논문 18-43-11-24 The Journal of Korean Institute of Communications and Information Sciences '18-11 Vol.43 No.11
https://doi.org/10.7840/kics.2018.43.11.1952

소프트웨어 정의 네트워크를 위한 ARP Poisoning 방어 시스템

김 영 빈◆, 박 민 호°, 주 양 익°°

ARP Poisoning Defense System for Software-Defined Networks

Young-pin Kim◆, Min-ho Park°, Yang-ick Joo°°

요 약

최근 새로운 네트워킹 기술 Software-Defined Networking(SDN)과 Service Function Chaining(SFC)의 빠른 성장 과 더불어 SDN과 SFC에 대한 보안 문제 또한 대두되고 있다. 그러나 아직도 새로운 네트워크 환경에 대한 보안성 및 안정성에 대한 분석 및 연구가 미흡한 상황이므로, 보안 취약성이 지속적으로 드러나고 있다. 본 논문에서는 이러한 문제점들 중에서SFC 취약점을 이용한 ARP Poisoning 공격을 소개하고, 이를 방어할 수 있는 기법을 제안한다. 제안하는 방법은 ARP Poisoning 공격의 특징인 반복적인 ARP reply를 탐지하여 ARP Poisoning 공격을 탐지한다. 제안된 방법은 기존의 탐지 및 방어 방법에서의 문제점인 정당한 유저의 MAC주소 변경을 공격으로 인식하는 것 과 ARP reply의 개수로 공격의 유무를 판단하는 문제점을 해결하고 더 정확하게 탐지한다. 또한, 반복적인 ARP reply전송이 공격탐지에 이용된다는 것을 간파한 공격자가 지능적인 ARP Poisoning 공격 역시 탐지한다.

Key Words : SDN, NFV, SFC, ARP, ARP Poisoning

ABSTRACT

Recently, the novel networking technology Software-Defined Networking(SDN) and Service Function Chaining(SFC) are rapid growing, security issues are also emerging for SDN and SFC. However, the research about security and safety on novel networking environment is still unsatisfactory, the vulnerabilities being reveal continuously. In this paper, among these security issues, we introduce the ARP Poisoning attack to use SFC vulnerability and propose method to be able to defend that attack. The proposed method detects repetitive ARP reply which is feature of ARP Poisoning attack and detects ARP Poisoning attack. The proposed method solves the problem of previous detection method which considering whether legitimate user's MAC address change is as an attack and decide attack as the number of ARP replies. Our proposed method also more accurately detects the presence of an attack. if an attacker know that reptitive ARP reply is used to detect attack, an attacker can intelligent ARP attack. but, our proposed method is able to detect intelligent ARP attack.

※ 이 논문은 2018학년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00254. SDN 보안 기술개발)

◆ First Author : (ORCID:0000-0001-6956-2755)Department of ICMC convergence technology, Soongsil University, ypk@ssu.ac.kr, 학생회원

° Corresponding Author : (ORCID:0000-0003-3033-192X)School of Electronic Engineering, Soongsil University, mhp@ssu.ac.kr, 종신회원

°° Corresponding Author : (ORCID:0000-0003-3125-5316)Division of Electrical and Electronics Engineering, Korea Maritime and Ocean University, yijoo@kmou.ac.kr, 종신회원

논문번호 : 201806-C-186-RE, Received June 8, 2018; Revised July 31, 2018; Accepted August 22, 2018

Ⅰ. 서 론

Control Plane과 Data Plane의 분리로 중앙 집중화 네트워크를 구축하여 적은 비용, 빠른 속도, 프로그래밍이 가능한 네트워킹과 같은 많은 이점을 가지고 있는 Software-Defined Networking(SDN) 은 최근 유망한 차세대 네트워크 기술로 연구 되고 있다. SDN의 중심인 SDN Controller는 SDN Switch를 통해 Flow 기반 Traffic을 제어하고 모니터링 한다. Service Function Chaining(SFC)는 침입탐지시스템이나 방화벽과 같은 다양한 네트워크 서비스 및 기능을 일련의 체인으로 묶어 경로를 설정해서 서비스를 제공받게 하여 높은 성능과 이용률을 제공하는 매우 유용한 기술이다.

