음성망 환경에서 DDoS 공격 탐지 알고리즘 설계 및 평가

윤성열* · 김환국** · 박석천*

Design and Evaluation of DDoS Attack Detection Algorithm in Voice Network

Sung-Yeol Yun* · Hwan-Kuk Kim** · Seok Cheon Park*

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였음.
[2008-S-028-02, SIP기반 응용서비스 보호를 위한 침입대응기술 개발]

요 약

본 논문에서 제안한 알고리즘은 IP데이터망에서 웜 스캐닝 공격을 탐지하는 TRW 알고리즘을 분석하고음성망에 적용하기 위해 연결 과정과 연결 종료 과정을 설계하며, 이를 카운트하는 확률 함수를 정의하였다. 제안한 알고리즘을 평가하기 위해 임계치를 설정하고, 공격트래픽 종류에 따른 연결확률을 변화시켜 알고리즘의 효율성을 측정하였으며, 공격패킷의 공격속도에 따른 탐지 시간을 측정하였다.

평가 결과 본 논문에서 제안한 알고리즘은 공격 속도가 초당 10패킷일 경우, DDoS 공격이 시도되고 약 1.2초 후에 탐지를 하고 초당 20개일 경우에는 약 0.5초 후에 탐지함을 확인하였다.

ABSTRACT

The algorithm that is proposed in this paper defined a probability function to count connection process and connection-end process to apply TRW algorithm to voice network. Set threshold to evaluate the algorithm that is proposed, Based on the type of connection attack traffic changing the probability to measure the effectiveness of the algorithm, and Attack packets based on the speed of attack detection time was measured.

At the result of evaluation, proposed algorithm shows that DDoS attack starts at 10 packets per a second and it detects the attack after 1.2 seconds from the start. Moreover, it shows that the algorithm detects the attack in 0.5 second if the packets were 20 per a second.

키워드
음성망, 분산 서비스 거부 공격, 탐지

Key word
Voice Network, DDoS, Detection, SIP

* 경원대학교
** 한국인터넷진흥원 보호기술팀

접수일자 : 2009. 09. 16
심사완료일자 : 2009. 11. 13

Ⅰ. 서 론

통신망의 발달로 수많은 인터넷기반 서비스들이 등장함에 따라 사용자는 다양한 콘텐츠를 이용할 수 있었다. 그러나 이런 인터넷기반 서비스는 유무선 환경에서 다양한 외부공격이 심화됨에 따라 사용자들이 정상적으로 서비스를 이용하지 못하거나, 악의적인 공격 등에 노출되는 문제점을 가지고 있다[1][2].

특히, 시스템 또는 네트워크 자원을 공격 대상으로 하는 서비스 거부 공격(DoS : Denial of Service) 및 분산 서비스 거부 공격(DDoS : Distributed DoS)의 문제가 대두되었는데, DoS는 대역폭, 프로세스 처리 능력 및 시스템 자원을 고갈시킴으로써 정상적인 서비스를 제공하지 못하게 만드는 모든 행위를 말한다. DDoS 공격의 공통점은 과도한 접속으로 네트워크 자원 및 대역폭을 소모시켜 다른 사용자의 정당한 접속을 불가능하게 하는 것이고, 때에 따라서는 네트워크 장비에 장애를 유발시키기도 한다. 간단히 생각한다면, 네트워크 대역폭이 굉장히 크거나, 네트워크 장비의 성능이 월등히 뛰어나다면 아무 문제없이 공격을 받아들일 수 있다고 생각할 수 있으나, 이는 매우 이상적인 경우일 뿐 실제로는 그렇지 않다. DDoS 공격을 받을 경우 IPS나 DDoS 공격 방어 장비 등의 보안장비가 구축되어 있지 않는 이상 피해를 고스란히 감수해야 하기 때문이다. 최근 빈번하게 발생하는 웜 바이러스에도 DDoS 공격 방식이 내장되어 피해를 주고 있어 DDoS 공격에 대한 대책이 시급하다[3][4].

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[5][6][7].

