Journal of Korea Multimedia Society Vol. 13, No. 4, April 2010(pp. 594-600)

SIP 환경에서의 DDoS 공격 탐지를 위한 확장된 TRW 알고리즘 검증

윤성열[†], 하도윤[††], 정현철[†††], 박석천[††††]

요 약

인터넷 망에서의 서비스 거부 공격에 대해서는 많은 연구가 진행 중이지만 음성망에서는 그 연구가 미흡한 실정이다. 따라서 본 논문에서는 위의 문제점을 해결하기 위해 IP 데이터망을 사용하는 음성망을 대상으로 한 DDoS 공격 트래픽 탐지 알고리즘인 확장된 TRW 알고리즘을 설계하고 평가하였다. 본 논문에서 제안한 알고리즘은 기존 DDoS 공격을 인터넷 망에서 탐지하는 TRW 알고리즘을 분석하고, 이를 음성망에 적용하기 위해 연결 과정과 연결 종료 과정을 설계하며, 이를 카운트하는 확률 함수를 정의하였다. 제안한 알고리즘을 검증하기 위해 임계치를 설정하고, NS-2 시뮬레이터를 이용하였다. 공격 트래픽 종류에 따른 탐지율을 측정하였으며, 공격 패킷의 공격속도에 따른 탐지 시간을 측정하였다. 평가 결과 0.1초당 1개의 INVITE 공격 패킷을 송신하였을 때 이를 탐지하기 위한 시간으로 4.3초가 소요되었고, 각기 다른 15,000개의 공격 패킷을 송신하였을 때 13,453개를 공격으로 판단하였기 때문에 전체 공격에 대한 탐지율로 89.6%의 성능을 확인할 수 있었다.

Verification of Extended TRW Algorithm for DDoS Detection in SIP Environment

Sung Yeol Yun[†], Do Yoon Ha[††], Hyun Cheol Jeong[†††], Seok Cheon Park[††††]

ABSTRACT

Many studies are DDoS in Internet network, but the study is the fact that is not enough in a voice network. Therefore, we designed the extended TRW algorithm that was a DDoS attack traffic detection algorithm for the voice network which used an IP data network to solve upper problems in this article and evaluated it. The algorithm that is proposed in this paper analyzes TRW algorithm to detect existing DDoS attack in Internet network and, design connection and end connection to apply to a voice network, define probability function to count this. For inspect the algorithm, Set a threshold and using NS-2 Simulator. We measured detection rate by an attack traffic type and detection time by attack speed. At the result of evaluation 4.3 seconds for detection when transmitted INVITE attack packets per 0.1 seconds and 89.6% performance because detected 13,453 packet with attack at 15,000 time when transmitted attack packet.

Key words: Voice Network(음성망), DDoS(분산 서비스 거부 공격), Detection(탐지), Session Initiation Protocol(세션 개시 프로토콜), Threshold Random Walk(경계 임의 보행)

※ 교신저자(Corresponding Author) : 박석천, 주소 : 경기도 성남시 수정구 북정동 산 65번지(461-701), 전화 : 031)750-5328, FAX : 031)750-5662, E-mail : scpark@kyungwon.ac.kr
접수일 : 2009년 11월 30일, 수정일 : 2009년 12월 18일
완료일 : 2009년 12월 24일
[†] 정회원, 경원대학교 전자계산학 박사과정
(E-mail : existmaster@ku.kyungwon.ac.kr)
[††] 정회원, 한국인터넷진흥원 융합보호R&D팀 책임연구원
(E-mail : dyha@kisa.or.kr)
[†††] 정회원, 한국인터넷진흥원 융합보호R&D팀 팀장
(E-mail : hcjung@kisa.or.kr)
[††††] 종신회원, 경원대학교 IT대학 정교수
※ 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT 산업원천기술개발사업의 일환으로 수행하였음. [2008-S-028-02, SIP기반 응용서비스 보호를 위한 침입대응기술 개발]

1. 서 론

네트워크에서는 정보 교환의 수요를 충족시키기 위해 수많은 인터넷기반 서비스들이 등장하였다. 그러나 이와 같은 서비스는 DDoS(분산 서비스 공격 : Distributed Denial of Service) 공격과 같은 응용 프로그램이나 네트워크 시스템의 취약성을 이용한 악의적인 공격이 발생할 경우 적절하게 대응하지 못하는 문제점을 가지고 있다[1].