그러나 SDN과 SFC의 새로운 네트워크 환경에서는 다양한 공격 취약성이 보고되고 있다.[1,2] 특히 ARP Poisoning 공격은 내부 공격자에 의해 네트워크에 쉽게 큰 피해를 줄 수 있는 공격으로서, 기존 네트워크 뿐 아니라 SDN기반의 SFC 환경에서도 역시 문제가 되고 있다.[3,4]

이러한 SDN기반 네트워크에서의 ARP Poisoning 공격에 대한 취약성을 해결하기 위한 여러 가지 연구들이 제안되었다. [5]에서는 MAC 주소 변경을 감지하여 ARP Poisoning 공격을 탐지 하였고, [6]에서는 MAC 주소와 IP주소 쌍이 ARP Table에 있는 주소 쌍과 하나 이상 다르면 차단하는 방법을 제안했다. [7]에서는 ARP reply의 개수를 세어서 100개 이상의 다량의 ARP reply가 감지되면 공격으로 간주하는 방법을 제안했다.

하지만, 이러한 기존의 ARP Poisoning 공격을 탐지 및 방지하는 방법에는 여러 문제점이 있다. [5]와 [6] 의 경우 정당한 유저의 MAC주소 변경으로 인해 발생한 ARP reply를 공격으로 착각하여 네트워크에 큰 혼란을 줄 수 있고, ARP reply의 개수에 의존하여 공격을 탐지하는 경우에는 최소한의 ARP reply를 사용하여 공격을 한다면 탐지 할 수 없다. [7]의 경우에서는 100개 이상의 ARP reply를 탐지하는데 100개 이하의 ARP reply를 사용하여 공격을 한다면 탐지 할 수 없다.

본 논문에서는 SFC가 가능한 SDN환경에서 ARP Poisoning을 이용한 Man in the Middle Attack을 소개하고, 이러한 공격을 방어하기 위한 ARP 상태 기반 ARP Poisoning 공격 탐지 시스템을 제안한다. 본 논문에서 제안하는 ARP 상태 기반 공격 탐지 시스템은 기존 방법과는 다르게 ARP Poisoning 공격의 특징인 반복적인 ARP reply를 탐지하여 ARP Poisoning 공격을 탐지 및 방지하기 때문에, 정당한 유저의 MAC 주소 변경에 영향을 주지 않고, ARP reply의 개수로 공격의 유무를 판단하지 않기 때문에 기존 방법보다 더 정확하게 탐지 및 방지 할 수 있다. 또한, 일반적으로 ARP Poisoning 공격은 공격 성공률을 높이기 위해 반복적으로 ARP reply를 전송하는 방법을 사용한다. 이러한 반복적 ARP reply 전송이 공격자 측면에서 공격 탐지에 취약하기 때문에 공격자는 한 개의 ARP reply로 ARP Poisoning공격을 시행하는 지능적인 ARP Poisoning공격을 할 수 있다. 하지만, 본 논문에서 제안하는 방법에서는 Host Tracking Service(HTS) 의 기능을 이용하여 지능적인 ARP Poisoning 공격 역시 탐지가 가능하다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 본문의 1절에서는 MAC주소 기반 SFC 시스템이 어떻게 동작하는지에 대해 설명하고, 2절과 3절에서는 본 논문에서 제안하는 시스템에 대한 설명과 동작 과정에 대해 설명하고, 일반적인 ARP Poisoning 공격과 지능적인 ARP Poisoning 공격에 대하여 설명하였다. 4절에서는 본 논문에서 제안한 시스템을 적용한 실험에 대하여 소개한다.

