Securing Named Data Networking: Attribute-Based Encryption and Beyond

doi: info:doi/10.1109/MCOM.2018.1701123

Securing Named Data Networking: Attribute-Based Encryption and Beyond

Licheng Wang*, Zonghua Zhang†, Mianxiong Dong‡, Lihua Wang§¶ Zhenfu Cao‖, Yixian Yang*
* State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, 10 West Tucheng Road, Haidian District, Beijing 100876, P.R. China
† IMT Lille Douai, Institut Mines-Télécom, and CNRS UMR 5157 SAMOVAR Lab, France
‡ Dept. of Information and Electronic Engineering, Muroran Institute of Technology
27-1 Mizumoto-cho, Muroran, Hokkaido, 050-8585, Japan
§ Graduate School of Engineering, Kobe University, 1-1 Rokko-Dai, Nada-ku, Kobe 657-8501, Japan
¶ Cybersecurity Research Institute, National Institute of Information and Communications Technology
Tokyo 184-8795, Japan
‖ School of Computer Science and Software Engineering, East China Normal University
3663 Zhongshan Road (North), Shanghai 200062, P. R. China

***Abstract*—As one of the promising information-centric networking (ICN) architectures, named data networking (NDN) has attracted tremendous research attentions and efforts in the past decade. In particular, security and privacy remain as one of the significant concerns and challenges, due to the fact that most of the traditional cryptographic primitives are no longer suitable for NDN architecture. For example, the traditional cryptographic primitives aim to secure point-to-point communications, always requiring explicit descriptions of where or whom the data packets are intended to, while network addressing or locating in NDN becomes implicit. To deal with such issues, the recently developed cryptographic primitives such as attribute-based encryption (ABE) have been applied to NDN. Also, to efficiently solve the trust-roots problem and seamlessly deploy cryptographic infrastructures, the concept of Software-Defined Networking (SDN) has been introduced to NDN as well. This tutorial is devoted to exploring the interesting integration between NDN, ABE and SDN.**

I. Introduction

While the Internet has become an indispensable part of our daily life, its access modes and functionalities experience dramatic change due to the rapid development of Internet applications and services. The legacy TCP/IP architecture has been increasingly recognized to suffer from some fundamental flaws in routing expandability, mobility, as well as security and privacy protection. Therefore, the future Internet architectures (FIA) [1] has been proposed and gained widespread recognition in the past decade, among which two representative new networking paradigms are information-centric networking (ICN) [2] and software-defined networking (SDN) [3]. Specifically, instead of using traditional network addressing techniques (e.g., IP address, NAT, DNS), ICN is focused on content-based routing by implementing the transformation from the idea of "WHERE to find the required contents" to the idea of "WHAT kind of contents to be found". Among the various ICN techniques, content-centric networking (CCN) [4] and named data networking (NDN) [5] have gained wider popularity, and CCN/NDN testbeds have already covered more than 30 cities across America and Asia. SDN, as another paradigm of FIA, provides not only conveniences for developing new network applications, but also unified and rapid deployment of various newly developed FIAs, thanks to the separation of control plane and data plane. At present, OpenFlow based SDN technique has won support from both academia and industry, and the related international standards and world-wide testbeds are gradually setup [6].

Despite their advantages, all kinds of ICN architectures face new challenges in security/privacy aspects [7], [8]. In particular, both NDN and SDN community pay far less attention to the security and privacy issues than they deserve. For example, although the name-based routing technique in NDN naturally provides a robust way to mitigate DDoS like attacks targeting IP networks, novel attacks that particularly exploit the features of NDN have been identified, e.g., interesting flooding attack (IFA). The same story occurs in SDN, in which an SDN controller compromised by malicious network app may lead to the failure of the whole network, while the SDN switches can be also poisoned to launch DDoS attacks to the controller. It is worth noting, however, the straightforward application of traditional security mechanisms to those novel networking paradigms are not effective, primarily because that the new networking architectures do not explicitly specify how to deploy security or privacy mechanisms. For instance, it remains unclear how to design effective cryptographic protocols in NDN architecture, considering the fact that most of those protocols heavily dependent on the network addresses or locations, which are not available in NDN.

This tutorial is intended to propose a framework which bridges NDN architecture with the newly developed cryptographic primitives such as attribute-based encryption (ABE), and specifically discusses the feasibility of coupling NDN and SDN together in solving the trust-roots problem by seamlessly deploying cryptographic infrastructures.

