情報保護學會論文誌
第13券 第1號, 2003. 2

마킹 알고리듬 기반 IP 역추적에서의 공격 근원지 발견 기법*

김 병 룡**, 김 수 덕***, 김 유 성****, 김 기 창*****

An Attack Origin Detection Mechanism in IP Traceback Using Marking Algorithm

Byung-yong Kim**, Soo-duk Kim***, Yoo-sung Kim****, Ki-chang Kim*****

요 약

인터넷을 통한 기업 활동을 방해하는 악의적인 공격 형태 중 최근 가장 빈번하게 그리고 큰 피해를 주는 공격 형태가 DoS(Denial-of-Service) 공격이다. DoS 공격은 공격자가 자신의 위치를 숨기기 위하여 자신의 IP를 속이는 IP 스푸핑(spoofing) 을 하기 때문에 피해 시스템에서 받아들인 패킷의 소스 IP 주소를 가지고는 공격자의 정확한 위치를 파악할 수가 없게 된다. 또한 공격에 대응하여 방어한다고 해도 공격 진원지를 찾아내지 못한다면 추후 동일한 공격자에 의해 재차 공격을 받을 가능성을 배제할 수 없는 실정이다. 이에 본 논문은 DoS 공격에 대응하는 하나의 방법으로 마킹 알고리듬을 이용하여 공격 경로를 찾아내고, 더 나아가 공격 진원지의 MAC 주소를 알아냄으로써 공격 진원지를 찾아내는 방법을 제안한다. 또한 마킹 알고리듬에서의 패킷 도착율을 향상시키는 기법을 제안하여 좀더 빠른 시간 내에 공격 위치의 탐지를 가능하게 함으로써 DoS 공격에 대한 적절한 대응과 공격자를 찾아내는 좀 더 향상된 성능을 보인다.

ABSTRACT

Recently, the number of internet service companies is increasing and so is the number of malicious attackers. Damage such as distrust about credit and instability of the service by these attacks may influence us fatally as it makes companies image falling down. One of the frequent and fatal attacks is DoS(Denial-of-Service). Because the attacker performs IP spoofing for hiding his location in DoS attack, it is hard to get an exact location of the attacker from source IP address only. and even if the system recovers from the attack successfully, if attack origin has not been identified, we have to consider the possibility that there may be another attack again in near future by the same attacker. This study suggests to find the attack origin through MAC address marking of the attack origin. It is based on an IP trace algorithm, called Marking Algorithm. It modifies the Marking Algorithm so that we can convey the MAC address of the intervening routers, and as a result it can trace the exact IP address of the original attacker. To improve the detection time, our algorithm also contains a technique to improve the packet arrival rate. By adjusting marking probability according to the distance from the packet origin, we were able to decrease the number of needed packets to traceback the IP address.

Keyword : *DoS공격, 공격 근원지, IP 역추적, MAC주소, 패킷 도착율*

---

* 이 논문은 인하대학교의 교수 연구 진흥비 지원에 의해 연구되었음.(INHA-22007)
본 연구는 한국과학재단 지정 인천대학교 동북전자물류연구센터의 지원에 의한 것임
** 인하대학교 전자계산공학과 인터넷보안 연구실(doolyn@super.inha.ac.kr)
*** 안철수 연구소 보안연구2실 보안응용팀(petitpri@ahnlab.com)
**** 인하대학교 정보통신공학부 부교수(yskim@inha.ac.kr)
***** 인하대학교 정보통신공학부 부교수(kchang@inha.ac.kr)

Ⅰ. 서 론

인터넷을 통한 기업 활동을 방해하는 악의적인 공격중의 하나로 DoS (Denial-of-Service) 공격이 있다[1]. DoS 공격은 공격자가 하나 이상의 공격 시스템을 사용하여 피해 시스템에 무한의 악의적인 패킷을 보냄으로써 피해 시스템의 정상적인 서비스를 방해하거나 시스템을 다운 시키는 등의 피해를 주는 공격 형태이다. 그러나 DoS 공격에 대응하는 적절한 방법이 없는 상황이기 때문에 피해 시스템의 입장에서는 마비된 서버를 재가동 하거나 IDS(Intrusion Detection System)등을 이용해서 공격을 차단하는 정도의 대응 이외의 다른 대응 수단이 없다는 것이 현실이다[2]. 공격자의 정확한 위치를 찾아내지 못한다면 추후 재차 공격의 가능성을 배제할 수 없게 되고, 이는 잠재된 위험 요소를 방치하는 결과를 초래하게 된다.

