서비스 거부 공격 대응을 위한 위험 탐지 모델링

문경원° 황병연
가톨릭대학교 컴퓨터공학과
{kwmoon°, byhwang}@catholic.ac.kr

Risk Detection Modeling Against DoS Attacks

Kyung-won Moon° Byung-yeon Hwang
Dept. of Computer Engineering, The Catholic University of Korea

요 약

인터넷 기술의 발전과 더불어 서비스 거부 공격(DoS : Denial of Service) 방법과 유형이 날로 다양해지고 있다. DoS 공격은 사용자 시스템에 네트워크 트래픽의 과도한 부하를 주어 서비스를 마비시키거나 시스템을 다운시킨다. DoS공격은 빠른 시간 안에 시스템을 위협하는 특징 때문에, 빠른 대처가 필요하다. 이러한 점에 착안하여 본 논문에서는 DoS 공격상황에서의 위험상황을 모델링 한다. 제안된 모델링은 패킷분석에 기반하여 의미 있는 요소들을 찾아내고, 수식화해서 위험 탐지 모델을 정의한다. 제안된 모델링을 통해서 DoS공격을 효과적으로 대처할 수 있을 것으로 기대된다.

1. 서 론

최근 컴퓨터 시스템의 공격경향은 자동화, 분산화되고 있다. 이러한 공격 경향은 시스템에 큰 피해를 불러일으키며 특히, 서비스 거부(DoS : Denial of Service)공격은 인터넷상에서 가장 치명적인 위협 중에 하나이다. 이러한 DoS 공격은 대량의 패킷을 네트워크로 보내서 호스트의 메모리, 프로세스, 네트워크 자원과 같은 시스템 자원을 고갈시키고 이로 인해 정상적인 트래픽에 대한 서비스마저 제공하지 못하게 하는 공격이다[1]. DoS의 한 형태로 DDoS(Distributed Denial of Service)[2]는 다중의 공격 에이전트를 사용해서 더 많은 양의 네트워크 트래픽을 발생시켜 빠르게 시스템을 다운시킨다. 하지만 현재 DoS 공격에 효과적으로 대처하지 못해 그 피해는 엄청난 규모로 커지고 있다. 관련 프로그램들이 나와 있기는 하지만 대부분 DoS가 발생하고 나서 대처하는 수준이며, 미연에 예방하는 시스템은 없는 실정이다. 따라서 효과적인 대처와 예방이 절실한 시점이다.

본 논문에서는 DoS의 급진적인 특성에 초점을 두어 시스템의 치명적인 상태를 위험 탐지 모델을 통해 제시한다. 현 시스템과 위험 탐지 모델간의 비교를 통해 시스템이 얼마나 치명적인 상태에 도달해 있는가를 제시해 줌으로써 DoS에 보다 효과적으로 대처할 수 있는 기준을 제공하고자 한다.

2. 관련연구

DoS 공격에 대처하려면 우선 DoS의 유형을 알아보고 그 특성을 파악하는 것이 중요하다. 대표적인 DoS공격의 2가지 공격 형태의 특징을 알아보겠다.

UDP Flooding 공격[2]은 2003년 1월 우리나라를 떠들썩하게 했던 MS-SQL 보안의 취약점을 틈타 발생했던 대표적인 DoS공격 형태이다. 목적 포트 번호를 19로 셋팅해 서브 넷의 브로드캐스트 주소 값을 목적지로 보내지는 UDP 데이터그램(Datagram)과 변형된(속임수를 쓴) 원천 IP(Source IP) 주소 값으로 구성돼 있다. 단순한 TCP/IP 서비스를 수행하는 윈도우 NT 컴퓨터는 각각의 브로드캐스트에 모두 응답하는데, 그 양이 많을 경우 UDP 데이터그램의 홍수사태가 발생하여 시스템이 더 이상 서비스를 할 수 없는 상태에 이른다.