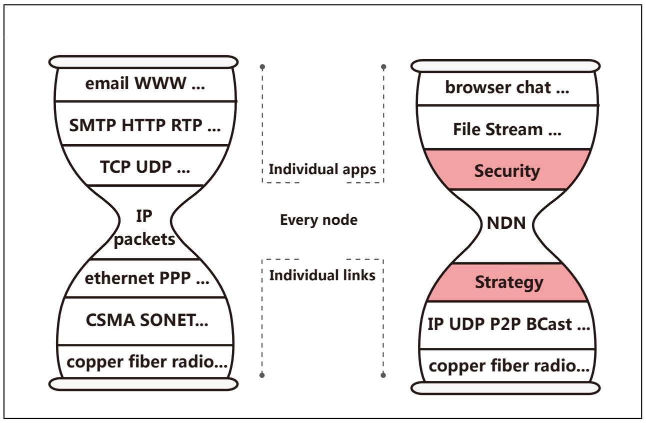


Fig. 1. TCP/IP Architecture vs. NDN Architecture [5]

II. Security in NDN

The original concept of ICN was proposed in 1999 [2], which was defined as a new networking paradigm that users are concerned with the contents or data instead of their locations or network addresses. Among various innovative practices of ICN, the alliance of CCN and NDN manifests a promising prospect, and the two terms are sometimes interchangeable.

Technically speaking, NDN is a clean-slate design that does not rely on TCP/IP architecture. As shown in Fig.1, the performance bottleneck (i.e. the so-called "this-waist" part) in NDN is due to NDN chunks instead of IP packets. That means, instead of treating host-based addresses as the first-class network objects, NDN regards data as the first-class network objects that are associated with globally unique names, finally leading to a name-based routing mechanism. Thus, the notion of "host" is no longer explicitly specified in NDN, while *interest* and *data* are the only two types of packets in NDN. To implement name-based routing algorithm, each NDN router maintains three major data structures: (1) Pending Interest Table (PIT), which contains currently unsatisfied interests and corresponding incoming interfaces; (2) Forwarding Interest Base (FIB), which contains name prefixes and corresponding outgoing interfaces; (3) Content Storage (CS) for data caching and retrieval. Then the communications in NDN use the pull model: a consumer requests content of interest by sending an interest packet; If an entity (a router or a host) can find a matched content object (i.e., named data packet) in its CS, the corresponding data packet will be returned to the requester by simply following the reverse path of the interest request. Naturally, such receiver-driven and data-centric communication protocol are immune from DDoS attacks targeting at traditional TCP/IP architecture. In particular, IP spoofing becomes impossible. Also, in NDN, it's usually the closest cache nodes which respond the requests. As a result, DDoS attacker can not simply overwhelm a victim node by repeatedly sending the interest requests. Moreover, NDN provides certain built-in security mechanisms for data protection. For example, all the data traveling in the network are digitally signed by the data producers, ensuring data authenticity and integrity.

Despite the aforementioned built-in mechanisms, a set of security challenges still remains in NDN, some of which are highlighted in the following.

- First, in TCP/IP networks, the deployment of traditional cryptography primitives rely on the trust roots, e.g., certificate authority (CA), public-key infrastructures (PKI), which are however hard to be deployed due to the lack of explicit network addressing in NDN.
- Second, due to the name-based routing mechanism and lack of explicit network address in NDN, content protection and access control become extremely challenging. In particular, as the data producers do not know the potential requesters, they cannot encrypt the data in advance without the knowledge of the receiver. In fact, the data producers are even not involved in the routing, and the data has already been cached in some NDN nodes that are close to the interest requesting nodes.
- Last but not least, NDN suffers from interest flooding attacks (IFA) and content poisonous attacks (CPA) [9]. Specifically, IFA aims to exhaust PIT resources of the related routing NDN nodes by exploiting the feature of name-based routing. IFA becomes even worse when malicious data published with an eye-catching or fancy name along with an invalid verification key. This will attract requests of potential consumers, which however lead to numerous repeated requests, since the return packet fails to pass the signature verification. Also, as the signature verification in NDN routing nodes is optional, the hijacked cache node might inject malicious data in the middle routing nodes, eventually the poisoned data will be cached in all the nodes along the request-response routing path.

