발생 메시지의 상한값을 고려한 SIP INVITE 플러딩 공격 탐지 기법연구

정회원 류 제 택*, 류 기 열*, 종신회원 노 병 희*

A SIP INVITE Flooding Detection algorithm Considering Upperbound of Possible Number of SIP Messages

Jea-Tek Ryu*, Ki-Yeol Ryu* ***Regular Members***, Byeong-hee Roh* ***Lifelong Member***

요 약

최근 VoIP(Voice over IP)나 IMS(IP Multimedia Subsystem)와 같은 멀티미디어를 기반으로 하는 응용에서는 시그널링과 세션 관리를 위해 SIP(Session Initiation Protocol)를 주로 이용하고 있다. 하지만 SIP는 인터넷을 기반으로 하기 때문에 기존 인터넷에서 발생할 보안 위협에 노출되어 있어 특히 멀티미디어와 같은 지연에 민감한 응용들에 서비스 거부 및 서비스 단절과 같은 문제를 야기하는 플러딩 공격에 영향을 받을 수 있다. 하지만 현재 제안된 탐지 기법인 CUSUM(Cumulative Sum), 헬링거 거리, 가변 임계치와 같은 방안들은 정상상태만을 고려하여 탐지하고 있어 지속적으로 변하는 네트워크 상황을 반영하지 못하고 있다. 그러므로 본 논문에서는 이러한 점을 고려하여 SIP INVITE 플러딩 공격 탐지에서 네트워크 상황을 반영 하여 보다 효과적인 플러딩 공격 탐지 방안을 제안한다. 본 방안은 SIP 기반의 INVITE 플러딩 뿐만이 아닌 BYE, CANCEL과 같은 다른 유형의 플러딩 공격 탐지에 적용이 가능하며 기존의 방안들 보다 정밀한 탐지가 가능하다.

Key Words : SIP INVITE flooding, Flooding detection, SIP security, SIP threat

ABSTRACT

Recently, SIP(Session Initiation Protocol) is used to set up and manage sessions for multimedia applications such as VoIP(Voice over IP) and IMS(IP Multimedia Subsystem). However, because SIP operates over the Internet, it is exposed to pre-existed internet security threats such as service degradation or service disruptions. Multimedia applications which are delay sensitive even suffers more from the threats mentioned above. The proposed methods so far to detect SIP INVITE flooding are CUSUM(Cumulative Sum), Hellinger distance and adaptive threshold, but among methods only take normal state into consideration. So, it is not capable of adapting the condition of the network congestion which are dynamically changing. In this paper, SIP INVITE flooding detection algorithm considering network congestion which enables efficient detections of such attacks is proposed. The proposed algorithm is expected to detect other types of attacks such as BYE and CANCEL more precisely compared to other methods.

Ⅰ. 서 론

최근 VoIP(Voice over IP)나 IMS(IP Multimedia

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발사업의 일환으로 [2008-S-028-01, SIP기반 응용서비스 보호를 위한 침입대응기술 개발]과 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (IITA-2009-C1090-0902-0003)

* 아주대학교 정보통신전문대학원 정보통신공학과(ricman@ajou.ac.kr), (kryu@ajou.ac.kr), (bhroh@ajou.ac.kr)

논문번호 : KICS2009-06-229, 접수일자 : 2009년 6월 2일, 최종논문접수일자 : 2009년 07월 15일

Subsystem)와 같은 멀티미디어를 기반으로 하는 응용에서는 시그널링과 세션 관리를 위해 SIP(Session Initiation Protocol)를 주로 이용하고 있다. 이는 SIP가 개방형 네트워크를 기준으로 개발되어 다양한 멀티미디어 서비스를 쉽게 수용할 수 있고 내용이 간단하고 개발이 쉬워 다른 프로토콜에 비해 확장성이 뛰어나기 때문이다. 하지만 이러한 장점은 반대로 SIP 보안에 있어 많은 문제를 낳는 주요 요인을 작용하고 있어 이에 대한 대응이 요구된다.

SIP의 보안 위협은 프로토콜의 취약점을 이용한 시그널링 공격과 다량의 SIP 메시지를 발생시켜 서비스 거부를 일으키는 플러딩 공격으로 구분된다. 현재 시그널링 공격에 대한 대응 기법은 SIP 프로토콜 자체의 취약점을 보완하거나 메시지 암호화를 통해 많은 해결 방안과 연구가 진행되어 있다[1]-[3]. 하지만 플러딩 공격의 경우 그 공격 특성상 인터넷의 DDoS(Distributed Denial of Servce) 공격과 유사하여 공격자의 위치가 노출되지 않고 정상 메시지와 비정상 메시지간의 구별이 어려워 이에 대한 대응 방안 연구가 미흡하다. 또한 각 공격에 대한 고유의 형태를 가지는 시그널링 공격과 달리 플러딩 공격은 공격의 패턴을 파악하기 쉽지 않아 탐지 자체가 어렵다.

