# SIPMan : SIP 트래픽 관리 도구의 구현*

강경철, 추승우, 이강희, 류연승
한림대학교 정보통신공학부
e-mail : kckang@center.cie.hallym.ac.kr, ysryu@hallym.ac.kr

# SIPMan : SIP Traffic Management Tool

Kyong-Cheol Kang, Seung-Woo Chu, Kang-Hee Lee, Yeon-Seung Ryu
Division of Information and Comm. Engineering, Hallym University

요 약

본 논문에서는 VoIP(Voice over IP) 표준 프로토콜로 사용되고 있는 SIP 프로토콜의 트래픽을 감시, 분석하는 관리 도구인 SIPMan 을 구현하였다. SIPMan 은 SIP 패킷을 실시간으로 캡처할 수 있으며 call 에 대한 정보를 분석하고 DB 에 저장하는 기능을 가진다. 관리자 인터페이스는 web-based 로 구현하였고 리눅스에서 구현되었다. SIPMan 관리자는 call detail record, SIP 트래픽 정보 등을 모니터링하고 분석할 수 있다.

## 1. 서 론

네트워크의 고속화, 컴퓨터의 고성능은 인터넷 상의 PC 간에 음성 및 화상 데이터를 실시간으로 통신하는 응용을 가능하게 하고 있다. VoIP (Voice over IP) 기술은 인터넷 망에서 음성 이나 화상으로 대화할 수 있는 인터넷 전화 기술이다. VoIP 를 위한 국제 표준 통신 프로토콜로는 90 년대 중반부터 제안되어 왔던 ITU-T H.323[1], 최근 대두되고 있는 IETF 의 SIP (Session Initiation Protocol)[2,3]과 MGCP(Media Gateway Control Protocol)[5], MEGACO[4] 표준 규격들이 있다. 국내에서는 VoIP 포럼이 조직되어 인터넷 전화를 활성화하기 위한 국가 표준을 만들고 있다.

최근 몇몇 업체에서 인터넷 전화 서비스를 무료 또는 유료로 제공하고 있다. 대부분 이러한 업체에서 사용하는 게이트웨이, 게이트키퍼와 같은 장비들은 H.323 프로토콜을 사용하는 것들이 대부분이었다. 그러나, H.323 은 기존의 PSTN 이나 ISDN 같은 통신망에서 사용하는 시그널링 프로토콜을 적용하여 구현이 복잡한 단점이 있다. 반면에 SIP 프로토콜은 간단하여 구현이 쉽고 모바일과의 확장이 간편한 장점이 있어 차세대 VoIP 프로토콜로 떠오르고 있다. 마이크로소프트의 메신저, PDA, 3GPP 등의 단말기에서는 SIP 프로토콜을 사용하여 인터넷 전화 기능을 제공하려는 추세에 있다. 향후에는 차세대 이동 통신과 무선 랜에서도 상호간에 SIP 를 이용한 인터넷 전화가 가능해지리라 예측된다. 한편, 게이트웨이의 제어 프로토콜로는 MGCP 와 MEGACO 프로토콜이 고려되고 있으며, softswitch 와 같이 연구되고 있다.

이와 같이 빠르게 발전하고 있는 VoIP 응용과 관심이 많아지면서 인터넷에서 VoIP 트래픽이 증가할 것으로 예측할 수 있다. 그러나, VoIP 트래픽을 감시, 분석하고 제어하는 도구들은 미비한 상태이다. 물론 네트워크 트래픽을 모니터링하는 도구들이 연구되어 왔지만[12, 13, 14], SIP 프로토콜을 사용하는 VoIP 망에서 VoIP 트래픽을 감시, 분석하는 도구에 대한 연구는 미비하다.

본 논문에서는 SIP 프로토콜을 사용하는 VoIP 네트워크에서 SIP 트래픽을 감시, 분석하는 관리 도구인 SIPMan 을 설계하고 구현한 연구를 기술한다. SIPMan 은 네트워크 패킷에서 SIP 패킷을 실시간으로 캡처할 수 있으며 call 에 대한 정보를 분석하고 DB 에 저장하는 기능을 가진다. 관리자 인터페이스는 web-based 로 구현하였고 리눅스에서 구현되었다. SIPMan 관리자는 call detail record, SIP 트래픽 정보 등을 모니터링하고 분석할 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 SIP 프로토콜과 네트워크 패킷 캡처에 관한 기존 연구에 대해서 살펴본다. 3 장에서는 SIPMan 의 구조와 구현에

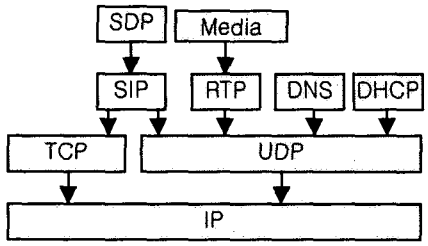
* 본 연구는 인터콘웨어㈜의 지원을 받아 수행되었습니다.