III. Security in SDN

In 2008, with a primary objective to simplifying the switch design of Ethane, OpenFlow protocol was proposed and quickly gained popularity in both industry and academy. Then the following years have witnessed the rapid development of SDN. In 2014, the open-source SDN operation system ONOS and the open NFV platform program OPNFV were announced respectively. Generally, SDN architecture consists of three planes [6]: *application plane*, which runs different network applications; *control plane*, which manages network intelligence and decision making from *data plane*, which contains the physical forwarding devices. The communications between the three planes are enabled by northbound APIs (app-control plane) and southbound protocols (control-data plane), e.g., OpenFlow. In addition, the configuration and communication compatibility and interoperability between different data and control plane devices can be enabled by open and standard west-east interfaces and protocols.

To date, non-trivial research efforts have been paid to identify security threats in SDN. As shown in Fig.2, seven critical threat vectors have been identified [6]. For example, the first threat vector refers to the DDoS attacks potentially caused by forged traffic flows. An attacker can exploit particular vulnerabilities of the forwarding devices (attack vector 2), as well as the logically centralized controllers (vector 4). The

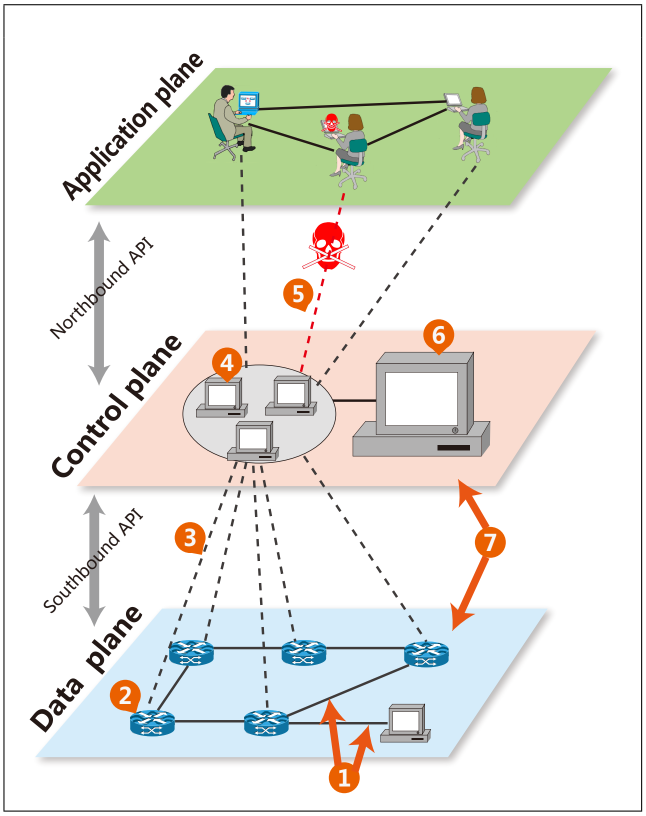


Fig. 2. SDN Architecture and Attack Vectors [6]

communications between data plane and control plane via OpenFlow can be also potentially compromised (vector 3). Vector 5 refers to the fact that the controller can be compromised by the malicious network apps. The administrative station hosting the controller is vulnerable to attacker as well (vector 6), and vector 7 represents the lack of trust resources for fast fault diagnosis and secure recovery. While vectors 1,2,6 and 7 are commonly seen in traditional networks, vectors 3, 4 and 5 are essentially resulted from the separation between control and data planes, as well as the SDN controller.

In [10], Grusho et al. pointed out that SDN security could be enhanced by at least two ways: One is to securely coupling SDN with other new FIAs for gaining complementary advantages, and the other is to, via cryptographic means, prevent malicious entities from accessing critical information. However, to the best of our knowledge, few specific solutions has been seen. We are therefore motivated to propose our solutions to put these two suggestions together in the next section.

IV. Leveraging ABE and SDN to Secure NDN

Attribute-based encryption (ABE) is an interesting extension of identity-based encryption (IBE). Different from those certificates of users in traditional PKI which are produced and maintained via Certificate Authority (CA), certificates in IBE are implicitly bounded with the relationship between the users' identities and their associated secrets, which are produced by a trust third party named Private Key Generator (PKG). Compared with CA, PKG has a much smaller workload in the sense that PKG need not to maintain users' certificates after sending the corresponding secret keys to users via secure channels. From 1984 to 2001 when Boneh and Franklin proposed the first practical IBE scheme, people took a 17 years long journey in probing this problem. After then, IBE manifests a quick development. To support using IBE in a hierarchical organization (say an international company), IBE was extended to hierarchical identity-based encryption (HIBE). To support living things features (such as iris) being used as users identities, fuzzy-identity based encryption (FIBE) was proposed in 2005, and this concept was quickly extended to attribute-based encryption (ABE) in 2006 to support more flexible and fine-grained access control. With ABE, the potential user who has the right to access some confidential contents are no longer a single user, instead of a set of users that are determined by an *access structure*, which is usually defined as a logical composition of users attributes such as name, gender, age, living features, and even social attributes such as affiliations, titles, etc. [11].