DoS(서비스 거부 공격 : Denial of Service) 공격은 흔히 말하는 보안의 3대요소인 CIA(Confidentiality, Integrity, Availability) 중 가용성을 저해하는 공격이다. DDoS는 이 목표를 달성하기 위하여 복수의 공격 엔티티가 참여한다. 그 결과로써 희생자는 악성 트래픽을 수신하게 되고 손실을 입게 된다[2].

DDoS 공격을 탐지하는 알고리즘으로는 TRW (Threshold Random Walk), DEWP(Detecting Early Worm Propagation through Packet Matching), Statistical Intrusion Detection 알고리즘 등이 있는데 이는 일반 인터넷망에서 DDoS 공격을 탐지하는 알고리즘이다[3-5].

그러나 DDoS 공격은 이런 인터넷망을 응용한 VoIP(Voice over IP) 네트워크에서도 발생할 수 있다. VoIP 네트워크에서 발생하는 DDoS 공격의 경우에는 응용계층에서의 공격 방식이 존재하는데, 이는 일반 인터넷망에서 DDoS를 탐지하는 알고리즘으로 탐지하기 어렵다.

따라서 본 논문에서는 음성망 환경에서 발생가능한 DDoS 공격을 탐지하는 알고리즘을 설계하고 검증하였다. 본 논문의 구성은 2장에서 관련연구로 SIP와 DDoS 공격에 대해 분석하고, 3장에서 확장된 TRW 알고리즘을 제안하고 임계값을 구하는 공식을 도출한다. 4장에서는 제안한 알고리즘을 검증하기 위해 시뮬레이션 환경 및 검증 파라미터를 정의하고, 임계값을 설정하며, 검증 결과에 대한 분석을 한다.

2. 관련 연구

2.1 SIP (Session Initiation Protocol)

SIP는 VoIP 서비스를 이용하기 위한 호 제어 프로토콜이다. 이 프로토콜은 세션을 설정하고, 이를 제어하기위한 다양한 명령어들을 정의한다.

과거에 비해 인터넷 전송 속도가 빨리지고 음질면에 있어서도 많이 향상되어, 저렴한 가격비용으로 점차 VoIP 사용자수가 크게 늘어났다[6].

전화를 걸고 받을 수 있는 터미널을 UAC(User Agent Client)라고 하고, 받는 쪽을 UAS(User Agnet Server)라고 한다. 또한 SIP 네트워크 망을 제어하는 것으로 H.323의 게이트키퍼와 비슷한 역할을 하는 Proxy Server와 사용자의 이동성을 보장하기 위한 Redirect Server가 주요 구성요소이다[7].

- UA (User Agent) : UAC(UA Client)와 UAS (UA Server)로 구분되며 실제 SIP 요청 및 응답 메시지를 처음 생성하는 주체이다.
- Proxy Server : 주된 역할은 수신된 SIP 메시지를 어디로 보낼지를 결정(라우팅)하는 것이다. 이를 굳이 구분하자면 Outbound Proxy Server와 Inbound Proxy Server로 구분할 수 있다.
- Outbound Proxy Server : UAC로부터 SIP 요청 메시지를 수신하면 이를 해석하고 필요할 경우 요청 메시지의 헤더 값을 재구성하여 UAS 측으로 전송한다.
- Inbound Proxy Server : 수행하는 역할은 Outbound Proxy Server의 역할과 비슷하지만 주된 역할은 UAC로부터 수신한 SIP 요청 메시지를 처리하여 해당 UAS로 전달하고, 이에 대한 처리 결과를 UAS로부터 수신하면 다시 이를 UAC로 응답 메시지의 전송이다.
- DNS Server : DNS Server는 Inbound Proxy Server의 주소 정보를 가지고 있다. UAC로부터 Outboud Proxy Server가 SIP 요청 메시지를 수신하였을 경우 해당 SIP 요청 메시지를 어디로 전송할지에 대한 address, port, transport 정보를 알고 있어야 한다.
- Location Server : Location Server는 사용자(SIP UA)의 위치 정보를 등록해 놓은 데이터베이스이다. 보통 Registration Server와 같은 물리적 서버에 상주하며, SIP REGISTER 요청 메시지를 통해 사용자의 현재 위치 정보가 등록 및 업데이트된다.

