JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 8, pp. 1485-1495, Aug. 2022

Check for updates

ARP 공격 시그니처 정보에 기반한 스푸핑 공격 탐지 및 차단 모델

최 준 호[1] · 이 수 원[2] · 서 영 건[3*]
[1]경상국립대학교 대학원 컴퓨터과학과 석사과정
[2*]경상국립대학교 컴퓨터과학과 교수

Spoofing Attack Detection and Blocking Model Based on ARP Attack Signature Information

Jun-Ho Choi[1] · Suwon Lee[2] · Yeong Geon Seo[3*]

[1]Master's Course, Department of Computer Science, Graduate School, Gyeongsang National University, 501 Jinju-daero, Jinju, Gyeongnam, Korea
[2,3*]Professor, Department of Computer Science, Gyeongsang Nat'l University, 501 Jinju-daero, Jinju, Gyeongnam, Korea

[요 약]

오늘날의 네트워크 환경은 일반 사용자가 필요한 정보에 쉽게 접근하고 서비스를 받을 수 있는 환경으로 빠르게 발전하고 있다. 하지만 이러한 네트워크 의존성은 관련 보안 문제를 발생시킨다. 네트워크 기반 보안 사고에는 다양한 문제점이 존재하며, 그중 ARP는 인증 절차 없이 호스트 간에 MAC 주소를 교환하기 때문에 보안에 매우 취약하다. 이러한 취약점이 발견된 이후 최근까지 피해 사례가 꾸준히 증가하고 있으며, 관련 연구도 활발히 진행되고 있다. 하지만 기존 연구 기법은 자동화 툴을 사용한 단일화 된 공격 기법에만 대응 과정을 보이며, 복합적인 ARP 스푸핑 공격 기법에 취약점을 노출 시킬 수 있다. 본 논문에서는 복합적인 ARP 스푸핑 공격 기법에 대한 공격 과정과 이를 방어할 수 있는 방법을 보인 후 다양한 ARP 스푸핑 공격 유형에 따른 공격 패턴을 분석하여 분석된 시그니처 정보를 기반으로 ARP 스푸핑 공격을 탐지 및 차단하는 모델을 제안한다.

[Abstract]

Today's network environment is rapidly developing into an environment in which general users can easily access necessary information and receive services. However, this network dependency creates related security issues. Various problems exist in network-based security incidents. Among them, ARP is very vulnerable to security because MAC addresses are exchanged between hosts without an authentication procedure. Since these vulnerabilities were discovered, the number of damage cases has been steadily increasing until recently, and related research is being actively conducted. However, existing research techniques only respond to a single attack technique using an automated tool, and can expose vulnerabilities to complex ARP spoofing attack techniques. In this paper, we propose a model to detect and block ARP spoofing attacks based on analyzed signature information by analyzing attack patterns according to various ARP spoofing attack types after showing the attack process for complex ARP spoofing attack techniques and how to defend them.

색인어 : MAC, ARP, ARP 스푸핑, 시그니처, 자동화 툴
Key word : MAC, ARP, ARP Spoofing, Signature, Automation Tool

http://dx.doi.org/10.9728/dcs.2022.23.8.1485

Received 13 July 2022; **Revised** 16 August 2022
Accepted 18 August 2022

***Corresponding Author; Yeong Geon Seo**
Tel: ※ 개인정보 표시제한
E-mail: young@gnu.ac.kr

Ⅰ. 서 론

오늘날 네트워크 환경은 일반 사용자들도 자신이 필요로 하는 정보에 접근한 다음 쉽게 서비스를 받을 수 있는 환경으로 빠르게 발전하고 있다. 그렇지만 네트워크 서비스에 대한 의존도는 관련 보안 문제도 함께 발생시키고 있다.

네트워크 기반 보안 사고에는 다양한 형태가 존재하는데 그 대표적인 공격 기법으로 서비스 거부 공격(DoS), 스니핑(Sniffing), 스푸핑(Spoofing), 포이즈닝(Poisoning), 세션 하이재킹(Session hijacking) 등 수많은 공격 기법들이 있으며, 이러한 공격 기법들은 조직 및 개인에게 치명적인 피해를 발생시킨다. 그중 ARP(Address Resolution Protocol) 스푸핑 공격 기법은 더미 허브 환경뿐만 아니라 스위치 환경에서도 스니핑 공격을 가능하게 한다[1].

더미 허브 환경은 스위치 환경과 다르게 장비 내부에 MAC 주소를 기록하는 메모리가 존재하지 않기 때문에 특정 목적지로 데이터 전송을 할 수 있는 기능이 없다. 그렇기 때문에 더미 허브 환경에서는 특정 노드에서 데이터 전송이 발생할 경우 허브에 연결된 모든 포트로 브로드캐스트 기반의 데이터 전송을 한다. 하지만 이러한 브로드캐스트 기반의 전송 기법은 모든 포트에 연결된 시스템으로 패킷 전송이 이루어지기 때문에 스니핑 공격에 대한 취약점을 가지고 있다. 반면에 스위치 환경에서는 MAC 주소를 기록하는 메모리가 존재한다. 그러므로 스위치의 메모리에 존재하는 포트들의 MAC 정보를 기반으로 특정 포트의 시스템으로 패킷을 포워딩 기반으로 전달할 수 있다. 이러한 이유로 스니핑 공격은 상대적으로 더미 허브 환경에서보다 스위치 환경이 더 어려울 수 있다. 즉, 더미 허브 환경에서는 브로드캐스트 전송 기법을 사용하기 때문에 공격자가 자신의 시스템에 있는 네트워크 카드를 프로미스큐어스 모드(Promiscuous mode)로 전환할 경우 연결된 모든 시스템의 패킷 열람이 가능하기 때문이다.

스위치 환경에서는 스위치의 메모리 정보를 기반으로 포워딩 전송을 하기 때문에 공격자 시스템의 네트워크 카드를 프로미스큐어스 모드로 전환하더라도 전반적인 패킷들을 열람할 수 없다. 그러므로 스위치 환경에서 공격자는 패킷에 대해 포워딩을 할 수 없도록 먼저 스위치의 메모리를 오버플로우 시키는데 이를 MAC 오버플로우 공격이라 한다. 이렇게 스위치에 대한 오버플로우 공격이 성공하면 공격자는 자신의 시스템 네트워크 카드를 프로미스큐어스 모드로 전환한 다음 패킷들을 열람하는 것이다. 아울러 스위치 환경에서 또 다른 스니핑 기법으로 ARP 스푸핑이 있다. 이는 특정 시스템에 대한 스니핑을 하기 위해 공격자의 MAC 주소를 스니핑을 시도하는 시스템으로 전달한 다음 중간에서 열람하는 기법이라 할 수 있다. 그러므로 이러한 공격 기법들은 해당 시스템에서 인지할 수 없는 경우가 일반적이기 때문에 큰 피해를 가져올 수 있다[2-5].

스위치 환경에서 스니핑 공격에 대한 국내 사례는 현재 발생 빈도가 미미하지만 해외 사례를 분석해 보면 중국의 경우 공공시설에서 발생하는 공격 기법 중 대부분이 ARP 기반의 공격으로 보고되고 있다. 아울러 이러한 공격 사례는 자동화와 고도화된 기법으로 제작되어 무작위로 배포되고 있다. 그렇지만 현재 우리나라의 경우 ARP 기반의 공격에 대해 경각심이 적기 때문에, 향후 이러한 ARP 공격은 국내 보안 분야에 공격 빈도를 증가시킬 수 있고 큰 피해로 나타날 수 있다[6].

ARP 기반의 보안 위협에 대해 많은 연구가 진행되고 있지만, 고가의 보안 장비를 요구하기 때문에 특정 기관에 한정되어 설치 운영되는 상황이다. 아울러 기존 연구 기법에는 새로운 프로토콜의 제안, Client-Agent와 MAC-Agent, 정적 테이블의 생성과 관리 등이 있다. 그렇지만 이러한 기법들은 현 네트워크 체계 및 보안 정책에 적용하는데 실현 가능성이 작거나 한계점을 가지고 있다[7-10]. 또한 기존 연구 기법은 ARP 스푸핑 공격을 위해 일반적으로 사용하는 “Arpspoof”와 “Ethercap”에 대한 ARP 캐시 테이블 분석과 그 대응 과정에 집중하고 있다. 하지만 이러한 분석 및 대응 과정은 이들 기법과 상이한 패턴을 보이는 ARP 스푸핑 공격 및 복합적인 ARP 스푸핑 공격에 그 취약점을 노출 시킬 수 있다. 본 논문에서는 기존 대응 기법의 문제점, ARP 스푸핑 공격의 다양성에 대응하기 위해 일반적인 ARP 스푸핑 공격 과정의 예를 살펴본 다음 공격 과정에서 발생하는 시그니처 정보를 기반으로 탐지 및 차단 모델을 제안한다.