The basic diagram of ABE can be illustrated in Fig.3. After the PKG publishes the system parameters, a data producer (say a document creator John or Tim) can encrypt the document with an access structure (say the logic tree marked with grey background), any NDN user (say Alice) with attributes that satisfy the access structure can decrypt the document by using the corresponding secret key $\mathrm{SK}_{\mathrm{att}}$. That is, the data producer does not need to know who will read the document in advance. Instead, he/she only needs to encrypt data based on the knowledge about what kind of user groups can access to the data. This feature makes ABE particularly useful in NDN, where a data producer/sender does not need to know who are the potential data consumer/receivers. More specifically, we illustrate four desirable properties of ABE that can be leveraged in NDN,

- Identities. In NDN, each data has a unique name, which can be naturally used as the identity of the data.
- Hierarchical identity. In NDN, prefix-based naming method caters to the framework of HIBE, which provides tailor made supporting on hierarchical routing.
- Fuzzy-identity. By nature, FIBE can support wildcard characters in name-based routing.
- Attributes. ABE enables the NDN data producers, via logical composition of attributes, to determine a fine-grained specification on what kind of users can learn the encrypted data during the process of encrypting, without worrying about the real identities of the potential receivers.

We therefore conclude that the cryptographic primitives IBE, HIBE, FIBE and ABE have significant potential to achieve data encryption in NDN. More specifically, the deployment of these cryptographic primitives in NDN are given in the following.

- First, we need to address the problem of transferring access rights. No matter IBE, HIBE, FIBE or ABE primitives are used, the potential decrypting groups are specified via certain logical composition of their attributes, and this kind of specification becomes fixed

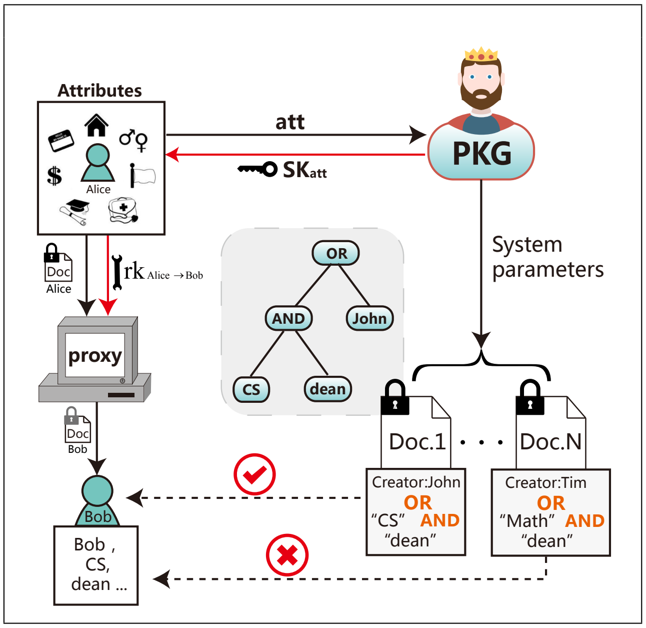


Fig. 3. Primitives for ABE and AB-PRE. (Here, $\mathbf{rk}_{\text{Alice}\to\text{Bob}}$ refers to the re-encryption key from Alice to Bob, and the system parameters include all settings related to keys and attributes.)

