논문 21-46-02-11 The Journal of Korean Institute of Communications and Information Sciences '21-02 Vol.46 No.02
https://doi.org/10.7840/kics.2021.46.2.268

SDN 환경에서 형태보존암호를 이용한 IP 주소 보호 기법

박 도 현◆, 김 민 태*, 임 종 훈*, 장 래 승*, 이 선 영°

IP Address Protection Method in SDN Using Format Preserving Encryption

Dohyeon Park◆, Mintae Kim*, Jonghoon Lim*, Raeseung Jang*, Sun-Young Lee°

요 약

SDN(Software Defined Network)은 중앙 제어를 통해 네트워크의 기능과 서비스를 관리할 수 있다. 그러나, SDN에는 기존 네트워크와 마찬가지로 IP 주소 노출에 의한 네트워크 자원 식별 및 IP 주소를 이용한 IP 스푸핑, 스니핑, 네트워크 스캐닝, Dos 등에 대한 취약점이 존재한다. 이를 해결하기 위해 공격 사전 준비 단계에서 시스템에 대한 공격을 지연하거나 방지하기 위해 지속적으로 환경을 변이하는 기술이 연구되고 있다. 본 논문은 프로토콜 구조의 변경을 최소화하면서 스니핑, 스푸핑 등 네트워크 보안 위협으로부터 IP 주소를 보호하기 위해 형태보존암호를 사용하여 IP주소를 암호화하는 방법을 제안하였다. 키 분배 과정에서 단말 인증을 사용하여 단말 인증을 통해 부인방지 및 흐름규칙충돌 등의 공격에 대응하였다. 실험을 통해 약 32%의 단말이 네트워크 스캐닝 공격에 안전함을 검증하였다. 그 결과 기존 자원 보호 기술과 비교하여 보안성 항목에 대응함을 확인하였다.

Key Words : SDN, FPE, IP Address Encryption, Network Scanning, Key exchange protocol

ABSTRACT

SDN(Software Defined Network) can manage the functions and services of the network through central control. However, SDN, like traditional networks, is able to identify network resources by IP address exposure and there are vulnerabilities to IP spoofing, sniffing, network scanning, and DoS using IP addresses. In order to solve this problem, a technology that continuously changes the environment is being studied to delay or prevent an attack on the system in the pre-attack preparation stage. This paper proposes a method of encrypting the IP address using a format-preserving encryption to protect the IP address from network security threats such as sniffing and spoofing while minimizing the change of the protocol structure. In the key distribution process, host authentication was used to counter attacks such as non-repudiation and flow rule conflict. In addition, experiments results showed that approximately 32% of hosts are safe for network scanning attacks. As a result, we confirmed that our proposal is better than the existing resource protection technology in the security.

※ 본 연구는 2020학년도 순천향대학교 교수 연구년제에 의하여 연구하였습니다.

◆ First Author : Soonchunhyang University, Department of Information Security Engineering, rharnr777@gmail.com, 학생(학사), 학생회원

° Corresponding Author : Soonchunhyang University, Department of Information Security Engineering, sunlee@sch.ac.kr 교수, 종신회원

* Soonchunhyang University, Department of Information Security Engineering, kimals0288@gmail.com, 학생(학사), 학생회원; jhl3185@naver.com, 학생(학사), 학생회원; rs0731@naver.com, 학생(학사), 학생회원

논문번호 : 202010-263-B-RN, Received October 19, 2020; Revised November 19, 2020; Accepted November 19, 2020

Ⅰ. 서 론

인터넷의 발달로 네트워크를 대상으로 한 공격이 다양화되고 있다. 지능적 지속 위협 공격은 정부, 정보통신, 금융기관 등 국가 주요 기반 시설을 대상으로 한다. 이에 대한 사례로 3. 20 사이버테러, 평창 동계올림픽 APT 공격 등 특정 대상을 노리는 공격이 증가하는 추세이다[1]. 공격자는 사이버 공격을 위해 기초 정보수집, 악성코드 침투 과정을 거쳐 기밀 정보를 유출한다. 정보수집 단계는 공격자가 타겟을 정하고 정보를 수집하는 단계이다. 타겟의 시스템이 어떤 취약점이 존재하는지 조사하고 악성코드의 제작을 통해 네트워크 침입을 시도한다[2]. 이러한 문제점을 개선하고자 등장한 것이 SDN(Software Defined Network)이다. SDN은 네트워크의 전달 기능과 제어 기능을 합쳐서 네트워크를 구성하는 새로운 방식으로 개방형 API를 통해 네트워크 트래픽 전달 동작을 소프트웨어의 작성으로 제어 가능한 기술이다.

네트워크의 제어 기능을 네트워크 장비들로부터 추상화시킴으로써 네트워크 서비스에 대한 효율성을 향상시킨 SDN 기술이 주목받고 있다[3]. 하지만 SDN도 여전히 기존 네트워크의 보안 취약점 중 IP 주소의 노출과 패킷 헤더 필드의 의도적 변경을 통한 네트워크 스캐닝, IP 스푸핑 등이 존재한다[4]. 이러한 문제를 해결하기 위하여 본 논문에서는 SDN 환경에서 형태보존암호를 이용한 IP 주소 암호화 기법을 제안한다. 형태보존암호로 IP 주소를 암호화함으로써 프로토콜의 구조 변경 없이 IP 스푸핑, 스니핑, 네트워크 스캐닝, 서비스 거부 공격으로부터 내부 자원을 보호할 수 있다. SDN 제어기는 사전에 인가된 단말의 네트워크 사용을 보장하기 위해 MAC 주소를 인증한다. 이후, SDN 제어기는 단말의 접근 권한을 구분하고 IP 주소를 암호화하기 위해 키 분배 프로토콜을 이용하여 단말에게 인증토큰과 IP 주소 암호화키를 전달한다. SDN을 이용하는 단말은 접근 권한에 따라 보안그룹을 구분하며, 보안그룹마다 각각 다른 암호화 키를 사용한다. 이때 암호화 알고리즘은 형태보존암호를 이용하며 IP 주소를 암호화하기 위해 사용된다. 암호화 키는 주기적으로 갱신되며 SDN 제어기는 보안그룹의 경로를 구성하는 스위치에게 IP 주소 암호화 키와 수신 단말까지의 경로 정보인 흐름제어규칙(flow rule)을 전달한다. 단말이 IP 주소 암호화 키와 인증토큰을 사용해야만 패킷을 전송할 수 있기 때문에 인증 받은 단말만이 네트워크를 사용함을 보장한다.

본 논문의 구성은 다음과 같다. 2장에서는 SDN, 형태보존암호에 대해 알아보고 이에 대해 분석한다. 3장에서는 SDN 환경에서 형태보존암호를 이용한 IP 주소 암호화 기법을 제안하고, 4장에서는 제안 기법에 대해 구현 및 실험을 통한 평가를 수행한다. 마지막으로 5장에서 본 논문의 결론을 맺는다.

