# ARP spoofing 바이러스에 감염된 단말을 효율적으로 분리하기 위한 네트워크 관리시스템의 설계

고봉구* · 정성종** · 조기환***

# A Design of Network Management System for Efficiently Isolating Devices Infected with ARP Spoofing Virus

Bong-koo Ko* · Seung-jong Chung** · Gi-hwan Cho***


## 요 약

ARP spoofing 공격은 자신의 MAC 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격유형이다. 네트워크 장비의 상태를 관찰함으로써 ARP spoofing 바이러스에 감염 PC를 찾아내 전산망으로부터 분리하는 형태로 대응하고 있다. 그러나 전산망 관리자의 수작업에 의한 대응은 시간과 정확성에서 한계를 지닌다. 본 논문은 ARP spoofing 공격의 수작업에 의한 대응 과정을 분석하고, 관리자의 지속적인 관찰을 대체할 수 있는 네트워크 관리시스템을 제안한다. ARP 분석기와 차단명령 발송기를 설계하여 기존 시스템에 추가함으로써 더욱 빠르고 정확하게 감염 PC를 찾아내는 기반을 제공한다. 그 결과로 전산망 서비스 중단을 최소화하고 네트워크 관리의 편의성을 높인다.

## ABSTRACT

ARP spoofing is a typical Internet attack, in which an attacker sends data by changing his's MAC address with the other's one. Currently, this attack is usually dealt with separating the attacking PCs infected with ARP spoofing virus, by keeping network devices investigating by the network manager. However, this manual process has some limitations in time and accuracy. This paper proposes a new network management system to replace the effort of network manager who has to keep on inspecting the network. Along with designing an ARP analyzer and a disconnection notifier and adding them into the existing network management system, the proposed system provides a basement to identify and notify the PC infected by an ARP spoofing virus with fast and high accuracy. As a result, it is expected to minimize the network break off and to make easy the network management.



키워드

스푸핑, 바이러스, MAC 주소, 네트워크 관리 시스템

Key Words

Spoofing, Virus, MAC Address, Network Management System



* 정회원 : 전북대학교 정보전산원(주저자)

** 정회원 : 전북대학교 IT정보공학과(공동저자)

*** 정회원 : 전북대학교 컴퓨터공학부(클라우드오픈R&D센터)

(교신저자, ghcho@jbnu.ac.kr)



접수일자 : 2012. 10. 19

심사완료일자 : 2012. 11. 07

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.3.641



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

Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

## Ⅰ. 서 론

군사적인 목적으로 시작된 인터넷은 최근 게임, 쇼핑, 연구 및 교육 등 우리의 생활의 모든 것을 대체하고 있다. 이러한 상황에서 해킹, 크래킹 등은 이미 도래한 정보화 중심의 사회에 치명적인 역기능으로 인하여 사회적 긴장감이 높은 현실이다. 많은 사람이 이용하는 인터넷 서비스의 중단, 남의 개인 정보 도용, 서비스 중단을 협박 등의 역기능이 보고되고 있다[1][11]. 이와 같은 폐해를 방지하기 위해서 최근에는 정보보호 기술의 발달, 또는 고가의 장비도입 등 순환적으로 정보통신 기술의 발달이 이루어지고 있다. 전산망 장비의 보완에도 불구하고 교내 전산망 서비스를 중단하게 하는 아주 심각한 원인중의 하나는 컴퓨터 바이러스(virus), 웜(worm)등 악성 소프트웨어에 의한 것이다. ARP(Address Resolution Protocol) spoofing(혹은 ARP poisoning)은 논리적 식별자인 인터넷(IP) 주소를 물리적 식별자인 하드웨어(MAC) 주소로 변환하는 ARP 프로토콜의 특성을 이용한 공격이다. 즉, 공격자가 MAC 주소에 대해 묻고 응답하는 ARP 패킷을 조작하여 다른 컴퓨터의 MAC인 것처럼 속이는 공격유형이다. ARP 프로토콜은 동일한 IP 주소를 사용하는 로컬네트워크에서 동작한다. 따라서 공격자는 심각한 네트워크 트래픽을 유발하여 해당 로컬네트워크의 정상적인 통신이 불가능하게 방해하거나, 심지어는 속임을 당한 컴퓨터로 위장하여 정상적인 통신에 참여하는 효과를 기대하고 공격한다[2][12].