현재 이러한 SIP 플러딩 공격을 탐지하기 위해 CUSUM[4](Cumulative Sum)]를 이용한 방안과, 헬링거 거리(Hellinger distance)[5]를 이용한 방안, 가변 임계치(Adaptive threshold)[6]를 이용한 방안이 제안되어 있으며 이에 대한 성능은 [7]의해 분석되어 있다. 하지만 현재 제안된 방안들은 정상상태의 트래픽을 기반으로 탐지하고 있어 지속적으로 변화하는 네트워크 상황을 반영하지 못하고 있다. 이는 정상 트래픽과 공격 트래픽, 그리고 혼잡에 따른 트래픽 가중을 구별하기 어렵게 하며 탐지의 정확도를 낮추는 문제를 낳게 한다.

이를 위해서 본 논문에서는 SIP 메시지를 대상으로 플러딩 공격을 효과적으로 검출하기 위한 방법을 제안한다. 제안 방법은 발생이 예상되는 메시지 개수의 상한값을 고려하여, SIP 서버가 수신할 것으로 예상되는 메시지 개수의 상한 값을 산출하고, 이를 기반으로 플러딩 공격을 검출한다. 제안방법은 INVITE 플러딩 뿐만아니라, BYE, CANCEL 플러딩 공격들에도 적용가능하다.

본 논문의 구성은 다음과 같다. 제2장에서는 SIP 시그널링에 대하여 간략히 소개하고, 제3장에서는 SIP 서버가 수신할 것으로 예상되는 SIP 메시지 개수의 상한값을 산출, 4장에서는 이를 기반으로 SIP 메시지 개수의 상한값을 이용한 INVITE 플러딩 공격을 탐지 알고리즘에 대해 기술한다. 제5장에서는 제안된 방법의 성능을 평가하고, 제6장에서 결론을 맺는다.

Ⅱ. SIP 개요

IETF에서 제안된 SIP는 멀티미디어 세션 또는 호를 설정하고 수정, 종료 할 수 있게 하는 응용계층의 시그널 프로토콜이다. SIP의 메시지 구조는 HTTP와 유사한 텍스트 기반의 구조를 가지고 있으며 이것은 요청 및 응답 메시지로 쌍을 이뤄 동작을 한다. SIP 메시지는 헤더와 바디로 구성되어 있으며 헤더는 SIP 시그널링 정보를 포함하며 바디는 호 설정 시 오디오 및 비디오 코덱과 같은 부가정보를 제공한다. 이러한 SIP 표준은 RFC 3261[8]에 의해 정의 되어 있다.

2.1 SIP 시그널링 절차

2.1.1 세션 설정 과정

SIP 기반의 세션 설정 과정은 그림 1과 같은 과정을 거치게 된다. 송신자는 수신자에게 하나의 세션을 생성하기 위한 INVITE 요청메시지를 보내게 된다. 이러한 메시지는 수신자에게 전달되기 위해서 몇 개의 SIP 프락시 서버를 거치게 된다. 메시지를 전달 받은 프락시 서버는 메시지를 통해 수신자를 인식하고 받은 메시지를 적절한 프락시 서버나 수신자로 전달하게 된다. INVITE 메시지를 받은 수신자는 INVITE 메시지에 대한 응답 메시지를 보내게 되는데 응답 메시지는 처리 결과를 나타내기 위해 상태 코드를 가지고 있다. 만약 수신자가 제대로 메시지를 받아서 처리했다면 "200 OK"라는 응답 메시지를 발신자에게 보내게 된다. 이러한 응답을

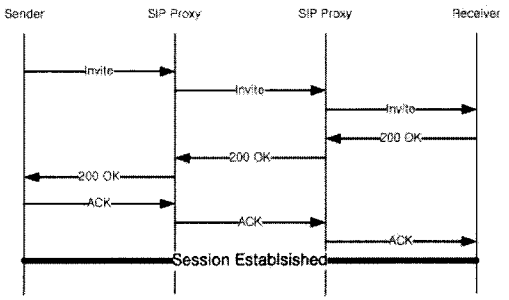


그림 1. SIP Session Setup 과정

받은 발신자는 수신자가 보낸 응답 메시지를 제대로 받았음을 알리기 위해서 ACK 요청 메시지를 수신자에게 다시 보내는 과정을 거쳐 하나의 세션이 생성된다.

2.2 SIP 재전송 메커니즘

일반적으로 SIP는 UDP 기반으로 메시지를 전달하게 된다. 그러므로 SIP는 패킷 손실에 대한 안전한 메시지 전달을 위해서 이를 위한 메시지 재전송 방안이 필요하다. 현재 이를 위해서 RFC 3261에는 SIP 메시지에 대한 재전송 방안 및 패킷 손실에 대한 타이머 T1, T2를 정의하고 있으며 재전송은 INVITE 요청 메시지와 non-INVETE 요청 메시지로 구분되어 사용되고 있다.