Ⅱ. 관련 연구

2.1 SDN

SDN은 네트워크 제어 기능이 패킷 포워딩과 분리되어 직접 프로그래밍을 지원하는 새로운 네트워크 아키텍처이다. SDN은 OSPF(Open Shortest Path First) 및 BGP(Border Gateway Protocol)와 같은 레거시 프로토콜에 비해 라우팅 복구가 더 유리하다는 장점이 있다[5]. 네트워크 운영자 및 관리자는 분산되어 있는 다양한 네트워크 장비에서 수동적인 코드 라인의 입력을 통해 설정하는 것보다 소프트웨어 방식으로보다 능동적으로 네트워크를 설정할 수 있다[6]. SDN의 평면 간 인터페이스 구조에 따라 Open Flow, ForCES가 잘 알려져 있고, Open Flow 구조가 가장 많이 사용되고 있다. SDN의 제어 평면과 데이터 평면 사이의 정보 교환에 대한 표준화 연구가 진행 중이다[7]. [그림 1]은 SDN의 기본적인 구조이다.

네트워크 지능화 기능을 담당하는 응용 평면(Application Plane), 운영체제 기능을 담당하는 제어 평면(Control Plane), 데이터 전송을 담당하는 데이터 평면(Data Plane) 세 가지로 구분되고 각 레이어는 다음과 같은 특징을 가지고 있다. 응용 평면은 소프트웨어를 이용하여 네트워크를 제어하는 레이어이다. 네트워크 통계 정보를 활용하여 소프트웨어를 개발할 수 있는 개방형 영역이다. 제어 평면은 전반적인 네트워크 제어 및 관리를 한다. 제어 평면의 SDN 제어기는

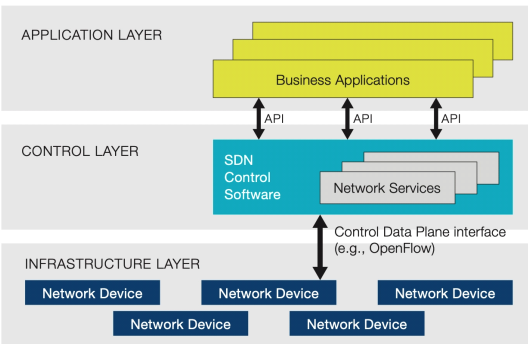

그림 1. SDN 기본 구조[7]
Fig. 1. SDN basic structure

패킷 흐름 제어를 위한 제어 논리를 가지고 있어야 한다. 제어 논리에는 스위칭, 라우팅, 방화벽 보안 규칙, DNS(Domain Name Service) 등이 있다[8]. 데이터 평면은 실제 네트워크 장비에 해당 되는 영역이며, 스위치나 라우터가 이 계층에 속한다.

SDN 제어기에는 네트워크 인프라를 제어하기 위한 흐름제어규칙이 있다. 흐름제어규칙은 프로토콜 정보, 포트, 우선순위 등이 저장되어 매치 되는 필드 정보에 따라서 발생한 패킷이 존재하는지에 대한 여부를 결정할 수 있다. 흐름제어규칙의 집합으로 정의된 흐름제어표(flow table)에 의해 우선순위대로 외부의 스위치로 전달하거나, 패킷을 수정하고 폐기하는 작업을 수행한다[9]. SDN의 패킷 전달 과정은 다음과 같다. SDN 제어기는 OVS(Open vSwitch)로 새로운 패킷과 흐름제어규칙을 전송한다. OVS는 자신의 흐름제어표를 흐름제어규칙의 우선순위와 비교하여 갱신하고 순위에 따라 패킷을 목적지로 전달한다.

2.2 SDN을 이용한 네트워크 자원 보호 연구

SDN이 발전하면서 보안 위협 또한 함께 증가하였다. 중앙집중형으로 운영되는 SDN은 공격자가 네트워크의 구조를 파악하기 쉽고 하나의 라우터를 공격하는 것보다 SDN 제어기에 대한 공격으로 전체 네트워크에 대한 공격이 가능하다. Yue Shi 외 2명은 SDN 환경에서 발생할 수 있는 보안 위협에 대해 연구하였다[10]. 제안한 기법은 목적지의 주소가 계속 바뀌거나, 공격자와 대상 사이의 네트워크와 접속 정책이 바뀌면 공격 성공률이 떨어지고 공격자의 노력이 크게 증가한다는 개념이다. 이외에도 SDN을 활용하여 네트워크 자원을 보호하기 위한 연구가 진행되고 있다.

Jafar Haadi 등은 주기적으로 단말 IP 주소 무작위 변이(Random Host Mutation)를 통해 스캐닝 공격의 성공률을 낮추는 기법을 제안하였다[11]. SDN 제어기에서 실제 IP로 변환되는 임의의 가상 IP를 할당하여 네트워크를 구성하였다. 제안한 기법은 스텔스 스캐닝(Stealthy Scanning), 웜 공격 및 기타 스캐닝 기반 공격에 효과적으로 대응 가능함을 보였다.

홍석찬은 SDN에서 검색 가능 암호화를 이용하여 IP 주소를 암호화하는 기법을 제안하였다[12]. 검색 가능 암호화를 통해 암호화된 패킷에서 목적지 IP를 추출한 후 스위치의 흐름 규칙에 따라 포워딩한다. 제안한 기법은 스니핑 및 위변조 공격으로부터 IP 주소를 보호하고 Host 인증 및 애플리케이션 서비스의 보안 그룹별 관리를 통해 SDN 내부 자원의 보호가 가능함을 보였다.

IP 주소 무작위 변이 기법과 검색 가능 암호화를 이용한 IP 주소 암호화 기법의 두 연구는 보안성 향상을 통하여 기존의 SDN에서 보다 내부 자원의 보호에 효과적인 대응이 가능함을 보였다. 하지만, IP 주소 무작위 변이 기법은 IP 주소 변이에 나머지 연산만을 사용하기 때문에 통신 중인 하나의 IP 주소가 유출되었을 때, 통신 중인 다른 IP 주소를 유추할 수 있는 보안 취약점이 존재한다. 검색 가능 암호화를 이용한 IP 주소 암호화 기법은 암호화를 위해 생성하는 암호화된 질의 키워드인 트랩도어들의 수에 의해 사용자가 이용할 수 있는 검색 질의의 수가 제한된다는 한계점을 갖는다. 또한, 트랩도어를 이용한 검색 방법은 외부 저장 공간에 저장된 데이터에 대한 수정을 가할 때마다 트랩도어의 업데이트와 재분배가 필요하다[13]. 본 논문은 세 가지 연구에서 제시된 문제에 대응하며 IP 주소를 보호하는 기법을 제안한다. 암호화를 사용하여 주소를 암호화하면 통신 중인 다른 단말의 IP 주소 유추가 불가능하다. 형태보존암호는 암호화 키와 트윅만 사용하여 암호화하기 때문에 외부 저장소가 필요하지 않다.

