선택적 라우터를 이용한 역추적 시스템의 설계

이 정 민* · 이 균 하*

요 약

최근 인터넷 사용자의 증가와 빠른 기술 개발로 인해서 많은 보안상의 문제가 발생하고 있다. 인터넷 망 자체가 보안보다는 속도를 중시한 구조이기 때문에 원천적으로 악의적인 공격에 취약한 구조를 가지고 있고, 이를 노리는 공격은 컴퓨팅 능력의 향상에 힘입어 점점 고도화, 지능화되어가고 있다.

본 논문에서는 네트워크 상에서 효과적으로 침입자를 역추적하는 방법을 제안하고, 필요한 기능 구성요소에 대해 논한다. 제안한 선택적 라우터를 이용한 역추적 시스템에서는 관리가 가능한 라우터들과 매니저 시스템으로 망을 구성하여 역추적을 작업을 수행한다. 선택된 라우터는 모든 패킷에 자신의 라우터 ID를 마킹하여 효과적으로 공격경로를 재구성할 수 있고, 그 피해를 줄일 수 있는 장점을 가지고 있다.

Design of Traceback System using Selected Router

Jeong-Min Lee* · Kyoon-Ha Lee*

ABSTRACT

as increasing of Internet user and fast development of communication, many security problems occur. Because of Internet is design and development for speed not security, it is weak to attack from malicious user. furthermore attack is more developed to have high efficiency and intelligent.

We proposed effective traceback system in network and consider that ability of constitution. Traceback by Selected Router system is consists of managed router and manager system. Selected router marks router ID to packet which passing selected router, and use this router ID for traceback and filtering. Consequently this system reduce damage of attack.

* 인하대학교 전자계산공학과

1. 서 론

인터넷에서는 자신의 위치를 나타내기 위해서 IP(Internet Protocol)의 주소값을 사용한다. 하지만 공격자가 자신의 위치를 숨기는 IP Spoofing 등의 방법이 등장함으로써, IP 역추적 기술은 어느 정도의 한계에 직면하게 되었다[2]. 따라서 패킷에 있는 IP 주소 이외의 다른 정보가 사용되는 방법이 연구되었지만, 이런 방법들은 공격 경로를 재구성하는데 필요한 시간이 걸린다는 문제에 직면하게 되었다. 본 논문에서 제안하는 선택적 라우터를 이용한 역추적 시스템(Traceback system by selected router : TBSR)은 기존의 IP 역추적 기법들보다 적은 비용으로 빠르게 역추적하는데 중점을 두었다. 제안한 TBSR 시스템은 (D)DoS와 같은 공격 기법을 이용해서 DNS 시스템이나 특정 시스템을 공격할 경우에 피해를 최소화하며 빠르게 그 근원지를 추적할 수 있는 장점을 가지고 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 기존의 역추적 방법들에 대한 개요와 특징을 제시한다. 제 3장에서는 앞에서 제시된 문제점들을 해결하기 위하여 제안한 TBSR 시스템에 대해서 소개를 한다. 그리고 제 4장에서는 모의실험을 보이고 마지막 제 5장에서는 결론과 향후 연구 방향에 대하여 기술한다.

2. 역추적 관련 기법

최근 들어서 인터넷 사용자의 폭발적인 증가로 인해 미처 인지하지 못했던 보안상의 허점들이 드러나게 되었고, 악의적인 의도를 가진 프로그램이나 사용자들이 나타나게 되었다. 이중 대표적인 것이 (D)DoS이다. (D)DoS란 멀티태스킹을 지원하는 운영체제에서 발생할 수 있는 공격방법으로써, 한 사용자가 시스템의 자원을 독점하거나, 모두 사용해서 이 시스템이 다른 사용자들에게 올바른 서비스를 제공하지 못하게 만드는 것을 말한다. 그러므로 (D)DoS 공격이 발생하게 되면 시스템이 원활한 서비스를 제공할 수 없으므로, 이를 재빨리 감지, 문제를 해결하여 사용자들에게 적절한 서비스를 제공할 수 있게 해주어야만 한다. 그러나 공격 기법 자체가 많은 패킷을 보내서 시스템을 마비시키는 것이기 때문에, 조속한 문제 해결을 위해서는 유해한 패킷을 전송하는 발신지를 찾아내야 하며, 이런 기법을 역추적(traceback)이라고 한다.

