

SIP 호 흐름에서 응답메시지의 신뢰성을 위한 메카니즘의 성능 시뮬레이션

이용희*, 박원배**

*, **경북대학교 정보통신학과

e-mail: *yhlee@inc.knu.ac.kr, **wbpark@ee.knu.ac.kr

Performance Simulation of Mechanism for Reliability of Response in SIP call flow

Yong-Hee Lee*, Won-Bae Park**

*, **Dept of Information and Communication, Kyungpook National University

요 약

VoIP(Voice over IP)는 차세대 인터넷 서비스에서 두각을 나타내고 있는 기술이다. 특히 SIP는 텍스트 기반의 프로토콜로써 구현이 쉽고 다른 서비스와의 호환이 쉬워 기존의 H.323을 대체할 기술로써 더욱 주목을 받고 있다. 하지만 SIP에서도 아직 논의되어야 할 부분이 많이 있다. SIP는 전송 프로토콜에 독립적인 응용계층 프로토콜이다. 따라서 종단대 종단 신뢰성 메카니즘이 필요하다. 본 논문에서는 SIP의 응답 메시지의 신뢰성을 위한 메카니즘을 소개하고 시뮬레이션을 통해서 그 성능을 분석한다.

1. 서론

SIP(Session Initiation Protocol)[1]는 응용 계층 컨트롤 프로토콜로써 현재의 VoIP의 주류인 H.323 [2] 프로토콜의 단점을 개선한 프로토콜이다. SIP는 응용 계층 프로토콜이므로 하위 전송 계층 프로토콜로 UDP를 기본으로 사용하고 있으며 TCP를 사용할 수도 있다. 그리고 최근에는 새로운 전송 프로토콜로 SCTP(Stream Control Transimission Protocol)[3]가 제정되었으며 SIP에서 이를 활용하기 위한 인터넷 드래프트[4]도 제안되었다.

SIP는 이동통신 프로토콜인 3GPP를 지원해 이동통신의 코어 네트워크를 IP 네트워크로 대체할 때 핵심적인 역할을 한다. 모든 유무선 인터넷 단말기와 응용 서버에 호 설정 기능은 필수적이므로 SIP의 응용은 무궁무진하다고 할 수 있다. 하지만 아직 논의 되어야 할 부분도 많이 있다. 그러한 문제들 중에는 신뢰성 및 혼잡 제어 등의 문제를 포함하면서

SIP의 메시지 전달 전송 프로토콜로서 TCP를 선택할지 아니면 UDP를 선택하고 추가적인 메카니즘을 제공할지에 대한 이슈도 포함하고 있다[5]. 본 논문에서는 이러한 문제와 관련하여 기존 전송 프로토콜의 대안으로 새로운 전송 프로토콜인 SCTP의 성능 비교 분석을 통해 SIP에서의 사용 가능성을 알아보았다.

본 논문의 구성은 2장의 관련 연구에서 SIP와 SCTP에 대해서 기술하고, 3장에서는 시뮬레이션을 통한 성능 분석에 대해서 기술하며, 마지막으로 4장에서 결론을 기술한다.

2. 관련 연구

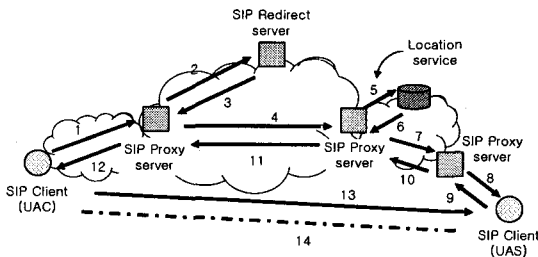
2.1 SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)는 세션 생성, 해제 및 변경 기능을 제공하는 시그널링 프로토콜로써 음성, 영상, 문자 등과 같은 하나 또는 그 이상의 미

디어 타입으로 이루어진 멀티미디어 회의, 인터넷 전화 및 유사한 응용에 적용 가능하다. 세션을 생성하기 위해 사용되는 SIP는 세션에 대한 정보를 전달하고 참가자 간의 호환 가능한 미디어 타입의 정보를 공유함으로써 참가자의 참석을 허락한다.

2.2 SIP의 구성 요소

SIP 구성 요소는 사용자 에이전트와 네트워크 서버로 구성된다. 사용자 에이전트(UA:User Agent)는 사용자 단말로서 일반적으로 세션 요청을 개시하는 사용자 클라이언트(UAC:User Agent Client)와 요청을 수신하고 응답하는 사용자 서버(UAS:User Agent Server)로 구성된다. 그리고 네트워크 서버로는 Proxy Server와 Redirect Server 두 종류가 있으며, Proxy Server는 목적지인 사용자 서버까지의 세션 요청을 전달하며, Redirect Server는 호출할 사용자 서버에 대한 변경된 위치 정보를 사용자 클라이언트에게 전송한다. [그림 1]은 SIP의 네트워크 구성도로서 호의 흐름순서를 나타내고 있다.



