.

For snooping attack, XIA mitigates them by using the public key and private key of a service (SID) to do encryption mechanism. For the other attacks, XIA mitigates them by using a hashed ID (CID/HID/SID) or by using the defense mechanisms provided by SCION architecture (LAP, AKI, or STRIDE defense mechanisms).

2.5.4. RINA

The basic design principle of RINA is that "Networking is only Inter-Process Communication (IPC)" [2][25]. IPC is a function to allow two communication processes (one in the sender and another in the receiver side) to communicate with each other. Examples of IPC function are: locating processes, determining permissions, passing information, scheduling, and managing memory. Process names are used as identifiers. For example, a source application process requests a service using the process name of the destination application. They communicate with each other by utilizing the services of the Distributed IPC Facility (DIF).

The security mechanisms in RINA are:

1. All members in the same DIF must be authenticated first before they can join in [26].
2. If the attacker is inside the DIF, he still needs to scan all of the possible Connection End Point id (CEP-id)

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	GUID can be used to encrypt the data
	Traffic Analysis	NONE: MobilityFirst cannot provide anonymous communication
Integrity	Modification	Hashed GUID
	Repudiation	Has PKI to provide non-repudiation message
Availability	Denial of Service	Routing update by GNRS
Authentication	Man-In-The-Middle	Self-certifying public key
	Reflection Attack	Self-certifying public key
	Masquerading	Self-certifying public key and every content has a unique GUID
	Replaying	NONE: MobilityFirst does not have any mechanisms to bind one communication session

Figure 6. Handling attacks in MobilityFirst

of the target, and the probability is 2^{16} (given that the CEP-id is 16-bit) [26].

3. RINA has a SDU protection module that is able to provide functions such as: encryption function, compression function, and error detection function [27].
4. The CEP-ids in RINA are used to distinguish between the new and the old data connection [26].

RINA is able to mitigate all of the reviewed attacks except the denial-of-service and repudiation attacks. The research to prevent denial-of-service attack from the inside is ongoing. Meanwhile, RINA does not have a trusted third party to prevent the repudiation attack.

For the other attacks, RINA mitigates them by utilizing the function of the SDU Protection Module, the authentication process by IPC Management, and a unique CEP-Id that is assigned to each user. The CEP-Id can also be used to distinguish the old and new communications. The CEP-Id can mitigate the replaying attack by distinguishing the messages from a new session and the messages from an old session.

2.5.5. MobilityFirst

In this approach, the end-user can request for a service using the Human-Readable Name (HRN) like Movie:LionKing. The naming architecture of the MobilityFirst has three identifiers: Network Address (NA), Globally Unique Identifier (GUID), and HRN [5]. It ensures mobility by separating network location information so called NA from its identity so called GUID. As with XIA, GUID is the hash of the content itself. MobilityFirst has two mapping services: Name Assignment Services (NAS) and Global Name Resolution Service (GNRS). The NAS binds a HRN with GUID and the GNRS maps GUID to NA. GNRS functions as a content location directory as it dynamically bind the name and the location. When the content is available in more than one location, GNRS chooses the content for the requester from the nearest location.

The security mechanisms in MobilityFirst are:

1. To retrieve the content, MobilityFirst uses Globally Unique Identifier (GUID) which is assigned to each

content as an address [5]. GUID is a result of hashing the content and can be used as a public key for encryption mechanism.

2. MobilityFirst enables frequent routing update using the function of GNRS [28].
3. MobilityFirst uses an integrated protocol that enables self-certifying public key names [29].

MobilityFirst is robust against the snooping attack because it has a mechanism to encrypt the packets by using the name or GUID of the content as the identifier. For the modification attack, MobilityFirst mitigates it by assigning a unique GUID to each content. GUID is a hash of a content, therefore, the receiver can check the correctness of the content. For the man-in-the-middle, reflection, and masquerading attacks, MobilityFirst mitigates them by using a protocol that is able to authenticate a user and having a unique GUID for every content. For the DoS attack, MobilityFirst prevents it by utilizing the function of GNRS to enable routing update. For the repudiation attack, MobilityFirst mitigates it by having a non-repudiation message, created by the PKI.