역추적 기법은 IDS나 IPS(Intrusion Prevent System)와 같이 피해 시스템만을 지켜내는 소극적인 태도의 보안이 아니라, 공격의 근원지를 찾아내어 제 2, 제 3의 재 침입을 막고자하는데 그 목적을 두고 있다.

2.1 Node Append, Node Sampling, Edge Sampling 기법

Node Append와 Node Sampling의 경우에는 라우터의 정보들이 sampling된 형태로 도착하기 때문에 공격 경로를 조합하기 위해서는 많은 양의 패킷이 필요하고, 같은 거리에 있는 multiple attacker의 경우 조건에 맞는 여러 개의 라우터가 존재할 수 있다는 한계점을 가지고 있다. 이 문제를 해결하기 위해서 Edge Sampling은 공격 경로상의 라우터를 개개의 노드가 아닌 공격 경로 상의 edge를 가지고 인코딩을 한다[8]. 32bits의 IP 주소 공간이 2개 필요하고, 5bits의 distance 필드가 요구되기 때문에, 64 비트 이상의 크기를 갖는 edge 정보를 16 비트로 인코딩하는 방식을 사용한다. 이런 인코딩으로 인하여 라우터에 미치는 부하가 크다[9].

2.2 Advanced Marking Scheme 기법

이 기법은 라우터의 전체 IP 주소를 마킹할 필

요성이 없다는 점에 착안하고 있다. Edge Sampling과 가장 큰 차이점은 edge에 라우팅 정보를 기록할 때, 전체 라우터 주소를 쓰는 대신 hash 값을 사용한다는 점이다. hash 함수를 어떻게 쓰는가에 따라 이전 버전의 Advanced Marking Scheme-I과 좀 더 발전시킨 방법의 Advanced Marking Scheme-II가 있다[9]. 전자는 총 16bits의 ID field 값을 11bits의 라우터를 나타내는 hash 값과 거리를 나타내는 5bits의 정보를 담아서 보내는 기법이다. 후자는 hash 값의 충돌문제를 해결하지 못하므로 hash 함수의 수를 늘리고 이를 16bits 내에 표기한다. 예시로 제시된 안은 거리를 위한 5bits, hash 함수를 구별하기 위해 3bits, 나머지 8bits가 IP address 값의 hash 값을 가지게 된다. 그러나 이 방법들은 상위 라우터의 맵을 알고 그에 따른 hash 함수 값을 배정해야하는 문제가 존재한다.

마킹을 기반으로 한 방법들은 기본적으로 지나쳐온 라우터의 정보를 패킷의 IP header의 Identification Field에 실어 보내는 방식이고, 저장할 공간이 작기 때문에 라우터 정보는 분할되어 조각으로 전송하며, 라우터에서 sampling 방식에 의해 확률로서 전송 여부가 처리된다[8]. 따라서 하나의 패킷 당 하나 혹은 그 이하의 라우터 정보만을 가지고 있기 때문에 전체 경로를 추적하기 위해서는 많은 수의 패킷을 수신해야하고, 수신 도중 발생할 수 있는 패킷 유실까지 고려하면 이를 계산하는데 많은 시간이 필요하게 된다는 한계점을 노출시킨다.