SYN Flooding 공격[3,4]은 TCP/IP의 3-handshake기법의 취약점을 이용한 공격 방법인데, 공격 목표가 되는 시스템으로 수천개의 TCP 접속(SYN) 요청 메시지를 보낸다. 이 때 이 패킷내부의 소스 IP 주소 값을 속이거나, 인터넷상에서 사용하지 않는 IP 주소 값으로 변형한다. 그러면 목표가 되는 시스템은 새로운 접속을 맺기 위해 실제로는 존재하지 않거나 동작하지 않는 IP 주소 값으로 ACK응답을 한다. 그런 다음 SYN-ACK 메시지가 ACK를 보낸 시스템으로부터 올 때까지 기다리게 되는데, 목표가 된 컴퓨터는 SYN-ACK 메시지를 절대 받지 못하게 되며 버퍼와 같은 자원을 계속 종료하지 않고 열어 두게 되는데, 계속 누적될 경우 결국은 시스템이 멈추어버리거나 서비스를 중단하는 사태가 발생하는 것이다.

이러한 SYN Flooding 공격은 DoS 공격의 90%이상을 차지하는 주된 공격 방법이다. 따라서 본 논문에서는 SYN Flooding공격에 집중해서 위험 탐지 모델을 기술해 나간다.

위의 2가지 대표적인 DoS공격 유형의 특성에서 살펴보았듯이 공격의 경향이 특정 포트를 공격한다든지, 원천 IP를 속여서 서비스 요청을 하는 등의 DoS대처에 있어 중요한 요소들을 파악할 수 있다[5,6].

3. 위험 탐지 요소

DoS 공격 상황에서는 패킷의 양(P)이 중요한 요소로 선정될 수 있는데, 일정 시간동안에 시스템이 처리할 수 있는 최대 패킷의 양과 현재의 패킷의 수로 표현 되어진다.

$$P = \frac{The\ number\ of\ packets}{Maximum\ packet\ Capacity} \quad - (1)$$

원천 IP와 관련해서는 3가지의 속성을 찾아 낼 수 있는데, 로컬 IP의 등장 빈도(Local IP Rate, **LIR**)와 동일한 원천 IP(Same Source IP Rate, **SSIR**)의 등장 빈도, IP의 무작위적인 분포정도(Randomness Distribution, **RD**)의 정보들이다.

$$LIR = \frac{The\ number\ of\ local\ ip\ packets}{The\ total\ number\ of\ packets} \quad - (2)$$

$$SSIR = \frac{The\ number\ of\ same\ ip\ packets}{The\ total\ number\ of\ packets} \quad - (3)$$

$$RD = \frac{The\ number\ of\ kind\ of\ ip}{The\ total\ number\ of\ packets} \quad - (4)$$

포트와 관련해서는 동일한 목적 포트(Same Destination Port, **SDP**)의 등장 빈도와 동일한 원천 포트(Same Source Port, **SSP**)의 등장 빈도 등의 정보를 알 수 있는데, 이들 정보들은 동일한 공격 루트에 대한 검사를 수행한다.

$$SDP = The\ total\ number\ of\ same\ destination\ port \quad - (5)$$

$$SSP = The\ total\ number\ of\ same\ source\ port \quad - (6)$$

표 1 SDP 와 SSP의 위험도

# of SDP	위험도	# of SSP	위험도
1	100%	1	100%
2-5	80%	2-5	80%
5-10	60%	5-10	60%
10-20	40%	10-20	40%
20-30	20%	20-30	20%
30이상	0%	30이상	0%

표 1은 SDP와 SSP의 개수에 관련해서 시스템의 위험도를 나타내주고 있다. SDP의 개수가 1개이면 공격을 하는 목적 포트가 하나라는 것이므로 100%의 위험도를 갖게 된다. SSP도 같은 맥락에서 SDP의 위험도와 같이 적용된다.