However, MobilityFirst cannot mitigate the traffic analysis and replaying attacks due to the following reasons:

1. MobilityFirst cannot mitigate the traffic analysis attack because it does not have a mechanism to enable anonymous communication.
2. The replaying attack is possible to do in MobilityFirst since it does not have a mechanism to bind the messages with the sessions.

2.5.6. NDN

NDN [7] defines two types of packets: one is for request (called interest packet) and another is for reply (data packet). The interest packet has mainly two fields: content name and nonce. The content name identifies the data to be retrieved and the nonce (number once) binds each communication session. The data packet carries both the name and the content of the data, together with the digital signature and signed information.

The security mechanisms in NDN [30] are:

1. An end-to-end encryption can be used in NDN. This is used to encrypt the NDN data.
2. Data packets are signed using the digital signature.
3. The clients in NDN send nonce (Number Once) within the interest packets.

NDN is vulnerable to the traffic analysis attack even though NDN is a content-centric network. Being content-centric is not enough to prevent that attack, it needs a mechanism such as a mechanism to conceal the packet, and this mechanism is not provided by NDN. The research for a method to mitigate

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	End-to-end data encryption
	Traffic Analysis	NONE: NDN does not provide anonymous communication
Integrity	Modification	Digital signature
	Repudiation	Digital signature and PKI
Availability	Denial of Service	NONE: The research of method to mitigate DoS is still ongoing
Authentication	Man-In-The-Middle	Digital signature
	Reflection Attack	Digital signature
	Masquerading	Digital signature and every content has a unique ID
	Replaying	Random number

Figure 7. Handling attacks in NDN

the DoS attack is ongoing, therefore, NDN is vulnerable to the DoS attack.

NDN is able to mitigate the replaying attack since it has a nonce in its interest packet. This nonce will distinguish the old and the new interest packet. For the modification, repudiation, man-in-the-middle, and reflection attacks, NDN prevents them by using a digital signature. For the masquerading attack, NDN prevents it by having a digital signature and unique name for every content.

2.5.7. NEBULA

NEBULA [6] facilitates data centers in a cloud environment to communicate in a reliable way. NEBULA consists of three components: NEBULA Core (NCore), NEBULA Data Plane (NDP), and NEBULA Virtual and Extensible Networking Techniques (NEVENT). NCore interconnects the data centers using a reliable routing mechanism. NDP is a data plane that provides flexible access control and security mechanisms. NEVENT, a control plane, is responsible for determining paths for the packets to arrive at the destination.

The security mechanisms in NEBULA [31] are:

1. Proof of Consent (PoC) mechanism to authorize a packet and a path.
2. Proof of Path (PoP) in order to make sure that the packet only flows on the authorized path.
3. NEBULA uses token to bind one authorized communication session.
4. There is a consent server in NEBULA that can act as a trusted third party. This server will prove that the communication between two users really took place because the users who want to send a packet will contact it to obtain the PoC.

NEBULA was not designed to mitigate the snooping and traffic analysis attacks. To mitigate these attacks, mechanisms such as end-to-end encryption or onion routing needs to be applied on top of NEBULA. NEBULA also cannot prevent the masquerading attack because the attacker can pretend to be the authorized user by getting the users address.

Security Goals	Security Attacks	Attack Mitigation Mechanisms
Confidentiality	Snooping	NONE: Does not provide encryption mechanism
	Traffic Analysis	NONE: Does not provide anonymous communication
Integrity	Modification	Proof of Consent: to authorize the packets and
	Repudiation	Proof of Path: to ensure the packets flow on the authorized path There is a consent server as a trusted third party
Availability	Denial of Service	Proof of Path: there is no unauthorized packets in a path
Authentication	Man-In-The-Middle	Proof of Consent: to authenticate the sender and the receiver of the packets
	Reflection Attack	Proof of Consent
	Masquerading	NONE: Does not provide anonymous communication
	Replaying	Token is used to bind one communication session