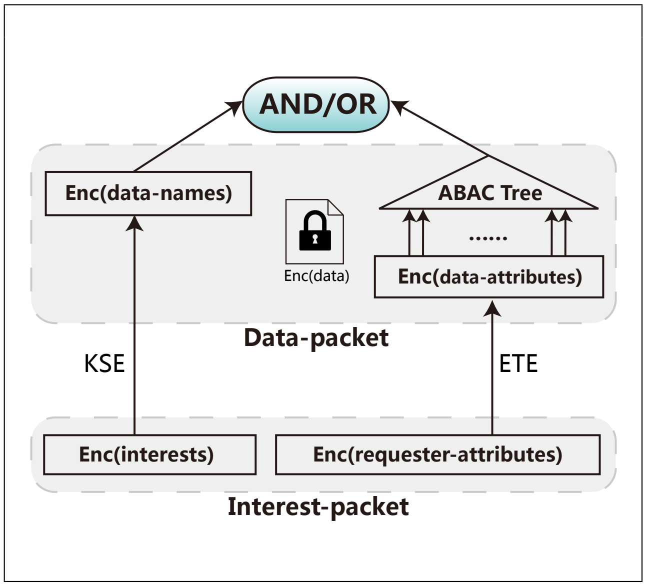


Fig. 4. Attribute Routing System in NDN. (Here, ABAC tree means attribute-based access control tree, data-names are the global unique names for identifying the data, data-attributes include all attributes used for defining the ABAC logic towards the data, while requester-attributes include all attributes possessed by the interest requester.)

once it is embedded in the corresponding ciphertexts. However, the traditional access control in general is a dynamic and time-variant system, say some users have promoted their accessibility levels, or the confidentiality policies towards some encrypted data have changed due to some unexpected events such as large scope leakages of information of user decryption keys. Thus, we indeed need a mechanism to, without decrypting-then-encrying process, transform an encrypted data for an old access structure/group to an encrypted data for a new access structure/group. To solve this problem, ABE has to combine another cryptographic primitive — proxy re-encryption (PRE), leading to the so-called attribute-based proxy re-encryption (AB-PRE). Again, let us take Fig.3 as an example, where AB-PRE enables a semi-trust proxy, without seeing the plaintexts, transforms the encrypted data for Alice to another encrypted data for Bob. After then, Bob can see the corresponding plaintexts by using his own decryption key [11]. Here, Alice and Bob could be representatives of identities, attributes, or even access structures.

- Second, privacy-preserving routing and interests-data matching are even more complex than encrypting and decrypting in NDN. Say, in NDN, we might want to look up some sensitive contents but we do not like to expose our interests to NDN caching nodes. This is a paradox since NDN caching nodes need the capability to perform matching between the requested interests and cached data. Fortunately, ABE has already coupled successfully with recently developed cryptographic primitives such as keyword searchable encryption (KSE) and equality testable encryption (ETE) [12]. KSE enables us to match encrypted keywords without decrypting, while ETE enables us to test whether two random ciphertexts contain the same plaintext without decrypting. It is clear that KSE and ETE are very useful in name-based routing and attribute-based routing in NDN (See Fig.4), where an interest-packet consists of two parts: encrypted interests, and encrypted requester-attributes. The first part will be confidentially matched with encrypted data-names, while the second part will be confidentially matched with encrypted data-attributes.
- Third, deploying trust-roots (say PKG) and security policies in NDN faces new challenges. In NDN architecture, security layer and strategy layer are separated by the "thin-waist" layer (See Fig.1). This kind decoupling mechanism is reasonable since in strategy layer, security policies are specified by the composition of security primitives (such as encryption, signature, authentication, etc.) and aim mainly at what we should do, without much concern on how to do, while in security layer, concrete security components (say cryptographic algorithms), are adopted according to security levels required by upper layer applications and aim at solving the problem of how to do. To tackle the challenges due to the lack of explicit identifies with respect to "host" and "network address" as mentioned above, SDN is introduced to NDN for achieving rapid and consistent deployment. More specifically, we follow the framework of [13], but with the following improvements, to bridge NDN with OpenFlow in deploying trust-roots for supporting ABE and other aforementioned cryptographic primitives (Fig.5):
  - At first, name-based routing system (NRS) is extended to attribute-routing system (ARS) (See Fig.4). This extension is naturally enlightened by the idea of attribute-based cryptography that is one of the most flexible and expressive access control technologies

