다중 침입 탐지 시스템 간 협력을 이용한 DDoS 공격 방어 메커니즘

류재현°, 송병학, 홍충선
경희대학교 컴퓨터공학과

DDoS Attack Defense Mechanism Using Collaborative Instrusion Detection System

Jae Hyun Ryu°, Byung Hak Song, Choong Seon Hong,
Department of Computer Engineering, Kyung Hee University
{jhryu, bhsong, cshong}@khu.ac.kr

요 약

DDoS(Distributed Denial-of-Service) 공격은 인터넷 침해 가운데 가장 위협적인 공격들 중 하나이며 이러한 공격을 실시간으로 방어하기 위한 연구는 활발히 이루어져 왔다. 그러나 분산된 공격 형태를 가지는 DDoS 공격을 특정 침입탐지대응시스템(IDRS)에서 탐지하고 대응하기에는 정확성과 속도 측면에서 한계를 가진다. 뿐만 아니라 기존의 탐지 방법을 피하거나 탐지를 지연시키는 지능화된 DDoS 공격에 대해서 높은 오탐지율을 가진다. 따라서 본 논문에서는 공격자(attacker)와 희생자(victim)의 네트워크에서 가장 가까운 탐지 지점에 위치한 각각의 침입탐지 대응시스템간의 상호 협력을 통한 효과적인 방어 시스템을 제안한다. 또한 탐지 임계값을 서서히 증가시키는 다양한 공격에 대해 조기에 탐지할 수 있는 메커니즘을 제안한다.

1. 서 론

초고속 인터넷 인프라가 구축되면서 해킹 및 인터넷 침해에 대한 사고 사례가 매년 증가하고 있다. 특히 DDoS 공격은 단순한 공격기법과 어디서나 구할 수 있는 툴로 인해 초급해커(Script kiddie)도 얼마든지 공격할 수 있다.

분산된 공격 형태를 가지는 DDoS 공격을 효과적으로 방어하기 위해서는 기존의 독립적이고 고립된 방법으로는 탐지 및 대응이 어려우며 침입탐지대응 시스템간의 상호협력이 필요하다[1]. 기존의 분산 IDRS(Intrusion Detection and Response System)은 특정 공격 형태나 시나리오에 있어서 좋은 성능을 보이지만, 다양하게 변형된 공격 형태[2]에 있어서 높은 오탐지율(false alarm rate)을 가지고 있다.

따라서 본 논문에서는 이러한 문제를 해결하기 위해 탐지의 정확도를 향상시키고 수집된 정보를 바탕으로 효과적으로 대응할 수 있는 메커니즘을 제안한다. 뿐만 아니라 탐지 임계값(threshold)을 서서히 증가시키는 다양한 공격을 조기에 탐지할 수 있는 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 침입탐지 및 대응 기법과 세 가지 비정상 행위 탐지 알고리즘에 대해서 알아보고 3장에서는 통계기반 탐지 기법을 바탕으로 source 네트워크와 victim 네트워크의 IDRS간 협력을 통한 침입탐지 및 대응 기법을 제안한다. 그리고 4장에서는 성능 측정을 하고 5장에서는 본 연구가 가지는 의의로 마무리한다.

* This paper was supported by ITRC and MIC

2. 관련 연구

2.1 침입탐지 및 대응 기법

IDRS는 탐지 위치에 따라서 source 네트워크와 victim 네트워크 IDRS로 구분된다. victim 네트워크의 IDRS는 네트워크의 리소스를 고갈시키는 매우 높은 트래픽 양의 DDoS 공격 형태에 대해서 대응 시간이 오래 걸리고 대응 방법의 계산 복잡도가 높다는 단점이 있다.

반면에 source 네트워크 IDRS[3]는 패킷 필터링(filtering)과 같이 공격에 대응하기에는 가장 효율적인 위치에 있지만 전체 DDoS 공격 트래픽의 일부만을 탐지의 판단 근거로 사용하기 때문에 victim 네트워크 IDRS보다 상대적으로 오탐지율이 높다는 단점이 있다. 그림 1은 source 네트워크와 victim 네트워크 IDRS의 위치를 나타낸다.