공격자의 정확한 위치를 찾아내기 위한 노력으로 IP 역추적 기술이 연구되었으나, 공격자가 자신의 IP를 스푸핑(Spoofing) 함으로써 이러한 IP 역추적은 어느 정도의 한계에 직면할 수밖에 없었다[3]. 따라서 패킷에 기록되어 있는 소스 IP 주소를 이용하는 방식이 아닌 다른 방식으로 공격자의 위치를 찾아내는 방법이 연구되어야만 했고 이를 위한 한 가지 대안으로서 마킹 방식 IP 역추적 기법이 제안되었다[4,5]. 이는 네트워크 상의 모든 라우터가 자신을 지나가는 패킷에 자신의 IP 주소를 마킹 하도록 하여 피해 시스템에서 이를 이용하여 공격 경로를 찾아내는 것이다. 하지만 이 방식은 수많은 패킷을 수집한 다음에야 공격 경로를 찾는 것이 가능하며 또한 공격지를 나온 패킷이 지나는 최초의 라우터까지의 추적은 가능하지만, 실제적인 공격 진원지의 위치를 찾아내지는 못한다는 단점을 안고 있다. 본 논문에서는 기존의 마킹 방식 IP 역추적 기법을 개선하여 최소한의 패킷만 수집하여 빠르게 공격경로를 찾을 수 있는 기법을 제안하고 또한 라우터가 자신의 IP 주소뿐만 아니라 공격 진원지의 MAC 주소를 마킹 하도록 함으로써 MAC 주소를 이용한 공격 진원지의 실제 위치를 찾아내는 방법을 제안한다. 본 논문의 구성은 다음과 같다. 제2장에서는 관련된 연구 방법들을 소개하고, 제3장에서는 공격 진원지 발견 문제를 해결하기 위한 MAC 주소를 이용한 해결 방법과 패킷 도착율을 향상 시킬 수 있는 기법을 제안한다.그리고 제4장에서는 성능 평가 및 실험 결과를 보이고, 마지막 제5장에서는 결론과 향후 연구 방향에 대해서 기술한다.

Ⅱ. 기존 연구의 고찰

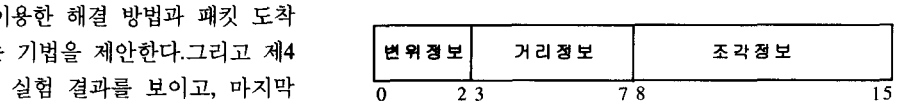
침입자를 역추적(Traceback)하려는 노력은 여러 가지 방향에서 논의되고 있다. 시스템 로그를 분석하는 방법[6,7], Logging[8], Ingress Filtering[9], Link Testing[10], ICMP Traceback[11] 등 다양한 방법으로 침입자의 흔적을 역추적하는 방법이 제시되었다. 하지만 이러한 여러 방법들은 각기 장단점을 가지고 있으며, 침입자를 올바르게 역추적하기에는 부족한 점이 많았다[4]. 이에 새롭게 제안된 방법이 마킹 알고리듬이다. 이는 중간 라우터가 패킷에 자신의 IP 주소를 표시하도록 하여 이를 토대로 공격 경로를 역추적하는 방식이다.

2.1 마킹 기반 IP 역추적

Fragment Marking Scheme(FMS) 이라고도 하는 이 방법은 모든 패킷을 대상으로 하지 않고 주어진 확률 p이하로 선정한 패킷에 대해서 라우터에서 이 패킷이 자신을 거쳐 갔음을 표시 하는 방법이다[4,5]. 즉, 각 라우터에서 p 이하의 확률로 선택된 패킷에 대해 이 패킷의 경로를 나타내는 추가 정보로 소스 필드에 이 라우터의 IP로 표시하고 거리정보, 즉 홉 수 표시는 0으로 설정한다. 이 패킷이 거치는 다음 라우터에서 이 패킷을 선택할 확률이 p 이상일 때 이 패킷에 표시되는 끝 라우터가 이 라우터의 IP가 된다. 이렇게 소스와 끝 IP가 다 기록이 된 것은 다음 라우터를 거칠 때 확률 p 이상이면 소스 라우터로부터 중간에 거친 라우터의 수만큼의 홉 수가 더해지며, 확률 p 이하면 이번의 기록 내용은 무시되고 다시 소스를 기록하는 과정을 거친다.

