SIP망에서 트래픽 측정 및 IP 추출을 통한 DDoS공격 탐지 기법 설계

윤성열*, 심용훈**, 박석천***
*, **, ***경원대학교 전자계산학과
e-mail:scpark@kyungwon.ac.kr

A Design of DDoS Attack Detection Scheme Using Traffic Analysis and IP Extraction in SIP Network

Sung-Yeol Yun*, Yong-Hoon Sim**, Seok-Cheon Park***
*, **, ***Division of Computer Science, Kyungwon University

요 약

통신망의 발달로 다양한 인터넷 기반 기술들이 등장함에 따라 현재는 데이터뿐만 아닌 음성에 대한 부분도 IP 네트워크를 통해 전송하려는 움직임이 발판이 되어 VoIP(Voice Over Internet Protocol)라는 기술이 등장하였다. SIP(Session Initiation Protocol) 프로토콜 기반 VoIP 서비스는 통신 절감 효과가 큰 장점과 동시에 다양한 부가서비스를 제공하여 사용자 수가 급증하고 있다. VoIP 서비스는 호(Call)를 제어하기 위해 SIP 기반으로 구성이 되며, SIP 프로토콜은 IP 망을 이용하여 다양한 음성과 멀티미디어 서비스를 제공하게 되는데 IP 프로토콜에서 발생하는 인터넷 보안 취약점을 그대로 동반하기 때문에 DoS(Denial of Service) 및 DDoS(Distribute Denial of Service)에 취약한 성향을 가지고 있다. DDoS 공격은 단시간 내에 대량의 패킷을 타깃 호스트 또는 네트워크에 전송하여 네트워크 접속 및 서비스 기능을 정상적으로 작동하지 못하게 하거나 시스템의 고장을 유도하게 된다. 인터넷 기반 생활이 일상화 되어 있는 현 시점에서 안전한 네트워크 환경을 만들기 위해 DDoS 공격에 대한 대응 방안이 시급한 시점이다. DDoS 공격에 대한 탐지는 매우 어렵기 때문에 근본적인 대책 마련에 대한 연구가 필요하며, 정상적인 트래픽 및 악의적인 트래픽에 대한 탐지 시스템 개발이 절실히 요구되는 사항이다. 본 논문에서는 SIP 프로토콜 및 공격기법에 대해 조사하고, DoS와 DDoS 공격에 대한 특성 및 종류에 대해 조사하였으며, SIP를 이용한 VoIP 서비스에서 IP 분류와 메시지 중복 검열을 통한 DDoS 공격 탐지 기법을 제안한다.

1. 서론

최근 정보통신 기술의 발달로 수많은 인터넷 서비스 기술들이 등장하고 있다. 현재는 이러한 서비스 기술들이 보급단계에 이르렀으며, 그 중에서도 통신 절감 효과가 크고 다양한 부가서비스를 제공하는 VoIP(Voice over Internet Protocol) 기술에 일반 사용자들의 관심이 증대되고 있다.

하지만 VoIP 서비스를 제공함에 있어 기술적 제약보다는 기존 인터넷망에서 발생해온 통화품질의 저하 및 개인정보 유출 등의 보안상의 문제를 그대로 상속하고 있어 이러한 문제를 해결하기 위한 연구가 이슈화되고 있다. 특히 VoIP 서비스에서는 호 연결 설정까지 텍스트화된 메시지를 이용한 인증 및 연결절차를 가지게 되므로 트랙픽을 무한히 발생시키는 DoS(Denial of Service) 및 DDoS (Distribute Denial of Service) 공격에 취약한 구조를 가지게 된다. 따라서 본 논문에서는 SIP(Session Initiation Protocol)을 이용한 VoIP 서비스에서 IP 분류와 메시지 중복 검열을 통해 DDoS 공격을 탐지할 수 있는 기법을 설계하였다. 본 논문의 2장에서는 SIP 프로토콜의 분석과 서비스 거부 공격의 특성 및 종류에 대해 알아보고, 3장에서는 DDoS 탐지기법을 제안하며 마지막으로 4장에서는 결론을 맺는다.