Ⅱ. 본 문

2.1 Layer 2 Address 기반 Service Function Chaining 구현

Service Function Chaining(SFC)는 여러 가지 구현 방법이 있지만, 본 논문에서는 Layer 2 Address 기반 SFC system을 구현하였다. Layer 2 Address 기반 SFC system에서 Layer 2 Address인 MAC Address는 Service instance들을 확인하기 위해 사용되고, Layer 3 Address인 IP Address는 Edge node의 신원을 확인하기 위해 사용된다. 또한, Service Chain을 구성하고 통신할 때, MAC Address가 사용된다.[8]

2.1.1 Service Function Chaining 동작 과정

Fig. 1에서 설명하는 것처럼 Layer 2 기반 SFC는 다음과 같이 동작한다. Fig. 1의 각 Packet A,B,C는 모두 같은 Packet 이지만 출발지 및 목적지 주소만 변경된 Packet이다.

(1) Client가 Server에게 Service instance의 Service가 요구된 Packet을 전송하고 Packet A가 SDN switch에 수신 된다. 이때 Packet A의 Src IP는

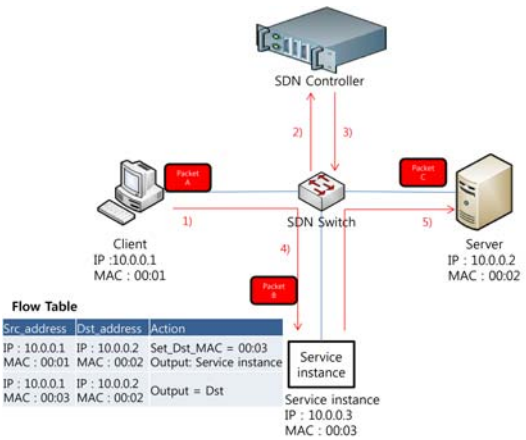

그림 1. Service Function Chaining 동작 과정
Fig. 1. Service Function Chaining Process

10.0.0.1, Src MAC은 00:01, Dst IP는 10.0.0.2, Dst MAC은 00:02이다.

(2) SDN Switch는 Service Function Chaining이 필요한 Packet A의 처리를 위해서 Packet_in Message를 SDN Controller 에게 전송한다.

(3) SDN Controller는 Service instance의 Service가 필요한 Packet의 목적지 MAC Address를 Service instance의 MAC Address로 설정 후 전송하는 Rule을 SDN Switch에게 전송한다.

(4) SDN Switch는 Packet B를 Service instance에게 전송한다. 이때 Packet B 의 Src IP는 10.0.0.1, Src MAC은 00:01, Dst IP는 10.0.0.2, Dst MAC은 Service instance의 MAC Address인 00:03이다.

(5) Packet B를 받은 Service instance는 요구된 Service를 처리한 후 Packet C를 다시 원래 목적지인 Server에게 전송한다. 이때 Packet C의 Src IP 는 10.0.0.1, Src MAC은 Service instance의 MAC Address인 00:03, Dst IP는 10.0.0.2, Dst MAC은 00:02이다. 이때 Src MAC Address가 Client의 MAC Address가 아닌 Service instance의 MAC Address인데, 이는 실제 데이터를 전송한 곳이 Service instance이기 때문이고, IP Address는 Client의 IP인데, 이는 Edge node가 Client이기 때문이다.

본 실험 역시 이와 같은 방법으로 SDN 환경에서 Layer 2 Address를 이용한 Service Function Chaining을 구성 하였다.

2.2 ARP Poisoning 방어 시스템 설계 및 구현

SDN을 위한 ARP Poisoning 방어 시스템을 Flow

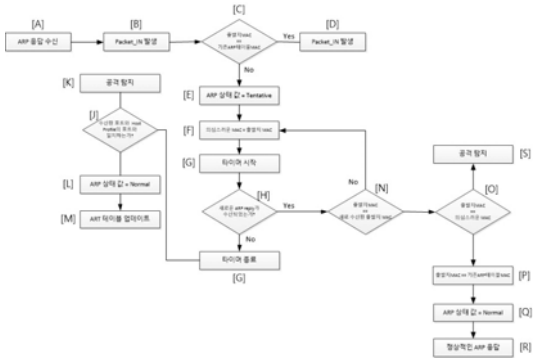

그림 2. ARP Poisoning 방어 시스템 동작 과정
Fig. 2. ARP Poisoning Defense system Process

chart로 나열하여 설명 한 것이다.

