BcN 상에서의 DDoS에 대한 Anomaly Detection 연구

Anomaly Detection Mechanism against DDoS on BcN

송 병 학* 이 승 연** 홍 충 선*** 허 의 남**** 손 승 원*****
Byung-Hak Song Seung-Yeon Lee Choong Seon Hong Eui-Nam Huh Seongwon Sohn

요 약

BcN(Broadband Convergence Network)은 통신, 방송, 인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스로 언제 어디서나 끊김 없이 안전하게 이용 할 수 있는 이용자 중심의 유비쿼터스 서비스 구현을 위한 핵심 인프라이다. BcN은 여러 가지 개별망이 통합된 망으로 그 특성상 보안 문제가 발생하면 전체 네트워크로 광범위 하게 확산돼 심각한 피해를 입게 된다. 따라서 BcN에서는 전체 네트워크를 통합하는 보안 정책을 세워야 할 것이다.

본 논문에서는 이러한 문제를 해결하기 위해 협력적인 침입방어 시스템의 탐지의 정확도를 향상시키고 수집된 정보를 바탕으로 효과적으로 대응할 수 있는 메커니즘을 제안한다. 또한 BcN 상에서의 정보 교환을 위한 분산-계층적 시스템 구조를 설계하였다.

Abstract

BcN is a high-quality broadband network for multimedia services integrating telecommunication, broadcasting, and Internet seamlessly at anywhere, anytime, and using any device. BcN is particularly vulnerable to intrusion because it merges various traditional networks, wired, wireless and data networks. Because of this, one of the most important aspects in BcN is security in terms of reliability. So, in this paper, we suggest the sharing mechanism of security data among various service networks on the BcN. This distributed, hierarchical architecture enables BcN to be robust of attacks and failures, controls data traffic going in and out the backbone core through IP edge routers integrated with IDRS. Our proposed anomaly detection scheme on IDRS for BcN service also improves detection rate compared to the previous conventional approaches.

☞ Keywords: BcN, DDoS, IDRS, Anomaly Detections, QoS

제1장 서론

광대역통합망(BcN)은 현재의 개별적인 망들이 갖고 있는 한계들을 극복하고 미래에 나타날 다양한 유·무선 접속환경에서 고품질의 음성, 데이터 및 방송이 융합된 광대역 멀티미디어 서비스를 언제 어디서나 이용할 수 있도록 하는 차세대 통합 네트워크이다. 다양한 접속 기술을 수용하는 BcN은 이에 따른 다양한 트래픽을 처리하게 됨에 따라 서비스의 품질보장(QoS), 보안, 트래픽 관리 등의 정보보호 인프라 연계 및 상호 운용이 필수적으로 요구 된다. BcN은 통합망이라는 특성에 따라 하나의 망에서 발생한 위협이 타 망으로 쉽게 전이되는 현상이 발생하는 등 보안의 위협이 날로 증가하고 있다. 그 중에서도 가장 심각한 보안 위협에 사례가 네트워크 트래픽 폭주 공격에 의한 피해이다. 트래픽 폭주 공격은 더욱 복잡한 형태의 공격 방식으로 발전하고 있으며 DDoS(Distributed Denial of Service) 공격과 같이 전체 네트워크의 기능을 마비시키는 공격 기술로 진화하고 있다[1].

* 정 회 원 : (주)플랜티넷 신기술개발팀
bhsong@plantynet.com
** 준 회 원 : 한국과학기술정보연구원 그리드컴퓨팅연구팀 seungyeon@kisti.re.kr
*** 정 회 원 : 경희대학교 컴퓨터공학과 교수
cshong@khu.ac.kr
**** 종신회원 : 경희대학교 전자정보공학부 부교수
huh@icns.khu.ac.kr(교신저자)
***** 정 회 원 : 한국전자통신연구원 IT융합서비스부문 수석단장 swsohn@etri.re.kr
[2006/11/21 투고 - 2006/11/22 심사 - 2006/12/20 완료]

DDoS 공격은 네트워크상에서 이루어지는 특정 서비스의 정상 동작을 방해함으로서 합법적인 사용자가 정상적인 서비스를 받지 못하도록 하는데 있으며 취약점을 가지고 있는 시스템들을 공격하기 때문에 탐지를 더욱 어렵게 한다. 또한 하나의 공격에 여러 호스트가 사용되어 공격에 대한 방어 또한 매우 어렵다[2].

