4G WiBro서비스에서 VoIP 암호화와 인증기술 연구

백종일* · 천우성* · 박대우*

*호서대학교 벤처전문대학원

A Study of VoIP Encryption and Authentication Technologies in 4G WiBro Services

Jong-Il Baek* · Woo-Sung Chun* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : jibaig101@empal.com · deux8522@gmail.com · prof1@paran.com

요 약

4G WiBro 서비스는 우리나라에서 세계표준화한 4세대 통신이다. WiBro 통신 기반에서 응용서비스의 하나인 VoIP가 활성화 되고 있다. WiBro 서비스에서 VoIP를 이용할 때 기존 VoIP 취약점을 보완한 암호화와 인증기술에 대한 연구가 필요하다. 본 논문에서는 4세대 WiBro, LTE를 정의하고, 1G, 2G, 3G와 4G를 비교한다. 그리고 WiBro 서비스에서 VoIP에 대한 기술적, 관리적, 물리적, 해킹 공격 취약점을 분석하고 보안 대책을 연구한다. 보안성 강화를 위한 대책으로 WiBro 서비스에서 VoIP 암호화와 인증을 통한 보안기술에 대하여 연구한다.

ABSTRACT

4G WiBro service in Korea, the world's fourth-generation communication is standardized. VoIP service has been activated one of the application in WiBro communications infrastructure. When using VoIP in the WiBro service, complementing the existing VoIP vulnerabilities in the encryption and authentication technology is a need for research. In this paper, fourth-generation WiBro, LTE, and the definition, 1G, 2G, 3G and 4G compares. And, WiBro service in the VoIP edaehan technical, administrative, physical, and hacker attacks and vulnerability analysis is the study of security measures. Enhanced security measures for the WiBro service to VoIP security through encryption and authentication technologies are studied.

키워드

4G, WiBro Service, VoIP Encryption, Authentication Technologies, Vulnerabilities,

Ⅰ. 서 론

국내 WiBro(Wireless Broadband) 서비스는 방송통신위원회로부터 2.3㎓ 대역 30㎒ 폭을 7년 기한으로 할당받아 서비스를 제공하고 있다. 최근 국내 LTE(Long Term Evolution)와 더불어 4세대(4 Generation) 서비스로 주파수 재할당을 받아서 WiBro 서비스를 제공하고 있다.

2011년 3월 KT는 국내 82개 도시에서 WiBro 망을 설치하여 전국지역의 85%를 커버한다. 서비스단말기로는 WiBro 스마트폰, WiBro 모뎀, 태블릿PC 등의 4G 단말기가 상용화되어 있다.

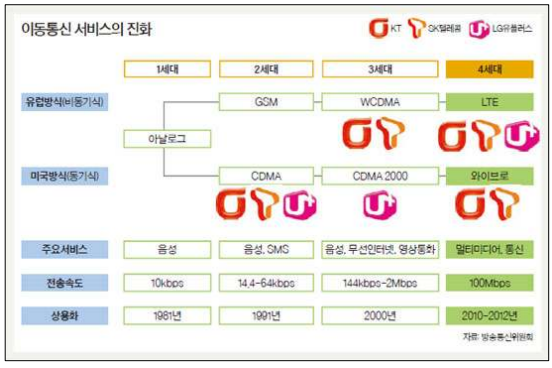

그림 1. 국내 이동통신 1-4세대 서비스 진화

특히 4G WiBro 서비스에서 VoIP(Voice over Internet Protocol)서비스는 통신료가 저렴하거나, 무료라는 개념으로 인식되면서 사용량이 증가하고 있다. 그림 1은 국내 이동통신의 1세대부터 4세대까지 서비스의 진화를 보여주고 있다[1][2].

하지만 국가정보원에서 제시한 VoIP 5대 보안 취약점에 노출 될 수가 있어서, 보안취약점에 대한 보안성 강화를 위하여 4G WiBro 서비스에서 제공하는 VoIP서비스에 대한 암호화와 인증기술에 대한 연구가 필요한 시점이다[3].

본 논문에서는 4세대인 WiBro, LTE를 정의하고, 3G와 4G를 비교하면서, WiBro서비스에서 VoIP에 대한 기술적, 관리적, 물리적, 해킹공격 취약점을 분석하고, VoIP 암호화를 연구하고, WiBro서비스에서 VoIP 인증기술을 연구한다.

Ⅱ. 관련연구

2.1 4G WiBro, LTE

국제전기통신연합(ITU)은 4G(4세대) 이동통신을 '정지 상태에서 초당 1Gbps, 250㎞ 이상 이동 시 100Mbps 이상의 데이터 속도를 제공하는 고속의 통신서비스'라고 정의했다. 현재 3G 7.2Mbps 기술 수준을 감안하면 약 14배 빠르다.