Figure 8. Handling attacks in NEBULA

Security Goals	Security Attacks	SONATE	NENA	XIA	RINA	MobilityFirst	NDN	NEBULA
Confidentiality	Snooping	✓	✓	✓	✓	✓	✓	X
	Traffic Analysis	X	X	✓	✓	X	X	X
Integrity	Modification	✓	✓	✓	✓	✓	✓	✓
	Repudiation	X	X	✓	X	✓	✓	✓
Availability	Denial of Service	✓	✓	✓	X	✓	X	✓
Authentication	Man-In-The-Middle	✓	✓	✓	✓	✓	✓	✓
	Reflection	✓	✓	✓	✓	✓	✓	✓
	Masquerading	X	X	✓	✓	✓	✓	X
	Replaying	✓	✓	X	✓	X	✓	✓

Legend:
✓: Has (by design) mitigation mechanism(s)
X: Has (by design) no mitigation mechanism(s)

Figure 9. Comparison of all architectures in terms of handling attacks

NEBULA is able to mitigate the other attacks by using the function of a PoC and a PoP that reside in the NDP. Moreover, NEBULA is able to prevent repudiation attack because it has a consent server as a trusted third party to create a non-repudiation message.

3. SURVEY RESULTS

The result of the comparison of all architectures is shown in Figure 9. It is seen that SONATE and NENA cannot mitigate the same attacks which are the traffic analysis, masquerading, and repudiation attacks. They cannot mitigate the traffic analysis attack because they do not have any mechanism to enable anonymous communication. SONATE and NENA cannot prevent the masquerading attack since they do not provide anonymous communication and the attacker can get the IP address of the communicating hosts to pretend to be the authorized users. Meanwhile, they cannot prevent the repudiation attack because they do not have a trusted third party.

In summary, none of the studied architectures, whether it is clean slate or evolutionary, can mitigate all of the studied attacks. However, it can be seen in Figure 9 that XIA is able to handle eight out of nine reviewed attacks. Moreover, XIA is Content-Centric Network (CCN). CCN is claimed by the Future Content Networks (FCN) Group as the Future Internet (FI) [17]. At last, since XIA has a demonstration and a prototype available, XIA can be considered as the most promising architecture to be deployed into the market.

4. CONCLUSION AND FUTURE WORK

This paper analyzes security of seven future network architectures. The goal was to ascertain which of those architectures can fulfill the security goals: confidentiality, integrity, availability, and authentication. The methodology of the research were 1, to specify the threats against each of the goal and then identify the counter mechanisms for each threat 2, to analyze each of the architectures based on it's literatures, prototypes, and demonstration to gather the available security mechanisms 3, to decide on which threat can be overcome by which security mechanism.

We found that none of the architectures has mechanisms to tackle all of the threats, resulting in unfulfillment of the security goals.

The subsequent work will be to reuse existing mechanisms or develop new algorithms / protocols for the fulfillment of the security goals of the studied future network architectures.

5. STANDARDIZATION CANDIDATE

The ITU-T Study Group 13 (SG 13) [32] is responsible for standardizing future networks. The SG 13 consists of several Focus Groups (FGs) including Cloud Computing (FG Cloud), Future Networks (FG FN), and Smart Grid (FG Smart). The main aim of the Focus Group Future Networks (FG FN) [33] is to collect FI architectures and technologies to be standardized. This security analysis can be an input for them to decide on which of the studied architectures can be standardized and which attacks must be mitigated before standardization.

6. ACKNOWLEDGEMENTS

We would like to acknowledge domain experts for providing feedback about the result of the survey. They are: Ken Birman and Andreas Haeberlen (NEBULA), Lixia Zhang and Xingyu Ma (NDN), Wade Trappe and Dipankar Raychaudhuri (MobilityFirst), Peter Steenkiste (XIA), Denis Martin and Helge Backhaus and Hans Wippel (NENA), Abbas Siddiqui (SONATE), and John Day (RINA).