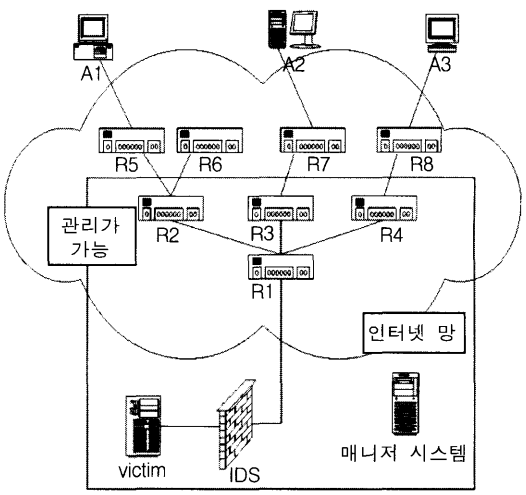
3. 선택적 라우터를 이용한 역추적 시스템(TBSR)

현재 인터넷의 주소로서 사용되는 IP는 빠른 전송을 목적으로 발전 해 왔기 때문에, IP spoofing과 같은 방법을 이용하면 IP 패킷 자체만으로는 추적이 불가능하다. 최근에는 MS-SQL Server Worm이나 W32/Blaster Worm[4]과 같이 바이러스에 의해 시스템을 공격되는 경우가 많아지고 있지만, 이에 대처하기는 쉽지 않다. 이를 추적하기 위해서 앞장에서 살펴본 것처럼 라우터에서 IP 헤더 주소 부분이외에 정보를 이용하는 마킹 기반의 방법들이 연구되어져 왔다.

하지만 마킹을 기반으로 한 방법들은 다음과 같은 문제가 발생할 수 있다. 첫째, 정보를 모으는데 시간이 걸린다. 둘째, 모든 라우터들을 교체해야만 한다. 셋째, 공격자가 ID 필드에 잘못된 정보를 입력하여 속일 수 있다. 마지막으로 모든 라우터들을 관리할 수 있어야만 한다.

3.1 TBSR 시스템 개요

제안하는 TBSR 시스템은 인터넷 망을 구성하는 라우터들은 아래의 그림과 같이 관리가 가능한 것과 관리가 불가능한 것으로 나뉠 수 있다는 점에 착안했다.



(그림 1) TBSR 시스템

기존의 역추적 방법들의 경우 victim에 (D)DoS 공격이 발생했을 때, 역추적 시스템이 R1 혹은 IDS에서부터 추적을 시작하게 된다. (그림

1)의 A1이 vi]ctim에게 공격을 가한 경우 R1 → R2 → R5 → A1의 단계를 거쳐야 한다. 하지만 제안한 TBSR 시스템은 R2, R3, R4의 관리를 통해 R2 → R5 → A1로 추적 과정을 줄 일 수 있고, 이는 공격경로를 재구성하는데 요구되는 시간과 노력을 줄일 수 있다. 또한 R1은 관리나 교체할 필요가 없으며, R2, R3, R4에 필터링 기능을 추가함으로써 피해를 최소화시킬 수 있는 장점을 가지고 있다. 마지막으로 R2, R3, R4를 지나는 모든 패킷은 반듯이 자신의 라우터 ID를 입력하므로 attacker가 IP 헤더의 ID 값을 속이더라도 찾아낼 수 있다.