2.2.1 INVITE 요청 메시지 재전송

발신자가 세션을 형성하기 위해 INVITE 메시지를 전달하였을 때 이에 대한 응답이 수신자로부터 T1(기본값 : 500ms) 내에 응답이 오지 않았을 경우 발신자는 해당 메시지가 네트워크 상에서 손실되었다고 판단한다. 그리고 발신자는 해당 메시지를 재전송하게 되며 이후에는 타이머를 T1의 2배씩 증가시켜 재전송을 수행하게 된다. 이러한 재전송은 최초 메시지를 생성하여 전달한 후 64*T1(기본값 : 32초) 시간이 지날 때 까지 수행하게 되며 이 경우 INVITE 요청에 대한 최대 메시지 재전송 횟수는 7회(최초 메시지수 포함)를 넘을 수 없게 된다.

2.2.2 None-INVITE 요청 메시지 재전송

INVITE 요청 메시지를 제외한 요청 메시지 및 응답 메시지에 대한 재전송은 INVITE 요청 재전송 방안과는 다른 재전송 주기를 가지고 있다. 이는 INVITE 요청 재전송과는 달리 None-INVITE 요청 재전송이 T1 타이머 이외에 T2(기본값 : 4초) 타이머를 하나 더 사용하기 때문이다. None-INVITE 요청 또는 응답 메시지를 발생시킨 발신자는 INVITE 요청 메시지 재전송와 동일하게 최초 메시지가 발생한 T1초 이후에 수신자로부터 이에 대한 응답이 없을 경우 해당 메시지에 대해서 손실이 발생하였다고 판단하고 재전송을 시도하게 된다. 이후의 INVITE 요청 메시지 재전송과 동일하나 그 간격이 T2초에 도달할 경우 이 시점 이후 부터는 T2의 간격을 유지한 채로 64*T1가 지날 때 까지 재전송을 수행하게 된다. 이 때 None-INVITE 요청 메시지 및 응답 메시지의 최대 전송 횟수는 11회(최초 메시지수 포함)를 넘을 수 없게 된다.

Ⅲ. SIP 메시지 수의 상한값

SIP 메시지들은 기본적으로 UDP를 사용하여 전달된다. 메시지 전달 과정 중에 손실이나 과도한 지연에 의하여 응답을 받지 못하게 될 경우에 SIP 요소들은 응용 계층에서 메시지를 재전송 하게 된다. 이러한 재전송은 네트워크의 혼잡 상황에 따라 지연과 손실이 과도하게 될수록 빈도가 더 커지게 된다. 따라서 네트워크의 혼잡도가 커질 경우 재전송에 의한 트래픽의 증가가 발생하고, SIP 메시지의 발생률이 커질수록 이러한 증가는 더 커지게 된다.

현재 이미 제안된 HD나 CUSUM은 정상 상태에서의 트래픽 변동에 대한 통계 데이터를 근간으로 하여 이를 벗어나는 경우를 비정상 행위로 규정한다. 그러나 이들 방법들에서는 네트워크 혼잡에 따른 재전송에 의한 트래픽의 증가 현상을 반영하지 못한다. HD나 CUSUM에 혼잡 상황에 의한 재전송의 효과를 반영하려면 정상 트래픽의 임계값을 매우 크게 설정하여야 하나, 이것은 INVITE 플러딩과 같은 비정상 행위를 탐지하는데 있어서 탐지시간이 증가하거나 탐지가 힘들 수 있게 되는 비효율적인 상황이 발생할 수 있다. 일반적으로, 정상상태에서 메시지의 평균 발생률은 특정시간대에 변화가 없지만, 네트워크의 혼잡상황은 수시로 변화할 수 있음에 주의한다. 여기에서는 네트워크 혼잡 상황을 고려하여 정상 트래픽에서 통계 패턴을 벗어나는 상한값을 산출하고, 이를 기반으로 이러한 정상 트래픽의 상한을 벗어나는 경우에 대하여 비정상 여부를 본 논문에서 제안하는 탐지 알고리즘에 반영하고자 한다. 여기에서는 망관리 시스템이나 측정 방법등을 통하여 네트워크 혼잡 상황을 알고 있는 것으로 가정한다. 시간을 일정한 크기인 T에 따라 t_0, t_1, t_2,... 와 같이 구분하기로 한다. 모든 시간 구간에서의 정상 메시지는 평균이 a인 지수분포를 갖고 발생한다고 가정하기로 한다. 네트워크에서의 혼잡에 의하여 주어진 시간 내에 응답을 못 받게 되어 재전송을 하게 되는 비율을 p로 정의하기로 한다. 본 절에서는 무한 재전송, INVITE 재전송, Non-INVITE 재전송에 환경에서 SIP 메시지의 발생 상한값을 각각 도출한다.

