JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 19, No. 4, pp. 837-844 Apr. 2018

인공지능 기술을 이용한 NFV 환경에서의 DDoS 공격 탐지 연구

김 현 진[1] · 박 상 호[2], 류 재 철[1*]
[1]충남대학교 컴퓨터공학과
[2]지란지교소프트

Research on DDoS Detection using AI in NFV

HyunJin Kim[1] · Sangho Park[2] · JaeCheol Ryou[1*]
[1]Department of Computer Engineering, Chungnam National University, 99, Daehak-ro, Yuseong-gu, Daejeon, Korea
[2]JiranSoft Researh Center, 87, Daehak-ro, Yuseong-gu, Daejeon, Korea

[요 약]

최근 클라우드 기술은 물리적인 네트워크를 구축하지 않고, 동적으로 논리적인 네트워크를 구축할 수 있게 만들 수 있다는 특징으로 인해 각광받고 있다. 최근의 클라우드 분야의 연구에도 불구하고, 가입자가 공개적으로 VNF를 이용한 서비스를 제공 받을 수 있는 NFV 환경의 특성으로 공격의 타겟이 될 수 있기 때문에 가짜 VNF에 대한 식별과 개체 간의 통신 암호화에 대한 연구가 필요하다. 따라서 본 논문에서는 가짜 VNF를 탐지하고, VNF 간의 상호 인증을 통해서 통신 구간의 보안성을 향상시킬 수 있는 Virtual PKI를 이용한 보안 메커니즘을 제안한다. 그리고 NFV 환경에서 DDoS 공격에 대한 공격의 탐지율을 향상시키기 위한 다수의 인공지능 알고리즘을 비교・분석함으로써 공격탐지에 효과적인 인공지능 알고리즘을 도출하였다.

[Abstract]

Recently, the cloud technology has made dynamical network changes by enabling the construction of a logical network without building a physical network. Despite recent research on the cloud, it is necessary to study security functions for the identification of fake virtual network functions and the encryption of communication between entities. Because the VNFs are open to subscribers and able to implement service directly, which can make them an attack target. In this paper, we propose a virtual public key infrastructure mechanism that detects a fake VNFs and guarantees data security through mutual authentication between VNFs. To evaluate the virtual PKI, we built a management and orchestration environment to test the performance of authentication and key generation for data security. And we test the detection of a distributed denial of service by using several AI algorithms to enhance the security in NFV.

색인어 : 가상화, 클라우드, NFV, DDoS, 경량화 PKI
Key word : Virtualization, Cloud, DDoS, Lightweight PKI

http://dx.doi.org/10.9728/dcs.2018.19.4.837

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-CommercialLicense(http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Received 18 April 2018; **Revised** 26 April 2018
Accepted 28 April 2018

***Corresponding Author; JaeCheol Ryou**
Tel: +82-42-821-7443
E-mail: jcryou@cnu.ac.kr

Ⅰ. 서 론

가상화 된 클라우드 컴퓨팅 기반의 서비스 플랫폼의 확산에 따라서 이를 활용한 서비스들이 급증하고 있다. 이에 따라 인프라 사용자의 요구사항도 점차적으로 복잡하고, 세분화 되면서 사용자 요구사항을 충족시키는 응용 서비스들이 새롭게 등장하고 있다. VNF(virtual network function) 는 가상환경에서 사용자 맞춤 서비스를 제공하기 위한 운영하기 위한 기술로써 NFV(Network Function Virtualization) MANO (Management and Orchestration)에서 시스템의 개념이 정립되었으며, 기술규격 개발과 VNFFG(VNF Forwarding Graph)에 대해 정의되어 단일 서비스 연동을 위한 표준화 작업이 진행 중이다. 현재 NFV 연구는 가상화 서비스 분야에 집중되고 있으며, 가상 인프라 내 VNF의 인증 및 보안에 대한 연구가 부족한 상황이다. NFV 환경에 보안위협은 크게 세 가지가 있다. 첫 번째는 가상 엔터티 간의 상호 인증 과정이 확립되지 않았기 때문에 VNF와 EM 또는 VNF간간의 통신과정에서 가짜 VNF와 가짜 EM이 테넌트 내에 등록되어 멀웨어 및 봇넷을 이용하여 내부 인프라를 위협할 수 있다. 두번째로 VNF 간의 데이터 통신 과정에서 암호화가 수행되지 않기 때문에 가짜 VNF 및 위협으로부터 오염된 VNF로부터 통신 상 전송되는 데이터가 탈취될 수 있다. 마지막으로 다수의 VNF가 공격으로 인해 봇넷으로 감염된 경우, 다수의 트래픽을 일으키는 DDoS 공격과 같은 악성 행위로 인해 전체 서비스가 마비되는 피해를 입을 수 있다. 본 논문에서는 위의 보안위협을 방지하기 위해서 가상환경을 고려한 Virtual PKI(Public Key Infrastructure), 즉 vPKI를 기반으로 EM과 VNF, VNF 간의 상호인증과 VNF 간의 데이터 전송 과정에서의 암호화를 수행하는 보안 메커니즘을 제안한다. 그리고 다수의 인공지능(AI, Artificial Intelligence) 알고리즘을 보안 메커니즘에 적용 및 비교·분석함으로써 효과적으로 DDoS 행위를 방지하는 알고리즘을 도출한다. 본 논문의 구성은 2장에서 관련연구로 PKI, 악성행위 및 다양한 인공지능기술을 알아보고, 3장에서 본 논문에서 제안하는 vPKI를 소개한다. 4장에서는 vPKI의 EM과 VNF, VNF 간의 상호인증 성능을 측정한다. 또한 2009년 실제 발생했던 공격 데이터를 이용하여 다양한 인공지능 알고리즘의 DDoS 공격 탐지 성능을 측정하고, 5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2-1 PKI

