Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.147

IP 스푸핑을 통한 DDoS 공격 탐지 방안에 대한 연구

서 정 우,† 이 상 진‡
고려대학교

A study on the detection of DDoS attack using the IP Spoofing

Jung-woo Seo,† Sang-jin Lee‡
Korea University

요 약

서비스거부공격은 여전히 많은 웹 서비스 사이트에서 중요한 취약 요소이기에 공공기관을 포함한 사이트에서는 방어 체계 구축에 많은 노력을 기울여야 한다. 최근에는 NTP의 monlist 기능을 이용한 대량의 네트워크 트래픽을 유발시켜 분산 서비스 거부 공격을 일으키거나 직접적인 방어가 불가능한 DNS 인프라에 대한 서비스거부 공격 등 형태로 이동하고 있다. 일례로 2013년 6월에 발생한 정부통합전산센터 DNS 서버를 대상으로 발생한 DNS 어플리케이션 서비스거부공격은 공공기관의 정보시스템들에 대한 정상적 서비스를 불가능하게 하는 것이 목적이었다. 이와 같이 분산 서비스거부공격은 특정 정보시스템에 대한 피해 뿐 아니라, 불특정 정보서비스에 대한 광범위한 피해로 이어질 수 있기 때문에 사이버위협을 최소화 하는 노력을 기울여야 한다. 본 논문에서는 해외정보시스템과 국내정보시스템 사이에 정해진 규약에 의해 자료를 전송하는 경우에 발생하는 IP 스푸핑을 통한 DDoS 공격에 대해 IP 헤더의 TTL(Time To Live) 값을 활용하여 스푸핑 여부를 탐지하는 방법을 제안한다.

ABSTRACT

Since the DoS(Denial of Service) attack is still an important vulnerable element in many web service sites, sites including public institution should try their best in constructing defensive systems. Recently, DDoS(Distributed Denial of Service) has been raised by prompting mass network traffic that uses NTP's monlist function or DoS attack has been made related to the DNS infrastructure which is impossible for direct defense. For instance, in June 2013, there has been an outbreak of an infringement accident where Computing and Information Agency was the target. There was a DNS application DoS attack which made the public institution's Information System impossible to run its normal services. Like this, since there is a high possibility in having an extensive damage due to the characteristics of DDoS in attacking unspecific information service and not being limited to a particular information system, efforts have to be made in order to minimize cyber threats. This thesis proposes a method for using TTL (Time To Live) value in IP header to detect DDoS attack with IP spoofing, which occurs when data is transmitted under the agreed regulation between the international and domestic information system.

Keywords: DDoS, IP Spoofing, Vulnerablilty, HCF

I. 서 론

인터넷 기본 프로토콜인 IP(Internet Protocol)는 생존성을 극대화하기 위해 가변적 망 경로에 따라 라우팅 되도록 구성되어 있으며, 출발지 혹은 목적지에서 양 구간의 경로를 확정하여 전송하지 않는 구조

접수일(2014년 11월 24일), 수정일(1차: 2014년 12월 29일, 2차: 2015년 1월 14일), 게재확정일(2015년 1월 22일)

† 주저자, korea002@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

이다. 그러므로, 송신자가 자신의 IP 주소를 변조하여 전송하는 경우 목적지에서 송신자의 실제 IP 주소를 추적하기 매우 어려운 구조로 설계되어 있다. 인터넷이 상호 신뢰를 기반으로 하는 소수의 연구자들 간의 실험망으로 존재하던 초기에는 큰 문제가 되지 않았으나, 상업적인 통신 환경이 활성화된 이후에는 이러한 취약점을 이용한 다수의 공격행위로 인해 경제적·사회적 손실이 발생하게 되었다.

서비스거부공격에서 출발지란 DDoS 공격에 사용되는 공격자의 컴퓨터 자원을 나타내며, 이는 크게 공격자가 직접 운용하는 경우와 봇넷(Botnet) 등을 구성하여 원격조정을 통해 집합적인 공격자원을 운용하는 경우로 나누어진다. 이때, DDoS 공격에서 스푸핑을 하지 않으면 좀비 목록을 알 수 있기 때문에 공격자는 IP 스푸핑을 통한 서비스거부공격을 수행한다. 서비스거부공격 대응을 위한 기술적인 관점에서는 공격에 사용된 자원의 소유자 보다는 해당 자원에서 위조된 패킷 생성을 통한 서비스거부공격 발생을 억제할 수 있는 방안에 대한 기술적 접근이 필요하다[1,2].

