Auto-configurable Security Mechanism for NFV

HyunJin Kim[1], PyungKoo Park[2], Jaecheol Ryou[1]
[1] Department of Computer Engineering, Chungnam National University
99, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea
[e-mail: be.successor@gmail.com]
[2] Network SW Research section, ETRI
218, Gajeong-ro, Yuseong-gu, Daejeon, Republic of Korea
[e-mail: parkpk@etri.re.kr]
*Corresponding author: Jaecheol Ryou

Received October 9, 2017; revised January 15, 2018; accepted February 12, 2018; published February 28, 2018

Abstract

Recently, NFV has attracted attention as a next-generation network virtualization technology for hardware -independent and efficient utilization of resources. NFV is a technology that not only virtualize computing, server, storage, network resources based on cloud computing but also connect Multi-Tenant of VNFs, a software network function. Therefore, it is possible to reduce the cost for constructing a physical network and to construct a logical network quickly by using NFV. However, in NFV, when a new VNF is added to a running Tenant, authentication between VNFs is not performed. Because of this problem, it is impossible to identify the presence of Fake-VNF in the tenant. Such a problem can cause an access from malicious attacker to one of VNFs in tenant as well as other VNFs in the tenant, disabling the NFV environment. In this paper, we propose Auto-configurable Security Mechanism in NFV including authentication between tenant-internal VNFs, and enforcement mechanism of security policy for traffic control between VNFs. This proposal not only authenticate identification of VNF when the VNF is registered, but also apply the security policy automatically to prevent malicious behavior in the tenant. Therefore, we can establish an independent communication channel for VNFs and guarantee a secure NFV environment.

Keywords: NFV, VNF, Authentication, Hash-Chain, ASMN , Sec-catalog, Sec-EM

A preliminary version of this paper was presented at APIC-IST 2017, and was selected as an outstanding paper. This work has been supported by the National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

http://doi.org/10.3837/tiis.2018.02.014 **ISSN : 1976-7277**

1. Introduction

As the interest and importance of the Internet increase, network traffic and devices are increasing and network operation is required to be advanced. Network operators in each country are focusing to NFV(Network Function Virtualization) with next-generation network technology and 5G core technology. NFV is a technology that seperates software functions from hardware-dependent network devices and provides services using infrastructure based on general-purpose server equipment. Service providers can reduce costs by simplifying infrastructure deployment and management by providing networking capabilities with virtualization. In addition, CAPEX and OPEX can be saved by managing resources efficiently and centrally [1].

However as virtualization technology becomes commercialized, it needs to be able to control virtual networks quickly. This is because logical networks can be built without physical configuration. So, the virtual networks change faster than traditional networks. And the ability for automatic configuration of multiple virtualized devices are required. Because if people control each tenant changing dynamically, the labor and cost of it will increase. Also in order to identify a malicious VNF, authentication function between VNFs and traffic control function of malicious VNFs are needed [2].

The proposed Auto-configurable Security Mechanism in NFV(ASMN) performs authentication and secure communication between VNFs using hash-chain of VNF image. Also it controls a VNF's abnormal traffic by setting security policy. The composition of this paper is as follow. Section 2 introduces the technology related to ASMN in this paper. Section 3 describes the structure and operation of ASMN. It explains the technical features of ASMN. In Section 4, we measure the hash generation time of the VNF image of ASMN, the packet transmission rate and the CPU usage rate according to the encrypted communication. And we confirtm the defense against flooding attack through VNF traffic control.

2. Related Work

2.1 Network Function Visualization

NFV(Network Functions Visualization) is a next-generation network technology that reflects the increasing demands of Internet devices. NFV uses VNF(Virtual Network Functions), which is implemented to separate and control various functions within the network equipment, and to control and manage them in software. Virtualization of physical network equipment's function is performed by using Virtual Machine(VM) server or hardware with general-purpose processor. Implementation methods of NFV is various, but NFV seperates the functions within the network equipment into servers, mass storage devices. Using NFV technology can reduce capital expenditure(CAPEX) and operating expense(OPEX) due to network equipment cost and power loss reduction. Also, it has the effect of shortening the time required for inputting the new network service into the market, increasing the investment cost recovery, flexible service development, and ease of scale management [3,4].

2.2 Authentication Protocol

In NFV environment, when a malicious attacker accesses the VM, the attack will be proliferated to the damaged VM as well as the entire VMs in tenant. Then, the attack can lead to critical information leakage in the VM. Therefore, an authentication protocol identifying the reliability of VM is needed in NFV environment. The authentication protocols that typically used in a network are as follows.

PSK(Pre-shared Key) is a network authentication protocol that does not use an authentication server. Before using, an user distributes the PSK to both ends of the network service through the secure channel, and uses this process to authenticate. Depending on the length, there are a 56-bit DES (Data Encryption Standard) algorithm, a 168-bit 3-DES algorithm, and a 128-bit or 256-bit AES(Advanced Encryption Standard) algorithm for PSK authentication [5].