PKI는 인터넷과 같이 안전하지 않은 공중망 환경에서, 사용자들이 신뢰 기관으로부터 받은 공개키와 개인키 상을 사용하여 안전한 데이터 교환을 보장할 수 있는 프레임워크이다. PKI는 인증기관인 CA(Certificate Authority), 등록기관인 RA(Registration Authority), 검증기관인 VA(Validation Authority)로 구성된다[1]. PKI 인프라 내 각 개체는 인증서와 자신의 공개키 쌍 및 CA의 공개키를 가진다. 각 개체 간 인증 과정에서 자신의 개인키를 이용한 인증서를 전송하면, CA의 공개키로 인증서를 복호화하여 얻은 상대방의 공개키 정보로 신원을 인증할 수 있다. 또한 개체 인증으로 획득한 상대방의 공개키는 데이터통신에 암호화 키로 활용될 수 있다[2]. PKI 기반 인증은 신뢰할 수 있는 인증기관으로부터 인증을 받아 상대방과의 안전한 통신을 보장받을 수 있는 기술이지만, PKI 구성요소인 RA, CA, VA를 인프라 외부에 위치하는 기존의 시스템을 가상인프라 내 VNF 인증에 적용한다면 가상 인프라 내 공유자원의 소모와 함께 인증에 소요되는 오버헤드가 발생할 수 있다[3]. 따라서 가상화된 환경에서는 기존의 PKI가 경량화한 형태로 설치되어야 한다. 본 논문에서는 MANO 기반의 가상환경에 적합한 가상화된 vPKI (Virtual PKI)를 제안하여 기존의 MANO 기능을 변경하지 않으면서 상호인증 및 데이터 통신 암호화를 보장할 수 있다.

2-2 악성 행위

최근 인터넷 사용이 급증하면서 각 기관들은 인터넷을 통해서 서비스를 제공하는데 DDoS(Distributed DoS)는 프로토콜의 설계상 취약점을 공략하는 공격이기 때문에 대응이 어렵다[4]. DDoS는 다수의 공격자들이 분산된 곳에 위치하여 동시에 공격을 수행하여 타겟을 서비스 불능 상태로 만드는 공격이다[5]. 대표적인 DDoS 공격은 대역폭 고갈 공격, 자원 고갈 공격, 어플리케이션 공격 등이 있다[6]. 대역폭 고갈 공격은 공격자가 다수의 좀비 PC를 이용하여 대량의 패킷을 발생하여 네트워크 대역폭의 처리 한계를 초과시키는 공격이다. 같은 네트워크에 있는 다른 시스템까지 접속장애를 유발시킬 수 있기 때문에 파급효과가 큰 공격이다. 이 공격은 대량의 UDP 패킷을 전송하는 UDP Flooding, 대량의 ICMP 패킷을 이용한 ICMP Flooding 공격이 대표적이다[7]. 자원 고갈 공격은 TCP 패킷을 이용하여 초당 패킷 처리량을 증가시킴으로써 시스템의 CPU 부하를 증가시키는 공격이다. 이 공격은 bps(bit per second)의 증가는 많지 않지만, pps(packet per second)의 증가로 시스템의 부하를 발생시키는 것이 특징이다. 대표적인 예로 SYN 패킷을 이용한 SYN Flooding 공격이 있다[8]. 마지막으로 어플리케이션 공격은 어플리케이션의 과다한 접속을 통해서 시스템 서비스에 장애를 일으키는 공격이다. 대량의 HTTP Get 메시지를 이용하는 HTTP GET Flooding이나 캐시 사용을 방해하는 HTTP CC 기법을 이용하는 것이 특징이며, 최근 증가하고 있는 Slowloris DDoS 이 대표적인 예에 속한다[9]. 가상환경에서는 공격자가 테넌트 내에 다수의 VNF가 로드되는 NFV 환경의 특징을 이용하여 네트워크 내 대량의 패킷을 발생시켜서 가상 네트워크 대역폭을 고갈 시키는 대역폭 소진 공격을 발생시킨다면 전체 네트워크가 마비되는 사태가 초래될 수 있다. 다시 말해서, NFV 환경에서 공격자가 테넌트 내 VNF를 봇넷으로 만든 경우에 다

