라우터 IP주소를 이용한 DDoS 공격경로 역추적

원 승 영*°, 구 경 옥**, 오 창 석*
충북대학교*, 강릉영동대학**

DDoS Attack Path Retracing Using Router IP Address

Won seung-young*°, Koo kyung-ok**, Oh chang-suk*
Chungbuk National Univ.*, Gangneung Yeongdong College**
E-mail : sywon@nwork.chungbuk.ac.kr

요 약

DDoS(Distributed Denial of Service) 공격으로부터 시스템 자원을 보호하기 위한 최선의 방법은 공격자에 의해 전송되어진 패킷의 경로를 역추적하여 공격자의 근원지로부터 근본적인 DDoS 공격을 차단하는 것이다. 기존의 패킷 마킹 기법은 IP 식별자필드를 마킹필드로 사용함으로써 ICMP의 사용이 불가능하고, 라우터 ID를 이용한 역추적기법은 라우터의 수가 증가할 경우 마킹필드의 크기가 증가하는 문제점을 가지고 있다. 본 논문에서 제안한 역추적 기법은 IP 헤더의 옵션필드를 마킹필드로 사용하여 ICMP를 사용을 가능하게 하였고, 라우터 IP 주소를 XOR 연산하여 얻어진 값을 마크정보로 사용함으로써 라우터 수의 증가에도 마크정보의 크기가 변하지 않도록 제안하였다.

Abstract

The best way in order to protect the system resource from Distributed Denial of Service(DDoS) attack is cut off the source of DDoS attack with path retracing the packet which transferred by attacker. Packet marking method can not use ICMP cause by using IP identifier field as marking field. And in case of increasing the number of router, retracing method using router ID has the size of marking field's increasing problem. In this paper, we propose that retracing method can be available the ICMP using marking field for option field in IP header and the size of making field do not change even though the number of router is increased using the mark information which value obtained through XOR operation on IP address.

I. 서론

전 세계적으로 인터넷의 보급이 급격하게 확산됨에 따라 인터넷을 이용한 범죄가 증가하고 있다. 그 중에서도 네트워크와 시스템 자원을 독점하여 인터넷 사용자가 정상적인 서비스를 받을 수 없게 하는 DDoS 공격에 대한 피해가 속출하고 있다. 현재 DDoS 공격은 전문적인 지식이 없어도 인터넷상에서 자동화된 도구들을 이용하여 누구나 손쉽게 사용할 수 있으며 이미 유명 사이트들이 DDoS 공격에 대한 피해를 입은 사례들이 빈번하다. DDoS 공격은 이미 잘 알려진 공격이지만 여전히 치명적인 피해를 주며 공격자들 사이에서 가장 많이 행해지고 있는 공격기법의 한 종류이다[1]. DDoS 공격은 공격자가 여러 대의 장비로 대량의 데이터를 한 피해호스트에 집중적으로 전송함으로써 피해호스트의 기능을 마비시켜 정상적인 서비스를 하지

못하게 하는 것이다. DDoS 공격으로부터 네트워크와 시스템 자원을 보호하고 인터넷 사용자에게 정상적인 서비스를 제공하기 위해서는 DDoS 공격에 대한 적극적인 대처방안이 필요하게 되었다[2]. DDoS 공격을 차단하기 위한 최선의 방법은 공격자의 근원지를 찾아내어 공격의 근원을 제거함으로써 더 이상의 피해를 발생하지 않도록 하는 것이다. 공격의 근원을 찾아내기 위하여 DDoS 공격에 이용된 패킷에 경로정보를 마킹하여 이 정보를 통해 경로를 역추적하는 기법들이 연구되고 있다. 하지만 아직까지 정확성과 효율성에서 부족한 현실이다.

본 논문에서는 DDoS 공격이 이루어질 때 패킷에 확률적으로 라우터 IP주소를 이용한 마킹을 통하여 공격의 근원지를 역추적할 수 있는 기법을 제안한다. 본 논문의 연구결과를 통해 공격자에 의한 DDoS 공격으로부터 피해호스트의 네트워크와 시스템 자원을 보호하고 정상적인 서비스를 지원할 수 있으리라 기대된다.