2.3 형태보존암호

형태보존암호(Format-preserving Encryption)는 평문의 형태와 길이를 그대로 유지하여 암호화하는 방식이다. 예를 들어 신용카드번호, 주민등록번호와 같은 개인식별정보에 형태보존암호화를 적용하는 경우, 평문과 형태가 동일한 암호문을 출력할 수 있다. 이러한 형태보존암호화는 여러 가지 방법으로 설계할 수 있는데 Prefix 암호, Cycle walking, Feistel 구조 채택 등이 그 방법들이다. 1997년 Michael Brightwell이 최초로 제안하여[14], 현재 다양한 형태보존암호 모드가 존재한다. 대표적으로 NIST 표준인 FF1, FF3-1[15]과 TTA 표준인 FEA[16]가 있다. Feistel 구조에 기반한 형태보존 암호 중 FF1은 Alternating Feistel 구조에 기반한 형태보존 암호 알고리즘으로 NIST 블록암호 운용모드 제안 후보 중의 하나이다. FF1의 암호화 과정은 [그림 2]와 같다. 형태보존 암호화를 위해 왼쪽 입력값(Left Input Value)과 오른쪽 입력값(Right Input Value)으로 구분한다. 왼쪽 입력값, 오른쪽 입력값 모두 트윅(T), 입력값 길이(n), 라운드 수와 함께 F 함수의 입력으로 사용되어 서브키(Sub Key)가 생성된다. 서브키를 사용하여 각 입력값을 한 블록씩 라운드 함수로 암호화 한다. 각 라운드 함수(FK)는 라운드마다 모듈러 덧셈(+)에 해당되는 블록의 길이에 맞춰 결

과값을 출력한다. 복호화 과정은 위와 동일하나 모듈러 덧셈 대신 모듈러 뺄셈을 사용한다. 암호화 과정을 통해 평문과 형태가 동일한 암호문을 정의된 radix 내의 문자로 출력하여 형태를 보존한다. FF1은 입력의 길이와 radix를 사용하여 스트링 포맷을 유지하고 서브키 생성을 위한 F 함수의 코어 알고리즘으로 블록 암호나 해시 함수를 사용한다. 안전성은 F 함수의 블록 암호나 해시 함수에 의존한다.

형태보존암호는 일반적인 암호화와는 달리 데이터와 연관된 부가정보인 트윅을 적용하여 암호화가 필요한 데이터의 길이를 유지할 수 있다. 또한, Feistel 구조와 유사한 수준의 안전성을 가지며, 평문 데이터의 길이를 보존하고 프로토콜이나 DB 스키마 변경을 최소화한다는 장점이 있다. 이와 더불어 형태보존암호에서 평문의 길이가 짧다면, 라운드 수를 증가시키는 방법을 적용하여 큰 비용을 발생시키지 않고 메시지 복구 공격에 충분한 안전성을 확보하는 기법 등 다양한 방법에 대한 연구가 진행 중이다[17].

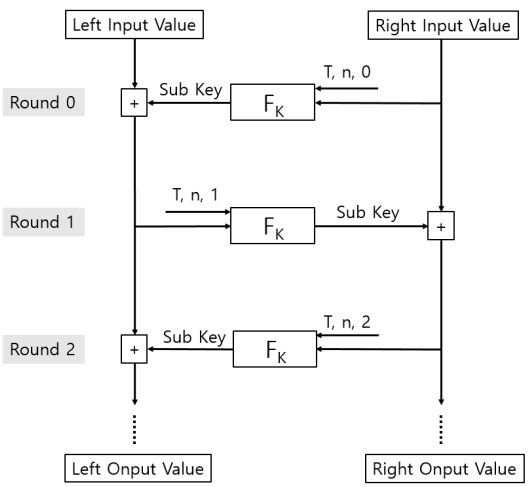

그림 2. FFX 알고리즘 구조
Fig. 2. FFX Algorithm structure

Ⅲ. 형태보존암호를 이용한 IP 주소 암호화 기법 제안

본 장에서는 SDN에서 IP 주소를 근본적으로 보호하기 위해 형태보존암호를 이용하여 IP 주소를 암호화하는 기법을 제안한다. 제안하는 기법은 단말과 SDN 제어기의 인증 과정, 단말의 접근 권한에 따른 보안 그룹화, 암호화, 패킷 전송으로 구성된다. SDN 제어기는 통신 경로 상의 스위치로 IP 주소 암호화 키와 수신 단말까지의 경로인 흐름제어규칙을 생성하여 전달한다. 스위치는 흐름제어규칙을 통해 다음 스위치로 패킷을 이동하고 수신 단말과 직접 연결된 해당 스위치는 패킷을 수신 단말로 전송한다. 단말 인증 및 형태보존암호화 키 관리 절차를 통하여 보안그룹별 암호화에 사용되는 키를 관리한다. 패킷을 전달할 때, IP 주소는 관리된 키로 암호화되어 전송된다.

3.1 단말 인증 및 형태보존암호화 키 관리 절차

제안하는 프로토콜은 SDN에서 단말이 내부 네트워크 자원을 사용할 수 있도록 SDN 제어기와 통신하기 위해 인증 및 키 분배를 위해 사용된다. 신뢰성을 필요로 하는 네트워크 인프라 서비스를 지원하기 위해서는 단말의 신뢰성을 확보하기 위한 단말 인증 기능이 필요하다. 프로토콜의 단말 인증 및 키 관리 절차는 단말과 SDN 제어기 사이에 어떠한 보안 프로토콜도 제공되지 않는 경우를 고려하여 작성하였다. [표 1]은 제안 프로토콜에서 사용되는 연산자와 함수에 대한 정의이다.

[그림 3]의 단말 인증 및 키 관리 절차에 대한 내용은 다음과 같다.

step 1. 단말은 자신의 ID(H)와 난수 N을 SDN 제어기에게 전송한다.

step 2. SDN 제어기는 단말에게 자신의 개인키(PR(C))로 암호화된 세션키 SK와 N+1을 단말의 공개키 PU(H)로 암호화하여 전송한다. 단말은 자신의 개인키(PR(H))로 암호문을 복호화하고 다시 이 값을 SDN 제어기의 공개키(PU(C))로 복호화하여 세션키

표 1. 제안 프로토콜 용어
Table 1. Notations

기호	정의
ID(H)	단말 식별 정보
N	난수값
A‖B	A와 B를 연접
PU(H)	단말의 공개키
PR(H)	단말의 개인키
SK	세션키
PU(C)	제어기의 공개키
PR(C)	제어기의 개인키
Token	인증 토큰(인증정보, 보안그룹)
FPEK	형태보존암호 키
K	인증토큰을 암호화하기 위한 대칭키

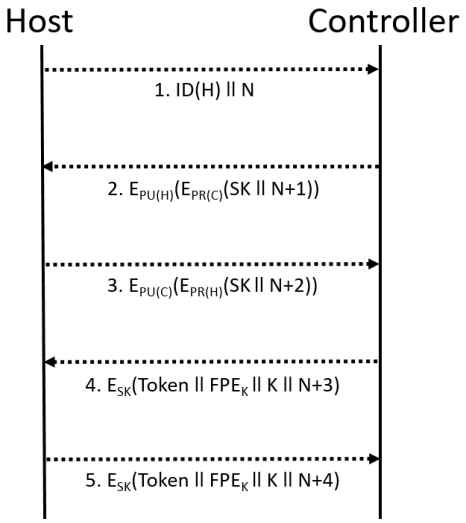

그림 3. 단말 인증 및 키 관리 과정
Fig. 3. Process for host authentication and key management protocol

를 얻는다.

step 3. 단말은 SDN 제어기에게 세션키를 사용한 통신이 준비됨을 알리기 위해 전달받은 세션키와 N+3을 자신의 개인키(PR(H))로 암호화한 후 SDN 제어기의 공개키로 암호화하여 전송한다.

step 4. SDN 제어기는 단말에게 형태보존암호 키(FPE_K)와 대칭키(K)와 N+4를 세션키로 암호화하여 전송한다. 단말은 SDN 제어기로부터 받은 암호문을 세션키로 복호화함으로 형태보존암호 키와 대칭키를 얻는다.

step 5. 단말은 SDN 제어기에게 세션키로 형태보존암호 키, 대칭키 및 N+5를 암호화하여 전송함으로 이후에 있을 통신 준비가 되었음을 알린다.

