A Design of Digital Signature Mechanism in NDN-IP Gateway

Dian Abadi Arji
Department of Electrical Engineering
University of Indonesia
dian.abadi@ui.ac.id

Fandhy Bayu Rukmana
Department of Electrical Engineering
University of Indonesia
fandhy.bayu@ui.ac.id

Riri Fitri Sari
Department of Electrical Engineering
University of Indonesia
riri@ui.ac.id

***Abstract*— Named Data Networking (NDN) is a new network architecture that has been projected as the future of internet architecture. Unlike the traditional internet approach which currently relies on client-server communication models to communicate each other, NDN relies on data as an entity. Hence the users only need the content and applications based on data naming, as there is no IP addresses needed. NDN is different than TCP/IP technology as NDN signs the data with Digital Signature to secure each data authenticity. Regarding huge number of uses on IP-based network, and the minimum number of NDN-based network implementation, the NDN-IP gateway are needed to map and forward the data from IP-based network to NDN-based network, and vice versa. These gateways are called Custom-Router Gateway in this study. The Custom-Router Gateway requires a new mechanism in conducting Digital Signature so that authenticity the data can be verified when it passes through the NDN-IP Custom-Router Gateway. This study propose a method to process the Digital Signature for the packet flows from IP-based network through NDN-based network. Future studies are needed to determine the impact of Digital Signature processing on the performance in forwarding the data from IP-based to NDN-based network and vice versa.**

Keywords — ***Digital Signature, NDN, Security, NDN-TCP/IP, Gateway***

I. INTRODUCTION

Named Data Networking (NDN) is a technology that relies on data as an entity, so users only need the content and applications based on data naming, so it no longer rely on client-server communication models based on IP addresses as current technology.

Named Data Networking (NDN) is a projects US National Science Foundation under the Future Internet Architecture Program [1]. Achieve NDN extensive usage in the future requires a connecting gateway between the Internet Protocol version 4 (IPv4) which is currently widely used in world infrastructure, with a NDN-based networks. In this case it will use Custom Router Gateway called Named-Data Border Router (NDBR) and custom DNS Server called Named-Data Name Server (ND-NS) [2]. To secure the data through a NDN-based network, each data will be signed by a Certificate Authority (CA), hence the data authenticity is guaranteed. We design a process mechanism for deploying Digital Signature in the data by NDBR that bridge the delivery between the IP-based network and the NDN-based Network.

This paper is structured as follows: in Section 1, we discuss the background of NDN based system, Section 2 contains literature review on the basic concepts of NDN architecture, and basic security mechanism on NDN. This section contains the concept of Custom Router Gateway, also called Named-Data Border Router (NDBR) and how NDBR works in NDN-IP Interconnection. Section 3 describes the design that we propose, also the Digital Signature mechanism process on the NDN-IP Custom Router, but in this paper, the encryption method will not be included for discussion.

This paper can be used as a reference for readers and researchers who are interested in NDN research, particularly research related to the security of data transmission between NDN-IP gateway. In this paper we propose that the Digital Signature mechanism can be used as a reference globally at the time on the transition between IP-based network and NDN-based network.

II. LITERATURE REVIEW

A. Named Data Network

Named Data Network (NDN) is an evolutionary project that will replace the IP architecture that generalizes all data transmissions from previously using address-to-address to become “fetching” the data identified by a name [3].

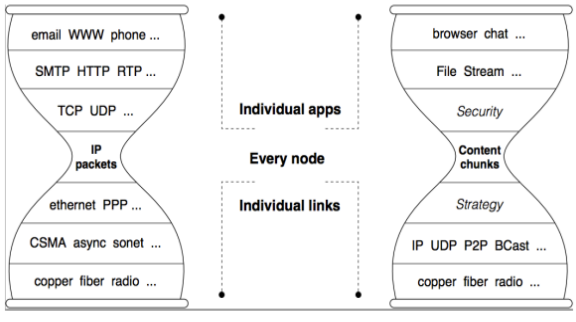

Figure 1. Internet and NDN Hourglass Architecture

The current Internet hourglass architecture illustrated by Figure 1 allows the top and bottom layers of the "Thin Waist" to innovate independently. As the core layer, Internet Protocol (IP) is originally designed for communication between two points (end-nodes). Along with the rapid growth of e-commerce, digital media and social networking, Internet communication has become increasingly dominated by content distribution. The