[그림 1] SIP Network

2.3 SIP의 주소

SIP 주소는 E-mail 주소와 유사한 형태인 user@host의 형식을 가지고 있다. 이러한 주소는 SIP에 붙여진 실제 호스트에서는 사용자이며 SIP URL이 된다. 또한 이는 사용자 에이전트의 위치 정보를 알려주는 역할을 하게 된다. user부분에는 사용자 이름이나 전화번호가 사용 가능하며 host부분에는 도메인명이나 IP(Internet Protocol) 주소가 사용 가능하다.

2.4 SIP 메시지

SIP 메시지에는 두 가지 종류가 있는데 요청(Request)과 응답(Response) 메시지이다. 사용자 클라이언트는 요청 메시지를 보내고, 사용자 서버는 응답 메시지를 보낸다. 이 요청 메시지와 응답 메시

지는 통신의 자세한 부분을 기술하는 서로 다른 헤더를 포함한다.

SIP는 다음과 같은 기본적인 요청 메시지가 있으며 INFO, COMET, PRACK, SUBSCRIBE 등의 확장 메시지가 있다.

- INVITE : 사용자를 세션으로 초대
 - ACK : INVITE에 대한 최종응답에 대한 확인
 - BYE : 클라이언트의 세션 참여 종료
 - CANCEL : 진행중인 위치탐색 또는 Ringing 중단
 - OPTIONS : 사용자의 Media Capability 조회
 - REGISTER : SIP 서버에게 현재 위치를 등록
- 응답 메시지는 헤더의 첫 라인에 100 ~ 699 사이의 숫자로 된 상태 코드와 사용자를 위한 텍스트 문구를 사용함으로써 요청 메시지에 대한 결과를 제공한다. 다음은 응답 메시지의 상태 코드를 그룹별로 나타내었다.

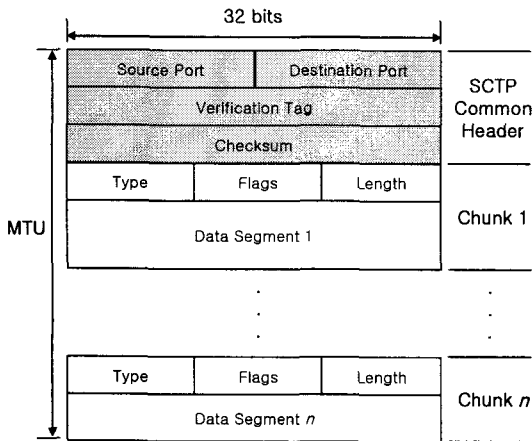
- 100 ~ 199 (1XX) : Informational
- 200 ~ 299 (2XX) : Success
- 300 ~ 399 (3XX) : Redirection
- 400 ~ 499 (4XX) : Client error
- 500 ~ 599 (5XX) : Server error
- 600 ~ 699 (6XX) : Global error

2.5 SCTP(Stream Control Transmission Protocol)

SCTP(Stream Control Transmission Protocol)는 IP를 기반으로 하는 네트워크상에서 PSTN 시그널링 메시지들을 전송하기 위해서 디자인되었다. TCP, UDP와 같은 전송계층 프로토콜로서 대부분의 인터넷 어플리케이션에 대해서 전송계층의 기능을 제공할 수 있다.

SCTP의 주된 새로운 특징 중의 하나가 TCP에서 connection의 개념과 같은 association이다. 2개의 SCTP 종단 사이의 association은 응용 데이터와 제어 데이터 두 가지 모두 전송하는 것을 허용한다. 그리고 전송된 데이터의 전달 순서와 신뢰성에 대해서 조정하는 것이 가능하다.

[그림 2]에서는 SCTP 패킷의 포맷을 보여주고 있다. 패킷의 처음 12bytes는 공통 헤더이다. 이러한 공통 헤더 뒤에는 type-length-value(TLV) 포맷을 사용하는 다양한 길이의 chunk가 하나 또는 그 이상이 포함될 수 있다. 여기에서 chunk란 SCTP 데이터 구조 내부에 위치하는 메시지를 말한다.

