SIP(Session Initiation Protocol) 트래픽 관리 도구의 설계와 구현*

강경철[0] 류연승
한림대학교 정보통신공학부
{kckang[0],ysryu}@hallym.ac.kr

Design and Implementation of SIP Traffic Management Tool

Kyoung-Cheol Kang[0] Yeon-Seung Ryu
Div. of Information and Comm. Eng. Hallym University

요 약

본 논문에서는 SIP(Session Initiation Protocol)을 사용하는 VoIP(Voice over IP) 네트워크에서 SIP 트래픽을 감시, 분석하는 관리 도구인 SIPMan 을 설계하고 구현하는 연구를 소개한다. 구현하는 SIPMan 은 실시간으로 SIP 패킷을 캡처하여 call 에 대한 다양한 정보를 분석하며 DB 에 저장할 수도 있다. VoIP 망 관리자는 SIPMan 의 web GUI 를 사용하여 call detail record, SIP 트래픽 정보 등을 모니터링할 수 있다.

1. 서 론

컴퓨터와 인터넷 기술의 발전으로 인터넷으로 음성 및 화상으로 대화할 수 있는 VoIP(Voice over IP) 서비스가 가능해지고 있다. VoIP 를 위한 국제 표준 통신 프로토콜로는 90 년대 중반부터 제안되어 왔던 ITU-T H.323[1]이나 최근 대두되고 있는 IETF 의 SIP (Session Initiation Protocol)[2,3]과 MGCP(Media Gateway Control Protocol)[5], MEGACO[4] 규격들이 있다. 그동안 VoIP 제품들은 H.323 프로토콜을 사용하여 개발되어 온 것들이 대부분이었으나 아직까지는 대중화되어 널리 사용되고 있지는 않다. 한편, 최근에는 게이트웨이의 제어 프로토콜로는 MGCP 와 MEGACO 를 고려하고 있으며, 마이크로소프트의 메신저, PDA, 3GPP 등의 단말기에서는 SIP 를 적용하려는 추세에 있다. 차세대 이동 통신과 무선 랜에서도 상호간에 SIP 를 이용한 인터넷 전화가 가능해지리라 예측된다.

이와 같이 빠르게 발전하고 있는 VoIP 응용과 관심에 비해 VoIP 트래픽을 감시, 분석하고 제어하는 도구들은 미비한 상태이다. 물론 기존의 네트워크 트래픽을 모니터링하는 도구들이 있지만[12, 13, 14], SIP 프로토콜을 사용하는 VoIP 망에서 VoIP 트래픽을 감시, 분석하는 도구는 거의 없다.

본 논문에서는 SIP 프로토콜을 사용하는 VoIP 네트워크에서 SIP 트래픽을 감시, 분석하는 관리 도구인 SIPMan 을 설계하고 구현하는 연구를 소개한다. 구현하는 SIPMan 은 실시간으로 SIP 패킷을 캡처하여 call 에 대한 정보를 분석하고 DB 에 저장한다. 관리자는 web GUI 를 사용하여 SIP 트래픽, call detail record 등을 살펴볼 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 SIP 프로토콜과 네트워크 패킷 캡처에 관한 관련 기술에 대해서 살펴본다. 3 장에서는 SIPMan 의 구조와 설계 및 구현에 대해 기술하며, 마지막으로 4 장에서 결론 및 향후 연구 방향에 대해 기술한다.

*본 연구는 인터콘웨어㈜의 지원에 의해 수행되었습니다.

2. 관련 연구

2.1 SIP(Session Initiation Protocol)

SIP 는 인터넷에서 멀티미디어 세션(session)을 개시하고 세션 안에서 음성, 영상, 메시지 등의 전송을 하는데 사용하는 표준 프로토콜이다. 자세한 내용은 IETF 의 RFC 2543[4]에 설명되어 있다.

SIP 는 다음과 같은 구성요소를 가진다.