통상 바이러스 형태의 악성코드에 의해 진행되는 ARP spoofing 공격은 정상적인 사용자 자신이 공격의 원천임을 인지하지 못하는 상태에서 진행된다. 즉 감염증상 확인 및 감염사실 여부 확인을 위해서 사용자로 하여금 별도의 노력이 필요하다[3]. 악성코드는 웹브라우저나 USB에 의해 감염될 수 있으며, 일단 감염되면 동일한 로컬네트워크에 연결된 컴퓨터 전체로 악성코드를 빠르게 전파할 수 있다. 또한 사용자 몰래 추가적인 악성코드 다운로드를 시도하여 각종 스파이웨어 등의 악성코드를 설치 할 수 있다. 이로 인해 전산망 서비스의 신뢰성이 훼손되고, 고가의 장비의 추가 설치와 같은 금전적인 손해가 발생된다[4][13].

본 논문은 네트워크 관리시스템을 기반으로 ARP spoofing 공격에 대해 효과적으로 대응하기 위한 방안을 제시한다. 먼저 일반적으로 현재 적용되고 있는 ARP spoofing 공격에 대한 대응절차를 분석하다. ARP spoofing에 감염된 PC를 식별하는 과정과, 감염됨 PC를 전산망에서 분리하여 전산망 서비스를 재개하기 위한 전산망 관리자가 수행하는 절차를 살펴본다. 다음으로 ARP 분석기를 기반으로 공격을 식별하고 원격에서 공격 PC를 분리하는 차단명령 발송기로 구성된 자동화된 네트워크 관리시스템을 설계를 제시한다. 제시된 시스템은 더욱 빠르고 정확하게 감염 PC를 찾아내는 기반을 제공함으로써 전산망 서비스 중단을 최소화하고 관리의 편의성을 높이는 기반을 제공한다.

본 논문은 2장에서는 ARP spoofing 의 동작 원리 및 기존의 대응 방안을 설명하고, 3장에서는 전산망 및 보안관리자가 공격자 PC 식별 과정과 이를 분리하기 위해서 수행하는 수동적인 절차를 분석한다. 4장에서는 3장의 분석을 기반으로 대응 시간과 절차에서 효과적인 네트워크 관리시스템의 설계를 구체적으로 서술한다. 5장에서는 본 논문의 결론을 맺는다.

## Ⅱ. 관련 연구

비록 응용에서는 사람의 편의를 위해서 논리적인 IP 주소를 사용하지만 이더넷(Ethernet)을 기반으로 운영되고 있는 로컬네트워크에서 실제적인 데이터 전송과정은 MAC주소에 의한 통신이 이루어진다. 네트워크 계층에서 라우팅을 수행하여 다음 홉의 IP 주소를 산출하였으나 해당 IP 주소의 MAC 주소를 알지 못하는 경우, 로컬네트워크에 접속하고 있는 모든 호스트에게 ARP request 메시지를 브로드캐스트 한다. 요청한 IP 주소에 대응하는 MAC 주소를 가지고 있는 호스트가 MAC 주소를 포함한 정보를 reply함으로써 MAC 주소를 획득한다. 매 통신시마다 반복해서 ARP 프로토콜을 수행하는 비효율성을 개선하기 위해서 각 호스트는 MAC 주소를 관리하기위한 ARP-cache를 운영한다. 호스트는 최신의 {IP 주소 : MAC 주소}로 구성된 ARP-cache 정보를 동적으로 유지, 관리한다. ARP spoofing 공격은 ARP 프로토콜의 특성을 이용한 공격유형이다. 공격자가 위조된 IP 주소 혹은 MAC 주소로 ARP를 수행하면 로컬네트워크에 연결된 각 호스트들은 위조된 정보로 ARP-cache를 갱신한다. 추후 위조된 주소를 사용하는 호스트에게 보내지는 데이터는 공격자에게 전달되게 된다. 그 결과로

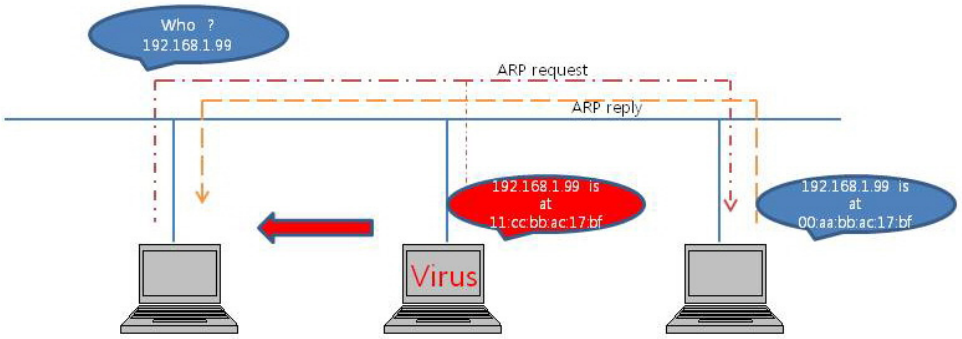


그림 1. ARP spoofing 공격 시나리오
Fig. 1 A demonstrative scenario for ARP spoofing attack

