휴대인터넷 정보보호 발전방향

국가보안기술연구소 윤이중

1. 서 론

국내 정보통신기술이 급속하게 고속화, 대용량화되고, 이동통신 기술의 서비스가 기존의 음성 중심에서 데이터 위주 서비스로 변모함에 따라 사용자들의 고속 멀티미디어 서비스에 대한 요구와 언제 어디서나 편리하게 이용할 수 있는 인터넷 접속 수요가 증대하면서 1Mbps 이상의 고속 데이터 전송을 보장하면서, 이동성이 지원되는 새로운 서비스에 대한 필요성이 대두되고 있다.

현재의 IMT-2000 시스템은 회선 및 패킷 서비스를 동시에 지원하기 위해 망 구조가 복잡하고 고가 장비로 인하여 높은 요금이 예상되고 있기 때문에 효율적인 이동 무선인터넷 접속 서비스로서 부절한 것으로 지적되고 있다. 한편, 무선랜과 같이 제한된 지역을 커버하는 시스템의 경우에는 저가로 고속의 데이터 서비스를 제공할 수 있으나, 이동성이 취약하고 실외 환경에서 신뢰성 있는 서비스의 제공에 한계가 예상된다. 따라서 국내에서는 2002년도부터 2.3GHz 대역을 활용하여 이와 같은 기존 시스템의 한계를 극복하고 ADSL (Asymmetric Digital Subscriber Line) 수준의 품질과 비용으로 정지 또는 저속 이동 중에도 고속 인터넷 접속이 가능한 준이동 무선인터넷 서비스로서 '휴대인터넷'이라는 새로운 서비스를 개념화한 바 있다. 휴대인터넷 서비스는 정액제 요금으로 "Always Connected" 형태로 유선 ADSL과 유사한 수준의 전송률과 품질을 보장함으로써 기존의 이동통신 및 3세대 이동통신과 차별화 하고자 한다.

이동성을 가지는 초고속 데이터 통신 서비스 필요성에 부흥하여 정보통신부는 "IT 839 전략"의 8대 신규서비스의 일환으로 휴대인터넷을 추진하고 있으며, 정보통신기술협회(TTA)에서도 휴대인터넷 표준화를 시작하여 2004년 6월 1차 표준을 완성하였다. 국내 휴대인터넷의 국제 표준화를 위해 IEEE 802.16과의 Harmonization을 추진하고 있으며, 2006년 국내 휴대인터넷 상용화를 목표로 추진 중이다.

국내 휴대인터넷의 보안 규격은 진행중인 IEEE 802.16의 국제 표준을 참조하여 작성되었으며, 이에 대한 취약성에 대한 연구는 아직 활발히 진행되고 있지 않다. 따라서 본 고에서는 휴대인터넷의 보안 메커니즘에 대해 살펴보고 휴대인터넷의 취약점을 분석한다.

2. 휴대인터넷 개요

2.1 휴대인터넷의 정의

휴대인터넷의 개념 및 정의에 대해 정보통신부는 언제 어디서나 정지 및 이동 중에 고속으로 무선인터넷 접속이 가능한 서비스로 정의하고 있다. 2.3GHz 대역의 휴대인터넷 서비스는 IP (Internet Protocol) 기반의 유선인터넷과 무선인터넷이 결합된 망에서 휴대인터넷 단말기를 이용하여 정지 및 보행상태에서 고속의 전송속도로 인터넷에 접속, 다양한 정보와 콘텐츠를 이용하는 서비스를 말한다.

휴대인터넷의 핵심기술인 스마트안테나, OFDM (Orthogonal Frequency Division Multiplexing), 그리고 MIMO (Multiple Input Multiple Output) 기술 등은 주파수 효율을 높이는 기술로써 4G 서비스의 기반기술 특성을 가진다.