실제로 허위 트래픽 탐지 기법에 대한 다양한 연구가 수행되어 왔으며, 일부 연구결과는 운영환경에서 적용 가능한 모델들로 제시되었다. IP 스푸핑을 통한 서비스공격 탐지 기법에 대한 대표적인 연구 모델은 IP traceback, SPM, StackPi, Bogon Filtering, uRPF, TCP Intercept, HCF 등이 있다. 특히, HCF(Hop Count Filtering) 기법은 패킷 전송 시 IP 헤더 필드에 존재하는 TTL(Time To Live) 값의 적절성을 검사하는 방법을 이용하여 허위 패킷을 탐지하는 방안을 제시하였다. HCF는 Raw Socket을 이용한 허위 패킷 생성을 통해 Source IP 및 TTL 값들의 변조가 가능하다는 이론적 바탕에 근거하여 연구를 수행하였다[1,2,5]. 하지만, HCF는 참조 테이블 구성에 대한 명확한 방법론 및 테스트 결과를 제시하고 있지 않아 본 논문에서는 참조테이블 구성 방법 및 테스트 결과를 함께 제시하고자 한다.

기존의 연구 결과를 실제 운영환경에 적용하기 위해서는 정보인프라에 대한 물리적·논리적 환경을 별도로 구축해야 하지만, 본 논문에서 제안된 연구는 HCF의 연구 기법을 기반으로 인터넷 환경에서 적용 가능한 IP 스푸핑 서비스거부 공격 탐지 방안을 제안한다.

II. 관련연구

2.1 IP 스푸핑 탐지 기법 연구 동향

최근 서비스거부공격에 대한 방어수준이 많이 향상되었으며, 웹 서버를 공격대상으로 하는 서비스거부공격은 큰 효과를 거두지 못하고 있다. 이에 따라 공격자는 웹 서버에 대한 서비스거부공격 대신에 직접적인 방어가 어려운 DNS나 NTP 등에 대한 서비스거부공격을 수행함으로 이에 대한 효과적인 공격대응체계 구축이 필요하다.

IP 스푸핑에 의한 서비스거부 공격 탐지 기법에 대한 많은 연구들이 수행되어 왔으며, 대표적인 탐지 기법으로 PPM(Probabilistic Packet Marking), SPM(Spoofing Prevention Method), StackPi, HCF(Hop Count Filtering), IP Traceback 등이 있다[1,2]. 하지만, 이들 탐지 기법은 실제 운영 환경에 적용할 경우 전체 네트워크 패스를 재구성하는 것이 어려우며, 인터넷 통신망의 라우터 사용을 위한 ISP 사업자의 협조를 받는 것도 쉽지 않다. 그리고 본 논문의 참조모델인 HCF(Hop Count Filtering)의 경우 스푸핑된 IP 주소의 탐지를 위한 Hop-count를 비교할 수 있는 참조테이블 구성 방법을 명확히 제시하고 있지 않다.(2.2절 참조) 실제 운영 중인 웹 서비스 환경에서 HCF 탐지 기법을 사용하기 위해서는 IP 스푸핑 여부를 비교 분석할 수 있는 참조테이블 구성이 필수 조건이다. 즉, 기존 연구에서 구체적으로 다뤄진 적이 없는 참조테이블 구성 방안을 본 논문에서 명확히 제시함으로서 IP 스푸핑을 통한 서비스거부공격을 효과적으로 탐지·차단하는 방안을 제시한다.