그러나 DDoS 공격은 일반 인터넷망 외에도 음성망 중 IP를 사용하는 VoIP(Voice over IP) 네트워크에서도 발생할 수 있다. VoIP 네트워크에서는 호 제어 프로토콜로 H.323과 SIP가 있는데, 최근에 사용하는 방식은 대부분 SIP를 사용하고 있다. 따라서 본 연구의 대상인 음성망 환경의 의미는 DDoS 공격이 가능한 SIP 환경에서 VoIP 네트워크 기반 환경으로 정의한다.

본 논문에서는 음성망 환경에서 발생가능한 DDoS 공격을 탐지하는 알고리즘을 설계하고 평가하였다.

Ⅱ. 관련 연구

2.1 VoIP

VoIP(Voice over IP)란 말 그대로 인터넷망의 근간인 IP 네트워크를 통해 음성을 전송하는 기술과 서비스를 말한다. 기존에 IP 네트워크는 데이터만을 전송했으나, 음성과 데이터를 하나의 망에서 통합 제공함으로써 망 자원의 효율적 사용과 인터넷과 연계된 다양한 부가 서비스의 제공이 가능하다는 장점이 있다. VoIP는 전화의 호(call)를 제어하는 프로토콜을 기반으로 한다.

VoIP 시스템의 구성요소는 크게 응용 계층(Application layer), 신호 계층(Signaling layer), 매체 계층(Media layer)으로 나눠지며, 각 계층별로 상대방과 같은 프로토콜을 이용하여 통신을 한다. 그림 1은 VoIP 시스템의 구조를 나타낸 것이다[8].

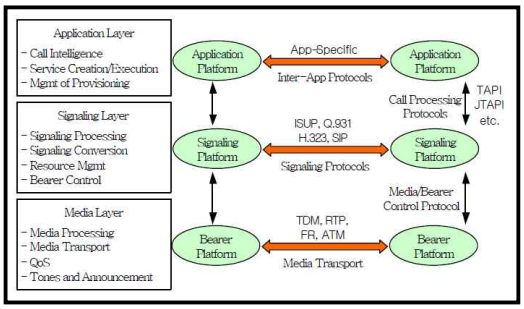

그림 1. VoIP 시스템의 구조
Fig. 1. Structure of VoIP System

이미 VoIP 기술은 90년대 중반부터 제기돼 다양한 프로토콜이 개발됐다. 이런 프로토콜에는 H.323, MGCP/MEGACO, SIP 등이 대표적이라고 할 수 있다[9].

2.2 SIP

SIP은 인터넷망을 이용한 음성 통신 서비스 또는 멀티미디어 서비스 등 융복합 서비스를 제공하기 위한 VoIP 서비스의 핵심 기술로서 파싱과 컴파일이 쉽고 텍스트 기반이기 때문에 H.323에 비하여 확장성이 뛰어나

고 구현이 쉬운 장점을 가지고 있다. 이를 이용하여 개발된 VoIP는 저렴하고 구현하기 쉬운 장점으로 급속도로 발전하였다.

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[10].

SIP은 Proxy Server를 통한 연결방법과 상대방과 직접 연결을 할 수 있는 방법 두 가지를 제공한다. 전화를 거는 쪽에서는 SIP에 맞는 주소방식을 사용하여 INVITE 메시지를 통화를 원하는 쪽에게 요청하게 된다.

SIP의 모든 메시지는 텍스트 기반이며 메시지를 전달할 때에는 TCP나 UDP를 사용하여 여러개의 메시지가 하나의 TCP 세그먼트나 UDP 데이터그램에 의해 보낸다. SIP 데이터 크기는 MTU를 알고 있는 네트워크에 대해서는 MTU의 값을 넘지 않는 한도에서 데이터를 보내고, MTU를 알 수 없는 네트워크에 대해서는 1KByte 이하의 데이터를 보낼 수 있도록 정의되어 있다.

2.3 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.

DDoS 공격은 여러 가지 형태로 구분되나 주로 대량의 트래픽을 유발하는 플러딩(Flooding) 공격, 과도한 세션을 요구하는 커넥션(Connection) 공격, 기타 애플리케이션(Application) 특성을 활용한 공격으로 나눌 수 있다[11].

특히 DDoS 공격 중 SIP Flooding 공격은 SIP 메시지를 대량으로 보내어 VoIP 사용자나 사업자가 정상적인 서비스를 이용 혹은 제공하지 못하게 하는 것이다[12].

2.4 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[13].