Wibro(WiBro)는 IEEE 802.16e 표준으로 무선 광대역의 줄임말로 2.3㎓ 대역의 주파수를 이용하면서 3G의 5㎒ 대역폭보다는 더 넓은 10~30㎒ 대역폭의 주파수를 사용하고 있다.

LTE는 IEEE 802.16m 표준으로 3G의 WCDMA에서부터 진화해 온 네트워크 기술로 텔리아소네라가 상용서비스를 처음 시작하여 이라는 의미다[4].

2.2 1G, 2G, 3G, 4G, Next4G

1981년 이동통신서비스는 아날로그 음성통화가 1G(1세대)로 구분된다.

이후 멀티미디어 형태의 수요가 증가하면서 문자 전송이 가능하게 된 것이 2G로 구분된다.

현재 3G 기술은 영상 통화 등 대용량의 멀티미디어 데이터 전송을 위해 속도를 높인 WCDMA 등의 기술이다. 3G는 여러 명의 사용자가 접속하기 위해 5㎒ 주파수 대역폭을 이용한 코드를 분할하는 CDMA 방식을 사용한다.

4G는 직교주파수분할 다중접속방식(OFDMA, Orthogonal Frequency Division Multiple Access)을 사용한다. OFDMA는 LTE와 WiBro의 핵심 기술로, 1.4㎒부터 최대 20㎒까지 광대역 주파수를 사용하여 다중 사용자 접속을 가능케 하며, 다중 안테나 채택(MIMO)으로 빠른 데이터 통신이 가능하다.

4G 이후의 차세대 버전인 LTE-Advanced는 최대 600Mbps(40MHz 대역폭 기준)의 데이터 전송이 가능하며, WiBro-Evolution(802.16m)은 기존 4G보다 넓은 대역폭과 많은 수의 안테나를 사용해 표준 IP기술이로 다양한 서비스가 가능하다.

Ⅲ. WiBro서비스에서 VoIP 공격위협과 VoIP 암호화 연구

3.1 WiBro서비스에서 VoIP공격 위협

SIP Scan을 통해 SIP에 연결되어 있는 시스템을 그림 2부터 그림 3과 같이 스캐닝을 통해 확인하였다.

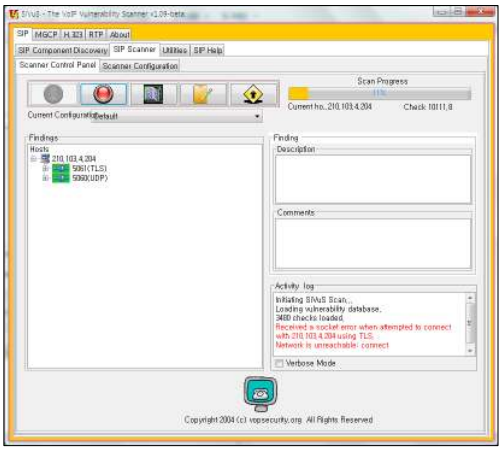

그림 2. SIP Scanner Control Panel

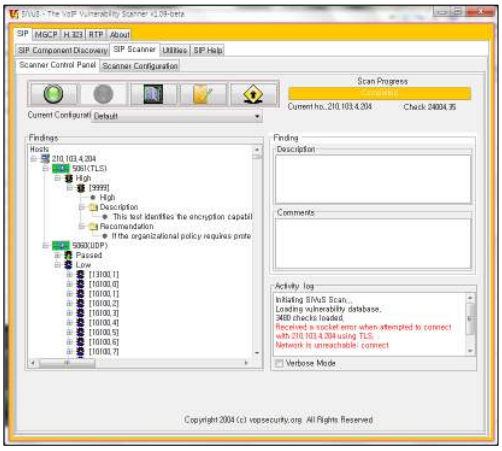

그림 3. SIP Scanning 결과

또한, 관리자로 접속하여 외부의 일반 전화를 내부전화처럼 등록하고 외부에서 통화를 실시하였을 때 암호화 기능이 없는 외부 VoIP폰과 통화를 하였을 때 도청이 되는 것을 그림 4와 같이 확인하였다[5].