른 VNF도 봇넷이 전파되어 제공 중인 서비스를 마비시킬 수 있다. 그러나 PKI 기반으로 인증서를 이용하여 VNF의 신원을 확인한 후에 통신을 수행한다면 DDoS 공격을 예방할 수 있다. 즉, 트래픽 전송자에 대한 인증을 통해서 인증자에 대한 목록에 대해 화이트리스트 기반의 통신을 수행한다면 VNF의 비정상 행위를 차단할 수 있다.

2-3 인공지능 알고리즘

최근 인공지능 기술의 연구가 가속화되고 있다. 인공지능 기술은 학습시간은 길지만, 학습 이후에는 관리자의 관여를 최소화하고, 다양한 공격에 대해서 능동적으로 대처할 수 있다는 장점이 있다. 인공지능 기술의 적용된 분야 중 비정상 행위 탐지 분야에서는 군집(Clustering) 알고리즘이 이용된다[10]. 군집 알고리즘을 이용하면, 대량의 데이터 집합으로부터 공통된 패턴을 찾아내어 해당 패턴을 보이는 데이터에 대한 악성행위 여부를 판단할 수 있다. 군집 알고리즘은 대표적으로 Farthest First, HierarchicalCluster, LVQ가 있다[11]. FarthestFirst 알고리즘은 관측 데이터들 중에서 특정 데이터를 선택하고, 지정된 데이터와 차이가 큰 데이터 순으로 데이터를 탐색하면서 분류 하는 알고리즘이다. 데이터 간의 차이를 이용하여 데이터 유사도를 판별하여 패턴을 분류한다[12]. Hierarchical Cluster 알고리즘은 분류할 그룹의 개수를 지정하지 않고, 데이터 분류를 수행하는 알고리즘이다. 즉, 특정 데이터들을 지정하고, 해당 데이터로부터 가까운 그룹과 병합(Agglomeration)하여 그룹을 확장하는 병합적 방법(Agglomerative Method)과 하나의 큰 그룹으로부터 기준에 따라 소규모 그룹으로 분류하는 분할적 방법(Divisive Method)을 사용한다[13]. LVQ 알고리즘은 경쟁학습(Competitive learning) 방식을 이용하여 초기 가중치에 따라 입력 벡터를 군집화하는 지도학습(Supervised learning) 알고리즘이다. 입력 계층 데이터와 출력 계층 데이터 사이의 유사성 여부를 결정하여 참조 데이터를 갱신하는 과정을 반복하여 이후에 관측되는 데이터를 분류한다 [14]. 인공지능의 군집 알고리즘을 이용하면 가상환경에서 VNF 간 전송되는 트래픽의 비정상 유무를 판단할 수 있다. 테너트 내의 VNF가 공격자에 의해 감염되어 비정상 행위를 하는 경우에 공격 위협 데이터 집합을 이용하여 정상 트래픽과 비정상 트래픽 패턴을 분류하고, 이후 입력되는 트래픽을 정해진 패턴에 따라 파악한다면 DDoS 공격 여부를 파악할 수 있다. DDoS 공격으로 판단된 경우에는 해당 전송지로부터의 트래픽을 차단하여 VNF를 보호할 수 있다.

Ⅲ. 제 3 장 Virtual Public Key Infrastructure

본 논문에서 제안하는 vPIK는 NFV 환경에서 Tenant 내의 가상 엔티티들에 대하여 인증서에 기반한 인증 및 암호화 통신과 AI 알고리즘을 이용하여 테넌트 내 VNF에 발생할 수 있는 DDoS 공격에 대해 방어를 수행할 수 있는 메커니즘이다.