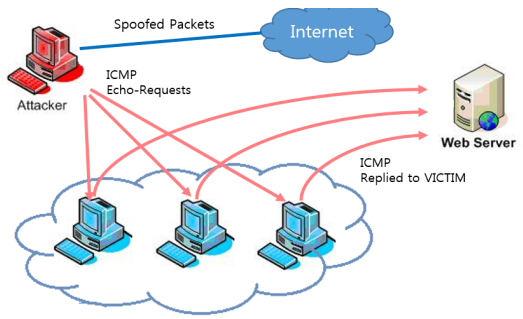

Fig. 1. Victim of DDoS(Distributed Denial of Service) attacks

2.2 HCF(Hop Count Filtering)

최근 HCF(Hop Count Filtering)는 패킷 전송 시 IP 헤더 필드에 존재하는 TTL(Time To Live) 값의 적절성을 검사하는 방법을 사용한다. 인터넷에서 패킷 정보는 목적지에 도달하기 위해서 각 라우터를 지날 때마다 TTL 값이 1씩 감소하게 된다. 이와 같이 IP-to-hop-count(IP2HC) 매핑 테이블을 구성하여 공격자에 의해 변조된 허위 IP 주소에 의한 서비스 거부 공격을 탐지하는 방법에 대하여 연구되었다[1,3,4].

MS Windows, Linux, Unix와 같은 OS들은 초기 TTL 값(30, 32, 60, 64, 128, 255)을 사용한다. 예를 들어, 최종 목적지의 TTL 값이 112 이라면, 초기 TTL 값은 128이 된다. 만약 IP 주소를 Spoofing한 DDoS 공격이 발생할 경우 비정상적인 초기 TTL 값을 가지는 패킷이 목적지 네트워크에서 탐지된다.

```
for each packet:
  extract the final TTL T_f and the source IP address S;
  infer the initial TTL T_i;
  compute the hop-count H_c = T_i − T_f;
  index S to get the stored hop-count H_s;
  if   (H_c ≠ H_s)
       the packet is spoofed;
  else
       the packet is legitimate;
```

Fig. 2. Hop-count inspection algorithm

2.3 패킷 마킹 기술

확률적 패킷마킹 기술은 위장된 패킷에 대해 원래의 패킷 전송 경로를 파악하기 위해 IP 계층을 중심으로 네트워크상에 전송되는 패킷에 대해 라우터에서 IP 패킷에 라우터 자신을 거쳐서 전달되었다는 정보를 삽입하는 방식이다. 즉, 인터넷을 통해 전달되는 패킷에 대해 라우터는 IP 계층을 중심으로 패킷 헤더 정보를 확인하여 라우팅하게 되는데 이때, IP 헤더의 변형 가능한 필드에 해당 라우터의 주소 정보를 마킹하여 다음 라우터로 전달하는 기법이다.

IP 헤더의 16비트 ID 필드에 라우터 자신의 IP 주소정보를 삽입할 수 있다. 각 라우터에서 삽입된 정보는 다시 다음 라우터로 전달되고 최종적으로 목적지 공격대상 시스템에 전달된다. 각 라우터에서 마킹된 정보가 전달되면 추후에 해킹 공격이 발생하였을 경우, 해킹 공격에 해당하는 패킷에 기록된 라우터 정보를 재구성하여 실제적인 패킷의 전달 경로를 재구성한다.

라우터에서 전달된 정보를 마킹하는 과정에서 모든 패킷에 마킹하게 되면 전체네트워크의 지연 현상이 발생하기 때문에 일반적으로 라우터에서는 확률 p로 패킷을 샘플링하여 마킹하게 된다. 이때 라우터에서 마킹하는 정보의 구성에 따라 노드 샘플링, 에지 샘플링 및 개선된 패킷 마킹기법 등이 제시된다.

노드 추가 기법은 라우터의 정보를 패킷에 순차적으로 추가시키는 기법으로서 라우터의 오버헤드, 패킷 경로 불확실성에 의한 저장 공간, 단편화 등을 초래할 수 있다. 노드 샘플링 기법은 패킷 경로를 샘플링하여 기록하는 방법으로서 라우터는 확률 값을 이용하여 IP 헤더에 경로정보를 마킹한다.

에지 샘플링 기법은 거리필드와 라우터의 IP 주소를 표현하기 위하여 출발주소 필드와 목적지주소 필드가 필요하다. 라우터가 패킷에 마킹을 수행하게 되면 출발주소 필드에 라우터 자신의 IP 주소를 기록하고 거리필드 값은 제로 값을 기록한다[3,5].