① UAC(User Agent Client)
SIP 세션을 개시하는 논리적 실체이며 SIP 요청 메시지를 보내어 세션을 요청한다. 요청 메시지의 존속기간동안 UAC 로 동작한다.

② UAS(User Agent Server)
UAC 가 보내는 SIP 요청 메시지에 응답하는 논리적 실체이며 요청 메시지를 수용, 거절, 또는 redirct 한다.

③ UA(User Agent) = UAC + UAS

④ Redirect Server

SIP 요청 메시지의 주소를 0 개 이상의 새로운 주소로 매핑, 클라이언트에게 새로운 주소를 반환한다.

⑤ Proxy Server

SIP 메시지를 내부적으로 처리하거나 다른 서버로 전달하고 해석하여 포워딩 전에 재작성 가능케 한다.

⑥ Registrar

REGISTER 요청 메시지를 수용하는 서버이다. Proxy Server 나 Redirect Server 와 함께 구현될 수 있다.

SIP 메시지는 크게 요청(request) 메시지와 응답(response) 메시지로 되어있다.

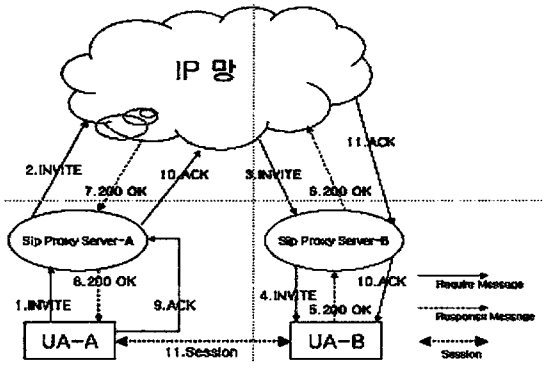
(가) 기본적인 메시지

① INVITE : 세션을 요청함
② ACK : INVITE 에 대한 최종 응답 메시지
③ BYE : 세션을 종료함
④ CANCEL : 세션을 취소함
⑤ OPTION : 상대방의 부가 능력을 알아봄
⑥ REGISTER : 사용자의 위치를 등록함

(나) 응답 메시지의 응답 코드

① 1XX : 요청메시지를 수신하고 계속 처리 중임.
② 2XX : 수신이 성공적으로 수용됨.
③ 3XX : 요청메시지 수용전에 더 취할 행동이 있음.
④ 4XX : 요청메시지에 에러가 있거나 서버에서 처리할 행동이 없음.
⑤ 5XX : 요청메시지는 유효하나 서버가 수행할 수 없음.
⑥ 6XX : 요청메시지가 다른 어떤 서버에서도 수행할 수 없음.

그림 1 은 UA-A 와 UA-B 가 Registrar 에 등록되어 있는 상태를 가정으로 상호간 세션 설정을 하는 절차를 보이고 있다.



[그림 1] SIP Call Flow 의 예

(1~4) : UA-A 에서 세션을 개시하기 위해 INVITE 메시지 보내고 이 INVITE 메시지는 proxy server 와 IP 망을 거쳐 UA_B 의 proxy server 를 통해 UA-B 에게 전달된다.

(5~8) : INVITE 메시지에 대한 수신이 성공적으로 수용되었음을 나타내는 200 OK 메시지를 UA-B 가 UA-A 에게 보낸다.

(9~12) : 200 OK 메시지가 도착하면 UA-A 가 ACK 메시지를 보내어 세션이 설정된다.

(11) : 설정되어진 세션을 통해 UA-A 와 UA-B 가 상호간에 통신을 하게 된다.

2.2 pcap

pcap 은 다양한 운영체제 상에서 패킷을 캡처하기 위한 도구로써 개발된 사용자 수준의 라이브러리이다[6,7]. 이것은 tcpdump[8]의 라이브러리로써 개발되었는데 운영체제에 독립적이라는 우수성 때문에 대부분의 네트워크 패킷 분석 도구에서 사용되고 있다. 리눅스(Linux)에서는 libpcap, 윈도우에서는 winpcap 이라는 이름의 pcap 라이브러리가 있다.