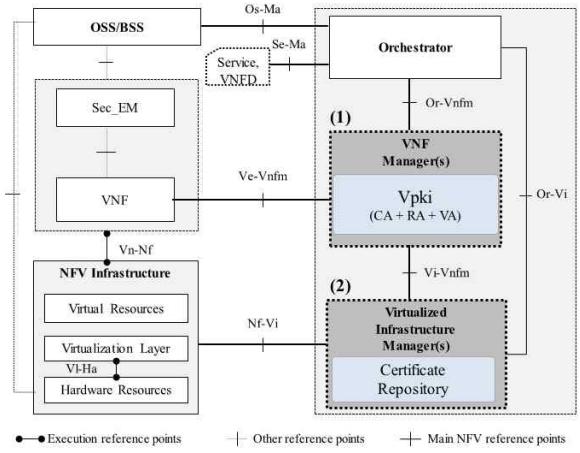

그림 1. Virtual PKI 구조
Fig. 1. The architecture of Virtual PKI

vPKI는 다음의 2단계로 이루어진다. 1단계에서는 PKI 인프라를 이용하여 각 VNF와 EM의 상호 인증 수행과 인증서를 이용하여 Tenant 내 VNF간, EM 및 VNF 간 공개키 인증서 기반 암호화 통신을 수행하는 단계이다. 2단계에서는 인공지능 알고리즘을 이용하여 VNF와 EM에서 발생 가능한 DDoS 공격에 대한 방어 성능을 비교한다.

4-1 VNF Instantiation

vPKI 구성은 인증서 발급 신청 모듈인 RM(Registration Module), 인증서 CM(Certificate Module), 인증서 검증 모듈인 VM(Verification Module), 인증서가 저장되는 Cert DB, 인증서에 대한 개인키가 저장되는 Key DB, 서버 내외의 트래픽을 처리하는 Server Engine으로 구성한다. 인증서 발급은 VNF가 Instantiation 과정에서 인증서를 발급한다. 인증서는 VNF가 최초 Tenant에 등록될 때 발급된다. Orchestrator는 VNF 활성화를 VIM과 VNFM에게 Security Description 정보와 함께 전달한다. 요청을 수신한 VIM은 vPKI 에게 인증서를 요청하게 되고 인증서 수신 후 VNF가 설치되는 가상머신을 컴퓨팅 노드에 Placement 할 때 함께 Instantiation하게 된다. VNF의 Instantiation 과정은 다음과 같다.

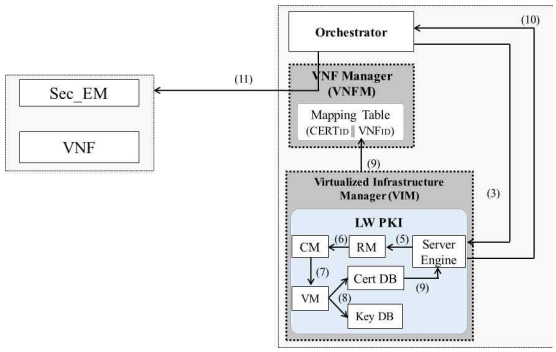

그림 2. 초기화 과정
Fig. 2. Instantiation process

(1) Orchestrator는 Instantiation 과정에서 VNF가 사용할 공유 자원의 정보와 VNFD(VNF Descriptor) 내의 인증서 발급과 관련된 보안 정보(Security Description)를 VIM 내 vPKI의 서버 엔진으로 전송한다. (2) VIM 내 vPKI의 서버 엔진은 전송된 정보를 통해 인증서 발급 모듈 (RM)으로 해당 정보를 전송한다. (3) RM은 발급 요청 메시지 내 Tenant_ID, VNF_ID, EM_ID, VNFD 정보를 이용하여 인증서 발급을 요청한 엔티티를 식별하고, CM에 인증서 발급을 요청한다. VNF 식별은 식 (i)을 이용하여 수행된다. (4) CM은 인증서를 발급하고, 발급된 인증서는 VM으로 전송한다. (5) VM은 등록된 인증서를 Cert DB에 보관하고, 인증서 암호화 키를 Key DB에 저장한다. 암호화키 생성식은 (ii)와 같다. 대칭키 생성 과정에서 사용한 Challenge는 Certificate Request 과정에서 각 엔티티가 전송한 임의의 난수를 이용했다. 엔티티 간 암호화 통신을 하거나 엔티티 인증 과정에서 VNF 인증서가 사용될 경우, Mapping Table에 기입된 VNF에 대응되는 인증서를 파악하여 인증서를 로드한다. (6) 인증서가 DB에 등록이 완료되었다는 응답 메시지를 Orchestrator에 전송한다. (7) Instantiation 완료 및 인증서 발급 완료 메시지는 해당 VNF가 생성될 Tenant의 EM으로 전송되어 컴퓨팅 노드에 Placement하게 된다.