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

SIP 프로토콜의 처음 연결을 위한 INVITE 패킷을 스캐닝 동작으로 보고 이 정보를 바탕으로 Sequential Hypothesis Testing 방식을 이용해서 비정상 트래픽 패턴을 찾아내게 된다[14].

- H_0 = Host 1 이 스캐닝공격을 받지 않음
- H_1 = Host 1 이 스캐닝공격을 받음

$$\begin{aligned} &\Pr[Y_i = 0|H_0] = \theta_0, \;\; \Pr[Y_i = 1|H_0] = 1 - \theta_0 \\ &\Pr[Y_i = 0|H_1] = \theta_1, \;\; \Pr[Y_i = 1|H_1] = 1 - \theta_1 \end{aligned} \quad (2)$$

- Θ_0 = 스캐닝 공격을 받지 않고, 연결이 성공할 확률
- Θ_1 = 스캐닝 공격을 받았으나, 연결이 성공할 확률

$$\Lambda(Y_n) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} \quad (3)$$

식 3에서 $\Lambda(Y_n)$은 정상인 상태에 반비례하고 공격을 받았을 때 비례하는 확률함수를 나타낸다.

$$\Lambda(Y_n) \equiv \prod_{i=1}^{n} \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} \quad (4)$$

식 4에서 각 확률함수를 파이로 표현할 수 있고, $\Lambda(Y_n)$의 특정 I번째의 확률을 식 5에서처럼 $f(Y_i)$로 나타낼 수 있다.

$$\phi(Y_i) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} = \begin{cases} \frac{\theta_1}{\theta_0} & \text{if } Y_i = 0(success) \\ \frac{1-\theta_1}{1-\theta_0} & \text{if } Y_i = 1(failure) \end{cases} \quad (5)$$

이때, $\Lambda(Y_n)$ 은 $\Lambda(Y_{n-1})$에 $f(Y_i)$로 표현이 가능하고, 이는 식 6으로 나타낼 수 있다.

$$\Lambda(Y_n) \equiv \prod_{i=1}^{n} \phi(Y_i) = \Lambda(Y_{n-1})\phi(Y_n) \quad (6)$$

$\Lambda(Y_0) = 1$을 가정하고, 그 이후부터 Y값에 따른 $\Lambda(Y_n)$을 그림 2로 표현할 수 있다.

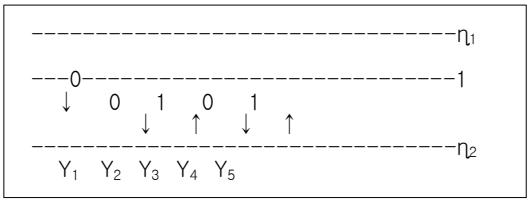

그림 2. TRW 임계치 측정
Fig. 2. TRW Threshold measurements

Ⅲ. 음성망 환경에서 DDoS 공격 트래픽 탐지 알고리즘 설계

제안하는 알고리즘은 TRW 알고리즘을 분석하여 음성망 환경에서 DDoS 공격 트래픽을 탐지할 수 있는 알고리즘을 설계하였다.

3.1 SIP-TRW

유무선망에서 사용하는 TRW 알고리즘의 Y값은 TCP SYN 패킷 등에 대해 반응하였으나 음성망에서는 이와 유사한 다른 패킷에 반응한다.

$$Y_i = \begin{cases} 0 \; if \; the \; connection \; succeeds \\ 1 \; if \; the \; connection \; fails \end{cases} \quad (7)$$

$$Z_i = \begin{cases} 0 \; if \; the \; endconnection \; succeeds \\ 1 \; if \; the \; endconnection \; fails \end{cases} \quad (8)$$

식 7에서 Y_i 값은 INVITE, Register, Ack 패킷에 반응하는 연결설정 관련 변수를 나타내고, 식 8에서 Z_i 값은 Cancel, Bye, OK 패킷에 반응하는 연결설정 관련 변수를 나타낸다.