DDoS 공격에 대응하기 어려운 가장 큰 이유는 해커가 발송하는 비정상적인 공격성 패킷과 정상적인 서비스 요청 패킷을 정확히 구분하는 것이 무척 어렵기 때문에 DDoS 공격을 탐지하는 것 자체가 힘들다는 점이다. 또한 아주 정교한 공격에 대해서는 속수무책인 경우가 많고 대응속도가 너무 느리며 정상적인 서비스 트래픽을 죽이는 빈도가 높다. 만약 BcN에서 여러 노드로부터의 다양한 종류의 트래픽이 통과하는 전송 노드가 DDoS의 공격으로 통제 불능 상태가 된다면 통과되는 QoS를 지원해야 하는 트래픽에 대한 서비스가 중단 될 것이며 이는 전체 네트워크의 장애로 확대 될 수 있다.

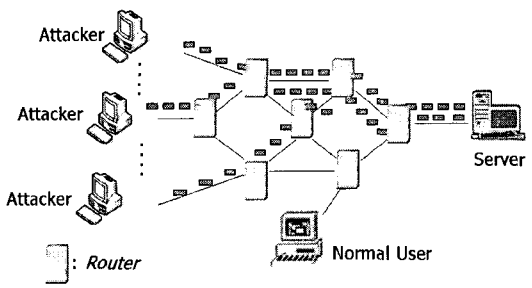
이러한 보안 위험의 가능성은 BcN 서비스 품질 보장에 있어서 매우 중요한 문제이며 본 논문은 이러한 문제점을 해결하기 위해 BcN 환경에 적합한 새로운 DDoS 공격 탐지 방법을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 DDoS 공격의 동작 원리와 공격 형태, 기존의 침입탐지 기법을 알아보고 3장에서는 새로운 공격 탐지 방법을 제안하고자 한다. 그리고 4장에서는 성능 평가를 하고 마지막 5장에서는 결론을 내린다.

제2장 관련 연구

2.1 DDoS 공격의 원리와 공격 유형

2.1.1 공격 원리

분산 서비스 거부 공격(Distributed Denial of Service, 이하 DDoS)은 이미 많이 알려진 바와 같이 인터넷의 구조적인 취약성을 공격하여 길게는 수일 동안 정상적인 서비스의 지연 혹은 마비상황을 불러일으키는 해킹 공격을 말한다. 모든 인터넷 사용자는 TCP/IP 프로토콜을 이용하여 임의의 데이터 패킷을 발송자의 IP 주소(Source IP)를 가지고 목적지의 IP 주소(Destination IP)로 발송할 수 있다. 이때 이 IP주소에 대한 특별한 인증 절차 없이 무제한적으로 대규모의 데이터 패킷을 전송할 수 있다는 것이 문제이며, DDoS 공격은 이러한 인터넷의 취약점을 악용하는 공격이다. 이는 공격 목표 호스트로 대량의 네트워크 트래픽을 발생시켜 대상 호스트의 네트워크 서비스 기능을 일시적으로 또는 완전히 정지시키는 공격의 유형으로 일반적인 DoS 공격보다 훨씬 더 강력한 파괴력을 지닌다. DDoS 공격은 수백 혹은 수천 개의 좀비 시스템들을 이용해서 공격의 목적이 되는 타깃 시스템을 공격하는 형태를 된다. 이때, 이 수많은 좀비 시스템들은 공격 명령이 떨어지면 일제히 타깃 시스템을 공격하게 된다. 결국, DDoS 공격은 엄청난 볼륨의 패킷들을 발송하거나 불완전한 형태의 요청 패킷을 발송하여 공격 대상이 되는 네트워크 장비나 서버가 정상적인 서비스 요청을 받아들일 수 없는 상태, 혹은 자신의 능력으로 처리할 수 있는 용량을 초과하여 처리 불능의 상태에 된다[3]. 다음 (그림 1)은 이러한 DDoS 공격의 기본 구조를 나타낸다.



(그림 2) DDoS 공격의 기본 구조

2.1.2 공격 유형

DDoS 공격은 직접적으로 시스템의 데이터를 장악하기 위한 방법이라기보다는 계획적으로 시

스템을 다운시키거나 TCP, UDP, ICMP 패킷들을 사용해 타겟 시스템 서버에 많은 양의 네트워크 트래픽을 전송함으로써 시스템의 성능 저하 및 시스템을 마비시키는 형태를 가진다[4].