3.2 형태보존암호를 이용한 IP 주소 암호화 과정

8개의 단말(h1~h8)을 3개의 OVS 스위치(s1~s3)와 연결한다. 단말 간 연결되는 3개의 스위치는 SDN 제어기(c0)에 연결한다. 제안 방식을 [그림 4]와 같이 구성하였다. 단말 인증 후 형태보존암호를 이용한 통신을 위한 IP 주소 암호화 과정은 다음과 같다.

[그림 5]는 송신 단말(Host1)에서 수신 단말(Host2)까지 통신 과정을 나타낸다. 송신 단말은 대칭키로 암호화한 인증토큰(Token) 및 형태보존암호화한 수신 단말의 IP 주소(enIP) 와 포트번호(Port)를 목적지로 한 패킷을 스위치(SDN Switch1)로 전송한다. 스위치는 패킷의 헤더와 일치하는 흐름제어규칙이 없으면 SDN 제어기(SDN Controller)로 패킷을 전달한다. SDN 제어기는 패킷의 인증 정보를 확인하여 인증되지 않은 사용자라면 패킷을 폐기하고 인증된 사용자라면 보안그룹의 키로 IP 주소를 복호화하여 목적지 IP 주소를 실제 수신 단말의 IP 주소(rIP)로 복호화한다. SDN 제어기는 권한이 없어 복호화에 실패한 경우 패킷을 폐기한다. SDN 제어기는 암호화된 IP 주소와

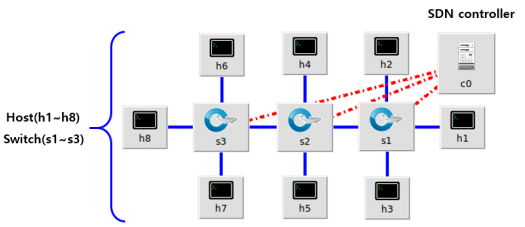

그림 4. 제안 방식 구성도
Fig. 4. Experiment Architecture

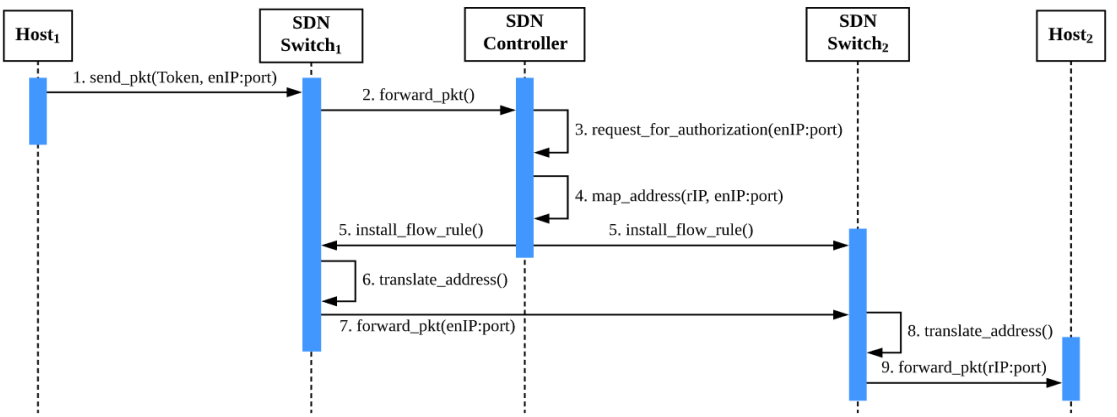

그림 5. SDN에서 형태보존암호를 적용한 패킷의 통신 과정
Fig. 5. Communication via FPE

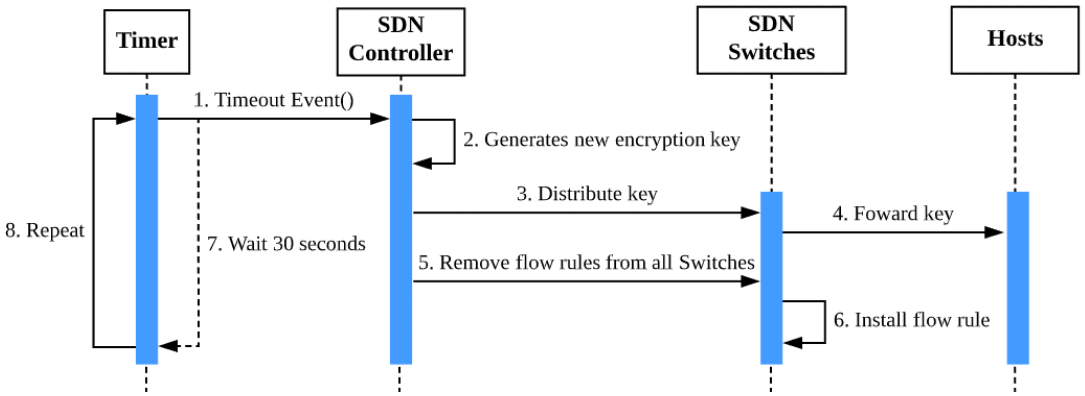

그림 6. 형태보존암호를 이용한 IP 주소 암호화 기법의 생명주기
Fig. 6. Lifecycle of communication via FPE

실제 IP 주소를 매핑시켜 같은 IP 주소에 대해 반복적인 복호화 요청이 입력될 때 빠른 주소 탐색이 가능하게 한다. 복호화가 완료되면 SDN 제어기는 통신 경로 상의 스위치에 흐름제어규칙을 추가한다. 스위치는 흐름제어규칙을 통해 경로 상의 다음 스위치 주소를 알 수 있고 패킷을 해당 스위치로 전달한다. 수신 단말과 직접 연결된 스위치(SDN Switch2)는 패킷을 수신 단말로 전송한다. 제안하는 기법은 [그림 6]의 생명주기를 가진다. SDN 제어기 내에 위치한 Timer 객체는 30초 주기로 timeout() 이벤트를 발생한다. timeout() 이벤트는 형태보존암호화 키를 생성하는 함수와 연결되어 있으며 암호화 키를 재생성하여 새로운 IP 주소로 암호화한다. SDN 제어기가 timeout() 이벤트를 수신하면 새로운 암호화 키를 생성하고 네트워크 상에 있는 모든 스위치에게 흐름제어표를 삭제하도록 한다. 스위치는 SDN 제어기로부터 받은 암호화 키를 단말에게 전달하고 이전 암호화 키로 암호화한 흐름제어표를 삭제한다. 만약 연결이 이미 성립되어 통신 중인 세션이 있는 경우 세션이 끝난 후에 흐름제어표를 삭제하도록 하여 통신의 가용성을 보장한다.