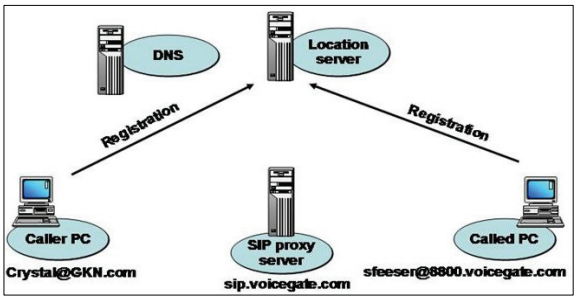
* 경원대학교 일반대학 전자계산학과 박사과정
** 경원대학교 일반대학 전자계산학과 석사과정
*** 경원대학교 IT대학 정교수(교신저자)

2. 관련연구

2.1 SIP(Session Initiation Protocol)

SIP는 VoIP 서비스에서 호 연결 설정을 위한 제어 프로토콜이다[1]. 음성을 포함한 화상, 텍스트 등 멀티미디어 통신 세션을 생성 및 삭제, 변경할 수 있는 프로토콜이다. SIP은 사용자와 서버 형식으로 TCP와 UDP 프로토콜을

모두 사용할 수 있으며 다양한 멀티미디어 서비스를 쉽게 수용할 수 있고, 간단한 프로토콜 구조, 개발이 쉬워 확장성이 뛰어나다는 장점을 가지고 있다. [그림 1]은 SIP 등록과정이다.



[그림 1] SIP 등록과정

[그림 1]에서 Location Server와 Proxy Server는 물리적으로 동일한 서버에 동작을 한다. 소규모 LAB 환경에서는 Proxy Server, Location Server, Registrar Server가 하나의 서버로 운영된다. [그림 1]에서는 각 사용자가 콜을 하기 이전에 자신의 위치정보를 Location Server에 제공하는 그림이다. 이들 정보에는 자신의 SIP Address와 IP Address 정보 등이 포함된다.

각 사용자와 서버들은 서로의 위치를 알아내기 위해 DNS와 Location Server를 통해 서로의 정확한 위치 정보를 받게 된다. 이를 이용하여 각 사용자들은 처음 INVITE를 하는 경우 Location Server를 통해 필요한 상대방의 위치정보를 획득하여 사용자들이 서로 호 설정을 할 수 있도록 도움을 준다.

SIP 메시지는 텍스트 기반 메시지 형태로 구성되어있다. 구체적인 내용을 보면 기존의 HTTP 언어형태의 메시지 구조를 사용한다.

일반적으로 VoIP 서비스에서는 호 연결 설정이 최우선으로 진행되어야 하며, 공격자가 DDoS 공격을 위해서는 호 연결 설정을 위한 Proxy Server를 공격 대상으로 한다. 이때 Proxy Server 에서는 정상적이지 않은 메시지를 서비스 에러 내지 공격을 의심할 수 있는 트래픽이라 간주하여 사전에 대처할 수 있으나 정상적인 INVITE 메시지를 통한 DDoS 공격은 탐지함에 있어 어려움이 있다.

2.2 SIP 공격기법

현재 SIP 공격 기법은 크게 두 가지가 있다[2]. 첫번째로 SIP 메시지를 대량으로 보내어 SIP 사용자나 사업자가 정상적인 서비스 이용 혹은 제공하지 못하게 하는 것으로, 일반 네트워크에서 DoS와 개념이 비슷한 Message Flooding 공격이 있다. 이 공격은 공격자가 INVITE, Register 등의 메시지들을 다량으로 보내어 정상적인 사용자 혹은 서버의 서비스 오작동이나 오류를 발생시켜 실질적인 사용자가 서비스를 사용할 수 없게 한다. 대표적인 Message Flooding 공격은 다음과 같다[3].

- Register Flooding 공격 : 공격자의 반복적인 register를 통해 다른 사용자가 서버를 사용하지 못하게끔 과부하를 거는 공격의 형태이다. 대표적으로 서버 flooding 공격이 있다.