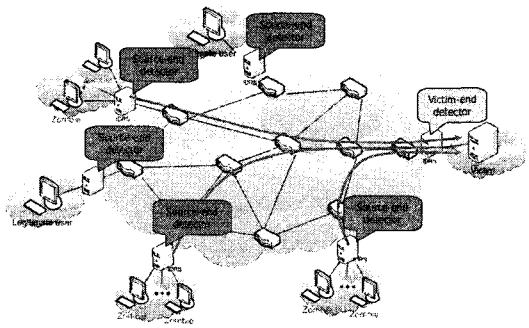
- Bandwidth Consumption : ICMP, UDP, TCP SYN flood
  많은 양의 트래픽을 유발하여 네트워크를 마비시키는 공격
- Resource Starvation : TCP SYN flood
  서버의 자원을 고갈시키는 행위 (CPU, 메모리, 파일시스템 등)
- Programming Flaw : Ping of death, IP fragmentation error
  응용프로그램, OS, embedded chip등의 예외처리 오류이용
- Routing and DNS Attacks : DoS on DNS
  라우팅 정보나 DNS서버에 대한 공격으로 정상적인 연결을 방해
- Generic DoS Attacks : DDoS툴 + Worm + Virus 등 다양한 종류의 시스템을 마비

2.2 침입탐지 및 대응 기법

IDRS(Intrusion Detection Response System)는 탐지 위치에 따라서 source 네트워크와 victim네트워크 IDRS로 구분된다.

일반적으로 IDRS는 victim 네트워크에 가장 가까운 에지(edge) 라우터에 위치한다[5]. 분산된 네트워크에서 들어오는 공격 트래픽을 통합적으로 분석해서 공격의 징후를 탐지하기 가장 좋은 위치이기 때문이다. 그러나 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 source네트워크 IDRS[6]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 2)는 source 네트워크와 victim 네트워크 IDRS의 위치를 나타낸다.



(그림 2) Source와 Victim 네트워크 IDRS

이러한 단점을 보완하기 위한 방법들[7][8]이 연구되어 왔지만 단순한 탐지 요소를 가지고 있기 때문에 false positive와 false negative가 높다.

2.2.1 통계기반 탐지 알고리즘

DDoS 공격은 일반적인 패킷으로 공격이 이루어지므로 합법적인 패킷과 구분하기 어려우며 탐지를 위해서는 탐지의 정확성과 복잡도가 동시에 고려되어야 한다[9]. 따라서 이를 탐지하기 위해서는 통계적인 방법을 사용하는 것이 가장 효율적이다.

통계적인 탐지 알고리즘에는 트래픽 볼륨(traffic volume), 패킷 속성 값의 엔트로피(entropy)[10], 카이 제곱 (chi-square) 검증법[10]등이 사용되고 있다.

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

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

위 공식은 각각의 패킷이 도착하는 시간을 측

정하여 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 속성 값에 대한 임의성(randomness)을 계산한 뒤, 그 값의 평균의 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 속성 값이 선택될 확률을 나타낸다.

카이 제곱 검증법은 속성값에 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 binding 값이다. (Ex. 패킷 길이는 0-64, 65-128, 129-255로 binding 될 수 있다) Ni는 N개의 샘플 패킷에서 각각의 binding 범위에 속하는 패킷의 개수이고, ni는 일반적인 분포에서 binding에 속하는 기대값이다.

제3장 제안하는 방법

3.1 개요

BcN은 QoS, 보안성, IPv6 주소 체계가 지원되는 통신망이다. 특히 BcN은 품질 보장성이 강조되는 망으로 품질 보장망의 구축을 위해서는 QoS 관리 및 트래픽 관리 등을 통합 수행하는 효율적인 기능을 갖춘 보안 기술이 필수적이다. 현재의 악의적인 공격들은 그 기법이 점점 지능화되고 다양해지면서, 하나의 공격이 서로 연관된 다수의 침입정보를 발생시킨다. 더욱이 대부분의 침입 탐지 시스템들은 그러한 다수의 탐지 정보들을 가공이나 분석 없이 그대로 관리자에게 전달함으로서 관리자의 부담만 가중시키는 형태를 띠고 있다[11]. BcN에서 서비스 품질 보장을 높이고 보안성이 강화된 침임 탐지를 위해서는 각각의 호스트들이 보안 관련 정보의 공유를 통하여 협력할 수 있어야 한다[12]. 따라서 본 논문에서는 각각의 컴포넌트 사이의 메시지 교환을 통하여 침임 탐지를 수행하는 체계적이고 계층적인 침임 탐지 시스템을 제안한다. 각각의 에이전트에서 독립적인 침입 탐지를 수행하여 그 결과를 상위 매니저에게 전송하는 특성을 가지고 있으므로 대규모 네트워크에서 트래픽의 과다한 증가와 다양한 공격에 보다 효율적으로 대응할 수 있다.