1) 정리1. (무한 재전송 환경에서의 상한값) 네트워크 혼잡등에 의하여 정해진 시간 내에 응답을 못 받은 SIP 구성요소는 성공적인 응답을 받을 때까지 재전송을 하는 경우를 고려하기로 한다. 모든 시간

구간에서의 신규 발생 트래픽의 상한을 A라 할때, 시간이 무한히 흐른 상황에서의 시간 구간 $t(=lim_{t\to\infty} t_k)$에서의 발생 메시지 개수의 상한값은 다음과 같이 된다.

$$m_U^{\infty} = A\frac{1}{1-p} \tag{1}$$

증명. 편의상, t_0에서 시스템이 시작한 것으로 가정하기로 한다. t_0에서 신규로 발생한 메시지 a_0들 중에서 $p \cdot a_0$개는 손실되어 다음 시간 구간 t_1에서 재전송에 의한 재발생이 이루어지게 된다. 따라서 t_1에서는 이 구간에서 신규로 발생하는 a_1개의 메시지와 이전 시간 구간에서 재발생 된 $p \cdot a_0$개의 메시지가 나타나게 된다. 즉, $m_1 = a_1 + p \cdot a_0$. 시간이 지나서 정상상태에 이르게 되면, 재전송 타임아웃 시간과 무관하게, r_k는 바로 이전 시간 구간 t_{k-1}에서 발생한 총 메시지들 중에서 확률 p에 의하여 재전송이 되는 메시지들이 된다. 따라서 t_k에 발생한 총 메시지의 수 $m_k(k=0,1,2,\cdots)$는 다음과 같이 나타낼 수 있다.

$$m_k = a_k + r_k = \sum_{i=0}^{k} a_i p^{k-i}, k=0,1,2,\cdots \tag{2}$$

신규 발생 트래픽의 상한을 A라 하면, 즉, $a_k \le A, \text{for} \forall k$. 또한 p는 1보다 작으므로, 정상상태에서의 총 발생 메시지 개수의 상한값은 다음과 같이 된다.

$$m \equiv \lim_{k\to\infty} m_k \le \sum_{i=0}^{\infty} Ap^{k-i} = A\frac{1}{1-p} \tag{3}$$

2) 정리2. (INVITE 메시지 재전송) 무한 재전송과는 달리 INVITE의 재전송의 경우는 최대 재전송 회수가 초기 전송을 포함하여 최대 7회가 된다. 이 때 재전송의 횟수는 6회가 되며 이를 $RT\max$로 정의하면 $RT\max$는 6이라는 최대의 값을 가지게 된다. 이때 시간이 무한히 흐른 뒤에 $t(=lim_{t\to\infty} t_k)$ 발생 메시지 개수의 상한값은 수식 (4)과 같이 된다.

$$m_k^{\infty} \le A\sum_{i=0}^{RTmax} p^i, \quad RTmax = 6 \tag{4}$$

증명. 무한 재전송이 이루어지는 경우와 달리 시스템이 시작점인 t_0에서 신규로 발생한 a_0개에 대한 손실된 메시지 수는 $p \cdot a_0$이 되고 이에 대한 재전송은 $t_{Tr(1)}$ 시점에서 이루어지게 된다. 그러므로 Tr(1)의 시간에서 메시지의 발생 수는 $m_{Tr(1)} = a_1 + p \cdot a_0$이 되고 t_1구간에서는 메시지 수는 $t_0 \sim t_1$사이에 발생 할 수 있는 최대 재전송 횟수는 수식 (5), (6)를 통해 얻게 되고 $RT\max$에 따라 m_1의 값이 정해지게 된다.

$$Tr(i) = 2^{(i-1)} * T1, \tag{5}$$
$$Tr(i) \le 64 * T1 (i=1,2,..)$$

$$RT\max = \max(i) \;\; T_k - 2^i * T1 \ge 0, \tag{6}$$
$$(RT\max < 7)$$

$$m_k = A\sum_{i=0}^{RTmax} p^i \tag{7}$$

즉 이것은 (6)을 통해 $t_0 \sim t_k$ 사이에서 발생 할 수 있는 재전송 횟수를 기반으로 $RT\max$값이 정해지게 되고 이 값을 통해 t_k에서 발생되는 메시지의 수 m_k값은 수식 (7)과 같이 정리된다. 그러므로 단위 구간당 m_k는 $A\sum_{i=0}^{RTmax} p^i$ 값을 넘을 수 없다.

3) 정리3. (None-INVITE 메시지 재전송) None-INVITE 메시지 재전송은 시간에 따른 $RT\max$의 값의 차이와 재전송의 횟수가 최대 10회가 이루어지는 것을 제외하면 INVITE 메시지 재전송과 동일하며 이 때 시간이 무한히 흐른 후 단위 구간에서의 m_k는 $RT\max$값이 10이 반영된 수식 (7)과 동일하다.