Ⅱ. 관련연구

2-1 ARP의 기능 및 ARP 스푸핑

ARP는 RFC 826[11]에서 정의한 바와 같이 네트워크 계층 주소(IP 주소)를 데이터 링크 계층 주소(MAC 주소)로 대응시키기 위해 사용되는 프로토콜이다. ARP 스푸핑은 ARP 기반의 메시지 송수신 과정에 대한 무결성 검증이 보증되지 않은 점을 이용하여 조작된 ARP 응답 패킷을 타깃 시스템으로 전송한 다음 MAC 주소를 속여 정상적인 서비스를 방해하는 공격방식이다. 그림 1은 호스트 A와 호스트 B가 LAN 환경에서 정상적인 통신을 하는 모습을 나타낸 그림이다.

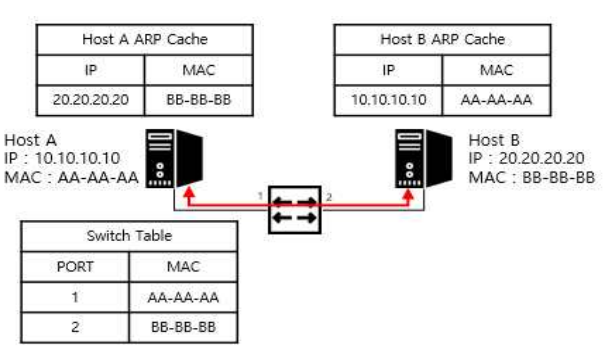

그림 1. 정상적인 통신 과정
Fig. 1. Normal communication process

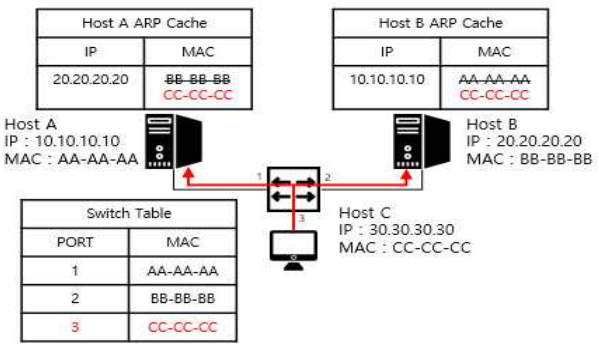

그림 2. ARP 스푸핑 후 통신 과정
Fig. 2. Communication process after ARP spoofing

```
220 (vsFTPd 3.0.2)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER junho
331 Please specify the password.
PASS jun123
230 Login successful.
```

그림 3. ARP 스푸핑 후 패킷 스니핑
Fig. 3. Packet sniffing after ARP spoofing attack

각 호스트의 ARP 캐시 테이블에는 통신하는 상대방 호스트의 IP 주소와 MAC 주소가 저장되어 있다. 그림 2는 공격자가 ARP 스푸핑 공격 후 통신 과정을 나타내는 그림이다. 공격자의 ARP 스푸핑 공격으로 인해 호스트 A와 호스트 B가 서로의 MAC 주소를 "CC-CC-CC"로 오인하고 있으며, 통신하는 모든 트래픽을 공격자에게 전달된다. 공격자는 호스트 A와 호스트 B에 릴레이(Relay) 기능을 사용하여 정상적인 통신을 하는 것처럼 속이고 스니핑을 할 수 있게 된다.

2-2 스니핑

스니핑은 스니퍼(Sniffer)를 이용하여 패킷들을 수집하고 순서대로 재조합 과정을 진행한다. 스니핑은 이러한 스니퍼를 사용하여 네트워크상에서 송신자와 수신자가 주고받는 중간에서 패킷을 도청하는 것을 의미한다.

첫째, 스위치 재밍 공격 기법이다. 스위치 재밍 공격은 스위치의 주소 테이블이 가득 차게 되면 더미 허브처럼 모든 네트워크의 세그먼트로 트래픽을 브로드캐스트하는 특징을 악용한 공격 기법이다. 공격자는 고의로 변조한 맥 정보를 가지고 있는 ARP Reply 패킷을 반복적으로 전송하여 스위치 허브의 주소 테이블을 오버플로우 시켜 더미 허브 환경처럼 만든다. 그 후, 네트워크 카드를 프로미스큐어스 모드로 설정하면 네트워크상에서 패킷을 스니핑할 수 있게 된다.

둘째, ARP Redirect 공격 기법이다. ARP Redirect 공격은 위조된 ARP Reply 패킷을 네트워크에 지속해서 브로드캐스트하여, 네트워크에 다른 호스트들이 공격자를 라우터로 인지하게 만든다. 이렇게 다른 호스트들의 ARP 캐시 테이블을 오염시키게 되면 외부 네트워크와 통신하는 과정에서 발생하는 모든 트래픽이 공격자를 거치게 된다.

스위치 재밍, ARP Redirect 공격기법 외에도 다양한 공격기법들을 통해 스니핑 공격을 성공하게 되면 그림 3과 같이 타깃의개인 정보가 공격자에게 노출되는 문제가 발생한다.

2-3 ARP 스푸핑 공격 패턴

스니핑 공격을 하기 위한 이전 단계의 공격으로 사용되는 대표적인 스푸핑 공격 기법들은 IP의 신뢰 관계를 악용하는 IP 스푸핑, DNS 프로토콜을 악용하여 잘못된 사이트로 이동되게 만드는 DNS 스푸핑, MAC 주소를 속여 랜에서의 통신 흐름을 왜곡시키는 ARP 스푸핑 등이 있다. 본 연구에서는 ARP 스푸핑 공격을 위해 사용되는 공격 방법 중 ARP 포이즈닝 기반 공격 패턴, ARP 포이즈닝 탐지 시스템 우회 공격 패턴, ARP 캐시 테이블에 대한 제로데이 공격 패턴에 대해 분석을 진행하였다.

ARP 스푸핑 공격을 위한 자동화 툴은 해킹 툴로써 많이 사용되고 있는 "Arpspoof"와 "Ethercap"을 사용하여 ARP 스푸핑 공격을 진행하였고, 와이어샤크를 통해 "Arpspoof"와 "Ethercap"에서 발생시키는 ARP 응답 패킷을 분석하였다. 와이어샤크를 통해 "Arpspoof"를 분석한 자료는 그림 4이며, "Ethercap"을 분석한 자료는 그림 5이다. 자동화된 ARP 스푸핑 공격 툴은 각각의 규칙적인 시간 주기를 가지고 ARP 포이즈닝 공격하는 패턴으로 인식할 수 있다.

자동화 툴 기반의 규칙적인 공격 패턴은 일정한 시간 주기를 가지고 반복적으로 위조된 ARP 응답 패킷을 전송하는 패턴을 띄고 있다. 하지만 일정한 시간 주기로 반복적으로 전송되는 ARP 응답 패킷을 분석하고 탐지하게 되면 ARP 스푸핑 공격을 방어할 수 있게 된다. 그러므로 규칙적인 시간 주기를 가지는 공격을 우회하여 위조된 ARP 응답 패킷 발생 시간 주기에 난수를 사용하여 랜덤한 시간으로 불규칙한 ARP 응답 패킷을 전송하게 되면 기존의 탐지 시스템을 우회하는 공격 패턴이 된다. 그림 6은 와이어샤크를 사용하여 랜덤한 시간 간격으로 위조된 ARP 응답 패킷이 전송되는 과정을 분석한 그림이며, 발생 시간 주기가 불규칙한 모습을 확인할 수 있다.

ARP 캐시 테이블에는 ARPCacheLife와 ARPCacheMinReferencedLife 기능이 존재하며, MAC 주소 테이블의 Aging 기능과 비슷한 역할을 한다. ARPCacheLife는 참조되지 않는 항목이 ARP 캐시 테이블에 남아 있을 수 있는 시간을 결정하며, 시간이 지나면 ARP 캐시 테이블에서 항목을 삭제한다. 그림 7은 와이어샤크를 사용하여 제로 데이 공격 패턴의 위조된 ARP 응답 패킷이 전송되는 과정을 분석한 그림이며, 발생 시간 주기가 항목 지속 시간에 맞춰 발생하는 것을 확인할 수 있다.