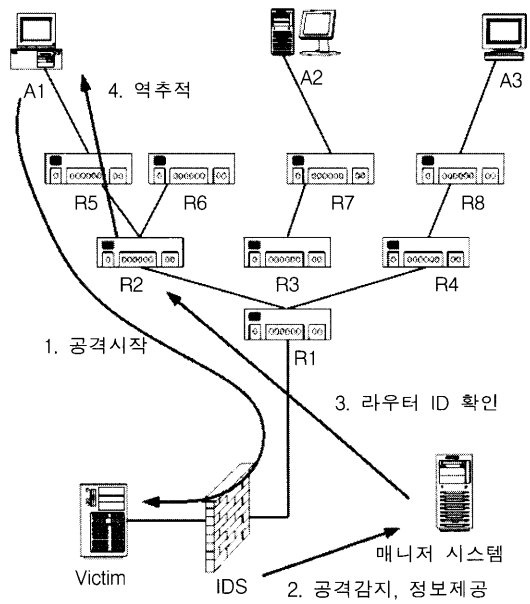
3.2 TBSR 시스템의 구성

제안한 TBSR 시스템은 관리가 가능한 라우터들과 매니저 시스템으로 구성되어져 있다. 관리가 가능한 라우터들은 각각 필터링이 가능하며 기존의 역추적 시스템을 구동시키고 계산이 가능한 능력을 가지고 있어야 한다. 이 라우터들은 (그림 1)의 R2, R3, R4로서 victim으로 향하는 모든 패킷에 자신의 라우터 ID를 마킹하는 역할을 한다. 앞장에서 나온 [8, 9]와 같이 IP 헤더의 Identification 필드를 마킹에 이용한다. 그림1에서처럼 관리가 가능한 라우터 R2, R3, R4를 지나는 모든 패킷의 Identification(ID) 필드에 라우터의 ID 값을 넣어준다. 이럴 경우 특정 라우터를 지나는 모든 패킷의 ID 필드가 반드시 고쳐지므로, 그 이전에 ID 값을 속인다 하더라도 이곳에서 정상적으로 바뀌게 된다. 그리고 특정 패킷만을 고치거나 조건이 주어졌을 경우에만 마킹을 하는 것이 아니기 때문에 라우터에 대한 부담도 감소하게 된다.

매니저 시스템은 이 라우터ID와 역추적을 관리하는 시스템이다. 만일 (그림 1)의 A1이 victim에게 공격을 가할 경우, victim의 IDS가 이를 감지하고 매니저 시스템에게 다음과 같은 세 가지 정보를 제공한다.

victim의 주소
공격 패킷 ID 필드의 router ID 값
공격 패킷 source IP address의 값

매니저 시스템은 위의 정보를 건네받은 후, 라우터 ID 값에 해당하는 라우터에게 위의 조건이 맞는 패킷을 필터링 하도록 명령을 내린다. 이로 인해 같은 attacker에게서 추가적으로 공격 패킷이 victim에 도달하는 것을 막을 수 있다. 그런 후, 이 라우터에서부터 기존의 역추적 알고리즘을 사용해서 원 공격자의 위치를 파악하도록 하면, 기존의 방법보다 공격자와의 거리가 짧아지게 되므로 더 빠르게 위치를 파악할 수 있다.

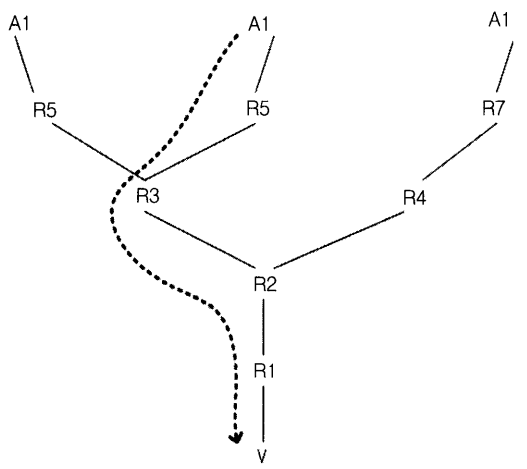


(그림 2) 역추적 순서

4. 성능 비교

MS-SQL Server Worm이나 W32/Blaster Worm과 같이 (D)DoS의 특징을 가지고 있는 바이러

스나 사용자에 의한 (D)DoS의 공격의 경우 라우팅 경로는 아래와 같이 트리(tree)의 구조로 나타내어질 수 있다.



(그림 3) 일반적인 (D)DoS 공격의 경로

이 때 [8, 10]에 의해서 Edge Sampling에서 victim과 hop 수를 d, 라우터가 마킹할 확률이 p일 때, 패킷 도착율은 다음과 같다.