- Invite, RTP Flooding : 공격 대상은 SIP 서버(Register, Redirect, Proxy), 소프트웨어 스위치, 사용자 단말 및 PC(소프트 폰)이며 공격자는 많은 수의 유효한 요청 메시지(SIP INVITE) 또는 음성메시지를 보내어 시스템이 이에 대하여 응답 메시지를 준비하게 함으로써 해당 시스템의 CPU 및 메모리 자원을 고갈시킨다. 피해내용은 시스템 자원의 고갈로 인하여 서비스의 이용 및 사용하고 있는 모든 사용자의 서비스 지연 또는 마비가 된다.

- Cancel 공격 : 공격자가 SIP 사용자 단말의 호 설정을 방해하기 위한 공격이다. 주로 연결되어 있는 호 설정을 끊기 위해서 사용된다.

- Bye 공격 : 이 공격은 Cancel 공격과 유사한 공격이다. Cancel 공격이 호 설정단계에서 수락 메시지가 오기 전에 Cancel 메시지를 보내야 하기 때문에 공격하는 시점이 매우 중요하지만 Bye 공격은 SIP 단말들이 통화 하고 있는 어느 시점에서도 공격이 가능하다는 특징이 있다. 두번째 공격 기법으로는 SIP Parser 공격으로 Malformed Message 공격(비정상 메시지 공격)이 있다. 이는 SIP의 헤더와 바디 내용이 일반 문자로 되어 있다는 점을 이용하여 다른 문자들로 삽입, 변조 혹은 삭제하는 것이다.

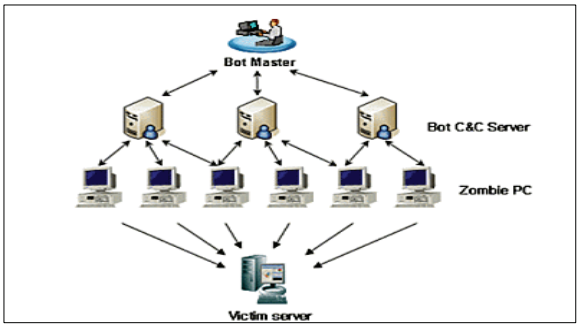
2.3 DoS/DDoS 공격의 특성

인터넷 공격의 최근 경향은 시스템 또는 망 자원을 공격 대상으로 사용가능한 자원을 모두 고갈시킴으로써 실제 자원을 사용해야 하는 사용자가 자원을 사용할 수 없게 하는 DoS 공격의 증가를 들 수 있다.

DoS 공격은 대역폭, 프로세스 처리 능력, 기타 시스템 자원 등을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격 형태이다. 대역폭을 목표로 한 공격은 시스템에 대량의 TCP, UDP, 또는 ICMP 패킷을 보내 이루어지며, 프로세스 처리 능력 등 시스템 자원 고갈을 목표로 하는 공격은 TCP 옵션 변경, 비정상적인 패킷 사이즈 등 비정상 패킷을 송신하여 자원을 고갈시키거나 비정상적으로 시스템을 멈추게 한다.

또한 최근에는 기존의 DoS 공격과 같이 공격자 한 사람에 의해 공격이 이루어지는 것이 아니라 지역적으로 널리 분산된 다수의 시스템에 공격 에이전트를 설치한 후,

동시에 공격함으로써 큰 파괴력을 보이는 DDoS 공격이 일반화되는 추세이다. [그림 2]는 DDoS 공격의 그림이다 [4].



[그림] 2 DDoS 공격

2.4 DoS/DDoS 종류

DoS/DDoS의 종류는 다음과 같다[5].

- Land 공격

  Land 공격은 라우터가 IP 패킷의 Address만을 보고 라우팅하는 구조를 악용하여 대상 서버를 공격하는 것이라 할 수 있다. 공격자는 공격 대상 서버의 주소를 Source IP Address 필드와 Destination IP Address 필드에 넣은 TCP SYN 패킷을 공격 대상 서버에게 전송한다.

- Smurf 공격

  Smurf 공격은 Land 공격과 유사하게 Source IP Address를 위장하여 이루어지나, Land 공격과는 달리 ICMP 프로토콜을 사용한다. Smurf 공격은 Spoofing Technique과 Broadcast Address를 사용한다. Source IP Address에는 공격대상의 IP Address를 삽입하고, Destination IP Address에는 Broadcast Address를 사용하여 공격대상 망에 ICMP ECHO 메시지를 보낸다. 공격대상 망은 이로 인해 대역폭을 많이 낭비하고, 아울러 대량의 ICMP 패킷 처리로 인해 CPU 사용을 낭비하게 됨에 따라 최종적으로 시스템 crash 및 통신 불능 상태가 될 수 있다.