Step A): Host가 ARP reply를 전송하고 SDN Switch가 받는다.

Step B): SDN Switch는 해당 Packet의 처리를 위해서 Packet_in Message를 발생시킨 후 SDN Controller에게 전송한다.

Step C): Packet_in Message를 받은 SDN Controller는 ARP reply packet의 출발지 MAC Address와 ARP table의 MAC Address를 비교한다. 만약 같다면 Step D)로 이동하고, 다르다면 Step E)로 이동한다.

Step D): ARP reply의 출발지 MAC주소와 ARP Table의 MAC 주소가 일치함으로 일반적인 ARP reply라고 판단한다.

Step E): ARP reply packet의 출발지 MAC Address와 ARP Table의 MAC Address가 다르다면, ARP Poisoning 공격이거나, 정상적인 MAC주소 변경임으로 ARP_State를 Tentative로 변경한다.

Step F): ARP reply packet의 출발지 MAC Address를 Suspicious_MAC에 임시 정한 한다.

Step G): 반복적인 ARP reply 탐지를 위해서 타이머를 작동시킨다.

Step H): 반복적인 ARP reply를 탐지하기 위해 새로운 ARP reply를 확인 한다. 만약 타이머가 종료되기 전 ARP_State의 값이 Tentative일 때, ARP reply를 다시 수신한다면, Step N)으로 이동하고, 다른 ARP reply를 수신하지 않는다면 Step I)로 이동한다.

Step I): Timer가 종료되었다면, 지능적인 ARP Poisoning 공격임을 확인하기 위해 Host Tracking Service로 Packet_in message를 전송한다.

Step J): HTS가 관리하는 Host Profile에 있는 해당

IP 및 MAC주소의 Switch Port와 ARP reply가 수신된 Switch Port를 비교한다. 만약 다르다면, ARP Poisoning 공격으로 간주하고 Step K)로 이동한다. 만약 두 Switch Port가 같다면 Step L)로 이동한다.

Step K): ARP Poisoning 공격이 탐지 되었으므로 해당 Port를 차단한다.

Step L,M): ARP reply가 수신된 Switch Port와 Host Profile의 Port가 같다면, 정상적인 MAC주소 변경임으로 ARP_state를 Normal로 변경 후 ARP Table을 업데이트 한다.

Step N): ARP reply의 출발지 MAC주소와 새로 수신된 ARP reply의 출발지 MAC주소를 비교한다. 만약 두 주소가 같다면, Step O)로 이동한다. 다르다면 Step F)로 이동한다.

Step O): ARP reply의 출발지 MAC주소가 이전에 임시 저장한 Suspicious_MAC와 같은지 비교한다. 만약 같다면 반복적인 ARP reply임으로 Step S)로 이동한다. 다르다면

Step P,Q,R): ARP reply의 출발지 MAC 주소가 ARP Table의 MAC주소와 같다면 MAC주소 변경이 없는 정상적인 ARP reply임으로 ARP_state를 Normal로 변경 한다.

Step S): 반복적인 ARP reply 전송임으로 ARP Poisoning 공격처리를 한다.

2.3 ARP Poisoning 방어 시스템 동작 과정

공격의 성공률을 높이기 위해 반복적인 ARP reply를 전송하는 일반적인 ARP Poisoning 공격과 ARP Update 타이밍에 맞춰 한 개의 ARP reply로 치명적인 공격을 하는 지능적인 ARP Poisoning 공격 두 가지 공격 시나리오에서 본 논문에서 제안한 시스템이 어떻게 동작하는지에 대해 설명한다.