Kerberos is a mechanism for authenticating users on a network. The Kerberos system authenticate the users using a symmetric key method, which is based on the reliable trusted third party and is the most widely used method on a network architecture. The Kerberos system includes both a function of key distribution and an authentication. The Kerberos system uses UDP-based messages and uses port 88. In the authentication procedure, the user receives a Ticket Granting Ticket (TGT) from the authentication server after authentication about the user. Then the user transmits a TGT and a user's ID to the TSG (Ticket Granting Server). After that, the user submits the Session Granting Ticket (SGT) to the desire server and server allow to access [6,7]. However, the Kerberos system must have a reliable authentication server and a ticket issuing server. It is not possible to use a Kerberos system for NFV because it is difficult to obtain a reliable server in a virtual environment where identification is unclear.

2.3 Hash-Chain

Hash-function maps a data having arbitrary length to data having fixed length. And since it is not a single function, it is impossible to reverse the operation. So though someone knows the hash value, it can not find the input of the hash function. Also, it does not guarantee that the s ame input values are the same even if they hav the same hash value. Even if only one bit of t he original input is changed, the hash value varies greatly due to the presence of the hash func tion. There are many types of hash functions such as MD5, CRC32, SHA-type [8].

Hash-Chain is a computation method of hash value continuously using arbitrary values 'se ed' set by the client. That is, to create a hash chain having length *n*, *x(seed)* is used as the inp ut of the hash function *h(x)* [9,10]. Through this process repeatedly, root value $h^{n+1}(x)$ can be calculated. The hash-function could not be inverted. Therefore, when a program that generate s a password as a hash-chain sends the hash-chain to the server, the attacker can not calculate a $h^{n-1}(x)$ even if it knows $h^{n}(x)$ by eavesdropping on the transmission process. By using this se cure characteristic of the hash, a hash-chain of One-Time Password is generated in the proces s of client-server authentication [11,12].

2.4 Malicious Behavior

Internet availability is a most important issue because the most of the institution use the servi ce by using the Internet. However, it is difficult to depend the DDoS(Distributed Denial of Se rvice) which is a typical representative service distruption attack because the attack exploits v ulnerability in design of a protocol [13]. DoS(Denial of Service) is an attack that attacker depl etes the resources of the system and paralyzes system [14]. On the other hand, DDoS is an att ack that the multiple attacker placed in a distributed location simultaneously DoS attack to th e target system [15]. Typical DDoS attacks are bandwidth consuming attack, resource consuming attack and application attack. Bandwidth consuming attack is an attack that an attacker uses a large number of zombie agents to generates a large number of packes, exceeding the limit of the target system's network bandwidth. The attack can causes a connection failure to other systems in the same network. And UDP flooding which tranmits a large number of UDP packes, and ICMP flooding which uses a large number of ICMP packets are belongs to the bandwidth consuming attack [16]. Resource consuming attack is an attack that an attacker increase the CPU load of a target system by increasing packet throughput using TCP packet. The attack doess not increase the bps(bit per seconds), but increases the system overhead due to an increases in pps(packet per second). The SYN flooding attack which depletes a resource using SYN packet is belongs to the resource consuming attack [17,18]. In the virtual environment, the attacker can exhaust the bandwidth and the resource of network to paralyze the entire network.

3. Trust Mechanism in NFV using Hash-Chain

The ASMN(Auto-configurable Security Mechanism in NFV) proposed in this paper is a mechanism for verifying and monitoring the authorized network traffic between the VNFs in the tenant in the NFV environment. The structure of ASMN is shown in **Fig. 1**.

