VOIP 서비스의 사용자 인증 기법

(User Authentication Technique for VoIP Service)

진 현 철 † 김 정 미 †
(Hyeon-Cheol Zin) (Jeong Mi Kim)

김 종 근 ††
(Chonggun Kim)

요 약 IP기반의 패킷망을 통해 음성 데이터를 전송하는 기술인 VoIP 기술은 PSTN 기반의 통신 방식과 달리 음성 데이터 뿐만 아니라 텍스트 데이터, 이미지 데이터, 멀티미디어 데이터 등도 전송할 수 있으므로 서비스 통합화, 비용절감 등의 장점을 가지고 있다. 또한, VoIP 단말기는 인터넷이 연결된 곳에서는 어디든 통신이 가능하므로 모바일 단말기와 유사한 이동성을 제공한다. 따라서, 부정사용자를 방지하기 위한 인증 서비스를 제공하는 것은 필수적이다. 본 논문에서는 VoIP 사용 환경에서 사용자 인증의 신뢰를 높이는 서비스 방안을 제안한다.

키워드 : VoIP, SIP, MVoIP, 인증시스템

Abstract VoIP technology for transmitting voice over IP network such as packet-based network has a lot of benefits by integrating services and reducing costs. The network is different from PSTN-based communications in some aspect such as transmitting not only voice but also text, image, multimedia data. In addition, portable terminals like a mobile phone, and ubiquitous communicator can easily access the internet for VoIP. Therefore, To prevent illegal users, offering certificate services is necessary. This study proposes a solution of user certification for a VoIP environment.

Key words : VoIP, SIP, MVoIP, Authentic Systems

· 이 논문은 중소기업청 산학협력연구소과제 지원으로 연구된 논문입니다.
· 이 논문은 2008 학술심포지움에서 'VoIP 서비스 사용자 인증 기법 연구'의 제목으로 발표된 논문을 확장한 것임

† 비 회 원 : 영남대학교 컴퓨터공학과
cyberzin@ynu.ac.kr
tkvkdldj@ynu.ac.kr
†† 종신회원 : 영남대학교 컴퓨터공학과 교수
cgkim@yu.ac.kr

논문접수 : 2009년 3월 13일
심사완료 : 2009년 6월 3일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제15권 제8호(2009.8)

1. 서 론

IP기반의 패킷망인 인터넷을 통해 음성을 전송할 수 있는 VoIP(Voice Over IP)기술을 이용하면 별도의 PSTN(Public Switched Telephone Network)을 사용할 필요가 없으므로 비용이 절감될 뿐만 아니라 음성 데이터 이외에도 텍스트 데이터, 이미지 데이터, 멀티미디어 데이터 전송 등이 가능하므로 통합 메시징 시스템을 비롯한 각종 부가서비스를 제공할 수 있는 시스템 구축이 가능하다.

비용절감, 효율적인 회선이용, 회선통합 등의 장점에도 불구하고 VoIP가 PSTN을 대체하기 위해서 해결해야 하는 여러 가지 문제점 중의 하나는 바로 보안과 관련된 문제이다. VoIP는 기존의 PSTN과 달리 개방형 네트워크인 인터넷을 사용하기 때문에 도청, 감청, 부정사용자 등의 보안상 취약 요소를 가지고 있다. 또, PSTN 단말기가 회선에 종속된 반면 VoIP 단말기는 이동성을 제공하므로 사용자 인증, 과금 등의 문제가 대두된다. 따라서 이용자의 안전한 통신을 위해 도청 및 감청 방지, 불법 사용자 차단 등의 보안문제 해결이 선결되어야 할 것이다.

본 논문은 총 5장으로 구성되어 있다. 2장에서는 관련 연구에 대해 논의하고 3장에서는 사용자 인증 시스템을 제안한다. 4장에서는 제안 시스템의 기대효과를 살펴보고 5장에서는 결론과 향후 연구에 대해 검토한다.

2. 관련연구

2.1 SIP(Session Initiation Protocol)[1)]

SIP는 사용자간 멀티미디어 세션의 개시, 변경, 폐지를 정의하는데 사용되는 어플리케이션 계층의 시그널링 프로토콜로 사용자에이전트(User Agent)와 SIP 서버로 구성된다.