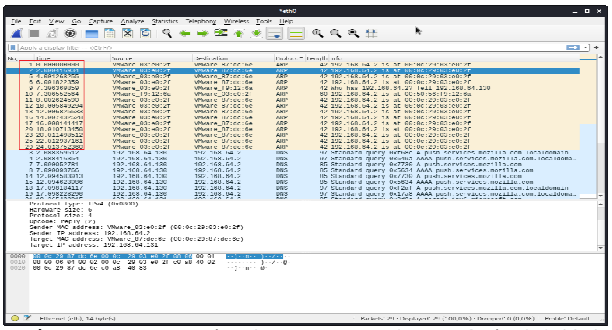

그림 4. Wireshark를 이용한 Arpspoof 툴의 ARP 응답 패킷 분석
Fig. 4. ARP response packet analysis of Arpspoof tool

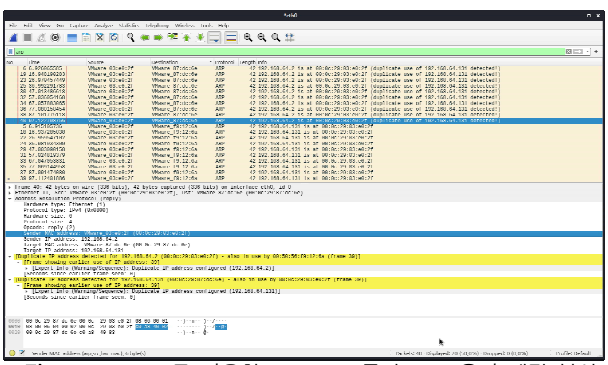

그림 5. Wireshark를 이용한 Ethercap 툴의 ARP 응답 패킷 분석
Fig. 5. ARP response packet analysis of Ethercap tool

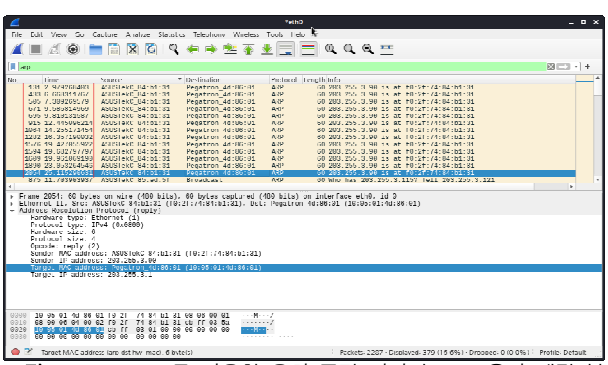

그림 6. Wireshark를 이용한 우회 공격 기법의 ARP 응답 패킷 분
Fig. 6. ARP response packet of bypass attack technique

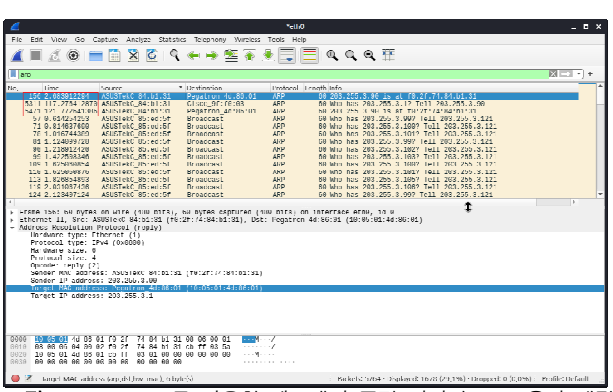

그림 7. Wireshark를 이용한 제로데이 공격 기법의 ARP 응답 패킷
Fig. 7. ARP response packet of zero-day attack technique

2-4 기존 기법의 문제점 및 개선 방안

ARP 응답에 대해 아무런 인증 없이 ARP 테이블을 갱신하는 취약점을 해결하기 위해 제안된 프로토콜 [7,8,12] 기법은 현 네트워크 체계를 변경하는 방법으로 근본적인 문제를 해결할 수는 있다. 프로토콜 기법의 제안은 인증 과정을 추가하여 ARP의 근본적인 취약점인 ARP 과정에서 아무런 인증 과정이 없는 취약점을 개선하여 문제를 해결하였지만 현 프로토콜 체계에 대한 전면적인 변경이 필요하다.

MAC 주소 정보를 관리하는 MAC-Agent와 ARP 테이블의 변조를 막는 클라이언트 에이전트를 설치하여 신뢰할 수 있는 MAC 주소 정보를 ARP 테이블에 갱신하는 방법[9]이며, 정적 테이블[10, 13]은 신뢰할 수 있는 ARP 테이블을 유지하기 위해 MAC 관리 서버를 두고, ARP 스푸핑 공격을 방어하기 위해 클라이언트에서 정적으로 ARP 테이블을 관리한다. 위의 에이전트를 사용하는 기법과 정적 테이블을 관리하는 부분에서는 동일하지만 에이전트 기법은 데이터 전송 방법에서 MAC 주소와 IP 주소를 암호화하는데 차이점이 존재한다. 기존의 제안 기법들은 ARP 캐시 테이블의 변조를 방지하기 위해 자동화 툴에서 발생하는 일정한 시간 간격을 가지고 반복 수신되는 ARP 응답 패킷에 대해서는 취약하지 않지만, 앞에서 언급한 다양한 ARP 공격기법에서 발생하는 비정상적인 ARP 패킷에는 취약한 부분들이 존재한다.

ARP의 구조는 이더넷 프레임 헤더와 ARP 헤더가 합쳐진 형태로 네트워크에 전송된다. 이러한 ARP 패킷을 공격자가 ARP 공격을 위해 정상적인 ARP의 정보를 악의적으로 위조하여 타깃 호스트에게 위조된 ARP 패킷을 전송시켜 타깃 호스트의 ARP 캐시 테이블 내용을 변조시킨다. 이때, 공격자가 정상적인 ARP 패킷의 정보를 위조하게 되면 정상적인 ARP 과정에서는 볼 수 없는 비정상적인 ARP 과정을 수행하는 패킷을 확인할 수 있다. 이러한 비정상적인 ARP 과정을 수행하는 패킷은 ARP 공격으로 판단할 수 있는 고유의 시그니처 정보를 가지고 있다. 본 연구에서는 다양한 ARP 공격 기법에서 발생하는 비정상적인 ARP 패킷에 대해 분석하며, 이러한 비정상적인 ARP 패킷에서 나타나는 시그니처 정보 기반으로 ARP 공격을 탐지 및 차단할 수 있는 모델을 제안한다.

Ⅲ. 시그니처 기반 탐지 모델

3-1 시그니처 정보

네트워크에서 발생하는 ARP 패킷의 구조는 이더넷 프레임 헤더와 ARP 헤더가 합쳐진 구조로 전송되며, 공격자는 ARP 패킷의 정보를 의도적으로 위조하여 위조된 ARP 패킷을 타깃 PC에 전송한다. 위조된 ARP 패킷을 수신한 타깃 PC의 ARP 캐시 테이블 정보는 위조된 ARP 패킷의 내용처럼 변

경된다. 타깃 PC의 ARP 캐시 테이블의 변조가 발생하면 스니핑 공격을 허용하게 되고 이러한 스니핑 공격은 개인정보 유출과 2차, 3차 그 이상의 더 큰 피해를 발생시킨다. 이 장에서는 ARP 공격을 탐지하기 위해 ARP 포이즈닝 기반의 공격 패턴, ARP 포이즈닝 탐지 시스템 우회 공격 패턴, 제로 데이 공격 패턴과 같은 ARP 스푸핑 공격이 발생할 때 ARP 패킷이 가지는 구조와 ARP 공격 패킷으로 판단할 수 있는 시그니처 정보를 다루었다.