Ⅳ. 구현 및 평가

본 장에서는 형태보존암호를 이용한 IP 주소 암호화 기법의 성능, 보안성을 평가한다. 제안한 기법을 가상 네트워크 환경에 구현하여 실제 동작 여부와 성능을 두 가지 실험을 통해 확인하였다. 실험 환경은 [그림 4]와 같이 구성하였고 모든 노드의 대역폭을 100Mbit/s로 설정하였다. 제안한 기법을 Intel i7-8700 @4.6GHz CPU와 8GB 램 환경에서 Ubuntu 16.04 운영체제와 Python 언어 기반인 SDN 제어기인 Ryu 4.34로 구현하였다.

4.1 구현

4.1.1 형태보존암호를 이용한 IP 주소 암호화 구현

인증 받은 단말은 다른 단말과 통신을 위해 제어기에게 암호화 키를 발급받고 목적지의 IP 주소를 암호화하여 패킷을 전송한다. 가상환경에서 단말 h2와 h8의 실제 IP 주소와 암호화된 IP 주소는 [표 2]와 같다.

단말 h2가 h8에 ICMP패킷을 보내는 것으로 가정하였을 때, 단말 h2는 h8의 암호화된 IP 주소인 “10.213.183.79”을 목적지 IP 주소로 패킷을 전송하게 된다. SDN 제어기는 암호화된 목적지 IP 주소를 h2가 속한 보안그룹의 키로 복호화한 후에 등록된 IP 주소가 존재한다면 h8까지 경로 정보인 흐름제어규칙을 스위치의 흐름제어표에 추가한다. 패킷은 스위치의 존재하는 흐름제어규칙에 의해 목적지까지의 경로를 탐색할 수 있고 이를 통해 목적지와 통신을 할 수 있다. [표 3]은 통신 과정 중 스위치 3의 흐름 제어 테이블을 나타낸 것이다.

패킷의 출발지 IP 주소(nw_src)가 10.145.154.56이고 목적지 IP 주소(nw_dst)가 “10.213.183.79”인 패킷

표 2. 단말 h2, h8의 실제 IP 주소와 암호화된 IP 주소
Table 2. Real IP address and encrypted IP address for terminal h2, h8

host	Original IP	Encrypted IP
h2	10.0.0.2	10.145.154.56
h8	10.0.0.8	10.213.183.79

표 3. 스위치 3의 흐름제어표
Table. 3. Switch 3 Flow table

Switch 3(s3)
NXST_Flow reply(xid=0x4): - cookie=0x0, duration=4.237s, table=0, n_packet=3, n_bytes=294, idle_age=2, priority=1, ip,in_port=1, nw_src=10.145.154.56, nw_dst=10.213.183.79, actions=mod_nw_dst:10.0.0.8,output:4 - cookie=0x0, duration=4.234s, table=0, n_packets=3, n_bytes=294, idle_age=2, priority=1, ip,in_port=4, nw_src=10.0.0.8, nw_dst=10.145.154.56, actions=mod_nw_src:10.213.183.79,output:1 - cookie=0x0, duration=23.415s, table=0, n_packets=2, n_bytes=196, idle_age=4, priority=0 actions=CONTROLLER:65535

이 스위치에 전달되면, 단말의 실제 IP 주소(mod_nw_dst)인 "10.0.0.8"과 단말과 직접 연결된 4번 포트(output:4)로 통신하도록 흐름제어규칙이 설정된 것을 확인할 수 있다. 두 번째 흐름제어규칙에서 출발지 IP 주소(nw_src)가 "10.0.0.8"이고 목적지 IP 주소(nw_dst)가 "10.145.154.56"인 경우 암호화된 출발지 IP 주소(mod_nw_src)인 "10.213.183.79"로 변경하여 패킷을 전송하도록 흐름제어규칙이 설정된 것을 확인할 수 있다.

4.1.2 스캐닝 공격 대응성 실험

본 항에서는 공격 성공 확률과 관련하여 네트워크 스캐닝 공격하에 제안한 기법의 효과를 평가한다. 공격자는 공격 대상 단말을 선정하기 위해 임의 IP 주소를 선정한 다음 단말에서 포트 검색을 수행하여 활성 서비스를 검색한다. 임의 IP 주소를 선정하기 위해 공격 대상 단말을 탐색하는 기술 중 비반복적 검색(Non-repeat Scanning)을 수행한다고 가정한다. 공격자는 모든 IP 주소를 순차적으로 목적지로 하여 ICMP, ARP 메시지를 단말로 전송하고 응답 여부를 통해 단말의 동작 여부를 확인한다. Nmap과 같은 네트워크 검색 도구를 사용하여 공격 대상 단말을 구분하고 이를 목록화하여 공격한다. 네트워크의 공격 성공률(Attack Success Probability)은 주소 공간, 스캔 시도 횟수, 키 재생성 빈도 등 다양한 변수의 영향을 받는다[18]. 고정 주소 네트워크와 제안하는 기법의 공격 성공률의 비교를 위해 주소 공간은 IP 주소의 Class-B(10.0.0.0/16) 대역을 사용하였고 스캔 시도 횟수는 IP 주소 대역 전체를 대상으로 1회씩 하였다. 암호화 키 재생성 주기를 30초로 설정하고 동작하는 단말을 30개, 60개 그리고 255개로 설정하여 실험하였다. 실험 결과는 [그림 7]과 같다.

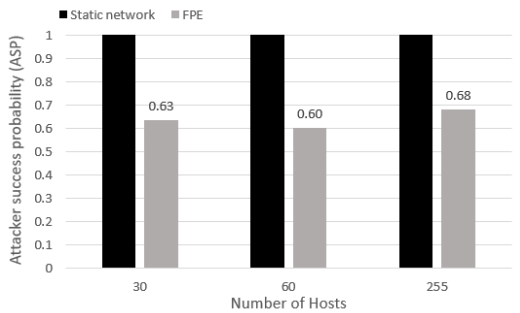

그림 7. Static Network와 FPE의 네트워크 단말 수에 따른 공격 성공률
Fig. 7. Attack success probability based on the number of network terminals on the static network and FPE

[그림 7]은 네트워크 단말 수에 따른 스캐닝 공격에 대한 공격 성공률을 나타낸다. 이를 위해서 단말 수를 변화시키면서 스캐닝 공격을 수행하였다. 고정 주소 네트워크는 전체 IP 주소 대역을 스캔했을 때 모두 100%의 공격 성공률을 보였다. 그러나 제안하는 기법을 적용했을 때 공격 성공률은 단말의 수에 따라 30대, 60대, 255대에서 각각 63%, 60%, 68%로 나타났다. 결과는 공격자가 네트워크 대역 전체에 대해 스캐닝 공격을 수행하였을 때, 공격 성공률은 최대 68%(0.68)로 나타났다. 이는 공격자가 전체 단말 중 약 32%의 단말을 발견하지 못했다는 것을 의미한다. 이를 통해 제안 기법 적용 시 네트워크 스캐닝 공격 방어에 유효함을 확인할 수 있었다.