- H_0 = Host I 이 DDoS 공격을 받지 않음
- H_1 = Host I 이 DDoS 공격을 받음

$$\Pr[Y_i = 0|H_0] = \theta_{Y0}, \;\; \Pr[Y_i = 1|H_0] = 1-\theta_{Y0} \quad (9)$$
$$\Pr[Y_i = 0|H_1] = \theta_{Y1}, \;\; \Pr[Y_i = 1|H_1] = 1-\theta_{Y1}$$

$$\Pr[Z_i = 0|H_0] = \theta_{Z0}, \;\; \Pr[Z_i = 1|H_0] = 1-\theta_{Z0} \quad (10)$$
$$\Pr[Z_i = 0|H_1] = \theta_{Z1}, \;\; \Pr[Z_i = 1|H_1] = 1-\theta_{Z1}$$

- Θ_{Y0}은 DDoS 공격을 받지 않고, 연결이 성공할 확률이다.
- Θ_{Y1}은 DDoS 공격을 받았으나, 연결이 성공할 확률이다.
- Θ_{Z0}은 DDoS 공격을 받지 않고, 연결이 정상적으로 종료될 확률
- Θ_{Z1}은 DDoS 공격을 받았으나, 연결이 정상적으로 종료될 확률

$$\Lambda(Y_n) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} \quad (11)$$

$$\Lambda(Z_n) \equiv \frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} \quad (12)$$

식 11과 12에서 $\Lambda(Y_n)$과 $\Lambda(Z_n)$는 정상인 상태에 반비례하고 공격을 받았을 때 비례하는 확률함수를 나타낸다.

$$\Lambda(Y_n) \equiv \prod_{i=1}^{n} \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} \quad (13)$$

$$\Lambda(Z_n) \equiv \prod_{i=1}^{n} \frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} \quad (14)$$

식 13과 14에서 각 확률함수를 파이로 표현할 수 있고, $\Lambda(Y_n)$의 특정 I번째의 확률을 $f(Y_i)$로 나타낼수 있다. 마찬가지로 $\Lambda(Z_n)$의 특정 I번째의 확률을 $f(Z_i)$로 나타낼수 있다. 식 15와 16은 도출된 $f(Y_i)$과 $f(Z_i)$의 일반식이다.

$$\phi(Y_i) \equiv \frac{\Pr[Y_n|H_1]}{\Pr[Y_n|H_0]} = \begin{cases} \frac{\theta_{Y1}}{\theta_{Y0}} & \text{if } Y_i = 0(success) \\ \frac{1-\theta_{Y1}}{1-\theta_{Y0}} & \text{if } Y_i = 1(failure) \end{cases} \quad (15)$$

$$\phi(Z_i) \equiv \frac{\Pr[Z_n|H_1]}{\Pr[Z_n|H_0]} = \begin{cases} \frac{\theta_{Z1}}{\theta_{Z0}} & \text{if } Z_i = 0(success) \\ \frac{1-\theta_{Z1}}{1-\theta_{Z0}} & \text{if } Z_i = 1(failure) \end{cases} \quad (16)$$

식 15와 16을 통해 각각 두 개의 식은 하나의 Time 축을 이용하여 좌표쌍으로 표현이 가능하다. $\Lambda(Y_0) = 1$, $\Lambda(Z_0) = 1$ 을 가정한다.

3.2 SIP-TRW의 임계값

SIP-TRW 알고리즘의 임계값을 인 η_1 과 η_0를 구하기 위해서 파라메터를 표 1에서 정의한다.

표 1. SIP-TRW 알고리즘의 파라메터
Table. 1. Parameter of SIP-TRW Algorithm

파라메터	내용
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

이때, P_c와 P_{cf}는 다음의 식을 만족해야 한다.

$$\alpha_0 \geq P_c \text{ and } \beta_0 \leq P_{cf} \quad (17)$$

즉, α_0값보다는 오탐율이 작아야 하고, β_0값 보다는 탐지율이 높아야 정상적으로 작동되는 알고리즘이라 판단할 수 있다. 이 변수를 이용해 임계값인 η_{c1} 과 η_{c0}를 정의하면 식 18과 같다.

$$\eta_{c1} \leq \frac{P_c}{P_{cf}} \quad \text{and} \quad \frac{1-P_c}{1-P_{cf}} \leq \eta_{c0} \quad (18)$$

이를 α_0와 β_0로 표현하면 식19와 과 같다.

$$\eta_{c1} \leftarrow \frac{\beta_0}{\alpha_0} \quad \text{and} \quad \eta_{c0} \leftarrow \frac{1-\beta_0}{1-\alpha_0} \quad (19)$$