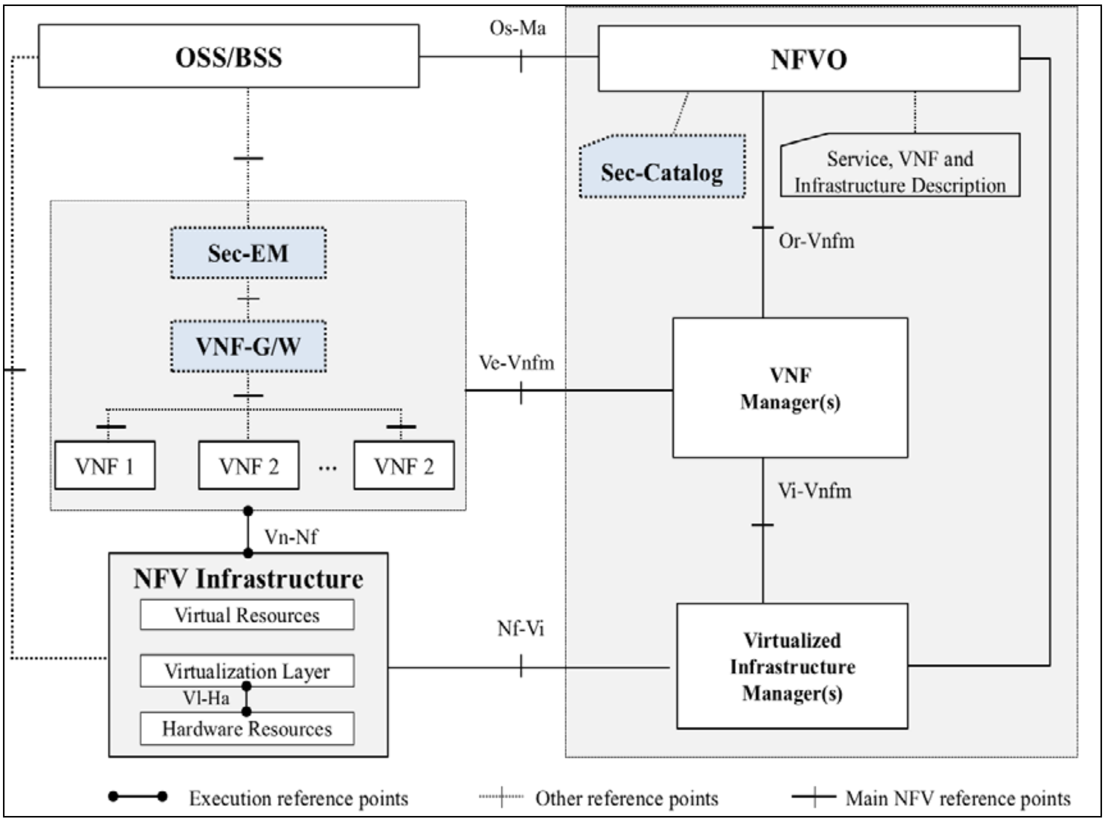

Fig. 1. The architecture of ASMN

ASMN is consisted of 3-Steps. In the 1st step, it is possible to identify the Fake VNF by performing authentication between the VMs in the tenant using the hash-chain of the VNF image. In the 2nd step, secure communication is performed between VNFs using secret key encryption based on hash-chain. Finally, in the 3rd step, 'Sec-catalog' is used to set a security policy to control an abnormal traffic between VNFs.

3.1 Sec-Catalog

Sec-catalog is used to set the security policy for traffic between VNFs. Based on whitelist, tra ffic matching with the information in the catalog is allowed communication between VNFs. There are protocol, port number, ingress policing rate, and ingress policing burst in the Sec-c atalog. Traffic that does not match the information in Sec-catalog is considered an abnormal t raffic. During the VNF Instantiation process, the Sec-catalog is registered at the same time th at VNFD(VNF Descriptor) is registered in the catalog. The security policy configured in Sec-catalog is applied to Phase 3: VNF-G/W, which is introduced in Section 3.3, to control the tra ffic between VNFs.

3.2 Phase 1 : Authentication between VNFs using Hash-Chain

ASMN performs hash-chain based authentication between Sec-EM and VNF, and authentication between VNFs to identify Fake-VNF. The hash-chain used for each authentication is created using VNF image, and the generation formula is as follows. VNF_{ID} is the VNF in the Tenant. And the Sec-EM manage the $ID = Tenant\_ID \oplus VNF\ ID \oplus Instance\_ID \oplus Nonce$ for VNF management.

For any $n > 0$

$$Hash^2(VNF_{ID}) = Hash(Hash(VNF_{ID})) \tag{1}$$

$$Hash^n(VNF_{ID}) = Hash(Hash^{n-1}(VNF_{ID})) \tag{2}$$

VIM generates the hash-chain of the VNF image, and VIM and Sec-EM share the hash value of VNF after image on-boarding and instantiation. When the VNF is running, the hash value of the image will be changed. So the hash-chain is periodically updated such as (3).

$$E_{Hash^{n-1}(VNF)}\{Hash^n(VNF_{ID})\} \tag{3}$$

To share the updated hash-chain with Sec-EM, updated hash-chain is shared using symmetric encryption algorithm with the previous hash-chain as an encryption key. Then VNF image share their updated hash-chain via VNFM form VIM.