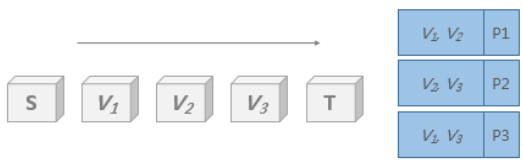

Fig. 3. Probabilistic packet marking

III. 참조테이블 설계

참조테이블 구성 방안은 실시간 웹 서비스를 제공하는 웹 서버로부터 IP 주소를 추출하고, 추출된 IP 주소를 목적지로 설정하여 Hop-count를 역으로 추적하여 계산하는 방식이다. 출발지 주소에서 목적지 주소까지 Hop-count는 N회에 걸쳐 수행한 후 평균값을 계산하여 기록하고, 목적지 IP 주소를 포함하는 IP 대역을 함께 참조테이블에 저장하고 Hop-count를 기록한다.

참조테이블은 IP 스푸핑 여부를 판단하는 핵심적인 기능을 담당하고 있으며, 등록된 IP 주소의 Hop-count가 많을수록 스푸핑된 DDoS 공격 탐지 결과의 정확성은 향상된다.

3.1 참조테이블 구성

실시간으로 수집되는 네트워크 트래픽에 대한 허위 IP 주소를 판단하기 위해서 참조테이블을 사용하게 되는데, 사용자 IP 주소를 추출하기 위한 절차로서 네트워크 장비(라우터)에 미러링 포트를 구성한 후 추출된 IP 정보를 사용하여 Hop-count 계산한다. Fig. 4는 Hop-count 계산 알고리즘이다.

참조테이블 HC(Hop-count) 값은 총 3회에 걸쳐 trace route를 수행하고, 최소값과 최대값에 대한 평균값을 기록한 후 inetnum object 정보를 함께 저장한다.

참조테이블 = {IP address, HC*, Country, inetnum object**}

$$* \text{ HC(Hop Count)} = \frac{1}{N}\sum_{i=1}^{3} \text{Hi} \qquad (1)$$

** inetnum object: 할당된 IP 대역

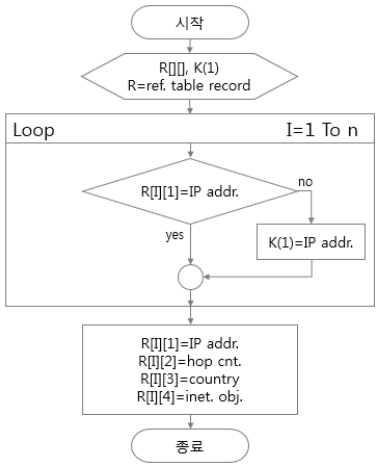

Fig. 4. Algorithm for configuration of reference table

3.1.1 전처리 작업

웹 서비스에 접근하는 네트워크 트래픽 정보를 분석하기 위해 라우터 장비에 미러링 포트를 구성한 후 트래픽분석 시스템을 사용하여 패킷정보 수집 및 분석 작업을 수행하였다. 그리고 트래픽분석 시스템에서 수집된 패킷 정보에서 사용자 IP 주소와 TTL(Time to Live) 값을 추출하여 참조테이블과 IP 스푸핑 여부를 체크한다.