978-1-7281-1655-6/19/$31.00 ©2019 IEEE

Internet is increasingly complex in its efforts to overcome the problem of distribution with a point-to-point communication protocol. Therefore, different architectural designs are proposed under a network research approach called Information-Centric Networking (ICN) or information-oriented networks. Named Data Network (NDN) is a simple model of Content Centric Networking (CCN) or Information Centric Networking (ICN) [14]. NDN specifically replaces network communications from packet delivery previously based on IP as the basis of delivery, becoming content as the basis delivery [10], in contrast to IP based communication, NDN is oriented toward data content rather than on establishing a session between two end nodes [13]

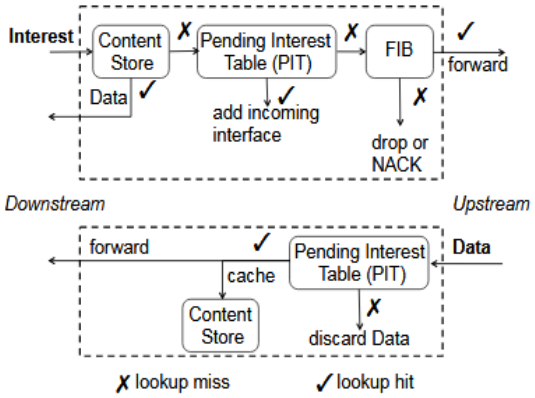

Figure 2. Forwarding Process in NDN Router [1]

NDN Commication is using three types of entites to deliver the information, namely consumer, producer, and router [15] NDN uses routing protocols to reach every Data Name Prefixes, instead of carrying source and destination IP addresses in each packet, NDN puts a dataname in each packet [7]. It is similar to how Internet Protocol (IP) works for reaching the desired IP prefixes. Each NDN node forwards the Interest Packet based-on the specified name, records the interface information from which the Interest Packet is received, and store in Pending Interest Table (PIT). After the Interest Packet finds the appropriate Data Packet, the copy of Data Packet is also be stored in the node's Content Store (CS) [17]. If there is the same Interest Packet request from another Client, the node will respond with the Data Packet in its Content Store [4]. To carry out the above functions, the NDN node uses 3 main structures: Pending Interest Table (PIT) that has been mentioned previously, Forwarding Information Base (FIB), and Content Store (CS). The Pending Interest Table (PIT)'s main function is to accommodate the Interest Packet sent by the other nodes, Content Store (CS) serves as a component to store the copy of the Data Packet, while Forwarding Information Base (FIB) has the information related which interface that is ready to forward the data content, three core modules above are part of NDN router [16]. Figure 2 describes the forwarding process flow in the NDN node.

B. NDN-IP Interconnection Design

The difference in the communication pattern between content-centric on NDN networks and host-to-host on IP-based network causes a special device that functions to interconnect and bridge the two different entities. Figure 3 specifies the devices involved in the interconnection design.

The NDNization introduces interconnection mechanism using two types of communication flows and also introduced two special nodes (NDBR and ND-NS). Communication flows are the vectors on how the Client in IP-based or NDN-based network communicate with the Server in opposite-based network. The first communication flow represent how NDN-based Client communicate with the Server in IP-based network, and the second communication flow represent how IP-based Client communicate with the NDN-based Server [2].