Ⅱ. DDoS 공격경로 역추적 기법

1. DDoS 공격경로 역추적 기법 제안

최근 DDoS 공격의 피해는 더욱 심각해지고 있다. 많은 유명 싸이트들의 피해로 정상적인 서비스를 제공하지 못하는 경우도 종종 발생함에 따라 이에 대한 효율적이고 정확한 대응 방법이 필요한 현실이다. 기존의 제안된 역추적 기법들은 IP 식별자필드를 마킹필드로 사용함으로써 ICMP 사용의 불가능과 라우터 ID필드의 사용으로 라우터 수의 증가에 따른 마킹필드의 증가를 초래하였다[1][2]. 마킹필드의 증가는 네트워크의 트래픽의 증가를 유발하여 DDoS 공격에 대응하기 위한 기법으로 적절하지 못하다. 이러한 문제점을 해결하기 위하여 라우터 수의 증가와 관계없이 고정된 마킹필드의 크기로 경로정보를 표현하기 위하여 라우터 IP주소를 암호화하여 공격패킷이 경유하는 라우터에서 공격경로의 정보를 마킹하고 피해호스트에서 경로정보를 추출하여 공격경로를 역추적하는 기법을 제안하였다. 그림 1은 DDoS 공격경로 역추적 기법의 처리 흐름도를 나타낸다.

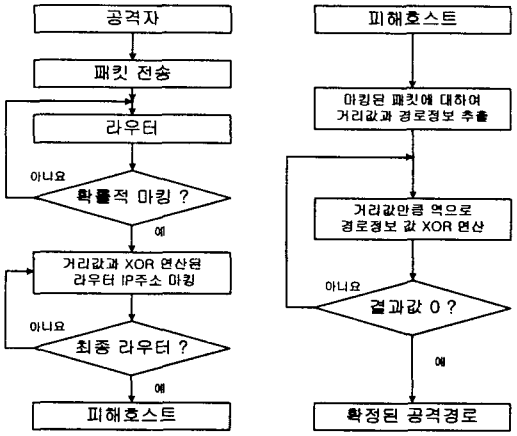

그림 1. 처리 흐름도

2. 마킹

라우터를 경유하는 패킷들은 확률적으로 패킷의 지정된 마킹필드에 거리값과 경로정보가 마킹하게 된다[1]. 그림 2는 거리값을 나타내는 거리필드와 XOR 연산된 라우터 IP주소의 값이 마킹되는 경로정보필드의 구조를 나타낸다[3][4].

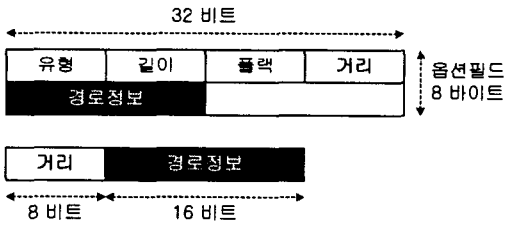

그림 2. 마킹필드의 구조

거리필드는 피해호스트로부터 최초 마킹을 시작한 라우터까지의 거리를 나타내며, 16비트의 경로정보필드는 XOR 연산을 통해 암호화된 라우터 IP주소를 누적하여 경로정보를 표현하는 필드이다[1]. 그림 3은 XOR 연산을 통한 라우터 IP주소의 암호화 과정을 나타낸다. 32비트의 라우터 IP주소를 16비트로 암호화하여 경로정보로 사용하게 된다. 패킷이 네트워크상의 라우터를 경유하는 동안 라우터에서는 확률적으로 패킷이 마킹하게 되는데 라우터에서 패킷에 마킹을 결정하게 되면 거리필드에 최초 마킹을 나타내는 0 값을 마킹하고 경로정보필드에는 16비트로 암호화된 라우터 IP주소를 마킹하게 된다.