대해 기술하며, 마지막으로 4장에서 결론 및 향후 연구 방향에 대해 기술한다.

## 2. 관련 연구

### 2.1 SIP (Session Initiation Protocol)

SIP 는 인터넷에서 멀티미디어 세션(session)을 개시하고 세션 안에서 음성, 영상, 메시지 등의 전송을 위해 IETF 에서 정의하고 있는 표준 프로토콜이다. SIP 는 TCP/UDP 에 정의되어 있어 응용 계층 프로토콜이며, 사용하는 문법(syntax)은 HTTP 1.1 에서 유래되었고 텍스트 기반으로 되어 있다. 그림 1 은 SIP 프로토콜 스택을 보여주고 있다.




[그림 1] SIP 프로토콜 스택

SIP 프로토콜은 클라이언트-서버 구조에서 정의되었으며, 구성요소는 다음과 같다.

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 redirect 한다.

③ UA(User Agent) = UAC + UAS
UAC 와 UAS 기능을 가진다.

④ Redirect Server
SIP 요청 메시지의 주소를 새로운 주소로 매핑하고 반환한다.

⑤ Proxy Server
User agent 로부터 SIP 메시지를 받아 내부적으로 처리하거나 다른 서버로 포워딩한다. 서비스 로직이 구현될 수 있으며 SIP 망의 핵심 기능을 가진다.

⑥ Registrar (Registration Server)
동적으로 사용자의 위치를 등록하는 서버이다.

⑦ Location Server
사용자의 정적인 정보를 가지는 서버이다.

SIP 메시지는 요청(request) 메시지와 응답(response) 메시지로 되어있으며, 보통 UDP 포트 5060 으로 주고받는다.

(가) 주요 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

SIP 메시지는 메소드(method), 헤더(header)와 몸체(body)로 정의되어있다. 메소드는 메시지 종류와 URL 을 기술한다. 헤더에는 From, To, Call-Id 등의 여러 필드가 정의되어 있다. 몸체는 SDP(Session Description Protocol) 형식을 사용하며 미디어 유형 등을 기술할 수 있다.

(나) 응답 메시지의 응답 코드
① 1XX : 요청메시지를 수신하고 계속 처리 중임.
② 2XX : 수신이 성공적으로 수용됨.
③ 3XX : 요청메시지 수용 전에 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 2 는 INVITE 메시지의 예를 보이고 있다.

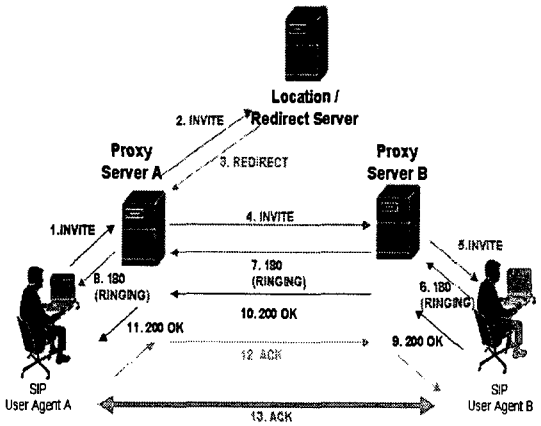
```
INVITE sip:userB@hostB.com SIP/2.0
Via: SIP/2.0/TCP hostA.com:2054
CSeq: 1 INVITE
Contact: sip:userA@hostA.com:5060
Expires: 3600
From: sip:userA@hostA.com
To: sip:userB@hostB.com
Call-ID: 460414147@hostA.com
Content-Type: application/sdp
Content-Length: 206

v=0
o=userA 103141879711 1006526069 IN IP4 hostA.com
s=Untitled
c=IN IP4 hostA.com
t=0
m=audio 10000 RTP/AVP 0
m=video 20000 RTP/AVP 0
m=wb 30000 RTP wb
m=text 40000 UDP chat
```

[그림 2] INVITE 메시지

INVITE 메시지에는 caller, callee 의 정보 및 사용하려는 미디어의 정보가 담겨있다. 또한, call 을 구분하기 위한 ID 등의 정보가 담겨있다.

그림 3 은 UA-A 와 UA-B 가 상호간 세션 설정을 하는 절차를 보이고 있다.