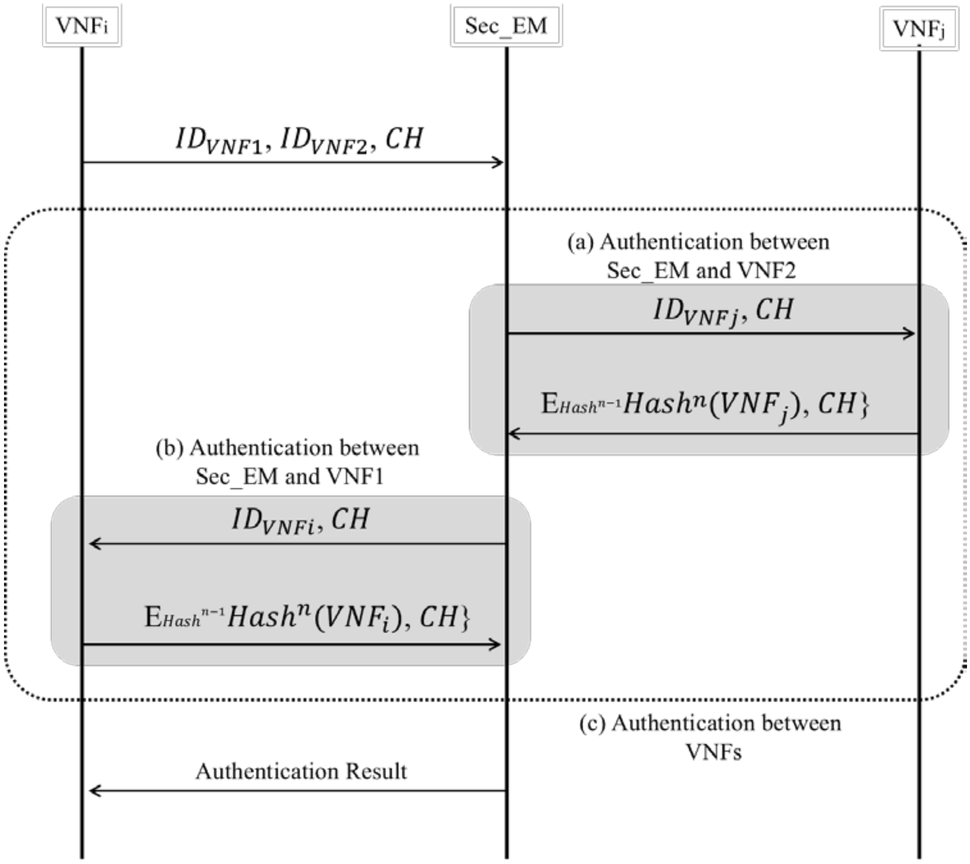

Fig. 2. Authentication Process between VNFs

Fig. 2 shows the authentication process of VNF using hash-chain of the VNF image. Authentication proceeds with two VNFs that want to communicate with Sec-EM. When VNF_1 want to communicate with VNF_2, it requests Sec-EM to verify the reliability of VNF_2 using (2). Since the *n*-th hash-chain in (a) is encrypted with the *n-1* th hash-chain, it can not be decrypted unless the hash-chain is updated regularly. When authentication for VNF_2 is completed, VNF_2 also requests confirmation of the reliability of VNF_1 to Sec-EM as shown in (b). Through the above process, it is possible to perform authentication between VNFs as well as between Sec-EM and VNF.

3.3 Phase 2 : Secure Communication between VNFs

After completing the VNF authentication process in Section 3.1, ASMN ready to secure communication using symmetric key encryption algorithm. The following is the process of sharing the encryption key based on the Diffie-Hellman(D-H) algorithm using the hash-chain. '*i*' and '*j*' represent the IDs of the VNF s to be communicated. '*p*' is a sufficiently large prime number over *300*, and '*q*' is an integer from *1* to *p-1*. $Hash^n(VNFi)$, $Hash^n(VNFj)$, the hash-chains of VNFs are integers greater than 100 digits. [19]

For any $n > 0$

$$R_i = q^{Hash^n(VNF_i)} \bmod p \tag{4}$$

$$R_j = q^{Hash^n(VNF_j)} \bmod p \quad (5)$$

$$K_{VNF\_ij} = R_i^{Hash^n(VNF_j)} \bmod p = \{q^{HashN(VNF_i)}\}^{Hash^n(VNF_j)} \bmod p \quad (6)$$

$$K_{VNF\_ij} = R_j^{Hash^n(VNF_i)} \bmod p = \{q^{HashN(VNF_j)}\}^{Hash^n(VNF_i)} \bmod p \quad (7)$$

The Seed of D-H uses hash-chain of each VNF image. Each VNF receives p and q from Sec-EM. When VNF_i and VNF_j communicate, R_i and R_j are calculated using (4) and (5). Then, VNF_i and VNF_j exchanges R_i and R_j with each other to obtain (6) and (7). That is, VNF shares q^a and q^b to obtain q^{ab}. At this time, because p is sufficiently large, the attacker could not find K_{VNF_ij} through $q^{Hash^n(VNF_i)}$ or $q^{Hash^n(VNF_j)}$ even if he tries to find the key to decrypt an encrypted message. Through this process, VNF_i and VNF_j ensure secure communication using K_{VNF_ij}.

3.4 Phase 3 : Traffic Control between VNFs

ASMN controls the traffic between VNFs using Sec-catalog and VNF-G/W of 3.1 after encrypted communication of 3.3.

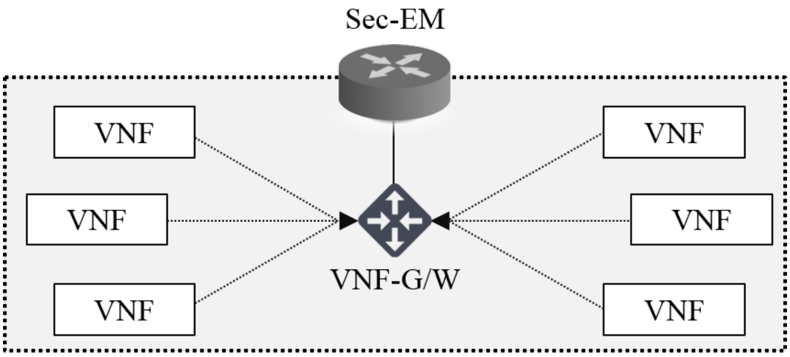

Fig. 3. Placement of VNF-G/W

Fig. 3 shows the placement of VNF-G/W. VNF-G/W is a gateway implemented by VNF, and it is located between VNFs in tenant to control the traffic between VNFs.