2.3.1 일반적인 ARP Poisoning 공격

본 논문에서는 일반적인 ARP Spoofing 공격의 특징인 반복적인 ARP reply packet 전송을 이용한 공격을 일반적인 ARP Poisoning 이라고 정의한다. 공격자가 자신의 MAC주소로 ARP Table을 수정하기 위해 악의적인 ARP reply를 전송한다. 이때 공격자는 ARP Poisoning공격 성공률을 높이기 위해 반복적인 ARP reply를 전송한다. SDN Switch는 ARP reply를 받고 해당 Packet 처리를 위해 Packet_in Message를 발생시킨다. Packet_in Message를 받은 SDN Controller는 ARP reply Packet의 출발지 MAC Address와 ARP Table의 MAC Address를 비교한다. 악의적인 ARP reply의 경우 기존 MAC주소와 다르기 때문에 ARP_state값을 Tentative로 변경 후 ARP reply의 출발지 MAC주소를 Suspicious_MAC에 임시 저장하고 반복적인 ARP reply 탐지를 위해 Timer를 작동 시키고 다른 ARP reply가 발생하는지 확인한다. 공격자는 반복적인 ARP reply를 전송하고, Timer 종료 전에 다시 수신된 ARP reply의 출발지 MAC주소가 또 다른 MAC주소인지 확인한다. 만약 이전에 수신된 MAC주소와 다르다면 해당 MAC주소를 Susipicious_MAC에 임시 저장하고 Timer를 재가동 시킨다. 만약 이전에 수신된 MAC주소와 같다면 반복적인 ARP reply임으로 공격을 탐지한다.

2.3.2 지능적인 ARP Poisoning 공격

공격자는 반복적인 ARP reply가 공격탐지에 이용된다는 것을 인지하고 ARP Table Update 시기에 맞춰서 Target SF보다 조금 늦게 ARP reply를 전송하는 ARP Poisoning 공격을 하는 것을 본 논문에서는 지능적인 ARP Poisoning 공격이라고 정의한다. SDN Switch는 ARP reply를 받고 해당 Packet 처리를 위해 Packet_in Message를 발생시킨다. Packet_in Message를 받은 SDN Controller는 ARP reply Packet의 출발지 MAC Address와 ARP Table의 MAC Address를 비교한다. 악의적인 ARP reply의 경우 기존 MAC주소와 다르기 때문에 ARP_state값을 Tentative로 변경 후 ARP reply의 출발지 MAC주소를 Suspicious_MAC에 임시 저장하고 반복적인 ARP reply 탐지를 위해 Timer를 작동 시키고 다른 ARP reply가 발생하는지 확인한다. 지능적인 ARP Poisoning은 타이밍에 맞춰 한 개의 ARP reply만 전송하기 때문에 반복적인 ARP reply를 전송 하지 않으므로 Timer 종료 후 지능적인 ARP Poisoning 공격 탐지를 위하여 Packet_in Message를 HTS에 전송한다. HTS가 관리하는 Host Profile의 해당 IP/MAC이 연결된 Switch Port와 ARP reply가 수신된 Switch Port를 비교한다. 정상적인 MAC주소 변경은 다른 Switch Port에서 발생되지 않지만, 지능적인 ARP Poisoning 공격의 경우 다른 Switch Port에서 발생됨으로 공격을 탐지하게 된다.

2.4 실험 및 결과

SDN 환경에서 SFC를 이용한 ARP Poisoning공격은 성공적이었다. 그 결과, 일반적인 ARP Poisoning 공격 및 지능적인 ARP Poisoning 공격으로 인해 Packet은 공격자에게 전송되어 공격자가 수신 할 수