이 라이브러리들은 패킷을 캡쳐할 수 있도록 다음과 같은 API 들을 제공하고 있다.

① 캡쳐할 디바이스 정보를 구한다.(pcap_loopupdev)
② 디바이스를 개방한다. (pcap_open_live)
③ 필터를 설정한다. (pcap_compile, pcap_setfilter)
④ 캡쳐한 패킷을 구한다. (pcap_next)
⑤ 콜백 함수를 설정한다. (pcal_loop, pcap_dispatch)

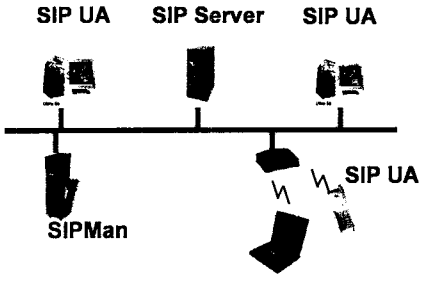
2.3 패킷 캡쳐 도구들

tcpdump 는 libpcap 를 사용하여 만들어진 프로그램이다[8]. 유닉스 명령어 행에서 사용하며, TCP, UDP 패킷의 흐름을 캡쳐하여 보여주거나 파일에 저장한다. 또한, 파일에 저장된 내용을 이용하여 필터된 내용을 보여주기도 한다.

mmdump 는 tcpdump 를 확대하여 멀티미디어 세션과 관련된 프로토콜을 캡쳐하고 보여주는 프로그램이다[14]. RTSP, H.323 세션을 캡쳐하는 기능이 있다.

3. SIPMan 의 설계와 구현

3.1 네트워크 구성



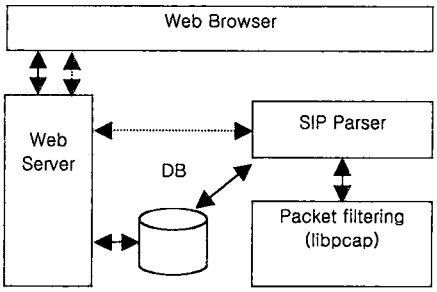
[그림 2] SIPMan 의 구성

그림 2 에 SIPMan 이 설치된 네트워크 구성도를 보이

고 있다. 본 연구에서는 Vovida 의 vocal 시스템을 활용하여 SIP 서버와 SIP UA 를 구축하였다[9]. SIP 서버는 proxy, redirection, registra 기능을 포함한다. SIP UA 는 PC 의 SIP phone 이나 Wireless LAN 이 장착된 Notebook PC, PDA 등에서 사용하는 SIP phone 이 된다. 구현하는 SIPMan 은 리눅스 운영체제를 사용하는 서버에 설치된다. 동일한 서버에 관리자를 위한 Apache 웹서버와 MySql 이 설치되었다.

3.2 소프트웨어 구성

SIPMan 의 소프트웨어 구성이 그림 3 에 나와있다. SIPMan 은 리눅스의 libpcap 을 사용하여 패킷을 캡처하고 SIP Parser 에서 SIP 패킷을 분석한다. 분석된 데이터는 DB 에 저장한다.



[그림 3] SIPMan 의 소프트웨어 구성

SIPMan 의 GUI 는 web browser 에서 구현된다. 관리자는 SIPMan 이 설치된 서버에 접속하여 실시간으로 모니터링하거나 기저장되어 있던 데이터를 분석할 수 있다.

3.3 기능 및 특징

SIPMan 은 SIP 패킷을 분석하여 다음과 같은 세션 정보를 알아낸다.