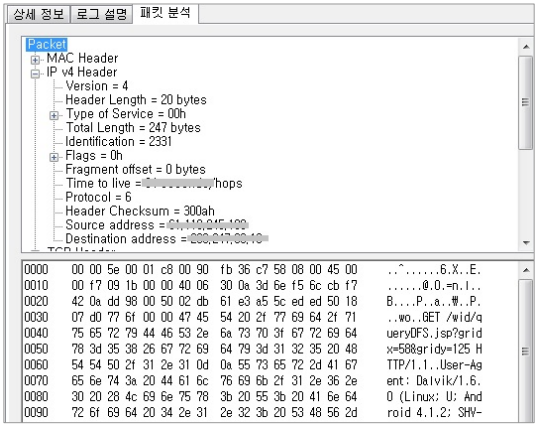

Fig. 5. Information of hop count about IP address

3.1.1 Hop-count 계산

Hop-count 계산을 위해 전처리 작업에서 추출된 IP 주소를 목적지로 설정하여 Trace route를 수행한다. 목적지까지의 Hop count를 총 3회에 걸쳐 수행하고 평균값을 참조테이블에 기록한다. 만약 보안장비나 ICMP 패킷 차단 등으로 목적지까지 Hop-count를 계산하지 못할 경우에는 해당 보안장비나 네트워크 장비까지의 Hop-count를 참조한다. 대부분의 기업에서는 외부 네트워크와 연결된 DMZ 구간에 보안장비나 라우터에서 ICMP 패킷을 차단하기 때문에 해당 영역까지의 Hop-count를 참조하여 사용한다.

```
Extract user ip address in Traffic Analysis System;
if reference_table don't include user ip address;
do
 Compute hop-count from source to destination;
 Compute inetnum object using WHOIS API;
 i++;
while(i < 3)
```

Fig. 6. Computation of the hop-count

3.1.2 inetnum object 추출

웹 참조테이블 구성을 위한 사용자 IP를 수집하는

것은 실제 웹 서비스 운영환경에서는 한계가 존재한다. 그러므로 이를 해결하기 위한 대안으로서 IP 주소 관리기관에서 할당한 IP 대역 중 전처리 과정에서 추출된 IP 주소를 포함하는 주소 대역을 활용하여 참조 테이블을 구성한다.

inetnum object의 추출방법은 WHOIS API를 활용하여 추출하며, inetnum object는 IP 스푸핑이 의심되는 경우에 동일 대역의 유사 IP 주소의 Hop-count를 비교 분석하여 정확도를 높이는데 사용된다.

```
NetRange:       140.172.[redacted]- 140.172[redacted]
CIDR:           140.172[redacted]/16
OriginAS:
NetName:        NOAA-BOULDER
NetHandle:      NET-140-172-0-0-1
Parent:         NET-140-0-0-0-0
NetType:        Direct Assignment
RegDate:        1990-05-08
Updated:        2000-12-20
Ref:            http://whois.arin.net/rest/net/NET-140-172-0-0-1
```

Fig. 7. Extraction of inetnum object using the WHOIS API

3.2 스푸핑 IP 주소 차단

DDoS 공격이 의심되는 패킷이 관제 모니터링 시스템에서 탐지될 경우 Fig. 8과 같은 알고리즘을 활용하여 IP 스푸핑 탐지 및 차단을 수행한다.

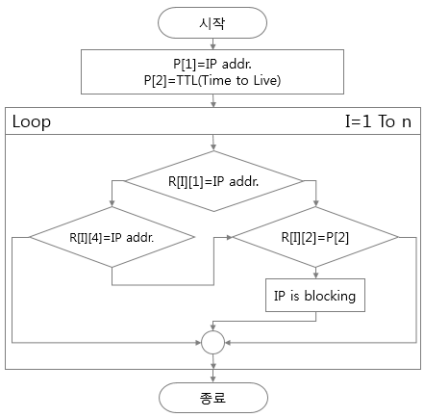

Fig. 8. Blocking of spoofed IP address

IV. 실험 결과

4.1 참조테이블 생성

IP 주소의 Spoofing 여부를 확인하기 위해 웹 서비스 영역으로 향하는 IP 헤더의 hop 수를 확인해야 하며, 참조 테이블에서 구성한 동일 IP의 hop-count 정보나 동일 IP 대역의 hop-count 정보를 비교 분석하여 판별한다. Table 1은 테스트 환경에서 수집된 IP 주소에 대한 정상적인 Hop-count를 계산한 참조 테이블 구성 정보의 일부를 나타낸다. 테이블의 필드 정보는 Hop-count를 계산할 IP 주소, Hop-count, 조직, 국가, inetnum object를 나타낸다.

