휴대인터넷망을 이용한 VoIP 서비스 구현

*김윤식, 정미영, 정현민, 이성춘
KT 인프라연구소
e-mail : analyzer@kt.com

VoIP Service Implementation over IEEE 802.16e Broadband Wireless Access System

*Yun Sik Kim, Mi Young Jung, HyunMeen Jung, Sung Choon Lee
Infra Laboratory. KT Corp.

Abstract

As broadband wireless access systems are widely accepted, VoIP service over the wireless network is being requested. Because previous VoIP implementations are designed to provide service over wired network, they does not consider security problem sufficiently that is one of the most vulnerable aspects of wireless communication. Therefore, this paper describes how to implement secure VoIP service over wireless network with minimum overhead.

I. 서론

휴대인터넷 (WiBro) 서비스는 OFDM기반의 무선통신 서비스로, 이동하면서도 초고속인터넷을 이용할 수 있는, 3.5세대 이동통신 서비스이다. 기존의 무선통신기술들은 음성 통화를 기본으로 개발되어, 음성 통화 외에 부가적으로 데이터통신 서비스를 제공하였으 나, 휴대인터넷기술은 기존의 무선통신기술 들과는 달리 데이터통신을 기본으로 개발되어, 데이터통신을 기본으로 제공하고 부가적으로 음성통화 서비스를 제공한다.

이러한 휴대인터넷서비스와 같은 무선데이터전용 네트워크가 보편화됨에 따라, 이를 이용하여 음성통화 서비스를 제공하기 위한 VoIP 기술들이 검토되고 있다. 기존에는 H.323 프로토콜을 이용하여 무선데이터전용 네트워크를 이용하여 VoIP서비스를 제공하는 방안이 검토되었으나[1], 최근에는 H.323 대신 보다 간단한 프로토콜 구조를 가지는 SIP 프로토콜을 사용하여 무선통신 네트워크를 이용하여 VoIP서비스를 제공하는 방안이 검토되고 있으며, 무선통신환경에서 VoIP서비스의 서비스 품질을 만족시키기 위한 연구들이 진행되어 왔다[2~4]. 그러나 무선통신망에서의 VoIP 서비스의 경우 외부의 도청에 매우 취약한데도 불구하고 아직까지 보안문제는 충분히 고려되고 있지 않다[5].

본 논문에서는 휴대인터넷 망에서의 음성통화 서비스 구현을 위하여 SIP 기술을 사용하여 VoIP를 구현하는 경우 지연시간 증가 없이 실시간 프로토콜(RTP)을 이용하여 양단간에 PKI (Public Key Infrastructure) 기반의 보안 통화를 가능하게 하는 방법을 제안한다..

II. VoIP 서비스의 구현방법

SIP를 이용한 보안통화 서비스를 구현하기 위한 PKI 구축을 위하여, 복호화 및 서명에 사용되는 개인키는 단말기내에 저장되며, 암호화에 사용되는 공개키는 SIP 레지스트리 서버에 주소 정보와 연결되어 저장되게 된다. 본 서비스를 제공하기 위해 복호화및 서명에 사용되는 개인키는 일반적으로 단말기에 구현되는 EPROM을 이용하여 저장할 수 있다. 그리고 암호화에 사용되는 공개

키는 SIP 레지스트리 서버에 주소 정보와 같이 연결되어 저장되게 된다. 일반적인 SIP 호 설정은 UAC와 UAS가 동일 도메인내에 존재하는지 아닌지에 따라 달라지게 되지만, SIP를 이용하여 구현되는 음성 통화 서비스를 이용하기 위해서는 UAC는 UAS와 직접적으로 또는 Proxy Server를 경유하여 통신을 하게 된다.

