

SIP 확장을 통한 비공개형 다자간 컨퍼런스의 보안성 확보에 관한 연구

심용범* · 나인호*

*군산대학교

A Study on Guarantee of Security for Closed Multiparty Conference using SIP Extension

Yong-bum Sim* · In-ho Ra*

*Kunsan National University

E-mail : bluelore@kunsan.ac.kr

요 약

VoIP(Voice over IP)에서 제공되는 SIP(Session Initiation Protocol) 기반의 다자간 컨퍼런스(Multiparty Conference) 서비스는 점차 그 사용이 확대되고 있으며, 지속적인 개발과 표준화 작업이 진행 중이다. 그러나 현재 SIP에서는 다자간 컨퍼런스 참가자의 정보 획득과 분배를 위한 기능을 제공하지 않고 있다. 본 논문은 SIP 기반의 다자간 컨퍼런스에서 보안성 확보를 위한 SIP 확장에 관한 연구이며, 새로운 메소드와 헤더필드 구성을 통한 SIP 확장에 대해 다루었다. 또한, 제안된 SIP 확장을 통해 비공개형 다자간 컨퍼런스에서 호 설정이 이루어질 때 사용자의 정보를 획득하고 사용자 정보를 각 컨퍼런스 참가자들에게 분배하는 것이 가능하도록 하였다.

ABSTRACT

The use of Multiparty Conference service based on SIP for VoIP provides is gradually magnified, and the work for continuous development and standardization on SIP is in the process of advancing. But, currently it is impossible for SIP to support identity discovery and distribution of each participant for multiparty conference. In this paper, we propose a SIP extension for guaranteeing security on the multiparty conference using SIP by adding new method and reconstructing header informations. With this, it is also possible to identify discovery and to distribute each participant using SIP extension when a call is established for closed multiparty conference.

키워드

SIP, Multiparty Conference, Signalling, Conference Server

1. 서 론

초고속통신망을 비롯한 네트워크 인프라가 완성되어가면서 네트워크는 광대역의 멀티미디어 망으로의 단계를 넘어서 이제는 유, 무선과 데이터망이 합쳐지는 통합망으로 발전하고 있다. 이와 같은 정보통신 기술의 발달로 인하여 커뮤니케이션 방식에도 많은 변화가 일어나고 있다.

현재의 VoIP(Voice over Internet Protocol) 서비

스가 제공하는 다자간 컨퍼런스(Multiparty Conference)는 편리한 사용자간의 커뮤니케이션 환경을 제공할 수 있으며 다양한 응용솔루션과 각종 부가 서비스 개발을 통해 발전 가능성이 매우 높은 서비스로 평가되고 있다. 또한 다자간 컨퍼런스는 최근 가장 주목받고 있는 서비스로서 차세대네트워크(NGN; Next Generation Network)의 핵심 어플리케이션으로 부상하고 있으며 그룹간의 회의서비스 수단으로서도 높은 활용도가 예상되고 있다.

이러한 서비스를 위한 표준 호 설정 프로토콜로서 H.323과 SIP가 사용되고 있다. 과거에는 주로 H.323을 기반으로 하는 다양한 서비스 개발이 이루어져 왔으나 최근에는 H.323의 단점을 보완하는 SIP가 여러 장점들을 제공함으로써 차세대 VoIP 표준 프로토콜로 자리 잡고 있다. 현재 IETF(Internet Engineering Task Force)에서는 SIP 기반의 서비스 개발과 표준화 작업을 통해 향후 높은 대역폭을 제공하는 고품질의 멀티파트 멀티미디어 서비스로 발전시킬 전망이다. 이를 위한 계속적인 작업이 진행 중이다.

현재 다자간 컨퍼런스를 위한 여러 표준화 작업들 중 다자간 컨퍼런스의 보안(Security)에 관한 표준화 작업은 신속히 해결해야 할 문제로서 다양한 논의가 진행 중이다. 특히, 다자간 컨퍼런스의 보안성 확보에 있어서 사용자의 정보를 획득하고, 이를 각 사용자들에게 분배하는 기능은 매우 중요한 부분으로 인식되고 있지만 현재 SIP는 다자간 컨퍼런스에서 사용자의 정보 획득과 분배를 위한 기능을 제공하지 않고 있다. 이것은 SIP를 기반으로 하는 비공개형(closed) 다자간 컨퍼런스에서는 큰 문제점으로 나타나고 있다.

본 논문은 차세대 VoIP 표준기술로서 주목받고 있는 SIP를 기반으로 하는 다자간 회의에서 SIP 확장을 통한 컨퍼런스 보안성 확보를 위한 메소드 설계와 헤더 구성 기법에 대해 연구하였다.