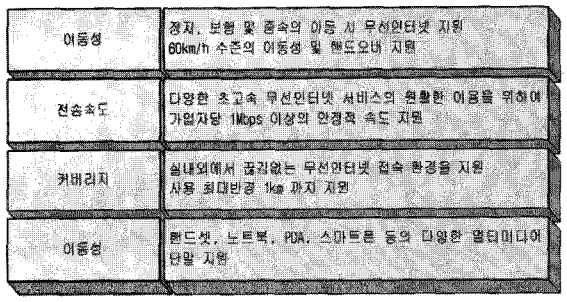


그림 1 휴대인터넷의 개념

휴대인터넷은 이동성, 핸드오버, 셀 단위 서비스, 휴대단말기 사용, 고품질(QoS) 그리고 보안성 등과 같이 이동통신과 유사한 특성을 가진다. 기존 이동통신 서비

스와 마찬가지로 셀 간의 핸드오버를 지원하며 이동 중에도 끊김없는 서비스 제공이 가능해야 한다. 현재 2.4GHz 대역의 무선 LAN 보다는 다소 높은 보행 수준의 '준 이동성 (Nomadic Mobility)'을 보장하고 있다. 전송속도 면에서도 무선링크에서 상향 최대 전송속도 1Mbps, 하향 최대 전송속도 3Mbps 이상의 안정적인 속도로 무선인터넷 서비스 제공을 목표로 하고 있다.

표 1 무선 접속 파라미터와 필수 요구사항

항목	방식 또는 값
다중화 방식 (Duplex)	TDD
다중접속방식 (Multiple Access)	OFDMA
채널대역폭	10MHz
가입자당 전송속도	상향최대전송속도1Mbps 하향최대전송속도 3Mbps
	상향최소전송속도128kbps 하향최소전송속도 512kbps
주파수 재사용 계수	1
주파수 효율	최대 주파수 효율 : DL(6), UL(2)
	평균 주파수 효율 : DL(2), UL(1)
핸드오프	기지국내 셀간, 기지국간, 주파수간 핸드오프 : 150ms 이하
이동성	최대 60Km/h
서비스 커버리지	Pico (100m), Micro (400m), Macro (1Km)

2.2 휴대인터넷의 구성

휴대인터넷 시스템은 OFDMA(Orthogonal Frequency Division Multiple Access)/TDD(Time Division Duplex)방식의 광대역 무선전송기술을 사용하여 셀룰러 형태의 망 구성을 가능하게 하고 IP 기반의 무선 데이터 서비스의 상하향 비대칭 전송 특성에 효과적으로 적응할 수 있다.

휴대인터넷 시스템 구조는 그림 2와 같이 휴대인터넷 단말 (MSS : Mobile Subscriber Station), 기지국 (BS : Base Station), 제어국 (ACR : Access Control Router), 그리고, 백본(Backbone)망으로 구성된다. 백본망은 AAA (Authorization, Authentication and Accounting)서버, HA (Home Agent)서버, 관리 서버와 다른 특정 목적을 위한 서버들을 포함할 수 있다.

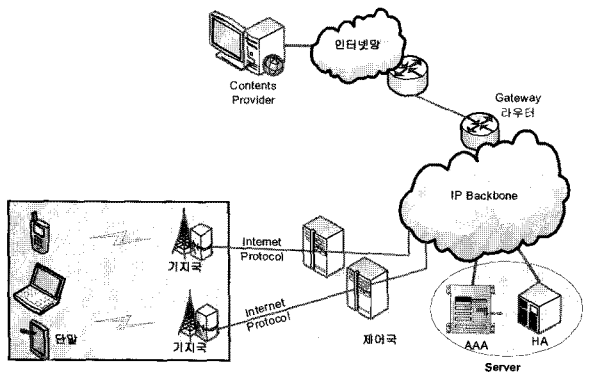


그림 2 휴대인터넷 망 구성도

휴대인터넷 단말은 무선 채널의 종단점으로 기지국과 OFDMA 방식으로 통신을 하며 무선 채널 송수신 기능, MAC(Medium Access Control) 처리 기능, 핸드오버 기능, 사용자 인증 및 암호화 기능, 무선링크 제어관리 기능 등을 수행한다. 기지국은 유무선 채널 변환 기능을 수행하여 단말과 제어국 사이의 데이터를 전달하는 역할을 수행하며 오류 없는 패킷 송수신을 위한 패킷 재전송 기능, 무선 자원의 효율적 운용을 위한 패킷 스케줄링 및 무선 대역폭 할당 기능, 레인징 기능, 패킷 호 연결 설정/유지/해제 등과 관련된 연결 제어 기능, 핸드오버 제어기능, 제어국의 접속 기능 등을 수행한다. 제어국은 다수의 기지국들을 관리하며 제어국내에서의 고속의 이동성을 보장하기 위한 핸드오버 제어 기능을 수행한다. 이를 위해 기지국과 제어국은 IP 프로토콜을 기반으로 접속되며, 고속 패킷 전송을 위해 기가 비트 이더넷 스위치를 기반으로 구성된다.