[그림 8]은 IPv4 Class-A와 Class-B, Class-C의 범위에서 단말 IP 주소의 발견을 목표로 하는 네트워크 공격 성공률을 나타낸다. Class-C(2^16 = 65,536)의 모든 단말 IP 주소를 스캔할 때 공격 성공률이 68%(0.68)으로 나타났다. Class-A(2^24 = 16,777,216), Class-B(2^20 = 1,048,576)의 주소 공간에서 Class-C와 동일한 스캔 시도(65536회)를 했을 때 Class-C에 비해 더 낮은 공격 성공률을 보였다. 따라서 Class-A와 Class-B의 단말 IP 주소를 스캔하기 위해서는 광범위한 IP 주소 공간의 스캔이 필요하다.

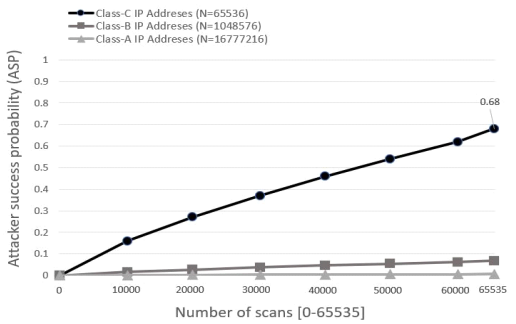

그림 8. Class-A, Class-B 와 Class-C의 단말 IP 주소 네트워크 스캐닝 공격 성공률
Fig. 8. Success probability of terminal IP address network scanning attacks by Class-A, Class-B and Class-C

4.2 비교 및 평가

4.2.1 네트워크별 보안성 비교

네트워크의 보안성은 기존 보안 장비들의 보안기능 및 기존 자원 보호 기술과 비교를 통해 평가하였다[19]. 내부 네트워크의 접근을 통제하는 보안 장비 중 방화벽(firewall)과 비교하여 평가하였다. 방화벽과 제안한 기법은 능동적으로 단말을 점검 관리하여 접속 단말에 대한 보안 평가, 문제점, 정책을 준수 여부 등을 지속해서 모니터링 하는 공통점이 있다. 또한, IPsec VPN과 제안한 기법은 IP 계층의 안전한 통신을 위해 패킷을 암호화하여 기밀성과 무결성을 제공한다는 공통점이 있다. SDN 자원 보호 기법 중 IP 주소 무작위 변이 기법(RHM)과 제안하는 기법은 SDN에서 네트워크 자원 중 IP 주소를 보호한다는 공통점이 있다. 네트워크 보안 기능은 여섯 가지 항목으로 보안성을 평가한다.

- 기밀성 : 패킷을 도청, 위변조 공격으로부터 안전하게 보호하기 위해 요구되는 항목이다. 헤더(header)와 페이로드(payload)로 구분하여 평가한다.
- 단말 인증 : 신뢰성을 필요로 하는 네트워크 인프라 이용 서비스를 지원하기 위해서는 단말의 신뢰성을 확보하기 위해 요구되는 항목이다.
- 불법 접근차단 : 취약 단말을 표적으로 하는 불법적인 네트워크 자원의 접근을 통한 데이터 스니핑 및 침입 시도를 방지하고 네트워크 자원을 안전하게 보호하기 위해 요구되는 항목이다.
- Flow 분리 : 네트워크 서비스 및 환경의 특성에 맞는 네트워크 보안정책을 분리 운영하기 위해 요구되는 항목이다.
- 보안 기능 확장성 : 변화하는 네트워크 및 네트워크 서비스 환경에 대응하여 신규로 요구되는 네트워크 보안 기능을 확장하기 위해 요구되는 항목이다.
- 브로드캐스트 도메인 설정 : 보안 관리 편의성에서 파생된 항목으로 보안그룹별 보안정책 수정 및 모니터링 등 보안 기능을 효율적으로 유지하고 관리하기 위한 항목이다.

네트워크별 보안성 항목 평가 결과는 [표 4]와 같다. O는 해당 기능을 수행함을, X는 수행할 수 없음을 의미한다.

방화벽(Firewall), IPSec VPN, IP 주소 무작위 변이 기법, 제안한 기법 모두 인증받지 않은 단말로부터 네트워크 불법 접근을 차단한다는 공통점이 있다. 하지만 방화벽은 패킷에 대한 검사만 수행하기 때문에 기밀성을 제공하지 않는다. IPSec VPN은 AH(Authentication Header)와 ESP(Encapsulating Security Payload)를 통해 패킷의 헤더와 페이로드의 기밀성을 보장한다. 제안한 기법은 패킷 헤더의 IP 주소를 암호화하기 때문에 헤더에 대한 기밀성을 보장한다. 페이로드의 기밀성은 응용 평면에서 암호화 기능을 제공하면 보완할 수 있다. 방화벽과 IPSec VPN은 펌웨어나 프로토콜에 정의된 규칙만 적용하여 패킷을 제어하기 때문에 확장성과 편의성을 지원하지 않는다. 하지만 SDN 제어기는 개방형 표준과 API를 사용하므로 다양한 제조사의 네트워크 장비의 제어 및 관리가 가능하다. 소프트웨어의 사용은 네트워크 장비에 덜 의존하는 환경 구축을 가능하게 한다. 또한, 중앙 집중식 제어로 인해 네트워크 장비를 신속하게 구성하고 배치할 수 있다. SDN 자원 보호 기법 중

표 4. 네트워크별 보안성 항목 평가
Table 4. Evaluation of security

구분		AS-IS Network		MTD	
		Firewall	IPsec VPN	RHM	Proposed SDN
기밀성	Header	X	O	O	O
	Payload	X	O	X	X
단말 인증		X	O	O	O
불법접근차단		O	O	O	O
Flow 분리		X	X	O	O
보안기능 확장성		X	X	O	O
브로드캐스트 도메인 설정		X	X	X	O

RHM은 브로드캐스팅 범위의 지정이 어려워 보안그룹별 정책의 적용이나 모니터링이 어렵다. 하지만 형태보존암호는 암호화 범위를 직접 지정할 수 있어서 보안정책의 관리가 용이해진다. 제안하는 기법은 대부분 항목에서 기존 장비나 기술에 비해 네트워크와 관련된 보안성 항목에 대응하는 것을 확인할 수 있다. IP 주소 무작위 변이 기법은 나머지 연산을 통해 주소를 분배한다. 따라서 하나의 단말 IP 주소가 유출되었을 때 나머지 단말의 주소를 알 수 있다. 하지만 제안하는 기법은 IP 주소를 직접 암호화하기 때문에 하나의 단말 IP 주소가 유출되더라도 전체 네트워크를 보호할 수 있다. 검색 가능 암호화를 이용한 IP 주소 암호화 기법은 트랩도어들의 수에 의해 사용자가 이용할 수 있는 검색 질의의 수가 제한된다. 하지만 제안하는 기법은 키생성과 키분배 프로토콜에 의해 호스트의 수와 관계없이 통신이 가능하다.