Custom Router Gateway called Named-Data Border Router (NDBR) is a custom router that bridges the communication between NDN-based network and IP-based network. NDBR has the task to advertise the allocation of each IP prefix for each domain on the NDN network to the nearest border router. NDBR is also responsible for translates the NDN header to the IP header and vice versa. To change the source and destination of IP addresses that are translated to other forms also need a special node called Named-Data Name Server (ND-NS). ND-NS responsible for handling name mapping in NDN networks with allocated IP addresses hence the IP-based network can reach the terminal in NDN network. The domain name records in ND-NS are broadcasted to other DNS (DNS on IP networks), and likewise the DNS on IP-based networks also broadcast its tables to ND-NS [2].

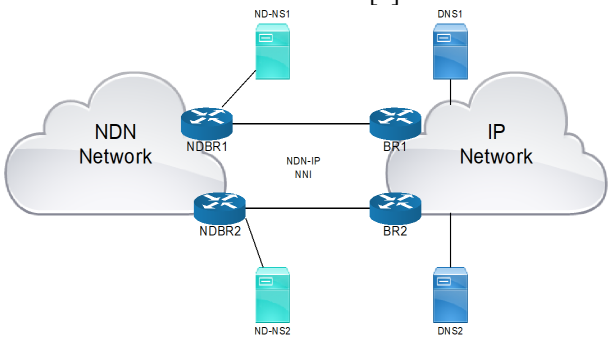

Figure 3. NDN-IP Interconnection Design (NDNization)

C. Digital Signature in NDN

In the contrary to the process of securing data communication in IP-based network that uses security from host-to-host or address-to-address, a special mechanism is needed to directly secure from address to address, but also directly secure data communication from consumers to producers for each content in NDN. To secure the data transfer and information exchange process in NDN networks, a scheme of Signed Interest is made. Signed Interest is a mechanism for publishing interest that has been authenticated. The signature of this Signed Interest is deployed inside the last components of the interest prefix. The signature covers the name, thecontent, and the metadata for signature verification [8]. One pieceof the metadata is the key locatorThis signature includes continuous block start from the first name to the last name of the TLV components as described in packet structure on Figure 4.

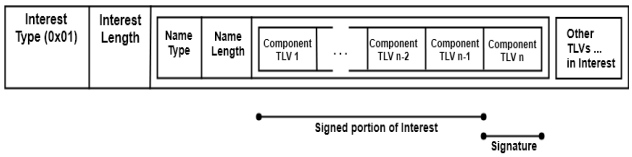

Figure 4. Signed Interest Packet Structure [9]

Specifically there are 4 additional components in Signed Interest Packet as follows:

- <timestamp>
- <nonce>
- <SignatureInfo>
- <SignatureValue>

For example, for the name below:

/signed/interest/name

hence the interest will become:

/signed/interest/name/<timestamp>/<random-value>/<SignatureInfo>/<SignatureValue>

Additional components of Signed Interest

When a producer receives an Interest Packet, according to the interest prefix, the producer must be able to decide whether the interest must be signed or not. If the receiving interest should be signed, the interest will be considered as invalid with the criteria as follows:

- One of the four components (Timestamp, Nonce, SignatureValue, and SignatureInfo) is missing;
- Key is not trusted to sign an interest;
- The signature cannot be verified with the Public Key designated by KeyLocator at SignatureInfo.

The recipients of the signed interest then can check the timestamp and the uniqueness of the signed interest. A sample case is when the signed interest carries certain commands. In this case, signed interest can be considered invalid if there is a valid signed interest with the same time stamp or longer than the received time stamp on the previous signed interest. To detect this situation, the recipient needs to update the latest time state and synchronize the time for each trusted public key [9].

D. IP Certificate Authority and NDNCert Mechanism

One part of the important infrastructure security of IP network is Public Key Infrastructure where there must be an independent and trusted institution (trust agent) as a Public Key agent [11]. This institution is known as the Certification Authority (CA) institution. With the existence of this institution, orders, electronic contracts that are guaranteed to be safe and which are officially impossible to be changed or falsified. Each order or contract that is transferred by using a combination of private key and public key, the order or contract that is already in place until the new recipient can be opened or known after the public key is approved by the CA. Main component of IP Certificate Authority is Certification Authority (CA) and Registration (RA) server, CA main job is import requests, create list request, export certificate, archive requests, delete and issues requests, verify RA operator identity, meanwhile main job of RA is create list of pending/deleted/archived, approve request, and export/import request to removable media. Figure 5 explains about key certificate authorization process in IP-based network [12].