4-2 VNF 인증

인증서 등록 및 발급 과정이 지난 후에 가상 엔티티 간 통신을 요청받으면, 인증서 기반의인증 과정을 수행한다. Sec_EM과 VNF는 각자의 인증서로 VNFM의 vPKI에 전송하고, VM은 VIM 내의 Certificate Repository에 보관된 인증서와 비교하여 변조 여부를 판단한다.

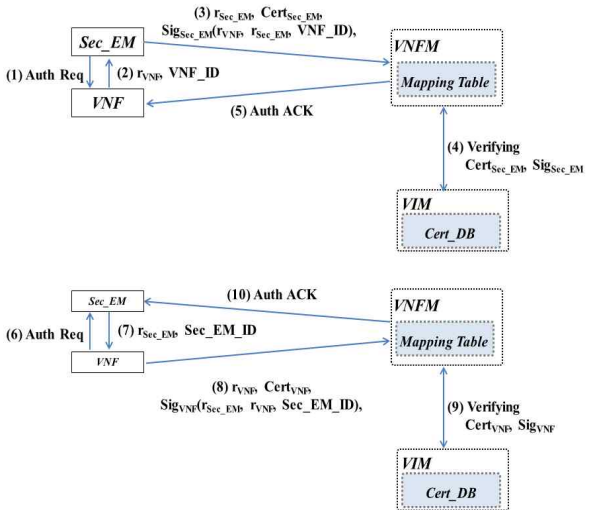

그림 3. VNF 인증
Fig. 3. Authentication between Sec_EM and VNF

4-3 VNF 간 상호 인증

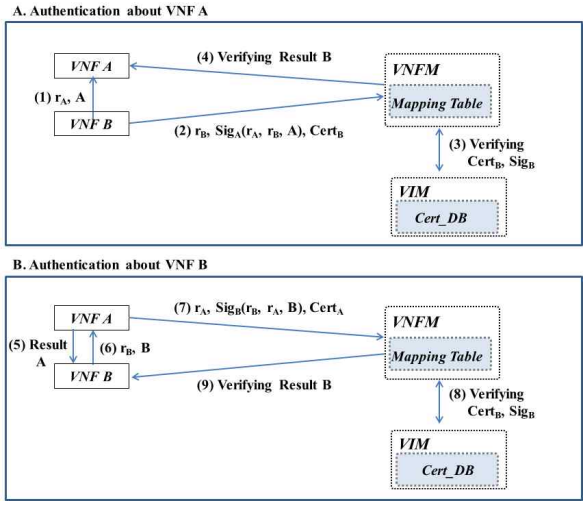

그림 4. VNF 간 인증
Fig. 4. Authentication between VNFs

A 과정은 VNF A의 인증 과정이다. VNF A가 VNF B에게 랜덤 값과 A의 식별자를 전송하면, VNF B는 자신이 생성한 임의의 값과 자신의 식별자에게 서명을 하여 자신의 인증서와 함께 VNFM에게 전송한다. VNFM은 전송된 서명 SigA(rA,rB,B)과 인증서 CertB를 이용하여 VIM 내 인증서와의 일치 여부를 확인하다. 그리고 VM(Verification Module) 내 등록된 인증서인지 확인하여 서명 및 인증서를 검증한다. B 과정은 VNF B를 인증하는 과정으로 A 과정과 동일하게 B에 대한 인증을 수행한다.

4-4 보안 통신

VNFM은 인증과정에서 VIM으로부터 전달받은 인증서를 이용하여 가지고 있으며, 각 엔티티의 인증서로 통신 암호화 키인 KEK를 암호화하여 엔티티들에 전달한다. 각 엔티티는 자신의 인증서 개인키를 이용하여 통신 암호화 키를 복호화하여, 안전한 통신을 수행한다.

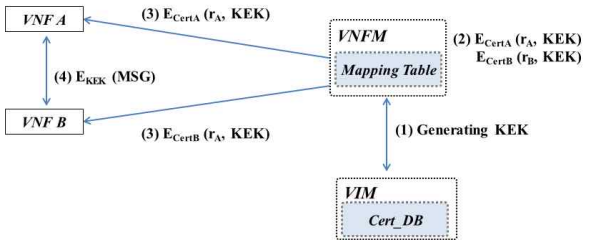

그림 5. VNF간 보안 통신
Fig. 5. Secure Communication between VNFs

Ⅳ. 제 4 장 성능 평가

본 4 장에서는 2가지 시험을 통해서 vPKI의 성능을 시험하였다. 첫 번째 시험에서는 PKI와 vPKI를 이용하여 VNF 인증에 소요되는 시간과 시스템 자원을 측정하였으며, 두 번째 시험에서는 DDoS 공격을 탐지하기 위해서 다양한 인공지능 알고리즘을 적용하고, 알고리즘 별 성능을 비교·분석하였다. 시험을 위해서 각 테넌트 별로 1개의 CPU와 2GB의 메모리를 할당한 가상머신 10개를 구동하였으며, 각 VM 당 한 개의 VNF를 구동했다.