1) 유니캐스트 시그니처 정보

정상적인 ARP 과정은 호스트 A가 호스트 B에 패킷을 전송하려고 할 때, 호스트 B의 MAC 주소 정보를 가지고 있지 않으면 ARP를 사용하게 된다. ARP는 호스트 B의 IP 주소와 FF-FF-FF-FF-FF-FF의 브로드캐스트 MAC 주소를 가지는 ARP 패킷을 네트워크상에 전송하게 되며, ARP 패킷을 수신한 호스트 B는 자신의 MAC 주소를 호스트 A에 유니캐스트 방식으로 전송하게 된다. ARP 요청 과정에서 발생하는 ARP 패킷 정보는 표 1과 같은 ARP 요청 패킷을 브로드캐스트 방식으로 전송하게 된다. 해당 패킷의 목적지 주소를 보게 되면 FF-FF-FF-FF-FF-FF로 브로드캐스트 방식인 것을 확인할 수 있다. 하지만 공격자가 ARP 공격을 시도하는 과정 중 나타나는 시그니처 정보는 ARP 요청 패킷의 전송 방식이 브로드캐스트 방식이 아닌 유니캐스트 방식으로 전송되는 경우이다. 공격자가 ARP 요청 패킷의 전송 방식을 유니캐스트 방식으로 보내게 되면 표 2의 목적지 주소가 FF-FF-FF-FF-FF-FF가 아닌 00-0C-29-41-FD-BA와 같은 특정 호스트의 MAC 주소가 입력되어 유니캐스트 방식으로 ARP 공격을 할 수 있다. 정상적인 ARP 요청은 브로드캐스트 방식으로 전송되지만 유니캐스트 방식으로 ARP 요청 패킷이 전송되면 비정상적인 ARP 패킷으로 판별할 수 있다.

2) 브로드캐스트 시그니처 정보

ARP 과정 중 호스트 A가 보낸 ARP 요청 패킷을 받은 호스트 B는 호스트 A에 ARP 응답 패킷을 전송하게 된다. 해당 과정에서 호스트 B가 보낸 ARP 응답 패킷은 호스트 A에 자신의 MAC 주소 정보가 담긴 ARP 패킷을 유니캐스트 방식으로 전송되며, 패킷의 정보는 표 3과 같다. ARP 응답 패킷의 정보를 확인하게 되면 목적지 주솟값이 호스트 A의 MAC 주소 F0-2F-74-84-B1-31을 확인할 수 있다. 공격자는 정상적인 ARP 응답 패킷의 목적지 주솟값을 F0-2F-74-84-B1-31이 아닌 FF-FF-FF-FF-FF-FF로 위조하여 브로드캐스트 방식으로 ARP 응답 패킷을 네트워크상에 전송해 ARP 스푸핑 공격을 가능하게 한다. 표 4는 위조된 ARP 응답 패킷의 정보이며, 정상적인 응답은 유니캐스트로 전송되지만 브로드캐스트 방식으로 응답 패킷이 전송되면 비정상적인 ARP 패킷으로 판별할 수 있으며, ARP 공격 시그니처 정보가 된다.

표 1. 브로드캐스트 ARP 요청 패킷 정보
Table 1. Broadcast ARP request packet information

Category	Value
Destination Address	FF-FF-FF-FF-FF-FF
Source Address	F0-2F-74-84-B1-31
Type	08 06 (ARP)
Hardware Type	00 01 (Ethernet)
Protocol Type	08 00(IP)
OP	00 01 (Request)
Source MAC Address	F0-2F-74-84-B1-31
Sender IP	203.255.3.90
Destination MAC Address	00 00 00 00 00 00
Destination IP	203.255.3.24

표 2. 유니캐스트 ARP 요청 패킷 정보
Table 2. Unicast ARP request packet information

Category	Value
Destination Address	00-0C-29-41-FD-BA
Source Address	F0-2F-74-84-B1-31
Type	08 06 (ARP)
Hardware Type	00 01 (Ethernet)
Protocol Type	08 00(IP)
OP	00 01 (Request)
Source MAC Address	F0-2F-74-84-B1-31
Sender IP	203.255.3.90
Destination MAC Address	00 00 00 00 00 00
Destination IP	203.255.3.24

표 3. 유니캐스트 ARP 응답 패킷 정보
Table 3. Unicast ARP reply packet information

Category	Value
Destination Address	F0-2F-74-84-B1-31
Source Address	00-0C-29-41-FD-BA
Type	08 06 (ARP)
Hardware Type	00 01 (Ethernet)
Protocol Type	08 00(IP)
OP	00 02(Reply)
Source MAC Address	00-0C-29-41-FD-BA
Sender IP	203.255.3.24
Destination MAC Address	F0-2F-74-84-B1-31
Destination IP	203.255.3.90

표 4. 브로드캐스트 ARP 응답 패킷 정보
Table 4. Broadcast ARP reply packet information

Category	Value
Destination Address	FF-FF-FF-FF-FF-FF
Source Address	00-0C-29-41-FD-BA
Type	08 06 (ARP)
Hardware Type	00 01 (Ethernet)
Protocol Type	08 00(IP)
OP	00 02 (Reply)
Source MAC Address	00-0C-29-41-FD-BA
Sender IP	203.255.3.24
Destination MAC Address	F0-2F-74-84-B1-31
Destination IP	203.255.3.90

3) 상이한 시그니처 정보

호스트 A가 호스트 B와 통신을 하기 위해 ARP 요청 패킷을 전송한다. 해당 패킷이 정상적인 패킷이면 표 1과 같은 정보를 가진다. 하지만 A와 B의 통신 과정에서 공격자의 악의적인 의도로 ARP 요청 패킷을 탈취한 후 패킷의 정보를 위조해 호스트 B에 재전송하여 ARP 공격을 시도할 수 있다. 이때, 발생할 수 있는 시그니처 정보는 이더넷 헤더의 출발지 주소와 ARP 헤더의 출발지 주솟값이 일치하지 않는 경우이다. 표 5는 공격자에 의해 위조된 ARP 패킷 정보이며, 이더넷 헤더의 출발지 주소와 ARP 헤더의 출발지 주솟값이 상이한 것을 확인할 수 있다.

4) 일정 시간 동안 반복 수신되는 시그니처 정보

자동화된 공격 툴은 일정한 시간 간격을 두고 ARP 응답 패킷을 타깃 PC에 재전송하는 시그니처 정보를 가지고 있으며,그림 5는 “Ethercap” ARP 스푸핑 공격 툴을, 그림 4는 “Arpspoof” ARP 스푸핑 공격 툴을 보이고 있다. 이를 통해 확인할 수 있는 시그니처 정보는 “Ethercap”은 약 10초, “Arpspoof”는 약 2초의 시간 간격을 가지고 ARP 응답 패킷을 재전송한다. 또한 “Ethercap”과 “Arpspoof”와 같이 일정한 시간 간격이 아닌 불규칙한 시간 간격으로 전송하는 ARP 공격 방법도 존재한다.

그림 6은 불규칙적 시간 간격을 가지고 ARP 응답 패킷을 재전송하는 것을 볼 수 있다. ARP 응답 패킷만 반복적으로 발생하게 되면 비정상 ARP 응답 패킷으로 판별할 수 있게 되며, ARP 공격 시그니처 정보가 된다. 하지만 공격자가 위조된 ARP 응답 패킷이 아닌 ARP 요청 패킷을 반복적으로 발생시키게 되면 독립적으로 발생한 ARP 응답 패킷과 다르게 ARP 요청에 맞는 ARP 응답 패킷이 발생하고, 독립적으로 발생하는 패킷을 탐지하는 시그니처 정보를 우회할 수 있게 된다.

공격자는 원활한 스니핑 공격을 실행하는 특정 시간 동안 타깃 PC에 반복적으로 ARP 패킷을 전송한다. 만약 반복적으로 ARP 패킷을 전송하지 않게 되면 정상적인 ARP 패킷으로 인해 원활한 스니핑 공격이 이루어지지 않는다.

표 5. 이더넷 헤더와 ARP 헤더의 주소 값이 다른 ARP 패킷
Table 5. ARP packet with different address values of Ethernet header and ARP header

Category	Value
Destination Address	FF-FF-FF-FF-FF-FF
Source Address	F0-2F-74-84-B1-31
Type	08 06 (ARP)
Hardware Type	00 01 (Ethernet)
Protocol Type	08 00(IP)
OP	00 01 (Request)
Source MAC Address	10-05-01-4D-86-01
Sender IP	203.255.3.90
Destination MAC Address	00 00 00 00 00 00
Destination IP	203.255.3.24

이러한 공격 특성을 활용하여 일정 시간 안에 반복 수신되는 ARP 패킷은 비정상 패킷으로 판단할 수 있는 시그니처 정보가 된다.