[그림 3] SIP Call Flow 의 예

[1,2,3,4,5] : UA-A 에서 UA-B 와의 세션을 개시하기 위해 proxy servr A 에게 INVITE 메시지를 보낸다 (1). Proxy server A 는 UA-B 가 현재 등록되어 있는 위치를 알아내기 위해서 Location Server 에게 INVITE 메시지를 전송한다 (2). Location Server 는 UA-B 의 현재 등록되어 있는 위치(여기서는 proxy server B 의 주소)를 알려준다 (3). Proxy Server A 는 proxy server B 에게 INVITE 메시지를 보내고 (4), INVITE 메시지는 UA-B 에게 전달된다 (5).

[6,7,8] : UA-B 는 INVITE 메시지를 받고 사용자에게 세션 요청을 알려준 후, UA-A 에게 응답을 보낸다. 응답 메시지는 180 RINGING 의 응답 코드를 가진다.

[9,10,11] : UA-B 의 사용자가 세션을 수용하면, UA-A 에게 알려준다. 200 OK 의 응답 코드를 가진 메시지를 보낸다.

[12] : UA-B 로부터 200 OK 응답 메시지를 받은 UA-A 는 ACK 메시지를 보냄으로써 세션의 설정이 이루어진다.

[13]: 두 UA 사이에 세션이 설정되어 미디어 통신을 한다.

### 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.

pcap 라이브러리는 패킷을 캡처할 수 있도록 다음과 같은 API 들을 제공하고 있다.

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

### 2.3 패킷 캡처 도구들

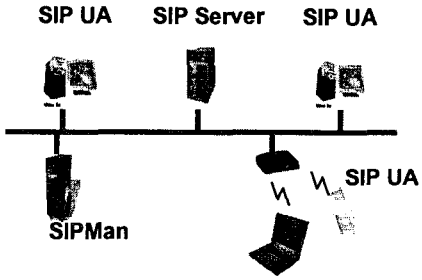
tcpdump 는 libpcap 를 사용하여 만들어진 프로그램이다[8]. 유닉스 명령어 행에서 사용하며, TCP, UDP 패킷의 흐름을 캡처하여 보여주거나 파일에 저장한다. 또한, 파일에 저장된 내용을 이용하여 필터된 내용을 보여주기도 한다.

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

## 3. SIPMan

### 3.1 시스템 구성

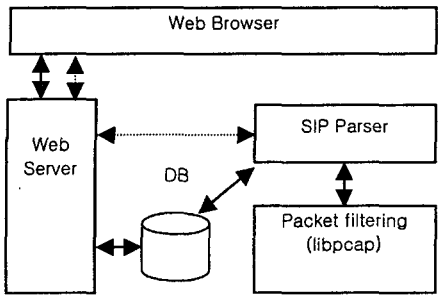
그림 4 에 SIPMan 이 설치된 네트워크 구성도를 보이고 있다. 본 연구에서는 Vovida 의 vocal 시스템을 활용하여 SIP 서버와 SIP UA 를 구축하였다[9]. SIP 서버는 proxy, redirection, registra 기능을 포함한다. SIP UA 는 PC 의 SIP phone 이나 Wireless LAN 이 장착된 Notebook PC, PDA 등에서 사용하는 SIP phone 이 된다. 구현하는 SIPMan 은 리눅스 운영체제를 사용하는 서버에 설치된다. 동일한 서버에 관리자를 위한 Apache 웹서버와 MySql 이 설치되었다.




[그림 4] SIPMan 의 구성

### 3.2 소프트웨어 구성

SIPMan 의 소프트웨어 구성이 그림 5 에 나와있다. SIPMan 은 리눅스의 libpcap 을 사용하여 패킷을 캡처하고 SIP Parser 에서 SIP 패킷을 분석한다. 분석된 데이터는 DB 에 저장한다.




[그림 5] SIPMan의 소프트웨어 구성

SIPMan의 GUI는 web browser에서 구현된다. 관리자는 SIPMan이 설치된 서버에 접속하여 실시간으로 모니터링하거나 이전에 저장되어 있던 데이터를 분석할 수 있다.

### 3.3 기능 및 특징

SIPMan은 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, SIPMan은 SIP 트래픽 정보를 취합한다.

① 초당 전송되는 바이트양
② 평균 트래픽
③ 최대 트래픽

관리자는 SIPMan이 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 연구개발이 필요하다.

본 논문에서는 SIP 프로토콜을 사용하는 VoIP 네트워크에서 SIP 트래픽을 감시, 분석하는 관리 도구인 SIPMan을 설계하고 구현하였다. 구현한 SIPMan은 리눅스 서버에서 구현되었으며, 실시간으로 SIP 패킷을 캡처하여 call에 대한 정보를 분석하고 DB에 저장한다. 또한, Web-based 관리자 용 GUI를 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.

### 참고문헌

[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