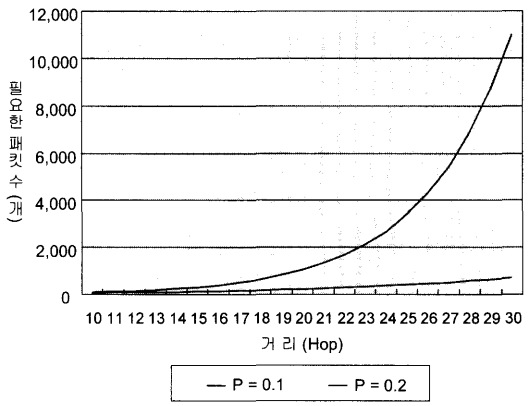
$$E(X) = \frac{1}{p(1-p)^{d-1}} \qquad (1)$$

그렇지만 멀리 떨어진 곳에 있는 라우터의 정보가 근처에 있는 라우터의 정보보다 도착할 확률이 낮아지기 때문에, 공격 경로를 구성하는 것은 가장 멀리 떨어져 있는 라우터의 정보를 모으는 것과 동일하다고 할 수 있다[8]. 이 때 패킷이 라우터의 정보를 가지고 올 확률은 $\frac{1}{dp(1-p)^{d-1}}$ 이 된다[8]. 여기서 잘 알려진 coupon collector problem에 의해서 각각의 라우터에 대한 정보를 얻기 위한 시도 횟수는 다음과 같다[11].

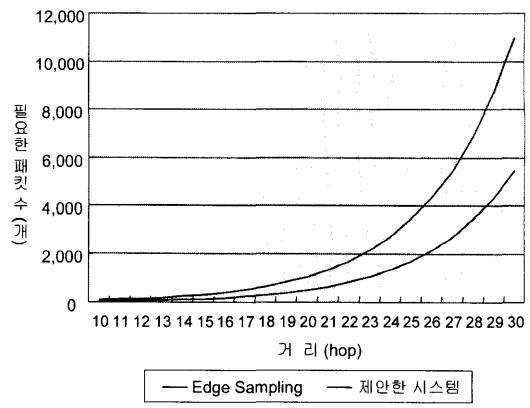
$$d(\ln(d) + O(1)) \qquad (2)$$

식 (1), 식 (2)와 [8, 9]에 의해서 공격 경로를 재구성하기 위한 패킷 수를 구하는 방법은 다음과 같이 식으로 표현될 수 있다.

$$E(X) < \frac{\ln(d)}{p(1-p)^{d-1}} \qquad (3)$$



[8]에 의해서 Edge Sampling의 경우, 위의 차트와 같이 victim과 attacker의 거리가 멀수록 공격경로를 재구성하는데 필요한 패킷의 수가 증가되는 것을 알 수 있다. 제안한 TBSR 시스템은 라우팅 경로에 있는 특정 라우터를 선택해서 관리하는 것이므로 victim과 attacker의 거리가 아닌 특정 라우터와 attacker의 거리를 계산하면 된다. 이럴 경우 거리가 줄어들기 때문에 경로를 구성하기 위한 패킷 수 역시 감소하게 된다.



위의 차트는 제안한 방법과 기존의 마킹 방법을 비교하여 나타낸 것이다. 여기서 확률 P는 0.2로 제안한 TBSR 시스템의 라우터는 victim으로부터 평균적으로 3Hop 떨어진 라우터에 설치되있다고 가정했다. [12, 13-14]에 의해서 최대 25 hop 이상 떨어진 공격자가 존재할 수 있다고 되어있기 때문에 30hop 떨어졌을 경우의 값까지 비교하였다.

5. 결 론

(D)DoS 공격은 인터넷 환경에 있어서 가장 단순한 공격인 동시에 가장 위협적인 공격이다. 아무리 인터넷 환경이 고속 통신으로 발전하고 고성능의 컴퓨터가 나온다고 하더라도 (D)DoS 공격은 막아내기 힘들 것이다. 이런 (D)DoS 공격에 대한 근본적인 대책은 단순히 공격을 막는 차원이 아닌 공격 근원지를 찾아내어 이에 대한 재발을 막는 것이지만 현재의 인터넷 프로토콜이 송신자에 대한 인증이 없고 추적에 대한 정보를 가지고 있지 않다는 문제점이 이를 어렵게 하고 있다.