동일한 로컬네트워크에 연결된 정상적인 호스트들의 통신을 방해하여 전산망 서비스를 중단시키는 결과를 초래한다[5]. 또한 APP spoofing을 Man-In-The- Middle 공격의 수단으로 활용하면 동일 로컬네트워크 상에서 공격대상 시스템 사이에 오고가는 통신 내용을 가로채는 스니핑 목적으로 악용되기도 한다[6]. 스니핑 뿐만 아니라 전송되는 데이터의 위변조 과정이 충분히 가능하며, 심지어 VoIP(Voice over IP) 환경에서 인터넷 전화의 도청도 가능할 수 있다.

이와 같은 ARP spoofing 공격이 가능한 근본적인 요인은 ARP request와 reply를 수행하는 호스트간에 신뢰성 있는 상호 인증절차가 없이 수행되기 때문이다. 이를 해결하기 위해서 그동안 다양한 노력이 진행되어 왔다. 로컬네트워크에 제 3자인 CS(Certification Authority)를 구성하고 암호화 키를 분배함으로써 상호인증과 기밀성을 확보하는 방법이 제시되었다[2][7]. 이 방법은 로컬네트워크마다 추가적인 구현 부담이 있고, 기존의 ARP 프로토콜과 호환성 문제가 발생하여 일반화된 기존의 ARP 프로토콜을 사용하는 전산망에서 사용하기는 부적절하다. 다른 접근으로 신뢰성 있는 ARP 테이블유지를 위해 MAC 관리 장비를 두고 새로운 PC 부팅 시 인증을 통하여 신뢰성 있는 장비인 경우 MAC table에 등록시키고 기존의 MAC 정보를 넘겨주는 방안이다[8-9]. 이 방안은 MAC 주소의 고유특성으로 인하여 로컬네트워크의 범주를 넘어서 관리하기 어려운 한계가 있다. 소규모의 전산망인 경우는 관리에 문제가 없으나 커다란 전산망인 경우는 관리해야 할 장비 수에 비례하여 관리의 복잡도가 크게 늘어나다. 즉, 신규 장비의 MAC 정보, 사용자 정보(연락처 및 신분 등), 연결 장비 정보(장비 IP, 해당 포트 정보 등)의 관리와 정보의 변화를 일관성 있게 수용하기 어렵다. 참고문헌[10]에서는 기존의 ARP 감시용 툴(sniffswitch, XARP, ARPwatch 등)을 이용하는 방안을 제시하고 있으나, 전산망 규모가 커지면 복잡도는 여전히 해결해야 하는 문제로 지적된다.

본 논문은 어차피 감염 PC는 전산망에 연결되어 있으나 없으나 전산망 사용이 불가능하다. 감염 PC가 있는 전산망에서 감염 PC를 고립함으로서 정상적인 PC는 전산망이용에 문제가 없다. 따라서, 감염PC를 발견 시 강제적으로 전산망에서 분리함으로서 정상PC 사용자에게는 바로 인터넷을 이용할 수 있게 하고, 감염 PC사용자는 PC를 치료하여 전산망을 사용할 수 있게 함으로 장비에 대한 투자 없이 피해를 최소화 할 수 있다. 이에 수동적인 방법으로 관리자가 L2 스위치, L3 스위치, MAC 관리 장비 등 여러 장비의 상황을 파악하여 대처하였는데 이를 자동화하여 서비스 중단을 최소화하고 관리의 편의성을 높일 수 있다.

## Ⅲ. ARP spoofing 공격에 대한 기존의 대응

전산망이 구성된 기관은 네트워크 운용 상태를 계속해서 모니터함으로써 전산망 서비스 중단을 바로 인지할 수 있도록 일반적으로 NMS(Net- work Management System)를 구축 운용한다. 하지만 NMS를 운용의 한계로

| Protocol | Address | Age (min) | Hardware Addr | Type | Interface | |
|---|---|---|---|---|---|---|
| Internet | 203.254.129.21 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | |
| Internet | 203.254.129.22 | 0 | 0007.e904.9196 | ARPA | Vlan429 | |
| Internet | 203.254.129.23 | 0 | 0007.e904.9446 | ARPA | Vlan429 | |
| Internet | 203.254.129.1 | 0 | 0018.73d6.b608 | ARPA | Vlan429 | 게이트웨이 |
| Internet | 203.254.129.15 | 0 | 0023.34f4.4b41 | ARPA | Vlan429 | |