일반적으로 SIP는 세션을 생성하기 위해서 INVITE, ACK, 200 OK등과 같은 메소드를 이용한다. SIP는 이러한 메시지를 UDP를 기반으로 전송을 하며 이에 대한 신뢰성을 보장하기 위해서 INVITE 재전송 방안과 None-INVITE 재전송 방안이 이용한다. 이는 특정 메시지에 증가나 혹은 그 메시지의 재전송 방안에 따라 혼잡도가 달라질 수 있음을 예상할 수 있다. 하지만 정리 1, 2, 3을 기반으로 각 전송 방안에 따른 메시지의 발생 수를 비교하여 보면 그 차이가 크지 않음을 알 수 있다. 그림 2는 이러한 것을 보여주는 실험 결과로 이 실험에서는 초당 50개의 세션 생성이 발생되고 서비스의 시간이 무한대로 증가 될 때 패킷 손실률에 따른 단위 시간당

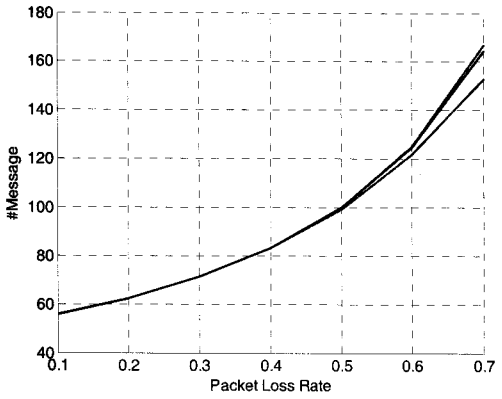


그림 2. 손실률에 따른 메시지 발생 수

의 메시지의 수를 나타낸 것이다. 손실률에 0.5이하에서는 거의 동일한 메시지의 발생 수를 나타내기 때문에 차이가 없는 것으로 나타났으며 이는 실제 네트워크 상에서 재전송 방안에 따른 것으로 이는 재전송의 메시지의 수가 차이가 없음을 알 수 있다. 그러므로 네트워크의 혼잡도에 따른 SIP 메시지의 상한값은 수식 (1)을 사용하여 결정하여도 그 결과에 많은 영향을 주지 않음을 알 수 있다.

Ⅳ. 네트워크 혼잡 상황을 고려한 SIP 플러딩 공격 탐지 알고리즘

앞 절에서의 유도한 식 (1)은 네트워크에 발생할 수 있는 단위 시간 내의 총 메시지 수를 나타냄을 알 수 있었으며 이는 다른 재전송 방식에서도 동일하게 적용함을 알 수 있는 것을 실험을 통해 보여주었다. 이는 발생 가능한 메시지의 상한으로서 여겨질 수 있으며, 통상 상태에서 이 값을 초과하는 경우에는 비정상 행위가 이루어지고 있음으로 판단하는 것이 가능하다는 것을 의미한다. 여기에서는 이를 활용한 비정상 행위 징후를 탐지하기 위하여 제안하는 알고리즘에 대하여 설명한다.

4.1 INVITE Flooding 탐지 알고리즘

INVITE 메시지의 경우 단위시간당 평균 발생하는 호(Call)수를 바탕으로 현재 네트워크에서의 혼잡도를 고려하여 상한값을 설정한다. 단위시간당 호수에 대한 상한값은 다음과 같은 식으로 앞 절의 식 (1)를 기반으로 구할 수 있다. 따라서 단위 시간당 발생하는 평균 호수를 A라고 했을 때 이에 대한 상한값은 $\frac{A}{1-p}$ 가 된다. 이는 네트워크에서의 혼잡도를 고려한 상한값으로 p는 재전송을 하게 될 확률을 의미한다.

실제 각각의 단위시간동안 발생하는 INVITE 메시지의 N_0수는 $N_0 . N_1, N_2 \cdots$ 로 구분한다. 실제 N_i의 가중 평균(Weighted average)는 수식 (8) 같이 구할 수 있다.

$$R_i = \alpha N_i + (1-\alpha) R_{i-1} \tag{8}$$

R_i는 가중 평균을 의미하며 α는 이를 위한 가중치가 된다. 따라서 본 알고리즘에서는 R_i의 값이 상한값 이상으로 발생할 경우 이를 비정상 징후로 탐지한다. 그러나 실제 네트워크에서는 손실이나 지연 또는 다른 여러 상황으로 인해 비정상적으로 많은 정상적인 트래픽이 발생하는 경우가 발생한다. 따라서 본 알고리즘에서는 이러한 네트워크 특성을 고려하여 각각의 단위 시간 내에서 발생하는 트래픽의 가중 평균값이 연속적으로 상한값 이상으로 발생하는 경우만을 비정상 징후로 탐지한다. 이 값은 L 로 정의하며 L 값 이전에는 경고 단계로 정의하고 L 값 이상이 되면 비정상 징후로 정의 한다. 공격의 종료를 인지하는 과정은 경고단계를 발생 수의 변화를 통해 인지할 수 있다. 즉, 비정상 징후 탐지 단계이후, 가중 평균가 상한값 이하의 값으로 발생할 경우 경고 발생수는 감소하게 된다. 따라서 초기에 설정했던 경고발생 임계치와 동일한 값이 될 경우 이를 공격 종료로 인지한다. 설명한 INVITE 메시지의 비정상 징후 탐지 알고리즘은 그림 3과 같다.

```
Algorithm : INVITE Flooding Detection

Definition
A: The Number of normal Call(per second)
P: Retransmission rate
L : The bound value of the warning
Ni : The numbers of normal INVITE message in ith(Interval time)
Ri : The Weighted average of the Ni
Count : Count value of the warning(Initial value is 0)

Procedure
Loop Check the number of Message Ni
    Calculate the weighted average Ri
    if(Ri > A/(1-p))
        Count++
            if(Count > L)
                detect the abnormal symptom
                  alarm VoIP administrator // Warning to the
                                              suspicisou message
            else if(count !=0)
                count --
    else
        alarm to VoIP administrator //there is no abnormal
                                      symptom
```

