https://doi.org/10.33778/kcsa.2019.19.3.003

BGP 보안을 위한 AS-PATH 식별 방법★

김 점 구*

요 약

인터넷 상의 사용자가 목적지 시스템으로 정보를 전송할 수 있도록 라우팅 정보를 서로 교환하여 라우팅 테이블을 생성하고 변화된 정보를 업데이트 해주는 라우팅 프로토콜 중 가장 중요한 프로토콜이 BGP 이다. 본 논문은 현재 사용되고 있는 BGPv4의 취약성을 이용하여 악의적인 공격과 네트워크 관리자의 실수로 발생할 수 있는 문제점을 사전에 차단하는 방법과 BGP의 대표적인 보안 취약점에 대한 공격기법인 AS-PATH 공격에 대한 실제 공격실험을 수행하여 공격기법들을 분석하고, AS-PATH 공격을 식별하는 알고리즘을 제안하였다

AS-PATH Authentication algorithm for BGP Security

Kim Jeom Goo*

ABSTRACT

BGP is the most important protocol among routing protocols that exchange routing information to create routing tables and update changed information so that users on the Internet can send information to destination systems. This paper analyzes how to prevent malicious attacks and problems caused by network administrator's mistakes by using vulnerabilities in BGPv4 that are currently used. We analyzed the attack methods by performing the actual attack experiment on the AS-PATH attack, which is the attack method for BGP's representative security vulnerability, and proposed the algorithm to identify the AS-PATH attack.

Key-words: Internet, BGP, router, AS-PATH, Vulnerability

접수일(2019년 8월 27일), 게재확정일(2019년 9월 21일)

★ 본 논문은 2018학년도 남서울대학교 교내연구비 지원에 의해서 연구되었음

* 남서울대학교 컴퓨터소프트웨어학과 교수

1. 서 론

인터넷 상의 사용자가 목적지 시스템으로 네트워크 정보를 전송할 수 있도록 라우팅 정보를 서로 교환하여 라우팅 테이블을 생성하고 변화된 정보를 업데이트 해주는 라우팅 프로토콜 중 가장 중요한 프로토콜이 BGP(Border Gateway Protocol) 이다[1].

BGP는 TCP/IP 네트워크에서 라우터들이 경로 정보를 주고받기 위한 프로토콜로 인터넷 서비스 사업자 및 대기업에서 주로 사용되며, 전 세계의 네트워크 장비들과 상호 연결되어 통신할 수 있도록 해 주는 역할을 한다. 현재 사용되고 있는 BGPv4에는 TCP/IP의 취약점으로 발생될 수 있는 많은 침해 문제점을 내포하고 있으며, BGPv4의 취약성을 이용하여 악의적인 공격과 네트워크 관리자의 실수로 발생할 수 있는 문제점을 사전에 차단하는 방법을 제시하고자 하였다[2].

이에 본 논문에서는 AS-PATH 공격에 대해 차단 및 예방을 위해, AS-PATH 식별 방법을 제안하고 제안된 알고리즘을 실험을 통하여 검증하고 AS-PATH 공격에 대한 문제점들의 해결 방안을 제시하고자 한다. 이는 BGPv4 프로토콜의 형식을 그대로 유지하면서 보다 안정적으로 사용하기 위한 것이다.

2. 관련연구

2.1 BGP 개요

BGP 연동이란 인터넷 데이터센터(IDC : Internet Data Center)에 분산된 서버들을 논리적으로 하나의 네트워크로 연결하는 것을 의미하며, IGP (Interior Gateway Protocol)인 EIGRP(Enhenced Interior Gateway Routing Protocol), OSPF(Open Shortest Path First) 프로토콜은 알고리즘에 따라 최적의 경로를 선택해 Local-RIB(Local Routing Information Base)에 인스톨 하지만, BGP는 Policy Routing 프로토콜로써 최적의 경로를 정의해 주어야 한다[17].

BGP의 최초버전은 1989년 6월 RFC 1105, “A Border Gateway Protocol”에서 발표되었다. 최초버전의 BGP는 주로 개념과 핵심 요소 그리고 동작 방식을 정의했으며 이후로 여러 번 개정되어 현재 사용되고 있는 BGP는 1995년 3월 RFC 1771에 규정된 프로토콜이다[1,23]. BGP는 많은 보안에 취약점들을 있다[6,7]. IGP 라우팅 프로토콜인 EIGRP, OSPF은 알고리즘에 따라 최적의 경로를 선택하여 Local-RIB에 인스톨 되지만 BGP은 Policy Routing 프로토콜로써 네트워크 관리자가 최적의 경로를 설정 해 주어야 하는 경우가 많다.