휴대인터넷 망 구성요소와 역할은 표 2와 같이 정리된다.

표 2 휴대인터넷 구성요소

구성 요소	휴대인터넷 구성요소 역할
단 말	가입자가 휴대인터넷 서비스를 제공 받기 위해 사용하는 휴대성, 이동성을 가진 단말기
기지국	유선네트워크 종단에서 무선 인터페이스를 통하여 단말과 송수신을 하는 AP (Access Point) 역할을 하는 구성요소
제어국	단말과 기지국을 제어하고 IP 패킷을 라우팅하는 구성 요소
서 버	인증 및 이동성 등을 지원하는 AAA, HA 등과 같은 망 구성요소

2.3 휴대인터넷 표준화

국내 휴대인터넷 표준화 작업은 2004년 6월에 TTA PG302 표준화 그룹에서 휴대인터넷 표준 Phase 1을 완성하였다. 7월에 정보통신부는 연말까지 휴대인터넷 사업자 허가 신청서를 접수하여 2005년 2월에 사업자 선정하는 계획을 포함한 휴대인터넷 사업 허가 일정과 IEEE 802.16 기술표준과 이동성, 전송속도, 이중화 방식, 채널 대역폭, 사업자 장비간 로밍 등 5가지 성능 기준을 수용하는 기술 방식을 결정하였다. 9월에 정보통신부는 휴대인터넷 서비스 와이브로 허가 정책 방안을 확정하고 3개 휴대인터넷 사업자를 선정하기로 발표하였으며 현재 KT, SK텔레콤, 하나로텔레콤 등 3 개사만

이 사업자 선정을 위한 사업 계획서를 제출하여 실질적인 예비 휴대인터넷 사업자들이 선정된 상황이다.

2004년 7월부터 TTA PG302에서는 서비스 및 시스템 용량과 기능을 향상시키기고 표준화의 국제화를 위하여 표준화 2단계를 진행하고 있다. 표준화 2단계는 국제 표준화를 위하여 802.16과의 Harmonization과 ITU-R 등의 타 표준화 기구와의 협력을 도모하고 있다. 다음 표 3은 TTA PG302의 표준화 2단계 추진 일정 및 목표를 나타내고 있다[3].

3. 휴대인터넷 보안 구조

3.1 휴대인터넷 보안 계층

휴대인터넷의 보안 기능은 고정 또는 이동 무선 망의 기지국과 단말 사이의 모든 연결을 암호화함으로써 사용자들에게 안정적인 정보보호 서비스를 지원하기 위해 수행된다. 또한, 이 보안기능은 망에 연결된 모든 서비스 플로우에 대하여 정보보호를 강화함으로써 기지국에 불법적으로 접근하는 것을 방지한다. 이러한 보안 기능을 지원하기 위해 인증 클라이언트와 인증 서버 개념을 도입하여 인증 서버는 인증 클라이언트인 단말을 인증하고 기지국은 트래픽 암호화 키 정보를 분배 및 관리한다.

휴대인터넷의 매체접근제어(MAC : Medium Access Control) 계층은 그림 3과 같은 인증, 암호키 교환, 암호화 등을 제공하는 독립된 암호 부계층을 포함한다. 보안 부계층은 패킷 데이터에 대한 암호화를 위한 프로토콜과 인증 및 트래픽 암호화 키 관리 프로토콜(PKM : Privacy Key Management)로 구성된다.

데이터 암호화 프로토콜은 패킷 데이터 트래픽의 암호화를 위한 프로토콜이다. 데이터의 암호화 방식과 인증 알고리즘을 나타내는 암호화 방법 (Cryptographic suits)과 MAC PDU payload에 적용되는 암호화 알고리즘을 의미한다. 패킷 데이터에 대한 암호화 정보는 일반 매체접근제어 계층 헤더에 나타낸다. 패킷 데이터에 대한 암호화는 일반 매체접근제어 계층 헤더에는 적용하지 않고 MAC PDU에 한정한다. 매체접근제어 계층 헤더에는 수신측 단말에서 Payload를 복호화 하기 위해서 필요한 모든 암호화 정보를 포함한다.