그림 2. 정상적인 ARP table의 예
Fig. 2 An example of ARP table in case of normal

| Protocol | Address | Age (min) | Hardware Addr | Type | Interface | |
|---|---|---|---|---|---|---|
| Internet | 203.254.129.21 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | |
| Internet | 203.254.129.22 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | |
| Internet | 203.254.129.23 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | |
| Internet | 203.254.129.1 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | 게이트웨이 |
| Internet | 203.254.129.15 | 0 | 0018.8b4b.fa42 | ARPA | Vlan429 | |

그림 3. ARP spoofing 발생한 ARP table의 예
Fig. 3 An example of ARP table in case of ARP spoofing attack

인하여 하위 네트워크상에서 발생하는 서비스 중단 현상은 대부분 최종 사용자의 신고에 의해 인지되는 경우가 많은 부분을 차지한다. 그림 2는 ARP spoofing 공격에 의한 전산망의 서비스 중단을 방지하기 위해서 전산망 관리자가 수행하는 수작업에 의한 일반적인 절차를 보이고 있다.

전산망 서비스가 중단되었음을 인지한 경우, 관리자는 ARP spoofing에 의한 서비스 중단인지 여부를 판단한다. 가장 널리 사용하는 방법은 L2 스위치 장비의 MAC table을 검색하여 이를 판단한다. 그러나 특이한 경우로써 여러 개의 IP주소로 운용되는 거대한 전산망의 경우에는 primary IP 주소를 제외한 secondary IP주소 등을 살펴 볼 수 없게 되다. 따라서 ARP spoofing 여부의 판단에 문제가 발생할 수도 있다. 이런 경우에는 L3 스위치의 MAC table을 분석하면 판단이 가능하다. 또한 L2 스위치의 경우에는 ARP spoofing으로 인하여 원격 접속이 불가능한 경우가 있으며, 이러한 경우도 L3스위치의 MAC table을 clear 하면 L2 스위치 접근이 가능하다.

L2 스위치에 접근해서 ARP table을 살펴보면 ARP spoofing 여부와 이를 발생시킨 MAC 주소를 쉽게 식별할 수 있다. 그림 2는 L2 스위치의 정상적인 ARP table을 예로 보이고 있다. 정상적인 ARP table을 보면 각 IP주소에 다른 MAC 주소(Hardware Addr)로 구성되어 있음을 볼 수 있다. 한편 그림 3은 ARP spoofing이 발생한 경우에 ARP table의 예를 보이고 있다. 이 경우에 서브넷에 연결된 모든 컴퓨터들의 MAC 주소가 동일하게 설정되어 있음을 보이고 있다. 또한 게이트웨이(예로 그림 2와 그림 4에서 203.254.129.1) 컴퓨터도 MAC 주소가 변경되어 있으며, 따라서 해당 서브넷은 동작할 수 없는 상태가 된다.

기존에 NMS를 수단으로 네트워크 관리자에 의해서 수행하는 ARP spoofing 공격의 대응 절차는 다음과 같다. 일단 ARP spoofing이 발견되면 해당 PC의 전산망 접속을 차단하기 위하여 사용자 정보와 L2 스위치의 해당 포트를 찾는 단계를 수행한다. 일반적으로 IP 및 MAC 주소를 관리하는 장비를 이용하여 특정 MAC 주소를 사용하는 PC 정보를 식별할 수 있다. NMS등을 이용하여 L2 스위치의 해당 포트를 disable함으로써 감염 PC를 고립화하거나 전산망 서비스를 차단하게 된다. 감염된 PC를 차단하면 다른 정상적인 사용자 서비스가 재개되게 된다. 정상서비스 개시 후 감염된 PC에 대한 최신 백신을 이용한 점검 및 보안 업데이트 등을 실시하여 안전성 여부를 확인 후 해당 PC에 대한 서비스 재개를 할 수 있다. 그림 4는 기존의 ARP spoofing 공격의 대응 절차를 보이고 있다.

그러나 ARP spoofing 공격에 대한 기존의 처리절차는 전산망 관리자의 경험과 지식을 기반으로 수작업으로 대응해야 하는 한계를 지닌다.