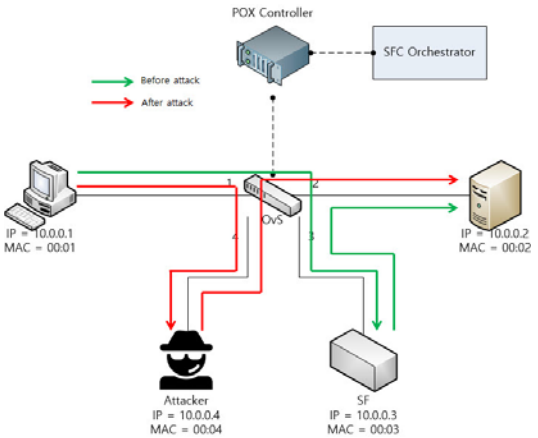

그림 3. ARP Poisoning 공격 실험 환경
Fig. 3. ARP Poisoning attack implement environment

있었고, 본 논문에서 제안한 ARP 상태 기반 ARP Poisoning 탐지 시스템은 위의 공격을 정확하게 탐지하였다. 이번 절에서는 성공적으로 공격이 되었는지, 성공적으로 탐지가 되었는지 확인하기 위해 목적지에 Ping Packet을 보내고, Wireshark[9] Tool을 사용해 Ping Packet을 캡쳐 하였다.

Fig. 3은 ARP Poisoning 공격 및 탐지를 위한 실험 환경이다. 본 논문의 실험에서는, Python[10] 기반의 프로그래밍이 가능한 SDN Controller인 POX Controller를 사용하였다. 또한, 가상 SDN환경을 사용하기 위하여 Mininet[11]을 사용하였다. 그림에서 설명 하는 것처럼, 초록색 화살표의 방향대로 10.0.0.1이 10.0.0.2에게 데이터를 전송 할 때, Service Function인 10.0.0.3을 거쳐 10.0.0.2에게 도착해야 한다. 하지만, ARP Poisoning 공격 이후 10.0.0.1이 10.0.0.2에게 데이터를 전송 할 때, OvS와 SDN Controller는 공격자를 SF로 생각하기 때문에 빨간색 화살표의 방향으로 데이터가 전송된다.

2.4.1 일반적인 ARP Poisoning 공격 및 탐지

출발지 IP 주소 10.0.0.1은 목적지 주소인 10.0.0.2에게 Packet을 보내지만 목적지 MAC 주소는 00:03으로 되어있다. 왜냐하면 모든 Packet은 SF를 거쳐 지나가야 하고 SF는 받은 Packet을 자동으로 목적지 IP에 다시 재전송 한다. 10.0.0.2는 10.0.0.1에게 받은 Packet에 대한 응답 Packet을 전송하고 10.0.0.1은 10.0.0.2에게 Packet을 받는다. 하지만, 본 실험에서, 공격자는 SF의 MAC 주소가 00:03 에서 00:04로 변경을 의미하는 ARP reply packet을 전송하고, SDN Controller는 ARP table을 00:03에서 00:04로 업데이트 한다. 그러므로 모든 Packet은 공격자의 SF를 거쳐가야만 한다. Fig. 4와 Fig. 5는 ARP Poisoning 공격에 의해 MAC 주소 변경을 통한 Packet의 경로 변화를 보여준다. 또한, ARP Poisoning 공격을 탐지하기 위해 본 논문에서 제안된 방법을 해당 실험에 적용하였다. MAC 주소 업데이트 타이머를 1 또는 2초 로 설정했다. 만약 공격자가 ARP Spoofing Tool을 사용하여 반복적인 ARP reply를 발생시키면, 해당 시스템은 ARP Poisoning 공격을 탐지하게 되고, 공격자는 더 이상 SF를 모방할 수 없다. 공격이 완벽하게 탐지되어진 것을 Fig. 6 에서 보여준다.