Code bits에서의 SYN과 ACK의 정보는 데이터에 대한 용도와 내용에 관련한 정보를 포함하고 있는데, SYN 플래그를 가지는 패킷의 비율(SYN Flag Rate, **SFR**)은 SYN Flooding에 대한 검사를 수행한다. 또한 데이터가 Null인 ACK 패킷의 비율(Null ACK Packet Rate, **NAPR**)은 공격 시에 데이터에 아무것도 넣지 않고 보내오는 것에 대한 검사를 수행한다.

$$SFR = \frac{The\ number\ of\ SYN\ Flag\ packets}{The\ total\ number\ of\ packets} \quad - (7)$$

$$NAPR = \frac{The\ number\ of\ null\ data\ packets}{The\ total\ number\ of\ packets} \quad - (8)$$

(1) ~ (8)의 8가지 요소를 선정해 보았다. 이 제약들은 SYN Flooding과 같은 DoS공격을 감지하기 위한 의미 있는 정보들이다. 이렇게 선정한 요소들 간의 가중치를 선정하는 작업이 필요하다.

4. 위험 탐지 모델

위험 탐지 모델은 표 2에서 보는 바와 같이 정의된 8개의 요소들의 가중치의 합으로 0-100%의 값으로 표현되어 진다. 100%에 가까울수록 위험한 상황이며, 취할 수 있는 행위도 제약적이 된다.

표 2 위험 탐지 요소 가중치

요소	요소 가중치
P (Packet의 양)	10%
LIR (Local IP Rate)	10%
SSIR (Same Source Ip Rate)	10%
RD (Randomness Distribution)	20%
SDP(Same Destination Port)	20%
SSP(Same Source Port)	10%
SFR(SYN Flag Packets Rate)	10%
NAPR(Null Ack Packets Rate)	10%
위험 탐지 모델	100%

A = {P, LIR, SSIR, RD, SDP, SSP, SFR, NAPR},

A는 위험 탐지 요소의 집합이며, A의 위험도(Risk)는 각 요소의 가중치의 합으로 표시되어 진다.

$$Risk(A) = \sum_{i=0}^{n} AttributeWeight_i \quad - (9)$$

n = 위험 탐지 요소의 개수

패킷에서 얻을 수 있는 정보를 가지고 위험 탐지 요소를 선정해 보았고 그 요소들을 가지고 위험 탐지 모델을 정의해 보았다. 정의한 모델을 가지고 시스템의 위험도를 표 3의 예시를 통해 계산해보면 다음과 같다.

표 3 위험 탐지 요소 예

P	LIR	SSIR	RD	SDP	SSP	SFR	NAPR
27/45	30%	50%	10%	7개	25개	60%	5%

$$Risk(A) = (\frac{60}{100} \times 10) + (\frac{30}{100} \times 10) + (\frac{50}{100} \times 10) + (\frac{10}{100} \times 20) + (\frac{60}{100} \times 20) + (\frac{20}{100} \times 10) + (\frac{60}{100} \times 10) + (\frac{5}{100} \times 10) = 36.5\%$$

위의 상황에서의 위험도는 36.5%이다.

위와 같은 위급상황에 대한 수치적인 표현은 실제 DoS공격 상황에서의 위급함에 대한 지표가 된다.

다음 장에서는 실제로 위험 탐지 모델을 시뮬레이션을 통해 알아보도록 하겠다.

5. 실험 및 구현

위험 탐지 모델을 간단한 시뮬레이터를 통해 구현해 보았다. 실험환경은 다음과 같은 상황에서 이루어졌다.

CPU : 1GHz Single CPU
OS : Windows 2000 Server
Laguage : Java (JDK1.4.2)

Input 데이터의 형태는 다음과 같다.

27|30|50|10|7|25|60|57

값은 좌측부터 P(%), LIR(%), SSIR(%), RD(%), SDP(개), SSP(개), SFR(%), NAPR(%) 값을 의미한다.