VoIP는 기존 IP 네트워크상에서 이루어 졌던 DoS/DDoS의 공격과 VoIP에서만 이루어 질수 있는

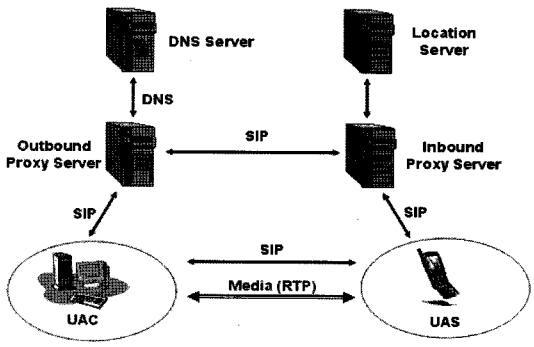


그림 1. SIP의 구성도

DoS/DDoS 공격들이 존재한다. 이런 공격들은 VoIP의 주요 요소인 SIP 서버의 자원을 고갈시키거나 파괴하여 해당 시스템이 정상적인 서비스를 할 수 없도록 무력화 시키는 공격, 다량의 VoIP Call 요청 및 비정상적인 패킷을 대량으로 발송하여 회선 자원을 고갈시켜 정상적인 서비스가 불가능하게 하는 공격, 불법 제어 메시지의 전송을 통하여 특정 사용자의 호 설정 또는 진행 중인 음성통화를 방해 및 중단시키는 공격, 해킹을 통하여 시스템의 장애를 일으키는 공격 등이 있다.

2.2 DDoS 공격

DDoS 공격은 인터넷에 개방되어 있으면서 동시에 한정된 자원(네트워크의 대역폭, 시스템의 패킷 처리 용량, 시스템에 도착한 패킷의 처리를 위하여 이용되는 시스템의 제반 자원 등)을 가진 모든 시스템들을 쉽게 공격의 대상으로 하여 피해를 입힌다는 점에서 매우 심각하게 여겨지고 있으며, 이에 대한 연구가 다양한 방향으로 진행되고 있다.

침입은 자원의 무결성, 비밀성 그리고 가용성을 위협하기 위해서 시도되는 일련의 행위들로 정의된다. DDoS 공격은 이들 위협 중 시스템 자원뿐만 아니라 네트워크 자원의 가용성을 침해하는 행위이며, 최근 들어 이러한 분산 서비스거부 공격으로 인한 피해 사례가 증가하고 있다. 분산 서비스거부 공격이 일반적으로 정상적인 프로토콜 패킷을 사용하기 때문에 이들 공격을 단지 사용자 인증 혹은, 암호화에 의한 정보보호 등의 침입 방지 기술로는 완전히 막기가 어렵다[8].

DDoS 공격이 위협적인 이유 중 하나는 자동화된 공격 툴 때문이다. 자동화된 공격 과정으로 인해 공격 자가 일단 취약한 시스템을 발견하면, 공격 툴을 설치하고 실제 공격을 수행하는데 5초 이상이 걸리지 않는다. 대표적인 DDoS 공격 툴로 Trinoo, Synk4, TFN, TFN2k 그리고 Stacheldraht가 있다. 이들 공격 툴은 특정 포트번호와 프로토콜을 사용하지만 쉽게 변경 가능하다. 따라서 공격자와 마스터, 마스터와 에이전트 간의 제어 메시지를 모니터링 하여 공격을 탐지한다는 것이 현실적으로 어렵다[9].

