제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

인증기능을 갖춘 SIP기반의 화상회의 시스템 구현

조현규° 김영학 장춘서
금오공과대학교 컴퓨터공학과
{blackjo° yhkim}@cespc1.kumoh.ac.kr, csjang@kumoh.ac.kr

Implementation of SIP based Video Conference System with Authentication Module

Hyun Gyu Jo° Young Hak Kim Choon Seo Jang
Dept. of Computer Enginnering, Kumoh National Institute of Technology

요 약

SIP(Session Initiation Protocol)는 기존의 VoIP(Voice over IP)를 위한 시스템에서 뿐만 아니라 호설정의 처리와 제어가 필요한 여러 인터넷 응용분야에 적용이 가능한 확장성이 뛰어난 프로토콜이다. 또한 HTTP(Hyper Text Transfer Protocol)와 유사한 텍스트 기반의 응용계층의 프로토콜로서 호처리시 절차가 비교적 간결하다. 본 논문에서는 이러한 SIP의 장점을 이용하여 화상회의를 위한 시스템을 구현하였다. 이때, 인증 기능을 부여하여 화상회의시 세션 연결을 위한 호설정을 이루는 과정에서 상대방을 인증할 수 있도록 하였고 인증방법으로는 메시지 인증기능과 함께 리플레이 공격(replay attack)의 방지기능을 가진 SIP 다이제스트 인증(Digest Authentication) 방법을 사용하였다. 본 화상회의 시스템에 사용된 SIP 사양은 최근에 발표된 RFC 3261을 기준으로 하였다.

1. 서론

IETF(Internet Engineering Task Force)에서 호설정을 위해 제안하고 표준화한 SIP는 ITU-T의 H.323에 대응하는 프로토콜로서 기능적인 측면에서는 유사하지만, SIP는 내용이 비교적 간단하여 구현이 쉽고 호설정의 처리과정이 간결하다는 장점을 가지고 있다[1]. 또한 근거리 통신망에서 멀티미디아 통신을 지원하기 위해 만들어진 H.323은 복잡한 구조로 인해 프로토콜의 확장이나 새로운 기능을 추가하는데 많은 제약이 있다. 반면 SIP는 텍스트 형태로 이루어진 메시지의 헤더필드를 추가함으로써 유연하게 확장이 가능하고, 처음부터 인터넷환경을 기준으로 만들어져 다양한 인터넷 응용서비스의 호설정에 사용과 접목이 쉽다[2].

본 논문에서는 SIP의 이와 같은 장점을 이용하여 회상회의 시스템에서 상대방과의 호설정이 SIP 메시지를 통해 이루어지도록 하였다. 이때, SIP 다이제스트 인증기능을 제공하여 보안 기능을 높였다. 호설정을 이루는 SIP의 동작은 가장 최근 발표된 RFC 3261 문서에 기반하여 구현하였다. 본 논문의 구성은 다음과 같다. 2장에서 SIP의 구성과 인증에 관해 언급하고 3장에서는 구현된 시스템의 전체적인 내용을 다루며 4장에서 결론을 맺는다.

2. SIP 구성 및 인증

2-1. SIP 구성

SIP는 하나 이상의 참가자간에 인터넷 텔레폰 콜, 멀티미디어 컨퍼런스 등의 세션을 생성, 변경, 종료하는 호설정을 위한 응용계층의 시그널링 프로토콜로서 HTTP처럼 텍스트 기반의 메시지를 통해 호처리를 하는 비교적 간결한 프로토콜이다[3]. 따라서 호설정에 사용되는 다른 프로토콜에 비해 구현이 쉬울 뿐만 아니라 뛰어난 확장성을 가지고 있어 호설정을 필요로 하는 여러 응용분야에 적용이 가능하다.

SIP는 요청과 응답메시지를 서로 교환하는 과정을 통하여 호설정을 처리한다. 요청메시지는 INVITE, ACK, BYE, CANCEL, OPTIONS 및 REGISTER와 같은 메소드를 사용하고 응답메시지는 HTTP의 경우와 유사하게 3자리 숫자로 된 상태

코드를 사용하며 여기에는 100, 200, 300, 400, 500, 600 클래스가 있다. 메시지의 바디 부분에는 SDP(Session Description Protocol)를 포함시켜 멀티미디아 데이터 전송에 필요한 정보를 지원한다[4]. SIP는 클라이언트/서버 구조로 동작하며 이에 대응하는 구성요소는 UAS(User Agent Server)와 UAC(User Agent Client)로 구분되는 UA(User Agent)와 프록시(Proxy) 서버, 리다이렉트(Redirect) 서버, 로케이션(Location) 서버, 레지스트라(Registrar)로 분류되는 네트웍 서버가 있다[5].