BGP를 이용하여 독자적인 경로를 설정하기 위해서는 자율 시스템(Autonomous System: AS) 이라는 것이 반드시 있어야 한다. BGP에서 사용되는 AS번호는 인터넷상에서 자신의 존재를 알리기 위한 하나의 공인 IP 주소와 같다. AS번호는 2Byte 형식으로 이루어져 있으며 AS번호도 공인 IP와 사설 IP처럼 사설 AS 와 공인 AS번호로 나누어져 있다. BGP에서 사용할 수 있는 AS번호는 “0~65,535”까지이며, 이중 “64,512~65,535”까지는 내부 네트워크에서 사용할 수 있는 사설 AS번호이다. 공인 AS번호를 사용하기 위해서는 “한국인터넷진흥원”을 통해 부여 받아야 한다.

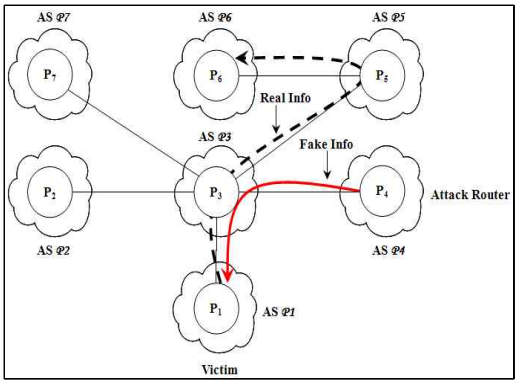
2.2 BGP 보안 위협

BGPv4는 1995년 RFC 1771에 규정된 이후 지금까지 사용되고 있으며 BGPv4는 여러 취약점을 가지고 있다. 이런 취약점을 이용해 악의적으로 공격할 경우 전 세계 IT 대란이 발생될 있으며 사례를 들면 2009년 7월 7일 7.7 DDoS(Distribute Denial of Service) 공격으로 인해 국내 12개 사이트와 해외 14개 사이트가 정상적인 서비스를 하지 못한 현상이 발생하기도 했다[40]. 이 방식은 이제까지 알려진 IRC(Internet Relay Chat) 서버를 통해 공격하지 않고 Zombie PC에 특정 파일을 심어 트래픽을 전송해 과부하 시킨 후 정상적인 서비스가 이루어지지 못하도록 한 것이다.

DDoS 공격은 주로 특정 시스템을 대상으로 이루어지며 장애 발생 시 해당 시스템만 정상적으로 동작하지 않는다. 하지만 BGP에 취약점을 이용해 공격할 경우 특정 시스템이 아닌 전 세계 IT 대란이 발생될 수 있다. BGP에서 가장 문제점으로 부각되고 있는 것이 AS-PATH, IP Hijacking, BGP Neighbor 공격이다[15].

2.2.1 BGP 공격

BGP는 Distance-Vector 방식을 이용하며, 이 방식을 Path-Vector라고도 부른다. Path는 AS-PATH를 의미하며, 목적지 네트워크까지 정보를 전송하기 위해 어떤 경로를 통해 전송할 수 있는지 의미한다. 또한 네이버 라우터로부터 수신한 네트워크 정보가 가짜(fake) 정보인지 BGP 라우터는 확인할 수 없으므로 문제가 될 수 있다. BGP 라우터는 네이버 라우터로부터 수신한 네트워크 정보를 최단 경로(shortest path)를 선택하기 위해 경로 속성을 비교하여 Local-RIB에 인스톨한다[4,5].



(그림 1) BGP Attack

(그림 1)에서 P_1라우터는 P_6라우터와 통신하기 위해 P_3라우터를 통해 이루어진다. 만약 P_4라우터가 P_6라우터에서 보유하고 있는 네트워크 정보를 Fake하여 전송할 경우 P_3라우터는 P_4와 P_6라우터로부터 수신한 정보를 경로 속성을 비교한 후 최단 경로 알고리즘을 이용해 선택한 후 Local-RIB에 인스톨하게 된다. 위와 같은 경우 Prefix Black holing이 발생하여 P_1과 P_6라우터는 정상적으로 통신이 이루어지지 못한다.

전 세계적으로 IT 산업이 발달되면서 보안에 문제점을 해결하려고 많은 노력을 하고 있지만 라우팅 프로토콜에 대한 문제점은 아직까지 크게 발표되지 않았다. 네트워크 공격은 악의적인 공격 외에도 네트워크 관리자에 실수 또는 네트워크 공부를 막 입문한 사람으로부터 주로 발생된다. 하지만, 라우팅 프로토콜의 핵심인 BGP의 취약점을 이용해 악의적으로 공격할 경우 속수무책으로 당할 수밖에 없다. BGP 공격으로 인해 발생 할 수 있는 유형으로는 Routing Instability, Traffic Redirection, Prefix Black holing, Traffic Delay 등이 있으며, 의미는 다음과 같다[15].

(1) Routing Instability : 특정 네트워크 정보에 대해서 추가 및 삭제 등을 반복적으로 하여 불안 한 네트워크 정보를 전송해 라우터에 성능을 저하시키는 방식이다.