Table 1. Configuration of reference table

IP addr	Hop count	Org	Country	inetnum object
128.104.x.x	17	University of Wisconsin	US	128.104.0.0
140.172.x.x	17	National Oceanic and Atmospheric Administration	US	140.172.0.0
210.98.x.x	14	Economy Cooperation Agency	KR	210.98.0.0
112.216.x.x	13	ISP assignment	KR	112.223.0.0
• • •				

4.2 실험 환경

참조테이블을 활용하여 IP 주소의 Spoofing 여부를 탐지하기 위해 Fig. 9.과 같은 웹 서비스 운영환경에서 테스트를 수행하였다. 테스트 환경은 해외 대학 및 국제기구와 자료를 교환을 위해 외부 자료공유 FTP 서버를 사용하여 DDoS 공격 서버로 활용하였다.

Spoofing된 아이피 주소를 사용하여 DDoS 공격을 수행하기 위해 'hping' 트래픽 생성툴을 사용하였

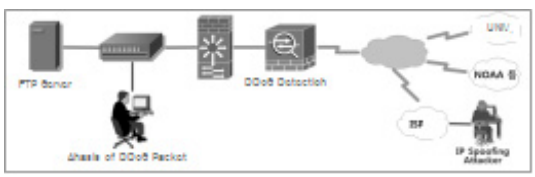

Fig. 9. Configuration for Testing

으며, DDoS 트래픽 탐지를 위해 DDoS 대응 장비와 트래픽 분석 서버를 활용하여 IP 주소의 위조 여부를 탐지하였다.

4.3 IP 위조 탐지 결과

Table 2는 DDoS 공격에 대해 IP 주소 스푸핑 여부를 측정한 결과이며, 스푸핑 여부를 확인하기 위해 참조테이블을 활용하였다. (A)는 허위여부를 판정하기 위해 전처리 작업을 완료한 IP 주소의 목적지까지 hop-count 계산 결과이며, (B)는 DDoS 대응 장비에서 탐지된 IP 주소의 스푸핑 여부를 확인하기 위해 사용한 참조 Hop-count이다.

탐지된 IP 주소의 동일 IP 주소가 참조테이블의 ip addr 필드에 존재하지 않을 경우 inetnum object의 동일 대역에 존재하는 해당 Hop count를 활용한다. Table 2는 스푸핑된 IP 주소의 탐지 결과를 나타내고 있으며, 실험 결과 값에서 '128.104.x.x'의 경우 해외에서 사용되는 IP 주소이지만 국내에서 IP 주소를 스푸핑하여 공격을 수행하였으며, 테스트 Tool로는 hping을 활용하여 커스텀 패킷을 전송하였다. 그 결과 참조테이블에 등록된 hop-count와 다른 결과 값을 확인하였다.

탐지된 IP 주소의 Hop count 대역을 국내·외로 구분하여 테스트한 결과 Fig. 10.와 같은 분류 영역을 확인할 수 있었으며, 결과에서 확인할 수 있듯이 국내와 국외 사이에 홉 카운트의 차이점을 확인할 수 있었다. 하지만 좀 더 정확한 분류 결과를 위해서 IP 주소에 대한 지연(delay)값 등을 활용하는 방안을 고려한다면 좀 더 향상된 결과 값을 얻는 것이 가능할 것이다.

위와 같은 실험결과에서 고려될 부분은 참조테이블은 공격 IP 주소의 허위 여부를 판단하는 주요한 역할을 함으로 관리 및 변경 등이 편리해야 하며, 최신의 hop-count 값으로 참조테이블을 업데이트하는 것이 필요하다.

Table 2. Result about detection of IP spoofing

Attacker	Hop count(A)	refHop count(B)	Country	Spoofing IP(Y/N)
128.104.x.x	14	17	US	Y
140.172.x.x	17	17	US	N
210.98.x.x	14	14	KR	N
112.216.x.x	13	13	KR	N