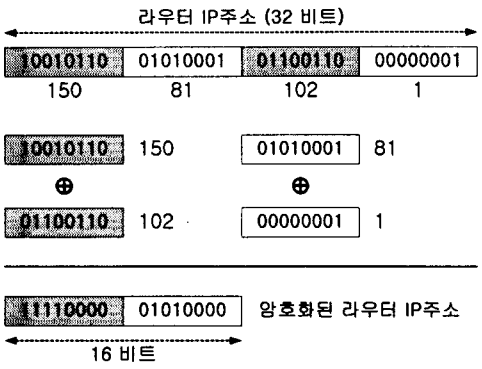

그림 3. 라우터 IP주소의 암호화 과정

마킹된 패킷이 다음 라우터에 도착하게 되면 라우터에서는 마킹필드를 검사하여 거리필드의 값이 null 값이 아니면 거리필드의 값에 1을 증가시키고 정보필드의 값과 암화화된 자신의 IP 주소를 XOR 연산을 통하여 누적시킨다[1]. 이렇게 경로정보가 누적되어 피해호스트로 전송된 패킷은 피해호스트에서 추출하여 경로 역추적을 하는데 사용된다. 그림 4는 마킹 알고리즘을 나타낸다.

```
Marking procedure at router Ri;
 let p be a marking probability
 let mark_fields be a fields for mark (distance, path_info)
 let encode_ip be a encoded router IP address
 for each packet P
    let x be a random number from [1..100)
    if x < p then
      if mark_fields[distance] == null then
        insert mark_fields in P
        P.distance <- 0
        P.path_info <- ecode_ip(Ri)
      else
        P.distance <- P.distance + 1
        P.path_info <- P.path_info ⊕ ecode_ip(Ri)
```

그림 4. 마킹 알고리즘

3. 공격경로 역추적

마킹된 패킷을 수신한 피해호스트에서는 마킹필드의 거리값과 경로정보의 값을 추출하여 공격경로를 역추적할 수 있다. 그림 5는 공격경로를 나타낸다.

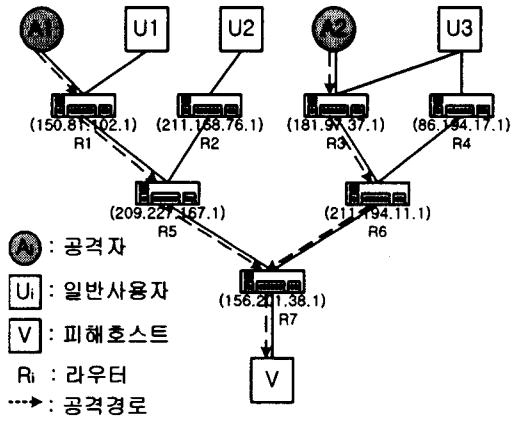

그림 5. 공격경로

공격자 A1과 A2는 피해호스트 V로 DDoS 공격을 하게된다. 공격자 A1로부터 수신된 패킷의 마킹필드 값을 추출하면 거리필드의 값은 2이고, 경로정보필드의 값은 R1⊕R5⊕R7의 값을 가지게 된다. 즉 이 값은 0011110001111010 이다. 이렇게 마킹된 거리필드의 값과 경로정보필드의 값을 이용하여 패킷이 마킹된 경로를 역추적할 수 있다. 그림 6은 공격경로의 역추적 과정을 나타낸다.

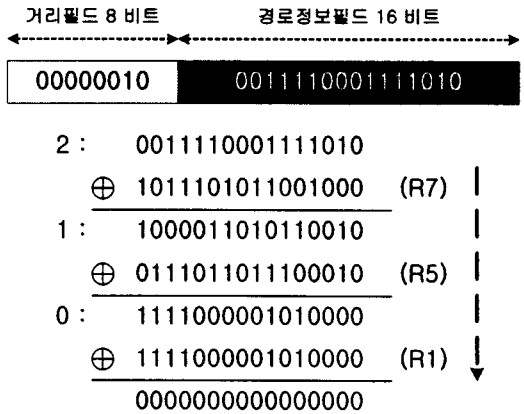

그림 6. 공격경로의 역추적 과정

그림 6에서 나타내듯 경로정보필드의 값을 거리필드의 값만큼 XOR 연산한 결과 값이 0 이라면 정확한 공격경로의 역추적임을 알 수 있다.