(2) Traffic Redirection : Fake IP 주소를 생성해 다른 라우터에서 사용하고 있는 네트워크 정보를 마치 공격 라우터가 보유하고 있는 것처럼 생성 한 후 트래픽이 공격 라우터로 전송될 수 있도록 하기 위한 방식이다. 또한 특정 시스템으로 전송되는 정보를 우회시켜 개인 정보도 확인 할 수 있다.

(3) Prefix Black holing : 인터넷상에서 특정 시스템으로 전송되는 정보를 Drop 시키는 방법이다. IANA에서 규정되어 있는 사설 IP 주소를 이용해 공격하므로 실망에서는 기본적으로 사설 IP 주소를 차단하여 실망으로 들어오지 못하도록 필터링 하기 때문에 위협적이지 않다.

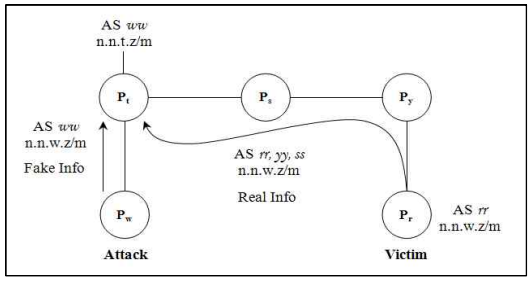
(4) Traffic Delay : 최단 경로 알고리즘 방식을 이용하지 못하고 긴 경로를 통해 전송될 수 있도록 하여 전체적인 통신 속도를 지연시키기 위한 것이다.

BGP가 취약점을 보유하고 있는 이유 중 하나는 구조적인 문제 때문이다. 즉 공격자로부터 BGP 메시지를 위·변조하여 공격할 수 있으며, BGP AS번호가 위조된 것을 BGP 라우터에서 확인 할 수 없기 때문이다. 결과적으로 BGP는 메시지에 의존하기 때문에 수신된 메시지가 잘못된 BGP 메시지인지 확인 할 수 있는 방법이 없으므로 보안에 취약하다[8].

2.2.2 AS-PATH

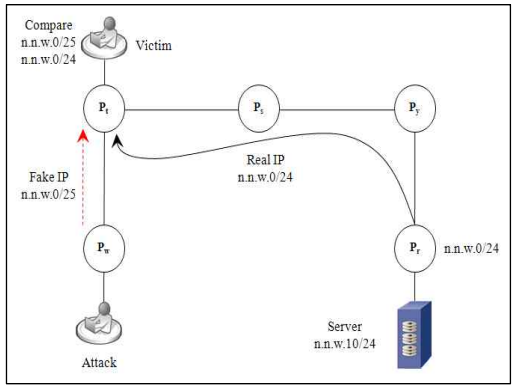
IP 주소는 인터넷상의 한 컴퓨터에서 다른 컴퓨터로 정보를 전송하고자 할 때 사용되는 프로토콜이다. BGP에서도 AS간의 상호연결을 통해 IP 주소를 서로 교환한다. 하지만 인터넷상에서 사용되고 있는 IP 주소를 다른 사용자가 사용할 경우 Collision이 발생된다. BGP는 인접한 라우터로부터 수신한 정보가 잘못된 정보인지 확인할 수 없으므로 수신한 네트워크 정보를 그대로 다른 네이버 라우터로 전송한다[3,13].

결과적으로 가짜 IP는 IP 주소를 속여 마치 자신이 사용하고 있는 것처럼 공격한다. 이러한 공격 행위를 IP Hijacking이라고 부른다. IP Hijacking은 고의적인 행위일 수도 있지만 대부분 네트워크 관리자의 실수로 빈번히 발생된다.



(그림 2) IP Hijacking

(그림 2)에서 P_r라우터는 자신의 네트워크 정보인 *n.n.w.z/m* 정보를 P_y,P_s를 통해 P_t라우터로 전송한다. 하지만 P_w라우터가 IP 주소를 위조하여 마치 *n.n.wz/m* 정보를 자신이 보유하고 있는 것처럼 생성해 P_t로 전송할 경우 P_t라우터는 두 라우터로부터 수신한 정보를 비교하여 S-PATH 길이가 짧은 경로를 선택해 Local-RIB에 인스톨한다. 위와 같은 경우 P_t라우터는 P_r라우터와 정상적인 통신이 이루어지지 못한다.



(그림 3) LPM을 이용한 공격 흐름

또한 LPM(Longest Prefix Match) 공격 방식을 이용해 정상적으로 통신이 이루어지지 못하도록 할 수 있다. LPM란 동일한 네트워크 정보를 수신할 경우 Subnet Mask를 비교해 긴 것을 우선적으로 선택하는 것을 의미한다[4].

