라우터들간의 협력에 의한 DDOS 공격 탐지 및 대응

최원주, 정유석, 홍만표
아주대학교 정보통신전문대학원
e-mail : brian@madang.ajou.ac.kr

Detection and Response scheme against DDOS attack using the cooperation between routers

Won Ju Choi, Yu Seok Jung, Man Pyo Hong
Dept. of Computer Science, Ajou University

요 약

1999 년 이후 DDOS 공격에 대한 많은 연구가 이루어지고 있고, 지금까지 많은 대응 방안이 제안되었다. 그 중에서 공격이 이루어질 때 라우터의 최소생존성을 기본 가정으로 하고 라우터의 출력 대역폭를 조절하는 방법이 가장 적합한 방안으로 인식된다. 그러나 실제 희생자주위의 라우터들은 과도한 패킷량으로 인한 생존성을 보장 받기 힘들다. 또한 대역폭 제어만으로는 정상 패킷과 공격 패킷의 구분 없이 전체 트래픽량을 조절하기 때문에, 네트워크 노드들의 보호는 가능하지만, 많은 정상 패킷의 손실로 인한 정상 서비스는 불가능하게 된다. 이러한 문제점을 해결하기 위해서 이웃라우터 상호협력을 통한 공격경로의 묘사 방법과 대응 방법에 있어서 특정패킷집단을 정의하고 패턴 필터링을 통한 공격 패킷의 차단 방안을 제안한다.

1. 서론

오늘날 인터넷(Internet)은 일상 생활의 한 부분으로 인식이 되고 있을 만큼 우리 주변에서 쉽게 접할 수 있다. 그러나 인터넷과 네트워크의 발전과 더불어 동반되는 많은 해킹(Hacking) 사례나 보안 침해 사건이 발생하고 있고, 그 기법이나 기술 또한 많이 발전되어 지고 있는 것이 현실이다.

특히 현재 가장 문제가 되고 있는 DDOS(Distributed Denial Of Service) 공격은 그 공격방법이나 공격경로가 특정하게 정해져 있는 것이 아니기 때문에 더 많은 피해와 우려를 낳고 있다.

2000 년 야후나 CNN 같은 대형 사이트들이 이 공격으로 서비스를 하지 못했던 사례를 보면 DDOS 공격의 심각성을 알 수 있다

DDOS 공격이란 그림 1 에서처럼 여러 개의 공격 에이전트(Agent)들이 하나의 공격 대상으로 동시에 많은 양의 패킷(Packet)을 보냄으로써 패킷 처리속도를 저하시키고 결국 패킷 처리마비 상태로 만들어 버리는 공격 형태이다.

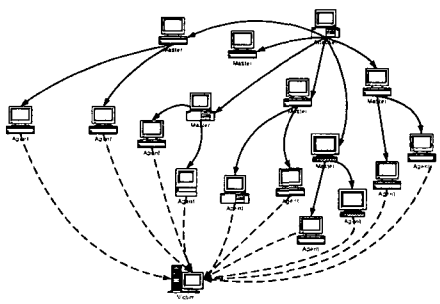

그림 1. DDOS 공격 네트워크

2. 관련연구

DDOS 공격은 실제 네트워크에서 아주 위험한 공격 형태로 간주되고 있으며, 지금 현재에도 많은 네트워크환경에서 DDOS 공격으로 서비스가 중단되거나 네트워크 노드가 사용 불능이 되고 있다. 따라서 현재까지 대응 방안에 대하여 많은 연구가 이루어졌으며, 다양한 방안들이 제시되었다. **Egress/Ingress filtering[6], packet marking[8,10], tracing[10], ICMP traceback[9]**등 이외에도 제안된 많은 방안들이 있다. 최근에 가장 타당성 있는 방법으로 인식되고 있는 방안으로는 공격 시에 라우터의 출력 대역폭(Bandwidth)으로써 패킷 처리양을 조절, 라우터 기반에서 공격에 대응하고자 하는 패킷 처리제한(Rate Limiting)방안이 있다.[2,4,8]