이런 과정은 임의도를 증가시켜 의도적인 패킷이 발생된 소스 주소에 수정을 가하더라도 실제의 패킷 소스를 밝히는데 상당한 신뢰를 줄 수 있는 방법이다. 그리고 이 정보를 기록하는 부분은 패킷의 IP 헤더에 분할을 위하여 패킷의 동일성을 표시하는 부분인 식별 필드로서 통계적으로 이 부분을 사용하는 율이 0.25%라는 데 착안을 하였다[4]. 따라서 기존 네트워크 체계의 위반되는 문제점은 존재하지 않는다.

[그림 1]은 새롭게 정의된 식별 필드이다.

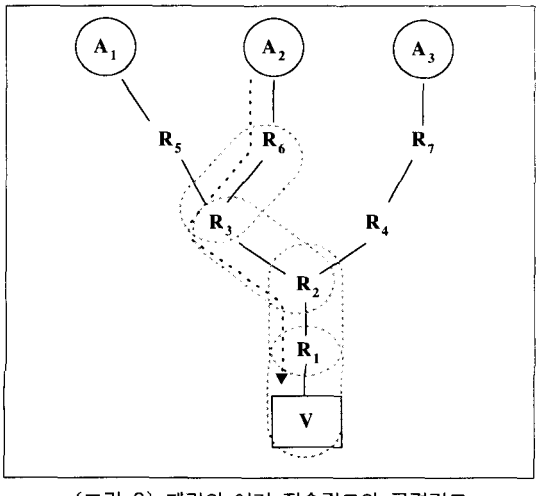


[그림 1] 재 정의된 IP 헤더의 식별 필드 구성

2.2 마킹 기반 IP 역추적의 문제점

기존 마킹 알고리듬은 라우터의 정보를 패킷의 IP 헤더의 식별 필드에 실어 보내는 방식으로 라우터의 정보는 분할하여 조각으로 전송하며, 또한 라우터에서의 마킹 과정은 샘플링 방식에 의해 확률로써 처리된다[4]. 각 라우터는 자신의 IP 주소 R과 이 IP 주소에 비트연산과 not을 사용하여 해쉬한 hash(R)값을 BitInterleave하여 64 비트의 R을 생성하며, 이 값을 8개의 조각으로 나누어 그 중 o(변위정보, 임의의 수)번째 조각을 패킷에 실어 보낸다. 즉 패킷에는 거리정보와 IP 주소의 조각, 그리고 그 조각의 위치를 나타내는 변위정보가 마킹 되는 것이다. 이렇게 거쳐온 라우터의 IP 주소를 표시한 패킷들은 피해 시스템에서 거리정보 별로 구분되어 조합되고, 이렇게 조합되어 구해지는 IP 주소가 올바른 라우터의 IP 주소로 판단되면 이를 경로 트리에 기록한다. 이러한 일련의 과정을 통해 경로 트리를 구성하면 이것이 바로 공격 경로가 되는 것이다.

[그림 2]는 패킷의 여러 전송 경로 중에서 기존 마킹 알고리듬을 통해 찾아낼 수 있는 실제적인 공격 경로를 나타내고 있다. [그림 2]에서 확인하듯이 기존의 마킹 알고리듬에서는 공격 경로의 첫 번째 라우터까지는 발견 가능하지만 공격 진원지(A_2)를 찾아낼 수 없다는 문제점을 가지고 있다. 또한 패킷이 피해 시스템에 도착하기까지 중간에서 각 라우터에 의해 처음의 정보를 유실(새로운 라우터의 정보를 마킹)하게 되는 알고리듬의 특성 때문에 첫 번째 라우터의 정보를 가진 패킷이 피해 시스템까지 도착할 확률이 상대적으로 적어진다. 이러한 패킷의 도착율은 공격자에서 피해 시스템까지의 홉 수가 많아질수록 더 작아진다. 각 라우터가 가진 확률값을 p라 하고, 라우터에서 피해 시스템까지의 홉 수를 d라고 할 때 패킷의 정보가 도착할 확률은 다음 식 (1)과 같다.