2.3 TRW 알고리즘

IP 데이터망에서 사용하는 DDoS 공격 트래픽 탐지 알고리즘인 TRW 알고리즘은 MIT에서 이루어지고 있는 연구로써 수학적 알고리즘인 TRW 수식을 이용해서 트래픽 패턴을 분석해 웜을 찾아내는 방법이다. 이 방식은 TCP 프로토콜을 사용한 웜을 대상으로 한 것으로, TCP 프로토콜의 처음 연결을 위한 SYN 패킷을 스캐닝 동작으로 보고 이 정보를 바탕으로 Sequential Hypothesis Testing 방식을 이용하여 식 1과 같이 비정상 트래픽 패턴을 찾아낸다[10].

$$Y_i = \begin{cases} 0 \; if \; the \; connection \; succeeds \\ 1 \; if \; the \; connection \; fails \; or \; end \; connection \end{cases} \quad (1)$$

Λ(Yn)의 특정 I번째의 확률을 식 2에서처럼 f(Yi)로 나타낼 수 있다.

$$\phi(Y_i) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} = \begin{cases} \frac{\theta_1}{\theta_0} & \text{if } Y_i = 0 (success) \\ \frac{1-\theta_1}{1-\theta_0} & \text{if } Y_i = 1 (failure) \end{cases} \quad (2)$$

이때, Λ(Yn) 은 Λ(Yn-1)에 f(Yi)로 표현이 가능하고, 이는 식 3으로 나타낼 수 있다.

$$\Lambda(Y_n) \equiv \prod_{i=1}^{n} \phi(Y_i) = \Lambda(Y_{n-1}) \phi(Y_n) \quad (3)$$

그러나 TRW 알고리즘은 TCP 계층에서의 DDoS 탐지 알고리즘이기 때문에 SIP 환경에 그대로 적용하기에는 문제점이 있다. 특히 TCP에서의 3-hand-shake만을 고려하였기 때문에 이외의 다른 프로토콜에는 적용하기 힘들다. 따라서 본 논문에서는 연결과정과 연결해제 과정에 따른 SIP 메시지를 고려하여 SIP 환경에서도 적용이 가능한 확장된 TRW 알고리즘을 제안한다.

3. SIP 환경에서 DDoS 공격 탐지를 위한 확장된 TRW 알고리즘

3.1 확장된 TRW 알고리즘

유무선망에서 사용하는 TRW 알고리즘의 Y값은 TCP SYN 패킷 등에 대해 반응하였으나 음성망에서는 이와 유사한 다른 패킷에 반응한다. 식 1에서 비정상 트래픽과 그때 연결상태를 나타내는 수식으로 확장된 TRW는 식 4와 식 5로 표현한다.

$$Y_i = \begin{cases} 0 \; if \; the \; connection \; succeeds \\ 1 \; if \; the \; connection \; fails \end{cases} \tag{4}$$

$$Z_i = \begin{cases} 0 \; if \; the \; endconnection \; succeeds \\ 1 \; if \; the \; endconnection \; fails \end{cases} \tag{5}$$

식 4에서 Yi 값은 INVITE, Register, Ack 패킷에 반응하는 연결설정 관련 변수를 나타내고, 식 5에서 Zi 값은 Cancel, Bye, OK 패킷에 반응하는 연결설정 관련 변수를 나타낸다. 이때, 식 3에서 표현되는 카운트 변수는 연결 설정과 연결 해제에 대한 특정 I번째의 확률을 f(Yi)로 나타낼 수 있다. 마찬가지로 Λ(Zn)의 특정 I번째의 확률을 f(Zi)로 나타낼 수 있다. 식 6과 식 7은 f(Yi)과 f(Zi)의 정의이다.

$$\phi(Y_i) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} = \begin{cases} \dfrac{\theta_{Y1}}{\theta_{Y0}} & \text{if } Y_i = 0 (success) \\ \dfrac{1-\theta_{Y1}}{1-\theta_{Y0}} & \text{if } Y_i = 1 (failure) \end{cases} \tag{6}$$

$$\phi(Z_i) \equiv \frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} = \begin{cases} \dfrac{\theta_{Z1}}{\theta_{Z0}} & \text{if } Z_i = 0 (success) \\ \dfrac{1-\theta_{Z1}}{1-\theta_{Z0}} & \text{if } Z_i = 1 (failure) \end{cases} \tag{7}$$

식 6과 7에서 각 확률함수를 파이로 표현할 수 있고, 식 8과 9는 식 6과 식 7을 이용하여 도출된 Λ(Yn)과 Λ(Zn)의 일반식이다.

$$\Lambda(Y_n) = \prod_{i=1}^{n} \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} \tag{8}$$

$$\Lambda(Z_n) \equiv \prod_{i=1}^{n} \frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} \tag{9}$$

각각 두 개의 식은 하나의 Time 축을 이용하여 좌표 쌍으로 표현이 가능하다. Λ(Y0) = 1, Λ(Z0) = 1을 가정한다.

