Content Name Privacy in Tactical Named Data Networking

Nikolai Leshov, Muhammad Azfar Yaqub, Muhammad Toaha Raza Khan, Sungwon Lee, and Dongkyun Kim
School of Computer Science & Engineering, Kyungpook National University, Daegu, Republic of Korea
Email: {nikolai, swlee}@monet.knu.ac.kr, {yaqub, toaha, dongkyun}@knu.ac.kr

***Abstract*—Named Data Networking architecture has significant benefits in military applications, such as in-network caching, security, support of mobile nodes, etc. Content security is provided using signature of the content producer and encryption, however, the content name is visible to everyone that can have sensitive information. Leakage of such information is not desirable in military applications. Therefore, we propose a Content Name Privacy (CoNaP) scheme. CoNaP ensures that the adversary is not able to obtain any information from the content name. Simulations show that CoNaP satisfies more Interest packets with less delay as compared to the recent forwarding solutions.**

***Keywords*—Named Data Networking; Tactical Network; Network Security; Asymmetric Encryption; Symmetric Encryption**

I. Introduction

Named Data Networking (NDN) [1] aims to provide efficient and secure content retrieval in a highly dynamic and errant network conditions. These network conditions are frequently observed in tactical networks, making NDN a well-suited architecture for tactile applications. Compared to NDN the TCP/IP based architecture hardly meets the requirements of tactical network. Additionally, the benefits of NDN are in line with the requirements of a tactical network, for example NDN provides in-network caching, security, support of mobile nodes, etc. [2].

NDN is a new network architecture that focuses on locating content instead of its location. To enable this communication, three data structures, namely Content Store (CS), Pending Interest Table (PIT), Forwarding Information Based (FIB), and a forwarding strategy are introduced. To retrieve a desired content, the consumer does not need to know where content is located/stored. Consumer simply sends an Interest packet with the name of desired content. The producer replies to the Interest with a Data packet that contains the requested content. Every intermediate node (IN) that receives the Interest packet checks its CS data structure for the requested name content. If CS does not have needed content, IN simply creates a new entry (name, incoming interface) in its PIT data structure and forwards the Interest packet to next hop. A node selects its next hop by matching the name with the entries in its FIB data structure. The content provider, upon receiving the Interest packet, replies with same name Data packet. The Data packet is forwarded towards the consumer by those INs that have a corresponding PIT entry.

This research was supported by the MSIP (Ministry of Science, ICT Future Planning), Korea, under the C-ITRC (Convergence Information Technology Research Center) support program (NIPA-2014-H0401-14-1004) supervised by the NIPA (National IT Industry Promotion Agency).

NDN forwards the content based on application-defined names. A hierarchical naming structure is followed that is semantically meaningful and consists of sequence of variable length components. An example of a requested content is '/producer_prefix/app/content_name'. Here, each portion of the name represents different characteristics of the content and can contain sensitive information of producer/consumer, such as producer type, service type, content format, etc. An adversary can easily eavesdrop and extracts information of consumer/producer from the name. Therefore, to preserve packet forwarding and prevent adversary's eavesdropping, content name should be shared only with trusted IN. In case of tactical network, leakage of any information can be fatal [3].

Therefore, in this paper we propose a Content Name based Privacy (CoNaP) scheme for the tactile named data networks. The objective of CoNaP is twofold. Firstly, symmetric keys are used by each consumer to encrypt the name part of the Interest packet. Secondly, in order to maintain the name-based mechanism of NDN, a three-way handshake mechanism is introduced. The handshake mechanism allows the consumer and IN to exchange the symmetric key. Signed Interest packets are used for authenticating consumer and IN- a signature is appended in the Interest packet by the consumer/IN. Thus, even though the Interest packet is eavesdropped by an adversary, no useful information is obtained.

The remainder of paper is organized as follows. Section II presents the related work. The proposed CoNaP scheme is presented in Section III. Evaluation and results are shown in section IV. Finally, a brief conclusion is given in Section V.