그림 3. INVITE Flooding Algorithm

V. 실험 평가

제안된 비정상 행위 탐지 알고리즘에 성능을 검증하기 위해서 실험 평가를 실시하였다. 실험 환경은 C를 이용하여 SIP를 기반으로 하여 호 생성기를 작성하였고 이를 기반으로 단위 초에 대한 호 발생수와 패킷 손실률에 대한 값을 이용하여 각각의 트래픽을 생성하였으며 단위 구간에서의 각호는 지수분포를 따른다. 각 실험시간은 1000초를 기준으로 하였다. 또한 공격에서는 실험 시간 60초에서 공격을 실험하여 단위 구간 당 발생하는 호의 2.5배를 초과할 때까지 공격을 수행하였으며 이후 공격을 점차 감소시켰다. 또한 기존 알고리즘인 CUSUM과의 비교 분석으로 통해서 그 성능을 검증하였다.

그림 8은 단위 시간당 50호가 생성되었을 경우와 평균 메시지 손실률을 0.0, 0.1, 0.3을 반영하였을 때 각 단위 구간 당 발생되는 INVITE 메시지의 수를 시간에 따라 나타낸 것이다. 이를 통해 손실률이 증가할수록 단위 시간당 발생되는 메시지의 수가 증가 됨 을 알 수 있다. 그러므로 네트워크 혼잡도가 발생하여 손실 메시지의 빈도가 증가할 경우 플로딩 공격 탐지 알고리즘에서는 이를 고려하여야 함을 알 수 있다 .

그림 4는 손실률에 따른 메시지 누적 분포 지수를 나타낸 것이다. 이는 총 실험시간동안 단위시간당 발생 된 메시지의 발생 수의 분포를 나타낸 것으로 손실률에 따라 그 분포 또한 일정하게 증가됨 을 알 수 있다. 또한 이 분포를 기준으로 임계치 $\frac{A}{1-p}$의 값을 이 분포에 적용하면 이 임계치에서 정상적으로 탐지할 수 있는 성능을 측정할 수 있다. 본 논문에서 제안한 알고리즘은 이 임계치를 넘을 경우를 공격이라 판단하지 않고 지속적으로 그 공격이 반복되었을 때 이를 공격 징후로 알리게 된다. 그러므로 이 임계치 값을 이용하여 탐지 알고리즘에 적용하였을 경우에는 그림 6과 같이 정상일 경우에는 82%, 공격이 있을 경우에는 94%로의 탐지 성능을 보였다. 하지만 이 임계치 값은 낮은 누적분포지수를 기준으로 설정된 임계치값 이용한 것으로 CDF가 0.7에 해당하는 임계치 값을 설정 하였을 경우 정상, 공격 모두 99% 이상의 탐지 성공률을 나타내었다.

본 알고리즘을 기존에 제안된 알고리즘과 비교하기 위해서 CUSUM을 비교하여 그 성능을 검증하였다. 본 실험에서는 공격을 수행한 후 약 100초에

