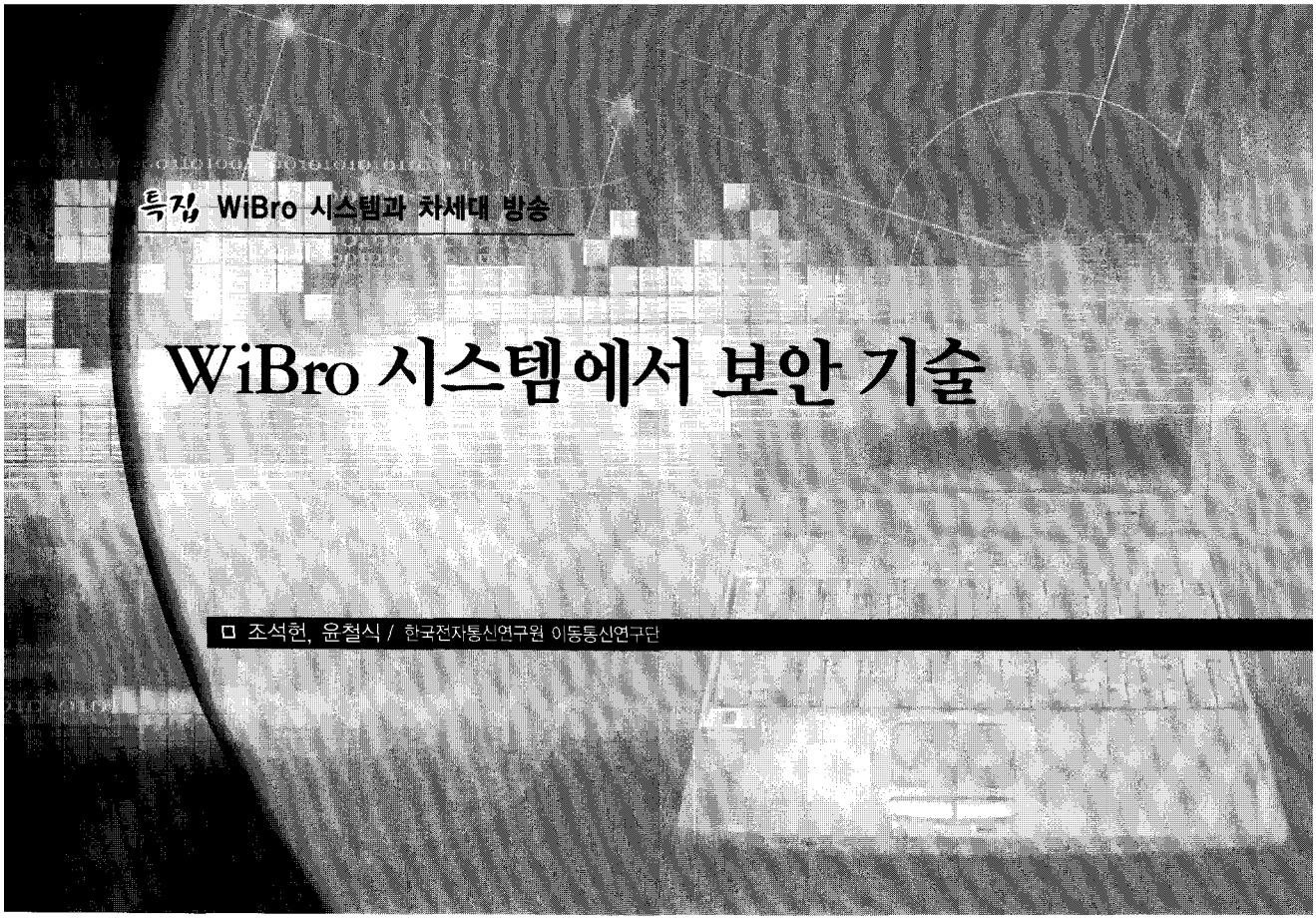


특집 WiBro 시스템과 차세대 방송

WiBro 시스템에서 보안 기술

□ 조석헌, 윤철식 / 한국전자통신연구원 이동통신연구단

1. 개 요

본 논문에서는 IEEE 802.16 Wireless MAN 시스템을 기반으로 하고 있는 휴대인터넷시스템인 WiBro 시스템에서 단말과 기지국 사이인 무선 구간에서의 보안 기술에 대한 전반적인 개념을 설명하고자 한다.