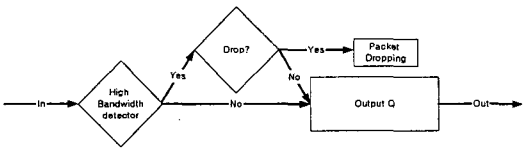

그림 2. 라우터내의 패킷 처리 제한

이 방안은 라우터가 공격에 이용당할 때도 최소한의 기능을 유지한다고 가정하고, 공격에 이용되는 라우터 자신이 공격을 탐지하고, 자체적으로 대역폭을 조절한다. 그러나 현실적으로 그러한 기능들을 가지고 있는 라우터는 많지 않을 뿐더러 희생자 주위의 라우터는 과도한 패킷밀집(Packet Congestion)으로 인하여 최소 생존성을 보장 받기는 어렵다. 라우터의 최소 생존성을 보장 받을 수 없다면 공격에 이용되는 라우터 자신이 공격을 인식하고 자체적으로 대응방안을 구현하기란 불가능하다.

3. 모델

3.1 라우터 상호 진단 기법

1997 년 UCDavis 에서는 라우터 상호 진단 기법[1]을 소개한다. 테스팅(Testing) 라우터에서 테스트(Test) 패킷인 일반 데이터(Data) 패킷의 귀환주소(Return Address)를 자기 자신으로 설정해서 보낸 후, 정해진 시간 안에 돌아오지 않으면 테스티드(Tested) 라우터를 비정상인 라우터로 판별한다.

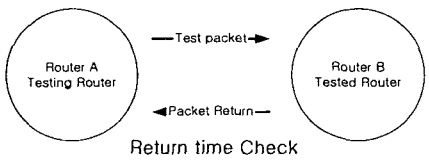

그림 3. 상호 진단 기법

실제 DDOS 공격에서 희생자 주위의 라우터는 많은 공격 패킷으로 인해 그림 4 처럼 패킷 밀집 현상이 발생하게 된다.

패킷 밀집 현상이 발생한 라우터는 이웃라우터(Neighbor Router)에서 보내는 테스트 패킷에 대한 응답으로 정상 데이터 패킷을 송신하게 된다. 그러나 테스티드 라우터의 대역폭을 초과하는 과도한 공격패킷으로 인해 테스트 패킷은 버려지게 된다.

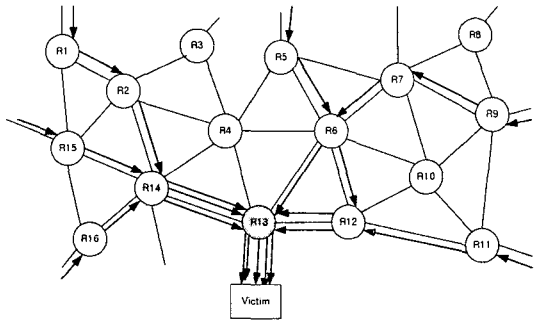

그림 4. 희생자 주위의 패킷 밀집 현상

공격 패킷량이 증가하면 증가할수록 테스트 패킷이 버려질 확률은 높아지게 된다. 희생자 주위의 라우터들의 버퍼(Buffer)는 공격 패킷으로 충분히 점유되어서 다른 정상 패킷을 처리하지 못하기 때문에, 이웃 라우터에서 테스트 패킷을 보내게 되면 응답을 보내지 못한다.

3.2 희생자 주위의 라우터에서의 공격 패킷 함량비

AT&T 에서는 그림 5 와 같은 간단한 네트워크를 구성하여 DDOS 공격 대응방안으로 대역폭 조절 방안의 효율성을 보여주고 있다. 본 논문에서는 이 실험에서 DDOS 공격시 고정된 대역폭에서의 정상패킷과 공격패킷의 함량을 보고자 한다.