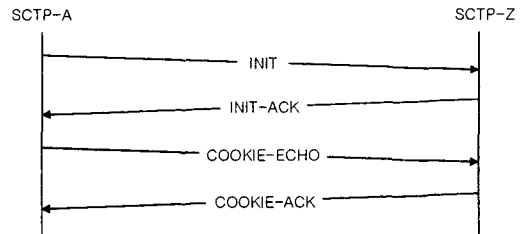


[그림 2] SCTP Packet Format

Association을 식별하기 위해서, 즉 SCTP 패킷 인지 확인하기 위해서 Source Port/Destination Port와 함께 32bits의 Verification Tag를 사용한다. 만약 이 tag를 포함하지 않은 SCTP 패킷이라면 drop 될 것이다. 또한 전송 에러로부터 데이터를 보호하기 위해서 32bits의 Checksum을 포함한다. 각각의 chunk는 data chunk와 control chunk를 구분하기 위한 필드로써 Type 필드를 가지며, 특정한 플래그를 포함하는 Flags 필드와 chunk의 길이를 표시하기 위한 Length 필드를 가진다.

SCTP와 TCP 모두 연결형 프로토콜이다. TCP connection은 2개의 IP 주소와 2개의 포트번호로 정의된다. 예를 들어 A와 Z 두 개의 호스트가 주어졌다면, TCP connection은 한쪽 끝에 있는 IP-A, Port-A를 가진 호스트와 다른 쪽 끝에 있는 IP-Z, Port-Z를 가진 호스트의 연결을 위해서는 $[IP-A]+[Port-A]+[IP-Z]+[Port-Z]$ 로 정의된다.

그러나 SCTP association은 [a set of IP address at A]+[Port-A]+[a set of IP address at Z]+[Port-Z]로써 정의된다. 여기에서 호스트에 대한 IP 주소는 IP 패킷에서 source나 destination으로 사용될 수도 있고 association을 식별하기 위해서 사용될 수도 있다. 앞서 언급했듯이 TCP나 SCTP는 연결형 프로토콜이므로 데이터를 교환하기 전에 통신 상태를 교환해야만 한다. TCP가 three-way handshake를 사용하는 반면, SCTP는 두 개의 호스트가 [그림 3]에서 보듯이 four-way handshake를 통해서 통신상태를 교환한다. 이러한 four-way handshake는 TCP SYN flooding attack[]에 대한 노출을 제거할 수 있다.



[그림 3] SCTP Four-Way Handshake

SCTP는 많은 부분에서 TCP가 지원하는 기능들을 지원하기 때문에 TCP상에서 실행되는 어플리케이션을 SCTP에서는 프로토콜 함수의 손실없이 porting 가능하며, TCP에는 없는 추가적인 기능을 제공한다[6].

- Message boundary preservation
- No "head-of-line" blocking
- Multiple delivery modes
- Multihoming support
- TCP-friendly congestion control
- Selective acknowledgments
- User data fragmentation
- Heartbeat keep-alive mechanism
- DOS protection

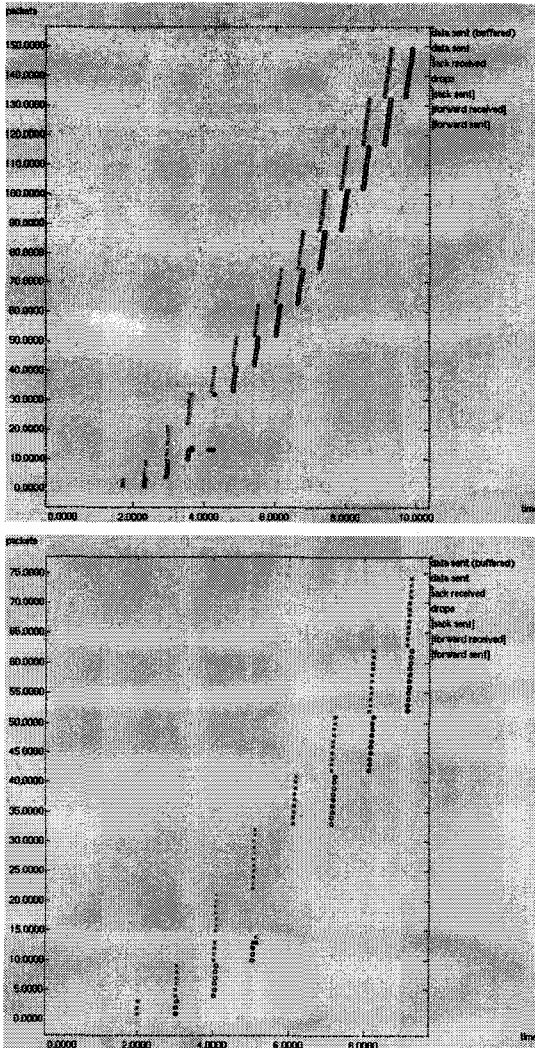
SCTP는 단일 연결만으로 여러 개의 데이터 흐름을 유지할 수 있는 용량 성능을 갖고 있어서 무선 휴대폰과 인터넷 어플라이언스의 연결 및 모니터링에 적합하다.