4.2.2 네트워크별 공격 대응성 평가

제안한 기법의 공격 대응성을 평가한다. 평가를 위해 SDN에서 발생할 수 있는 공격 유형인 "Threats to Security in SDN Environments"을 평가항목으로 선정하였다[20]. 공격자는 네트워크 외부에서 발생할 수 있는 모든 공격을 수행할 수 있다고 가정한다. [표 5]는 제안하는 기법의 네트워크 공격 대응성을 평가하고 대응 상세 내용을 보여준다.

- Eavesdropping : SDN 제어기와 스위치, 스위치와 단말 사이의 패킷을 도청하는 공격이다.
- Network scanning : 외부에서 IP 주소, 포트 번호 등 네트워크 자원 정보를 수집하는 공격이다.
- Dos attack : 외부에서 조작된 트래픽을 대량으로 발생시켜서 스위치나 SDN 제어기의 정상적인 동작을 불가능하게 하는 공격이다.
- Flow rule confliction : 동일한 우선순위를 가진 흐름제어규칙을 여러 개 생성하여 규칙이 충돌하면서 흐름 제어 의도와 맞지 않는 트래픽을 발생하는 공격이다.
- Fake flow rule insertion : 조작된 흐름제어규칙이 추가되면 기존의 보안정책을 우회하거나 패킷의 흐름을 변경하는 공격이다.
- Spoofing : 공격자가 정상적인 사용자 또는 관리자로 위장하여 중요 정보를 가로채거나 조작하는 공격이다. SDN에서 중요 정보는 스위치의 흐름제어표나 전체 단말 정보가 된다.
- Repudiation : 사용자가 흐름제어표에 삽입한 악의적인 흐름제어규칙의 생성 사실을 부인하는 공격이다.

제안하는 기법은 단말의 IP 주소를 암호화하여 기밀성을 제공하기 때문에 단말을 특정하여 시도하는 공격인 Eavesdropping, Network scanning, Dos attack, Spoofing 공격에 일부 대응하거나 완전대응한다. 암호화된 IP 주소로는 공격자가 단말을 특정할 수

표 5. 제안하는 기법의 네트워크 공격 대응성 평가
Table 5. The relationship between security requirements and attackt threats

구분	대응성	내용
Eavesdropping	△	- 패킷의 출발지와 목적지의 암호화된 IP주소를 도청하더라도 단말을 특정할 수 없다. - 헤더에 대한 기밀성은 제공하지만 페이로드는 보호되지 않는다. - 애플리케이션 계층에서 페이로드 암호화를 제공하는 방식으로 보완 가능하다.
Network Scanning	O	- IP 주소의 암호화로 기밀성을 보장한다.
Dos attack	O	- 보안 그룹별 IP 주소를 암호화를 제공함으로 서비스 거부 공격을 위한 목적지 주소 설정이 어렵다. - 주기적으로 새로운 암호화 키로 IP 주소를 암호화하기 때문에 지속적인 공격이 불가능하다.
Flow rule Confliction	O	- SDN 제어기는 각 보안그룹 별 단말 접근 권한을 확인 후 보안 등급으로 우선순위를 지정하여 흐름제어규칙을 생성하기 때문에 충돌이 발생하지 않는다.
Fake flow rule insertion	O	- 인증 받은 단말만이 목적지 IP 주소까지의 경로 생성 요청이 가능하고 SDN 제어기가 중복여부를 검사한 후 흐름제어규칙을 생성한다.
Spoofing	O	- 패킷의 IP 헤더에 대한 암호화를 수행하므로 IP 주소에 대한 기밀성과 무결성을 제공한다. 따라서 IP 주소에 대한 위변조 공격은 불가능하다.
Repudiation	O	- 흐름제어규칙 생성 요청 시 단말 인증 정보를 패킷에 추가하여 SDN 제어기에 전송하기 때문에 부인방지가 가능하다.

없기 때문에 단말의 상태, 사양, 취약점 등 각종 정보를 식별할 수 없다. 단말을 식별하더라도 주기적으로 암호화 키를 변경하기 때문에 같은 단말을 탐색하기 위해서 네트워크 대역에 대한 스캐닝을 다시 수행해야 한다. 또한, 인증받지 않은 단말은 SDN 제어기에 흐름제어규칙 추가 메시지를 전송할 수 없기 때문에 스위치의 흐름제어표의 무결성이 보장되며 보안그룹에 따라 흐름제어규칙의 우선순위를 관리하기 때문에 Flow rule confliction, Fake flow rule insertion 등의 공격에 대응 가능하다.

4.2.3 제안한 기법과 기존 기법의 네트워크 지연 비교

제안하는 기법이 네트워크 성능에 얼마나 영향을 미치는지 확인하기 위한 실험이다. 이를 위해서 네트워크의 성능을 판단하는 요소 중 왕복 지연시간(RTT;Round Trip Time) 지연을 측정하였다. 제안한 기법과 비교 평가를 위해 기존 SDN 환경의 IP 주소 보호 기법 중 Jafar Haadi 외 2명이 제안한 RHM(Random Host Mutation)기법을 동일 환경에 구현하여 비교하였다. 실험 결과는 [그림 9]와 같다.

RHM 기법과 제안한 기법의 지연시간을 측정한 결과 약 95%가 0.1~0.2ms의 값으로 측정되었다. 지연시간의 평균을 비교했을 때 형태보존암호기법의 적용 시 약 7ms의 속도 개선이 있었다. TCP 네트워크의 특징과 SDN 제어기에서 흐름제어규칙을 가져오는 과정 때문에 기법 적용 직후 첫 번째 패킷에서 높은 지연이 발생하였다. 그 이유는 TCP는 네트워크 혼잡을 줄이면서 전송률을 최대한 높이기 위해 혼잡 제어(Congestion Control) 알고리즘을 사용하기 때문이다. 데이터 전송 초기에는 네트워크 상태의 혼잡 여부를 판단할 수 없기 때문에 느린 시작을 수행하여 작은 혼잡 윈도우 크기에서부터 시작하여 패킷 전송을 천천히 시작하지만 윈도우의 크기를 지수적으로 증가시켜 전송량을 급격히 증가시킨다[21]. 그리고 스위치는 처음 흐름제어표에서 경로를 정의하기 위해 제어기를 경유해야 한다. 흐름제어규칙이 설치되지 않은 첫 번째 패킷에서 다른 패킷에 비해 비교적 높은 지연율이 측정되었다.