이러한 단점을 보완하는 방법들[4][5]이 연구 되

어 왔지만 false positive와 false negative가 높다.

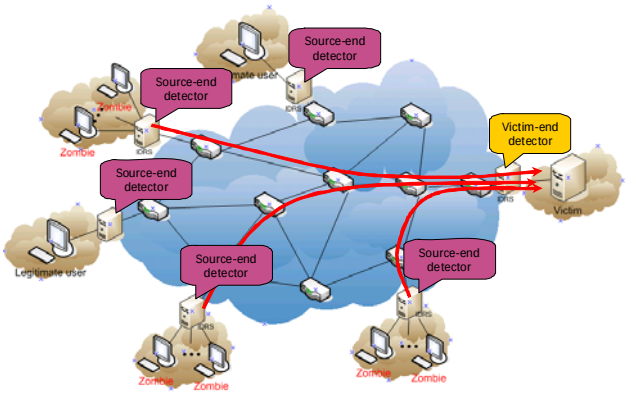


그림 1 Source와 Victim 네트워크 IDRS

2.2 통계기반 탐지 알고리즘

통계적인 탐지 알고리즘에는 트래픽 볼륨(traffic volume),패킷 속성값의 엔트로피(entropy)[6], 카이 제곱(chi-square) 검증법[6]등이 사용되고 있다.

이 가운데 트래픽 볼륨 측정은 패킷이 이더넷 카드(network interface card)에 도착하는 시간을 계산하는 것이다.

$$T = \sum_{i=1}^{n} (PAT[i] - PAT[i-1])$$

위 공식은 각각의 패킷이 도착하는 시간을 측정하여 그룹 단위로 패킷이 도착한 시간을 계산한다. 즉 100개의 패킷을 한 그룹으로 설정을 했다면 100개의 패킷이 이더넷 카드에 도착하는 시간을 측정하는 것이다. 트래픽 볼륨 값이 낮을수록 이더넷 카드에 도착하는 패킷의 수가 증가했다는 것을 의미한다. 이것은 현재의 트래픽이 갑자기 증가했다는 것으로 이상 트래픽 발생 가능성을 암시한다.

다음 엔트로피 연산법은 어떠한 네트워크 속성값에 대한 임의성(randomness)을 계산한 뒤, 그 값의 평균 변화량을 탐지하는 방법이다.

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

위의 공식은 n개의 속성 값에 대한 엔트로피 H를 구하는 공식이다. 여기서 pi는 i번째의 속성값이 선택될 확률을 나타낸다.

카이 제곱 검증법은 속성 값에 대한 분산도를 측정하는 방법이다. 여기서는 기대값에 대한 분산도를 계산하여 그 값에 따라 비정상적인 속성값을 탐지할 수 있다. 이 방법의 구체적인 식은 다음과 같다.

$$x^2 = \sum_{i=1}^{B} \frac{(N_i - n_i)^2}{n_i} \quad , n_i = \frac{n}{B} \quad , n = total\ sample\ size$$

여기서 B는 샘플 패킷들이 가질 수 있는 값들을 묶어놓은 binning 값이다. Ni는 N개의 샘플 패킷에서 각각의 binning 범위에 속하는 패킷의 개수이고, ni는 일반적인 분포에서 binning에 속하는 기대값이다.

3. 협력적인 DDoS 공격 대응 시스템

source 네트워크의 탐지 기법과 victim 네트워크의 탐지 기법 간 협력을 통해 기존의 source 네트워크와 victim 네트워크의 탐지 방법의 단점을 보완하고 탐지 및 대응 성능을 향상 시키는 방법을 제안하다. 뿐만 아니라 지능화된 DDoS 공격 형태에 대한 탐지 메커니즘을 제시한다.

3.1 Source 네트워크에서의 침입 탐지

Source 네트워크의 탐지 구조는 크게 두 가지 모듈로 구성된다. 하나는 IP 스푸핑(spoofing) 검사 모듈이고 다른 하나는 DDoS 공격 탐지 모듈이다.