본 논문의 구성은 다음과 같다. II장에서는 관련 연구를 통해 현재 SIP의 특징과 SIP에서 사용되는 메시지들의 동작을 기술하였다. III장에서는 비공개형 다자간 컨퍼런스의 보안성 확보를 위한 SIP 확장과 구성을 소개하고, IV장에서는 SIP 확장의 동작과 성능 평가를 하였다. 마지막 V장에서 결론을 맺는다.

II. 관련연구

2.1 SIP 개요

SIP는 기존의 H.323에 대응되는 프로토콜로서 단말간 또는 사용자들간에 다양한 서비스의 호 설정(call signaling) 프로토콜로서 사용자간의 멀티미디어 세션에 대한 변경, 초기화 및 종료를 정의한 응용계층의 프로토콜이다. SIP는 H.323과 같이 여러 프로토콜들의 조합으로 VoIP 서비스를 한꺼번에 수행하는 프로토콜이 아니라 단순하게 세션 설정만을 다루는 프로토콜로서 간단하면서도 여러 다른 프로토콜들과 함께 사용될 수 있는 확장 가능한 프로토콜이다[1]. 현재 SIP는 여러 분야의 응용 서비스에서 시그널링 프로토콜로서 사용되고 있으며, 인터넷 텔레포니와 멀티미디어 응용 분야와 같은 다양하고 넓은 범위에서의 응용 서비스에 활용될 수 있도록 확장이 진행되고 있다. SIP는 SMTP(Simple Mail Transfer Protocol), E-Mail, HTTP(Hypertext Transfer Protocol) 기반으로 모델링 되었다. 이러한 기존의 텍스트 기반 인터넷

표준들에 따름으로서 고장 수리와 네트워크 디버깅 등이 쉽고 복잡한 구조의 호 설정을 간결히 함으로써 구현의 용이성과 서비스 추가의 편리성을 제공한다. 또한 사용자가 통신망에 접속하는 지점을 변경하거나 다른 단말기를 사용하여도 동일한 구별자(identifier)에 의하여 세션을 연결함으로써 사용자 이동성을 지원한다. SIP는 클라이언트들이 호출을 시작하면 서버가 그 호출에 응답을 하는 클라이언트/서버 구조에 기반을 두고 있으며 URL(Uniform Resource Location) 사용 방식을 이용하는 프로토콜이다. TCP, UDP, ATM 등의 하위 레벨의 트랜스포트 프로토콜과 독립적으로 동작하도록 설계되었다[2].

그림 1은 VoIP에서 사용되는 프로토콜들과 SIP의 위치를 보이고 있다.

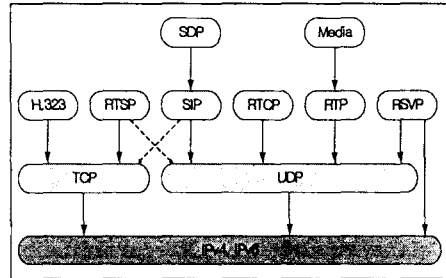


그림 4. Internet Telephony 프로토콜

2.2 SIP 메시지

SIP 메시지는 텍스트로 구성된다. 메시지는 헤더(header)와 메시지바디(message body)로 구성되며 헤더는 SIP 제어정보를 포함한다. 메시지 바디는 호 설정시 음성 및 비디오 코덱과 같은 양측의 능력을 조정하기 위한 정보를 포함하며 SDP(Session Description Protocol)로 기술된다. SIP 메시지 포맷은 start-line, message header, CRLF(Carriage Return Line Feed; 빈줄), message body로 구성되며, Request 메시지와 Response 메시지로 분류된다[2]. SIP 메시지의 종류와 포맷을 그림 2에서 보이고 있다.

SIP-message = Request | Response

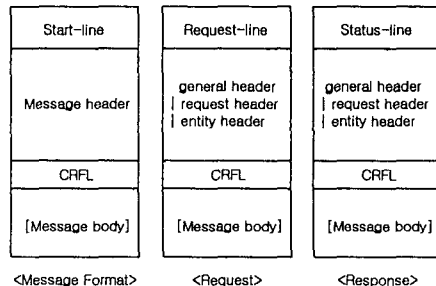


그림 5. SIP 메시지 종류 및 포맷

2.2.1 헤더 영역

- General Header : Request/Response 메시지에 모두 사용된다.
- Entity Header : 메시지의 기타 정보를 나타내거나 전송되는 데이터가 없을 때에는 Request 메시지에서 지정한 해당 자원에 대한 정보를 알려줄 때 사용된다.
- Request Header : 클라이언트의 추가적인 요청 정보를 나타낸다.
- Response Header : 서버의 추가적인 응답 정보를 나타낸다.