본 논문에서는 이런 (D)DoS 공격에 대한 공격 근원지를 추적하고 피해를 최소화하는 TBSR 시스템을 제안하였다. 제안한 방안은 기존에 나와있는 방법들을 보완하여 시스템을 구성하여 공격이 발생시에 피해를 최소화고 빠른 시간 내에 공격자를 추적할 수 있는 시스템을 목표로 하고 있다. 가장 핵심이 되는 내용은 특정 라우터를 선택하여 지나는 패킷에 이 라우터에 대한 값을 마킹하여, 공격이 발생했을 때, 찾아올 수 있는 정보를 남기는 것이다. 이를 사용함으로써, 공격 패킷이 지나온 모든 경로를 알 수는 없지만, 하나의 라우터는 정확히 알 수 있게 되고, 이 라우터에서 필터링함으로써, 피해를 최소한으로 줄일 수 있는 장점을 가지게 된다. 그런 후에, 이 라우터로부터 기존에 나와 역추적 기법들을 사용해서 원래의 공격자를 찾을 수 있고, 이때, 지나온 라우터의 수가 감소함으로 적은 비용으로 찾아낼 수 있다. 또한 사용되는 라우터의 수가 많지 않으므로 적은 비용으로 기존의 네트워크 환경에 적용시킬 수 있다는 장점을 가지게 된다.

향후 연구 과제로는 관리되어지는 라우터의 최적화된 개수를 구하는 문제와, ID v6로 이행될 때의 연구가 필요하다.

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, January 2000.

[2] Computer Emergency Response Team(CERT), "CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks", http://www.cert.org/advisories/CA-1996-21.html, Nov. 2000.

[3] Computer Emergency Response Team(CERT), "CERT Advisory CA-2003-04 MS-SQL Server Worm", http://www.cert.org/advisories/CA-2003-04.html, January 2003.

[4] Computer Emergency Response Team(CERT), "CERT Advisory CA-2003-20 W32/Blaster worm", http://www.cert.org/advisories/CA-2003-20.html, Aug. 2003.

[5] David A.Curry, "Unix System Security", Addison Wesley, pp.36-80, 1992.

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

[7] S. M. Dellovin, "The ICMP Traceback Messages", Internet Draft : draft-bellovin-itrace-00.txt, http://www.research.att.com/~

smb, Mar. 2000.

[8] 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.

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

[10] 김병룡, 김수덕, 김유성, 김기창 "마킹 알고리듬 기반 IP 역추적에서의 공격 근원지 발견 기법", 정보보안학회논문지, 제13권, 제1호, 2003.

[11] W. Feller, "An Introduction to Probability Theory and Its Applications (2nd edition)", Wiley and Sons, Vol.1, 1966.

[12] R. L Carter and M. E. Crovellam, "Dynamic Server Selection Using Dynamic Path Characterization in Wide-Area Networks", In Proc. of the 1997 IEEE INFOCOM, Kobe, Japan, Apr. 1997.

[13] W. Theilmann and K. Rothermel, "Dynamic Distance Maps of the Internet", In Proc. 2000 IEEE INFOCOM, Tel Aviv, Israel, Mar. 2000

[14] "Cooperative Association for Internet Data Analysis. Skitter Analysis", http://www.caida.org, 2000.

이 정 민

1999년 인하대학교 전자계산공학과(공학사)

1999~현재 인하대학교 전자계산공학과 통합과정

이 균 하

1970년 인하대학교 전기공학과(공학사)

1976년 인하대학교 전자공학과(공학석사)

1981년 인하대학교 전자공학(공학박사)

1981~현재 인하대학교 전자계산공학과 교수