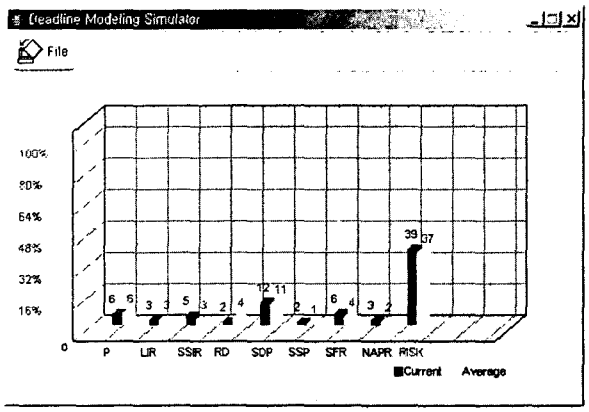

그림 1 위험 탐지 모델링 시뮬레이터

위험 탐지 모델 시뮬레이터는 앞에서 설계한 위험 탐지 모델 객체와 각 요소들의 입력을 통해 실험을 하게 된다. 계산된 결과는 그래프의 형태로 나타내어지며, 종합적인 위험도는 Risk로 표현하여 나타내어 주게 된다. 시뮬레이터는 그림 1에서 보는바와 같은 GUI를 가지고 있다. 그래프는 현재상황(Current)과 누적평균(Average) 수치의 2가지로 나타내어진다. DoS에 대한 공격감지와 대처에 있어 현재상황에 대한 위험도도 중요 하겠지만, 누적평균 또한 중요한 참고가 될 수 있을 것이다.

6. 결론

DoS 공격의 급진적인 특성 때문에 시간의 제약을 받아 왔고, 실시간적으로 시스템의 위험함의 정도를 알 수 있는 모델이 필요하게 되었다. 시스템 공격 기술의 발전과 더불어 앞으로도 많은 피해가 예상되는 DoS 공격에 대비하기 위해서는 DoS에 대한 명확한 인식과 기반 지식의 숙지가 절실하다. 대부분의 기업에서는 DoS의 공격에 대한 대비책으로 방화벽을 채택하고 있으나 급변하고 진화하는 공격형태에 대처하기에는 방화벽으로는 미흡하다.

본 논문에서는 DoS의 공격의 특성을 기반으로 의미 있는 요소를 찾아내고 요소들 간의 계산을 통해 시스템의 위급성을 진단할 수 있는 모델을 제안하였다.

향후 연구에서는 본 논문에서 제시한 위험 탐지 모델을 적용하여 실시간으로 시스템의 위급함을 모니터링해줄 수 있는 솔루션을 개발할 것이다.

[참고문헌]

[1]CERT, "Denial of Service Attacks," http://www.cert.org/tech_tips/denial_of_service.html, 1997.

[2]이철호, 최경희, 정기현, 노상욱,"웹 서버에 대한 DDoS공격의 네트워크 트래픽 분석," 정보처리학회논문지C, 제10-C권, 제3호, pp.253-264, 2003년 6월.

[3]Chang and R.K.C., "Defending against flooding based distributed denial-of-service attacks: a tutorial," IEEE Communications Magazine, Vol. 40, No. 10, pp.42-51, Oct 2002.

[4]정연광, 문종욱, 최경희, 정기현, 임강빈, "SYN Flooding 공격 상황에서 적합한 패킷선정을 위한 엔진 모듈," 한국정보처리학회 추계학술발표대회 논문집, 제10권, 제2호, pp.1929-1932, 2003년 11월.

[5]C. L. Schuba, I. V.Krsul, M. G.Kuhn, E. H.Spafford, A. Sundaram and D. Zamboni, "Analysis of a Denial of Service Attack on TCP," IEEE Symposium on Security and privacy, 1997.

[6]오성민, 홍충선, 이대영, "DDoS 공격에 대처하기 위한 효율적인 패킷 필터링 방안," 한국정보처리학회 추계학술발표대회 논문집, 제10권, 제2호, pp.1125-1128, 2003년 11월.