(그림 3)에서 Pr라우터에 있는 Server IP 주소는 n.n.w.10이다. 하지만 라우터는 Host Route 네트워크 정보를 전송하지 않는다. Host Route란 Subnet Mask부분이 32Bit인 정보를 말한다. <그림 2-20>에서 Pt라우터에 존재하고 있는 Victim 사용자가 Server로 접속하기 위해 정보를 전송할 경우 n.n.w.0/24로 갈 수 있는 경로는 알고 있으므로 전송하게 된다. 하지만 Pw라우터가 위조된 IP 주소를 생성하여 n.n.w.0/25 네트워크 정보를 Pt라우터로 전송할 경우 Pr과 Pw네트워크 정보를 Local-RIB에 인스톨하게 된다.

위와 같은 경우 Pt 클라이언트 사용자가 Server 접속하기 위해 Pt 라우터에게 요청할 경우 Pt 라우터는 Local-RIB에 인스톨되어 있는 정보를 보고 Subnet Mask 길이가 긴 Pw라우터로 전송하지만 Pw라우터는 n.n.w.10을 보유하고 있지 않으므로 패킷을 Drop하게 됨으로 통신이 이루어지지 않는다.

2.2.3 AS-PATH 보안 취약점

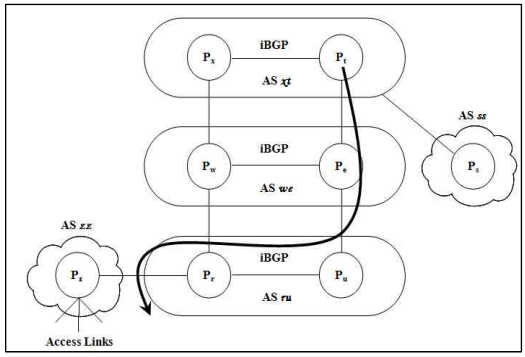
BGP를 사용해 독자적인 경로를 설정하기 위해서는 AS번호를 반드시 사용해야 하며, AS번호는 “Single Technical Administration”에 속한 Network Aggregation이다[28]. BGP AS번호는 국내에서는 “한국인터넷진흥원”으로부터 할당받아 사용하며, 공인 IP 주소와 이 AS번호를 다른 곳과 동일하게 사용할 경우 Collision이 발생한다. 이와 같은 경우 BGP를 통해 네이버 라우터로부터 수신한 네트워크 정보를 Local-RIB 인스톨하지 못하므로 정상적인 통신이 이루어지지 않는다.

위와 같은 취약점을 이용해 AS-PATH 공격이 이루어진다. AS-PATH는 목적지로 패킷을 전송할 때 거쳐야 할 경로를 나열하기 위한 것이다. 즉 eBGP 네이버 라우터로 네트워크 정보를 전송할 때 AS번호를 붙여 전송하게 되며 AS-PATH 길이가 짧은 경로를 선택해 Local-RIB에 인스톨한다. BGP AS번호를 붙여 전송하는 것은 Loop가 발생되지 않도록 하기 위한 것이며, 만약 수신된 네트워크 정보 중 자신의 AS번호가 존재할 경우 해당 정보를 Drop한다.

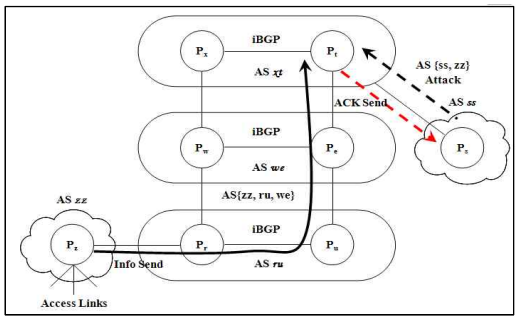
AS-PATH는 두 종류가 존재한다. AS_SEQUENCE와 AS_SET이며 AS_SEQUENCE 타입의 AS-PATH는 네트워크 경로를 통과한 AS번호들을 순차적으로 나열된 것이다. AS_SET 타입은 AS번호들이 무질서하게 나열된 것이며 MOAS(Multiple Origin Autonumous System)경로가 있을 때 만들어진다[22]. AS_SET은 인터넷에서 많이 사용되지 않는다. 예를 들면 2004년 8월 1일 기준으로 161,796중 47개를 AS_SET을 이용해 생성하였다[9].

(그림 4)에서 AS{xt}는 AS{zz}에 있는 시스템과 통신할 때 정상적인 경로가 AS{xt, we, ru} 경로를 통해 통신하게 된다. 만약 [그림 2]와 같이 Ps라우터가 AS{*xt*}로 AS-PATH 공격을 할 경우 정상적으로 통신이 이루어지지 않게 된다.

(그림 5)에서 AS{*ss*} 공격 라우터가 AS{*zz*}번호를 붙여 전송할 경우 AS{*xt*}는 P_s와 P_z로부터 수신한 정보를 보고 ShortestPath 알고리즘을 이용해 P_s 라우터로 정보가 전송될 수 있도록 Local-RIB에 인스톨한다. 위와 같은 경우 AS{*xt*}는 AS{*zz*}로 정보를 전송하기 위해 위조된 경로인 AS{*ss*}로 전송하며, AS{*ss*} 라우터는 AS{*zz*}와 AS{*xt*}간에 전송되는 정보를 확인한다.