• SIP UA(User Agent)

SIP 메시지를 생성하는 요청사용자(UAC; User Agent Client)와 수신된 요청 메시지에 응답하는 응답사용자(UAS; User Agent Server)로 구성된 사용자 측면 응용 프로그램이다.

• 프락시 서버(Proxy Server)

프락시 서버는 UAC의 SIP 호 요청에 대해 UAS의 최종 위치를 등록서버나 DNS를 통해 해당 정보를 요청하고 다음 SIP 서버로 SIP호 요청 정보를 전달한다. SIP 요청을 하지 않고 단순히 UA로부터 요청에 대한 응답 또는 포워딩만 수행한다.

• 재지정 서버(Redirect Server)

재지정 서버는 UA로부터 요청에 응답하지만 메시지를 포워딩 할 수 없기 때문에 UAS의 최종위치를 SIP 호 연결을 요청한 UAC로 보낸다. 즉 수신한 메시지가 전달되어야 할 새로운 노드 주소를 알려 준다.

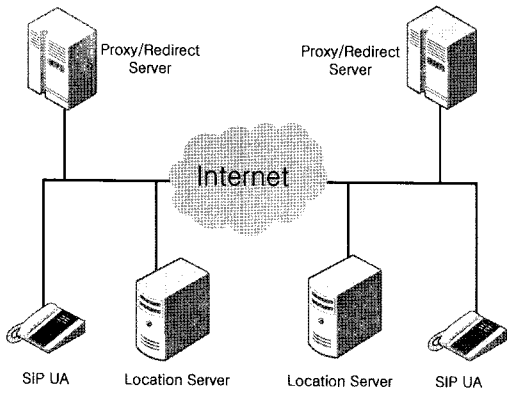

그림 1 SIP 구성도

• 위치 서버(Location Server)

위치 서버는 한 도메인 내 속하는 사용자의 위치를 기록하여 알려준다.

• 등록 서버(Registrar Server)

등록 서버는 e-mail 형태의 SIP 주소로 구분된 사용자 정보를 관리한다. 등록 서버는 각 SIP 주소에 대하여 현재 사용자의 위치 정보(IP 주소)를 우선 순위 정보와 함께 지정된 시간만큼 저장, 관리하며, 인증과정을 통해 인증된 사용자의 요구에 따라 사용자 정보를 제공해 준다. VoIP 단말기 간 음성 통신을 위해 SIP를 사용하여 사용자간 세션을 설정하고 종료하는 절차를 그림 2에서 보이고 있다.

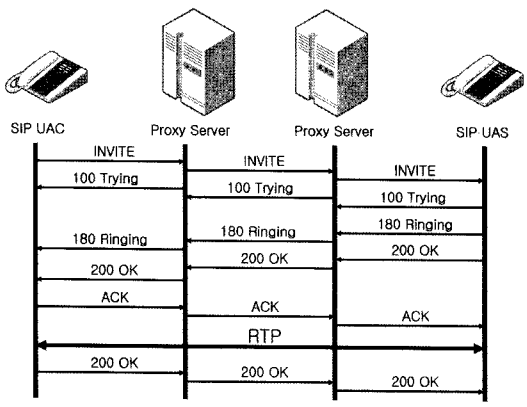

그림 2 세션 설정 및 종료

UAC가 UAS를 목적지로 하는 INVITE 메시지를 생성하여 전송하면 UAC가 속한 프락시 서버는 UAS가 위치한 프락시 서버로 INVITE 메시지를 포워딩한다. 그런 다음 100 Trying 메시지를 전송하여 포워딩 사실을 UAC에게 알려준다.

UAS가 속한 프락시 서버는 위치 서버를 통해 UAS의 위치를 확인하고 수신된 INVITE 메시지를 UAS에 전달한다. UAS는 200 OK 메시지를 전송하여 수신을 확인 해주고, 200 OK 메시지를 받은 UAC는 ACK를 UAS에 보냄으로써 세션을 연결하고 데이터를 송수신한다. 세션의 종료는 어느 한 쪽이 BYE 메시지를 보내고, 그에 대한 응답으로 200 OK 메시지를 수신함으로써 이루어진다.

2.2 SIP 보안기술

SIP에서는 기존에 사용하고 있는 보안 메커니즘을 보안 기준 모델로 제시하고 있다. 복잡성을 최소화하기 위해 새로운 기반구조나 알고리즘 확장을 가급적 사용하지 않는다.