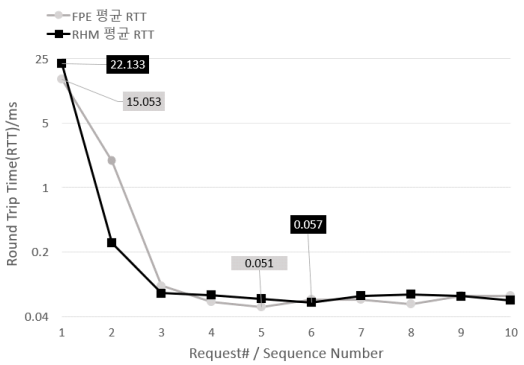

그림 9. RHM 기법과 FPE 기법의 왕복 지연시간 비교
Fig. 9. Comparison of latency between RHM and FPE

V. 결 론

SDN은 기존 네트워크 취약점을 그대로 물려받아 IP 주소 노출에 의한 네트워크 자원 식별 및 IP 주소 위변조 공격에 대응하지 못한다. 이에 본 논문에서는 SDN환경에서 형태보존암호를 이용한 IP 주소 암호화 기법을 제안하였다. 패킷의 목적지 IP 주소에 대하여 형태보존암호를 이용한 암호화 및 보안그룹별 흐름제어규칙 설정 및 암호화 키 관리 기법으로 구성된다. 제안하는 기법의 검증은 네트워크에서 필수적으로 요구되는 보안성 항목을 선정하여 기존 네트워크 보안장비와 비교하여 평가하였다. 가상환경에서 제안 기법을 적용하여 전체 단말 중 약 32%의 단말이 네트워크 스캐닝 공격에 대응 가능함을 보였다. 속도 비교 실험을 통해 기존 SDN의 네트워크 자원 보호 기법인 RHM과 비교하여 약 3%의 지연시간 감소를 확인하였다. 제안하는 기법의 네트워크 공격 대응성 평가를 통해 네트워크 스캐닝 공격에 대한 대응 가능성을 확인하였다. 향후 연구에서는 가상 환경을 구축하여 서비스 거부, 스푸핑 등 네트워크 공격 대응에 대한 연구를 진행할 예정이다.

References

[1] S. K. Kwak, “A study on effective APT attack defense of endpoint level at enterprise,” M.S. Thesis, University of Dongguk, 2020.

[2] B. D. Han and S. H. Woo, “Cyber attack and security using machine learning,” in *Proc. KIICE Int. Conf. Commun.,* pp. 551-553, Gyeongju, Jul. 2020.

[3] E. J. Son, “Entropy based DDoS attack defense technique using cooperative QoS in SDN environment,” M.S. Thesis, University of Hanyang, 2019.

[4] J. W. Seo and S. J. Lee, “A study on detection of DDos attack using the IP spoofing,” *J. KIISC*, vol. 25, no. 1, pp.

147-153, Feb. 2015.

[5] H. Zhang and J. Yan, "Performance of SDN routing in comparison with legacy routing protocols," *IEEE Commun. Cyber C*, 2015.

[6] C. H. Oh, J. H. Kang, and M. S. Jun, "Trend of software defined network," in *Proc. KIPS Int. Conf. Commun.*, pp. 131-133, Busan, Nov. 2016.

[7] IEEE ComSoc, *SDN Standards Activities in ITU-T and other SDOs*(2015), Retrieved Sep. 5, 2020, from https://techblog.comsoc.org/2015/07/05/sdn-standards-activities-in-itu-t-and-other-sdos

[8] H. Arora, *Software Defined Networking(SDN) - Architecture and role of OpenFlow*(2015), Retrieved Sep. 12, 2020, from https://www.howtoforge.com/tutorial/software-defined-networking-sdn-architecture-and-role-of-openflow/

[9] J. Y. Hong, "A scalable message flow control mechanism in SDN," M.S. Thesis, University of Ajou, 2015.

[10] Y. Shi, F. Dai, and Z. Ye, "An enhanced security framework of software defined network based on attribute-based encryption," *IEEE ICSAI*, pp. 965-969, Hangzhou, China, 2017.

[11] J. H. Jafarian, E. A. Shaer, and Q. Duan, *OpenFlow Random Host Mutation: Transparent Moving Target Defense using Software Defined Networking*(2012), Retrieved Aug. 13, 2020, from http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p127.pdf

[12] S. C. Hong, "IP address encryption method in sdn environments using searchable encryption," M.S. Thesis, University of Soongsil, 2014.

[13] M. K. Joo, "Shared and searchable encrypted data for semi-trusted servers with controllable sharing property," M.S. Thesis, Pohang University of Science and Technology, 2015.

[14] B. Michael and S. Harry, "*Using datatype preserving encryption to enhance data warehouse security*(1997)," Retrieved Sep. 20, 2020, from https://csrc.nist.gov/csrc/media/publications/conference-paper/1997/10/10/proceedings-of-the-20th-nissc-1997/documents/141.pdf

[15] NIST, Special Publication 800-38G Revision 1: *Recommendation for Block Cipher Modes of Operation-Methods for Format-Preserving Encryption*(2019), Retrieved Aug. 23, 2020, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38Gr1-draft.pdf

[16] *Format-Preserving Encryption Algorithm FEA*(2015), Retrieved Sep. 3, 2020, from http://www.tta.or.kr

[17] S. Y. Jeong, D. W. Hong, and C. H. Seo, "Secure format preserving encryption for message recovery attack," *J. KIISE*, vol. 44, no. 8, pp. 860-869, Aug. 2017.

[18] D. P. Sharma, D. S. Kim, S. Yoon, H. Lim, J. H. Cho, and T. J. Moore, "FRVM: Flexible random virtual IP multiplexing in software-defined networks," *IEEE Commun. Trustcom*, vol. 17, pp. 579-587, 2018.

[19] S. W. Ahn, "Defense against SYN flooding attack for SDN network," M.S. Thesis, University of Soongsil, 2018.

[20] J. Spooner and S. Y. Zhu, "A review of solutions for SDN-Exclusive security issues," *IJACSA*, vol. 7, no. 8, pp. 113-122, Nov. 2016.

[21] J. H. Jung, "Communication history based latency reduction for QUIC protocol," M.S. Thesis, University of Changwon, 2018.

박 도 현 (Dohyeon Park)

2015년 3월~현재 : 순천향대학교 정보보호학과 학사

<관심분야> 정보보안, SDN, 네트워크 보안, 모바일 보안

장 래 승 (Raeseung Jang)

2015년 3월~현재 : 순천향대학교 정보보호학과 학사

<관심분야> 정보보안, 네트워크 보안, 정보보호 컨설팅

김 민 태 (Mintae Kim)

2015년 3월~현재 : 순천향대학교 정보보호학과 학사

<관심분야> 정보보안, 네트워크 보안, 데이터 분석

이 선 영 (Sun-Young Lee)

1993년 2월 : 부경대학교 전자계산학과(이학사)

1995년 2월 : 부경대학교 전자계산학과(이학석사)

2001년 3월 : 일본도쿄대학 전자정보공학(공학박사)

2004년 3월~현재 : 순천향대학교 정보보호학과 교수

<관심분야> 콘텐츠 보안, 암호이론, 정보이론, 정보보안

[ORCID:0000-0002-4686-9436]

임 종 훈 (Jonghoon Lim)

2015년 3월~현재 : 순천향대학교 정보보호학과 학사

<관심분야> 정보보안, 네트워크 보안