SCTP를 이용하여 연결 및 신호 경로를 모니터링할 수 있고, 세션 에러 또는 손실을 즉각적으로 탐지할 수도 있다.

3. 성능 분석

SIP 프로토콜은 전송계층 프로토콜에 독립적이다. 그러므로 중단대 중단 신뢰성 메커니즘을 추가할 필요가 있다. 특히 provisional responses의 신뢰도로써 알려진 SIP 확장은 SIP 호 흐름에서 provisional response를 위한 추가적인 신뢰도 메커니즘으로 SCTP를 소개한다[7]. 여기에서 provisional response란 SIP의 응답 메시지들 중에서 Trying(100), Ringing(180) 등의 1XX 코드를 가지는 것들을 말한다. SIP를 위한 전송 프로토콜로써 TCP 프로토콜이 지원된다. 그러나 시그널링에 대한 TCP의 주요 단점 중의 하나가 프로토콜의 긴 연결 셋업 시간이다. SIP의 기본적인 전송 프로토콜인 UDP는 비신뢰성이라는 단점을 가진다. 특히 이러한 것들은

신뢰도가 중단대 중단에 있다는 사실과 많은 중간 링크를 가지는 3GPP 환경에서 문제를 발생시킬 수 있다. 새로운 전송 프로토콜인 SCTP는 세션 셋업 시간과 처리율 등에서 같은 계층의 전송 프로토콜인 TCP나 UDP에 비해 상당한 장점들을 가지고 있다. SIP에서의 SCTP 사용 가능성에 대해서는 인터넷 드래프트 draft-ietf-sip-sctp-03.txt에서도 언급하고 있다. 본 논문에서는 network simulator(ns-2)[8]에서의 시뮬레이션을 위한 과정으로 SIP 모듈[9]과 SCTP 모듈[10]을 분석, 수정하였다.



[그림 4] Sctp(상)와 TCP(하)에서의 시뮬레이션 결과

시뮬레이션을 위한 네트워크 토폴로지의 구성은 간단하게 노드와 노드의 연결로 구성하였다. 중간

링크의 대역폭은 0.5Mbps로 하였으며 MTU는 1500bytes로 하였다. 그리고 시간에 따른 패킷 전송을 시뮬레이션한 결과 [그림 4]에서 보듯이와 같이 TCP에 비해서 SCTP의 경우가 좀 더 빠른 응답과 전송이 가능하다는 것을 알 수 있었다. 추가적으로 zero loss 상태에서는 비슷한 결과를 보였다.

4. 결론

SIP 프로토콜이 차세대 All-IP망에서 호 제어 프로토콜로써 제안되어 표준화가 진행되고 있는 만큼 SIP가 이러한 무선 환경에서의 메시지의 신뢰성 보장을 위해서는 기존의 전송 프로토콜을 그대로 사용하거나 추가적인 메카니즘을 제공하는 것보다는 새로이 제정된 SCTP를 사용하는 것이 더 효율적이라고 볼 수 있다.

참고문헌

- [1] J. Rosenberg, H. Schwarzbauer, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP:Session Initiation Protocol", RFC3261, IETF, Jun. 2002.
- [2] ITU-T Recommendation H.323 Version4, "Packet Based Multimedia Communications Systems", Nov. 2000.
- [3] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson, "Stream Control Transmission Protocol", RFC2960, IETF, Oct. 2000.
- [4] J. Rosenberg, H. Schulzrinne, "The Stream Control Transmission Protocol as a Transport for the Session Initiation Protocol", Internet Draft, draft-ietf-sip-sctp-03.txt, Jun. 2002.
- [5] "SIP 관련 기술에 대한 IETF 표준화 동향 및 이슈", ETRI 주간기술동향, Sep. 2002.
- [6] Randall Stewart, Chris Metz, "SCTP:New Transport Protocol for TCP/IP", IEEE INTERNET COMPUTING, p.64-69, Nov. 2001
- [7] Alexander A. Kist, Richard J. Harris, "SIP Signalling Resources in 3GPP IP Multimedia Subsystems", 2002.
- [8] <http://www.isi.edu/nsnam>
- [9] <http://www.diiie.unisa.it/arec/telecomunicazioni/persona/collab/dgm/nsmod.htm>
- [10] <http://pel.cis.udel.edu>