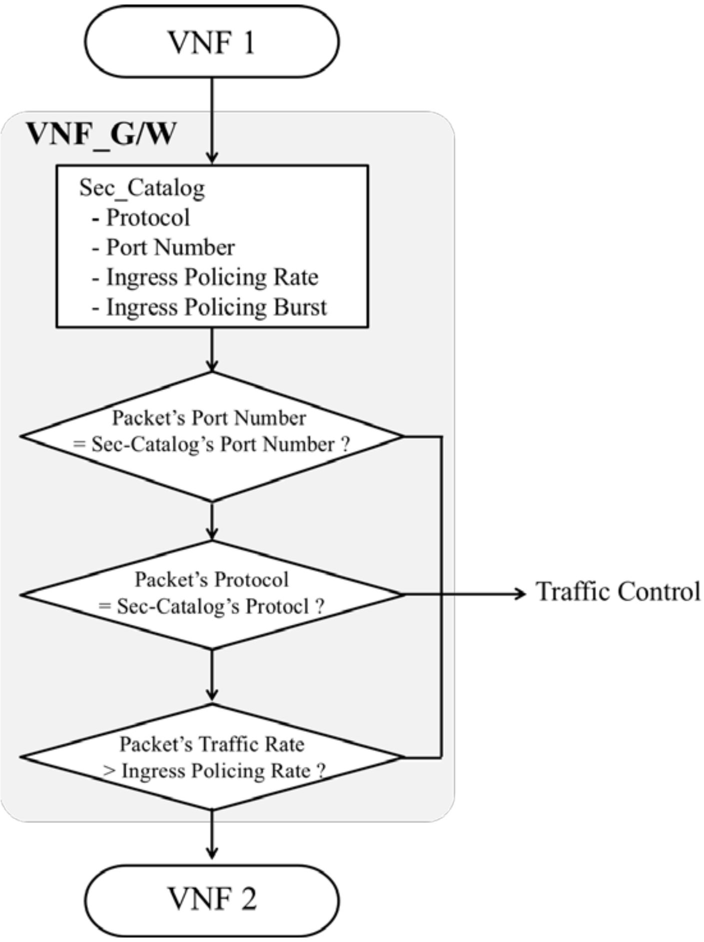

Fig. 4. Traffic Control of VNF-G/W

Fig. 4 shows the process of VNF-G/W receiving traffic information in Sec-catalog and controlling traffic transmitted between VNFs. When the Sec-catalog is reflected in VNF-G/W, the traffic different from the information configured in the Sec-catalog can be regarded as a threat and the QoS(Quality of Service) level can be lowered and the bandwidth of the transmission traffic can be lowered. We can detect the abnormal traffic patterns between VNFs using a traffic control technique and prevent an accident for information leakage. For example, when an attacker transmits a large volume of traffic from VNF_1 to VNF_2 in order to bring down a running server in VNF_2 as a Flooding attack, the traffic control can prevent accidents. In addition, when important information including personal ID or Address is stored in the server using the VNF, it is possible to prevent information leakage by detecting a flow of large amount of traffic from the corresponding VNF to the outside and analyzing a user's abnormal patterns like transferring a data at dawn

4. Implementation and evaluation

For performance evaluation of ASMN, we configured VNF-G/W and VNF Client, VNF Server in one tenant.

4.1 Time required for authentication between VNFs using Hash-Chain

Proposed mechanism contains a process verifying the integrity of VNF image using hash-chain. We calculate the time required for authentication between VNFs using hash-chain and compare the time by size of VNF image.

Table 1. VNF Image Size

	Size
VNF_1	2.55 GB
VNF_2	3.72 GB
VNF_3	1.42 GB
VNF_4	3.14 GB
VNF_5	3.91 GB
VNF_6	2.55 GB

We prepare the 6 VNF images like **Table 1**. The hash algorithms to generate hash-chain are CRC32, MD5, SHA-1.

Table 2. Time required for extracting a hash value of VNF image

	CRC32	**MD5**	**SHA-1**
VNF_1 vs VNF_2	16.2 s	17.1 s	17.5 s
VNF_3 vs VNF_4	18.5 s	19.4 s	20.1 s
VNF_5 vs VNF_6	16.2 s	17.3 s	18.3 s

The time required to generate and compare the hash value of the VNF image is about 15-20 seconds, depending on the size of the VNF image. Since the generation and verification of a hash-chain implement at VNF restart process and VNF registration process in the tenant, it is possible to perform authentication between VNFs in same tenant.

4.2 Packet transmission rate between VNFs

We analyze the packet transmission rate in ASMN. The data for the test is as follows.

Table 3. ASMN Traffic Input Rate

ICMP traffic	**TCP traffic**	**UDP traffic**
64 byte 4096 byte	64 byte 4096 byte	64 byte 4096 byte

The client generates random packets of 64 bytes and 4,096 bytes for the ICMP protocol, and transmits the packets to the server for measuring the RTT(Round-Trip-Time) between VNFs in the same tenant using ASMN.