(그림 4) 정상적인 AS-PATH



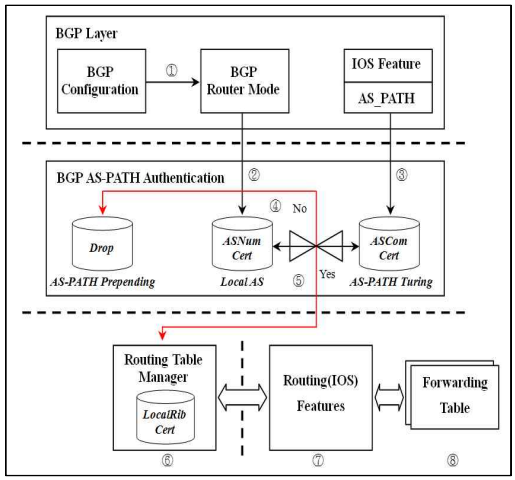
(그림 5) AS-PATH를 이용한 공격

3. AS-PATH 식별방법 제안

이미 설명한 바와 같이 BGP를 사용하기 위해서는 IANA로부터 반드시 AS번호를 할당 받아야 한다. BGP AS번호는 목적지 네트워크로 정보를 전송하기 위해 어떤 경로를 통해 도달할 수 있는지 표시하기 위한 것이다. 또한 BGP는 최적의 경로를 선택하기 위해 짧은 AS-PATH를 선택한다. 인접한 네트워크 장비로부터 수신한 네트워크 정보 중 자신에 AS번호가 있을 경우 해당 네트워크 정보를 폐기한다.

현업에서도 AS-PATH는 네트워크 경로를 조

율할 때 많이 사용한다. 하지만 관리자의 실수 또는 악의적으로 AS-PATH를 이용해 공격이 이루어질 경우 정상적으로 BGP 통신이 이루어지지 않는다. 본 논문에서 AS번호를 이용해 네트워크 경로를 조율할 때 IANA로부터 할당 받은 AS번호를 입력하지 않고 다른 AS번호를 이용해 "*AS-PATH Prepending*"을 이용해 이루어지지 못하도록 (그림 6)과 같이 인증한다.



(그림 6) AS-PATH Authentication

(1) BGP Configuration은 BGP를 사용하여 통신하기 위해 필요한 정보가 등록되어 있는 것을 의미한다.

(2) BGP Router Mode는 IANA로부터 할당 받은 AS번호가 설정되어 있는 정보를 BGP AS-PATH Authentication에 있는 "ASNumCert" 전송한다.

(3) IOS Feature에서 AS-PATH를 이용해 네트워크 경로를 조절하기 위해 사용한 BGP AS 번호를 "ASComCert"로 전송한다.

(4) BGP AS-PATH Authentication에서 "ASNumCert"와 "ASComCert"를 서로 비교하여 동일하지 않을 경우 IOS Feature에서 설정한 정보를 Drop한다.

(5) "ASNumCert"와 "ASComCert"를 서로 비교해 동일할 경우 BGP DB로 전송하여 네트워크 경로를 조절할 수 있도록 한다.

(6) Routing Table Manager(BGP DB)는 인접한 라우터로부터 수신한 BGP 정보를 BGP DB에 저장한 후 알고리즘을 사용해 최적의 경로를 선택해 Routing Table 인스톨된 정보이다.

(7) Routing (IOS) Features는 라우팅 테이블에 인스톨되어 있는 정보를 다른 네이버 라우터로 전송하기 전에 BGP 정책에 의해 필터링 한 정보를 처리하거나 다른 네이버 라우터로부터 수신한 정보 중 BGP 정책에 의해 필터링 한 정보만 수신하기 위한 것이다.

(8) 인접한 라우터로 수신한 정보를 Routing Table로 전송하기 위한 것과 Routing Table에 인스톨되어 있는 정보를 최종적으로 인접한 라우터로 전송하기 위한 것이다.

위 과정에서 $SC\ mCert$는 0 값을 가지며, (*ASNumCert-ASComCert*)의 결과 값이다. 이에 대한 알고리즘은 (그림 7)과 같다.

```
#define ASNumCert SYSTEM_INPUT_ASNumCert
// IANA 에서 부여받은 BPG AS 번호를 장비에 입력
char ASComCert = USER_INPUT_ASNumCert
// 네트워크 관리자가 경로조절을 위해 입력한 AS 번호
if (!CHECK_ASNumCert(ASComCert))
{
// ASNumCert 검사
  printf('You have entered an incorrect AS Number.');
  exit(0);
}
boolean CHECK_ASNumCert (ASComCert)
// ASNum 검사를 위한 비교 함수
{
 if ( ASNumCert !== ASComCert ) return 0;
 // AS 번호 비교검사 수행
else return 1;
}
```