WiBro 시스템의 망 전체적으로 효율적인 관리와 안전한 서비스 제공을 위해서 보안 기능은 무엇보다도 중요한 기능이다. WiBro 시스템에서 보안 기능은 크게 트래픽 패킷 데이터에 대한 암호화 및 복호화를 수행하는 암호화 프로토콜 (Encapsulation protocol) 부분과 기지국과 단말 사이의 무선 링크상에서 사용되어지는 모든 키들을 안전하게 생성하고 공유하기 위해 정의하는 보안 키 관리 (PKM: Privacy Key Management) 프로토콜 부분으로 구성되어 있다. 하지만, WiBro 시스템의 보안 계층에서는 암호 알고리즘들을 새롭게 정의하는 것이 아니라 기존에 널리 알려진 암호 비도가 높은 알고리즘 (예: AES: Advanced Encryption Standard)들을 암호화 프로토콜 부분에 단순히 채택하여 사용하는 개념이다. 따라서, WiBro 시스템에서는 채택한 알고리즘을 보다 효율적으로 이용하면서도 다양한 키들을 안전하게 전달하고 관리하기 위한 PKM 프로토콜 개발에 역점을 두고 있다.

현재 WiBro 시스템에서는 크게 두 개의 PKM 프로토콜이 존재한다. IEEE 802.16 #32번째 회의를 통해 IEEE 802.16 TGe에 기존에 정의되어 있던 PKM 프로토콜 (PKMv1)보다도 비도가 높은 새로운 PKM 프로토콜 (PKMv2)을 제시하였다. 이 장에서는 강력하고 새로운 PKM 프로토콜인 PKMv2를 다루도록 하겠다. 또한, WiBro 시스템에서 실제적으로 사용되고 있는 보안 기술들에 대해서도 다루

도록 하겠다.

본 논문의 구성은 다음과 같다. 제 2장에서는 WiBro 시스템에서 실제적인 인증 절차 수행 전에 필요한 보안 관련 파라미터들을 협상하는 방법에 대해 설명하고, 제 3장에서는 WiBro 시스템에 채택한 PKMv2에서 정의한 인증키 체계 구조, 인증 절차, 그리고 메시지 인증 기능 및 트래픽 데이터 암호화 기능들에 대해 설명한다. 제 4장에서는 단말의 핸드오버 시 지원되어야 할 인증 기능에 대해 언급하고, 마지막으로 제 5장에서는 WiBro 시스템의 보안 기술에 대한 결론을 통해 본 논문을 마무리 짓고자 한다.

2. 보안 관련 파라미터 협상

WiBro 시스템에서는 단말 장치 및 기지국 장치 그리고 사용자에 대한 실제적인 인증을 수행하기 전에 단말과 기지국 사이의 보안 관련 파라미터를 협상한다. 단말은 자신이 지원 가능한 모든 보안 관련 정보를 SBC-REQ (SS Basic Capability Request) 메시지에 포함시키고 이 SBC-REQ 메시지를 기지국으로 전송함으로써 보안 관련 파라미터 협상을 요청한다. 이 SBC-REQ 메시지를 수신한 기지국은 단말이 지원 가능한 모든 보안 관련 정보와 기지국 자신이 지원 가능한 보안 관련 정보를 비교하여 앞으로 단말과 기지국 사이에서 사용할 보안 관련 정책들을 최종적으로 선택한다. 기지국은 이 협상된 보안 관련 정보를 SBC-RSP (SS Basic Capability Response) 메시지에 포함시키고 이 SBC-RSP 메시지를 단말로 전송함으로써 보안 관련 파라미터 협상을 완료한다.