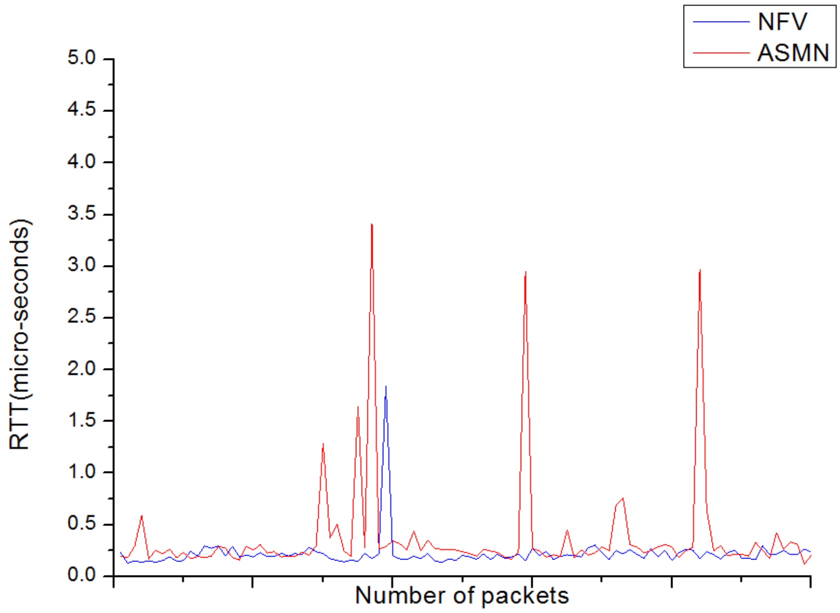

Fig. 5. Test for ICMP RTT

As shown in **Fig. 5**, increase of RTT is less than 5 mirco-seconds. So, we confirm that we provide the service without performance degradation because of ASMN within micro-second s.

4.3 Total CPU utilization for secure communication

We transmit random packets for 25 seconds to check the change of CPU usage for ICMP, TCP, and UDP protocols in ASMN.