(그림 7) AS-PATH Authentication algorithm

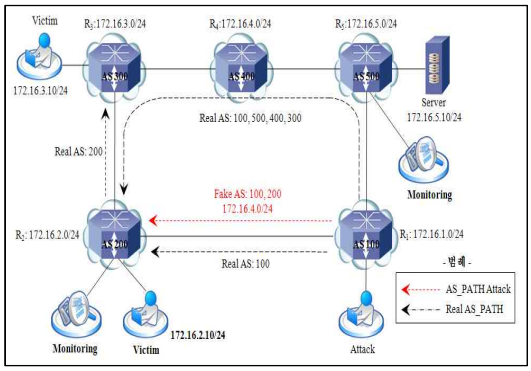
4. AS-PATH 식별방법

4.1 AS-PATH 실험 환경

AS-PATH 공격을 이용한 [그림 8] [실험 1]을 통해 AS-PATH 공격이 이루어지는 방식을

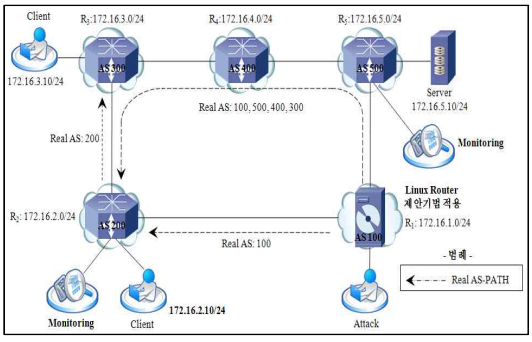
확인 할 수 있으며, [그림 9]의 [실험 2]는 제안기법을 적용하였을 때 공격 차단 효과를 확인하였다.

(그림 8)의 [실험 1]에서 R1 라우터가 R5 라우터의 네트워크 정보를 수신한 후 R2 라우터로 전송할 때 AS 200번을 추가한다.



(그림 8) [실험 1]의 환경 구성도

그 외 나머지 라우터들은 정상적으로 BGP을 통해 네트워크 정보를 송·수신하며 R2 라우터의 Monitoring은 R1 라우터에서 AS 200을 추가한 후 R5 네트워크 정보를 전송할 때 위조된 AS-PATH를 분석하기 위한 것이다. R5 라우터의 Monitoring은 R2 라우터가 정보를 요청할 경우 R5 라우터가 어떤 경로를 통해 응답 패킷을 전송하는 것을 확인하기 위한 것이다.



(그림 9) [실험 2]의 환경 구성도

(그림 9) [실험 2]의 구성도는 Linux Router에 제안기법을 적용한 알고리즘으로 구현된 장비이다. 일반 라우터와 LA-BGP를 적용한 라우터 비교를 통해 얼마나 효율적인 탐지 효과가 나타나는지 확인하기 위한 실험이다.

4.2 AS-PATH 공격 실험 및 분석

[그림 8] [실험 1]은 MOAS 방식을 사용하고 있으며, R1 라우터가 R5 네트워크 정보에 대해서만 R2 라우터로 전송할 때 AS 200번을 추가해 전송할 경우 R2 라우터는 자신에 AS번호가 있는 것을 확인하여 R5 네트워크 정보를 [그림 10]과 같이 Drop하는 것을 확인 할 수 있었다.

R2 라우터는 (그림 10)과 같이 172.16.5.0/24 네트워크 정보를 삭제함으로 R3 라우터에서 전송해 준 172.16.5.0/24 네트워크 정보를 선택해 라우팅 테이블에 인스톨되는 것을 (그림 11)과 같이 확인하였다.

```
// R2 BGP Neighbor Message
// R1 라우터에서 R2 라우터로 BGPv4로 Message 전송.
BGP: 10.10.12.1 send message type 4, length (incl. header) 19
// R1 라우터에서 보낸 BGP 업데이트 정보 및 BGP Attribute.
BGP(0): 10.10.12.1 rcv UPDATE w/ attr: nexthop 10.10.12.1, origi
n i, originator 0.0.0.0, path 100 200 400, community , extended co
mmunity
// R1 라우터에서 업데이트한 BGP Attribute에 172.16.5.0/24 네트
워크 정보에 대해서 R2 라우터에 AS-PATH 정보가 있는 것을 확
인한 후 해당 정보를 삭제 Message.
BGP(0): 10.10.12.1 rcv UPDATE about 172.16.5.0/24 -- DENIE
D due to: AS-PATH contains our own AS;
```