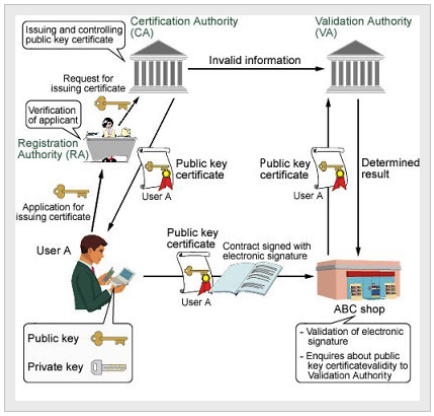

Figure 5. Certificate Authorization Process [6]

In NDN Network, every data packet must have a signature, the signature could data consumer to check integrity and determine the data trusted issued by producer. NDNCert enables to facilitate certificate issuing and management process, NDNCert could automated intra-node and inter-node trust management using NDN with obtained or self-signed, each node can become authority for its namespace.

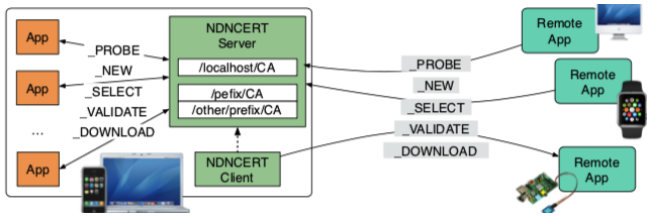

Figure 6. NDNCert Overview [5]

Figure 6 describe NDNCert overview, on single node or the same node. The node could act as NDNCert and NDN Client at the same time if necessary.

III. PROPOSED MECHANISM

A. In this research, we use the following parameters:

- Security on NDN
- Certificate Authority on NDN-IP Interconnection

B. Digital Signature Mechanism in NDN-IP Gateway Router

The Named Data Networking (NDN) architecture builds the security primitives into the network layer, all retrieved data packets must be signed to ensure their integrity, authenticity, and provenance. Different from IP network where only well-known node could become CA, every single node or entity could be a CA. In this case, all namespace, even all sub-namespace should be have trust between certificate, there is a problem when we will integrate all different entity such as IP network and NDN

network, there should be a flexible mechanism to delegate trust between certificates on within a single device (managing permissions for local applications on a node to operate under a given namespace) and across devices or entities. Using NDNCert mechanism could solve the problem above.

Based on NDNization Communication flow, there should be an entity that could be a CA to bridge communication between IP network and NDN network, in this case would be NDBR (NDN) and CA (IP), this node would take responsibility to sign and verify the data that would across the network is proven authenticity. In Client (NDN) to Server (IP) communication flow, NDN client would be act as certificate requester and represent request from client NDN to Server (IP), and NDBR would be act as Certificate Authority and represent all network behind this NDBR, including all IP network behind this entity, but in IP network NDBR will communicate with traditional CA on IP network before sends data to BR (IP) to proven authenticity on IP network. In Client (IP) to Server (NDN) communication flow, before sends data to NDN network, Clinet (IP) will communicate to local IP CA (IP) to proven authenticity, and then after the data pass through NDN network, NDBR would act as certificate requester and server (NDN) would act as Certificate Authority and also represent all namespace and all subnamespace behind this entity. All signature of interest/data will be verified by CA and requester.

Since the data will be sent between two different entities, the communication will be separated into two different flows. There are the communication vector from NDN-based Client to IP-based Server, and also communication vector from IP-based Client to NDN-based Server.