2.2.2 Request 메시지

현재 SIP 2.0에는 6가지의 메시지가 사용된다. 이것들은 메소드(method)로서 언급되며 그들의 기능에 따라 다음과 같이 분류된다.

- INVITE : UA들 간의 미디어 세션을 설립할 때 사용되며 항상 ACK 메소드에 의해 최종 확인된다.
- ACK : INVITE에 대한 최종 응답의 확인에 사용된다. 다른 모든 요청에 대해서는 확인 응답을 하지 않는다.
- BYE : 설립된 미디어 세션을 종료하기 위해서 UA가 BYE 메소드를 사용한다.
- CANCEL : 진행중인 요청을 취소하는데 사용되며 이미 완료된 경우에는 영향을 주지 않는다.
- OPTIONS : 통신 능력에 대한 정보를 요구하는데 사용되지만 연결 설정 시에는 관여하지 않는다.
- REGISTER : 사용자 위치에 대한 정보를 SIP 서버에게 전달한다.

그림 3에서는 SIP 메시지 형식을 보이고 있다.

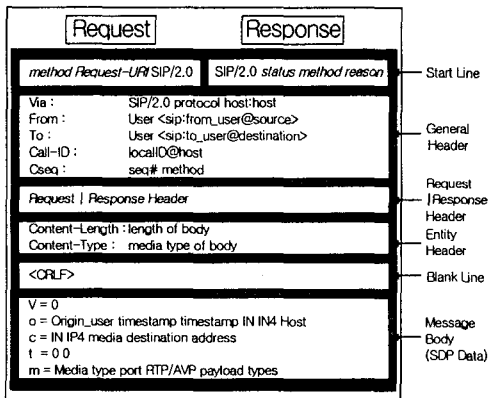


그림 6. SIP 메시지 형식

2.2.3 Response 메시지

SIP Response 메시지는 UAC의 요청에 대한 응답으로 UAS 또는 SIP 서버에 의해서 만들어지며 UAC가 필요한 정보를 포함하는 추가적인 헤더를 포함한다. 표 1에서 SIP Response의 코드들을 보여

주고 있다.

표 1. SIP Response Code

Response Code	의 미 s	상태
1XX	Informational Messages	Provisional
2XX	Success Responses	Final
3XX	Redirection Responses	Final
4XX	Client-Error Responses	Final
5XX	Server-Error Responses	Final
6XX	Global Failure Responses	Final

III. 비공개형 다자간 컨퍼런스를 위한 SIP 확장

비공개형 컨퍼런스에서 컨퍼런스 참가자들은 각 참가자들간의 사용자 정보를 통한 신원확보가 필요하다. 또한 새로운 사용자가 컨퍼런스에 참여하려 할 때 새로운 사용자의 세션이 설립되기 이전에 컨퍼런스 참가자들은 새로운 사용자의 신원을 알 수 있어야 한다. 그러나 현재 SIP에서는 이러한 참가자 발견을 지원하지 않는다.

본 논문에서의 SIP 확장을 위해 새로운 메소드 (INFORM method)와 헤더(Users Header)를 설계하였다. INFORM 메소드와 Users 헤더를 이용하여 사용자 정보의 획득과 분배가 가능하다.

INFORM 메소드는 컨퍼런스내에서 사용자 정보를 분배하는데 사용되며 Users 헤더를 포함하게 된다. Users 헤더는 모든 컨퍼런스 참가자들의 SIP 어드레스 정보와 각 참가자들의 컨퍼런스 참여상태를 파라미터로서 나타낼 수 있다.

3.1 INFORM 메소드

INFORM 메소드는 컨퍼런스내 사용자 정보를 각 컨퍼런스 참가자들에게 분배하며, 각 참가자들이 갖고 있는 컨퍼런스 참가자 리스트를 업데이트 하는데 사용된다. 기본적으로 request 메시지와 같은 메커니즘을 갖는다. INFORM 메소드는 보통 사용자가 컨퍼런스에 들어올때와 참가자가 컨퍼런스를 떠날 때 동작한다. INFORM 메소드는 컨퍼런스내에서만 동작이 허용된다. 그렇지 않을 경우 INFORM 메소드는 481(call leg or transaction doesn't exist) response로 응답된다. INFORM 메소드에 대한 정확한 수신 여부는 200(ok) response로 응답된다. INFORM 메소드는 각 사용자 정보와 상태 정보를 표시하는 Users 헤더를 통해 사용자 정보를 분배함으로써 각 참가자들은 컨퍼런스 참가자들의 정보를 획득할 수 있다. 이를 통해 비공개형 다자간 컨퍼런스에 필요한 보안성 확보가 가능하게 된다.