7. REFERENCES

- [1] Ashok Anand, Fahad Dogar, Dongsu Han, Boyan Li, Hyeontaek Lim, Michel Machado, Wenfei Wu, Aditya Akella, David Andersen, John Byers, Srinivasan Seshan, and Peter Steenkiste, "XIA: An Architecture for an Evolvable and Trustworthy Internet," in *Proceedings of the tenth ACM Workshop on Hot Topics in Networks (HotNets-X)*. 2011, pp. 1–32. Article No. 2, ACM.
- [2] John Day, Ibrahim Matta, and Karim Mattar, "Networking is IPC: A Guiding Principle to a Better Internet," in *Proceedings of the 2008 ACM CoNEXT Conference*. 2008, pp. 1–6. Article Number 67, ACM.
- [3] Bernd Reuther and Paul Müller, "Future Internet Architecture - A Service Oriented Approach," in *In it - Information Technology, Volume 50, Number 6*, 2008, pp. 1–7.
- [4] Denis Martin, Lars Völker, and Martina Zitterbart, "A flexible framework for Future Internet design, assessment, and operation," *Journal Computer Networks: The International Journal of Computer and Telecommunications Networking*, pp. 910–918. Volume 55 Issue 4, March 2011.
- [5] Ivan Seskar, Kiran Nagaraja, Sam Nelson, and Dipankar Raychaudhuri, "MobilityFirst Future Internet Architecture Project," in *Proceeding of: AINTEC '11, Asian Internet Engineering Conference*, 2011, pp. 1–3.
- [6] Robert Broberg, Matthew Caesar, Douglas Comer, Chase Cotton, Michael J. Freedman, Andreas Haeberlen, Zachary G. Ives, Arvind Krishnamurthy, William Lehr, Boon Thau Loo, David Mazires, Antonio Nicolosi, Jonathan M. Smith, Ion Stoica, Robbert van Renesse, Michael Walfish, Hakim Weatherspoon, and Christopher S. Yoo, "The NEBULA Future Internet Architecture," *Lecture Notes in Computer Science*, pp. 1–24. Volume 7858, 2013.
- [7] Lixia Zhang, Deborah Estrin, , Jeffrey Burke, Van Jacobson, James D. Thornton, Diana K. Smetters, Beichuan Zhang, Gene Tsudik, KC Claffy, Dmitri Krioukov, Dan Massey, Christos Papadopoulos, Tarek Abdelzaher, Lan Wang, Patrick Crowley, and Edmund Yeh, "Named Data Networking (NDN) Project," pp. 1–26, 2010.
- [8] Rowan Klöti, "OpenFlow: A Security Analysis," M.S. thesis, Swiss Federal Institute of Technology Zurich, 2013.
- [9] Jie Wang, *Computer Network Security: Theory and Practice*, Higher Education Press, 2009.
- [10] Ltd Hangzhou H3C Technologies Co., "Attack Prevention Technology White Paper," 2008.
- [11] Emmett Dulaney, *CompTIA Security+ Study Guide*, Wiley, Indianapolis, 4th edition, 2009.
- [12] Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall, 2005.
- [13] Mark Ciampa, *Security Plus Guide to Network Security Fundamentals*, Cengage Learning, 3rd edition, 2009.
- [14] Ling Dong and Kefei Chen, *Cryptographic Protocol: Security Analysis Based on Trusted Freshness*, Springer, 2012.
- [15] Hamid Jahankhani, David Lilburn Watson, Gianluigi Me, and Frank Leonhardt, *Handbook of Electronic Security and Digital Forensics*, Handbook of electronic security and digital forensics, 2010.