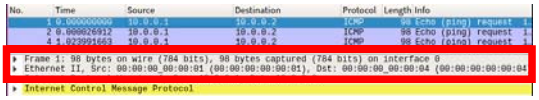

그림 4. 일반적인 ARP Poisoning 공격 실험 결과 1
Fig. 4. Result of Normal ARP Poisoning attack implement 1

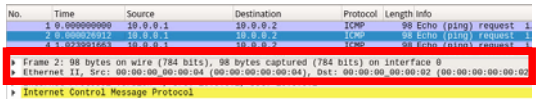

그림 5. 일반적인 ARP Poisoning 공격 실험 결과 2
Fig. 5. Result of Normal ARP Poisoning attack implement 2

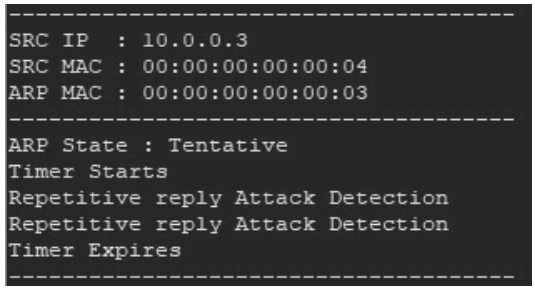

그림 6. 일반적인 ARP Poisoning 공격 탐지 결과
Fig. 6. Detection result of normal ARP Poisoning attack

2.4.2 지능적인 ARP Poisoning 공격 탐지

공격자는 반복적인 ARP reply packet 탐지하는 시스템에 대해 간파하고 있다고 가정한다. 공격자는 가장 최근 ARP reply의 정보를 ARP Table에 업데이트 한다는 점을 악용하여 SF가 ARP 자신의 MAC주소 정보를 포함한 ARP reply packet을 보낸 뒤에 공격자는 공격자의 MAC주소인 00:04가 10.0.0.3이라는 정보를 포함한 ARP reply packet을 전송한다. 하지만, 본 연구에서 제안한 시스템은 먼저 반복적인 ARP

reply packet을 탐지하기 위해 ARP_state를 Normal에서 Tentative로 수정 후 타이머를 시작 시킨다. 반복적인 ARP reply가 없으므로 Switch Port 상태를 확인하기 위해 해당 Packet_in을 HTS로 전송한다. Host Profile의 해당 주소의 Switch Port와 ARP reply가 수신된 Switch Port를 비교한다. 다르기 때문에 해당 ARP reply를 공격으로 간주하고 공격을 탐지한다. Fig. 7은 공격자의 MAC 주소와 ARP table의 MAC 주소와 비교한 뒤 HTS의 Host Profile에 있는 기존 Switch Port의 연결 상태를 확인 한 뒤 공격을 탐지를 보여준다.

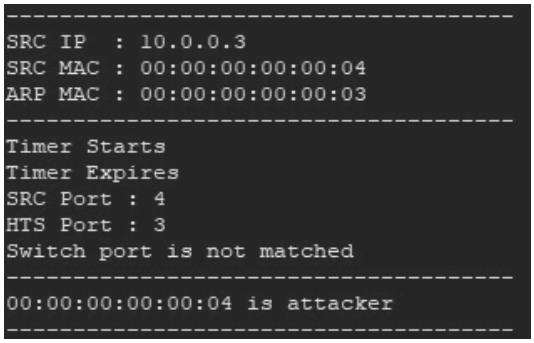

그림 7. 지능적인 ARP Poisoning 공격 탐지 결과
Fig. 7. Detection result of intelligent ARP Poisoning attack

Ⅲ. 결 론

SDN 메커니즘은 계속해서 성장 중 이고, SDN 과 SFC의 결합은 많은 이점을 가지고 있지만, 이 기술들은 많은 문제점과 잠재적인 취약점 또한 가지고 있다. 현재 SDN과 SFC는 보안 문제에 직면했다, 본 논문에서는 SFC가 가능한 SDN 환경에서 SFC의 취약점을 이용한 공격시나리오를 제시했고, 이러한 공격은 SDN 환경에 매우 치명적이기 때문에, ARP Poisoning 공격을 탐지하기 위한 ARP 상태 기반 탐지 시스템을 제안했다. 아직 해결되지 않은 잠재적인 취약점을 해결하기 위해, 네트워크 연구자들은 SDN 보안에 대해 계속해서 관리하고 연구해야 한다.

본 논문에서 제안한 SFC 취약점을 이용한 ARP Poisoning 공격 방법 및 탐지 방법이 SDN을 원하는 기업이나 사용자에게 기여하길 바란다.