3.2 Users 헤더 필드

Users 헤더는 SIP에 사용되는 General Header에 추가된다. Users 헤더 구문(syntax)은 다음과 같다.

```
Users = "Users" ":" ( name-addr | addr-spec )
      [ *( ";" Users-parameter ) ]
```

각 참가자들의 상태 정보를 나타내는 Users 파라미터들은 아래와 같으며 선택적으로 사용될 수 있다. 기본값은 active로 설정된다.

```
Users-parameter = "status" "=" ( "active"
                                | "joining" | "departed"
                                | "failed" )
```

각 파라미터 값들은 다음과 같이 정의된다.

- active : 컨퍼런스에 참여하여 활동중이다.
- joining: invited 다음의 파라미터로서 INVITE request를 수신하고 컨퍼런스에 들어오고 있다.
- departed : BYE request를 전송하여 컨퍼런스를 떠나고 있다.
- failed : 사용자 정보 표시 오류를 뜻하며, failed 상태인 사용자는 다시 한번 사용자 정보가 조회된다.

각 참가자들이 이러한 Users 헤더를 수신하게 되면 헤더에 담겨있는 참가자 리스트와 참가자들이 가지고 있는 참가자 리스트를 비교하여 참가자 리스트를 업데이트 한다.

IV. SIP 확장은 동작 및 분석

확장한 SIP 메소드와 헤더필드를 컨퍼런스 서버가 존재하는 컨퍼런스 모델에 적용하여 동작과 분석을 하였다.

그림 4는 사용자 A와 B는 이미 세션이 설립되어 컨퍼런스 활동을 하고 있는 상태이다. 이때 새로운 사용자 C가 컨퍼런스에 참가하려 할 때의 INFORM 메소드의 동작이다.

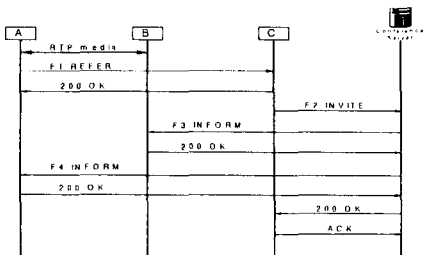


그림 7. INFORM 메소드의 동작

A와 B는 C가 컨퍼런스에 초대되었을 때 C의 호 설정이 완료되기 이전에 INFORM 메소드를 통해

서 C가 컨퍼런스에 들어오려 한다는 것을 알 수가 있다. 또한 사용자 C도 REFER 메소드에 포함된 Users 헤더 정보를 통해 현재 컨퍼런스에 A와 B가 활동중이라는 것을 알 수 있다. 그림 5와 그림 6에 Users 헤더와 INFORM 메소드의 형식을 보이고 있다.

```
F1 REFER A→C
REFER c@c_machine.example.com SIP/2.0
...
Users : <b@example.com>;status=active
...
```

그림 5. F1 Users 헤더를 포함한 REFER 메소드

```
F3 INFORM Conference Server→B
INFORM b@b_machine.example.com SIP/2.0
...
Users : <a@example.com>;status=active
      <c@example.com>;status=joining
...
```

그림 6. F3 Users 헤더를 포함한 INFORM 메소드

V. 결론

본 논문에서는 사용자 정보 획득과 분배를 위한 SIP 확장을 설계하였다. 확장을 통한 INFORM 메소드와 Users 헤더를 이용하여 비공개형 다자간 컨퍼런스에서 사용자의 정보 획득과 분배가 가능하게 하였다. 새로운 사용자가 컨퍼런스에 들어오기 이전에 컨퍼런스 참가자들은 새로운 사용자의 사용자 정보를 획득할 수 있다. 확장된 SIP INFORM 메소드와 Users 헤더를 이용하여 비공개형 다자간 컨퍼런스에 필요한 컨퍼런스 보안성 확보에 도움을 줄 수 있게 하였다. 별도의 프로토콜을 추가하지 않고, 사용자의 정보 획득과 분배가 가능하기 때문에 프로토콜 추가의 부담을 줄일 수 있으며, 이에 따라 SIP만을 이용한 빠른 호 설정 서비스를 제공해 줄 수 있다.

결과적으로 SIP 확장을 이용하여 효과적인 사용자 정보획득을 제공함으로써 컨퍼런스 보안성 확보를 위한 효율적인 방법으로 이용될 수 있을 것이다.

참고 문헌

- [1] J. Rosenberg, H. Schulzrinne. "Guidelines for Authors of SIP Extensions", IETF Internet Draft, work in progress, 2002
- [2] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg. "SIP : Session Initiation Protocol", IETF RFC 3261, June. 2002.