[그림 2] 패킷의 여러 전송경로와 공격경로

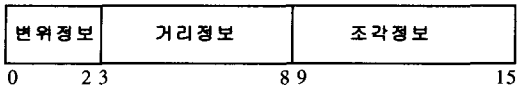
$$E(X) = \frac{1}{p(1-p)^{d-1}} \quad (1)$$

Ⅲ. 저비용의 정확한 공격 진원지 발견 기법

3.1 MAC 주소의 사용

최초 공격진원지를 노출시키기 위해서는 라우터가 자신의 IP 주소뿐만 아니라 바로 앞 단(이전 라우터 또는 공격 진원지)의 MAC 주소까지도 패킷에 마킹하도록 해야한다. 이렇게 함으로써 공격 진원지의 MAC주소와 공격 경로상의 라우터의 MAC주소도 알게 되어 신뢰성 향상을 노릴 수 있다. MAC 주소를 지원하지 않는 WAN환경에서는 WAN Router의 egress Port의 시리얼 번호를 MAC주소 대신 마킹하고, *input debugging feature*[10]을 이용하면 공격진원지 역추적이 가능하다. 그러나 MAC 주소를 마킹함으로써 얻어지는 이익에 따르는 또 다른 문제점이 생긴다. 문제점은 32 비트의 IP 주소와 48 비트의 MAC 주소를 같은 방식으로 전송할 수 없다는 것이다. IP 주소의 경우 32 비트의 해쉬값을 만들어 기존 IP 주소에 덧붙여 64 비트로 만들고, 이를 8 조각으로 나누어 전송하는 방식을 사용하고, 또 이의 역과정을 이용하여 무결성 확인을 할 수 있었다. 하지만 48 비트의 MAC 주소를 64 비트로 만들어 이를 8 조각으로 나누어 전송하는 경우, 각 라우터는 자신의 IP 주소를 마킹하는 과정과 앞 단의 MAC 주소를 마킹 하는 과정의 두 과정을 처리해야 하며, 이를 각각 구별하기 위하여 하나의 라우터가 2개의 거리정보를 소비하게 되는 결과를 초래하게 된다. 이 때문에 역추적 가능한 홉의 수가 기존 방식의 절반 수준인 16 개로 한정되게 되고, 이것은 공격 진원지를 찾아낸다는 당초의 목표에 있어서 상당한 문제점을 갖게 되는 것이다. 따라서 MAC 주소를 마킹 하는 방식도 허용되면서 기존 방식에서 가능했던 역추적 범위도 줄어들지 않는 새로운 방식이 필요하게 되었다.

본 논문에서는 IP 주소와 MAC 주소를 56 비트의 조각조합으로 만들어 이를 조각 단위로 전송하는 방법을 제안한다. 이때 56 비트로 구성함에 있어서 여기



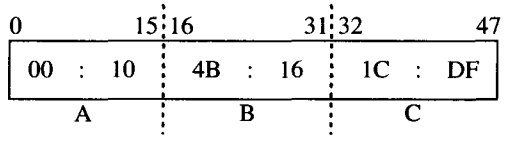
〔그림 3〕 제안하는 IP 헤더의 식별 필드 구성

에 무결성 확인을 위한 방법을 추가해야 한다. 이를 위해서 IP 헤더의 식별 필드를 재구성해야 한다. 제안하는 재구성 방식은 식별 필드 16 비트를 3 비트의 변위정보 필드, 6 비트의 거리정보 필드, 7 비트의 조각정보 필드로 구성하는 것이다. 따라서 IP주소와 MAC주소를 사용하여 공격 진원지 추적 경로의 재구성을 위한 패킷의 오버헤드를 해결 할 수 있다. 이를 그림으로 나타내면 [그림 3]과 같다.

공격 경로상의 각 라우터가 패킷에 자신의 IP 주소를 마킹 하는 것처럼 앞 단의 MAC 주소까지도 마킹 하도록 하게 되면, 피해 시스템에서 패킷에 전달되어온 IP 주소의 무결성을 확인 하듯이 전달되어 온 MAC 주소의 무결성도 확인할 필요가 있게 된다. 또한 중간 라우터가 앞 단의 MAC 주소를 마킹 하도록 함으로써 각 라우터는 실제적으로 거리정보를 두 개씩 소비하게 된다(자신의 IP 주소 - 거리정보 0, 앞 단의 MAC 주소 - 거리정보 1). 이것은 기존 방식의 추적 가능 홉 수를 반으로 줄어들게 만드는 새로운 문제점을 야기하게 된다.