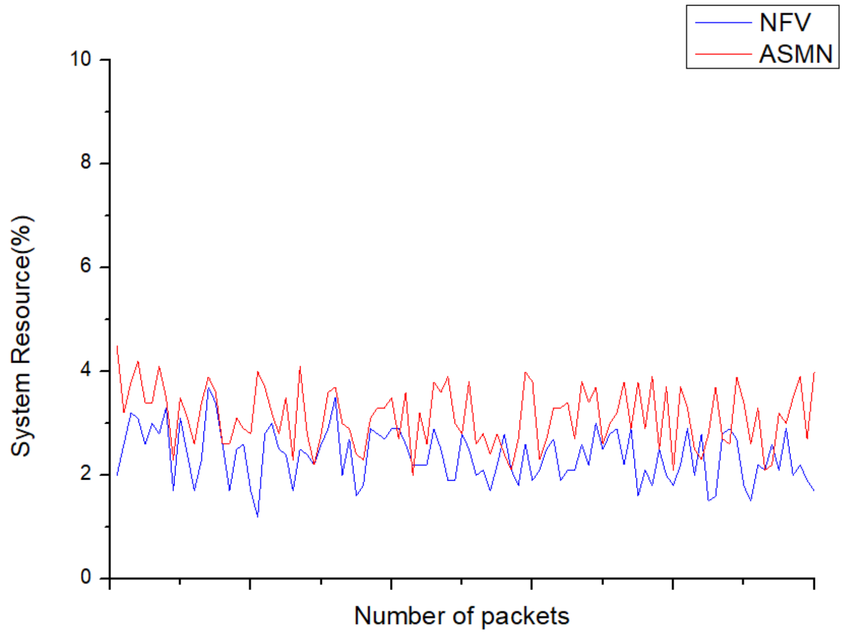

Fig. 6. CPU Utilization on ICMP traffic

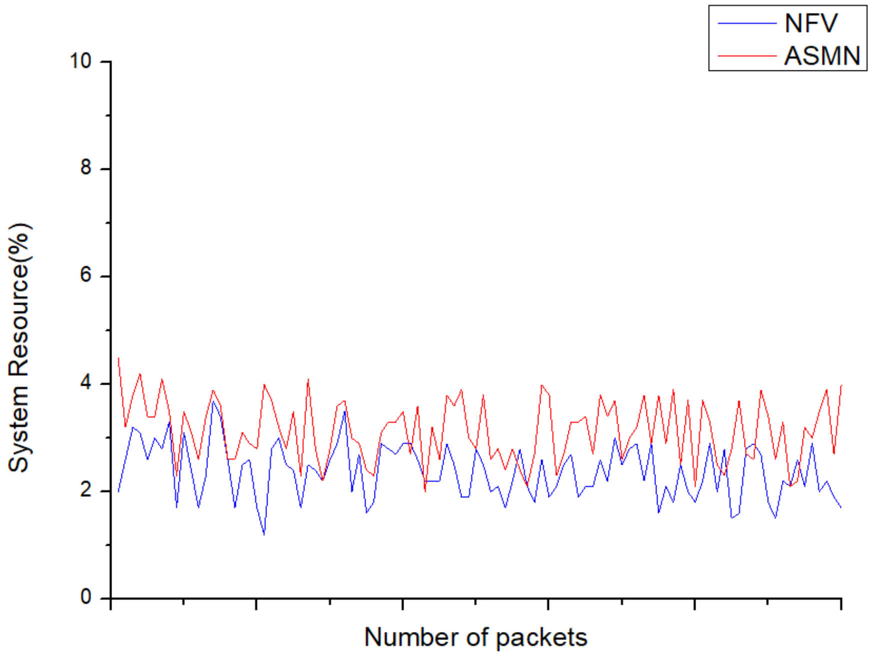

Fig. 7. CPU Utilization on TCP traffic

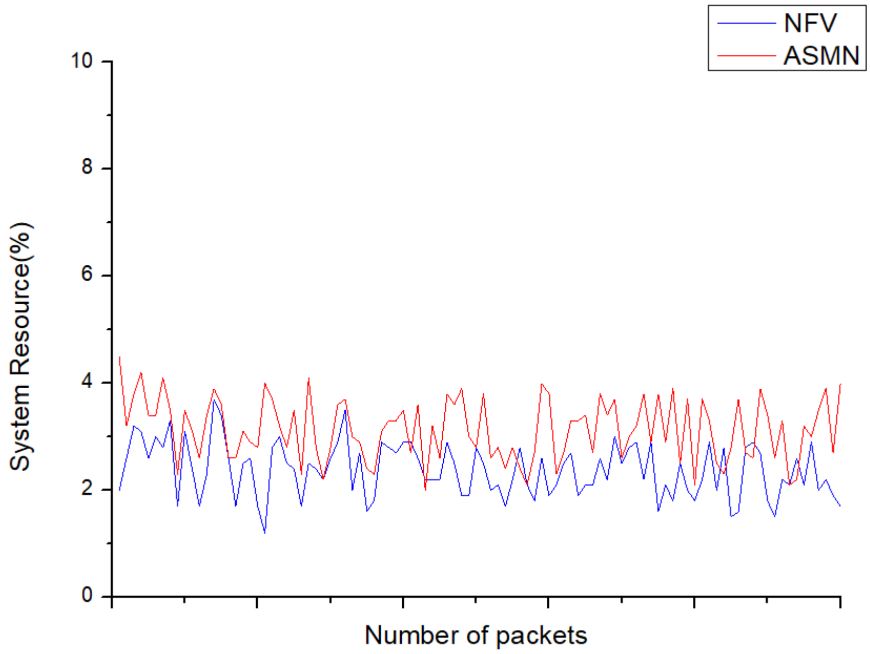

Fig. 8. CPU Utilization on UDP traffic

Like **Fig. 6, 7, 8**, the total CPU utilization in ASMN has increased to less than 1% for the ICMP, TCP, UDP in normal NFV environment. Therefore, we confirmed that there is no performance degradation on VNF to VNF communication within micro-seconds.

4.4 Flooding attack defense using traffic control

The ASMN include the defense mechanism against the malicious traffic from VNFs. Typical malicious attack using traffic from VNFs is flooding attack. The data for defense test is as follows.

Table 4. ASMN Traffic Input Rate

TCP SYN traffic
5 Mbyte

We attempt TCP SYN flooding attack to the VNF server for 100 seconds. Then we apply the Sec-catalog including traffic shaping rule of 10 Mbit/s on VNF-G/W after 11 seconds since attack start.

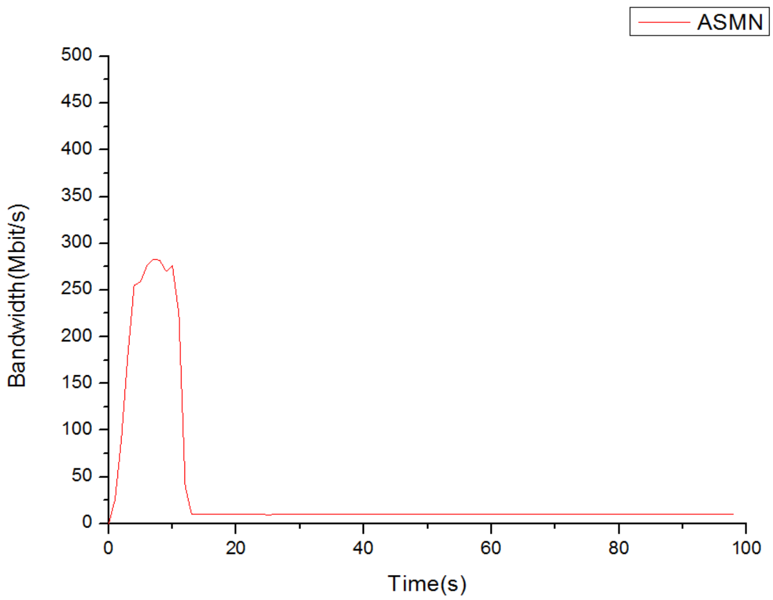

Fig. 9. TCP Shaping on VNF-G/W

In **Fig. 9**, we transmit the traffic at 280 Mbit/s to VNF server. After applying Sec-catalog, traffic was restricted at 9.76 Mbit/s within 1 second after applying rule. That is, we confirmed that flooding attacks can be prevented through incoming traffic control.

5. Conclusion

Recently, as the use of virtualization technology increases, NFV technology is attracting attention. Within the NFV, there are security issues with virtual machines and entities in NFV.

In this paper, we propose ASMN to solve the identification problem between VNFs in existing NFV environment and to guarantee secure communication environment between VNFs. ASMN performs an authentication of VNF using the hash-chain of the VNF image, and identification of the malicious VNF. In addition, VNF in a tenant is able to communicate with other VNFs in the same tenant using encryption key for hash-chain. Lastly, we can control the traffic between VNFs to prevent malicious behavior using VNF-G/W of ASMN. Through performance evaluation, we confirm that the performance of ASMN is similar to the existing NFV environment. Therefore, now that NFV is being commercially available, we can guarantee the safety of VNFs in the NFV environment using ASMN.

Acknowledgements

This work has been supported by the National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

References

[1] Han, B., Gopalakrishnan, V., Ji, L., & Lee, S., "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, 53(2), 90- 97, 2015. Article (CrossRefLink).