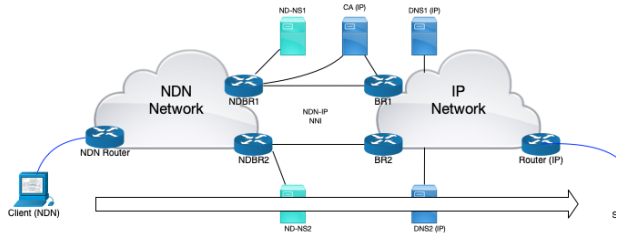

Figure 7. Network Topology Client (NDN) to Server (IP) Communication

Figure 7 describes the network topology and the position of each component related the communication from IP-based network to the NDN-based network.

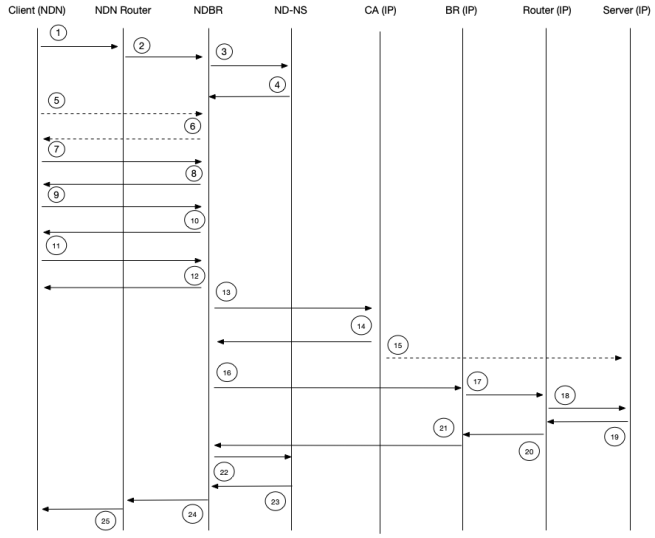

Figure 8. Client (NDN) to Server (IP) Communication Flow State Diagram

Figure 8 describes the communication flow how client (NDN) request data and how NDBR act as CA and represent all IP network behind, the detail as follows:

1. Client (NDN) request the packet
2. If the NDN Routers do not have the copy of the data, it sends the request to NDBR
3. NDBR ask ND-NS for IP Address resolve to
4. ND-NS answers with IP Address resolve
5. Client (NDN) discovery of available sub-namespace
6. NDBR assigned/selected namespace
7. Client (NDN) generate key pair and send certificate request to NDBR
8. NDBR collect available challenges, store the request instance, give the challenge option to client (NDN)
9. Client (NDN) select a the challenge, and send to NDBR
10. NDBR prepare the challenge and send to Client (NDN)
11. Client (NDN) perform the challenge, and sends a _VALIDATE command to finish the challenge
12. NDBR check challenge result, if valid NDBR issue the certificate, if not generate status info, and the certificate not given
13. NDBR generate public and private key, send application for issuing certificate to RA, RA do verification of application and send request issuing certificate to CA, CA do issuing and controlling public key certificate
14. CA determined the result of validation, and send public key certificate to NDBR
15. CA announced status of validation of NBR packet to server (IP)
16. NDBR translate NDN packet to IP Packet and send the packet to BR (IP)
17. Border Router (BR) send the packet to Router
18. The Router sends the packet to Server
19. The Server sends back the response to Router
20. The Router sends the packet to Border Router (BR)
21. Border Router (BR) sends the packet to NDBR
22. NDBR asks ND-NS for the domain name
23. ND-NS sends the response to NDBR

24. NDBR translates IP Packet to NDN Packet, then sends the packet to NDN Router
25. NDN Router copy the data and sends the packet to Client

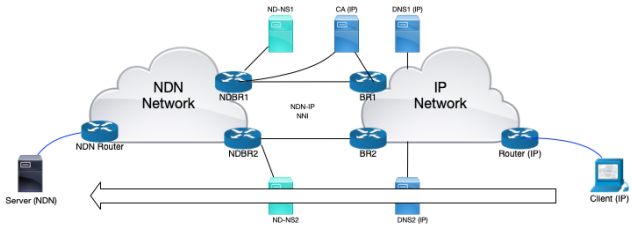

Figure 9. Network Topology Client (IP) to Server (NDN) Communication

Figure 9 shows the network topology related to the communication from the NDN-based network to the IP-based network. It is also describes the positioning of each node on interconnection between IP-based network and NDN-based network.