이를 보완하기 위하여 본 논문에서는 식별 필드의 구성을 조정하여 거리정보 필드를 6 비트로 하고, 조각정보 필드를 7 비트로 구성함으로써 기존 마킹 알고리듬과 같은 수준의 추적 가능 홉 수를 유지 할 수 있게 하였다. 또한 조각정보 필드가 1 비트 줄어들게 되는 문제점은, 기존 64 비트 조각조합을 56 비트로 조정하고 이를 이용하여 무결성 확인을 가능하게 하는 방법을 제안함으로써 해결하였다.

[그림 4]는 이 기법을 설명하기 위하여 사용한 예제이다.



〔그림 4〕 MAC 주소 예제

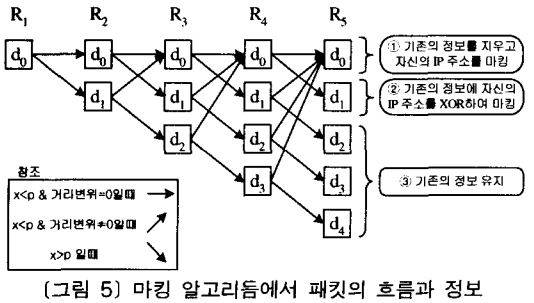
3.2 샘플링 확률 p의 보정

각 라우터에서 받은 패킷에 대해서 기존의 값을 무시하고 자신의 IP 주소로 식별 필드에 새로운 값을 마킹 할 것이냐, 아니면 기존의 값에 자신의 IP 주소를 XOR하여 마킹 할 것이냐를 결정하는 기준이 바로 샘플링 확률 p이다.기존의 마킹 알고리듬에서는 각 라우터마다 확률 p가 고정되어 있었다. 알고리듬의 특성상 라우터가 받은 패킷은 확률 p를 기준으로 p보다 작으면 이전의 정보를 상실하고 현 라우터의 정보를 새롭게 마킹 하게 된다. 평균적으로 p=0.5로 설정하게 되면 라우터를 하나 지날 때마다 처음 정보를 가진 패킷의 수가 반으로 줄어들게 된다. 모든 라우터의 확률값이 일정하게 설정되어있다면 거리가 먼 패킷 일수록 피해 시스템에 도착하는 확률이 적어지기 때문에 패킷 도착률의 향상을 기하기 위해서는 거리가 먼 패킷일수록 가중치를 두어 확률값을 보정하는 방법을 취할 수 있다.

[그림 5]는 라우터 R_1에서 라우터가 패킷에 자신의 정보를 마킹 하여 보내기 시작한 패킷이 중간의 각 라우터를 거쳐 최종적으로 라우터 R_5까지 도착하는 과정에서 이 패킷에 저장된 라우터의 정보가 새롭게 생성되거나 변경되는 모습을 보여주고, 이러한 패킷에 저장된 라우터의 정보에 따라 각 패킷을 구별하여 보여주는 것이다.

[그림 5]에서 d_0는 라우터에서 패킷에 실려 온 기존의 정보를 지우고 새롭게 자신의 IP 주소를 마킹 하는 것이고, d_1은 패킷에 실려 온 앞 라우터의 정보에 자신의 IP 주소를 XOR하여 마킹 하는 것이며, d_2 이후의 값들은 기존 정보를 그대로 유지한 채 패킷의 거리정보만을 증가시켜 보내는 것이다.

[그림 5]에서 화살표는 확률 p를 적용하여 다음 라우터로 보내는 것을 의미하는 것으로서, 예를 들어 R_1의 d_0에 확률 p를 적용한 값이 R_2의 d_0와 d_1이다. 이때 확률 p의 적용은 임의의 수 x를 발생시켜서 $x<p$이면 [그림 5]에서의 ①의 과정을 적용하고, 패킷의 거리정보가 0이고 $x>p$이면 ②의 과정을 적용하며, 패킷의 거리정보가 0보다 크고 $x>p$이면 ③의 과정을 적용한다.



〔그림 5〕 마킹 알고리듬에서 패킷의 흐름과 정보

이를 식으로 나타내면 다음과 같다.

$$R_2[d_0] = R_1[d_0] \times p \quad (2)$$

$$R_2[d_1] = R_1[d_0] \times (1-p) \quad (3)$$

기존의 방법에서는 모든 라우터마다 확률 p는 고정된 값이다. 이제 이 확률 p를 거리정보에 따라 가중치를 부여함으로써 패킷의 유실율과 도착율을 향상시키려 한다. 라우터를 지날 때 마다 자신이 가진 정보를 유실하는 것은 어쩔 수 없지만, 원거리의 정보를 가진 패킷이 최대한 많이 피해 시스템에 도착하도록 하여 공격 경로를 찾는데 소요되는 시간을 최소화할 필요가 있다.