3.2 상호 협력적인 DDoS 탐지 시스템 구조

다수의 분산된 네트워크에 설치된 침임 탐지 호스트들로부터 침임 탐지 정보를 모아 상호 협력 가능한 보안 정책을 수행하는 시스템의 구성은 다음 (그림 3)에서 보여지며 각각의 기능은 다음과 같다.

- Host Security Agent

  바이러스 웜이나 불법침입, 분산서비스 거부 공격 등의 비정상적인 이상 신호를 발견한다.

- Network Security Agent(IDRS: Intrusion Detection and Response System)

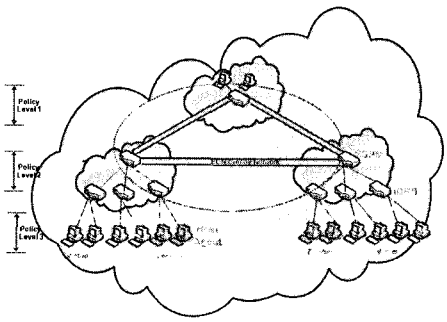
  데이터 수집 및 분석을 위한 요소로서 침입과 관련된 이벤트들을 모니터링 한다. 침입 탐지에 필요한 데이터들을 수집하여 기록함과 동시에 수집 데이터들의 내용을 분석하는 역할을 한다. 비정상적이거나 침입과 관련된 행위를 상위 계층에 보고하고 호스트에 대한 의심스런 행위를 감시한다.

• Security Service Policy Manager(SSPM)

SSPM은 Policy Decision, Security Information Sharing, Aggregation 로 구성되어 있어 네트워크에서 동작중인 IDRS에서 발생된 보고를 받고 발생된 보고에 따라 해당 시스템에 대한 대응을 적용한다. 또한 IDRS부터의 결과를 재검사하여 필터링함으로서 오판율을 줄이고 보다 정확한 결과를 이웃 SSPM에 보고하고, 분석 결과에 대해 최종적인 침입 여부를 결정하고 이의 결과에 따라 유해한 트래픽에 대한 제어를 Policy Decision 상위 레벨에서 하게 된다.

SSPM은 이웃한 SSPM에게 정보를 공유하기 위하여 Overlay 네트워크 기법을 활용하여 공유 정보의 기밀성과 안전성을 보장하도록 설계 하였다.

다음 (그림 3)은 본 시스템의 정책 기반 네트워크 관리 구조로 보안 서비스의 관리 정책을 정의하고 이를 기반으로 네트워크 및 서비스를 자동으로 관리 하는 구조를 따른다[13]. Policy Level 3은 네트워크 상태를 정기적으로 모니터링 하고 상위 보안 레벨에 수집된 정보를 보고한다. Policy Level 2는 Policy Level 3에서 수집된 정보를 기반으로 보안 정책을 결정하고 해당 트래픽에 대한 정책 제어 정보를 전달한다. Policy Level 1은 침입 탐지 유형에 따라 대응 방법들을 제공하며 망의 보안 정책을 제어 하며 보안 정책을 하위에 에이전트들에 전달한다. 이러한 단계별 정책을 바탕으로 보안 네트워크 구조가 제공되며 침임 탐지 시스템들 사이의 정보 교환을 허용할 수 있다.



(그림 3) BcN overly Network에서 Distributed Domain Secure Management 시스템 구조

3.3 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 스푸핑한다면 차단된다.

DDoS 공격 탐지 모듈은 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.