4-1 PKI 인증서 기반의 인증 성능

테넌트 내 인증은 Sec_EM과 VNF간 인증, VNF들간의 인증을 수행한다. 인증 수단으로는 PKI 기반 인증서를 이용하였으며, 인증서 기반 인증에 소요되는 시간은 다음과 같다.인프라 외부에서 PKI 시스템을 위치시키고, 인증을 수행했을 때와 가상 환경에서 인프라 내부에 vPKI 시스템을 이용하여 인증을 수행했을 때, 인증에 소요되는 시간을 비교하였다. 인프라 외부에서는 인증 소요시간이 평균 0.28s 소요되었으며, 가상 환경에서는 인증에 평균 0.59s가 소요된 것을 확인하였다. 가상 환경에서는 실제 환경에 비해 0.31s이 더 소요되었다.

그리고 인프라 외부와 가상환경에서 인증서 기반 인증을 수행할 때 소요되는 시스템 자원의 사용률을 비교한 결과, 인프라 외부에서 PKI 기반 인증을 수행할 때는 평균적으로 전체 시스템 자원 중 4.2%가 소요되었으며, 가상 환경에서도 마찬가지로 4.2%가 소요되었다. 즉, 정리하자면 외부에 PKI 시스템을 위치시키고, 인증을 수행하는 기존의 인증 시스템에 비해서 가상 환경의 인프라 내에 vPKI를 위치시키고 인증을 수행했을 경우 인증에 소요되는 시간은 0.31s가 더 소요되었으며, 시스템 자원 사용률은 두 가지 경우 동일했다.

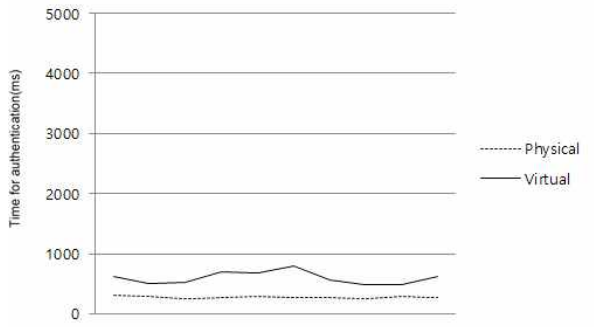

그림 6. PKI 기반 인증에 소요되는 시간
Fig. 6. The time for authentication based on PKI

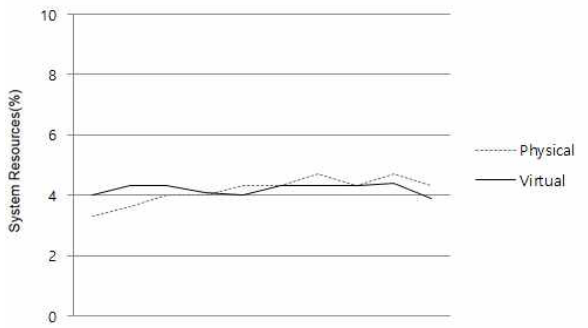

그림 7. 인증에 소요되는 시스템 자원
Fig. 7. The system resources for authentication

4-2 AI 기반의 DDoS 공격 탐지

VNF 간에 발생할 수 있는 대표적인 DDoS 공격인 ICMP Flooding, SYN Flooding, UDP Flooding 공격의 탐지율을 측정하기 위해서 테넌트 내 VNF 간 전송되는 트래픽의 통계 정보를 데이터 집합으로 활용하여 인공지능 알고리즘에 적용했다. 시험에 사용되는 알고리즘은 FarthestFirst, HierarchicalCluster, LVQ(Learning Vector Quantization)이며, 시험에 사용되는 트래픽은 다음의 표와 같다.