3-2 시그니처 기반 탐지 알고리즘

다음은 ARP 공격을 탐지하기 위해 제안한 알고리즘이며, ARP 공격에서 발생하는 시그니처 정보를 기반으로 ARP 공격을 탐지한다. 본 연구에서 제안하는 모델의 동작 과정을 그림 8에 도식화하였으며, ARP 요청 패킷이 발생하면 다음과 같은 과정을 수행한다.

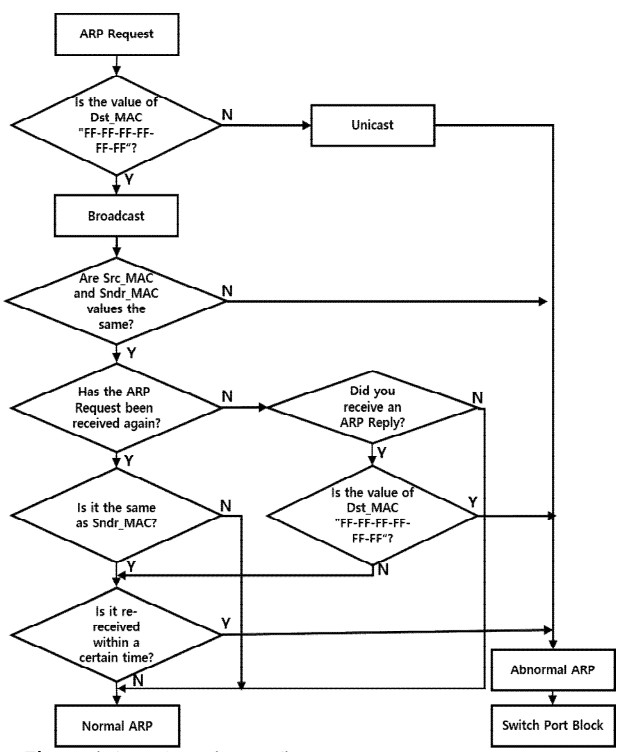

그림 8. 제안 모델 운영 프로세스
Fig. 8. Proposal model operation process

1. ARP 요청 패킷이 발생한다.
2. Dst_MAC의 값이 FF-FF-FF-FF-FF-FF와 일치하면, 3 과정을 수행하며, 불일치하면 10 과정을 수행한다.
3. Src_MAC 과 Sndr_MAC의 값이 일치한다면 4 과정을 수행하고, 불일치하면 10 과정을 수행한다.
4. ARP 요청 패킷이 재수신 되었다면 5 과정을 수행하고, 재수신 되지 않았다면 6 과정을 수행한다.
5. 재수신된 패킷의 Sndr_MAC이 전에 수신된 패킷의 Sndr_MAC과 일치하면 8, 일치안하면 9 과정을 수행한다.
6. ARP 응답 패킷을 수신했다면 7 과정을 수행하고, 수신하지 않았다면 9 과정을 수행한다.
7. Dst_MAC의 값이 FF-FF-FF-FF-FF-FF와 일치하면 10 과정을 수행하고, 일치하지 않다면 8 과정을 수행한다.

8. 일정 시간 안에 ARP 패킷이 반복 수신되지 않는다면 9 과정을 수행하고, 반복 수신된다면 10 과정을 수행한다.
9. 정상적인 ARP 패킷으로 간주한다.
10. 비정상인 ARP 패킷으로 간주한다.
11. 비정상인 패킷을 송신한 MAC 주소의 포트를 차단한다.

Ⅳ. 실험 및 평가

공격자 시스템은 리눅스 운영체제를 사용하였으며, 타깃 시스템은 윈도우, 서버의 운영체제는 센트 7을 사용하였다. 일반적인 네트워크 환경에서 시뮬레이션을 위해 이용된 시스템 구성도는 그림 9와 같다. 2.3장에서 언급한 ARP 포이즈닝 기반의 공격 패턴, ARP 포이즈닝 탐지 시스템 우회 공격 패턴, ARP 캐시 테이블에 대한 제로 데이 공격 패턴을 이용하여 ARP 스푸핑 공격을 진행하였다. 그림 10은 ARP 스푸핑 공격 전의 타깃 PC의 ARP 캐시 테이블을 보인다. 여기서, IP 주소 : 203.255.3.1는 게이트웨이, IP주소 : 203.255.3.24는 서버, IP주소 : 203.255.3.91는 공격자이다.

4-1 ARP 스푸핑 공격

일반적인 네트워크 환경에서 ARP 스푸핑 공격을 타깃 PC를 대상으로 실험을 진행하였다. 타깃 PC의 ARP 캐시 테이블 변조의 대상은 게이트웨이와 서버를 대상으로 진행하였으며, 게이트웨이를 대상으로 한 ARP 스푸핑 공격의 결과는 그림 11과 같고 서버를 대상으로 ARP 스푸핑 공격을 진행한 결과는 그림 12와 같다. 그림 11은 게이트웨이의 MAC 주소 00-00-0C-9F-F0-03이 공격자 PC의 MAC 주소 10-05-01-4D-86-01로 변경된 타깃 PC의 ARP 캐시 테이블 정보를 볼 수 있다. 그림 12는 공격 대상이 게이트웨이가 아닌 서버를 대상으로 공격을 진행한 결과이며, 서버의 MAC 주소 00-0C-29-41-FD-BA가 공격자 PC의 MAC 주소 10-05-01-4D-86-01로 변경된 ARP 테이블을 확인할 수 있다.

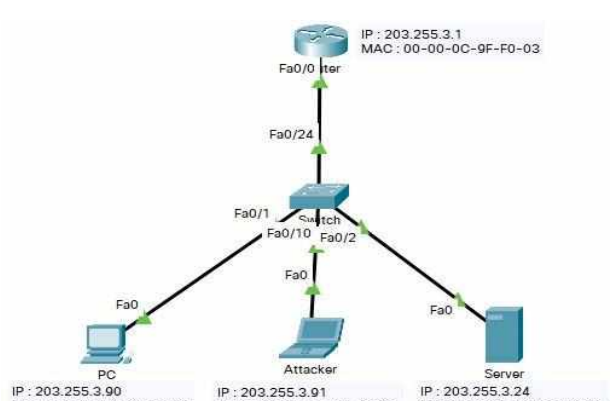

그림 9. 시뮬레이션 네트워크 구성도
Fig. 9. Simulation network diagram

```
Interface: 203.255.3.90  --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           00-00-0c-9f-f0-03     dynamic
  203.255.3.2           00-03-2e-24-06-c0     dynamic
  203.255.3.3           00-de-fb-84-d4-43     dynamic
  203.255.3.12          1c-69-7a-73-e6-cd     dynamic
  203.255.3.16          94-c6-91-3d-db-b7     dynamic
  203.255.3.22          50-b7-c3-ab-57-fa     dynamic
  203.255.3.24          00-0c-29-41-fd-ba     dynamic
  203.255.3.27          00-d8-61-8a-67-35     dynamic
  203.255.3.41          00-03-2e-24-06-c0     dynamic
  203.255.3.58          1c-69-7a-97-49-6e     dynamic
  203.255.3.72          64-e5-99-16-5f-21     dynamic
  203.255.3.91          10-05-01-4d-86-01     dynamic
  203.255.3.92          64-e5-99-16-5f-21     dynamic
```

그림 10. ARP 스푸핑 공격 전 대상 PC의 ARP 캐시 테이블
Fig. 10. ARP cache table of target PC before ARP spoofing attack

```
Interface: 203.255.3.90  --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           10-05-01-4d-86-01     dynamic
  203.255.3.2           00-03-2e-24-06-c0     dynamic
  203.255.3.58          1c-69-7a-97-49-6e     dynamic
  203.255.3.72          64-e5-99-16-5f-21     dynamic
  203.255.3.91          10-05-01-4d-86-01     dynamic
  203.255.3.92          64-e5-99-16-5f-21     dynamic
```