각 라우터에 도착되는 패킷의 수를 나타내는 값 X를 다음과 같이 정의 한다.

정의 : 홉 수가 n일때 거리정보가 i인 패킷이 라우터에 도착하는 수를 X_i^{n+1} 라고 표현한다.

또한 확률 p에 대한 함수 f를 다음과 같이 거리정보에 따른 가중치를 부여하는 다음과 같은 식으로 제안하여 정의한다.

$$f_i = \frac{1}{(i+1)\times 2} \quad (i\text{=거리정보}) \quad (4)$$

위의 두 정의를 적용하여 홉에 따른 값을 식으로 나타내면 다음과 같다.

n=0 일 때,

$$X_0^1 = X_0^0 \cdot f_0$$
$$X_1^1 = X_0^0 \cdot (1-f_0)$$

n=1 일 때,

$$X_0^2 = X_0^1 \cdot f_0 + X_1^1 \cdot f_1$$
$$X_1^2 = X_0^1 \cdot (1-f_0)$$
$$X_2^2 = X_1^1 \cdot (1-f_1)$$
$$\vdots$$

위의 계산식들을 조합하여 함수식으로 표현하면 다음과 같다.

$$X_0^{n+1} = X_0^n \cdot f_0 + X_1^n \cdot f_1 \cdots X_n^n \cdot f_n \quad (5)$$

$$X_i^{n+1} = X_{i-1}^n \cdot (1-f_{i-1}) \text{ for } i=1,\cdots,n+1 \quad (6)$$

위와 같이 확률 p를 고정값으로 설정하지 않고 패킷의 거리정보에 따라 가중치를 부여하게 되면, 라우터를 거쳐 갈 때 마다 크게 줄어들던 이전 정보를 가진 패킷의 도착율이 크게 향상된다. 제안한 기법에 의한 패킷 도착율의 향상과 그 편차의 감소에 대한 실험 결과는 제4장에서 보인다.

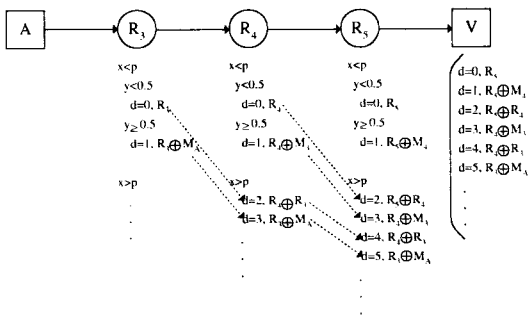
Ⅳ. 성능 평가 및 실험 결과

4.1 공격 진원지의 발견

[그림 6]은 제안한 알고리듬을 이용하여 공격 진원지 A에서 중간 라우터 R_3, R_4, R_5를 거쳐서 피해 시스템 V에 도착하는 패킷들의 흐름을 보여주는 것이다. 중간 라우터들은 자신을 지나가는 패킷에 자신의 IP 주소와 앞 단의 MAC 주소를 마킹 한다. 기존의 마킹 알고리듬과는 다르게 MAC 주소까지를 마킹 해야 하므로, 라우터는 임의의 수 y를 발생시켜서 y<0.5이면 거리정보를 0으로 하고 자신의 IP 주소를 마킹하고, y≥0.5이면 거리정보를 1로 하고 앞 단의 MAC 주소와 자신의 IP 주소를 XOR하여 마킹 하도록 한다. 즉, IP주소와 MAC주소를 확률에따라 교대로 전송함으로써 부하가 증가하는 문제를 해결할 수 있다.

[그림 6]에서 받은 패킷들의 조각들을 가지고 같은 거리정보를 가진 조각별로 테이블을 구성한 후 같은 거리정보를 가지는 조각들을 조합하여 거리정보 별로 나타내면 [표 1]과 같다.

[표 1]에서 첫 번째 노드(거리정보 0)의 조각조합(R_5)과 두 번째 노드(거리정보 1)의 조각조합($R_5 \oplus M_4$)를 XOR하면 다음과 같은 결과를 얻을 수 있다.