• Step1: 트래픽 볼륨

$$T < T_t$$

T : *traffic volume*

T_t : *threshold of traffic volume*

• Step2:소스 주소 엔트로피

$$\frac{H_s(s)}{H_s(r)} > T_{H_s}$$

$H_s(s)$: *source address entropy of sent packets*

$H_s(r)$: *source address entropy of received packets*

T_{H_s} : *threshold of source address entropy*

• Step3: 카이 제곱

$$x^2(s) > T_{x^2}$$

$x^2(s)$: *chi – square of sent packets*

T_{x^2} :*threshold of chi–square*

• Step4: 목적지 주소 엔트로피

$$\frac{H_d(s)}{H_d(r)} < T_{H_d}$$

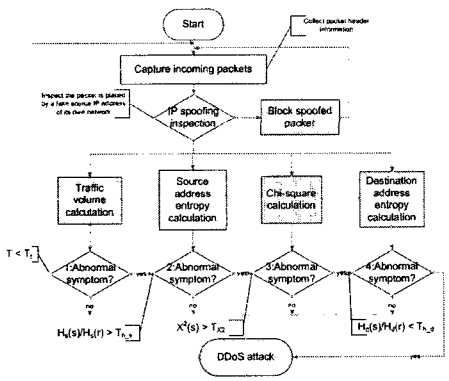
$H_d(s)$: *destination address entropy of sent packets*
$H_d(r)$: *destination address entropy of received packets*
T_{H_d} : *threshold of destination address entropy*

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

$$\mu_n(x) = \alpha\mu_{n-1}(x) + (1-\alpha)\mu_{n-2}(x) \quad ,0 < \alpha < 1$$
$$T(x) = \mu_n(x) + k\sigma(x) \quad , k = 1, 2, 3\cdots$$
$$where\ x = T,\ \frac{H_s(s)}{H_s(r)},\ x^2(s),\ \frac{H_d(s)}{H_d(r)}$$

μ : *average*
α : *weighted value*
σ : *standard deviation*

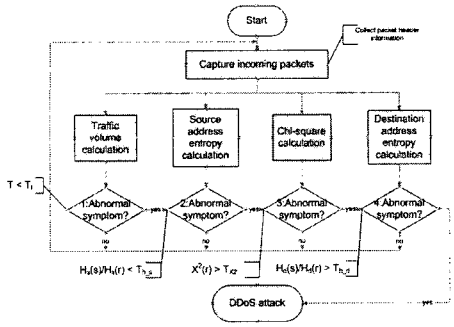
아래 그림은 source 네트워크의 탐지 기법 과정을 나타낸 순서도이다.



(그림 4) Source 네트워크의 탐지 순서도

3.3.1 Victim 네트워크에서의 침입 탐지

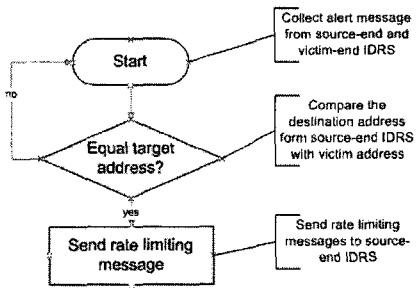
Victim 네트워크의 탐지 기법은 source 네트워크의 DDoS탐지 모듈과 같은 구성을 가진다. 그러나 DDoS 공격 시 소스 주소 엔트로피, 카이 제곱, 그리고 목적지 주소 엔트로피 값은 Source-end 탐지의 수식과 반대의 특성을 가진다. 즉 Hs(s)/Hs(r) 값은 정상범위보다 작아지고 T, Hd(s)/Hd(r)과 x2(r) 값은 정상범위보다 커진다. (그림 5)는 source 네트워크의 탐지 기법 과정을 나타낸 순서도이다.



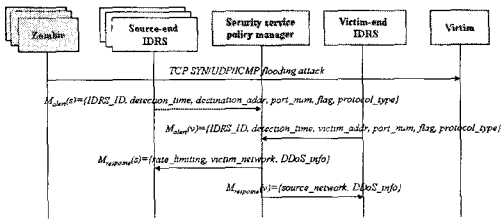
(그림 5) Victim 네트워크의 탐지 순서도

3.3.2 SSPM의 Aggregator

공격 발생 시 victim 네트워크와 source 네트워크의 IDRS에서 탐지된 alert은 상위레벨로 모아진다. Victim 네트워크 IDRS의 탐지 정확도가 source 네트워크의 탐지 정확도보다 높기 때문에 통합 서버는 victim네트워크의 alert정보를 기준으로 source 네트워크에서 보낸 alert메시지와 비교한다. 그리고 공격 여부가 일치하는 에지 라우터의 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 통계 정보를 각 IDRS의 관리자에게 제공해 공격에 대한 통합적인 분석이 가능하도록 돕니다. (그림 6)은 통합 서버의 대응 순서도를 나타내고 (그림 7)은 협력적인 방어 시스템의 시퀀스 다이어그램을 나타낸다.