표 1 SIP 정보보호 기술

구분	기술요약	기능
HTTP 인증	· Digest인증만 사용하며, 재사용 공격방지와 인증기능 제공	사용자인증
TLS	· SIP메시지에 대한 암복호화를 통해 신뢰구간 형성 · TCP기반 SIP에만 적용가능	홉간 보안
S/MIME	· 종단간 SIP사용자에게 보안기능 제공 · 메시지에 대한 기밀성, 무결성, 상호 인증 기능 제공	양단간보안

SIP 기반의 VoIP 환경에서는 사용자 인증을 위해 HTTP 다이제스트 인증기법, S/MIME, TLS를 이용한다. TLS는 각 홉간 보안을 위해 선택적으로 적용하고 S/MIME은 UAC와 UAS 양단 간의 보안을 위해 선택적으로 적용한다.

2.3 HTTP Digest 사용자 인증

Digest 인증은 HTTP 기본 인증이 사용자 이름과 패스워드를 암호화하지 않고 전송하는 문제점을 보완하기 위해 만들어진 메커니즘으로 사용자 인증을 위해 사용자와 프락시 서버 사이에 사전에 공유하고 있는 패스워드와 임의의 값을 해시 함수 기반의 MD5나 SHA-1 Digest를 전송한다. 그림 3은 Digest 인증의 동작과정을 보여주고 있다.

이러한 Digest인증을 사용자에이전트 - 등록서버, 사용자에이전트 - 프락시서버, 사용자에이전트 - 재지정서버 간의 사용자 인증을 위한 SIP 보안에 적용한다. 인증 방법은 시도-응답(challenge-response) 형태로 UAC에서 request 메시지를 보내면 각 서버에서 시도(challenge)메시지에 랜덤정보와 realm 정보를 보내주게 되고

이를 받은 UAC에서 서버로부터 받은 정보와 자신의 정보를 사용하여 생성된 인증정보를 각 서버에 응답(response)으로 보낸다.

각 서버는 UA로부터 받은 정보와 자신이 가진 UA정보를 가지고 생성된 값을 비교하여 같은 값이면 UA를 인증한다. 이러한 Digest 사용자 인증은 INVITE, ACK, BYE 메시지 등에도 적용되어 SIP VoIP시스템에서 세션 연결 시에도 정당한 사용자 여부를 확인할 수 있다.[2] HTTP 인증은 SIP단말, 프락시 서버, 등록 서버에서 구현되어야 한다. SIP에서 발신자를 인증하기 위한 기법으로 DKIM(Domain Keys Identified Mail)[3]이나 SPF (Sender Policy Frame work)[4] 기법이 있다.

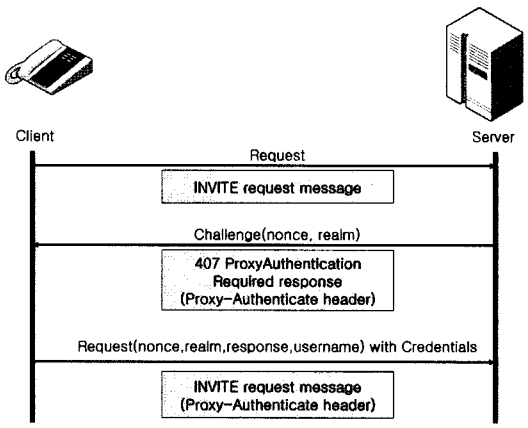

그림 3 Digest 인증

2.4 홉간(Hop by Hop) 보안

SIP의 UA - 등록 서버, UA - 프락시 서버, 프락시 서버 - 프락시 서버, 프락시 서버 - UA 간에는 TLS(Transport Layer Security), IPSec 등의 홉간 보안 기법이 적용된다. Hop간 보안은 보안 채널을 통해 SIP메시지를 전달하므로 기밀성과 무결성을 제공하며 사용자간 인증은 인증서를 통해 제공한다.[5]

2.5 양단간(End to End) 보안

양단(End to End) 채널인 UA - UA에는 S/MIME 적용하고 있다. S/MIME은 기존 MIME를 확장하여 제안된 것으로 양단간의 메시지에 대한 기밀성과 무결성, 인증서를 통한 상호간 인증을 제공한다. SIP에서는 SDP 암호화 모드, SIP 전체 메시지 서명 모드, SIP 전체 메시지 암호 및 서명 모드로 구분된다.