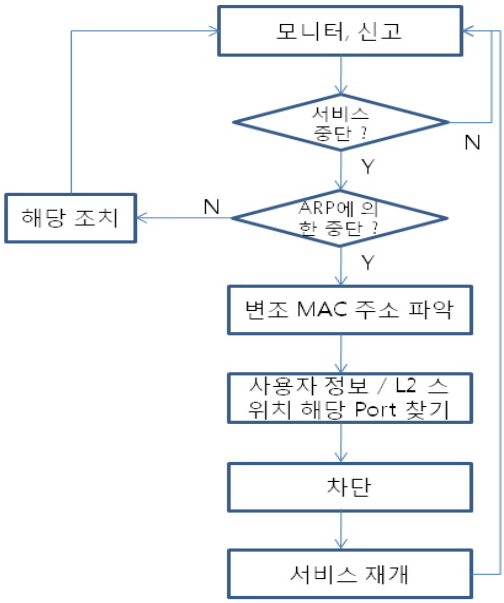


그림 4. 기존의 ARP spoofing 대응 절차
Fig. 4 The traditional respond sequence for ARP spoofing attack

특히 관리자가 전산망을 지속적으로 관찰하고 대응해야만 실효성을 얻을 수 있다. 또한 공격에 대한 대응과정에서 여러 장비가 연계되고, 각종 table의 내용에 근거하여 관리자가 판단하고 차단하고 재가동하고 절차를 수행하는 관리자의 능력, 시간, 그리고 노력에 따라서 대응 결과는 다르게 된다. 이러한 전산망 관리자에 의한 수동적 대응의 한계를 해결하고자 본 논문에서는 자동화 대응을 수행하는 네트워크 관리시스템을 제시한다.

## Ⅳ. 효율적인 ARP spoofing 대응을 위한 네트워크 관리시스템 설계

수작업에 의한 ARP spoofing 바이러스에 감염된 단말을 분리하는 일련의 작업은 전산망은 물론 보안에 대한 충분한 이해와 작업자의 성숙도에 따라 요구되는 시간의 편차와 업무의 정확성에 차이가 발생할 수 있다. 이러한 현실적인 제약을 완화하기 위하여 ARP spoofing 바이러스에 감염된 단말을 자동으로 분리하는 네트워크 관리시스템을 구축함으로써 작업을 빠르고 일괄적으로 수행하는 보다 적극적이고 자동화된 시스템에 대한 필요성이 최근 제시되고 있다. 본 논문에서 제안된 시스템은 여러 장비 정보를 분석하여, 판단하고, 실행하는 일련의 과정을 전산망 관리자의 직관에 의존하기 보다는 자동화 도구를 활용하는 접근이다. 제안된 네트워크 관리시스템은 기존의 네트워크 관리시스템에 ARP 분석기과 전산망접속 차단명령 발송기를 추가함으로써 구성된다.

전산망 서비스의 중단 여부를 감시하는 과정은 기존의 수작업 대응과 유사하게 기존 NMS 장비를 이용한다. 만약 특정 건물 서비스가 중단되었음을 발견하게 되면, ARP 분석기를 이용하여 ARP spoofing에 의한 중단인지 여부와 ARP spoofing 인 경우 원인이 되고 있는 MAC 주소를 결정한다. ARP 분석기는 전송된 ARP table 및 MAC table에서 MAC주소의 중복 여부를 판단한다. ARP table은 Protocol, Address, Age(min), Hardware Addr, Type, Interface 등의 정보로 구성된다. 또한 MAC table은 VLAN, MAC Address, Type, Ports 등의 정보로 구성된다. MAC 주소의 중복여부를 구현하기 위해 ARP 분석기가 ARP table 및 MAC table 정보를 받으면 일정 기준으로 정렬하여 MAC 주소를 비교하여 같은 지 여부를 판단한다. 이러한 과정에서 일부만 중복되고 있는지 전체가 중복되고 있는지를 판단할 수 있다. 표 1은 본 논문에서 제안하고 있는 시스템에서 사용되는 정보를 보이고 있다.