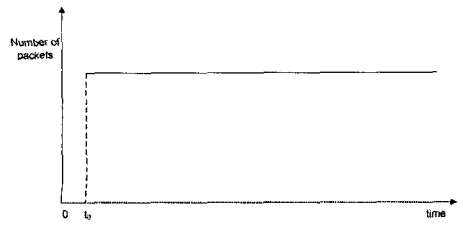
(그림 6) 통합 서버의 대응 순서도



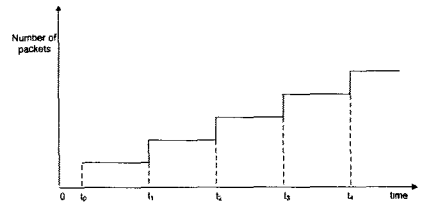
(그림 7) 시퀀스 다이어그램

3.3.4 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 탐지를 피하면서 victim의 대역폭을 고갈시킬 수 있다. (그림 8)(a)는 t0에서 일시적으로 트래픽 양을 증가시키는 전형적인 공격 형태를 나타내고 (그림 8)(b)는 to에서 t4에 이르기까지 장시간 점차적으로 임계값을 증가시켜 공격을 피하면서 ISP(Internet service provider)의 네트워크에 장애를 일으키는 형태를 나타낸다.



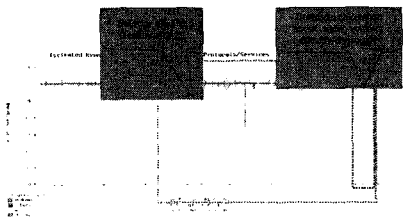
(a) Constant rate 공격



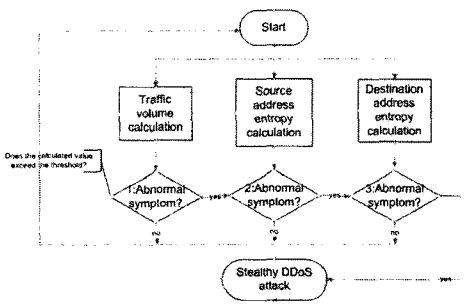
(b) Increasing threshold 공격

(그림 8) 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 9) 이중 탐지 윈도우를 이용한 방법



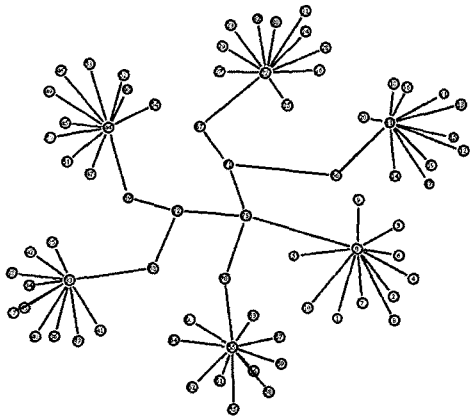
(그림 10) Increasing threshold 공격 탐지 순서도

(그림 9)는 이러한 이중 탐지 윈도우를 이용한 탐지 방법을 나타내며 (그림 10)은 임계값에 대한 트래픽 볼륨, 소스 주소와 목적지 주소 엔트로피 값을 이용해 지능적인 공격 형태를 탐지하는 방법의 순서도를 나타낸다.

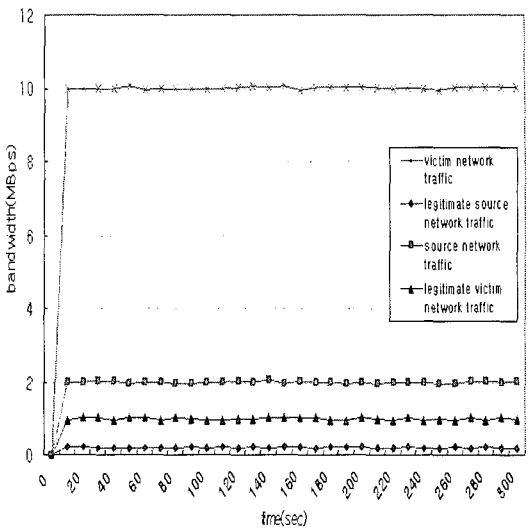
제 4장 성능 평가

4.1 테스트 환경

제안한 탐지 알고리즘의 성능 평가를 위해서 Linux RedHat 9.0에서 NS-2를 이용하였다. 공격 테스트를 위해서 대표적인 DDoS 공격 툴 중 하나인 Stacheldraht V4[14]를 참고하였다. 네트워크 토폴로지는 (그림 11)과 같이 구성하였으며 각 링크는 100Mbps로 연결하였다. source 네트워크의 에지 라우터는 5개로 구성하였으며 각 에지 라우터는 정상적인 노드와 공격자 노드가 연결되어 있으며 평균적으로 정상적인 트래픽은 약 200Kbps, 공격 발생 시는 최대 대역폭은 약 2,000Kbps가 발생한다. 그리고 Victim 네트워크에서는 정상적인 경우 약 1,000Kbps, 공격 시는 최대 10Mbps의 대역폭을 갖는다.