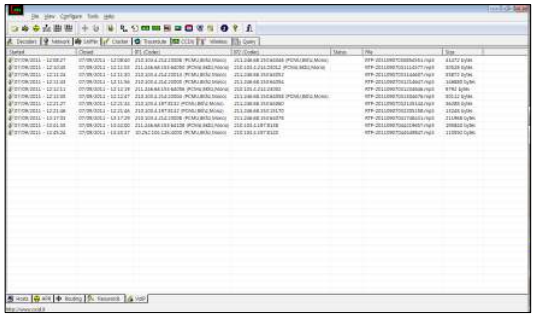

그림 4. 암호화 기능 없는 외부 VoIP폰과 통화시 도청 가능

3.2 WiBro서비스 보안 취약점

WiBro 서비스에서 발생할 수 있는 취약점 중에서 무선 구간에서 발생 가능한 취약점은 다음 표와 같다. 실제 사용자가 서비스를 제공 받는 과정에서 일어날 수 있는 것들이며, 대응방안을 고려해야 한다. WiBro 기술은 기술적인 특징을 기반으로 Physical Layer와 MAC Layer의 취약점을 구분하여 표 1과 같이 정리 할 수 있다[6].

표 1. WiBro 기술적 취약점 분류

PHY Layer	MAC Layer
·Dos형태의 공격이 가능함 ·Jamming attack, Scrambling attack – 소음을 발생시켜 전파 방해 하는 공격 ·Water torture attack : 휴대용 장치의 한정된 자원을 사용하지 못하도록 함 ·기타 : 위조 공격, 재생공격 가능 적법한 송수신자의 채널을 무선 환경에서 공격자가 사용가능	·단말기와 기지국의 초기 연결 시 사용하는 메시지의 노출 위험성 ·홉 간 이동 시 각 네트워크 접근에 대한 보안 취약성 ·인증 취약점 (가장의 위협, 중간자 공격 가능)

3.3 WiBro 기반 VoIP 암호화 기법 적용 구성

WiBro 기반 VoIP에는 WiBro에서 사용되는 암호화 기법인 PKMv2를 적용할 수 있다. 기존의 PKMv1에 비해 데이터 암호화방식에서는 DES 알고리즘 뿐 아니라, 암호강도가 높은 128bit AES 알고리즘을 사용해 전송하기 때문에, 보다 안전하다. 데이터 암호화 알고리즘 식별자에 따라 DES-CBC, AES-CCM, AES-CTR, AES-CBC 알고리즘 중 선택하여 사용할 수 있으며, 인증키는 단말과 기지국이 각각 생성하는 방식을 사용함으로써 인증키가 무선구간에 직접 노출되지 않아 보안성이 강화됐다[7][8].

Ⅳ. WiBro서비스에서 VoIP 인증기술 연구

4.1 WiBro서비스 취약점 대응 방안

WiBro의 무선 구간에서 발생 가능한 취약점에 대한 보안대책은 표 2와 같다.

표 2. WiBro 기술적 취약점 대응방안

PHY Layer	MAC Layer
·신호에 대한 파워 또는 대역폭 증가 ·지속적인 모니터링을 통한 비정상 행위 탐지 ·복잡한 메커니즘을 방지하기 위해, 사용하지 않는 프레임을 폐기 ·배터리 또는 전산 자원의 고갈을 막을 수 있음 ·상호 인증	·PKMv2에 기반한 AES 암호화 알고리즘을 활용한 데이터 암호화 및 HMAC/CMAC을 통한 메시지 무결성 인증 ·간단하고 효율적인 키 교환 방법인 PKI 기법을 통해 해결 ·RSA/X.509인증을 통해 사용자 인증 PKMv2를 통한 사용자 상호 인증(중간자 공격 불가)

4.2 PKMv2 인증

WiBro에서는 PKMv2를 통해 망 접속을 위한 단말 및 네트워크 간 양방향 인증, 암호화된 데이터 통신에 사용될 TEK(데이터 암호화 키) 교환이 가능하다.

WiBro 표준에서는 무선네트워크에서의 단말과의 안전한 통신을 위한 인증 및 기밀성을 제공하기 위해 보안 부계층(Security Sublayer)을 정의하고 있으며, 보안 부계층 내 PKM을 정의한다. 현재 PKM은 버전 2를 사용하고 있으며, 인증 방식으로 RSA인증 방식과 EAP인증 방식의 다른 메커니즘을 사용할 수 있다. 두 가지 인증 방식 중 한가지를 선택하여 사용하거나, 두 가지 모두 사용할 수 있다.

4.3 RSA(Rivest-Shamir-Adleman) 인증방식

PKM RSA 인증 프로토콜은 공개 RSA 암호화 키와 단말의 MAC주소를 결합하여 RSA방식을

이용한 공개키 알고리즘인 X.509 디지털 인증서 방식을 사용한다. 기지국과 초기 인증 교환 절차를 통해 클라이언트 단말에 대한 인증을 수행한다. 각 단말기는 제조업체에서 발행한 고유의 X.509 디지털 인증서를 가지고 있으며, 디지털 인증서 안에는 단말의 공개키와 MAC주소를 포함하고 있다. 기지국은 디지털 인증서 검증을 통해 단말의 공개키를 검증하며, 검증된 공개키를 통해 인증키를 암호화하여 인증을 요청한 단말에 인증키를 전송한다.