그림 11. 게이트웨이를 대상으로 ARP 스푸핑 공격 후 타깃 PC의 ARP 캐시 테이블
Fig. 11. ARP cache table of target PC after ARP spoofing attack on gateway

```
Interface: 203.255.3.90  --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           00-00-0c-9f-f0-03     dynamic
  203.255.3.16          94-c6-91-3d-db-b7     dynamic
  203.255.3.22          50-b7-c3-ab-57-fa     dynamic
  203.255.3.24          10-05-01-4d-86-01     dynamic
  203.255.3.27          00-d8-61-8a-67-35     dynamic
  203.255.3.41          00-03-2e-24-06-c0     dynamic
  203.255.3.58          1c-69-7a-97-49-6e     dynamic
  203.255.3.72          64-e5-99-16-5f-21     dynamic
  203.255.3.91          10-05-01-4d-86-01     dynamic
  203.255.3.92          64-e5-99-16-5f-21     dynamic
```

그림 12. 서버를 대상으로 ARP 스푸핑 공격 후 타깃 PC의 ARP 캐시 테이블
Fig. 12. ARP cache table of target PC after ARP spoofing attack on server

```
Interface: 203.255.3.90  --- 0xa
  Internet Address      Physical Address      Type
  203.255.3.1           00-00-0c-9f-f0-03     dynamic
  203.255.3.2           00-03-2e-24-06-c0     dynamic
  203.255.3.3           00-de-fb-84-d4-43     dynamic
  203.255.3.12          1c-69-7a-73-e6-cd     dynamic
  203.255.3.16          94-c6-91-3d-db-b7     dynamic
  203.255.3.22          50-b7-c3-ab-57-fa     dynamic
  203.255.3.24          00-0c-29-41-fd-ba     dynamic
  203.255.3.27          00-d8-61-8a-67-35     dynamic
  203.255.3.41          00-03-2e-24-06-c0     dynamic
  203.255.3.58          1c-69-7a-97-49-6e     dynamic
  203.255.3.72          64-e5-99-16-5f-21     dynamic
  203.255.3.91          10-05-01-4d-86-01     dynamic
  203.255.3.92          64-e5-99-16-5f-21     dynamic
```

그림 13. 양쪽 대상으로 ARP 스푸핑 공격 후 타깃 PC의 ARP 캐시 테이블
Fig. 13. ARP cache table of target PC after ARP spoofing attack on both targets

그림 13은 게이트웨이와 서버를 동시에 ARP 스푸핑 공격을 진행한 결과이며, 게이트웨이의 MAC 주소 00-00-0C-9F-F0-03이 공격자 PC의 MAC 주소 10-05-01-4D-86-01로 서버의 MAC 주소 00-0C-29-41-FD-BA가 공격자 PC의 MAC 주소 10-05-01-4F-86-01로 변경된 ARP 캐시 테이블을 확인할 수 있다.

4-2 ARP 스푸핑 공격 패킷 탐지

본 연구에서는 위와 같은 ARP 스푸핑 공격 기법들의 탐지를 위해 ARP 패킷을 수집하고, 그림 14는 패킷 분석 테이블이며, idx는 패킷이 수집되는 순서를 기록하기 위한 인덱스 번호로 사용되며, arp_type은 ARP 패킷의 요청 또는 응답의 종류를 구분하기 위해 사용된다. timestamp는 ARP 패킷의 발생 시간을 기록하기 위해 사용되며, is_garp는 GARP를 ARP 스푸핑 공격으로 오탐하는 것을 방지하기 위해 사용한다. 그림 15는 패킷 분석 테이블을 기반으로 ARP 공격을 탐지하기 위해 ARP 요청과 응답 패킷을 수집하는 과정이다. 이 과정을 통해 수집된 패킷을 시그니처 정보 기반으로 분석하여 ARP 공격을 탐지하게 된다. 정상적인 ARP 요청 패킷은 브로드캐스트 방식으로 전송되며, recv_mac이 00:00:00:00:00:00으로 값이 비어있거나 FF:FF:FF:FF:FF:FF와 같이 브로드캐스트의 MAC 주솟값이 입력되어 전송된다. 그림 16은 ARP 요청 패킷이 유니캐스트 방식으로 전송된 패킷이다. 해당 패킷은 ARP 요청 패킷이 유니캐스트인 시그니처 정보에 해당하며, 비정상적인 ARP 패킷으로 간주한다.

idx	arp_type	send_mac recv_mac	send_ip recv_ip	timestamp	is_garp

그림 14. 패킷 분석 테이블
Fig. 14. Packet analysis table

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
1	ARP Request	84:25:19:A3:15:C6	00:00:00:00:00:00	203.255.3.150	203.255.3.138	23:57:06.188	N
2	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.220	23:57:06.417	N
3	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.117	23:57:06.439	N
4	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.229	23:57:06.439	N
5	ARP Request	F4:4D:30:49:62:45	00:00:00:00:00:00	203.255.3.60	203.255.3.5	23:57:06.453	N
6	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.176	23:57:06.513	N
7	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.246	23:57:06.513	N
8	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.11	23:57:06.649	N
9	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.253	23:57:06.671	N
10	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.13	23:57:06.671	N
11	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.249	23:57:06.708	N
12	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.31	23:57:06.708	N
13	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.174	23:57:06.711	N
14	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.58	23:57:07.459	N
15	ARP Request	F4:4D:30:49:62:45	00:00:00:00:00:00	203.255.3.60	203.255.3.5	23:57:07.463	N
16	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.173	23:57:07.471	N
17	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.19	23:57:07.475	N
18	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.239	23:57:07.568	N
19	ARP Request	F8:D3:A9:A9:8E:85	FF:FF:FF:FF:FF:FF	203.255.3.41	203.255.3.1	23:57:07.626	N
20	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.38	23:57:07.684	N
21	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.178	23:57:07.714	N
22	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.220	23:57:08.429	N
23	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.230	23:57:08.453	N
24	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.39	23:57:08.471	N
25	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.187	23:57:08.511	N
26	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.145	23:57:08.571	N
27	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.237	23:57:08.571	N
28	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.167	23:57:08.631	N
29	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.81	23:57:08.691	N
30	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.76	23:57:09.412	N
31	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.211	23:57:09.461	N
32	ARP Request	00:DE:FB:84:D4:43	FF:FF:FF:FF:FF:FF	203.255.3.3	203.255.3.173	23:57:09.477	N

그림 15. ARP 패킷 수집 과정
Fig. 15. ARP packet collection process

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
800	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	23:43:33.769	N

그림 16. 유니캐스트 방식의 ARP 요청 패킷
Fig. 16. ARP request packet in unicast method

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
992	ARP Reply	10:05:01:4D:86:01	FF:FF:FF:FF:FF:FF	203.255.3.1	203.255.3.90	05:38:39.718	N

그림 17. 브로드캐스트 방식의 ARP 응답 패킷
Fig. 17. ARP reply packet in broadcast method

ARP 과정은 ARP 요청 패킷에 대응해 응답 패킷이 전송된다. 정상적인 응답 패킷은 요청 패킷을 보낸 PC에 자신의 MAC 주소를 보내기 위해 유니캐스트 방식으로 요청 PC에 응답 패킷을 송신한다. 하지만 그림 17은 ARP 응답 패킷을 브로드캐스트 방식으로 전송된 패킷이다. 해당 패킷은 ARP 응답 패킷이 브로드캐스트인 시그니처 정보에 해당하며, 비정상적인 ARP 패킷으로 간주한다.

그림 18은 IP : 203.255.3.1, MAC : 00:00:0C:9F:F0:03에서 IP : 203.255.3.90, MAC : 00:00:00:00:00:00으로 전송되는 정상적인 ARP 패킷이다. 그림 18의 이더넷 프레임 헤더의 출발지 주솟값과 ARP 헤더의 출발지 주솟값을 확인하게 되면 00:00:0C:9F:F0:03으로 동일한 값인 것을 확인할 수 있다. 하지만 그림 19의 이더넷 프레임 헤더의 출발지 주솟값과 ARP 헤더의 출발지 주솟값을 확인하게 되면 Source MAC : 00:00:0C:9F:F0:03, Sender MAC Address 값이 10:05:01:4D:86:01로 ARP 헤더의 출발지 주솟값이 공격자의 MAC 주소로 서로 상이한 값을 가지는 ARP 요청 패킷으로 볼 수 있다. 해당 패킷은 이더넷 헤더와 ARP 헤더의 MAC 주솟값이 상이한 시그니처 정보에 해당하며, 비정상적인 ARP 패킷으로 간주한다.

```
Frame 92: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_9f:f0:03 (00:00:0c:9f:f0:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Source: Cisco_9f:f0:03 (00:00:0c:9f:f0:03)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Cisco_9f:f0:03 (00:00:0c:9f:f0:03)
  Sender IP address: 203.255.3.1
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 203.255.3.90
```