(그림 10) UPDATE Drop

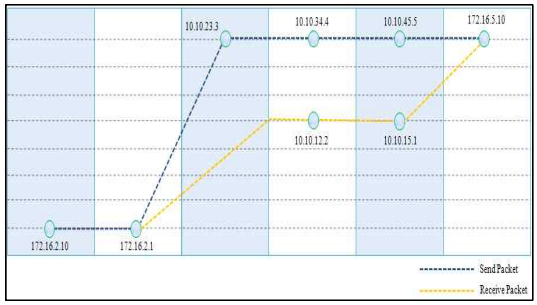
```
// R2 Routing Table
     172.16.0.0/24 is subnetted, 3 subnets
// R1 라우터로부터 수신한 네트워크 정보.
B        172.16.1.0 [20/0] via 10.10.12.1, 00:18:32
// R3 라우터로부터 수신한 R4 네트워크 정보.
B        172.16.4.0 [20/0] via 10.10.23.3, 00:01:02
// R3 라우터로부터 수신한 R5 네트워크 정보.
B        172.16.5.0 [20/0] via 10.10.23.3, 00:01:39
// R3 라우터로부터 수신한 네트워크 정보.
B        172.16.3.0 [20/0] via 10.10.23.3, 00:02:46
```

(그림 11) R2 Routing Table

R5 라우터는 R1 라우터가 172.16.5.0/24 네트워크 정보를 R2 라우터로 전송할 때 R2 라우터에서 사용하고 있는 AS 200번을 추가하여 전송할 때 필터링을 통해 R2 라우터로만 전송했기 때문에 알지 못한다. 그리고 R2 라우터에 BGP 데이터베이스 테이블을 확인한 결과 R2 라우터가 172.16.5.0/24 라우터로 전송하기 위해서는 AS-PATH 길이가 긴 곳을 선택하는 것을 (그림 12)와 같이 확인 할 수 있었다. 위와 같은 현상은 R1 라우터로부터 수신한 172.16.5.0/24 네트워크 정보를 R2 라우터가 삭제했기 때문에 R3 라우터로부터 수신한 정보를 선택한 것을 확인 할 수 있었다.

```
// R2 라우터에 BGP 데이터 베이스
BGP table version is 6, local router ID is 172.16.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.1.0/24    10.10.12.1               0    0      100 i
*> 172.16.2.0/24    0.0.0.0                  0    32768      i
*> 172.16.3.0/24    10.10.23.3               0    0      300 i
*> 172.16.4.0/24    10.10.23.3               0    0      300 400 i
*> 172.16.5.0/24    10.10.23.3               0    0      300 400 500 i
```

(그림 12) R2 BGP Database

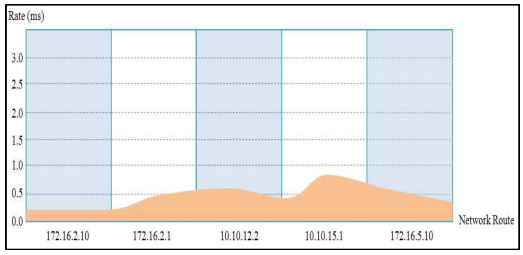


(그림 13) Roundabout Network Route

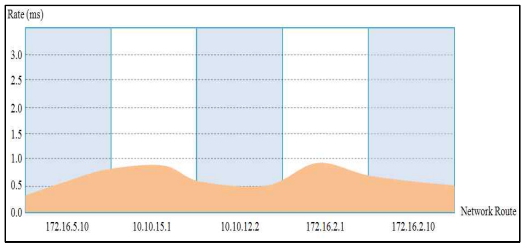
(그림 13) 네트워크 경로를 통해 R2 라우터에서 R5 라우터에 있는 서버로 접속을 정보를 전송한 결과 R5 라우터는 R2 라우터로 응답 패킷을 전송할 때 R4 라우터로 전송하지 않고 R1 라우터로 전송하는 것을 R2 Monitoring을 통해 같이 확인 할 수 있었다. (그림 14)를 보면 R5 라우터에 인스톨되어 있는 정보를 확인해 보면 172.16.2.0/24로 전송하기 위해서는 R1 라우터로 전송한다는 것을 확인 할 수 있었다.

```
// R5 Routing Table
     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.5.0 is directly connected, GigabitEthernet0/0
// R1 라우터로부터 수신한 네트워크 정보.
B       172.16.1.0 [20/0] via 10.10.14.1, 01:21:25
// R1 라우터로부터 수신한 R2 네트워크 정보.
B       172.16.2.0 [20/0] via 10.10.14.1, 00:21:45
// R4 라우터로부터 수신한 R3 네트워크 정보.
B       172.16.3.0 [20/0] via 10.10.45.4, 00:04:14
// R4 라우터로부터 수신한 네트워크 정보.
B       172.16.4.0 [20/0] via 10.10.45.4, 00:04:14
```