RSA 인증 프로토콜을 사용하기 위해 단말에 RSA 키 쌍(비밀키/공개키), 또는 키 쌍을 생성할 수 있는 내부 알고리즘이 탑재되어 있어야 한다. 또한, 제조업체에서 탑재한 X.509인증서 탐재가 가능한 메커니즘을 지원해야 한다.

4.4 EAP(Extensible Authentication Protocol) 인증방식

PKM EAP 인증방식은 IEEE802.1x 포트기반의 가입자 인증데이터 전송을 위한 표준 프로토콜로 EAP-MD5, EAP-씬, EAP-AKA (Authentication and Key Agreement) 등 다양한 인증 프로토콜을 사용할 수 있으며, 사용자 인증 및 단말, 그리고 네트워크 간 상호인증이 가능하다. 또한 AAA인증 서버를 통해 인증을 수행하기 때문에 사용자가 증가해도 기지국에 오버헤드가 생기지 않는다는 장점이 있다. 현재 PKMv2 EAP 기반 인증방식에 AKA 메커니즘을 적용한 EAP-AKA 인증방식으로 표준 및 사용화를 추진중에 있다. EAP-AKA 인증방식은 현재 3GPP와 무선 랜 간의 연동 시 끊김 없는 서비스제공을 위해 필요한 보안인증 프로토콜로 3GPP에서 제안한 상황이다. EAP-AKA의 경우 사전에 키를 공유하는 방식을 사용하여 인증을 하므로 키 노출에 대한 위험을 가지고 있다. 그러나 EAP-TLS의 경우 RSA인증 방식과 같이 X.509인증서를 사용하여 인증을 수행하므로, 이러한 위험요소를 갖지 않는다.

V. 결 론

4G WiBro 서비스에서 VoIP서비스를 활용하여 통신료를 저렴하게 사용하고 무료라는 개념으로 인식되면서 사용량이 증가하고 있다. 하지만 국가정보원에서 제시한 VoIP 5대 보안취약점에 노출되어 보안취약점에 대한 보안성 강화를 위하여 4G WiBro 서비스에서 제공하는 VoIP서비스에 대한 암호화와 인증기술에 대한 연구가 필요하다.

4세대인 WiBro, LTE를 정의하였고, 공격위협에 대해 SIP 스캐닝툴을 사용하여 취약점을 분석하고 WiBro 기반 VoIP 암호화 기법 적용을 구성하였다. WiBro서비스 취약점 대응 방안으로 PKMv2, RSA, EAP 인증방식을 적용하여 도청이 안되었다.

향후 연구에서는 4G에서 암호화와 인증에 대해 보안을 강화할 수 있는 연구가 이루어져야 하겠다.

참고문헌

[1] 표현명, "WiBro 사업 추진 현황 및 전개 방향," 정보과학회지, 제25권, 제4호, page(s): 7-13, 2007년 4월.

[2] 김명균, 엄윤성, "WiBro망에서 VoIP를 이용한 그룹통신 서비스 성능분석," 한국해양정보통신학회논문지, Vol.15, No.6, pp.1256-1264, 2011년 6월.

[3] 윤석웅, "IETF 국산 암호기술의 국제표준화 동향," 정보보호학회지, 제21권, 제2호, pp.78-82, 2011년 4월.

[4] 박대우, 임승린, “WiBro에서 공격 이동단말에 대한 역추적기법 연구,” 한국컴퓨터정보학회논문지, 제12권, 제3호, 185-194쪽, 2007년 7월.

[5] Dea-Woo Park, “A Study of Packet Analysis regarding a DoS Attack in WiBro Environments”, International Journal of Computer Science and Network Security, IJCSNS (1738-7906), December 2008.

[6] Woo-Sung Chun, Dea-Woo Park, "Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network," International Journal of Computer Science and Network Security, Vol. 9, No. 12, December 2009.

[7] Dea-Woo Park, "A Study on Real-time Cooperation Protect System Against Hacking Attacks of WiBro Service," International Journal of Maritime information and Communication Sciences, Vol.9, No.4, pp.353-357, August 2011.

[8] 김종환, 전흥우, 신경욱, "WiBro 보안용 AES 기반의 Key Wrap/Unwrap 코어 설계," 한국해양정보통신학회논문지, Vol.11, No.7, pp.1332-1340, 2007년 7월.