그림 18. 정상적인 ARP 요청 패킷
Fig. 18. Normal ARP request packets

```
Frame 36: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
Ethernet II, Src: Cisco_9f:f0:03 (00:00:0c:9f:f0:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Source: Cisco_9f:f0:03 (00:00:0c:9f:f0:03)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Pegatron_4d:86:01 (10:05:01:4d:86:01)
  Sender IP address: 203.255.3.1
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 203.255.3.90
```

그림 19. 이더넷 MAC 값과 ARP MAC 값이 일치하지 않는 ARP 요청 패킷
Fig. 19. ARP request packet whose Ethernet MAC and ARP value do not match

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
2124	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:38:26.546	N
2239	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:38:36.545	N
2347	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:38:46.542	N
2442	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:38:56.564	N
2558	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:39:06.595	N
2643	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:39:16.608	N

그림 20. 10초 간격으로 반복적으로 수신되는 ARP 응답 패킷
Fig. 20. ARP response packet received repeatedly at 10-second intervals

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
2672	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:02.858	N
2685	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:04.853	N
2717	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:06.863	N
2739	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:08.873	N
2758	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:10.880	N
2777	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:12.887	N
2793	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:14.892	N
2816	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:16.896	N
2835	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:18.900	N
2858	ARP Reply	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:42:20.903	N

그림 21. 2초 간격으로 반복적으로 수신되는 ARP 응답 패킷
Fig. 21. ARP response packet received repeatedly at 2-second intervals

idx	arp_type	send_mac	recv_mac	send_ip	recv_ip	timestamp	is_garp
2915	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:48:06.155	N
2973	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:48:09.933	N
3039	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:48:15.653	N
3106	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:48:20.901	N
3299	ARP Request	10:05:01:4D:86:01	F0:2F:74:84:B1:31	203.255.3.1	203.255.3.90	08:48:29.478	N

그림 22. 일정 시간 동안 반복적으로 수신되는 ARP 요청 패킷
Fig. 22. ARP request packet received repeatedly for a certain period of time

Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0c9f.f003	DYNAMIC	Fa0/24
1	000c.2941.fdba	DYNAMIC	Fa0/2
1	1005.014d.8601	DYNAMIC	Fa0/10
1	f02f.7484.b131	DYNAMIC	Fa0/1

그림 23. 정상적인 스위치의 MAC 주소 테이블
Fig. 23. MAC address table of normal switch

Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0c9f.f003	DYNAMIC	Fa0/24
1	000c.2941.fdba	DYNAMIC	Fa0/2
1	f02f.7484.b131	DYNAMIC	Fa0/1

그림 24. 공격자 차단 후 MAC 주소 테이블
Fig. 24. Switch MAC address table after blocking attackers

그림 20, 그림 21, 그림 22는 ARP 패킷이 일정 시간 동안 반복 수신되는 시그니처 정보를 가진 패킷이다. 패킷 정보를 확인하면 send_mac : 10:05:01:4D:86:01, send_ip : 203.255.3.1, recv_mac : F0:2F:74:84:B1:31, recv_ip : 203.255.3.90이며, 공격자가 게이트웨이의 MAC 주소를 공격자의 MAC 주소로 변경하여 일정 시간 동안 반복 전송하는 형태의 ARP 공격 패킷을 확인할 수 있다.

그림 20은 약 10초 간격으로 위조된 ARP 응답 패킷이 타깃 PC로 전송되고 있으며, 그림 21은 약 2초 간격으로 위조된 ARP 응답 패킷이 타깃 PC로 전송되고 있다. 그림 20과 그림 21은 자동화 ARP 스푸핑 툴을 사용한 형태로 2초, 10초와 같은 일정한 시간 간격을 가지고 타깃 PC에 재전송되는 시그니처 정보를 보인다. 하지만 그림 22는 자동화 ARP 스푸핑 툴을 사용한 것과는 다르게 일정한 시간 간격으로 타깃 PC에 ARP 패킷을 전송하지는 않는다.

그림 22는 랜덤한 시간 간격을 가지고 ARP 패킷을 타깃 PC에 전송하여 ARP 포이즈닝 탐지 시스템을 우회할 수 있는 패턴이다. 하지만 공격자는 원활한 스니핑 공격을 실행하는 특정 시간 동안 타깃 PC에 반복적으로 ARP 패킷을 전송한다. 만약 반복적으로 ARP 패킷을 전송하지 않게 되면 정상적인 ARP 패킷으로 인해 원활한 스니핑 공격이 이루어지지 않는다. 이러한 공격 특성을 활용하여 일정 시간 안에 반복 수신되는 ARP 패킷은 비정상 패킷으로 판단할 수 있는 시그니처 정보가 된다.

4-3 ARP 스푸핑 공격 차단

그림 23은 ARP 스푸핑 공격을 탐지하기 전 정상적인 스위치 테이블이며, 그림 9와 같이 게이트웨이의 MAC 주소 0000.0C9F.F003과 포트 Fa0/24, 타깃 PC의 MAC 주소 F02F.7484.B131과 포트 Fa0/1, 서버의 MAC 주소 000C.2941.FDBA와 포트 Fa0/2, 공격자의 MAC 주소 1005.014D.8601과 포트 Fa0/10의 정보를 확인할 수 있다. 본 논문에서 제안한 ARP 공격 시그니처 정보에 기반하여 ARP 스푸핑 공격 탐지하는 과정을 보였다. ARP 공격 시그니처 정보에 기반하여 탐지하는 과정에서 공격자로 판단되는 PC의 MAC 주소는 10:05:01:4D:86:01이며, 해당 MAC 주소에 대응하는 스위치 포트를 차단한다. 공격자를 차단한 후 스위치의 모습은 그림 24와 같다.

4-4 기존 기법과 비교 평가

본 연구에서 제안한 기법과 기존의 방법을 비교한 내용은 표 6에 나타나 있다. 프로토콜 기법은 ARP 응답에 대해 아무런 인증 없이 ARP 테이블을 갱신하는 취약점을 해결하기 위해 제안된 기법이며, ARP의 근본적인 취약점을 해결할 수 있다. 프로토콜 기법은 인증 과정을 추가하여 ARP의 근본적인 취약점을 해결하였다. 하지만 현 네트워크 체계의 전면적인 변경이 필요하다. 또한 정상 호스트를 다운시키고 호스트의 MAC 주소를 복제하여 위장 가능하며, 공개키를 얻거나 호스트를 확인하기 위해 발생하는 추가 처리시간이 ARP에 비해 성능 오버헤드를 발생시키고 관리하는 노드의 숫자가 많아질수록 과부하가 발생한다. 또한, 프로토콜 기법은 ARP 과정에서 ARP 응답 패킷에 대한 인증 과정만 수행한다. ARP 응답 패킷에 대한 인증 과정은 위조된 ARP 응답 패킷을 송신한 호

스트를 탐지할 수 있지만, ARP 요청 패킷에 대한 인증 과정은 존재하지 않아 위조된 ARP 요청 패킷과 이더넷 헤더와 ARP 헤더의 주솟값이 상이한 패킷의 경우 ARP 공격을 탐지하지 못하는 취약점을 가지고 있다.

정적 ARP 테이블 기법은 신뢰할 수 있는 MAC 주소 정보와 기존 네트워크 체계에 적용 가능한 장점이 있다. 정적 ARP 테이블 기법은 신뢰할 수 있는 IP 주소와 MAC 주소를 수동으로 매칭시켜 ARP 테이블에 등록한다. 하지만 신뢰할 수 있는 ARP 테이블 유지를 위해 MAC 주소에 대한 빈번한 리셋 과정이 필요하다. 일반적으로 공격자가 송신한 위조된 ARP 응답 패킷을 수신하게 되면 위조된 ARP 패킷 정보로 ARP 캐시 테이블 정보가 변조되지만, 정적 ARP 테이블 기법은 IP 주소와 MAC 주소가 변경되지 않는다. 해당 기법은 위조된 ARP 응답 패킷으로 고정된 IP 주소와 MAC 주소의 변경을 시도할 때 변조를 방지하고 ARP 공격자를 탐지할 수 있지만, 위조된 ARP 요청 패킷과 이더넷 헤더와 ARP 헤더의 주솟값이 상이한 패킷은 탐지하지 못하는 취약점을 가지고 있다.