- [16] Hannes Gredler and Walter Goralski, *The Complete IS-IS Routing Protocol*, Springer, 2004.
- [17] Future Internet Assembly (FIA) Future Content Networks (FCN) Group, "Technical Report. Why do we need a Content Centric Future Internet?," pp. 1–23, 2009.
- [18] M. Rahamatullah Khondoker, Abbas Siddiqui, Bernd Reuther, and Paul Müller, "Service Orientation Paradigm in Future Network Architectures," in *Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2012)*, 2012, pp. 346–351.
- [19] Paul Müller, Bernd Reuther, and Markus Hillenbrand, "Future Internet: A Service-Oriented Approach - SONATE," in *Würzburg Workshop on Visions of Future Generation Networks (EuroView2007)*, 2007, pp. 1–35.
- [20] Oliver Hanka and Hans Wippel, "Secure Deployment of Application-Tailored Protocols in Future Networks," in *Proceedings of the Second International Conference on the Network of the Future (NoF 2011)*, 2011, pp. 10–14.
- [21] Thomas Gamer and Hans Wippel, "A Collaborative Attack Detection and its Challenges in the Future Internet," in *Proceedings of the Joint ITG, ITC, and Euro-NF Workshop "Visions of Future Generation Networks" (EuroView)*, 2010, pp. 1–2.
- [22] Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Akira Yamada, Samuel C. Nelson, Marco Gruteser, and Wei Meng, "LAP: Lightweight Anonymity and Privacy," in *Proceedings of the IEEE Symposium on Security and Privacy*. 2012, pp. 506–520, IEEE Computer Society.
- [23] Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Sangjae Yoo, Xin Zhang, Soo Bum Lee, Virgil Gligor, and Adrian Perrig, "STRIDE: Sanctuary Trail Refuge from Internet DDoS Entrapment," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS)*. 2013, pp. 415–426, ACM.
- [24] Tiffany Hyun-Jin Kim, Lin-Shung Huang, Adrian Perrig, Collin Jackson, and Virgil Gligor, "Accountable Key Infrastructure (AKI): A Proposal for a Public-Key Validation Infrastructure," in *Proceedings of the 22nd international conference on World Wide Web*. 2013, pp. 679–690, International World Wide Web Conferences Steering Committee.
- [25] Eleni Trouva, Eduard Grasa, John Day, Ibrahim Matta, Lou Chitkushev, Patrick Phelan, and Miguel Ponce de Leon Steve Bunch, "Is the Internet an unfinished demo? Meet RINA!," in *TERENA Networking Conference*, 2011, pp. 1–12.
- [26] Gowtham Boddapati, John Day, Ibrahim Matta, and Lou Chitkushev, "Assessing the Security of a Clean-Slate Internet Architecture," in *Proceedings of the Seventh Workshop on Secure Network Protocols (NPSec)*. 2012, pp. 1–6, 20th IEEE International Conference Network Protocols (ICNP).
- [27] Jeremiah Small, "Patterns in Network Security: an Analysis of Recursive Inter-Network Architecture Security Module Efficiency," M.S. thesis, Boston University, 2012.
- [28] Feixiong Zhang, Kiran Nagaraja, Yanyong Zhang, and Dipankar Raychaudhuri, "Content Delivery in the MobilityFirst Future Internet Architecture," in *Sarnoff Symposium (SARNOFF)*, 35th IEEE, 2012, pp. 1–5.
- [29] MobilityFirst Project Team, "MobilityFirst: A Robust and Trustworthy Mobility-Centric Architecture for the Future Internet," Tech. Rep., 2010.
- [30] Paolo Gasti, Gene Tsodik, Ersin Uzun, and Lixia Zhang, "DoS and DDoS in Named-Data Networking," 2012, pp. 1–10. Volume abs/1208.0952.
- [31] Jad Naous, Michael Walfish, Antonio Nicolosi, David Mazieres, Michael Miller, and Arun Seehra, "Verifying and Enforcing Network Paths With ICING," in *Proceedings of the Seventh Conference on emerging Networking EXperiments and Technologies*. 2011, pp. 1–12. Article No. 30, ACM.
- [32] "ITU-T SG13: Future networks including cloud computing, mobile and next-generation networks," <http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx>, Online; accessed 06-Dec-2013.
- [33] "ITU-T FG FN: Focus Group on Future Networks (FG FN)," <http://www.itu.int/en/ITU-T/focusgroups/fn/Pages/Default.aspx>, Online; accessed 06-Dec-2013.