II. Related Work

In this section we present recent works that employ name-based security.

Authors in [4] proposed a security mechanism using signed Interest, i.e., before sending an Interest packet, consumer appends his signature to the name. Thus, final name has form /app/fixture/command/signature. Signed Interest is used in smart home environment, when one fixture (producer), for example lighting control, needs to authenticate sender's command (consumer). Fixture can authenticate consumer through standard NDN signature verification process.

One of first work where content name was hidden was proposed in [5]. ANDaNA is an anti-censorship protocol, which based on onion routing. Every packet is encapsulated in layers of encryption. Consumer encrypts Interest by corresponding anonymizing routers' (AR) public keys. On the way back, content packet is encrypted by each AR using symmetric keys,

which were shared before communication starts. ANDaNA requires additional latency and computational capacity due to encryption/decryption operations. Also, since packet is hidden only on part of path, such kind of approach cannot be widely used for another tasks.

Another anti-censorship protocol was proposed by Reza Tourani et al. in [6]. Authors assume that packet filtering based on content name. To avoid filtering, mechanism hides content name by using Huffman coding. Anonymizer generates Huffman tree on consumer's membership request. After receiving Huffman tree encrypted by consumer's public key, consumer encodes desired content name by corresponding Huffman tree. To enable forwarding, full name cannot be encoded, at least anonymizer's prefix still should be open. Also, Huffman coding is prone to chosen-plaintext attack [7]. Therefore, using Huffman coding to hide sensitive information becomes questionable. Moreover, content caching on IN is disable because every consumer uses its own Huffman tree.

In [8], authors provide an overview on VPN-like mechanism for NDN. Proposed mechanism requires new type of entity gateway. Gateways are located on consumer side and producer side. Gateway encrypts/decrypts and encapsulates/decapsulate packets. To preserve in-network caching, authors assume gateways use the same set of keys. That means if adversary gains access to one of the gateways, adversary will gain access to the entire network. Additionally, such approach brings new challenge of keys revocation. The authors also mentioned the issue of name privacy, but did not propose any specific solution.

Another VPN-like approach was proposed in [9]. The authors proposed that consumer side gateway includes symmetric key in Interest which is used for content packet encryption on producer side gateway. Caching on IN is disabled and forwarding requires an open portion of name, which might be not desirable in tactical network.

III. Content Name Privacy

We consider a tactical network scenario as shown in Figure 1. The network topology consists of a General Headquarter which is the content producer, a Command and Control Center which operates as an IN between the end devices. The end devices can be military personnel, vehicles, tanks, etc. that are deployed in a certain terrain. General Headquarter and Command and Control Center are connected through satellite. Command and Control Center and end devices communicate through wireless link.

A. Overview

Traditionally, encryption is used to hide information, however, NDN uses names in its forwarding mechanism. In CoNaP, we use symmetric encryption to hide name. Before sending Interest, consumer encrypts desired content name. As stated earlier the name-based forwarding of NDN requires the name to be open. Therefore, to obtain the symmetric key used by the consumer, CoNaP initiates a three-way handshake at the IN. Additionally, the consumer and IN use signed Interest to validate their authenticity. The signed Interest allows the both the consumer and IN to authenticate each other.