인증 및 트래픽 암호화 키 관리 프로토콜은 기지국과 단말이 인증 서버로부터 인증키 시드를 받아 인증키(AK : Authentication Key)를 생성하고 기지국은 트래픽 암호화 키(TEK : Traffic Encryption Key)를 생성하여 이를 단말에게 안전하게 분배하는 방식을 의미한다. 이 프로토콜을 통하여 단말과 기지국은 인증키 및 트래픽 암호화 키를 공유하게 되고 사용자들의 망에 대한 접근제어를 수행할 수 있다.

표 3 TTA PG302 표준화 2단계 추진일정 및 목표

일정	목표
2004 3Q	서비스 및 시스템 요구사항 정의 시스템 용량 향상 기술 범위 결정 IEEE 802.16과의 Harmonization (국제협력포함) 지적 재산권 처리 세부지침 마련
2004 4Q	시스템 용량 향상 기술 평가도구 설계 시스템 용량 향상 기술 제안 및 평가 시스템 기능 향상 기술 평가방안 작성 IEEE 802.16과의 Harmonization 지적 재산권 관련업무 (요소기술특허이슈, 특허포럼 등)
2005 1Q	시스템 용량/기술 향상 기술 제안 및 평가 표준초안 작성 IEEE 802.16과의 Harmonization 지적 재산권 관련업무
2005 2Q	표준안 완성 IEEE 802.16과의 Harmonization 지적 재산권 관련업무

단말에 대한 인증 및 권한 검증과 인증키 시드는 상위 인증 프로토콜인 EAP-TLS(Extensible Authentication Protocol-Transport Level Security) 기반으로 운용된다.

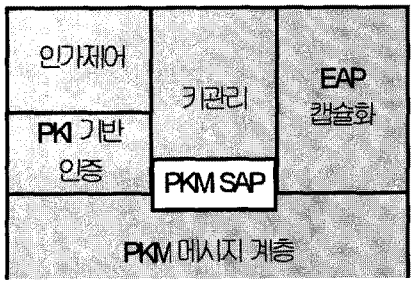


그림 3 보안 부계층

3.2 PKM(Privacy Key Management) 프로토콜

PKM 프로토콜은 기지국과 단말 사이에서 EAP 메시지를 전달하기 위해 사용한다. 기지국과 단말은 EAP-TLS 메시지를 캡슐화한 PKM 프로토콜을 통해 인증 서버로부터 단말의 인증 및 권한 검증과 인증키 시드를 얻게 되고, 단말은 PKM 프로토콜을 통해 주기적인 재인증과 새로운 트래픽 암호화 키 정보들을 요청한다.

PKM 프로토콜은 인증 클라이언트와 인증 서버 모델을 참조한다. 단말은 트래픽 암호화 키 정보를 요청하는 인증 클라이언트가 되고 이러한 요청에 응답을 하는 기지국은 인증 서버 역할을 수행한다. 단말은 자신에 대한 권한 검증이 성공적으로 이루어진 경우에 한해서만 트래픽 암호화 키 정보들을 수신 받는다.

보안 연결(SA : Security Association)은 하나의 기지국과 이 기지국에 접속한 인증 클라이언트인 다수개의

단말이 안전하게 통신하기 위해서 공유하는 보안 정보들의 집합이다. SA에는 Primary SA, Static SA 와 Dynamic SA 등 세 가지의 종류가 존재한다. 각각의 단말은 초기 접속 절차에서 Primary SA를 생성한다. Static SA들은 기지국에서 제공되고, 동적 SA들은 특정 서비스 플로우에 따라 생성 또는 해제된다. Static SA와 Dynamic SA 는 다수의 단말들과 공유할 수도 있다. SA에는 암호화 방법, 트래픽 암호화 키와 초기 벡터 (IV : Initial Vector)들이 포함될 수 있다. 이러한 보안 연결들은 SA ID로 식별한다. 각각의 단말은 기지국과 독립적인 Primary SA들을 공유한다. 단말의 Primary SA의 SA ID는 해당 단말의 Basic CID (Connection ID)와 동일한 값을 가진다.