2-2. SIP 인증

새로운 SIP 표준문서인 RFC 3261 에서는 기존의 SIP 표준문서와는 달리 SIP 인증방법으로 RFC 2617에 정의되어 있는 HTTP 다이제스트 인증만을 사용하도록 하고 있다[6]. 다이제스트 인증에서는 요구-응답 인증 메커니즘(Challenge-Response Authentication Mechanism)을 사용한다. 사용자 이름과 비밀번호가 아무런 암호화 과정 없이 텍스트 형태로 전달되어 쉽게 노출되는 기본인증과는 달리 다이제스트 인증은 비밀번호를 포함한 인증에 필요한 정보들을 암호화시켜 수행하여 기본인증의 단점을 보완한다[7]. 그림 1은 다이제스트 인증의 일반적인 처리방식이다.

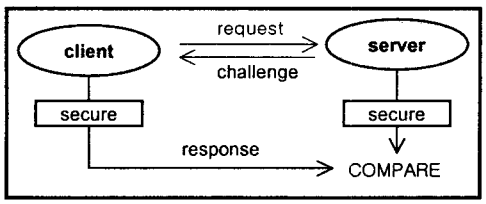

그림 1: 다이제스트 인증 처리

SIP에서는 두 가지 형태의 인증을 가지고 있는데 리다이렉트 서버, 레지스트라, UA간의 인증에 필요한 User-to-User 인증과 프록시 서버와 UA간의 인증에 사용되는 Proxy-to-User 인증이다. SIP에서는 인증에 필요한 내용들을 요청과 응답메시지의 일부분으로 포함시켜 송수신 한다.

인증을 위한 절차는 다음과 같다. 먼저 UA가 인증을 위한 헤더필드를 포함하지 않고 호설정을 시도하거나 사용자 등록을 요구하는 SIP 요청메시지를 보내게 되면 서버는 인증에 필요한 nonce값 등의 정보를 응답메시지 내에 포함하여 인증을 요구한다. 인증요구를 받은 UA는 서버가 요구하는 사항에 맞추어 서명과 함께 새로운 요청메시지를 다시 생성하여 재요청을 시도한다. 이러한 역할을 위해 두 가지 형태의 인증에서 사용하는 메시지와 포함되는 헤더필드는 다음과 같다. User-to-User 인증은 WWW-Authenticate 헤더필드를 포함한 401(Unauthorized) 응답메시지로 서버가 인증을 요구하며 UA는 Authorization 헤더필더를 포함하는 요청메시지를 생성한다. Proxy-to-User 인증은 Proxy-Authenticate 헤더필더를 포함하는 407(Proxy Authorization Required) 응답메시지와 Proxy-Authorization 헤더필드를 포함하는 요청메시지를 사용한다[8].

그림 2와 그림 3은 두 가지 인증형태 중에서 프록시 서버와 UA간에 인증요구와 응답에서 생성되는 헤더필드의 예이다.

```
Proxy-Authenticate: Digest
  realm="sip2.kumoh.ac.kr",
  qop="auth",
  nonce="74edc353752b14dfa58e5ed0dcd61e55",
  opaque=""
```

그림 2: Proxy-Authenticate 헤더필드

```
Proxy-Authorization: Digest username="johg",
  realm="sip2.kumoh.ac.kr",
  nonce="74edc353752b14dfa58e5ed0dcd61e55",
  opaque="",
  uri="sip:kmh@sip1.kumoh.ac.kr",
  response="c0c784a9e6ba4459014efd2967f3faf1"
```

그림 3: Proxy-Authorization 헤더필드

여기서, realm은 인증을 위한 서버상의 관리영역을 의미하고 nonce는 리플레이 공격을 방지하기 위한 타임스탬프이다. qop는 quality-of-protection의 의미로 값이 auth일 경우에는 단지 인증만을 수행하고 만약 int-auth가 부여되면 인증과 함께 무결성도 같이 체크되어야 한다. 서버에 의해서 opaque 파라미터의 값이 기술되어져 인증요구가 되면 UA는 재요청시 동일한 값을 포함하여야 한다. algorithm 파라미터는 생략시 기본적으로 MD5 알고리즘을 사용하는 것으로 간주한다. uri는 Request-URI 값이고 response는 사용자 이름과 비밀번호 등 인증에 필요

한 값들을 포함하여 MD5 해시값으로 인코딩한 값이다. 그림 4는 Proxy-to-User 인증을 요구하는 두 개의 프록시 서버를 거쳐 UA간에 호설정을 이루는 과정의 흐름의 예를 나타낸다.