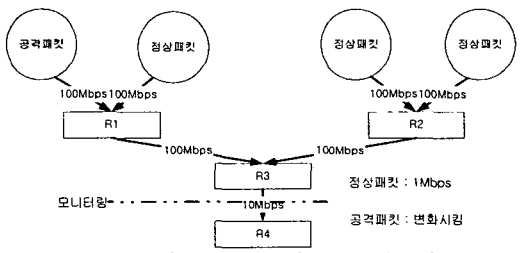

그림 5. 간단한 DDOS 공격 실험 네트워크

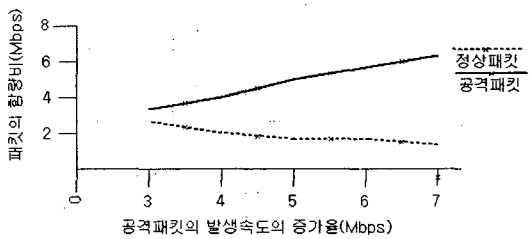

그림 6. 공격패킷 발생속도 변화와 패킷함량비

그림 6 은 정상패킷을 1Mbps 로 고정되게 발생시키고, 공격패킷의 발생 속도를 변화시키면서 공격패킷의 발생 속도의 변화에 따른 라우터 R4 에서의 패킷의 함량을 입력버퍼에서 모니터링(Monitoring)한 값을 도시한 것이다. 공격패킷의 생성 속도가 7Mbps 일때 공격

패킷의 전체 트래픽량에서 차지하는 비율을 계산해보면,

$$6 / (6 + 1.3) * 100 = 82.19\ \%$$

이다. 전체 패킷 트래픽량이 10Mbps 를 넘어가게 되면 패킷량은 라우터의 고정된 대역폭에 의해서 버려지게 되겠지만, 그 이전과정에서 공격패킷의 발생률이 높아지면 정상패킷이 버려질 확률은 더 높아지게 되는 것을 볼 수 있다. 따라서 라우터 R4 는 이웃 라우터로부터 테스트 패킷을 받게 되면 처리하지 못하고 버리게 되고, R4 는 공격에 이용되고 있는 라우터로 판별이 된다.

3.3 탐지 모델

그림 7 을 보면 정상적인 상태(좌측)에서 라우터 R4 와 R3 는 상호 테스트 관계에 있다. 그러나 라우터 R3 가 공격에 사용되게 되면(우측) 공격 패킷으로 인한 과도한 트래픽량으로 인해 라우터 R4 에서 보내는 테스트 패킷을 되돌려 보내지 못하고 버리게 되고, R4 는 응답 패킷을 받지 못하게 된다.

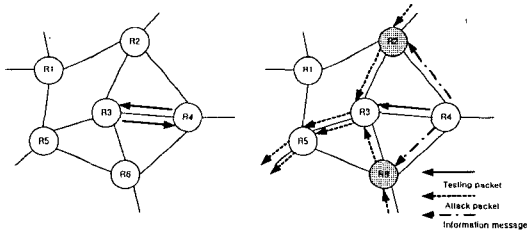

그림 7. 탐지 및 대응 모델

라우터 R4 는 R2 와 R6 에게 R3 가 DDOS 공격에 사용되고 있음을 알리고, R2 와 R6 는 자신의 출력 대역폭을 조절한다. 공격의 중간 단계에 있는 라우터 R3 의 최소 생존성이 보장되지 않더라도 문제가 되지 않는다.

그러나 무작위적으로 패킷들을 라우터의 대역폭 이상은 버림으로써 정상 서비스 패킷까지 버려지게 되어 네트워크 노드들의 보호는 가능하지만, 정상 서비스는 완전하게 보호 받을 수 없다. 결론적으로 DDOS 공격은 이루어진 것이다.

3.4 대응 모델

위에서 언급한 바와 같이 이웃 라우터에서 테스트 패킷을 보내서 공격에 이용되는 라우터를 탐지한 이후 특정패킷집단(Aggregation)의 패턴(Pattern)으로 필터링(Filtering)을 함으로써 공격 패킷과 정상 패킷을 구분하여 공격 패킷만을 버린다면 DDOS 공격을 막을 수 있다.