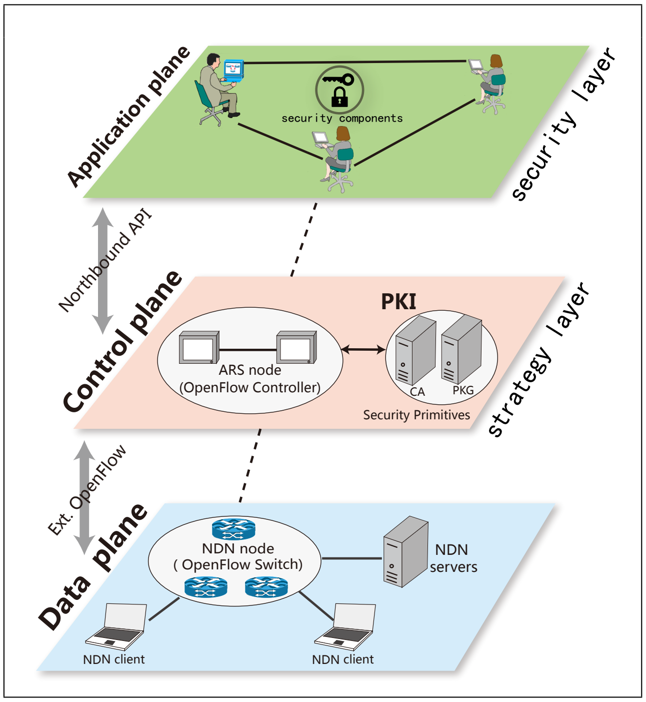
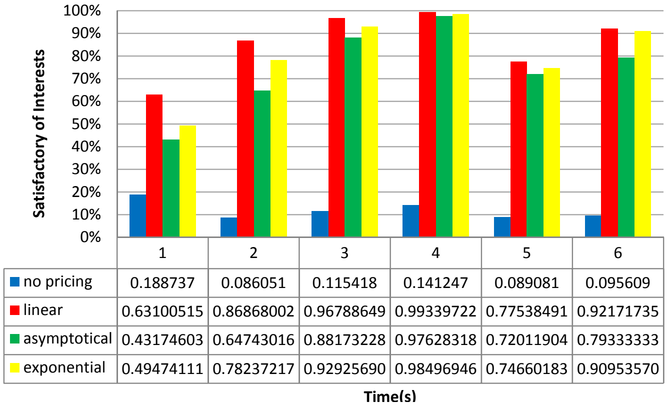


Fig. 5. Integration between NDN, ABE and SDN



	1	2	3	4	5	6
🟦 no pricing	0.188737	0.086051	0.115418	0.141247	0.089081	0.095609
🟥 linear	0.63100515	0.86868002	0.96788649	0.99339722	0.77538491	0.92171735
🟩 asymptotical	0.43174603	0.64743016	0.88173228	0.97628318	0.72011904	0.79333333
🟨 exponential	0.49474111	0.78237217	0.92925690	0.98496946	0.74660183	0.90953570

Fig. 6. Ratio of Satisfied Interests to Total Requests

available today. The feasibility of this extension lies in that Ion et al. [14] had already implemented ARS by using CCNx. However, our extension introduces the following remarkable improvements in the sense that the Broker in Ion et al.'s framework is removed, while an "AND/OR"-switchable logic node at top of the attribute-based access control (ABAC) tree is newly introduced. More specifically, the interest forwarding routing and the interest-data matching process are still inherited from the idea of NRS, but the backward data packet routing process is changed in a fully compatible manner: For the intermediate NDN routing interfaces, the "OR" logic is used, while for the last hop interfaces (i.e., reaching the target users), the last data forwarding condition is automatically switched to "AND" logic. The intuition behind this modification is: For the target users, only if his/her attributes satisfy the access policy embedded in the encrypted data, he/she has the ability to read the data; while for intermediate NDN routing interfaces, it is reasonable to relax the "AND" logic to the "OR" logic for keeping a trace of requested data for potential subsequent similar – either similar in names or similar in attributes – requests.

– After then, OpenFlow is extended by adding cryptographic primitives and new control plane is built thereon. The extended OpenFlow controller can be viewed as nodes of ARS, and the new control plane consists of ARS and security infrastructures such as CA, PKG, etc. As for data plane, Salsano's architecture can be followed. That is, the data plane consists of a series of CCN/NDN nodes and clients. The extended OpenFlow acts as the communication interface between control plane and data plane. For strategy layer, the extended OpenFlow supports primitive calling specified by security policies, while for upper security layer, the extended OpenFlow provide mapping between the primitives and the concrete security techniques such as running-time library of cryptographic algorithms.

– Finally, the trust-roots and the authentication chains are established based on certificate objects. Bian et al. [15] proposed a deploying hierarchy for key management in UCLA NDN testbed, where the key-certificated pair of the testbed own is taken as the trust-root, while key-certificate pairs of other sites, users, devices are authenticated transitively via the chains of key-certificate pairs contained in NDN data packets. Moreover, with introducing the IBE/ABE into NDN, the certificate objects can be even simplified, say let the names or attributes alone acting as the public-keys. By doing so, most communication cost on certificates transportation is saved, since explicit certificates are no longer needed. In practice, key evolution strategy should be also taken into consideration in case of someone's secret key might be lost or stolen.