3.2 확장된 TRW 알고리즘의 임계값

확장된 TRW 알고리즘의 임계값은 알고리즘의 유효탐지율을 설정하기 위한 값이다. 본 논문에서 확장된 TRW 알고리즘을 검증하기 위해 시뮬레이션 모델을 사용하였는데, 이때 필요한 임계값인 ηl1 과 ηl0를 구하기 위해서 파라미터를 표 1과 같이 정의하였다.

정상적으로 작동되는 알고리즘은 오탐율이 α0값 보다는 작아야 하고, 탐지율이 β0값 보다는 높아야 한다. 이 변수를 이용해 임계값인 ηc1 과 ηc0를 정의하면 식 10과 같다.

$$\eta_{c1} \le \frac{P_c}{P_{cf}} \quad \text{and} \quad \frac{1-P_c}{1-P_{cf}} \le \eta_{c0} \tag{10}$$

이 식을 Pcf의 형태로 정리하면 식 11과 같이 임계치인 ηc1의 값을 구할수 있다.

$$P_{cf} < \frac{1}{\eta_{c1}} = \frac{\alpha_0}{\beta_0} \tag{11}$$

이와 마찬가지로 1-Pc의 확률도 다음과 같이 정리하면 식 12와 같이 ηc0의 값을 구할 수 있다.

$$1 - P_c < \eta_{c0} = \frac{1-\beta_0}{1-\alpha_0} \tag{12}$$

연결 종료와 관련된 임계치도 위의 단계를 이용하여 식 13과 14로 나타낼 수 있다.

$$P_{ef} < \frac{1}{\eta_{e1}} = \frac{\alpha_1}{\beta_1} \tag{13}$$

$$1 - P_e < \eta_{e0} = \frac{1-\beta_1}{1-\alpha_1} \tag{14}$$

표 1. 확장된 TRW 알고리즘의 파라미터

파라미터	내 용
η_{c1},η_{c0}	$\Lambda(Y_n)$의 임계값
η_{e1},η_{e0}	$\Lambda(Z_n)$의 임계값
P_c	연결 과정 DDoS 공격시의 탐지율
P_{cf}	연결 과정 DDoS 공격이 없을 때 오탐율
P_e	연결종료 과정 DDoS 공격시의 탐지율
P_{ef}	연결종료 과정 DDoS 공격이 없을 때 오탐율
α_0,β_0	연결 과정 오탐율의 최고점, 탐지율의 최저점
α_1,β_1	연결종료 과정 오탐율의 최고점, 탐지율의 최저점

IV. SIP 환경에서 DDoS 공격 탐지를 위한 확장된 TRW 알고리즘 검증

4.1 시뮬레이션 환경 및 검증 파라미터

기존의 TRW 알고리즘은 음성망 환경에서 적용할 수 없기 때문에 제안한 알고리즘은 TRW 알고리즘을 기반으로 SIP 환경에서 적용할 수 있게 확장하였다. 따라서 확장한 TRW 알고리즘이 음성망 환경에서 정상적으로 적용할 수 있는지를 검증해야 한다. 본 알고리즘의 검증은 NS-2 시뮬레이터를 이용 하여 가상의 음성망을 시뮬레이션 하였으며, 설계한 시뮬레이션 모델은 그림 2와 같다. 그리고 확장된 TRW 알고리즘 검증을 위한 시뮬레이션 파라미터는 표 2와 같이 정의하였다.

DDoS 탐지 알고리즘의 성능 측정을 위한 검증 파라미터는 공격이 시작되고 난 후 얼마나 빠른 시간에 공격을 탐지하는 지에 대한 탐지속도와, 공격인지 아닌지를 판단하는 탐지율 두 가지이다.

탐지속도를 측정하기 위해 공격자 노드는 0.1초당 1개의 INVITE 공격 패킷을 송신하고, 이때 Λ(Yn)값의 변화를 탐지한다.