[그림 6] 제안한 알고리듬을 이용한 공격 진원지의 발견

〔표 1〕 조합된 조각들과 거리정보

거리정보	조각조합
0	R_5
1	R5 ⊕M4
2	$R_5 \oplus R_4$
3	R_4,M_3
4	$R_4 \oplus R_3$
5	$R_3 \oplus M_A$

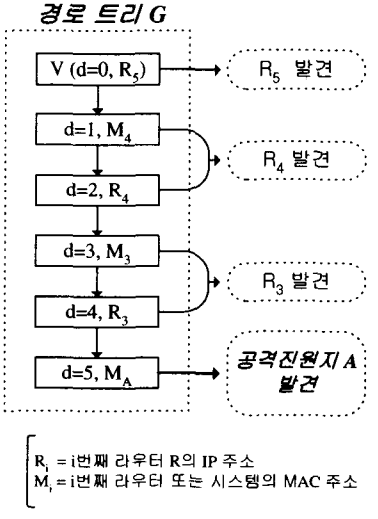
$$R_5 \oplus (R_5 \oplus M_4) = M_4$$

또한 첫 번째 노드(거리정보 0)의 조각조합(R_5)와 세 번째 노드(거리정보 2)의 조각조합($R_5 \oplus R_4$)를 XOR 하면 다음과 같은 결과를 얻을 수 있다.

$$R_5 \oplus (R_5 \oplus R_4) = R_4$$

이처럼 위의 두 가지 과정을 통하여 라우터 R4의 IP 주소와 MAC 주소를 얻을 수 있다. 위와 같은 과정을 [표 1]의 각 노드에 적용해보면 공격 경로상의 각 라우터의 IP 주소와 MAC 주소를 알아 낼 수 있고, 최종적으로는 공격 진원지의 MAC 주소까지도 알아 낼 수 있게 된다.

[표 1]의 정보를 가지고 위와 같은 XOR 과정을 거쳐서 알아 낸 공격 경로상의 각 라우터의 정보를 이용하면 [그림 7]과 같은 경로 트리 G를 구성할 수 있게 된다.



〔그림 7〕 경로 트리

4.2 확률 p의 보정에 따른 패킷 도착율과 편차

앞에서 패킷의 거리정보에 따라 라우터의 확률 p에 가중치를 부여하는 방법을 제안하였다. 식 4가 최적화된 식인가를 확인하기 위하여, 확률 p에 대한 함수식을 다음과 같이 a, b 두개의 계수를 가지는 함수로 바꾼다.

$$f_i = \frac{1}{ai+b} \quad (i\text{=거리정보}, a \geq 0, b > 0) \tag{7}$$

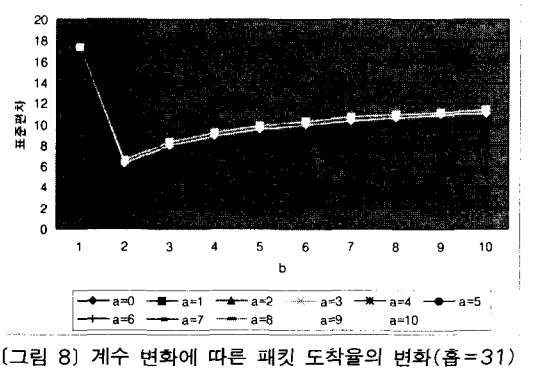
위의 식 (7)을 $0 \leq a \leq 10$, $1 \leq b \leq 10$의 범위 내에서 계수 변환하여 라우터에 도착하는 패킷의 도착율의 편차를 계산하여 본다. [그림 8]에서 a, b값의 변화에 따른 패킷 도착율의 편차의 최저값은 a=2, b=2인 경우(편차=1.975759)임을 알 수 있다. 즉, a=2, b=2 일 때 패킷의 도착률 편차의 감소를 최대화 할 수 있다. a=2, b=2를 식 (7)에 적용해 보면 다음과 같은 확률 함수를 구할 수 있다.

$$f_i = \frac{1}{2i+2} \quad (i\text{=거리정보}) \tag{9}$$

식 (9)는 패킷 도착율의 편차를 최저로 하는 최적의 함수식이다. 또한 식 (9)와 제안한 확률 p의 함수식인 식 (4)를 비교해 보면, 두 식이 서로 같음을 알 수 있게 된다.

$$\frac{1}{(i+1)\times 2} \quad (4) \qquad = \qquad \frac{1}{2i+2} \quad (9)$$

따라서 제안한 확률 p의 함수식인 식 (4)는 패킷도착율의 편차를 최저로 하는 최적의 함수식임을 알 수 있다.