It is worth noting that employing ABE to NDN cannot solve all the security and privacy issues in NDN. To make our proposed framework useful, one of the assumptions is to securely implement and efficiently deploy ABE and the related cryptographic components. Otherwise, the new attacks or scalability issues can be potentially introduced. Today, most of implementations of ABE are based on pairing technique. During the past decade, we have witnessed the rapid progress of fast and lightweight computations on pairings, and the core algorithms of ABE can be implemented in milliseconds. The practices reported in [13], [14] also indicate the feasibility on combining NDN with ABE and SDN.

Beyond securing NDN with ABE, we proceed to address the IFA attacks mentioned in Section II. On the one hand, proper use of cryptography can mitigate the scope and effectiveness of IFA attacks. For instance, the cryptographic primitive of attribute-based signature (ABS) can be used to enforce the users in sending interest requests, and we can deliberately choose those ABS schemes in NDN security policy such that the workload of verification process is much lighter than the workload of signing process. To further block IFA attacks, the signatures in interest requests are even enforced to involve some freshness, say containing timestamps, fresh random salts, or solving online puzzles. On the other hand, we have envisioned a lightweight payment prototype for mitigating IFA attacks in NDN by charging virtual money for interest querying. In our study, three pricing functions — linear, asymptotical and exponential — were simulated[1] and we found that the simpler the better: Linear pricing strategy is good enough for ensuring a high ratio of the number of satisfied interests to the total number of interst requests (See Fig.6). In brief, the whole NDN network in this prototype is viewed as an analogy of economic society: each user can request and obtain interested data via paying some virtual money, and the charge automatically contains the cost for content producing, searching/matching, forwarding, and warehousing. As a result, an IFA attacker will be blocked when its virtual money is used out. Meanwhile, each NDN router can earn virtual money carried in the original interest request packet in providing services of interest/contents delivering and caching. In a very abstract perspective, we think the only difference between this analogical NDN society and the real economic society lies in that a digit product in NDN society can be copied almost infinite times with little copying cost, while in real economic society, making two copies of the same kind of products at least means double of the material cost. Therefore, an NDN router, by caching popular contents and providing them to a huge number of down-stream requests, might quickly become a virtual nabobism, even richer than the content producers. This mechanism has the potential to incentive reasonable NDN nodes to request and deliver contents honestly and collaboratively, resulting in a healthy networking "ecological" environment.

V. Conclusion

Although in the named data networking (NDN) architecture, data communications are assumed to be encrypted, the lack of explicit identities with respect to "host" and "network address" make it extremely hard, if not impossible, to apply traditional PKI-based cryptographic primitives in NDN. Thus, this tutorial was intended to propose a framework of using the newly developed identity/attribute-based encryption (IBE/ABE) in NDN, by associating identities and attributes with the proper ingredients of NDN. To further enhance the privacy-preserving capability of NDN, the mechanism of attribute-based routing (ARS) was proposed. Finally, SDN architecture is coupled with NDN for deploying trust-roots (such as PKG). Beyond securing NDN with ABE, a lightweight prototype of virtual payment mechanism was also suggested to mitigate interest flooding attacks (IFA).

Acknowledgment

This work was supported by the National Key Research and Development Program of China (No. 2016YFB0800602), the National Natural Science Foundation of China (NSFC) (Nos. 61502048 and 61632012), and Shandong provincial Key Research and Development Program of China (2018CXGC0701). The third author is also partially supported by JSPS KAKENHI Grant Number JP16K00117, JP15K00028, KDDI Foundation.

References

[1] J. Rexford and C. Dovrolis, "Future Internet Architecture: Clean-Slate Versus Evolutionary Research," *Communications of the Acm*, vol. 53, no. 9, 2010, pp. 36-40.

[2] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan et al., "The Design and Implementation of an Intentional Naming System," *Seventeenth ACM Symposium on Operating Systems Principles*, vol. 33, 1999, pp. 186-201.

[3] N. Mckeown, T. Anderson, H. Balakrishnan et al., "Openflow: Enabling Innovation in Campus Networks," *Acm Sigcomm Computer Communication Review*, vol. 38, no. 2, 2008, pp. 69-74.

[4] V. Jacobson, D. Smetters, J. Thornton, et al., "Networking named content," In Proceedings of the ACM international conference on emerging networking experiments and technologies, pages 112. ACM, 2009.

[5] Named Data Networking: Executive Summary. https://named-data.net/project/execsummary/ (Accessed on April 12, 2018.)

[6] D. Kreutz, F.M.V. Ramos, P. Esteves Verissimo et al., "Software-defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, 2014, pp. 10-13.