① 세션의 개시 시간
② 세션에 연결되어 있는 사용자 (caller, callee)
③ 사용된 미디어의 종류(voice, video 등)
④ 실제로 연결된 세션의 위치
⑤ 세션의 기간 (duration)

여기서, 세션의 기간은 SIP 메시지에서 ACK 메시지를 수신했을 때부터 시작하고 BYE 메시지를 수신했을 때 종료하는 것으로 정의하였다.

또한, SIPMan 은 네트워크 트래픽 정보를 취합한다.

⑥ 초당 전송되는 바이트양
⑦ 평균 트래픽
⑧ 최대 트래픽

관리자는 SIPMan 이 취합한 정보에서 다양한 통계를 도출할 수 있다. 예를 들면, 사용자별 세션 횟수, 기간별 세션 횟수, 기간별 트래픽, 세션 기간의 분포 등 SIP 망을 효율적으로 관리할 수 있도록 분석한다.

4. 결 론

저렴한 가격에 의한 통신비 절감, 다양한 IP 응용과의 통합 등의 장점을 제공하는 VoIP 기술은 멀지않은 장래에 더욱 확대되고 일반화될 것으로 예측되고 있다. 그러나, VoIP 응용의 보편화를 위해서는 음성/화상 품질의 보장, 보안, 전화번호 체계 등이 해결되어야 할 것이다. VoIP 트래픽의 관리 기술은 음성/화상 품질의 보장 및 보안 기능을 위한 필수 기술이다. 그러나, VoIP 트래픽을 감시, 분석하고 제어하는 도구들은 많지 않다. 특히, 차세대 VoIP 프로토콜인 SIP 프로토콜을 이용하여 인터넷 전화를 하는 VoIP 망에서 VoIP 트래픽을 감시, 분석하는 도구의 연구 개발이 필요하다.

본 논문에서는 SIP 프로토콜을 사용하는 VoIP 네트워크에서 SIP 트래픽을 감시, 분석하는 관리 도구인 SIPMan 을 설계하고 구현하였다. 구현한 SIPMan 은 리눅스 서버에서 구현되었으며, 실시간으로 SIP 패킷을 캡처하여 call 에 대한 정보를 분석하고 DB 에 저장한다. 또한, Web-based 관리자 용 GUI 를 개발하고 있다.

향후에는 SIP 패킷의 제어(control) 기능을 구현할 계획이다. 리눅스 커널의 네트워크 모듈과의 인터페이스를 구현하고 SIP 패킷의 실시간 제어 및 정책 기반의 제어를 통해 QoS(Quality of Service)를 보장하는 연구를 진행할 계획이다.

5. 참고 문헌

[1] ITU-T Recommandation H.323 Version 4, "Packet Based Multimedia Communications System", Nov. 2000.
[2] Hendley, M., H. Shulzrinne, E. Schooler and J. Rosenberg, "SIP:Session Initiation Protocol", IETF RFC 2543, Mar. 1999.
[3] http://www.cs.columbia.edu/sip/
[4] ITU-T Recommandation H.248 Version 1,Jun. 2000.
[5] IETF RFC 2705, " Media Gateway Control Protocol (MGCP)," Oct. 1999.
[6] http://www.tcpdump.org/pcap.htm
[7] http://kldp.org/KoreanDoc/html/Libpcap-KLDP/
[8] http://www.tcpdump.org
[9] http://www.ethereal.org
[10] http://www.vovida.org/vocal
[11] Vern Paxson, " Automated Packet Trace Analysis of TCP Implementation" , SIGCOMM, pp. 167-179, 1997
[12] Vern Paxson, " Bro: A System for Detecting Network Intruders in Real-time" , Computer Networks, Vol. 31, No.23-24, 1999.
[13] Marcus Ranum, et al, " Implementing A Generalized Tool For Network Monitoring" , Proceedings of the Eleventh Systems Administration Conference (LISA '97), 1997
[14] R. Caceres, et al, " mmdump - A Tool for Monitoring Multimedia Usage on the Internet" , ACM Computer Communication Review, 30(4), Oct. 2000