표 1. 제안된 시스템에서 ARP spoofing 대응을 위해 사용되는 정보
Table. 1 Information used for the proposed system to respond ARP spoofing attack

| table | 포맷 |
|---|---|
| 차단 목록 | IP, MAC, 사용자, L2 port |
| 건물별 IP | 건물명, 전산망 주소 |
| IP-MAC table(PMS, VMS, 기타) | IP, MAC |
| IP 사용자 table | IP, 사용자명, 연락처 |
| 건물별 L2/L3 스위치 IP | L2/L3 스위치 IP 정보, snmp |

MAC table은 PMS(Patch Management System)나 백신 서버로부터 해당하는 정보를 얻어서 구성할 수 있다. 또한 전용 MAC table을 네트워크 관리자가 구현할 수도 있다. PMS는 MAC 주소와 IP 주소로 구성되어 있고, PMS

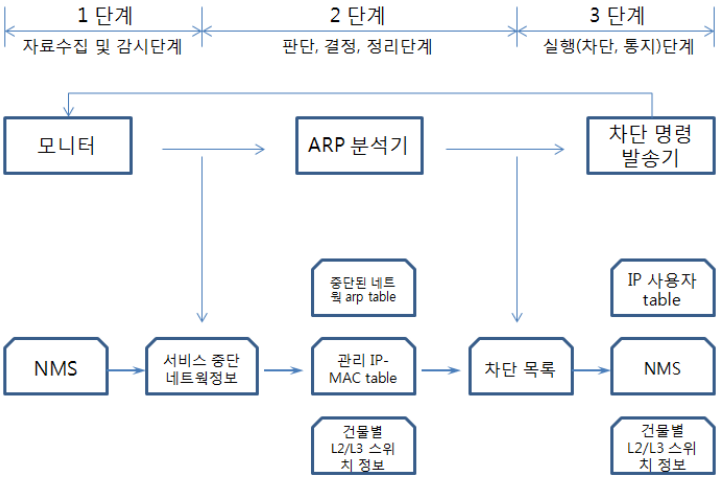


그림 5. 제안한 시스템에서 ARP spoofing 대응절차
Fig. 5 The proposed respond sequence for ARP spoofing attack

의 IP 주소에 대한 MAC 주소의 변경 여부도 알 수 있다. 사용자 정보 table은 계속해서 update되므로 MAC table의 IP 주소로 사용자 정보를 식별할 수 있다.

제안한 시스템에서 ARP spoofing에 대응하는 절차는 다음과 같다. 먼저 전산망 관리자는 ARP 분석기를 이용하여 ARP spoofing을 발생시킨 PC의 정확한 MAC 주소를 얻는다. 또한 기존의 사용관리 시스템에서 해당 MAC의 IP 정보 및 사용자 정보(전화번호, 사용자 이름, 사용위치 등)를 얻을 수 있다. 이러한 과정을 거쳐 ARP spoofing 공격은 인지하게 되면 전산망 관리자는 해당 컴퓨터를 사용하는 사용자에게 이 사실을 긴급연락 한다.

또한 ARP 분석기는 전산망접속 차단명령 발송기에 L2 스위치의 해당 port 차단하도록 지시한다. 만약 해당 MAC 주소를 사용하는 컴퓨터의 사용자 정보가 없을 경우 우선 해당 컴퓨터를 격리조치하여 다른 정상적인 사용자는 인터넷을 사용할 수 있도록 한다. 이는 ARP spoofing 바이러스가 해당 건물에 빠르게 확산될 것을 대비하여 즉시 감염된 PC의 고립화 및 분리가 필요하기 때문이다. 그리고 해당 건물에 백신을 원격으로 최신 버전으로 업데이트하고 바이러스 검사를 실시하고 해당 건물의 서비스 재개 여부를 판단한다.

차단명령 발송기는 802.11x를 지원하는 스위치에만 적용할 수 있고 건물별 L2/L3스위치 table의 SNMP (Simple Network Management Protocol)를 참조한다. 이 경우는 사전에 해당 스위치의 SNMP 값은 write 가능하게 조정해야한다. 차단할 port가 정해지면 차단명령 발송기로 port를 차단할 수 있도록 신호를 보낼 수 있다. 제안한 네트워크 관리시스템은 향후는 NAC(Network Access Control)과 연동하면 더 쉽게 구현할 수 있을 것이다.

ARP spoofing 바이러스는 L2 수준에서 감염되고 활동하는 바이러스로써 전산망 전염보다는 이동형 저장 매체인 USB를 매체로 주로 전파되고 있다. 따라서 보안업데이트, 최신 백신업데이트를 유효적절하게 수행한다면 예방할 수 있다. 그러나 실습실과 같은 공동의 사용공간에서 안전상의 이유로 하드보안관과 같은 보안장치가 설치되어 백신 및 보안업데이트가 정상적으로 이루어지지 않는 곳에 주로 발생하게 된다. 이러한 보안에 취약한 공간에서 발생한 바이러스 감염은 동일한 IP 주소 영역의 전산망에 속한 PC들의 전산망 서비스를 중단시키는 원인이 된다.