References

[1] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. 2013 SDN for Future Netw. and Serv.*, pp. 1-7, 2013.

[2] A. Feghali, R. Kilany, and M. Chamoun, "SDN security problems and solutions analysis," in *Proc. Protocol Eng. and Int. Conf. New Technol. of Distrib. Syst.*, pp. 1-5, 2015.

[3] M. Antikainen, T. Aura, and M. Särelä, "Spook in your network: Attacking an SDN with a compromised OpenFlow switch," in *Nordic Conf. Secure IT Syst.*, pp. 229-244, 2014.

[4] M. Brooks and B. Yang, "A Man-in-the-middle attack against OpenDayLight SDN controller," in *Proc. 4th Annu. ACM Conf. Res. in Inf. Technol.*, pp. 45-49, Chicago, Illinois, USA, 2015.

[5] Z. Sasan and M. Salehi, "SDN-based defending against ARP poisoning attack," *J. Advances in Comput. Res.*, vol. 8, no. 2, pp. 95-102, 2017.

[6] M. Z. Masoud, Y. Jaradat, and I. Jannoud, "On preventing ARP poisoning attack utilizing software defined network (SDN) paradigm," in *Proc. 2015 IEEE Jordan Conf. AEECT*, pp. 1-5, 2015.

[7] A. M. Abdelsalam, A. El-Sisi, and V. Reddy, "Mitigation ARP spoofing attacks in software-defined networks," *ICCTA*, Alexandria, Egypt, 2015.

[8] J. Blendin, J. Rückert, N. Leymann, G. Schyguda, and D. Hausheer "Position paper: Software-defined network service chaining," in *Proc. 2014 Third Eur. Workshop on Software-Defined Networks*, pp. 109-114, 2014.

[9] Wireshark, For the packet capture, Retrieved 2018 [Online]. From https://www.wireshark.org

[10] POX, SDN controller, Retrieved 2018 [Online]. From https://github.com/noxrepo/pox

[11] Mininet, Estanblishing structure, Retrieved 2018 [Online]. From http://www.mininet.org

[12] G. Lee, I. Jang, W. Kim, S. Joo, M. Kim, S. Pack, and C.-H. Kang, "SDN-based middlebox management framework in integrated wired and wireless networks," *J. KICS*, vol. 39, no. 6, pp. 379-386, Jun. 2014.

[13] Y. Kyung, K. Hong, S. Park, and J. Park, "Load distribution method over multiple controllers in SDN," *J. KICS*, vol. 40, no. 6, pp. 1114-1116, Jun. 2015.

[14] D. H. Shin, K. K. An, S. C. Choi, and H.-K. Choi, "Malicious traffic detection using k-means," *J. KICS*, vol. 41, no. 2, pp. 277-284, Feb. 2016.

김 영 빈 (Young-pin Kim)

2016년 8월 : 숭실대학교 컴퓨터공학과 졸업

2016년 9월~현재 : 숭실대학교 정보통신소재융합학과 석사과정

<관심분야> 컴퓨터공학, 통신공학

박 민 호 (Min-ho Park)

2000년 2월 : 고려대학교 전자공학과 학사 졸업

2002년 2월 : 고려대학교 전자공학과 석사 졸업

2010년 2월 : 서울대학교 전기컴퓨터공학과 박사 졸업

2013년 3월~현재 : 숭실대학교 전자정보공학부 교수

<관심분야> 전자공학, 컴퓨터공학, 통신공학

주 양 익 (Yang-ick Joo)

1998년 2월 : 고려대학교 전자공학과 학사 졸업

2000년 8월 : 고려대학교 전자공학과 석사 졸업

2004년 8월 : 고려대학교 전자공학과 박사 졸업

2004년 9월~2012년 2월 : 삼성전자 DMC 연구소 책임연구원

2012년 3월~현재 : 한국해양대학교 전자전기정보공학부 교수

<관심분야> 통신 보안, 무선자원관리