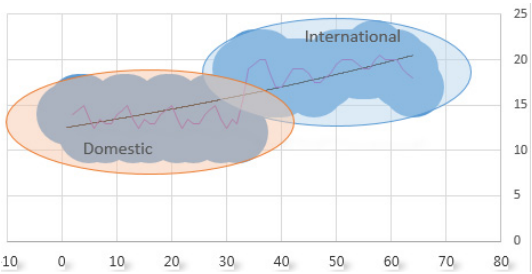

Fig. 10. Compare hop-count of domestic with international

V. 결 론

본 연구는 IP 주소의 스푸핑에 의한 DDoS 공격을 탐지하기 위한 방안으로 참조테이블을 활용하여 허위 여부를 검사하는 방법을 사용하였으며, 참조테이블 구성은 실험 환경의 웹 서비스 환경에 접속한 이력이 있는 목적지 IP 주소의 홉 수를 전처리 작업으로 추출하여 구성한다. 특히, 국외에서 출발한 IP 주소와 국내에서 접속한 IP 주소의 hop-count는 라우팅 경로 등에 의해서 차이가 발생하며, 국외 IP 주소의 네트워크 경로에서는 특정 영역에서 delay가 발생하는 것을 확인할 수 있었으며, 홉 수에서도 약 20% 정도의 차이를 확인할 수 있었다. 참조테이블은 웹 서비스에 접속한 목적지 IP 주소의 hop- count를 전처리 작업을 통해 관리하게 되며, 정기적인 업데이트를 통해 관리 IP에 대한 최신의 홉 수를 관리한다.

본 연구를 수행함으로서 허위 IP 주소 기반의 DDoS 공격을 탐지하여 트래픽을 차단함으로서 전산자원 인프라의 안정된 운영을 수행한다. 하지만 국내 서비스공격을 수행하는 공격자들은 좀비PC를 획득하여 서비스거부 공격을 수행함으로서 실제 허위 IP 주소 기반의 공격은 거의 탐지되지 않았다. 하지만 최근에는 DNS 증폭 방식의 DDoS 공격이 증가하고 있으며, NTP 서버의 취약점을 활용한 서비스 공격에 대한 위험이 늘어나고 있기 때문에 IP 주소 스푸핑을 통한 DDoS 공격의 탐지 및 차단을 적절히 수행할 수 있어야 한다.

본 논문의 연구 결과를 이용하면 허위 패킷을 이용한 서비스 공격을 탐지 및 대응할 수 있으며, 정보자산 인프라에 대한 보안성을 향상할 수 있을 것으로 기대된다.

References

〔1〕 Wang, Haining, Cheng Jin, and Kang G. Shin. "Defense against spoofed IP traffic using hop-count filtering," *IEEE/ACM Transactions on Networki ng*, pp. 40-53, Sep. 2007.

〔2〕 *Korea Internet & Security Agency*, "Study on the Method of a spoofed IP detection about the DDoS attack," 2013.

〔3〕 K.Park, H.Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," *Department of Computer Sciences, Purdue University*, 2000.

〔4〕 D.Song, A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," *IEEE INFO COM 2001*, 2001.

〔5〕 M. Adler, "Tradeoffs in Probabilistic Packet Marking for IP Traceback," *Department of Computer Science, University of Masachusetts*, 2001.

〔6〕 G. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," *IEEE/ACM Trans. Networking*, vol.9, pp. 226-237, June 2001.

〔7〕 T. Peng, C. Leckie, and K. Ramamo hanarao, "Adjusted probabilistic packet marking for IP traceback," *in Proc. Networking*, May 2002, pp. 697- 708, 2002.

〔8〕 M. Adler, "Tradeoffs in probabilistic packet marking for IP traceback," *Proc. 34th ACMSymp. Theory of Computing (STOC)*, pp. 407-418, May 2002.

〔9〕 S. S. Rana1 and T. M. Bansod, "IP Spoofing Attack Detection using Route Based Information," *in International Journal of Advanced Research in Computer Engineering & Technology*, ISSN: 2278 - 1323, Volume 1, Issue 4, June 2012.

〈저자소개〉

서 정 우 (Jung-woo Seo) 학생회원
2004년 2월: 고려대학교 정보보호대학원 석사
2004년 2월~2012년 8월: 삼성전자 책임연구원
2012년 8월~현재: 기상청
2013년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 네트워크 포렌식, 시스템 보안, 사물인터넷 보안

이 상 진 (Sang-jin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년2월: ETRI 선임연구원
1999년 3월~2001년8월: 고려대학교자연과학대학조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수