탐지율을 측정하기 위해 DDoS 탐지모듈에 1000개의 공격자 노드를 붙이고 각 노드는 Resitser공격, INVITE공격, Bye 공격, Cancel 공격이 가능하다. 각각의 공격은 그 패킷이 발생되는 수가 다른데, Register 패킷은 정기적으로 UA의 등록을 담당하는 패킷으로, 일정 주기마다 발생한다. 또한 INVITE 패킷은 접속을 설정할 때 발생한다. 이 두가지 패킷은 평소에 발생하는 양이 매우 많으므로 공격에 응용하기 위해서 많은 수를 할당하였다. 본 논문에서는 Register 공격은 총 5700번, INVITE 공격은 6300번, Bye 공격은 1000번, 그리고 Cancel 공격은 2000번시도한다.

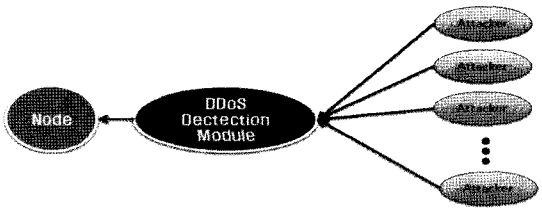


그림 2. 확장된 TRW 검증을 위한 시뮬레이션 모델

표 2. 확장된 TRW 검증을 위한 시뮬레이션 파라미터

파라미터	값
$\Lambda(Y_n)$의 임계값	1980
$\Lambda(Z_n)$의 임계값	1980
Θ_{Y0}	0.7
Θ_{Y1}	0.4
시간당 공격패킷 수	0.1초당 1개

4.2 확장된 TRW 임계값 설정

확장된 TRW 알고리즘의 탐지율과 탐지 시간을 측정하려면 먼저 정상적으로 동작하는 알고리즘의 기준으로 임계값을 설정해야 한다. 이를 위해서는 허용되는 오탐율의 최고값인 α값과 허용되는 탐지율의 최저값인 β값을 설정해야 한다. 이는 다음과 같이 나타낼수 있다.

$$\alpha_0 = 0.0005,\ \beta_0 = 0.99$$
$$\alpha_1 = 0.0005,\ \beta_1 = 0.99$$

DDoS 공격이 아닌데도 공격으로 탐지할 확률을 0.0005, DDoS 공격이 시도되었을 때 공격으로 탐지할 확률 0.99를 목표로하는 임계값을 유도 하면 식 15와 식 16과 같다.

$$\eta_{c1} = \frac{\beta_0}{\alpha_0} = \frac{0.99}{0.0005} = 1980$$
$$\eta_{c0} = \frac{1-\beta_0}{1-\alpha_0} = \frac{0.01}{0.9995} \fallingdotseq 0.01 \quad (15)$$

$$\eta_{e1} = \frac{\beta_0}{\alpha_0} = \frac{0.99}{0.0005} = 1980$$
$$\eta_{e0} = \frac{1-\beta_0}{1-\alpha_0} = \frac{0.01}{0.9995} \fallingdotseq 0.01 \quad (16)$$

즉, 구해진 임계값에 따르면 Λ(Yn)와 Λ(Zn)는 1980이라는 수치를 초과하게 되면 DDoS라 판단하게 된다.

4.3 확장된 TRW 알고리즘 검증 및 분석

확장된 TRW 알고리즘을 검증하기 위해서 NS-2 시뮬레이터를 이용하여 알고리즘의 탐지율과 탐지 시간을 측정하였다. NS-2에서는 Application Level에의 패킷내용에 대한 정의는 지원하지 않기 때문에 이를 대체하기 위해 공격으로 설정한 패킷은 각 공격의 이름으로 라벨링 하였다.

그림 3은 0.1초당 1개의 INVITE 공격 패킷을 보냈을 때 Λ(Yn)의 값을 나타낸다. 이 값이 임계치를 초과하였을 때 본 알고리즘은 공격임을 탐지할 수 있다.

그림 3에 따르면 공격이 시작되고 약 4.3초가 지났을 때 Λ(Yn)가 최초로 임계치값인 1980에 도달하고 이때 공격임을 판단한다. 그리고 시간당 공격패킷의 수가 더욱 많다면 이를 탐지하는데 걸리는 시간은 더 빠를 것이라 예상할 수 있다.