[7] E.G. AbdAllah, H.S. Hassanein, and M. Zulkernine, "A Survey of Security Attacks in Information-Centric Networking," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, 2015, pp. 1441-1454.

[8] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, 2018, pp. 566-600.

[9] P. Gasti, G. Tsudik, E. Uzun et al., "DoS & DDoS in Named-Data Networking," *Acm Sigcomm Computer Communication Review*, vol. 44, no. 3, 2013, pp. 66-73.

[10] A. Grusho, N, Grusho, E. Timonina et al., "Five SDN-oriented Directions in Information Security," *IEEE Science and Technology Conference*, 2014, pp. 1-4.

[11] Z. Cao, "New Directions of Modern Cryptography," *CRC Press Inc*, ISBN: 1466501383, 2012, pp. 1-400.

[12] H. Zhu, L. Wang, H. Ahmad et al., "Key-Policy Attribute-Based Encryption With Equality Test in Cloud Computing," *IEEE ACCESS*, vol. 5, 2017, pp. 20428-20439.

[13] S. Salsano, N. Blefari-Melazzi, A. Detti et al., "ICN over SDN and OpenFlow: Architectural Aspects and Experiments on the OFELIA Testbed," *Computer Networks*, vol. 57, no. 16, 2013, pp. 3207-3221.

[14] M. Ion, J. Zhang, and E.M. Schooler, "Toward Content-Centric Privacy in ICN: Attribute-Based Encryption and Routing," *ACM SIGCOMM 2013 Conference on SIGCOMM*, vol. 43, 2013, pp. 513-514.

[15] C. Bian, Z. Zhu, A. Afanasyev et al., "Deploying Key Management on NDN Testbed," *NDN Technical Report NDN-0009*, Revision 2, February, 2013. https://named-data.net/publications/techreports/ (Accessed on April 12, 2018.)

[1] Our simulations were carried out by running ndnSIM (http://ndnsim.net/2.3/index.html) at a Windows 7 desktop with 2.93GHz CPU and 2GB memory. The simulations were set as follows: (1) The prepayment of an interest request: 100, the maximum number of PIT items: 1000; (2) A random generated topology consisting of 167 nodes, among which 15% were randomly set as malicious.

Licheng Wang received his B.S. degree in engineering from Northwest Normal University in 1995, M.S. degree in mathematics from Nanjing University in 2001, and Ph.D. degree in engineering from Shanghai Jiaotong University in 2007, respectively. He is currently an associate professor in Beijing University of Posts and Telecommunications. His current research interests are cryptography, blockchain and future internet architecture.

Zonghua Zhang is now with IMT Lille Douai, Institut Mines-Télécom. He holds a Ph.D. degree (JAIST, Japan) in information science, and a HDR diploma (UPMC, France) in computer science. His research topics cover anomaly detection, network forensics, trust and reputation management, and security protocols. The current target scenarios include Software-Defined Networking (SDN), Network Functions Virtualization (NFV), and Cyber-Physical Systems (CPS).

Mianxiong Dong received his B.S., M.S., and Ph.D. in computer science and engineering from the University of Aizu. He is currently an associate professor in the Department of Information and Electronic Engineering at Muroran Institute of Technology. He currently serves as an Editor for IEEE Transactions on Green Communications and Networking (TGCN), IEEE Communications Surveys & Tutorials, IEEE Network, IEEE Wireless Communications Letters, IEEE Networking Letters, IEEE Cloud Computing, and IEEE Access.

Lihua Wang received her B.S. degree from Northeast Normal University, M.S. degree in mathematics from Harbin Institute of Technology, China, and Ph.D. degree in engineering from University of Tsukuba, Japan, respectively. She is currently an associate professor in Graduate School of Engineering, Kobe University, and serves as an Invited Advisor for National Institute of Information and Communications Technology, Japan. Her research interests are cryptography and privacy-preserving data mining.

Zhenfu Cao received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from the Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively. He is currently a Distinguished Professor with East China Normal University, China, and one of the winner of National Outstanding Youth Funding. His research interests mainly include number theory, cryptography, and information security.

Yixian Wang received the M.S. degree in applied mathematics in 1986 and the Ph.D. degree in electronics and communication systems in 1988 from Beijing University of Posts and Telecommunications (BUPT) . He is now a Yangtze River Scholar Program professor, and one of the winner of National Outstanding Youth Funding. He majors in coding and cryptography, information and network security, signal and information processing.