[2] Ahamed Aljuhani, Talal Alharbi, "Virtualized Network Functions security attacks and vulnerabilities," in *Proc. of Computing and Communication Workshop and Conference*, January, 2017. Article (CrossRefLink).

[3] Sang Il Kim, Hwa Sung Kim, "A high available service based on virtualization technology in NFV," in *Proc. of International Conference on Information Networking*, pp. 649-652, January, 2017. Article (CrossRefLink).

[4] Faqir Zarrar Yousaf , Michael Bredel, Sibylle Schaller, Fabian Schneider, "NFV and SDN – Key Technology Enablers for 5G Networks," *IEEE Journal on Selected Areas in Communications*, Issue 99, October 6, 2017. Article (CrossRefLink).

[5] Fang-Chun Kuo, Hannes Tschofenig, Fabian Meyer, Xiaoming Fu, "Comparison Studies between Pre-Shared and Public Key Exchange Mechanisms for Transport Layer Security," in *Proc. of IEEE International Conference on Computer Communications*, April, 2006. Article (CrossRefLink).

[6] A. H. Harbitter, D. A. Menasce, "Performance of public-key-enabled Kerberos authentication in large networks," in *Proc. of IEEE Symposium on Security and Privacy*, May, 2000. Article (CrossRefLink).

[7] Eman El-Emam, Magdy Koutb, Hamdy Kelash, Osama Farag Allah, "An optimized Kerberos authentication protocol," in *Proc. of International Conference on Computer Engineering & Systems*, pp.508-513, December, 2009. Article (CrossRefLink).

[8] M. Naor, M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proc. of the twenty-first annual ACM symposium on Theory of computing*, pp.33-43, January, 1989. Article (CrossRefLink).

[9] Min-Qing Zhang, Bin Dong, Xiao-Yuan Yang, "A New Self-Updating Hash Chain Structure Scheme," *Computational Intelligence and Security*, pp.315-318, December, 2009. Article (CrossRefLink).

[10] Yuta Kurihara, Masakazu Soshi, "A novel hash chain construction for simple and efficient authentication," in *Proc. of Annual Conference on Privacy, Security and Trust*, pp.539-542, December , 2016. Article (CrossRefLink).

[11] Xiangyang Jiang, Jie Ling, "Simple and effective one-time password authentication scheme," in *Proc. of International Symposium on Instrumentation and Measurement, Sensor Network and Automation*, pp.529-531, December, 2013. Article (CrossRefLink).

[12] Huiyi Liu, Yuegong Zhang, "An improved one-time password authentication scheme," in *Proc. of IEEE International Conference on Communication Technology*, November 17-19, 2016. Article (CrossRefLink).

[13] Saket Acharya, Namita Tiwari, "Survey of DDoS Attacks Based On TCP/IP Protocol Vulnerabilities," *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 18, Issue 3, pp. 68-76, 2016. Article (CrossRefLink).

[14] Wentao Liu, "Research on DoS Attack and Detection Programming," in *Proc. of International Symposium on Intelligent Information Technology Application(IITA)*, pp.207-201, November 21-22, 2009. Article (CrossRefLink).

[15] SteveMansfield-Devine, "The growth and evolution of DDoS," *Network Security*, vol. 2015, Issue 10, pp.13-20, October, 2015. Article (CrossRefLink).

[16] Neha Gupta, Ankur Jain, Pranav Saini, Vaibhav Gupta, "DDoS attack algorithm using ICMP flood," *Computing for Sustainable Global Develop*, pp.4082-4084, March, 2016. Article (CrossRefLink).

[17] Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing," in *Proc. of Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, April, 2006. Article (CrossRefLink).

[18] Resul Das, Abubakar Karabade, Gurkan Tuna, "Common network attack types and defense mechanisms," in *Proc. of Signal Processing and Communications Applications Conference (SIU)*, 2015. Article (CrossRefLink).

[19] Mahmood Khalel Ibrahem, "Modification of Diffie-Hellman Key Exchange Algorithm for Zero Knowledge Proof," in *Proc. of International Conference on Future Communication Networks*, pp.147-152, April, 2012. Article (CrossRefLink).

HyunJin Kim is a Ph.D. student in the Department of Computer Engineering at Chungnam National University in Republic of Korea. He received the B.S. degree in Information Communications Engineering from Chungnam National University in 2015, the M.S. degree in Computer Science & Engineering from same university in 2017. He is interested in most aspects of information security, both theoretical and practical, and his recent research is largely about NFV security, cloud service security and applied cryptography.

PyungKoo Park received his B.S. and M.S. in computer science from Korea University, Korea, in 1998 and 2000, the Ph.D. degree in Computer Network and Security System at Chungnam National University, Korea in 2013. Since 2000, he is Principal Member of Researcher with Electronics and Telecommunications Research Institute. His research interests are Internet Security, SDN, 5G, NFV and Computer Networks.

JaeCheol Ryou is a professor in the Department of Computer Engineering at Chungnam National University in Korea. He received the B.S. degree in Industrial Engineering from Hanyang University in 1985, the M.S. degree in Computer Science from Iowa State University in 1988, and the Ph.D. degree in Electrical Engineering and Computer Science from Northwestern University in 1990. His research interests are Internet Security and Electronic Payment Systems.