PKM 프로토콜을 사용하여, 단말은 기지국에게 SA의 키 정보들을 요구한다. 기지국은 이 SA를 통해 각각의 인증 클라이언트 단말이 접속할 수 있도록 권한이 부여되었는지를 판단한다. SA 정보들은 유효 시간을 가지고 있다. 기지국이 SA 키 정보를 단말로 전송할 때, 기지국은 단말에게 해당 SA 키 정보들의 남아있는 유효 시간도 알려준다. 단말은 저장하고 있는 SA 정보들의 유효 시간이 만료되기 전에 새로운 SA 정보들을 요청해야 한다.

그림 4는 PKM 프로토콜을 나타낸다. PKM 프로토콜은 상위 인증 프로토콜인 EAP를 사용하여 기지국과 해당 단말간에 인증키를 교환하는데 사용되고, 교환된 인증키는 패킷 데이터를 암호화하기 위한 트래픽 암호화 키를 생성하는데 사용된다.

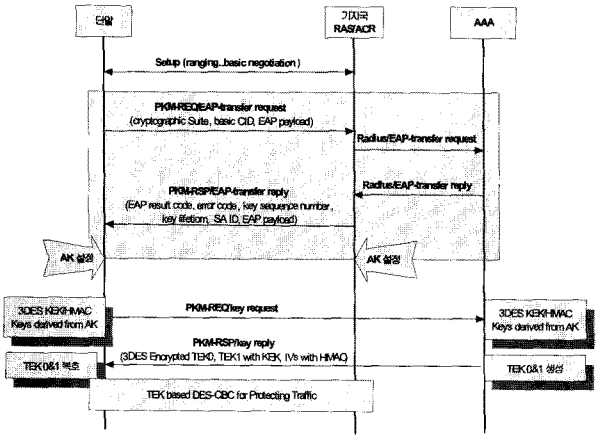


그림 4 인증키 및 트래픽 암호화 키 교환 과정

단말은 PKM 프로토콜을 사용하여 기지국으로부터 권한 검증 및 트래픽 키 정보들을 얻게 되고 주기적인 재인증과 새로운 트래픽 암호화 키 정보들을 요청한다. 여기에서 단말에 대한 실질적인 권한 검증은 IETF (Internet Engineering Task Force) 에서 정의한 표준화를 따르는 EAP-TLS 프로토콜을 기반으로 운용되고, MAC의 암호화 부계층의 암호화 프로토콜에서는 EAP-TLS 인증 프로토콜을 단말과 기지국 사이에 전달하기 위해 사용된다.

기지국은 초기 인증 단계에서 모든 단말에 대한 권한 검증을 실행한다. 다시 말해서, 단말과 기지국이 여러 번의 PKM-REQ MAC 메시지와 PKM-RSP MAC 메시지의 교환을 통해 기지국은 해당 단말에 대한 권한 검증을 실행하고 최종적으로 인증키를 생성하여 인증을 요청한 단말로 인증키를 생성할 수 있는 시드를 분배한다.

EAP Transfer Request 메시지에 대한 응답으로 기지국은 EAP를 통해 인증을 요청한 단말에 대하여 권한 검증을 수행하고, 단말과 공유할 암호화 알고리즘과 프로토콜들을 정하여, 해당 단말에 대한 인증키를 할당하고 단말에게 EAP Transfer Reply 메시지를 통해 이를 분배한다. 단말과 기지국은 인증키 시드의 상위 20바이트를 인증키로 사용한다.

인증 절차 후, 단말은 EAP Transfer Reply 메시지에 포함된 각각의 SA ID에 대한 개별적인 트래픽 암호화 키 상태 머신을 운용한다. 단말 안에서 운용되는 개별적인 트래픽 암호화 키 상태 머신은 각각의 SA ID와 관련된 트래픽 암호화 키 정보들을 제어한다. 단말의 트래픽 암호화 키 머신은 각각의 SA ID에 해당하는 새로운 트래픽 암호화 키 정보들을 요청하기 위해 주기적으로 기지국에게 Key Request 메시지를 전송한다. Key Request 메시지를 수신한 기지국은 하나의 SA ID에 대한 트래픽 암호화 키를 포함하는 Key Reply 메시지를 단말로 송신한다.

기지국은 트래픽 암호화 키를 EDE (Encrypt-Decrypt-Encrypt) 방식의 Two-key 3-DES 알고리즘을 사용하여 암호화하고 암호화된 트래픽 암호화 키를 Key Reply 메시지를 통해 단말에게 전송한다.