2.6 단말의 보안

기존의 PSTN에 접속하여 사용하는 단말기는 물리적인 회선을 연결하는 작업이 필요하며 단말에 대한 회선 이동이 임의로 이루어 질 수 없었다. 반면 VoIP 단말은 IP망이 설치된 곳이라면 어디서든 통신이 가능하므로 모바일 단말기와 유사한 이동성을 가진다. 뿐만 아니라 시스템 설정 정보를 자동적으로 다운로드할 수 있으므로 이용 권한이 없는 단말의 접속을 방지할 수 있는 인증이 요구 된다.

3. 사용자인증시스템

본 논문에서는 허가되지 않은 사용자가 네트워크에 참여하여 통신하는 것을 방지하기 위해 정상적인 사용자임을 인증하는 시스템을 제안한다. 이를 위해 기존의 VoIP 통신 시스템에 인증 서버를 추가하여 VoIP 단말에 대한 인증을 수행한다. 그림 4에서 보는 바와 같이 단말간 통신을 수행할 때 인증 서버(Authentic Server)를 사용함으로써 부정사용자의 네트워크 사용을 한 참여를 방지하고 도청 및 감청을 예방할 수 있다.

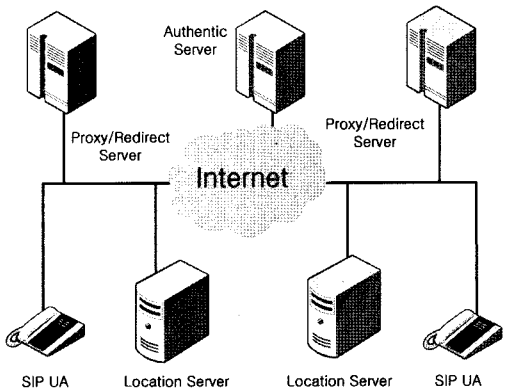

그림 4 제안시스템의 구조

그림 4에 나타낸 것처럼 시스템에 참여하는 프락시 서버는 인증 서버에 연결되어 있고 인증서버는 프락시 서버를 통해 연결된 각 UA의 인증을 수행한다. 제안된 시스템구조에서 인증 은 크게 두 가지로 구분된다. 첫 번째 각 서버간의 인증이며 두 번째는 사용자 단말과 서버 사이의 인증이다. 서버간의 인증 절차는 불법적인 사용자나 해커가 서버에 접근하여 정보를 유출하거나 불법적인 통신이 가능하도록 서버 정보를 조작하는 것을 예방하기 위해 필요한 절차이다. 사용자 단말과 서버간의 인증은 복제된 단말기에 의한 불법적인 통신을 예방하기 위한 것이다. 두 가지 인증 모두 HTTP Digest 인증을 사용하며 인증을 수행하는 절차는 아래와 같다.

1. UA가 다른 UA와 연결을 시도하기 위해 INVITE 메시지를 보낸다. 이 때 연결을 시도하는 UA에 연결된 프락시 서버는 INVITE 메시지에 자신의 주소를 추가하고 인증서버의 공개키로 암호화하여 전송한다.

2. INVITE 메시지를 받은 UA가 연결된 프락시 서버는 인증 서버에 인증서 검증을 요청한다.
3. 인증 서버는 요청받은 인증서에 대해 검증하고 이상이 없는 경우 사용자 정보를 INVITE 메시지를 받은 UA의 프락시 서버로 전송한다.
4. INVITE 메시지를 받은 프락시 서버는 UA에게 INVITE 메시지를 전송하여 RTP세션을 열어서 통신을 시작한다.

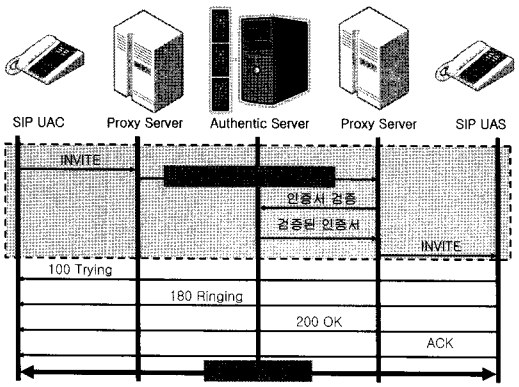

그림 5 제안시스템의 서비스 흐름도

그림 5는 제안 시스템의 서비스 흐름도를 나타낸 것이다. 암호화된 INVITE를 상대편 프락시 서버에 전달하고 INVITE 검증을 통해 인증을 수행한다. 인증이 완료되면 RTP를 통해 통신을 수행하게 된다.