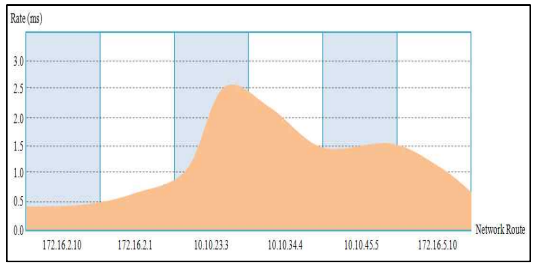
(그림 14) 공격 전 R2 전송속도



(그림 15) R5 Routing Table

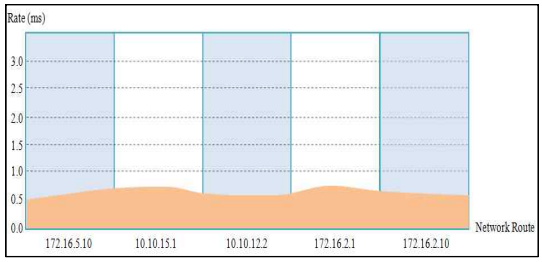


(그림 16) 공격 전 R5 응답속도



(그림 17) 공격 후 R2 전송속도

(그림 14)와 같은 경우 처리속도에 대해서 (그림 15)와 (그림 16)을 통해 정상적인 처리속도이며, (그림 17)과 (그림 18)은 비정상적인 처리속도를 확인 할 수 있었다.



(그림 18) 공격 후 R5 응답속도

5. 결 론

초기 라우팅 프로토콜을 연구할 때 보안성보다는 보다 효율적으로 정보를 주고받을 수 있는가에 중점을 두고 설계 되었지만, 시대의 변화에 따른 보안상 취약점의 노출로 인해 많은 피해가 발생되고 있다. 이러한 문제들은 라우팅 프로토콜뿐만 아니라 모든 IT 산업전반에 걸쳐 문제가 되고 있다.

BGP의 문제점을 보완하기 위해 개선방안을 연구한 기존 여러 논문들이 발표되었지만 모두 인증체계의 방식으로 이루어져 있으므로 추가 비용이 발생되고 또한 새로운 BGP 메시지 형식을 이용하기 때문에 현재 사용되고 있는 BGP와 호환성 문제가 있어 당장 적용하기 힘들다고 볼 수 있다. 하지만 본 논문에서 제시한 Local Authentication 기법을 적용한 별도의 인증체계와 추가적인 비용 없이 AS-PATH 공격을 효과적으로 차단되는 것을 실험을 통해 확인하였다.

참고문헌

[1] Paul Watson, "Slipping In The window: TCP Reset Attacks", CanSecWest conference, 2014

[2] R White, "Securing BGP through secure origin BGP (soBGP)", BUSINESS COMMUNICATIONS REVIEW, 2013

[3] E, Kranakis, P.C. van Oorschot, and Tao Wan, “Security Issues in the Border Gateway Protocol (BGP)” , Technical Report 05-07, Carleton University, Ottawa, Canada, Mar. 19, 2005.

[4] O. Nordstrom, C. Dovrolis, “Beware of BGP Attacks”, ACM SIGCOMM Computer Communications Review, Vol 34, No 2, April 2014.

[5] S. Kent, C. Lynn, and K. Seo, “Secure Border Gateway Protocol (Secure-BGP)”, IEEE Journal on Selected Areas in Communications (JSAC), Vol. 18, No. 4, Apr. 2010, pp. 582-592.

[6] Yih-Chun Hu , Adrian Perrig , Marvin Sirbu, "SPV: secure path vector routing for securing BGP", In Proc. of ACM SIGCOMM Internet Measurement Workshop, August 30-September 03, 2004, Portland, Oregon, USA

[7] James Ng, “Extensions to BGP to Support Secure Origin BGP (soBGP)”, Internet Draft, draft-ngsobgp-bgp-extensions-01, June 2003.

[8] R White, "Securing BGP through secure origin BGP (soBGP)", BUSINESS COMMUNICATIONS REVIEW, 2003

[9] J. Karlin, J. Karlin, S. Forrest, and J. Rexford, “Pretty Good BGP: Improving BGP by Cautiously Adopting Routes”, In Proc. of the 2006 IEEE International Conference on Network Protocols (ICNP), Santa Barbara, CA, USA, Nov. 12-15, 2006, pp. 290-299.

[10] S. Gibson, DRDoS(Distributed Reflection Denial of Service), Gibson Research Corporation, Feb 22 nd, 2012

[11] Selma Yilmaz, “An adaptive policy management

approach to BGP convergence" , Boston University Graduate school of Arts and Science Docter of Philosophy , 2016

[12] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, Jan. 2016.

[13] T. Wan, E. Kranakis, P. van Oorschot, "Pretty secure BGP(psBGP)", In Proc. NDSS (2005)

[14] 윤종호, "라우터와 라우팅 프로토콜", 교학사, 2003

[15] 김점구 "안전한 BGP를 위한 Fakr IP 식별방법", 한꾸차세대컴퓨팅학회 논문지, 2018

[16] http://www.zdnet.co.kr/ArticleView.asp?artice_id=20090729112938

[17] http://www.juniper.net/techpubs/software/erx/erx50x/swconfig-routing-vol2/html/bgp-config9.html

〔저자소개〕

김 점 구 (Jeom Goo Kim)
1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장
email : jgoo@nsu.ac.kr