IP 스푸핑 검사 모듈은 outgoing 트래픽에 대해서 자신이 속한 서브넷이 아닌 소스 IP 주소를 가진 패킷을 필터링한다. 그래서 좀비(zombie) 에이전트는 공격 시 자신의 소스 IP 주소를 외부 네트워크의 IP 주소로 스푸핑 한다면 차단된다.

표 1 통계 감지 알고리즘

Traffic-volume	Rate of source address entropy
$T < T_t$ T : traffic volume T_t : threshold of traffic volume	$\frac{H_s(s)}{H_s(r)} > T_{H_s}$ $H_s(s)$: source address entropy of sent packets $H_s(r)$: source address entropy of received packe T_{H_s} : threshold of source address entropy
Chi-square	Rate of destination address entropy
$x^2(s) > T_{x^2}$ $x^2(s)$: chi – square of sent packe T_{x^2} :threshold of chi-square	$\frac{H_d(s)}{H_d(r)} < T_{H_d}$ $H_d(s)$: destination address entropy of sent packets $H_d(r)$: destination address entropy of received packe T_{H_d} : threshold of destination address entropy

DDoS 공격 탐지 모듈은 표1에서 언급한 트래픽 볼륨, 소스 주소 엔트로피, 카이 제곱, 그리고 목적지 주소 엔트로피 값은 이용하여 계산한다. DDoS 공격 시 전체 트래픽에 대한 T값은 감소하고 Victim의 응답 패킷이 증가하므로 소스 주소 엔트로피 값은 감소하게 된다. 그리고 좀비 에이전트가 보내는 트래픽의 증가로 송신하는 소스주소 엔트로피와 카이 제곱 값은 증가한다. 따라서 Hs(s)/Hs(r) 과 x2(s) 값은 급격히 증가한다. 그리고 목적지 주소 엔트로피는 소스 주소 엔트로피와 반대의 특성을 가지기 때문에 Hd(s)/Hd(r) 값은

$$\mu_n(x) = \alpha\mu_{n-1}(x) + (1-\alpha)\mu_{n-2}(x) \quad , 0 < \alpha < 1$$

$$T(x) = \mu_n(x) + k\sigma(x) \quad , k = 1, 2, 3\cdots$$

$$where\ x = T,\ \frac{H_s(s)}{H_s(r)},\ x^2(s),\ \frac{H_d(s)}{H_d(r)}$$

μ : average

α : weighted value

σ : standard deviation

급격히 감소한다.

4개의 탐지 모듈의 임계값은 최근 측정값에 가중치를 부여한 평균값과 분산값을 이용하여 동적으로 변화하는 트래픽에 대해 일정한 간격(observation interval)마다 임계값을 산출한다.

그림 2는 source 네트워크의 탐지 기법 과정을 나타낸 순서도이다.