4. 제안 시스템의 분석 및 기대효과

제안 시스템은 VoIP 단말에 대한 통합적 인증을 수행하는 단일 인증 서버를 사용하여 통신망에 접속된 사용자가 정상적인 사용자인지 판별하는 시스템이다. 기존의 인증 시스템이 통신 서비스 제공자별로 독자적인 인증 서버를 사용하므로 인증 서버 상호간 추가적인 상호 인증이 필요한 반면 제안된 시스템은 단일 공인 인증 서버를 사용함으로써 인증 서버간 인증 절차가 필요 없고 설치 및 유지비용이 절감된다. 뿐만 아니라 공인된 단일 인증 서버가 서로 다른 통신망(통신서비스 제공자) 사이의 인증이 용이해 지므로 통신 서비스 제공자와 사용자간의 과금이나 부가서비스 이용에 대한 분쟁이 일어날 소지가 적다.

표 2는 다수 인증 서버와 단일 인증 서버를 비교한 것이다. 제안된 시스템의 단일 인증 서버는 국가 또는 통신망에 참여하는 통신 서비스 제공자가 공동으로 소유 관리하며 개별 통신 서비스 제공자는 외부망과 통신할 때 공인 인증 서버를 통해 인증을 받게 된다. 개별

표 2 단일 인증서버와 다수 인증서버의 비교

	단일 인증서버	다수 인증서버
서버 위치	1	다수
서버 소유권	공동 또는 공인기관	개별통신사
서버간 인증	불필요	필요
서버 유지비	저렴	고가
인증 절차	간단	복잡

통신 서비스 제공자는 공인 인증 서버의 인증을 받으면 어떤 통신 서비스 사업자와도 별도의 인증 절차 없이 통신이 가능하다. 반면, 통신사별 인증 서버를 사용하면 통신 서비스 제공자들의 인증 서버 사이의 별도의 인증 절차가 요구된다. 따라서 공인인증서버의 사용은 인증 절차의 간편성, 서버 유지 비용 절감, 통신 투명성 보장 등이 가능하다.

5. 결론 및 향후 연구

본 논문은 SIP를 기반 VoIP 서비스에서 부정 사용자를 방지하기 위한 단말 인증시스템을 제안하였다. 개방된 인터넷망을 통한 VoIP 서비스는 그 특성상 모바일 단말과 이동성을 가진다. 따라서 복제 단말기나 부정사용자의 단말에 대한 인증은 필수적으로 요구된다. 인증 시스템이 제공되지 않으면 사용자의 불안감이 증가할 수 있다. 제안 시스템을 사용하여 이러한 불안감이 해소된다면 사용자 수가 확대될 것이다. 하나의 인증 서버 도입에 따른 장단점 분석 및 성능의 평가 구현에 따르는 문제 분석 등의 연구가 추후 계속되어야 한다.

제안된 인증 방법은 VoIP 서비스를 모바일로 확장한 MVoIP(Mobile VoIP)의 활성화에 많은 기여를 할 것으로 기대된다. 따라서 CDMA, WCDMA, GSM 등에 사용되는 인증 기술을 응용하여 MVoIP에 적합한 사용자 인증 시스템을 구축하는 것이 필요하다.

참 고 문 헌

[1] "The Information Security Guide for VOIP," Korea Internet & Security Agency, Dec. 2005.
[2] S. Yun, S. Park, "Study User Certification Technique of VoIP Service With a Certification Service," *Korea Society for Internet Infomation, Conference 2008*, vol.9, no.1, pp.117-212, May. 2008. (in Korean)
[3] J. Fenton, "Analysis of Threats Motivating Domain Keys Identified Mail(DKIM)," IETF RFC 4686, September 2006.
[4] M. Wong and W, schlitt, "Sender Policy Framework(SPF) for Authorizing Use of Domains in E-Mail, Version 1," IETF RFC 4408, April 2006.
[5] J. Choi, T. Jung, S. Jung, Y. Kim, "Implementation of a Secure VoIP System based on SIP," *Journal of Information and Communication Society*, vol.29, no.9B, pp.799-807, Sep. 2004. (in Korean)