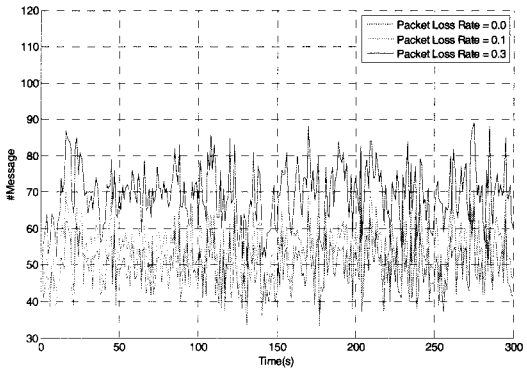


그림 4. 손실률에 따른 단위 시간당 INVITE 메시지 발생 수

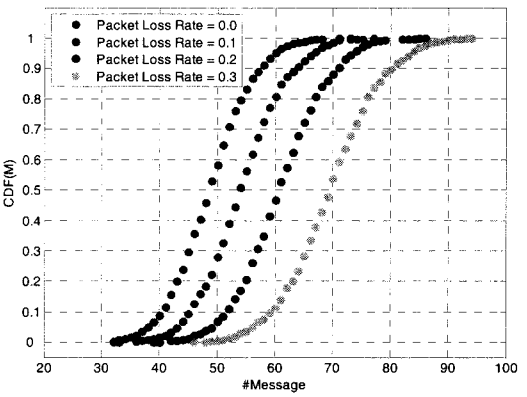


그림 5. 손실률에 따른 메시지의 누적 분포 지수

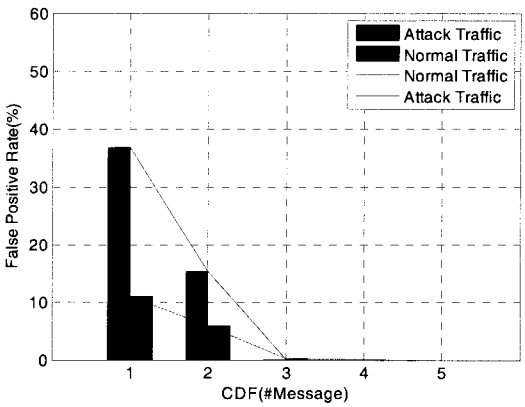
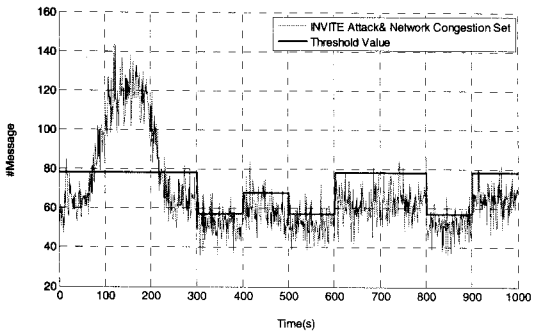


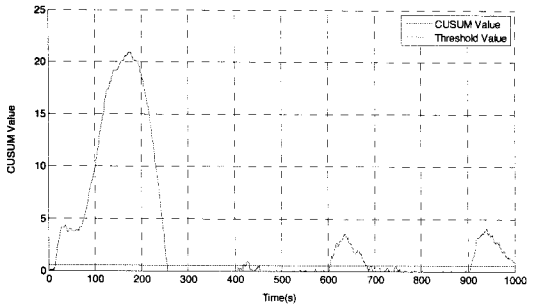
그림 6. CDF(X)의 값에 따른 제안된 탐지 알고리즘의 오탐률

따라 네트워크의 패킷 손실률을 가변적으로 주고 지속적으로 변화하는 네트워크 상황을 반영하였으며 이러한 과정에서 이 CUSUM과 제안된 알고리즘이 어떠한 성능을 나타내는지 평가하였다.

그림 7(a)은 공격 메시지와 손실에 따른 단위 시간에서의 메시지의 발생 수와 그에 따른 제안된 알고리즘의 임계치 변화를 나타낸 것이다. 반면 CUSUM



(a) 가변적인 네트워크 상황에서
제안된 알고리즘의 임계치 변화



(b) 동일조건 하에서의 CUSUM 값과 임계치

그림 7. CUSUM과 제안된 알고리즘의 임계치와 CUSUM의 변화

의 경우 공격과 손실률에 따른 트래픽의 CUSUM 값이 그림 7(b)와 같이 나타나며 이때 임계치의 값은 일정하게 고정되게 된다. 이는 CUSUM의 경우 정상트래픽의 패턴을 분석하여 이를 기반으로 고정된 임계치를 가지기 때문으로 이는 네트워크의 가변적인 변화를 반영하지 못하기 때문이다. 즉 그림 7(b)에서 보는 봐와 같이 임계치를 넘는 구간을 비정상이라고 판단하므로 그 오탐률은 상대적으로 제안된 알고리즘보다 크다고 할 수 있다. 또한 제안된 알고리즘의 경우 임계치를 넘는 것이 반복적으로 일어날 경우 이를 공격으로 판단하는 것과 달리 CUSUM의 경우는 단위 구간 당 메시지의 발생 수의 차가 표준편차 급격하게 일어날 경우 CUSUM 값이 크게 나타나고 이러한 것이 임계치를 넘을 때 공격으로 판단하기 때문에 오탐률은 더 발생하게 된다.

그림 8은 제안된 알고리즘과의 CUSUM을 성능을 비교한 것이다. CUSUM의 경우는 임계치 값은 제안된 알고리즘의 CDF의 0.8에 해당하는 값을 임계치로 정한 것이다. 다만 CUSUM의 경우 표준 편차를 기준으로 변화 범위가 1~2배 사이를 오차범위로 두어 CUSUM 값의 변화를 가변적으로 하였으