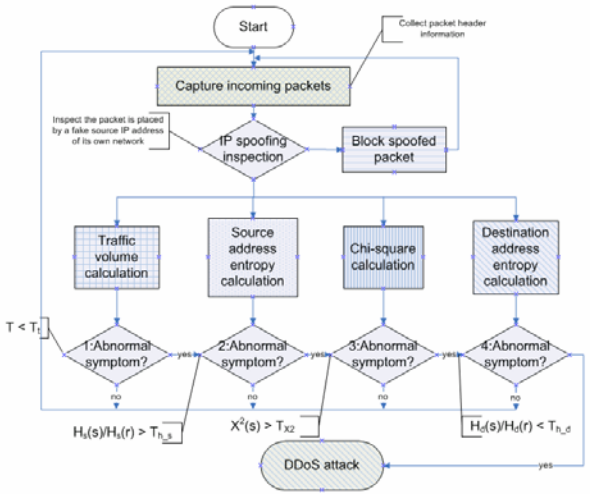


그림 2. Source 네트워크의 탐지 순서도

3.2 Victim 네트워크에서의 침입 탐지

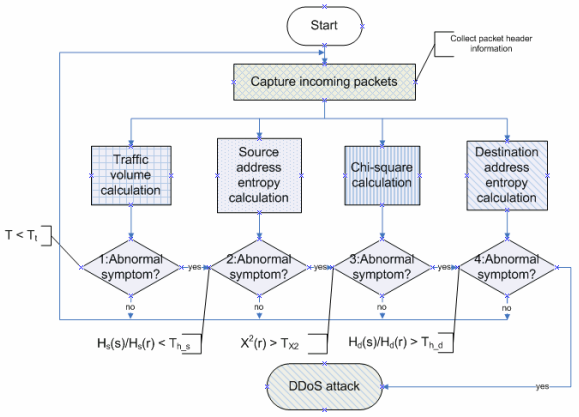


그림 3. Vicvim 네트워크의 탐지 순서도

Victim 네트워크의 탐지 기법은 source 네트워크의 DDoS탐지 모듈과 같은 구성을 가진다. 그러나 DDoS 공격 시 소스 주소 엔트로피, 카이 제곱, 그리고 목적지 주소 엔트로피 값은 Source-end 탐지의 수식과 반대의 특성을 가진다. 그림 3은 source 네트워크의 탐지 기법 과정을 나타낸 순서도이다.

3.3 통합 서버(Aggregate server)

공격 발생시 victim 네트워크와 source 네트워크의 IDRS에서 탐지된 alert은 통합 서버로 모아진다. Victim 네트워크 IDRS의 탐지 정확도가 source 네트워크의 탐지 정확도보다 높기 때문에 통합 서버는 victim 네트워크의 alert정보를 기준으로 source 네트워크에서 보낸 alert메시지와 비교한다.

그리고 공격 여부가 일치하는 에지 라우터의

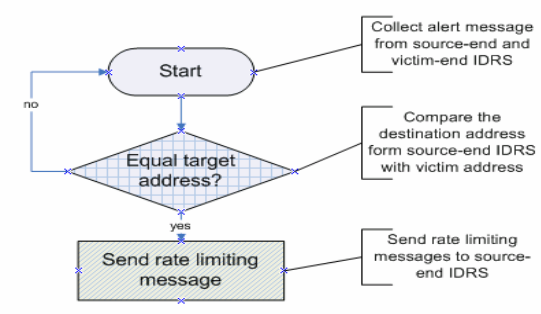
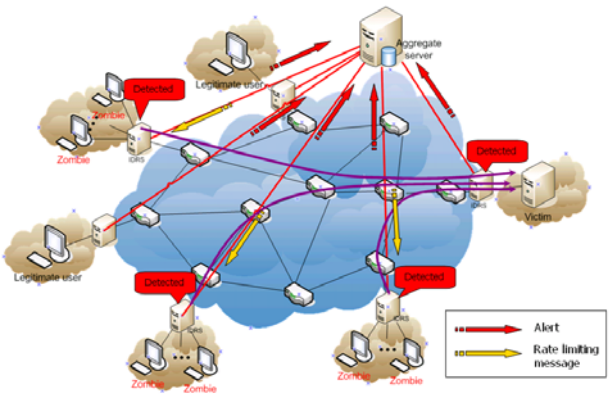
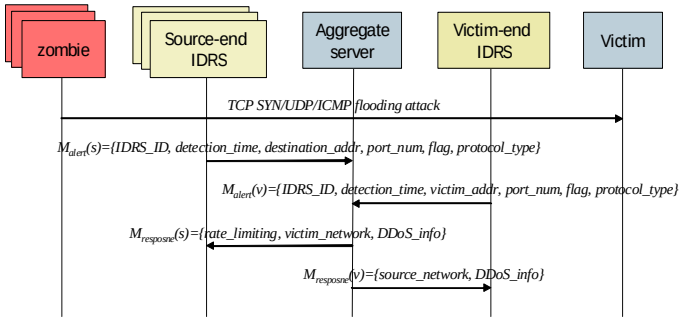


그림 4. 통합 서버의 대응 순서도

IDRS에 Rate limiting 메시지를 보내 적정 범위를 초과하는 이상 트래픽에 대해 대역폭(bandwidth)를 제한하도록 한다. 뿐만 아니라 victim 네트워크와 source 네트워크의 IDRS에서 보낸 포트번호, 프로토콜 타입, 플래그 값 등의 통계정보를 각 IDRS의 관리자에게 제공해 공격에 대한 통합적인 분석이 가능하도록 돕니다. 그림 4는 통합 서버의 대응 순서도를 나타내고 그림 5는 협력적인 방어 시스템의 시스템 구조와 시퀀스 다이어그램을 나타낸다.