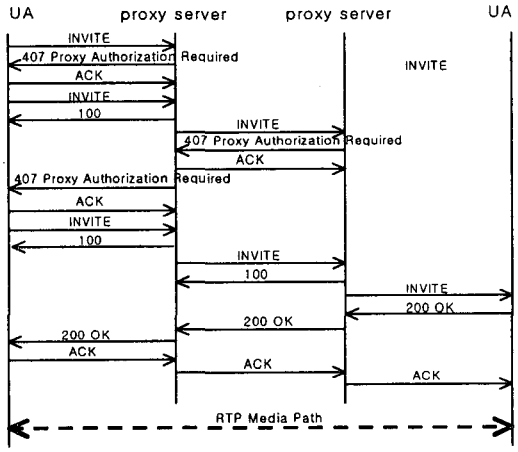

그림 4: Proxy-to-User 인증 예

3. 시스템 구현

본 구현에서는 각 사용자가 사용할 화상회의 소프트웨어에 SIP UA를 포함시켰고 각 사용자간의 호설정을 위한 SIP 메시지 전달을 위해 SIP 프록시 서버를 구성하였다. 또한 로케이션 서비스(location service)와 사용자 등록(registration) 부분을 프록시 서버에 포함시켜 linux OS상에서 운영하였다.

구현된 시스템에서 UA의 역할은 사용자가 회의에 참여하기 위해 호설정에 필요한 요청메시지를 생성하고 전송하며 받은 메시지를 파싱하고 처리하여 응답 메시지를 생성 및 전송하는것이다. 이때, 송수신되는 메시지의 바디부분은 SDP를 사용하여 화상 스트림 데이터 전송에 필요한 각종 세션정보를 상대방과 협상할 수 있도록 하였다. 이 세션정보에는 화상데이터의 송수신에 필요한 포트번호 및 코덱종류 등이 포함된다. 프록시 서버는 UA로부터 받은 메시지를 파싱하여 처리하거나 포워딩을 한다. 또한, 호처리 과정에서 User-to-User 인증과 Proxy-to-User 인증의 두 가지 형태를 모두 구현하여 시스템에 포함시켰다. 이를 위해 레지스트라를 포함한 프록시 서버에는 "User_to_User_AUTH" 플래그와 "Proxy_to_User_AUTH" 플래그를 내부적으로 두었다. UA간에 인증처리에 있어서는 화상회의 사용자 인터페이스 화면에서 "Authentication Active" 체크버튼을 이용하여 내부 플래그를 세팅하도록 하여 필요시에만 인증기능을 사용할 수 있도록 구현하였다.

본 시스템에서 제공하는 인증기능 중에서 프록시 서버와 UA간에 필요한 인증절차는 다음과 같다. 먼저 UA가 호설정을 개시하기 위한 INVITE 요청메시지를 프록시 서버에게 전달한다. 서버는 메시지를 포워딩 하기 전에 인증에 필요한 realm, nonce, qop, opaque 파라미터를 포함하는 헤더필드를 생성하여 407 응답메시지를 통해 UA에게 인증을 요구하게 된다. 이를 받은 UAS는 그림 5와 같은 사용자 인터페이스를 메인화면과 독립적인 팝업창으로 모니터 화면에 띄우고 사용자는 아이디와 패스워드를 입력한다. 이때, UA의 내부적으로는 서버로 부터 받은 407 응답메시지에 기술된 nonce, realm 값과 요청메시지의 메소드, uri값 및 서명에 사용된 아이디와 패스워드를 MD5 모듈을 통과시켜 response 값을 구하고 Proxy-Authorization 헤더필드에 부여하여 재 INVITE 요청을 시도한다. 재요청을 받은 프록시 서버는 요청메시지를 검사하여 서명된 내용이 서버가 요구한 인증요구 내용과 일치하면 INVITE 요청처리를 계속 진행시킨다. 만약 서명된 내용이 요구한 내용과 일치하지 않으면 서버는 다시 인증을 요구하게 된다. 재 인증을 요구할 때는 새로운 nonce 값을 생성하여 보내며 UA는 이에 맞추어 재 인증을 시도한다.

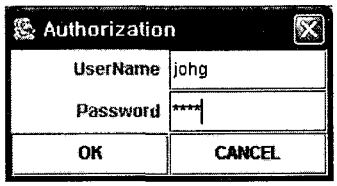

그림 5: 인증을 위한 사용자 인터페이스

본 구현에서는 인증요구를 위한 헤더필드 가운데 algorithm과 stale 파라미터는 생략하였고 기본적으로 MD5와 false값을 가지는 것으로 간주하였다.