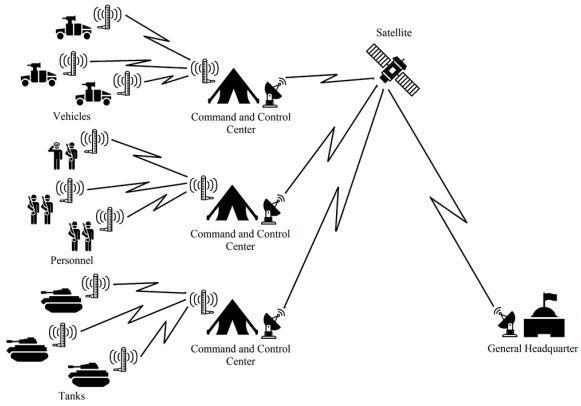

Fig. 1: Considered Scenario

B. Working Principle

Initially, all nodes follow the standard NDN bootstrapping, where nodes obtain trust anchor, certificates, generate private/public keys, and learn the trust policy. In addition, CoNaP allows each node to generate symmetric keys for each content name. Symmetric key can be generated to a specific content name (e.g. /producer_prefix/app/content_name) or to a prefix (e.g. /producer_prefix/app/). In case of last, all content name after prefix will be encrypted by one symmetric key. It is worth noting that symmetric keys are stored and named like any another content packet.

The namespace consists of four parts, i.e., encrypted content name, label "encrypted_by", name of symmetric key, and signature of consumer. An example name has the form, /encrypted_content_name/encrypted_by/key_name/signature. The "encrypted_content_name" is the encrypted content name, the label "encrypted_by", and "key_name" provides the name of the corresponding symmetric key, the "signature" is added by the consumer to authenticate the Interest name.

The consumer creates the encrypted name and broadcasts the Interest packet. The IN first checks the authenticity of the incoming Interest packet. KeyDigest is extracted from the signature_info field of Interest packet that has the location of certificate. This certificate is used to verify the signature of the consumer. In case of authentic request, IN initiates the three-way handshake mechanism to decrypt the name.

First, IN sends an Interest packet with the extracted "key_name" and IN signature in the name, i.e., "/key_name/signature". This allows the consumer to verify the authenticity of the IN. Next, if the signature is verified, consumer replies with the encrypted symmetric key in the Data Packet. The payload contains the encrypted "key_name" symmetric key. Public key of the IN is used to encrypt the symmetric key. Lastly, the IN verifies the authenticity of the received data packet and uses its private key to decrypt the symmetric key. This allows the content name to be decrypted and the NDN forwarding mechanism is proceeded. In case content is not located in the CS of IN, the encrypted name and signed interest is further forwarded. Thus, forwarding of Interest packet and the symmetric key of the consumer is repeated at each hop until the Interest packet reaches the producer. The content provider replies with the Data packet

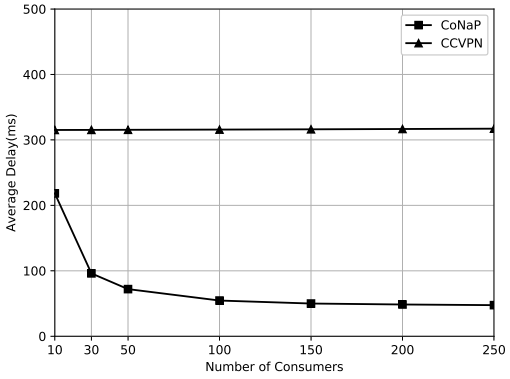

Fig. 2: Interest Satisfaction Delay

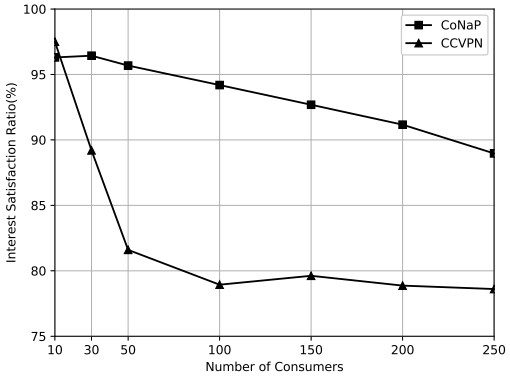

Fig. 3: Interest Satisfaction Ratio

with the same encrypted name. On the reverse path, only those IN(s) that have a corresponding PIT entry help in relaying the Data packet towards the consumer.