소극적인 방안으로 보안 업데이트에 취약한 공동실습실과 같은 장소에 설치된 PC를 위한 전산망을 최소화함은 물론 IP 주소를 재분배하는 대처방안을 고려해볼 수 있다. 이러한 접근은 해당 전산망에서 ARP spoofing과 같은 바이러스 사고 발생시 서비스가 중단되는 공간적 영역을 최소화함으로써 다른 정상적인 PC에게 피해를 줄일 수 있다.

## Ⅴ. 다른 접근방법과 비교분석

본 논문에서 제안한 ARP spoofing에 효율적으로 대처하기 위한 접근방법과 기존의 다른 방법과 차이점을 분석하면 다음과 같다. ARP spoofing 대응 영역에서 가장 널리 참조되고 있는 S-ARP[2]의 접근은 암호학적 구조를 이용하고 있다. 각 서브넷에서 CA를 기반으로 인증된 MAC 주소만을 관리, 유지한다. 따라서 예방적이고 근본적인 해결 방법으로 인식되는 반면에, 서브넷마다 CA를 추가 구축되어져야 하며, 기존의 프로토콜을 바꿔야하는 이유로 대규모 전산망에 적용하기 어려운 한계를 지닌다. 또한 전체 전산망에 적용되어야만 효과를 기대할 수 있다.

다른 방안으로 참고문헌[8]은 MAC 주소 신뢰성을 확보하는 접근에 기반하고 있다. 각 서브넷에 MAC 주소를 관리하는 MAC agent와 ARP table의 변조를 방지하는 client agent를 설치하여 신뢰할 수 있는 MAC 주소만은 유지하는 접근이다. 기존 프로토콜을 수정할 필요가 없으며 소규모 전산망에 쉽게 적용할 수 있는 장점에도 불구하고 전산망이 커지면 관리 대상 또한 급격하게 증가하게 되어 관리비용이 증가하는 단점이 지적되고 있다.

제안한 네트워크 관리시스템은 기존에 사용하고 있는 네트워크 관리시스템에 자동화 도구를 추가하는 공격에 대응하는 접근이다. 따라서 위에서 분석한 2가지 접근에 대비하여 상대적으로 전산망 규모와 상관없이 적용될 수 있는 확장성과 범용성을 갖는다. 그러나 ARP spoofing 공격이 발생한 이후에 대응하는 소극적인 접근 방법이다. 또한 감염된 PC를 발견하는 과정에서 전산망 및 보안에 관련된 경험과 지식이 대응의 품질에 큰 영향을 미치는 한계를 갖는다.

표 2. 다른 방법과 비교분석
Table. 2 A comparison with other methods

| 구분 | 장점 | 단점 |
|---|---|---|
| Secure ARP[2] | ◦ 근본적인 문제 해결을 위한 접근 기법임 | ◦ 기본 방법과 혼합 적용이 어려우며, 전제적인 적용을 전제로 함 |
| MAC관리 agent[8] | ◦ 소규모 망에 쉽게 적용할 수 있음 | ◦ 관리비용이 과다하며, 대규모 망에 부적합 |
| 제안 방법 | ◦ 망의 규모에 무관하며, 추가 장비, 비용이 없음 | ◦ 망관리 보안에 관한 지식이 요구되며, 소극적인 조치구조 임 |

표 2는 본 연구와 유사한 기존연구들을 비교분석한 결과가 제시하고 있다. 제안한 네트워크 관리시스템은 향후 IPv6, 무선랜, 다양한 mobile 단말(스마트폰, 아이패드 등 테블릿 PC, 노트북 등)을 고려하면 재설계되어야 할 것이다.

## Ⅵ. 결 론

인터넷이 정보공유의 수단으로 사용되는 한 계속해서 프로토콜 및 운영의 취약점에 의한 악의적인 공격은 진화하고 다양화될 것으로 예상된다. 따라서 ARP spoofing을 비롯한 컴퓨터 바이러스에 의한 전산망 서비스 중단 등의 폐해는 예방하거나 방지하는 것은 분명히 한계를 지닌다. 신뢰성을 갖는 ARP 테이블 유지를 위해서는 기존 ARP 프로토콜 변경 없이는 쉽게 해결되지 않을 것으로 예상된다. 본 논문에서는 기존의 네트워크 관리시스템에 자동화 도구를 추가하여 ARP spoofing에 감염된 PC를 식별하고 전산망에서 자동적으로 분리하는 시스템을 제안하였다. 이는 전산망 서비스의 중단 시간을 최소화함을 목적으로 하고 있다.