또한 DDoS 공격의 탐지 시간뿐만 아니라 DDoS 공격의 종류에 따른 탐지 율을 측정하였다. 제안한 검증 모델과 동일하게 검증을 시도하였을 때 이에 대한 탐지율은 그림 4와 같다.

Register 공격에는 5700번의 공격 중 5329개를 공격이라 탐지하였고, INVITE 공격은 6300번 중 5980번을, Bye 공격은 1000번 중 568번을, Cancel 공격은 2000번 중 1576번을 공격이라 탐지하였다. 각각의 탐지 율은 57%에서 93%까지의 분포를 보이고, 총 공격 패킷에 대한 탐지율은 89.6%로 측정되었다.

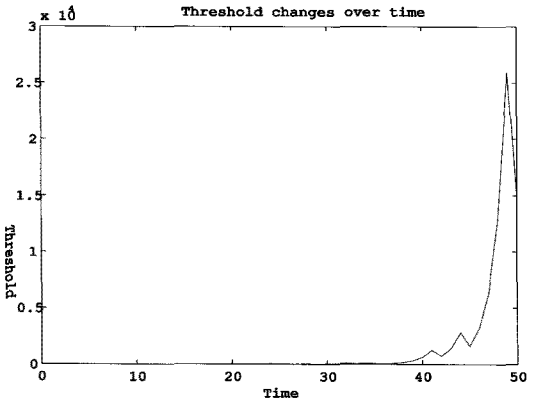


그림 3. 시간값에 따른 Λ(Yn)의 값의 변화

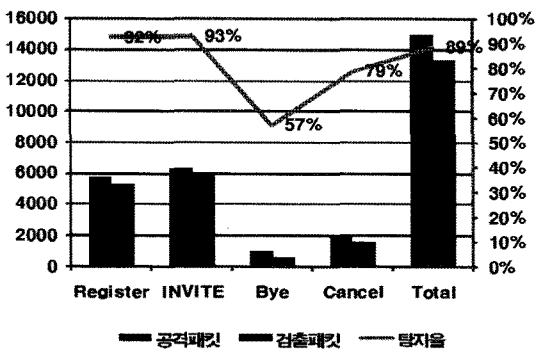


그림 4. DDoS 공격종류에 따른 탐지율

실험을 통하여 제시된 알고리즘은 전체 공격중 공격 패킷이 적은 Bye공격에는 약간 낮은 수치의 탐지율을 보였으나 이는 전체 시도된 공격에 비해 상당히 적은 양임을 고려할 때 전체 탐지 율이 높기 때문에 실제 공격에는 강한 탐지 율을 보임을 확인하였다.

5. 결 론

음성망 네트워크는 다양한 응용 서비스와 향상되는 VoIP 서비스로 인해 나날이 발전하고 있으며 사용자 수도 급증하고 있다. 그러나 이런 음성망 환경은 DDoS 공격과 같은 응용 프로그램이나 네트워크 시스템의 취약성을 이용한 악의적인 공격이 발생할 경우 적절하게 대응하지 못하는 문제점을 가지고 있다.

주로 일반 인터넷 망에서의 서비스 공격에 대해서는 많은 연구가 진행 중이지만 음성망에서는 그 연구가 미흡한 실정이다. 따라서 본 논문에서는 위의 문제점을 해결하기 위해 IP 데이터망을 사용하는 음성망을 대상으로 한 DDoS 공격 트래픽 탐지 알고리즘인 확장된 TRW 알고리즘을 설계하고 평가하였다.

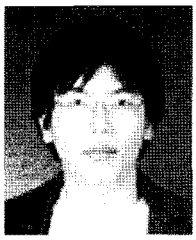
본 논문에서 제안한 알고리즘은 기존 DDoS 공격을 인터넷 망에서 탐지하는 TRW 알고리즘을 분석하고, 이를 음성망에 적용하기 위해 연결 과정과 연결 종료 과정을 설계하며, 이를 카운트하는 확률 함수를 정의하였다. 제안한 알고리즘을 검증하기 위해 임계치를 설정하고, NS-2 시뮬레이터를 이용하여 공격트래픽 종류에 따른 탐지율을 측정하였으며, 공격패킷의 공격속도에 따른 탐지 시간을 측정하였다. 측정결과 0.1초당 1개의 INVITE 공격 패킷을 송신하였을 때 이를 탐지하기 위한 시간으로 4.3초가 소요되었고, 각기 다른 15000개의 공격 패킷을 송신하였을 때 13453개를 공격으로 판단하였기 때문에 전체 공격에 대한 탐지율로 89.6%의 성능을 확인할 수 있었다.