프록시 서버에 포함된 레지스트라에게 UA가 REGISTER 요청메시지를 보내는 경우와 UA가 다른 UA에게 호설정을 요구하는 요청메시지를 보내는 경우의 인증은 서버가 WWW-Authenticate 헤더 필드를 포함한 401 응답메시지로 인증을 요구하며 UA는 Authorization 헤더필드를 요청메시지에 포함하여 재요청을 한다. 여기서, 내부적으로 포함하는 파라미터나 생성방법 등은 프록시 서버와 UA간에 처리하는 인증방법과 동일하다. 단, REGISTER 요청메시지에 대한 인증이 되면 서버는 200 OK 메시지

로 응답하고 UA간의 인증이 완료되면 호설정에 필요한 나머지 절차가 계속 진행이 된다.

그림 6은 구현된 시스템 가운데 인증기능을 포함한 메시지의 파싱 및 처리, 포워딩 기능을 하는 프록시 서버의 기능 흐름도를 간략하게 나타낸다.

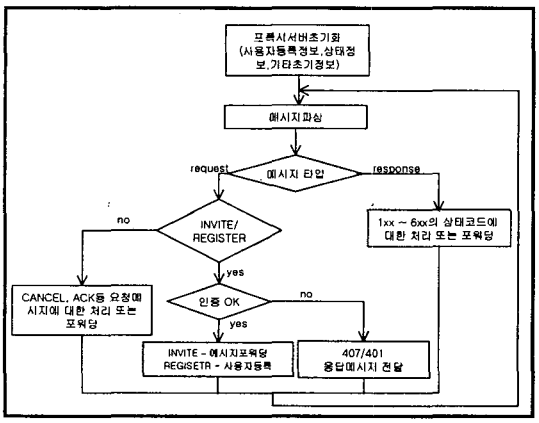

그림 6: 인증기능을 포함한
프록시 서버의 기능 흐름도

그림 7은 구현된 시스템에서 UA간에 호설정을 위한 과정에서 프록시 서버가 인증을 요구할 경우 이에 맞추어 UA가 인증내용을 포함한 INVITE 메시지를 새로 생성하고 서버에게 전송하는 실제 메시지 내용이다.

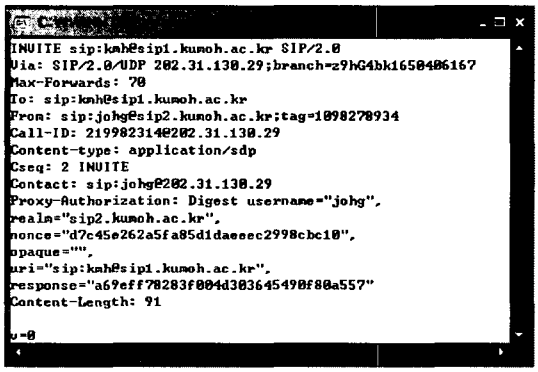

그림 7: 인증을 위한 재요청메시지

그림 8은 인증절차를 포함한 호설정이 이루진 후 화상회의 시스템에서 실제 화상을 송수신하는 화면을 보였으며 화상 스트림 전송에는 RTP(Real-time Transfer Protocol)를 사용하였다.

그림 8: 구현된 시스템 상에서의 화상회의 화면

4. 결론

본 논문에서는 인터넷 상에서 화상회의를 위한 시스템을 최근에 발표된 RFC 3261을 기준으로 SIP를 기반으로 하여 구현하였다. 또한 사용자 사이의 호설정을 처리하는 과정에서 메시지 인증기능과 함께 리플레이 공격방지 기능을 가진 인증 메커니즘으로 SIP 다이제스트 인증방식을 사용하여 보안기능을 강화하였다. SIP 인증은 User-to-User 인증과 Proxy-to-User 인증방법을 모두 구현하여 상황에 맞추어 선택해서 적용할 수 있도록 하였다. 회의를 위한 화상 스트림 전송에는 RTP 프로토콜을 사용하였으며 SIP 메시지의 바디부분에는 SDP를 기술하여 화상 스트림 데이터 전송에 필요한 각종 세션 정보를 상대방과 협상할 수 있도록 하였다.

5. 참고문헌

[1] H. Schulzrinne and J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony," NOSSDAV, July 1998.

[2] Stephen R. Jones, "Session Initiation Protocol", MITRE Technical Papers, Feb. 2001

[3] Session Initiation Protocol, RFC 3261

[4] Session Description Protocol, RFC 2327

[5] H. Schulzrinne, J. Rosenberg, "The Session Initiation Protocol: Internet-Centric Signaling", IEEE Communications Magazine, Vol.38, Oct 2000.

[6]Jonathan Rosenberg, "SIP security Mechanisms Update", dynamicsoft presentation, 05, 2002.

[7] HTTP Authentication: Basic and Digest Access Authentication, RFC 2617

[8] Aki Niemi, "Authentication of SIP calls", Tik-110.501 Seminar on Network Security, Helsinki University of Technology, 2000