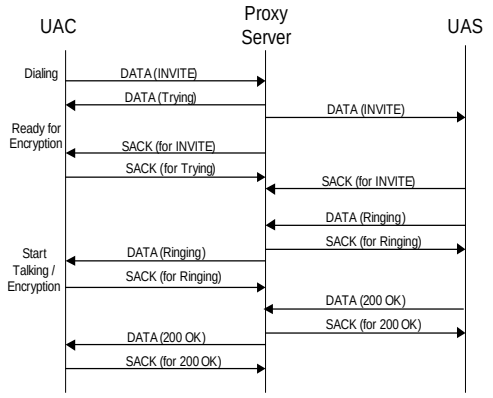

그림 1. 보안 통화를 제공하기 위한 UAC와 UAS간 호 설정 과정

실제 호 설정을 위해서 UAC는 INVITE 메시지를 SIP 프록시 서버에게 보내게 되고, INVITE 메시지를 수신한 SIP 프록시 서버는 SIP 레지스트리 서버에 주소 정보 요청을 보내, UAS의 IP 주소 및 UAC 및 UAS의 공개키를 전송받고 다시 UAS에 INVITE 메시지를 보낸다. UAS의 사용자가 통신을 위해 호출 (Ringing)에 대한 응답을 하게 되면, UAS에서는 프록시 서버에 200 OK메시지를 보내게 되는데, 프록시 서버는 UAS로부터 200 OK 메시지를 받게 되면 UAS에게 200 OK에 대한 SACK 메시지를 보낼 때 SACK 패킷에 UAC의 공개키를 같이 실어보낸다. 그리고 나서 UAC에게200 OK 신호를 포워딩할 때 UAS의 공개키를 첨부하여 같이 보내게 된다. 이를 통해 PKI 연결이 만들어지고 보안통화서비스가 제공 가능하게 된다.

이후 송신측에서는 VoIP 통화를 위한 음성데이터는 샘플링되어 디지털화된 다음, 상대방의 공개키 값을 이용하여 암호화되고 단말기의 EPROM에 저장된 개인키를 사용하여 디지털 인증서를 암호화하여 뒤에 첨부하여 전송하게 된다. 최종적으로 데이터는 다중 접근 부호화 및 변조를 거쳐 전송된다.

수신측에서는 수신된 데이터를 복조하고 다중 접근 복호화한 후에 상대방의 공개키로 디지털 인증서를 확인하고, 수신측의 개인키를 이용하여 상대방의 데이터를 복호화하여 원래의 음성을 듣게 된다.

비밀키 암호화 방법을 병행하여 사용하는 경우에는 초기 호 설정단계에서 송신 또는 수신 단말기에서 처음 패킷에 비밀키를 전송하여 이후 이 비밀키를 이용하여 암호화를 수행하거나 또는 비밀키를 통신서비스회사의 서버로부터 받아 비밀키를 이용하여 암호화를 수행 할 수 있다.

따라서 이러한 방법을 통하여 보안통화를 위한 호 설정에 필요한 추가 지연시간 없이 SIP 프로토콜을 이용하여 보안 통화 서비스를 제공하는 것이 가능하다. 또한 단말기에 따라 고유한 개인키 값을 단말기내 하드웨어에 저장함으로써, 개인키의 외부 노출을 사전에 차단하여, SIP 레지스트리 서버가 해킹 당하는 경우에도 사용자 정보를 보호할 수 있다.

III. 결론 및 향후 연구 방향

본 논문에서는 휴대인터넷 망에서의 음성통화 서비스 구현을 위하여 SIP 기술을 사용하여 VoIP를 구현하는 경우 실시간 프로토콜 (RTP)을 이용하여 양단간에 PKI 기반의 통화를 가능하게 하는 방법을 제안하였으며, 이 방법을 사용하는 경우, 보안을 위한 추가 지연시간 없이 안전한 통화 서비스를 제공하는 것이 가능하다. 또한 단말기에 따라 고유한 개인키값을 단말기 내 하드웨어에 저장함으로써, 외부 노출을 사전에 차단하여, SIP 레지스트리 서버가 해킹 당하는 경우에도 보안상의 문제가 없도록 하였다.

참고문헌

[1] Das, S.K., Lee, E., Basu, K., Sen, S.K., "Performance optimization of VoIP calls over wireless links using H.323 protocol," IEEE Transactions on Computers, Vol. 52, Issue 6, June 2003, Page 742-752.

[2] Fathi, H. , Chakraborty, S., Prasad, R., "Optimization of VoIP session setup delay over wireless links using SIP," IEEE Global Telecommunications Conference, 2004, Vol. 6, Nov. 29-Dec. 3, 2004. Page 4092-4096.

[3] Fathi, H., Chakraborty, S.S., Prasad, R., "Optimization of SIP Session Setup Delay for VoIP in 3G Wireless Networks," IEEE Transactions on Mobile Computing, Vol. May 9, 2006, Page 1121-1132.

[4] Seung-Eun Hong, Oh-Hyeong Kwon, "Considerations for VoIP Services in IEEE 802.16 Broadband Wireless Access Systems,"IEEE 63rd Vehicular Technology Conference, 2006, Vol. 3, Page 1226-1230.

[5] Holly Xiao, Zarrella, P. "Quality effects of wireless VoIP using security solutions," IEEE Military Communications Conference, 2004. Vol. 3, Oct. 31-Nov. 3, 2004. Page 1352-1357.