향후에는 실제 VoIP 환경에서 발생되는 패킷에 대한 분석을 통해 다양한 공격에도 탐지할 수 있는 알고리즘으로 개선하고자 한다.

참 고 문 헌

[1] 유경민, 심상헌, 한경은, 소원호, 김영선, 김영천, "DDoS 공격 탐지를 위한 확장된 블룸 필터

기반의 효율적인 목적지 주소 모니터링 기법", 한국통신학회, 한국통신학회논문지 제33권 제3호(네트워크 및 서비스), pp. 152-158, 2008. 3.
[2] 전용희, 장종수, 오진태, "DDoS 공격 및 대응 기법 분류", 정보보호학회, 정보보호학회지 제19권 제3호, pp. 46-57, 2009. 6.
[3] J.Y. Jung, S. Schechter, and Arthur W. Berger, "Fast Detection of Scanning Worm Infections," RAID 2004, Sophia Antipolis French, Sep. 2004.
[4] Xuan Chen and John Heidemann, "Detecting Early Worm Propagation through Packet Matching," *ISI Tech. Report* 2004-585, Feb. 2004.
[5] Cliff Changchun Zou, Weibo Gong, and Don Towsly, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," ACM WORMS '03, Washington DC, USA, Oct. 2003.
[6] 최재덕, 정태운, 정수환, 김영한, "SIP 기반의 VoIP 보안 시스템 구현", 한국통신학회, 한국통신학회논문지 제29권 9B호, pp. 799-807, 2004. 9.
[7] 최경호, 임을규, "SIP Call Signaling을 위한 사용자 인증 기법", 한국정보과학회, 한국정보과학회 2008 종합학술대회 논문집 제35권 제1호(D), pp. 110-115, 2008. 6.
[8] 김미희, 나현정, 채기준, 방효찬, 나중찬, "분산 서비스거부 공격 탐지를 위한 데이터 마이닝 기법", 한국정보과학회, 한국정보과학회논문지, 정보통신 제32권 제3호, pp. 279-290, 2005. 6.
[9] Paul J. Criscuolo, "Distributed Denial of Service - Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht," CIAC-2319, Feb. 2000.
[10] 조제경, 이형우, 박영준, "IAD 기반 패킷 마킹과 유무선 트래픽 분류를 통한 무선 DDoS 공격 탐지 및 차단 기법", 한국콘텐츠학회, 한국콘텐츠학회논문지 제8권 제6호, pp. 54-65, 2008. 6.



윤 성 열

2007년 한국교육개발원 학사
2009년 경원대 전자계산학과 석사
2009년~현재 경원대 전자계산학과 박사과정
관심분야 : 음성통신, 네트워크 시큐리티, RFID/USN

하 도 윤

1998년 동아대 환경공학과 학사
2006년 전남대 정보보호학과 석사
2005년 전남대 박사과정
2000년~현재 한국인터넷진흥원 융합보호R&D팀 책임연구원
관심분야 : 정보보호, 시스템보안, 침해사고대응

정 현 철

1996년 서울시립대 전산통계학 학사
1999년 광운대학교 전산학과 석사
1996년~현재 한국인터넷진흥원 융합보호R&D팀 팀장
관심분야 : IPTV, 봇넷, VoIP 보안, 침해사고대응

박 석 천

1977년 고려대 전자공학과 학사
1982년 고려대 컴퓨터공학 석사
1989년 고려대 컴퓨터공학 박사
1979년~1985년 금성통신연구소
1991년~1992년 UC, Irvine Post Doc.
1988년~현재 경원대학교 컴퓨터공학과 정교수
관심분야 : 차세대 인터넷, 멀티미디어 통신, 네트워크 시큐리티, 액티브 네트워크