4. 휴대인터넷 취약성

4.1 휴대인터넷 기밀성

DES는 대칭 블록암호로서 평문의 각 블록의 길이가 64비트이고 키가 64비트(실제로는 56비트가 키이고 8비트는 검사용)이며 암호문이 64비트인 암호이다. DES 알고리즘에서는 64비트의 평문이 16라운드의 Feistel 연산을 거쳐 64비트의 암호문이 출력된다.

DES 암호 알고리즘은 공개되어 있고 암호키의 수가 유한인 256개여서 1970년대 설계 당시부터 전수공격에 대한 우려가 있었으나, 표준 암호 알고리즘으로 채택될 당시에는 해독이 어려운 암호였다. 그러나, 선택 평

문 공격법의 하나로, 1990년에는 Biham과 Shamir에 의해 두 개의 평문 블록들의 비트의 차이 (예 : 1001과 1101의 차이는 1001⊕1101 = 0100이 됨)에 대응하는 암호문 블록들의 차이를 이용하여 사용된 암호열쇠를 찾아내는 차분 암호 해독법(Differential Cryptan alysis)이 발표되어, 실질적인 공격이 가능하게 되었다. DES 설계자의 한 사람인 Coppersmith에 의하면 설계 당시부터 이미 차분공격법에 대해 알고 있어, 그에 대한 대비책으로 S-함수 설계조건이 나왔다고 한다. 1993년 Biham과 Shamir에 의하면, DES 암호는 계산량 247의 차분공격으로 해독이 된다. 1993년에는 일본의 Matsui가 DES S-함수의 입력비트와 출력비트 사이의 상관도를 선형 근사하여 해독하는 선형근사공격법을 발표하여, 243개의 기지 평문과 12대의 Workstation으로 50일 만에 해독하였다. 1997년 2월에는 RSA사에서 개최한 DES Challenge I에서 78,000대의 컴퓨터를 이용하여 96일 만에, 1998년 7월에는 DES Challenge II에서 250,000달러의 전용칩을 제작하여 56시간 만에, 1999년 1월 18일 DES Challenge III에서 1만 여대의 컴퓨터와 전용칩을 이용하여 DES암호를 22시간 15분 만에 해독을 하였다[4].

다음 표 4는 Handbook of Applied Cryptography에 기재된 DES 알고리즘의 암호학적 강도를 나타낸 표이다. 표 4에서 보여주는 각 공격 유형에 따른 DES의 암호학적 강도를 보더라도 DES는 충분히 안전하지 않음을 알 수 있다[5].

4.2 휴대인터넷 무결성

휴대인터넷에서 메시지 무결성 보장을 위해 사용되는 CRC가 선형함수라는 점을 이용해서 CRC 체크섬에 의해 발견되지 않고 메시지 변조가 가능하다. 이는 기존의 무선랜에서 무결성 알고리즘으로 사용하는 CRC-32가 CRC의 선형성을 이용하여 메시지를 변조함으로써 보안에 취약함을 분석한 문서들을 참고하여 알 수 있다[6]. 따라서 휴대인터넷에서 제공하는 체크섬으로는 메시지 무결성을 보장할 수 없다는 사실을 알 수 있다.

4.3 핸드오버 시 취약성

휴대인터넷은 서비스 접속 중인 단말이 기지국과 통신 중에 이동으로 인하여 해당 단말이 서비스 중인 셀 영역을 벗어나 다른 셀 영역으로 진입하여 핸드오버 절차를 수행하면 이전 기지국에서 이동한 새로운 기지국으로 인증에 필요한 정보를 넘겨주어야 한다. 또한 핸드오버한 기지국에 대한 인증 절차가 필요하다.

휴대인터넷 시스템은 기본적으로 새로운 통신 채널을 열기 전에 기존 채널의 통신을 먼저 끊는 Break before make 방식의 하드 핸드오버에 대해 정의하였으나, IEEE 802.16e를 수용하면서 Make before break 방식인 소프트 핸드오버에 대한 방안도 연구되고 있지만 아직 미흡한 상황이다.

단말이 기지국에 접속하기 위하여 초기 망 진입 절차를 수행할 때는 단말인증과 키교환을 수행한 후에 Serving 기지국에 등록을 한다. 이후 Serving 기지국에서 이동하고자 하는 Target 기지국으로 핸드오버 절차를 수행할 경우 레인징을 수행하고 basic capability만을 협상한 후 단말의 인증과 키교환 절차 없이 바로 재등록과 재연결 설정을 수행한다.