(그림 11) NS-2 네트워크 토폴로지



(그림 12) 공격 및 정상 트래픽 대역폭

(그림 12)는 source 네트워크와 victim 네트워크의 IDRS에서 정상적인 경우와 공격 발생 시의 대역폭을 비교한 그래프이다

4.2 성능 평가 요소

침입 탐지의 성능을 평가하는 기준은 크게 2가지 요소를 가진다. 하나는 탐지 딜레이(detection delay)[15]이고 다른 하나는 탐지 정확도[15]이다. 탐지 딜레이는 공격이 탐지가 된 시간에서 공격이 발생한 시간의 차로 측정하였다.

$$T_d = T_a - T_s$$

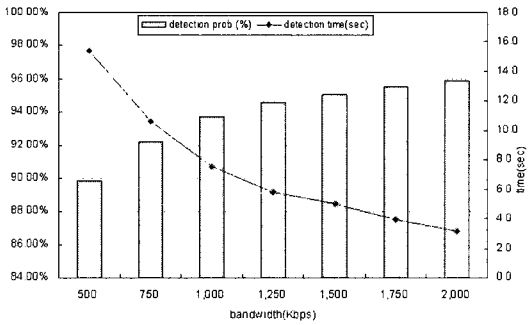
T_d : detection delay
T_a : time alarm is raised
T_s : time DDoS attack is started

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

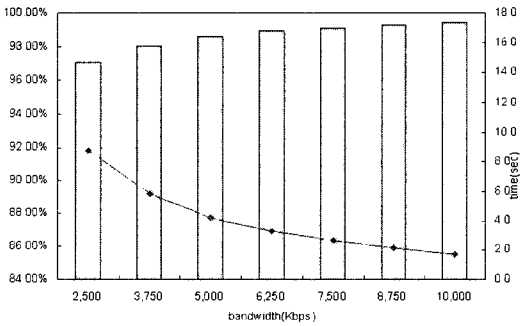
$$R_d = \frac{N_d}{N_a}$$

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

4.3 성능 평가 결과



(a)Source 네트워크



(b)Victim 네트워크

(그림 13) 탐지 시간과 탐지율

(그림 13)은 source 네트워크와 victim 네트워크에서 공격 트래픽의 대역폭이 증가함에 따라 탐지 시간과 탐지율을 나타낸 그래프이다. 대역폭이 작을수록 탐지 시간은 길어지고 탐지율은 작아지며 대역폭이 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 다소 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 1은 공격 source 탐지 딜레이 및 정확도를 나타낸다.

(표 1) 공격 source 탐지 딜레이 및 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

BcN의 발전은 정보 기술의 패러다임을 변화시키고 있으며 개인 정보 보호에 대한 보안을 보장하는 문제가 중요한 이슈가 되고 있다. 본 논문에서는 BcN의 QoS를 보장할 수 있는 신뢰성 있고 안전한 보안 시스템을 제시 하였다. 제안한 방법은 Victim 네트워크와 source 네트워크의 IDRS에서 각 구성 컴포넌트간 협력을 통해 신속하고 정확한 대응이 가능한 탐지 기법으로 네트워크 전역의 트래픽 이상 징후를 탐지하여 이상 트래픽에 대한 정책을 생성하고 적용할 수 있는 정책 기반 시스템이다. 이를 통해 BcN에서 DDos 위협이 확산되는 것을 방지하는데 매우 큰 효과를 볼 수 있을 것이라 기대한다. 또한 분산, 계층적 구조를 통한 효율적 정보 공유와 overlay 기술을 이용한 안전한 전송을 제안하였다.

향후 연구 과제로는 본 논문에서 제안한 탐지 메커니즘을 실제 네트워크에 테스트베드로 구축하고 다양한 공격 트래픽[14]에 대한 분석 및 제안한 IDRS에 대한 성능 평가를 하는 것이다.