따라서, 임계치인 η_{c1}의 확률은 $0 < P_c < 1$ 이므로 식 20을 도출할 수 있다.

$$\eta_{c1} \leq \frac{P_c}{P_{cf}} < \frac{1}{P_{cf}} \quad (20)$$

그리고, 이 식을 P_{cf}의 형태로 정리하면 임계치인 η_{c1}의 값을 구할수 있다.

$$P_{cf} < \frac{1}{\eta_{c1}} = \frac{\alpha_0}{\beta_0} \quad (21)$$

이와 마찬가지로 1-P_c의 확률도 다음과 같이 정리하면 η_{c0}의 값을 구할 수 있다.

$$1 - P_c < \eta_{c0} = \frac{1-\beta_0}{1-\alpha_0} \quad (22)$$

연결 종료와 관련된 임계치도 위의 단계를 이용하여 식 23과 24로 나타낼 수 있다.

$$P_{ef} < \frac{1}{\eta_{e1}} = \frac{\alpha_1}{\beta_1} \quad (23)$$

$$1 - P_e < \eta_{e0} = \frac{1-\beta_1}{1-\alpha_1} \quad (24)$$

Ⅳ. 음성망 환경에서 DDoS 공격 트래픽 탐지 알고리즘 평가 및 분석

SIP-TRW 알고리즘을 평가하기 위해서 연결확률에 따른 탐지 속도와 공격패킷 속도에 따른 탐지 시간을 수학적으로 증명한다. 우선 Network 트래픽을 가정하려면 본 알고리즘의 임계값을 가정해야 한다. 임계값을 가정하기 위해 네트워크 관리자 기준으로 알고리즘의 탐지율과 오탐율을 정할 수 있다. α는 오탐율의 최고점, β는

탐지율의 최저점을 뜻하는 것으로 다음과 같이 나타낼 수 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 확률을 0.99를 목표하는 임계치를 유도 하면 식 25와 식 26과 같다.

$$\eta_{c1} = \frac{\beta_0}{\alpha_0} = \frac{0.99}{0.0005} = 1980$$
$$\eta_{c0} = \frac{1-\beta_0}{1-\alpha_0} = \frac{0.01}{0.9995} \fallingdotseq 0.01 \quad (25)$$

$$\eta_{e1} = \frac{\beta_0}{\alpha_0} = \frac{0.99}{0.0005} = 1980$$
$$\eta_{e0} = \frac{1-\beta_0}{1-\alpha_0} = \frac{0.01}{0.9995} \fallingdotseq 0.01 \quad (26)$$

음성망 환경에서 가상의 트래픽을 정의하고, 정의한 트래픽 속성에서의 중요한 변수는 다음과 같다.

- ΘY_1 = DDoS 공격 중 연결이 정상적으로 연결될 확률
- ΘZ_1 = DDoS 공격 중 연결이 정상적으로 종료될 확률

ΘY_1 와 ΘZ_1 값에 따라 본 알고리즘의 성능을 측정할 수 있다. 본 알고리즘에서 $\Lambda(Y_n)$의 특정 I번째의 확률을 $f(Y_i)$로 나타낼수 있는데, 공격이 시도되면 Y의 값은 지속적으로 1을 나타내고, 그럴 경우 $f(Y_i)$의 값이 특정 기대치를 나타 낼 수 있다. 이 기대치를 $\Lambda(Y_n)$에 적용 시키면 임계점으로 다가가는 속도를 측정할 수 있으며 식 27, 식 28과 같다.

$$\Lambda(Y_n) \equiv \prod_{i=1}^{n} \phi(Y_i) = \Lambda(Y_{n-1})\phi(Y_i) \quad (27)$$

if DDoS Attack then

$$\Lambda(Y_n) = \Lambda(Y_{n-1})\phi(Y_i) = \Lambda(Y_{n-1})\left(\frac{(\theta_{Y1})^2}{\theta_{Y0}} + \frac{(1-\theta_{Y1})^2}{1-\theta_{Y0}}\right) \quad (28)$$

그림 3은 ΘY_1 의 값이 변화함에 따라 몇 개의 공격패킷을 수신했을 때 공격을 탐지 해낼 수 있는지를 계산한 그래프이다.