제안한 시스템은 공격에 대한 추후 대응을 중심으로 설계되어 본질적으로 수동적인 입장의 한계를 지닌다. 바이러스 감염을 방지하는 적극적인 수단과 제안한 시스템의 연결 방안에 대한 설계를 추가할 계획이다.

## 참고문헌

[1] 인터넷침해대응센터, 인터넷 침해사고 동향 분석 및 월보, http://www.krcert. or.kr

[2] D. Bruschi, A. Ornaghi, and E. Rosti, “S-ARP: a Secure Address Resolution Protocol,” Proc. on 19th Annual Computer Security Applications, pp. 66-74, Dec. 2003

[3] N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, “LAN Attack Detection using Discrete Event Systems,” ISA Transactions, vol. 50, no. 1, pp. 119-300, 2011

[4] 서우일, 박현민, 최병석, 박재현, "TCP Connection ARP Spoofing/Hijacking에 대한 탐지 및 추적에 대한 연구," 2000년도 정보통신산업진흥원 추계종합학술발표회 논문집
[5] 신윤호, 임광혁, 임을규, "TCP/IP환경에 기반한 SCADA 시스템의 ARP Spoofing 공격 가능성 연구," 한국사이버테러정보전학회, 정보보안논문지, 제9권, 제3호, pp. 9-17, 2009. 9
[6] G. Hao and G. Tao, "Principle of and Protection of man-in-the-middle Attack based on ARP Spoofing," Journal of Information Processing Systems, vol. 5, no. 3, pp. 131-134. Sept. 2009
[7] 서우석, 전문석, "통합보안정책 알고리즘 적용에 따른 최적화 방어 시스템 구축에 관한 연구," 한국정보보호학회 논문지, 제21권, 제4호, 2011. 8
[8] 홍승표, 오명진, 이수연, 이상준 "신뢰적인 ARP 테이블의 운영을 통한 ARP 스푸핑 공격에 대한 효율적인 방어 기법," 정보과학회 논문지: 컴퓨팅의 실제 및 레터, 제17권 제1호, pp. 26-30, 2011. 1
[9] V. Ramachandran and S. Nandi, "Detecting ARP Spoofing: An Active Technique," Proc. on ICISS, pp. 239-250, 2005
[10] 정인환, "자동노드 인식 기능을 갖는 ARP 스푸핑을 이용한 인터넷 차단기," 한국인터넷방송통신학회 논문지, 제11권, 제6호, pp. 93-106, 2011. 12
[11] 이승재, ARP Spoofing과 Network Sniffing 연동 공격의 탐지 및 추적에 관한 연구, 성균관대학교, 정보통신대학원, 석사학위논문, 2006
[12] 이보만, 박대우, "해외에서 Proxy Server를 연동한 우회적인 공격기법 연구," 한국해양정보통신학회 춘계학술대회 논문집, pp.432-435, 2011
[13] J. Koo, S. Ahn, Y. Lim, and Y. Mun, "Evaluation of Network Blocking Algorithm Based on ARP Spoofing and Its Application," LNCS 3481, pp. 177-186, 2005
[14] J. Bae, S. Ahn, and J. Chung, "Network Access Control and Management using ARP Spoofing in Various Windows Environment," Proc. on Information Science and Applications (ICISA), pp. 1-10, 2011

## 저자소개

**고봉구(Bong-koo Ko)**

1992년 2월 : 전북대학교 컴퓨터공학과 졸업
1999년 2월 : 전북대학교 컴퓨터공학과 석사
1999년 3월 ~ 현재 : 전북대학교 컴퓨터공학과 박사과정
※관심분야 : 컴퓨터통신, 보안, 무선네트워크

**정성종(Seung-jong Chung)**

1975년 2월 : 한양대학교 전기공학과 졸업
1981년 2월 : 휴스턴 대학교 전자공학과 석사
1988년 2월 : 충남대학교 전자공학과 박사
1985년 ~ 현재 : 전북대학교, IT정보공학과, 교수
※관심분야 : 인터넷 응용 기술, 지능공학

**조기환(Gi-hwan Cho)**

1985년 2월 : 전남대학교 계산통계학과 졸업
1987년 2월 : 서울대학교 계산통계학과 석사
1996년 2월 : Newcastle대학교 전산학과 박사
1987년 9월 ~ 1997년 8월 : 한국전자통신연구원, 선임연구원
1997년 9월 ~ 1999년 2월 : 목포대학교 컴퓨터과학과 전임강사
1999년 3월 ~ 현재 : 전북대학교 컴퓨터공학부 교수
※관심분야 : 이동컴퓨팅, 컴퓨터통신, 분산처리 시스템, 무선보안, 무선네트워크