〔그림 8〕 계수 변화에 따른 패킷 도착율의 변화(홉=31)

V. 결론 및 향후 연구 방향

본 논문에서는 DoS 공격에 대한 대응 방법으로서의 기존 마킹 알고리듬의 문제점인 공격 진원지의 발견 문제와 공격 경로를 찾아내는데 필요 되는 많은 양의 패킷 문제에 대한 해결 방법으로서, 공격 진원지의 MAC 주소를 발견해 내는 기법과 라우터의 샘플링 확률값에 가중치를 두어 패킷의 도착율을 향상하는 기법을 제안하여 이를 효과적으로 개선 하였다. 기존 마킹 알고리듬 방식에서 찾아내지 못했던 공격 진원지를 중간 라우터에서 MAC 주소를 마킹하도록 하여 피해 시스템에서 공격 경로를 역추적하여 공격 진원지의 MAC 주소를 찾아 낼 수 있도록 하였으며, 고정값으로 설정되어 있었던 라우터의 샘플링 확률값을 패킷의 거리정보의 값에 따라 가중치를 부여하는 유동적인 값으로 바꿈으로써 실제적인 패킷의 도착율과 그 도착율의 편차를 크게 줄일 수 있었다.

참 고 문 헌

[1] Computer Emergency Response Team(CERT), "CERT Advisory CA-2000-01 Denial-of-service developments," http://www.cert.org/advisories/CA-2000-01.html, Jan. 2000.

[2] "Project IDS - Intrusion Detection System," http://www.cs.columbia.edu/ids/index.html, 2002.

[3] Computer Emergency Response Team(CERT), "CERT Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections," http://www.cert.org/advisories/CA-1995-01.html, Jan. 1995.

[4] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson, "Practical network support for IP traceback," in Proc. of ACM SIGCOMM, pp. 295~306, Aug. 2000.

[5] Dawn Xiaodong Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," in Proc. IEEE INFOCOM, April. 2001.

[6] David A. Curry, "UNIX System Security," Addison Wesley, pp. 36~80, 1992.

[7] Computer Emergency Response Team(CERT), http://www.cert.org/index.html, 2002.

[8] G. Sager. Security Fun with Ocxmon and Cflowd. Presentation at the Internet 2 Working Group, Nov. 1998.

[9] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," RFC 2267, Jan. 1998.

[10] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," In to appear in Proceedings of thje 2000 USENIX Security Symposium, Denver, CO, July. 2000.

[11] S. M. Dellovin, "The ICMP Traceback Mess ages," Internet Draft: draft-bellovin-itrace-00.txt, http://www.research.att.com/~smb, Mar. 2000.

〈著者紹介〉

김 병 룡 (Byung-yong Kim)
2000년 2월 : 건양대학교 컴퓨터공학과(이학사)
2002년 2월 : 인하대학교 전자계산공학과(공학석사)
2002년 3월~현재 : 인하대학교 전자계산공학과 박사과정
<관심분야> 정보보호, 무선 프로토콜, P2P

김 수 덕 (Soo-Duk Kim) 학생회원
2000년 2월 : 인하대학교 산업공학과(이학사)
2002년 8월 : 인하대학교 전자계산공학과(공학석사)
2002년 2월~현재 : (주)안철수연구소 연구원
<관심분야> 정보보호, 네트워크 보안, 시스템 보안

김 유 성 (Yoo-Sung Kim) 정회원
1986년 2월 : 인하대학교 전자계산공학과(이학사)
1988년 2월 : 한국과학기술원 전산학과(공학석사)
1992년 2월 : 한국과학기술원 전산학과(공학박사)
1992년 8월~현재 : 인하대학교 정보통신공학부 부교수
<관심분야> 멀티미디어 정보검색, ebXML, 정보보호

김 기 창 (Ki-chang Kim)
1984년 6월 : California State Polytechnic University at Pomona, 전산학, 학사
1988년 6월 : University of California at Irvine, 전산학, 석사
1992년 3월 : University of California at Irvine, 전산학, 박사
1992년 4월~1994년 8월: IBM T.J. Watson 연구소, 연구원
1994년 9월~현재 : 인하대학교, 정보통신공학부 부교수
<관심분야> 컴퓨터 시스템보안, 유무선 네트워크 보안, 실시간 운영체제, 병렬화 컴파일러