표 4. 입력 트래픽
Table 4. Input Traffic

ICMP Traffic	SYN Traffic	UDP Traffic
74 byte -1000 byte	1500 byte	74 byte-1000 byte

시험 트래픽은 한국에서 2009년에 발생한 7.7 DDoS 공격의 트래픽 정보[15]를 기반으로 시험에 사용할 트래픽에 대한 데이터 집합을 작성했다. 트래픽에 포함된 프로토콜은 ICMP, SYN, UDP이며, bps는 최대 200Kbps, pps는 최대 3Kpps이다. 해당 시험 트래픽의 DDoS 여부를 판별하고, 판별 결과가 실제 결과와 동일한지를 비교하는 방식으로 탐지율을 계산했으며, 데이터 셋의 개수를 증가시키면서 각 알고리즘 별로 계산된 탐지 오차를 비교했다.

각 알고리즘은 공통적으로 데이터 셋의 수가 많아질수록 탐지 정확도가 상승되었다. 알고리즘 별 탐지 오차 평균을 비교하면, Farthest First 알고리즘은 11.3%, Hierarchical cluster 알고리즘은 12.0%, LVQ 알고리즘은 22.1%로 측정되었다. 그리고 Farthest First 알고리즘이 Hierarchical cluster 알고리즘과 LVQ 알고리즘의 탐지율 오차보다 0.7%, 10.8% 우수했다. 그리고 각 알고리즘을 동작시켰을 때의 자원 점유율을 비교한 결과, 공통적으로 시스템 자원 1% 이내를 소모했다. Farthest First 알고리즘은 0.30%, Hierarichical clustering 알고리즘은 0.49%, LVQ 알고리즘은 0.52%의 자원을 사용했다. Farthest First이 Hierarichical Clustering보다 0.19%, LVQ보다 0.22% 자원을 더 적게 소모했다.

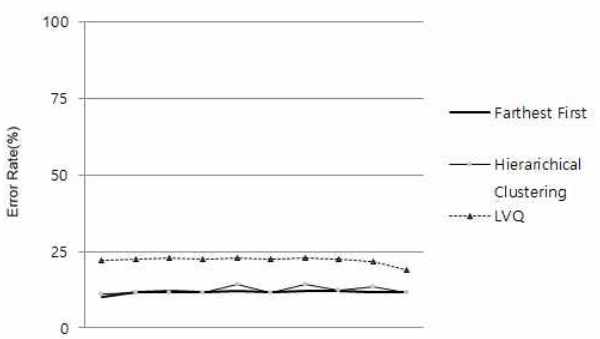

그림 8. 알고리즘 별 탐지 오차
Fig. 8. The error rate for algorithms

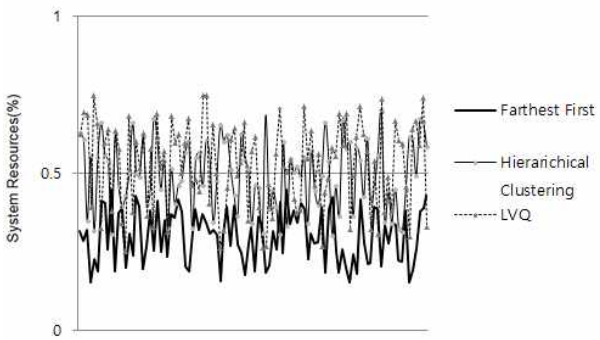

그림 9. 알고리즘 별 DDoS 공격 탐지에 소요되는 시스템 자원
Fig. 9. The system resources on DDoS detection for algorithms

따라서 종합하면 세가지 알고리즘 중 Farthest First 알고리즘이 Hierarichical clustering 알고리즘, LVQ 알고리즘보다 높은 탐지율을 가지면서 더 적은 CPU 자원을 소모한 것을 확인할 수 있었다.

Ⅴ. 결 론

가상화 기술의 발달로 많은 NFV에 대한 연구가 진행되고 있다. 본 논문에서는 NFV 환경에서 VNF의 인증 및 데이터 보안을 위한 vPKI를 제안했다. vPKI는 가상환경에 적합한 PKI로 인증서 기반의 상호인증을 수행하고, 보안 키를 이용하여 데이터 유출을 방지할 수 있는 메커니즘이다. 외부에 PKI 시스템을 위치한 기존의 시스템은 가상 환경 내에 vPKI를 위치시킨 시스템보다 인증에 소요되는 시간은 적었지만, 인증 과정에 소요되는 시스템 자원은 동일하였다. 인증 소요시간은 기존 시스템에 비해 길었지만 테너트 별로 VNF가 제공하는 서비스에 따라서 동적으로 정책을 변경해야하는 NFV 특징상, vKI를 이용하면 서비스 별로 동적으로 적용되는 정책에 유연하게 대응할 수 있다. 그리고 오염된 VNF가 수행할 수 있는 VNF의 DDoS 공격을 탐지하기 위해서 적용한 알고리즘 중 Farthest First 알고리즘을 적용하면 그 외 알고리즘보다 적은 시스템 자원을 사용하여 높은 공격 탐지율을 얻을 수 있었다. 즉, vPKI를 이용하여 NFV 내 엔터티를 상호 인증 및 VNF 통신 과정 내 메시지를 암호화하고 , VNF에 대한 인공지능 기술을 이용하여 DDoS 공격을 탐지한다면 NFV 환경에서의 보안성을 향상시킬 수 있을 것이다.