- SYN Flooding 공격

  SYN 공격은 SYN 패킷을 대량으로 송신하여 이루어진다. TCP는 SYN 패킷과 ACK 패킷의 교환을 통해 상대방의 상태를 확인하고 세션을 설립하며 데이터를 교환한다. SYN 공격에서는 이를 악용하여 SYN 패킷만을 대량으로 공격 대상에게 전송한다. 공격 받은 대상은 SYN 패킷마다 TCP 소켓을 열기 때문에 CPU와 메모리를 과도하게 사용한다. 그러나 ACK가 없기 때문에 세션을 위해 할당한 자원을 해제하지 않고 그대로 유지하게 되어 최종적으로 자원을 소진하여 응답 불능상태에 빠지게 된다. SYN 공격에는 최초의 SYN 패킷만을 대량으로 송신하는 것과 SYN, SYN ACK, ACK 까지의 핸드쉐이크를 하고, 데이터를 송수신하지 않는 것이 있다.

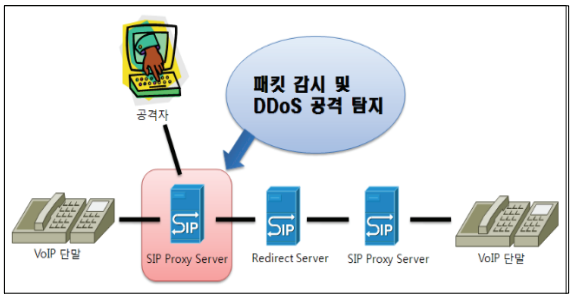
- Ping of death 공격

  UNIX의 'Ping' 명령은 여러 파라미터를 이용하여 다양한 ICMP request를 보낼 수 있는데, 사용자는 이러한 방법을 사용하고 패킷크기를 조절하여 전송할 수 있다. Ping of death 공격은 이를 악용하여 비정상적으로 큰 사이즈의 ICMP 패킷을 대량으로 송신(65 Kbytes 이상의 ICMP request를 송신)하는 공격을 의미한다. 이러한 대량의 비정상적인 크기의 ICMP 패킷으로 인해 누적되어 응답 불능 상태에 빠질 수 있다.

VoIP의 경우 SIP 단말의 등록을 위한 Register 패킷을 과도하게 요청하는 Register storm 공격, 통화를 과도하게 시도하는 INVITE/BYE 공격등이 있다[6]. DDoS 공격은 수분 내에 공격이 급속도로 전파되는 특징을 가지며, 초당 수천에서 수만 개의 비정상적인 패킷들을 네트워크에 흘려보낸다. 이로 인해 부수적으로 응답 패킷 및 ICMP 패킷들이 다량으로 발생하여 공격의 대상이 되는 시스템은 물론이고, 경로상의 네트워크 전체를 마비시킬 위험이 있다. 따라서 본 논문에서는 SIP를 이용한 VoIP 서비스에서 IP 분류와 메시지 중복 검열을 통해 DDoS 공격을 탐지할 수 있는 기법을 설계하였다.

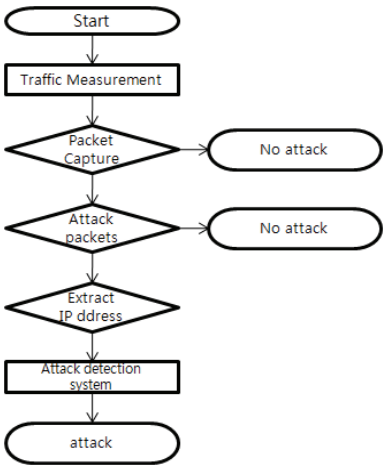
3. 제안하는 DDos 공격 탐지 기법

본 논문에서 제안하는 DDoS 공격 탐지 기법은 INVITE /BYE 공격 등의 SIP 환경에서 주요한 공격들과 기존의 IP 네트워크에서 발생하는 UDP/ICMP/TCP SYN Flooding과 같은 공격들을 탐지하는 기법으로 기존 네트워크에서의 평균 트래픽과 실시간 트래픽 양을 비교하고, SIP 환경에서 발생하는 INVITE 중복 메시지 검열 및 IP 분류를 통해 DDoS 공격 탐지 기법을 설계한다. [그림 3]은 DDoS 공격 탐지 시스템의 구성도를 나타낸다.