특정패킷집단이란 같은 성격을 가진 패킷들의 묶음이다. 예를 들어서 TCP SYN 패킷이 정해진 시간에 일정량으로 보내어진다면, 이러한 SYN 패킷을 하나의 묶음으로서 특정패킷집단이라고 정의한다.

특정패킷집단은 표 1 과 같이 시간 기반과 콘텐츠 기반, 2 가지로 나눌 수 있다.

Aggregation property	
Contents Based property	1) TCP SYN 패킷 2) UDP 패킷 3) ICMP ECHO 패킷 4) Etc
Time Base property	1) 같은 TTL 을 가진 패킷 2) 같은 시간안에 생성된 패킷 3)Etc

표 1

특정패킷집단을 정의하기 위해선 많은 양의 패킷을 모니터링해야 하는데, 네트워크의 과부하(Overhead)를 줄이기 위해서 패킷의 헤드(Head)만을 본다. 또한 지나가는 모든 패킷을 모니터링하지 않고, 일부 패킷을 선택적으로 모니터링 할 수 있다.

특정패킷집단의 패턴으로 필터링한다면 공격 패킷과 정상 패킷을 구분할 수 있으므로 공격 패킷만을 버릴 수 있다. 즉 정상 패킷의 정상 서비스 처리를 보장한다.

그림 7 의 라우터 R4 에서 라우터 R3 가 공격에 이용되고 있음을 라우터 R2, R6 에게 알려주면 특정패킷집단의 패턴을 추출, 라우터 R4 를 통해서 패턴을 비교, 분석하여 필터링함으로써 공격 패킷에 대한 필터링이 가능하다. 공격패킷은 라우터 R2, R6 에서 버려지게 되고, R3 에서는 패킷밀집 현상이 사라지게 된다.

R4 에서 R3 가 공격에 이용되고 있음이 인식되면 R6 와 R2 로 보낼 정보 메세지(Information Message)는 그림 8 과 같이 구성된다.

테스트패킷을 받은 라우터 ID
테스트패킷을 보낸 라우터 ID
공격 패킷의 특정 패킷집단 패튼
필터링 실행 여부(0/1)

그림 8. 정보 메시지

라우터 R4 에서 R3 로의 테스트는 항상 이루어지는 것은 아니다. 네트워크의 과부하를 고려해서 정상일 때와 공격이 탐지되었을 때에는 테스트의 횟수에 차이를 두어야 한다.

필터링의 실행 여부 또한 네트워크의 과부하를 고려해야만 한다. 공격이 인식되고 난 후, R4 에서 R3 으로의 테스트는 계속적으로 이뤄지게 되는데, R3 에서 패킷의 밀집이 계속적으로 존재하게 되면 '1'로 설정되어서 보내지게 되고, 더 이상 패킷 밀집이 존재하지 않게 되면 '0'의 값으로 보내지게 된다. '1'로 설정되어 있으면 상위 라우터에서의 필터링은 계속 된다. 그리고 '0'으로 설정되어지면 필터링은 끝나게 된다. 즉 R3 에서 패킷 밀집이 사라진 후 정보 메시지는 필터링 실행 여부을 위해서 마지막으로 한번 더 보내어진다. 이웃 라우터에서 패킷의 밀집으로 인한 공격의 인식여부에서 필터링까지 과정은 자동적으로 이루어지게 된다.

현재의 라우터들은 'Hello' 패킷등과 같은, 라우터간

의 상태 여부를 묻는 패킷을 보내지만, 그러한 패킷들의 처리 순위는 일반 데이터 패킷보다 높으므로 라우터가 고정된 대역폭를 가지고 생존하는 순간에는 라우터의 상태는 이상이 없는 것으로 판단된다. 반면 본 논문에서 제시한 테스트 패킷은 일반 데이터 패킷으로서 DDOS 공격 하에 라우터에서 일어나는 패킷의 밀집을 탐지하는데 효과적이다.