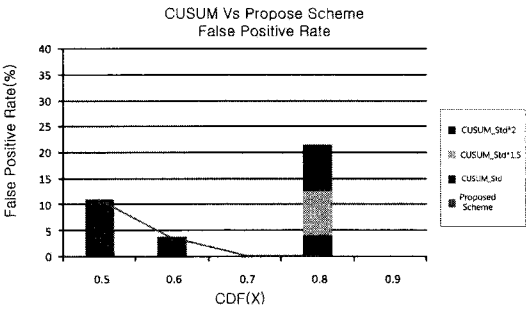


그림 8. 네트워크 상황을 고려한 탐지 알고리즘 Vs. CUSUM

며 이에 따라 그 성능은 달라진다. 하지만 제안된 알고리즘의 경우에는 $\frac{A}{1-p}$의 값을 통해 얻어진 결과를 통해 설정된 임계치인 CDF 0.6을 놓았을 경우와 유사한 성능을 나타내었으며 CDF를 증가 시켰을 경우 탐지률이 99%에 달하는 성능을 보였다. 이는 제안된 알고리즘이 보다 정밀하게 탐지를 할 수 있을 나타내는 것으로 보다 효과적인 탐지를 할 수 있다고 볼 수 있다.

Ⅵ. 결 론

본 논문서 제안한 탐지기법은 기존의 비정상 트래픽 탐지 기법들이 고려하지 않았던 실제 네트워크의 혼잡도를 고려하여 설계되었다. 그에 따라 혼잡도가 높은 네트워크에서 정상 트래픽이 비정상 트래픽으로 오인할 확률이 낮아진다. 또한 실제 탐지 알고리즘에서 사용되는 가중평균 값이나 임계치 값, L값 등을 변경할 수 있어 각각의 응용서비스에 적합한 값을 설정해서 사용할 수 있다. 실제로 가중평균의 α 값이나 경고 단계를 설정하는 L값 등을 조절하면 실제 공격탐지 시간을 단축할 수 있지만, 실제 정상 트래픽을 비정상 트래픽으로 오인할 확률이 높아지는 등의 트레이드 오프(Trade off)가 발생하게 된다. 따라서 실제 사용될 서비스에 적합한 값을 설정하여 사용하여야 한다.

참 고 문 헌

[1] A. Bremler-Barr, R. Halachmi-Bekel, "Unregister attacks in SIP", NPSEC 2006, Nov. 2006.

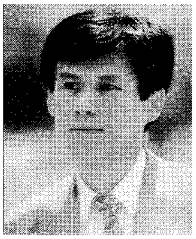
[2] Fengjiao Wang et al., "A New Provably Secure Authentication and Key Agreement Mechnism for SIP Using Certificateless Pubilic-Key

Cryptography", ICCIS 2007 Dec. 2007.
[3] Geneiatakis, D et al., "A lightweight protection mechanism against signaling attacks in a SIP-based VoIP environment", Telecommunication system 1018-4864, Dec. 2007.
[4] Yacine Rebahi et al., "Detecting Flooding Attack against IP Multimedia Subsystem(IMS) Network", AICCSA April 2008.
[5] Hemant Sengar et al., "Detecting VoIP Floods Using the Hellinger Distance", IEEE Transaction on Parallel and Distributed Systems, vol. 19, no. 6, June 2008.
[6] V. Siris and F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks," Computer Communications, vol. 29, no. 9, pp. 1433-1442, 2006.
[7] Akbar, M.A.; Tariq, Z.; Farooq, M. "A comparative study of anomaly detection algorithms for detection of SIP flooding in IMS", IMSAA 2008, 10-12 Dec. 2008
[8] J.Rosenberg et al "SIP : Session Initiation Protocol", RFC 3261, June 2002. system 1018-4864, Dec. 2007.

류 제 택 (Jea-Tek Ryu) 정회원

2005년 2월 아주대학교 정보 및 컴퓨터 공학부(학사)
2007년 2월 아주대학교 정보통신 전문대학원 정보통신공학과(석사)
2007년~현재 아주대학교 정보통신전문대학원 박사과정
<관심분야> 유/무선 인터넷 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, 인터넷 보안, 센서 네트워크

류 기 열 (Ki-Yeol Ryu) 정회원



1985년 2월 서울대학교 컴퓨터 공학과 졸업
1987년 2월 한국과학기술원 전산학과(석사)
1992년 2월 한국과학기술원 전산학과(박사)
1993년~1994년 동경대 전산학과 연구원
1994년~현재 아주대학교 정보통신전문대학원 부교수
<관심분야> 유비쿼터스 컴퓨팅, 서비스 지향 컴퓨팅, 컴포넌트 모델 및 프레임 워크, 객체지향 프로그래밍 언어, 분산 오브젝트 시스템, RFID 시스템

노 병 희 (Byeong-hee Roh) 종신회원

1987년 2월 한양대학교 전자공학과 졸업
1989년 2월 한국과학기술원 전기및전자공학과 졸업(석사)
1998년 2월 한국과학기술원 전기 및 전자공학과 졸업(박사)
1989년~1994년 한국통신 통신신망 연구소
1998년~2000년 삼성전자
2000년~현재 아주대학교 정보통신전문대학원 부교수
<관심분야> 유/무선 인터넷 멀티미디어 통신 및 응용, 트래픽 제어, 유비쿼터스 네트워킹, RFID 네트워킹, 인터넷 보안, 국방전술통신 네트워크