그림 7은 공격경로 역추적 알고리즘을 나타낸다.

```
Reconstruction procedure at Victim V;
 let mark_fields be a fields for mark (distance, path_info)
 let encode_ip be a encoded router IP address
 for each packet P
     if P.mark_fields[distance] ≠ null then
       let path be a P.mark_fields[path_info]
     for P.mark_fields[distance] to 0
       path <- path ⊕ encode(Ri)
       if path is 0
  extract path(Ri..Rj) by path in attack path
```

그림 7. 공격경로 역추적 알고리즘

Ⅲ. 실험 및 결과고찰

본 논문에서 제안한 알고리즘의 검증을 위하여 그림 5와 같은 시뮬레이션 환경을 설정하고 리눅스 시스템에서 실험하였다. 그림 8은 패킷의 이동경로에 따라 라우터에서 확률적으로 패킷에 마킹한 경로와 마킹필드의 값을 나타낸다.

```
3813    R1 -> R5 -> R7 -> V
        0x023c7a
3814    R3 -> R6 -> R7 -> V
        0x02c86b
3815    R7 -> V
        0x00bac8
3816    R6 -> R7 -> V
        0x01620b
3817    R5 -> R7 -> V
        0x01cc2a
3818    R3 -> R6 -> R7 -> V
        0x02c86b
```

그림 8. 라우터에서의 경로정보 마킹

마킹된 패킷들 중 3818번째 패킷은 R3 -> R6 -> R7의 경로를 통하여 피해호스트로 전송된 패킷으로 마킹필드의 값은 0x02c86b이다. 이 값은 2(00000010)의 거리 값과 1100100001101011의 경로정보필드의 값으로 구분할 수 있다. 이렇게 경로정보가 마킹된 패킷이 피해호스트로 전송되면 피해호스트에서는 그림 9와 같이 공격경로를 역추적한다.

```
3813    0x023c7a
        3c7a : V -> R7 -> R5 -> R1
3814    0x02c86b
        c86b : V -> R7 -> R6 -> R3
3815    0x00bac8
        bac8 : V -> R7
3816    0x01620b
        620b : V -> R7 -> R6
3817    0x01cc2a
        cc2a : V -> R7 -> R5
3818    0x02c86b
        c86b : V -> R7 -> R6 -> R3
```

그림 9. 공격경로 역추적

피해호스트에서 수신한 패킷중에서 3818번째 패킷의 마킹필드를 추출하여 그림 6과 같은 공격경로의 역추적 과정을 통하여 패킷의 이동경로를 정확하게 역추적할 수 있다.

Ⅳ. 결론

본 논문에서는 DDoS 공격의 경로 역추적 기법을 제안하였다. 패킷이 경유하는 라우터에서 확률적으로 패킷의 마킹필드에 마킹하고 피해호스트에서는 패킷에 마킹된 경로정보를 추출하여 공격경로를 정확하게 역추적한 것을 실험결과로 확인하였다. 차후에 본 논문에서 제안한 DDoS 공격경로 역추적 기법을 네트워크 침입탐지 시스템에 적용한다면 DDoS 공격으로부터 네트워크와 시스템자원을 보호하여 인터넷 사용자로 하여금 정상적인 서비스를 받을 수 있을 것으로 기대된다.

참 고 문 헌

[1] 원승영, 한승완, 서동일, 김선영, 오창석 "패킷 마킹을 이용한 해킹경로 역추적 알고리즘", 한국콘텐츠학회논문지, 제3권, 제1호, pp.21-30, 2003.

[2] D. Song, A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," in IEEE INFOCOM 2001, 2001.

[3] 오창석, 데이터통신(수정판), pp.475, 영한출판사, 서울, 2001.

[4] W. Stevens, TCP/IP Illustrated Volume 1, 2, Addison Wesley, 1994.