IV. Performance Evaluation

We simulated our proposed CoNaP using ndnSIM which is based on NS-3 [10]. To assess the performance, we use topology of network based on Figure 1. Network topology consists tree groups of consumers. Each group of consumers connected to corresponding IN wirelessly. Each IN connected to producer through satellite. Due to wireless characteristic of communication, we set up 5% of packet loss for satellite communication and 0.1% of packet loss for wireless communication between consumers and IN. We ran simulation with different number of consumers started from 10 nodes and increased up to 250 nodes. Each consumer sends one Interest for the same content. For performance comparison CCVPN [9] scheme is implemented in the same network setup.

To measure and compare performance of CoNaP, we utilized two performance parameters. Interest satisfaction delay (ISD) is a time taken to send an Interest packet and retrieve a corresponding Data packet. Interest satisfaction ratio (ISR) is total received Data packets to total sent Interest packets.

First, we examine the Interest satisfaction delay of CCVPN and CoNaP as shown in Figure 2. The proposed CoNaP shows less ISD then CCVPN since CoNaP allows in-network caching of data, i.e., only first Interest packet is forwarded to the producer and the remaining requests are satisfied by IN(s). On the other hand, in CCVPN in-network caching is disabled, thus, each Interest packet can only be satisfied by the Producer.

Figure 3 shows the Interest satisfaction ratio for both schemes. In CCVPN each Interest packet must be forwarded to the Producer, thus, higher probability to have losses. On the other hand, CoNaP allows in-network caching at INs, thus, future request for the same content can be satisfied by IN itself.

V. Conclusion

In this paper, we presented CoNaP that is designed to provide content name privacy in NDN based tactical networks. CoNaP allows secure sharing of content name among trusted nodes. CoNaP does not require any additional infrastructure, like crypto router, anonymizer, etc. or significant change in architecture. Moreover, each content name is encrypted with separate symmetric key, so even if the adversary gets hold of the symmetric key, it can only decrypt one content name. Simulation results show that CoNaP has high ISR and less ISD compared to the recently proposed CCVN scheme.

References

[1] L. Zhang, et al., "Named data networking", SIGCOMM Comput. Commun. Rev. 44, 3 (July 2014), pp. 66-73.

[2] M. A. Yaqub, et. al. "Interest forwarding in vehicular information centric networks: a survey" In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC '16), pp. 724-729, Pisa, Italy, 2016.

[3] J. Burke, A. Afanasyev, T. Refaei and L. Zhang, "NDN Impact on Tactical Application Development," 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, 2018, pp. 640-646.

[4] J. Bruke, P. Gasti, N. Nathan and G. Tsudik, "Securing Instrumented Environments Over Content-Centric Networking: the case of lighting control and NDN" 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Turin, 2013, pp. 394-398.

[5] S. DiBenedetto, P. Gasti, G. Tsudik, E. Uzun, "ANDaNA: Anonymous Named Data Networking Application" in Proceedings of the Network and Distributed System Security Symposium, NDSS, San Diego, California, USA, January 2012.

[6] R. Tourani, S. Misra, J. Kliewer, S. Ortegel, and T. Mick, "Catch Me If You Can: A Practical Framework to Evade Censorship in Information-Centric Networks." In Proceedings of the 2nd ACM Conference on Information-Centric Networking. ACM, New York, NY, USA, 2015, pp. 167-176.

[7] G. Jakimoski and K. P. Subbalakshmi, "Cryptanalysis of Some Multimedia Encryption Schemes," in IEEE Transactions on Multimedia, vol. 10, no. 3, pp. 330-338, April 2008.

[8] C. Partridge, S. Nelson, and D. Kong, "Realizing a virtual private network using named data networking." In Proceedings of the 4th ACM Conference on Information-Centric Networking. ACM, New York, NY, USA, 2017, pp. 156-162.

[9] I. O. Nunes, G. Tsudik and C. A. Wood, "Namespace Tunnels in Content-Centric Networks," 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017, pp. 35-42.

[10] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the Evolution of ndnSIM: an Open-Source Simulator for NDN Experimentation." SIGCOMM Comput. Commun. Rev. 47, 3, September 2017, pp. 19-33.