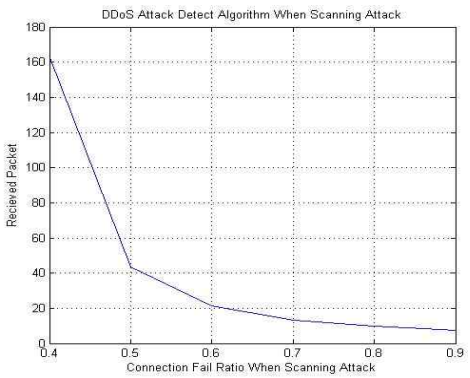

그림 3. 연결실패확률에 따른 탐지 속도
Fig. 3. Detection speed based on the connection fail probability

그림 3에서 1-ΘY_1 값(DDoS 공격 중 연결실패확률)이 증가함에 따라 DDoS 공격을 탐지 하기 위해 필요한 패킷의 수가 감소함을 확인할 수 있다. 연결실패확률이 0.4일 경우 DDoS 공격을 탐지하기 위해 필요한 연결실패패킷은 약 160개 이고, 0.7일 경우에는 약 17개이다.

본 알고리즘을 실제 네트워크에 적용하였을 때 성능에 영향을 미치는 평가 항목으로 공격자의 DDoS 공격 패킷이 얼마나 많은 양이 발생하느냐에 따른 탐지 시간이 있다. 본 알고리즘에서 DDoS 공격 중 연결실패확률을 0.7이라 가정하고 유입되는 패킷의 발생 속도에 따라 탐지 성능을 확인할 수 있다. 그림 4는 공격 패킷의 수에 따른 탐지 알고리즘의 탐지 시간을 나타낸 그래프이다.

그림 4에서 공격 패킷의 발생 속도가 빨라짐에 따라 공격을 탐지하는 시간이 점점 짧아짐을 확인할 수 있다. 초당 공격 패킷이 10개씩 만들어 진다면 이를 탐지하는데 걸리는 시간은 약 1.2초이고, 초당 공격 패킷이 20개일 경우 약 0.5초이다.

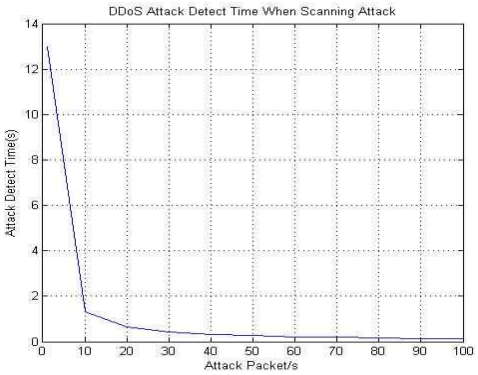

그림 4. 공격패킷 발생 속도에 따른 탐지 시간
Fig. 4. Detection time based on the Attack created packets speed

실제 네트워크에서 DDoS 공격이 이루어진 후 이를 대응하기 위해 공격 탐지 시간이 짧을수록 유리하다. 따라서 본 논문에서 제안한 알고리즘이 음성망에서의 DDoS 공격이 시도되었을 때 이를 효과적으로 탐지 가능함을 확인하였다.

V. 결론

고속 인터넷 기반 서비스가 많이 등장함에 따라 서비스 이용자는 다양한 컨텐츠를 이용할 수 있는 환경이 제공 되었다. 그러나 이와같은 인터넷 기반 서비스는 악의적인 공격에 노출되는 문제점을 가지고 있다. 특히 시스템이나 네트워크 자원을 공격 대상으로 하는 분산 서비스 거부공격의 문제가 대두되었으며, 이와 같은 공격이 음성망 환경에서도 발생할 수 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 알고리즘을 설계하고 평가하였다.

본 논문에서 제안한 알고리즘은 IP데이터망에서 웜 스캐닝 공격을 탐지하는 TRW 알고리즘을 분석하고, 이를 음성망에 적용하기 위해 연결 과정과 연결 종료 과정을 설계하며, 이를 카운트하는 확률 함수를 정의하였다. 제안한 알고리즘을 평가하기 위해 임계치를 설정하고, 공격트래픽 종류에 따른 연결확률을 변화시켜 알고리즘의 효율성을 측정하였으며, 공격패킷의 공격속도에 따른 탐지 시간을 측정하였다.