참 고 문 헌

[1] 이철호, 최경희, 정기현, 노상욱, "웹 서버에 대한 DDoS공격의 네트워크 트래픽 분석", 한국정보처리학회 논문지, VOL. 10-C, NO. 03 pp., 0253 ~ 0264, 2003. 06

[2] http://www.secureosform.org

[3] http://ko.wilipedia.org

[4] 박필용, 홍충선, 최상현, "검증된 IP 테이블을 사용한 통계 기반 DDoS 대응 시스템", 한국정보처리학회 논문지, VOL.12-C, NO. 06 pp., 0827 ~ 0838, 2005. 10

[5] Ratul M., Steven M., Sally F, John I., Vern P., Scott S., "Controlling high bandwidth aggregates in the network", ACM SIGCOMM Computer Communication Review, July 2002

[6] 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

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

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

[9] Carl G., Kesidis G., Brooks R.R., Suresh Rai, "Denial-of-service attack-detection techniques", Internet Computing, IEEE, Jan.-Feb. 2006

[10] 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

[11] 장정숙, 전용희, 장종수, "BcN 인프라 보호를 위한 다중 도메인 보안 관리 프레임워크와 성능 평가",한국정보처리학회 논문지 C, VOL.12-C, NO.06, pp.0817~0826 2005. 10

[12] 박진호, 정진욱, "안전한 망 관리를 위한 보안정책 협상모델 설계", 한국 정보처리학회 논문지, VOL.11 NO.02, pp.0171~0176 2004. 04

[13] 윤여웅, 황윤철, 엄남경, 김건우, 이상호, "계층적 구조 보안 정책 모델을 위한 데이터베이스 구조 설계", 한국정보처리학회 논문지, VOL. 8-C, NO.06, pp. 711 ~ 0720, 2001. 12

[14] The "stacheldraht" distributed denial of service attack tool, http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

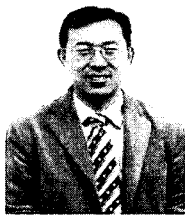
[15] Yu Chen, Kai Hwang, "Collaborative Change Detection of DDoS Attacks on Community and ISP Networks", Collaborative Technologies and Systems, May 2006

◐ 저 자 소 개 ◑

송 병 학(Byung-Hak Song)
2005년 경희대학교 컴퓨터공학과 졸업(학사)
2007년 경희대학교 대학원 컴퓨터공학과 졸업(석사)
2007년~현재 (주)플랜티넷 신기술개발팀
관심분야 : Network Security, Network Management, Broadband Network
E-mail : bhsong@plantynet.com

이 승 연(Seung-Yeon Lee)
2004년 서울여자대학교 컴퓨터공학과 (학사)
2007년 경희대학교 일반대학원 컴퓨터공학과 졸업(석사)
2007년~현재 한국과학기술정보연구원 그리드컴퓨팅연구팀
관심분야 : Mobile IPv6, Security, Telemetics. Grid Computing
E-mail : seungyeon@kisti.re.kr

홍 충 선(Choong-Seon Hong)
1983년 경희대학교 전자공학과 졸업(학사)
1985년 경희대학교 대학원 전자공학과 졸업(석사)
1997년 Keio대학교 대학원 정보통신공학과 졸업(박사)
1988~1999년 KT 통신망 연구소 수석연구원/네트워킹연구실장
1999~현재 경희대학교 컴퓨터공학과 교수
관심분야 : Network Management, Next Generation Internet, Mobile Computing, Network Security
E-mail : cshong@khu.ac.kr



허 의 남(Eui-Nam Huh)
1990년 부산대학교 전산통계학과 졸업(학사)
1995년 Univ. of Texas at Arlington 컴퓨터공학과 졸업(석사)
2000년 Ohio University 컴퓨터공학과 졸업(박사)
2002년 삼육대학교
2003년 서울여자대학교 정보통신공학부 조교수
2005년~현재 경희대학교 전자정보공학부 부교수
관심분야 : 텔레메틱스, 그리드 컴퓨팅, 센서 네트워크, 보안
E-mail : huh@icns.khu.ac.kr

손 승 원(Seong-won Sohn)
1984년 경북대학교 전자공학과 졸업(학사)
1994년 연세대학교 대학원 전자공학과 졸업(석사)
1999년 충북대학교 대학원 컴퓨터공학과 졸업(박사)
1998년 한국전자통신연구원 교환전송기술연구소 NTB 팀장, 인터넷구조팀장
2000년 한국전자통신연구원 정보보호기술연구본부 정보보호응용연구부장
2004년 한국전자통신연구원 정보보호연구단장
2007년~현재 한국전자통신연구원 IT융합서비스부문 수석단장
관심분야 : 정보보호
E-mail : swsohn@etri.re.kr