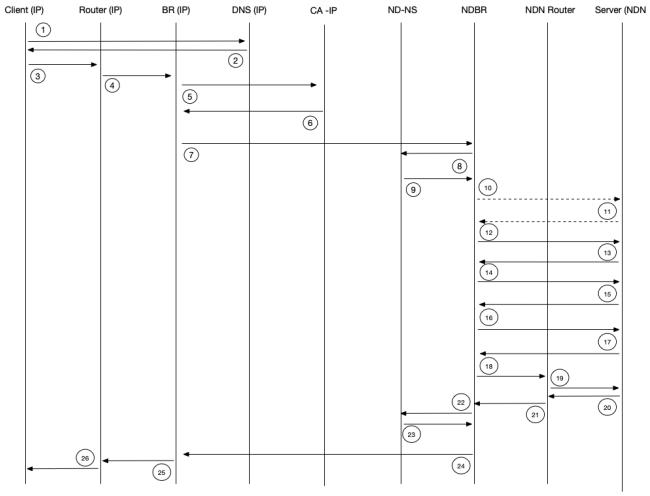

Figure 10. Client (IP) to Server (NDN) Communication Flow State Diagram

Figure 10 describes the communication flow how client (IP) request data and how CA (IP) interact to client IP and then NDBR act as certificate requester, the detail as follows:

1. Client (IP) request domain name resolve from DNS (IP)
2. DNS (IP) sends the resolve query to Client
3. Client (IP) sends the packet to Router (IP)
4. Router (IP) forwards the packet to Border Router (BR)
5. BR (IP) generate public and private key, send application for issuing certificate to RA, RA do verification of application and send request issuing certificate to CA, CA do issuing and controlling public key certificate
6. CA determined the result of validation, and send public key certificate to BR (IP)
7. CA announced status of validation of BR (IP) packet to NDBR
8. Border Router sends the packet to NDBR
9. NDBR asks ND-NS for the destination domain name
10. ND-NS sends the response to NDBR
11. NDBR discovery of available sub-namespace
12. Server (NDN) assigned/selected namespace
13. NDBR generate key pair and send certificate request to server (NDN)
14. server (NDN) collect available challenges, store the request instance, give the challenge option to NDBR
15. NDBR select a the challenge, and send to server (NDN)
16. Server (NDN) prepare the challenge and send to NDBR
17. NDBR perform the challenge, and sends a _VALIDATE command to finish the challenge
18. Server (NDN) check challenge result, if valid server (NDN) issue the certificate, if not generate status info, and the certificate not given
19. NDBR translates IP Packet to NDN Packet, then sends the packet to NDN Router
20. NDN Router sends the packet to Server (NDN)
21. The Server (NDN) sends back the response to NDN Router
22. NDN Router sends the response packet to NDBR
23. NDBR asks ND-NS for the destination IP Address
24. ND-NS sends the response to NDBR
25. NDBR translates NDN Packet to IP Packet, then sends the packet to Border Router (IP)
26. Border Router sends the packet to Router (IP)
27. Router (IP) forward the packet to Client (IP)

Using this methodology, it will be easier to see and deploy the process of certificate authorization in NDBR for the packet came from IP-based network. Hence the data from IP-based network will match with the certificate of origin server.