(a) 시스템 구조



(b) 시퀀스 다이어그램

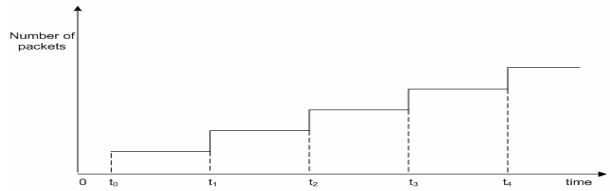
그림 5. 협력적인 방어 시스템

3.4 지능화된 DDoS 공격 탐지

기존의 가중치를 가지는 평균과 분산을 이용하여 변화하는 트래픽에 대한 임계값 계산 방법의 문제는 마스터(master)가 좀비 에이전트의 개수를 서서히 증가시키면서 플러딩(flooding) 공격을 할 경우 탐

지를 피하면서 victim의 대역폭을 고갈시킬 수 있다. 그림 6(a)는 t0에서 일시적으로 트래픽 양을 증가시키는 전형적인 공격 형태를 나타내고 그림 6(b)는 t0에서 t4 에 이르기까지 장시간 점차적으로 임계값을 증가시켜 공격을 피하면서 ISP (Internet Service Provider)의 네트워크에 장애를 일으키는 형태를 나타낸다.

(a) Constant rate 공격



(b) Increasing threshold 공격

그림 6. DDos 공격 형태

이러한 공격은 소스 주소 엔트로피 값은 서서히 증가하고 트래픽 볼륨과 목적지 주소에 대한 엔트로피 값은 서서히 감소하는 특징이 있다. 따라서 트래픽 볼륨, 소스 주소 엔트로피 그리고 목적지 주소 엔트로피의 임계값에 대한 평균과 분산을 이용해 다양한 형태로 탐지 임계값을 피하는 공격 형태에 대한 탐지가 가능하다. 일반적으로 네트워크 관리 시스템은 대역폭을 기반으로 시스템에 위협적인 트래픽을 탐지하는 정적인 임계값을 가지고 있지만 제안한 메커니즘을 이용하면 탐지 임계값을 증가시키는 공격을 조기에 탐지하고 대응할 수 있는 판단 근거를 제공할 수 있다는 장점이 있다.

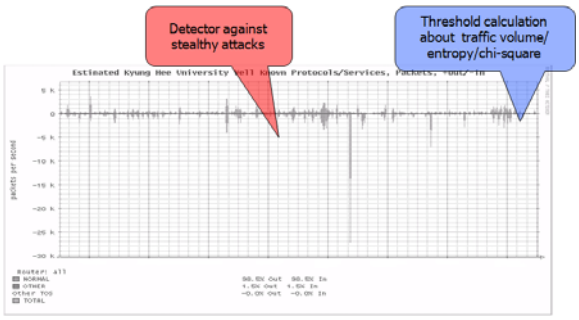


그림 7 이중 탐지 윈도우를 이용한 방법

그림 7은 이런 이중 탐지 윈도우를 이용한 탐지 방법을 나타내며 그림 8은 임계값에 대한 트래픽 볼륨, 소스 주소와 목적지 주소 엔트로피 값을 이용해 지능적인 공격 형태를 탐지하는 방법의 순서도를 나타낸다