평가 결과 본 논문에서 설계한 알고리즘은 공격중 호 설정이 끊어질 확률이 70%이고, 공격 속도가 초당 10패킷일 경우, DDoS 공격이 시도되고 약 1.2초 후에 탐지를 하고 초당 20개일 경우에는 약 0.5초 후에 탐지함을 확인하였다. 실제 네트워크에서 DDoS 공격이 시도되고 이를 대응하기 위해 공격 탐지 시간은 짧을수록 좋다. 따라서 본 논문에서 제안한 알고리즘이 음성망에서의 DDoS 공격이 시도되었을 때 이를 효과적으로 탐지 가능함을 확인하였다.

감사의 글

본 연구는 2009년도 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 지원에 의하여 이루어진 연구로서, 관계부처에 감사 드립니다.

참고문헌

[1] 구민정, 오창석, “IPv6환경에서 DDoS 침입탐지”,한국컴퓨터정보학회논문지, 제11권 제6호, , pp 185~192, 2006. 12.

[2] 신승원, 오진태, 김기영, 장종수, “인터넷 웜 공격 탐지 방법 동향”, 전자통신동향분석 제 20권 제 1호, 2005년 2월.

[3] 임채태, “봇넷(Botnet) 동향 및 대응기술 현황”, TTA Journal No.118, 2008. 8.

[4] 강석민, 노병희, 홍만표, 김환국, “SIP Signaling 공격에 대한 방어 기법”, 한국정보과학회 2008 가을 학술발표논문집 제35권 제2호(D), pp 40~45, 2008. 10.

[5] J.Y. Jung, S. Schechter, and Arthur W. Berger, “Fast Detection of Scanning Worm Infections,” RAID 2004, Sophia Antipolis French, Sep. 2004.

[6] Xuan Chen and John Heidemann, “Detecting Early Worm Propagation through Packet Matching,” Technical Report ISI-TR-2004-585, 2004.
[7] 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.
[8] 박진범, 백형구, 원용근, 임채태, 황병우, “VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구”, 정보보호학회지 제17권 제5호, pp 57~65, 2007. 10.
[9] 한승철, “VoIP 서비스 및 시스템 DoS 공격 탐지 및 대응 기법 연구”, 한국정보보호진흥원, 2006. 12.
[10] 최경호, 임을규, “SIP Call Signaling을 위한 사용자 인증 기법”, 한국정보과학회 2008 종합학술대회 논문집 제35권 제1호(D), 2008. 6.
[11] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, 정보통신연구진흥원, 주간기술동향 통권 1377호, 2008. 12. 17.
[12] 김영백, 염흥열, “DNS 싱크홀에 기반한 새로운 악성봇 치료 기법”, 정보보호학회논문지, 제18 권 제 6(A) 호, pp. 107~114, 2008. 12.
[13] 유대성, 오창석, “공격 탐지를 위한 트래픽 수집 및 분석 알고리즘″, 한국콘텐츠학회 논문지, 제4권 4호, pp.33-43, 2004. 12.
[14] 조제경, 이형우, 박영준(Yeoung-Joon Park), ″공학 IAD 기반 패킷 마킹과 유무선 트래픽 분류를 통한 무선 DDoS 공격 탐지 및 차단 기법″, 한국콘텐츠학회, 한국콘텐츠학회논문지 제8권 제6호, pp 54~65, 2008. 6.

저자소개

윤성열(Sung-Yeol Yun)

2007년 한국교육개발원 학사
2009년 경원대 전자계산학과 석사
2009년~현재 경원대 전자계산학과 박사과정

※관심분야:음성통신, 네트워크 시큐리티, RFID/USN

김환국(Hwan-Kuk Kim)

1998년 항공대 전자계산학과 학사
2000년 항공대 컴퓨터공학과 석사
2009년~현재 고려대 경영정보공학 전문대학원 정보보호 박사과정

2002년 ~ 2006년 한국전자통신연구원 연구원
2007년 ~ 현재 한국인터넷진흥원 선임연구원
※관심분야 : 인터넷전화보안, 네트워크 보안 등

박석천(Seok- Cheon Park)

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