[그림 3] 제안 DDoS 탐지 시스템 구성도

VoIP의 Proxy Server와 여러 단말이 연계되어있고, 이 Proxy Server는 DDoS 공격 초기에 공격자와 단말이 서로 통신하는지를 판단하는 패킷 감시 모듈을 탑재한다. 이에 따라 Proxy Server로 출입하는 모든 패킷들을 감시하여 공격자로 판단한 IP 주소를 탐지한다. [그림 4]는 공격 탐지 기법 순서도를 나타낸다.



[그림 4] 공격 탐지 기법 순서도

시스템이 작동되면 실시간 네트워크로 외부에서 유입되는 트래픽의 모든 패킷을 측정한다. 일정 시간동안 트래픽을 측정하여 평균 트래픽의 양보다 크게 나타날 경우 DDoS 공격으로 간주하며, 공격 패킷인지 일시적인 비정상 패킷인지를 판단한다. 이후 공격 패킷에 대한 IP 검열을 통해 공격 IP 주소를 추출하고 공격 차단 시스템으로 전달한다. [그림 5]는 Proxy Server의 구성도이다.

[그림 5] Proxy Server의 구성도

Proxy Server의 패킷 캡쳐 모듈은 외부에서 유입되는 트래픽의 모든 패킷을 실시간으로 탐지하며, 트래픽 계산기는 일정시간 유입되는 트래픽의 양을 측정하게 된다. 측정한 트래픽의 양이 평균트래픽의 양보다 크게 나타날 경우 DDoS 공격으로 간주하여 IP 분류기를 통해 IP 검열을 하게 되며, 공격 차단 시스템으로 전송하여 각 프로토콜의 공격을 추출해 낸다.

4 .결 론

SIP 기술은 통신 절감 효과가 크고 다양한 부가서비스를 제공함에 따라 지속적으로 발전하고 있으며, 이에 따라 사용자 또한 급속도로 증가하고 있는 추세이다. 하지만 다양한 음성 및 멀티미디어 서비스를 제공함에 있어 네트워크를 통한 보안상의 취약점 또한 동반하고 있기 때문에 근본적인 취약점은 해결하고 있지 못하고 있는 실정이다. 본 논문에서는 SIP 기반의 VoIP 환경에서 안전하고 원활한 SIP 통신을 위해 DDoS 공격으로 인한 트래픽 과부하 및 IP 분류를 통한 DDoS 공격 탐지 기법을 제안하였다. 제안 시스템을 사용함으로써 SIP 환경에서 발생하는 DDoS 공격에 따른 서버/클라이언트 통신상의 트래픽 과부하를 파악하고 IP 분류기를 통한 기존의 SIP 프로토콜의 취약점에 대한 대응 방안을 제시하였다. 향후 연구방향으로는 실제 구현을 통해 DDoS의 공격을 얼마나 탐지할 수 있는지 트래픽 계산에 대한 연구가 필요하다.

참고문헌

[1] D.Malas. SIP performance metrics. Internet draft draft-malas-performance-metrics-06.txt (work in progress), IETF, 2007

[2] 박진범, 백형구, 원용근, “VoIP 보안 취약점 공격에 대한 기존 보안장비의 대응 분석 연구”, 한국정보보호학회, 한국정보보호 학회지 제17권 제 5호, P.57~65, 2007

[3] 한국정보보호진흥원. “VoIP 정보보호 가이드” 2005

[4] A3시큐리티컨설팅, http://www.a3sc.co.kr/

[5] 구자현 “서비스 거부 공격(Denial of Service)의 유형 및 대응”, ITFIND 주간기술동향 1377호, 2008

[6] “VoIP 서비스 및 시스템 DoS 공격탐지 및 대응기법 연구”, 한국정보보호진흥원, 2006