IV. CONCLUSION

IP network and NDN network are two different entities that have different ways of work and have different mechanism to secure end-to-end communication. The problem is how we could integrate two different entities like IP network and NDN network without eliminating their security aspect. This research discuss about a new mechanism in Digital Signature on NDN-based network and IP-based network by integrating NDNCert technology and Certificate Authorization in IP-based network. Hence the data authenticity can be verified when the data are passing through the NDN-IP Router Gateway in NDN-IP integration, the digital Signature mechanism proposed above can be used as a reference globally at the time on the transition between IP-based network and NDN-based network. The future work need to explore more on how much network performance will be affected by this mechanism implementation, and need to explore more to create a hybrid entity as CA that could handle NDN traffic and IP traffic at once, so that will save more cost and processing time.

V. ACKNOWLEDGMENT

We thank University of Indonesia for financial support for this research under the Pit9 Grant, under the contract number: NKB.0072/UN2.R3.1/HKP.05.00/2019.

VI. REFERENCES

[1] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, et al., "Named Data Networking (NDN) Project", Named Data Networking Technical Report NDN-0001, October, 2010

[2] F. Rukmana, N. Hendrarini, R. Sari, "NDNization of IP Network Based On Communication Flow Modem", ICAIIT, March 2019.

[3] L. Zhang, P. Crowley, C. Papadopoulus, L. Wang et al. "Named Data Networking", ACM SIGCOMM Computer Communication Review, July, 2014.

[4] Z. Zhang, Y. Yu, H. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyef, L. Zhang " An Overview of Security Support in Named Data Networking", Named Data Networking Technical Report NDN-0057, April 2018

[5[Z. Zhang, Y. Yu, A. Afansyev, L. Zhang "NDN Certificate Management Protocol (NDNCert)", NDN, Technical Report NDN-0050, April 2017

[6] S. F. Al-Janabi, A. Obaid "Development of Certificate Authority Service for Web Applications" International Conference on Future Communication Networks, 2012

[7] V. Lehman, M Hoque, Y. Yu, L. Wang, B. Zhang, L. Zhang, "A Secure Link State Routing Protocol for NDN", NDN, Technical Report NDN-0037, 2016

[8] "NDN packet format specification," http://named-data.net/doc/ndn-tlv/

[9] "Signed Interest NDN C++ Library with eXperimental eXtensions", https://named-data.net/doc/ndn-cxx/current/specs/signed-interest.html

[10] Y. Yu, Y. Li, X. Du, R. Chen, B. Yang, "Content Protection in Named Data Networking Chalenges and Potential Solutions", arXiv:1810.11179v1, October, 2018

[11] B. Jayaraman, H. Li, D. Evans, "Decentralized Certificate Authorities, University of Virginia, June, 2017

[12] M. A. Spencer, "The Economics of Cryptographic Trust: Understanding Certificate Authorities", Massachusetts Institute of Technology, February, 2016

[13] Yuliandi, D. V. Wahyuda, D. Achmadi, R. F Sari, "Comparison of Different WLAN Standard on Propagation Performance in V2V Named Data Networking", 2017 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), November, 2017

[14] B Susilo, M. R. Rotinsulu, R. F Sari, "Performance Evaluation of Ideal Nearest Replica Routing (NRR) Against Several Forwarding Strategies on Named Data Networking(NDN)", 2018 IEEE Region Ten Symposium (Tensymp), July, 2018

[15] D. Vektorendra, R. F. Sari, "Performance Evaluation of Relay Node and Power Transmission Selectionon V2V Communication in Named Data Networking", The 21st International Symposium On Wireless Personal Multimedia Communications (WPMC-2018), November, 2018

[16] B. Susilo, A. Prasekal, R. F. Sari, "Measuring QoS of Nearest Replica Routing Forwarding Strategyon Named Data Networking for Triple Play Services", The 21st International Symposium On Wireless Personal Multimedia Communications (WPMC-2018), November, 2018

[17] Y. A. Phanama, F. A. Ekadiyanto, R. F. Sari, "Serverless Mobile Multiuser Chat Application Based on ChronoSync for Named Data Networking", Transactions on Networks and Communications 4, August, 2016