4. 성능 평가

4.1 테스트 환경

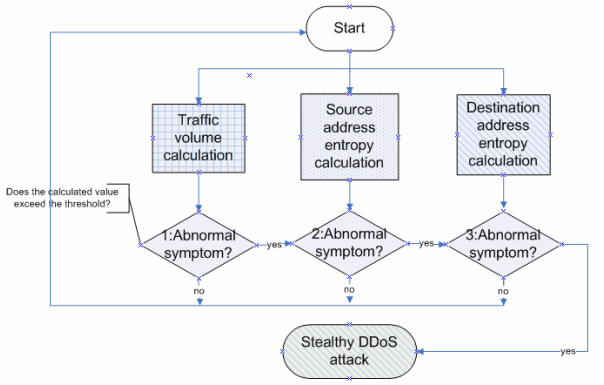


그림 8. Increasing threshold 공격 탐지 순서도

성능 평가를 위해서 Linux RedHat 9.0에서 NS-2를 이용하였다. 공격 테스트를 위해서 대표적인 DDoS 공격 툴 중 하나인 Stacheldraht V4를 참고하였다. 각 링크는 100Mbps로 연결하였고 source 네트워크의 에지 라우터는 5개로 구성하였으며 각 에지 라우터는 정상적인 노드와 공격자 노드가 연결되어 있으며 평균적으로 정상적인 트래픽은 약 200Kbps, 공격 발생 시 최대 대역폭은 약 2,000Kbps가 발생한다. 그리고 Victim 네트워크에서는 정상적인 경우 약 1,000Kbps, 공격 시는 최대 10,000Kbps의 대역폭을 갖는다.

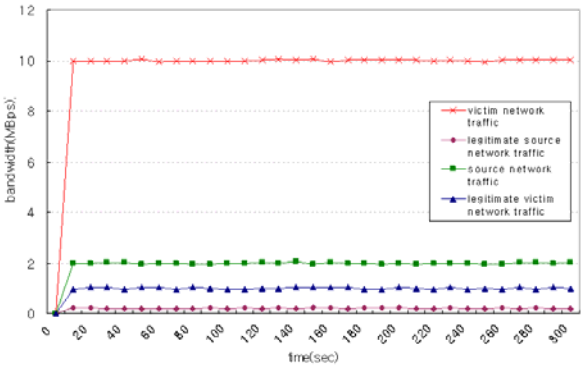


그림 9 공격 및 정상 트래픽 대역폭

그림 9는 source 네트워크와 victim 네트워크의 IDRS에서 정상적인 경우와 공격 발생 시의대역폭을 비교한 그래프이다.

4.2 성능 평가 요소

침입 탐지의 성능을 평가하는 기준은 크게 2가지 요소를 가진다. 하나는 탐지 딜레이(detection delay)이고 다른 하나는 탐지 정확도이다. 탐지 딜레이는 공격이 탐지가 된 시간에서 공격이 발생한 시간의 차로 측정하였다.

그리고 탐지 정확도는 전체 공격 트래픽 중에서 탐지된 트래픽의 양의 비율로 측정하였다.

$$T_d = T_a - T_s$$

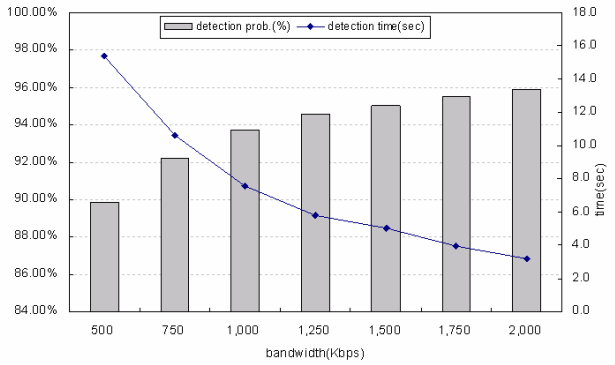
T_d : detection delay
T_a : time alarm is raised
T_s : time DDoS attack is started

$$R_d = \frac{N_d}{N_a}$$

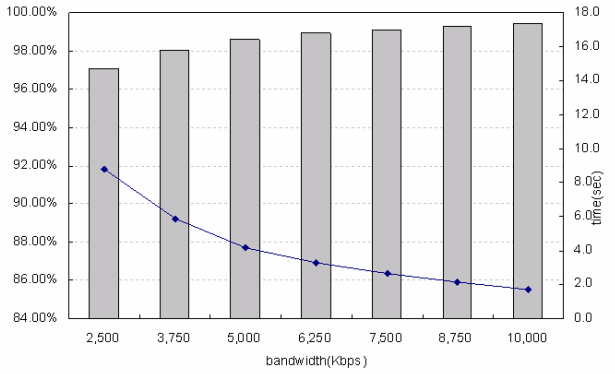
R_d : detection rate
N_d : number of detected attacks
N_a : total number of attacks