감사의 글

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(R0190-17-2009, 화이트리스트와 상황인지 기술을 이용한 엔드포인트 보호기술 개발)

참고문헌

[1] Sanjeet Kumar Nayak, Sujata Mohanty and Banshidhar Majhi. “CLB-ECC: Certificateless Blind Signature Using ECC”, Journal of Information Processing Systems(JIPS), Vol. 13, pp. 392-397, 2017.

[2] Mihir Bellare, Anand Desai, David Pointcheval; Phillip Rogaway, “Lecture Notes in Computer Science”, CRYPTO: Annual International Cryptology Conference, Vol. 1462, pp. 26-45, 1998.

[3] Ki-Woong Park, Jaesun Han, JaeWoong Chun and Kyu Ho Park, “THEMIS: A mutually Verifiable Billing System for the Cloud Computing Environment”, IEEE Transactions on Services Computing, Vol. 6, Issue 3, pp. 300-313, 2013.

[4] Saket Acharya and 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.

[5] Won Min Kang, Seo Yeon Moon and Jong Hyuk Park, “An enhanced security framework for home applicances in smart home”, Human-centric Computing and Information Sciences(HCIS), 2017.

[6] Syed Mujtiba Hussain and Ghulam Rasool Beigh, “Impact of DDoS attack (UDP Flooding) on queuing models”, 4th International Conference on Computer and Communication Technology (ICCCT), pp.210-216, 2013.

[7] Neha Gupta, Ankur Jain, Pranav Saini and Vaibhav Gupta, “DDoS attack algorithm using ICMP flood”, Computing for Sustainable Global Development(INDIACom), pp. 4082- 4084, 2016.

[8] Dimitrios Moustis and Panayiotis Kotzanikolaou, “Evaluating security controls against HTTP-based DDoS attacks”, 4th International Conference on Information Intelligence, Systems and Applications (IISA), 2013.

[9] Wei Chen and Dit-Yan Yeung, “Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing”, Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006.

[10] Nathan Keegan, Soo-Yeon Ji, Aastha Chaudhary, Claude Concolate and Byunggu Yu, “A survey of cloud-based network intrusion detection analysis”, Human-centric Computing and Information Sciences, 2016.

[11] U. Maulik and S. Bandyopadhyay, “Performance evaluation of some clustering algorithms and validity indices”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, Issue 12, pp.1650-1654, 2002.

[12] Sharmila and Mukesh Kumar, “An optimized farthest first clustering algorithm”, Nirma University International Conference on Engineering (NUiCONE), 2013.

[13] Seema Bandyopadhyay and E. J. Coyle, “An energy efficient hierarchical clustering algorithm for wireless sensor networks”, INFOCOM, Vol. 3, pp.1713-1723, 2003.

[14] R.Inokuchi and S. Miyamoto, “LVQ clustering and SOM using a kernel function”, International Conference on Fuzzy System, Vol. 3, pp.1497-1500, 2004.

[15] Sin-seok Seo, Young J. Won and James Won-Ki Hong, “Witnessing Distributed Denial-of-Service traffic from an attacker’s network”, Network and Service Management (CNSM), pp. 241-247, 2011.

김현진(HyunJin Kim)

2015년 : 충남대학교 정보통신공학 (학사)
2017년 : 충남대학교 컴퓨터공학 (석사)
2017년~현 재: 충남대학교 컴퓨터공학 (박사과정)

※관심분야 : 네트워크 보안, 클라우드 보안, 인증, 암호 응용 등

박상호(Sangho Park)

2008년 : 충남대학교 컴퓨터공학 (학사)
2010년 : 충남대학교 컴퓨터공학 (석사)
2013년~현 재: 충남대학교 컴퓨터공학 (박사수료)

※관심분야 : 정보보안, 엔드포인트 보안 플랫폼 등

류재철(JaeCheol Ryou)

1985년 : 한양대학교 산업공학 (학사)
1988년 : Iowa 주립대학 전산학 (석사)
1990년 : Northwestern 대학 전산학 (박사)\

1991년~현 재: 충남대학교 컴퓨터공학과 교수
※관심분야 : 인터넷보안, 정보보안, 전자지불 시스템 등