프로토콜 기법과 정적 ARP 테이블 기법의 공통점은 ARP 포이즈닝 기반 공격 패턴에서 발생하는 위조된 ARP 응답 패킷 탐지는 가능하지만, 그 외 ARP 공격으로 사용되는 유니캐스트 방식의 ARP 요청 패킷 공격, 일정 시간 동안 반복 수신되는 ARP 요청 패킷 공격, 이더넷 헤더와 ARP 헤더의 주솟값이 상이한 공격은 탐지하지 못하는 취약점을 보인다.

표 6. 비교 평가표
Table 6. Comparative evaluation table

Proposed Method / Attack Method	Protocol method	Static ARP Table Method	Proposed Signiture Method
ARP Request Packet Attack of Unicast Method	X	X	○
ARP Reply Packet Attack of Broadcast Method	○	○	○
Attack that MAC addresses of Ethernet and ARP Headers are Different	X	X	○
ARP Request Packet Received Repeatedly During a Certain Amount of Time	X	X	○
ARP Reply Packet Received Repeatedly During a Certain Amount of Time	○	○	○

Ⅴ. 결론

네트워크에 대한 의존도가 높아질수록 관련 보안 문제도 빈번하게 발생하고 있으며, 이러한 네트워크 기반의 보안 사고로 인한 피해 사례도 급격하게 증가하는 추세이다[6]. 본 논문은 이러한 문제점들과 피해 사례를 방지하는 데 그 목적이 있다. 또한 ARP 스푸핑 공격을 막기 위해 다양한 기법들이 제안되어왔으나 기존의 네트워크에 적용하기 어렵거나 금전적인 비용 때문에 대중화되지 못하였다[7-10]. 이에 본 논문에서는 기존 네트워크 프로토콜의 변경 없이 쉽게 적용할 수 있는 시그니처 정보를 기반으로 ARP 스푸핑 탐지 및 차단 기법을 제안하였다.

원활한 스니핑 공격을 위해 다양한 ARP 스푸핑 공격 기법들이 사용되지만, 공격 기법마다 고유한 시그니처 정보를 가지고 반복적으로 비정상적인 ARP 패킷을 전송하게 된다. 하지만 기존의 연구 기법에서 사용된 ARP 스푸핑 공격 기법은 자동화 툴을 사용하여 단일화된 공격 패턴으로 ARP 캐시 테이블 내용의 변조를 방어하는 다양한 기법들을 제시해왔다. 이러한 연구들은 단일화된 ARP 스푸핑 공격에 대해 ARP 캐시 테이블의 변조를 방어하는데 좋은 성능을 발휘할 순 있지만 다양하고 복합적인 ARP 스푸핑 공격 기법에는 취약한 부분도 존재한다. 그로 인해 본 논문은 다양한 ARP 스푸핑 공격 기법에서 나타나는 ARP 패킷의 형태를 대상으로 ARP 스푸핑 공격을 판단하는 연구를 진행하였다. 연구 과정은 ARP 스푸핑 공격 기법에 대해 실질적으로 다양한 공격 과정들을 보인 다음 다양한 공격 기법에서 나타나는 시그니처 정보를 분석하였다. 분석된 시그니처 정보를 통해 ARP 스푸핑 공격 탐지를 위한 정보로 사용되는 결과를 보였다. 하지만 시그니처 정보는 특정 목적을 가지고 발생시키는 정상적인 패킷을 비정상적인 패킷으로 판단하는 한계점을 가지고 있다. 하지만 제안한 기법은 과거의 ARP 스푸핑 공격을 방어하는 연구들이 보여주지 못한 다양한 ARP 스푸핑 공격 기법과 방어하는 방법으로 과거의 메커니즘을 벗어나 새로운 가능성을 보여주었다. 향후 연구과제로는 FP(False Positive)를 줄이는 연구가 지속되어야 할 것이다.

참고문헌

[1] D. Bruschi, A. Ornaghi and E. Rosti, “S-ARP: A Secure Address Resolution Protocol,” *19th Annual Computer Security Applications Conference*, pp. 66-74, July 2003. https://doi.org/10.1109/CSAC.2003.1254311

[2] B. Scott and et al., “An Interactive Visualization Tool for Teaching ARP Spoofing Attack”, *2017 IEEE Frontiers in Education Conference (FIE),* pp. 1-5, December 2017. https://doi.org/10.1109/FIE.2017.8190531

[3] H. S. Kang and C. S. Hong, “A Defense Technique against ARP Spoofing Attacks using a Keystone Authentication Table in the OpenStack Cloud Environment,” *The Journal of KIISE,* Vol. 45, No. 8, pp. 755-760, August 2018.

[4] A. M. AbdelSalam, A. B. El-Sisi and V. Reddy, “Mitigating ARP Spoofing Attacks in Software-Defined Networks,” *25th International Conference on Computer Theory and Applications(ICCTA)*, pp. 126-131, August 2015.

https://doi.org/10.1109/ICCTA37466.2015.9513433

[5] S. Y. Nam, D. Kim and J. Kim, "Enhanced ARP: Preventing ARP Poisoning-based Man-in-the-middle Attacks," *in IEEE Communications Letters,* Vol. 14, No. 2, pp. 187-189, February 2010.
https://doi.org/10.1109/LCOMM.2010.02.092108

[6] G. Lim, M. Liu and J. Lee, "A Study on the Damage Cost Estimation Model for Personal Information Leakage in Korea", *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 28, No. 1, pp. 215-227, 2018.
https://doi.org/10.13089/JKIISC.2018.28.1.215

[7] W. Lootah, W. Enck and P. McDaniel, "TARP: Ticket-based Address Resolution Protocol," *Computer networks*, Vol. 51, pp. 4322-4337, October 2007.
https://doi.org/10.1016/j.comnet.2007.05.007

[8] S. Hong, M. Oh, S. Lee and S. Lee, "Efficient Technique for Preventing ARP Spoofing Attacks using Reliable ARP Table", *The Journal of KIISE : Computing Practices and Letters*, Vol. 17, No. 1, pp. 26-30, January 2011.

[9] D. Pansa and T. Chomsiri, "Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol," *2008 Third International Conference on Convergence and Hybrid Information Technology*, Vol. 2, pp. 21-26, November 2008.
https://doi.org/10.1109/ICCIT.2008.345

[10] S. Kumar and S. Tapaswi, "A Centralized Detection and Prevention Technique against ARP Poisoning," *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec),* pp. 259-264, July 2012.
https://doi.org/10.1109/CyberSec.2012.6246087

[11] D. C. Plummer, "RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," *Internet Engineering Task Force*, Network Working Group, November 1982.

[12] S.Morsy and D.Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing", *in IEEE*, Vol. 10, pp. 49142-49153, May 2022.
https://doi.org/10.1109/ACCESS.2022.3172329

[13] Girdler and V. Vassilakis, "Implementing an intrusion detection and prevention system using Software-defined Networking:Defending against ARP spoofing attacks and Blacklisted MAC Addresses", *Computers and Electrical Engineering*, Vol. 90, pp. 106990, March 2021.
https://doi.org/10.1016/j.compeleceng.2021.106990

최준호(Jun-Ho Choi)

2020년 : 경상국립대학교 컴퓨터과학과 (공학사)
2022년 8월 : 경상국립대학교 대학원 컴퓨터과학과 (공학석사)
2021년~현 재 : SK 쉴더스

※관심분야 : 정보보호(Personal Information), 네트워크 보안(Network Security) 등

이수원(Suwon Lee)

2010년 : 경북대학교 컴퓨터학부 (공학사)
2012년 : 한국과학기술원 전산과 (공학석사)
2017년 : 한국과학기술원 전산과 (공학박사)
2018년~현 재 : 경상국립대학교 컴퓨터과학과 부교수

※관심분야 : 증강현실, 컴퓨터비전, SLAM, 머신 러닝, 네트워크보안

서영건(Yeong Geon Seo)

1987년 : 경상대학교 전산과 (이학사)
1997년 : 숭실대학교 전산과 (공학박사)
1989년~1992년 : 삼보컴퓨터
1997년~현 재 : 경상국립대학교 컴퓨터과학과 교수
2022년~현 재 : 경상국립대학교 정보전산처장

※관심분야 : 의료 영상 처리, 머신 러닝, SLAM, 영상 인식, 컴퓨터 네트워크 등