4.3 성능 평가 결과

그림 10은 source 네트워크와 victim 네트워크에서 공격 트래픽의 대역폭이 증가함에 따라 탐지 시간과 탐지율을 나타낸 그래프이다. 대역폭이 작을수록 탐지 시간은 길어지고 탐지율은 작아지며 대역



(a) source 네트워크



(b) Victim 네트워크

그림 10 탐지 시간과 탐지율

폭이 커질수록 탐지 시간과 탐지율은 그 반대가 된다. 즉 트래픽 양이 많을수록 공격의 증후를 빨리 파악할 수 있으며 탐지의 정확도 역시 높아지게 된다. 실험 결과 Source 네트워크와 victim 네트워크의 IDRS 간의 탐지율의 차이는 3.5~7.3%로 적게 나타났다. 이러한 이유는 비교적 적은 수의 좀비 에이전트로 공격 트래픽을 생성해서이고 에이전트를 수를 늘릴수록 탐지 정확도의 차이는 커질 것이다.

Source 네트워크와 victim 네트워크의 IDRS가 상호 협력하게 되면 공격 근원지 네트워크를 찾는 정확도는 증가하게 된다. 즉 source 네트워크와 victim 네트워크의 alert 메시지를 비교하여 탐지의 정확도가 높은 victim 네트워크의 alert 메시지를 기준으로 공격 근원지를 찾게 되면 더 정확하게 공격의 근원지를 찾을 수 있다. 표 2는 공격 Soruce 탐지 딜레이 및 정확도를 나타낸다.

표 2 공격 source 탐지 딜레이 정확도

Source-end (Kbps)	Victim-end (Kbps)	Defense delay (sec)	Defense accuracy (%)
500	2500	15.8	97.1
750	3750	10.8	98.0
1000`	5000	7.8	98.6
1250	6250	6.0	98.9
1500	7500	5.2	99.1
1750	8750	4.2	99.3
2000	10000	3.4	99.4

5. 결론

본 논문은 기존의 협력적인 DDoS 방어 시스템이 가지고 있는 문제점을 언급하고 침입 탐지에 초점을 맞춰 해결 방안을 제시하였다. Victim 네트워크와 source 네트워크의 IDRS에서 트래픽 볼륨, 소스 주소 엔트로피, 카이 제곱, 그리고 목적지 주소 엔트로피를 이용하여 실시간으로 신뢰성 있는 탐지할 수 있으며 각 구성 컴포넌트간 협력을 통해 신속하고 정확한 대응이 가능하다. 또한 탐지 임계값을 피하면서 victim의 대역폭을 고갈시키는 increasing threshold 공격에 대해 이중 탐지 윈도우를 이용한 방법을 이용해 탐지할 수 있다. 따라서 source 네트워크와 victim 네트워크의 IDRS간 통계적인 탐지 기법을 이용한 협력적인 방법으로 다양한 DDoS 공격 형태에 대해 효과적인 탐지 및 대응이 가능하다.

참 고 문 헌

[1] Mirkovic J., Robinson M., Reiher P., "Alliance formation for DDoS defense", Proceedings of the 2003 workshop on New security paradigms, 2003

[2] Mirkovic J., Reiher P., "A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, April 2004

[3] Mirkovic J., Prier G., Reiher P., "Source-end DDoS defense", Network Computing and Applications, NCA 2003. Second IEEE International Symposium on, 16-18 April 2003

[4] Jelena Mirkovic, Max Robinson, Peter Reiher, "Alliance formation for DDoS defense", New Security Paradigms Workshop, August 2003

[5] Papadopoulos C., Lindell R., Mehringer J., Hussain A., Govindan R., "Cossack: coordinated suppression of simultaneous attacks", DARPA Information Survivability Conference and Exposition, April 2003

[6] Feinstein L., Schnackenberg D, Balupari R., Kindred D., "Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition(DISCEX 2003), April 2003