즉, 단말이 기존 기지국에서 이동하여 새로운 타깃 기지국으로 핸드오버 시 Target 기지국은 기존의 Serving 기지국으로부터 해당 단말에 대한 인증 정보를 수신하여 수행하므로 망 재진입 시에는 초기 진입 때와 같은 단말 인증 절차 및 키 교환을 수행하지 않는다.

기지국은 인증 서버를 통해 인증과 서비스 인가를 받음을 알 수 있다. 그리고, 단말에 대한 인증정보는 제어국간의 통신으로 전달한다. 현재 표준문서에는 단말의 인증 정보와 같은 중요 데이터를 전송하는 제어국간의 통신에 대한 정보보호 방안이 수립되어 있지 않다. 또한 단말이 이동하고자 하는 Target 기지국으로 핸드오버 했을 때, 단말이 접속을 시도하는 기지국이 적합한 기지국인지 확인할 수 있는 인증절차가 필요하다. 또한 단말이 핸드오버하는 동안 기존의 Serving 기지국이 단말에 전달해야 할 데이터를 버퍼링하고 있다가 핸드오버가 완료되면 Target 기지국에 접속되어 있는 해당 단말에게 안전하게 데이터를 전송하는 방안이 필요하다.

5. 결 론

지금까지 국내 휴대인터넷 1차 표준문서의 보안 구조와 보안 취약성 측면에서 살펴보았다.

휴대인터넷의 기밀성 측면에서 데이터 트래픽을 암호화 하기 위해 사용하는 암호 알고리즘으로 DES의 CBC 모드를 사용하는 것은 취약하다. DES 외에 추가적인 새로운 알고리즘을 제공하는 방안이나 DES보다 효율적이면서 하드웨어 구현이 용이한 국제 표준인 AES 알고리즘을 추가하는 방안 등을 고려해야 한다. 무결성 측면에서도 에러검증을 위한 CRC 대신 암호학적으로 무결성을 검증할 수 있는 MIC (Message Integrity Code)을 사용하고, MIC 계산을 위한 알고리즘을 제공하는 방안이나 그외 추가적인 데이터 인증을 위한 방안도 고려해야 한다. 또한, 핸드오버에 관한 적절한 정보보호 방안 및 다른 통신망과의 상호연동시 인증문제에 관한 방

안도 고려해야 한다.

현재 국내 휴대인터넷 보안 규격은 IEEE 802.16의 보안 규격을 따르고 있으며, 국내에서 보안 규격에 대한 연구는 아직 활발하지 않은 상태에 있다.

향후 국내 휴대인터넷의 정보보호 서비스를 제공하기 위해 휴대인터넷 보안 취약성 분석과 그에 따른 정보보호 방식에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] TTAS.KO-06.0065, "2.3GHz 휴대인터넷 표준(매체접근제어계층)", TTA PG302, 2004

[2] IEEE P802.16-2004, "Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE 802.16WG, 2004.

[3] 홍대형, "TTA 휴대인터넷 표준화 동향", 한국통신학회, September 2004.

[4] DES Challenge III Broken in Record 22 Hours, http://www.rsasecurity.com/press_release (2004.11.29)

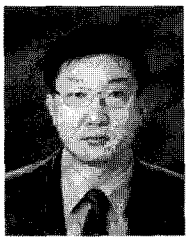
[5] A. Menezes, P. Oorschot and S. Vanstone "Handbook of Applied Cryptography," CRC Press, 1996.

[6] J. Walker, "Unsafe at Any Key Size: an Analysis of the WEP Encapsulation," Tech. Rep. 03628E, IEEE 802.11 committee, March 2000.

[7] TTAR.KO-0016, "2.3GHz 휴대인터넷 무선접속 기술 평가기준", TTA PG302, 2004.

[8] TTAR.KO-0020, "2.3GHz 휴대인터넷 서비스 요구사항 및 네트워크 참조 모델", TTA PG302, 2004.

윤 이 중



2002 충남대학교 컴퓨터공학(박사)
1991~2000 ETRI 정보보호연구단
2000~현재 국가보안기술연구소 책임연구원
관심분야 : 시스템 보안, 접근제어
E-mail : yej@etri.re.kr