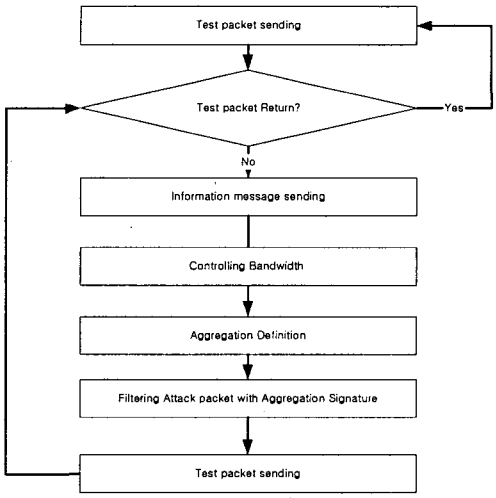

그림 7. 공격 탐지 및 대응 흐름.

4. 논의및 결과

이제까지 라우터의 기본 생존성을 보장 받지 못할 경우 이웃 라우터와 서로 협력을 통해서 라우터의 패킷 밀집 현상을 이용하여, 테스트 패킷을 보냄으로써 패킷의 리턴(Return) 여부를 보고 공격에 이용되는 라우터 탐지 기법을 제안했다.

공격의 탐지 이후 공격에 이용되고 있는 라우터의 출력 대역폭을 조절함에 있어 특정패킷집단의 패턴을 추출해서 정상패킷과 공격 패킷을 분리하여 필터링함으로써 실질적인 네트워크 서비스가 가능하게 하는 방안을 제안했다.

	공격시 라우터의 생존성 가정	과중한 네트워크 부하 (Overhead)	네트워크 노드들의 지능화 (Intelligent-ialization)
Egress/Ingress filtering[6]		O	O
packet marking[8,10]	O	O	O
tracing[10]	O	O	O
ICMP traceback[9]			O
Rate limiting[2][4][8]	O	O	O
본논문에서 제안한 방안			O

표 2. 기존 방안들과의 비교

표 2 는 이미 제안된 라우터 기반의 대응 방안들과 본 논문에서 제안한 방안을 비교한다.

DDOS 공격 네트워크의 탐지 방법에 있어서 네트워크 과부하를 고려할 때 테스트 패킷의 전송 횟수와 패킷 밀집이 발생하는 라우터에서의 패킷 버림의 비율은 계산으로는 적용하기가 힘든 상황이므로 앞으로 실험을 통한 정확한 수치의 값이 필요하다.

또한 라우터 상호간의 협력을 요구함으로써 현재 네트워크상에서 직접 적용하기는 힘들다. 따라서 지능적인 라우터를 기반으로 한 네트워크가 기본 바탕이 되어야 한다. 이는 차후 앞으로 네트워크가 발전되어가는 방향과 같은 입장이 될 것이다.

참고문헌

[1] Steven Cheung, Karl N. Levitt,. "Protecting Routing Infrasturcture from Denial of Service using Cooperative Intrusion Detection" Ucdavis 1997.

[2] John Ioannidis, Steven M. Bellovin. "Pushback: Router-Based Defense Against Ddos Attacks" AT & T Labs. 2001.

[3] Yin Zhang and Vern Paxson. "Detecting Stepping Stones"

[4] Ji-Young Song. "A mechanism to DDOS Attack on a Router Defense Using the Survivalility" Soongsil University. SAM'02 2002

[5] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Olsson, "Detecting Disruptive Router : A Distirbuted Network Monitoring Approach." Ucdavis. 1998

[6] Kihong Park and Heejo Lee, " On the Effectiveness of Route-Based Packet Filtering for Distributed DOS Attack Prevention in Power-Low Internets," ACM SIGCOMM'01, 2001.

[7] Robert Storm, "Center Truck: IP overlay network for tracking Dos flooding", October 1999.

[8] Ratul Matajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, vern Paxson, and Scott Shenker. "Controlling high · bandwidth aggregates in the network" ACM SIGCOMM 2001.

[9] Steve M. Bellovin." ICMP Traceback Messages." Work in Progress, Internet Draft draft-bellovin-itrace-00.txt, March 2000.

[10] Stepan savage, David Wetherall, Anna karlin, and Tom Anderson, "Practical Network Support for IP Traceback,"