SBC-REQ/RSP 메시지를 통해 협상되는 대표적인 보안 관련 파라미터들을 〈표 1〉에 보였다.

〈표 1〉 보안 관련 파라미터

인증 버전	인증 정책	메시지 인증 코드 방식
PKMv1	RSA 기반 인증	HMAC
PKMv2	RSA 기반 인증	HMAC
	EAP 기반 인증	short HMACs
	인증된 EAP 기반 인증	CMAC

WiBro 시스템에는 두 개의 PKM 프로토콜이 존재하고 있다. 단말과 기지국이 이 두 개의 PKM 프로토콜 버전에 대한 협상은 SBC-REQ/RSP 메시지에 포함된 인증 버전 (PKM version) 필드를 통해 이루어진다.

또한, 이 인증 버전에 따라 다양한 인증 정책들이 PKM 프로토콜에 정의되어 있다. PKMv1에는 RSA (Rivest Shamir Adleman) 기반의 인증 정책만이 정의되어 있다. 이 RSA 기반의 인증 정책은 오직 단말 장치에 대한 인증을 수행하는 것을 특징으로 한다. 이와는 달리, PKMv2에는 RSA 기반의 인증 정책, EAP (Extensible Authentication Protocol) 기반의 인증 정책과 선 수행된 RSA 또는 EAP를 통해 얻은 키를 가지고 보다 안전하게 EAP 기반의 인증을 수행하는 인증된(authenticated) EAP 기반의 인증 정책들이 존재한다. PKMv2에서 RSA 기반의 인증 정책은 단말 장치 뿐만 아니라 기지국 장치에 대한 상호 인증 수행을 특징으로 한다. EAP 기반의 인증 정책과 인증된 EAP 기반의 인증 정책은 단말 또는 기지국 자체의 장치 인증 뿐만 아니라 사용자 인증을 MAC (Medium Access Control) 계층이 아닌 상위 EAP 인증 프로토콜을 (예: TLS: Transport Layer Security, AKA: Authentication and Key Agreement, 등등) 통해 수행하는 것을 특징으로 한다. 단말과 기지국은 다양한 인증 정책에 대한 협상은 SBC-REQ/RSP 메시지에 포함된 인

증 정책 지원 (Authorization Policy Support) 필드를 통해 이루어진다. 특히, WiBro 시스템의 서비스 사업자 정책에 따라 시스템 성능 향상을 위해 인증 절차가 생략될 수 있으며, 이러한 사항도 인증 정책 지원 필드를 통해 협상된다.

게다가, WiBro 시스템에서는 인증 버전에 따라 다양한 메시지 인증 코드 (MAC: Message Authentication Code) 방식들이 정의되어 있다. 이 메시지 인증 코드는 단말과 기지국 사이에 교환되는 메시지에 대한 인증 기능을 지원하기 위해서 사용되는 코드이다. PKMv1에는 HMAC (Hashed Message Authentication Code)가 정의되고, PKMv2에는 HMAC, CMAC (Cipher-based Message Authentication Code), 그리고 다양한 사이즈를 가지는 short HMAC들이 정의되어 있다. 단말과 기지국은 이런 다양한 메시지 인증 코드에 대한 협상은 SBC-REQ/RSP 메시지에 포함된 메시지 인증 코드 방식 (MAC Mode) 필드를 통해 이루어진다.

현재 WiBro 시스템에서는 PKMv2만을 고려하고 있고, 단말에 PISIM (Portable Internet Subscriber Identity Module) 카드를 장착한 AKA 프로토콜을 지원하는 EAP기반의 인증정책을 통해 사용자 인증만을 수행하며 인증된 단말과 기지국 사이의 제어 메시지 교환 시 메시지 인증 코드로써 가장 강력한 CMAC만을 사용한다.

3. PKMv2에서 단말 인증

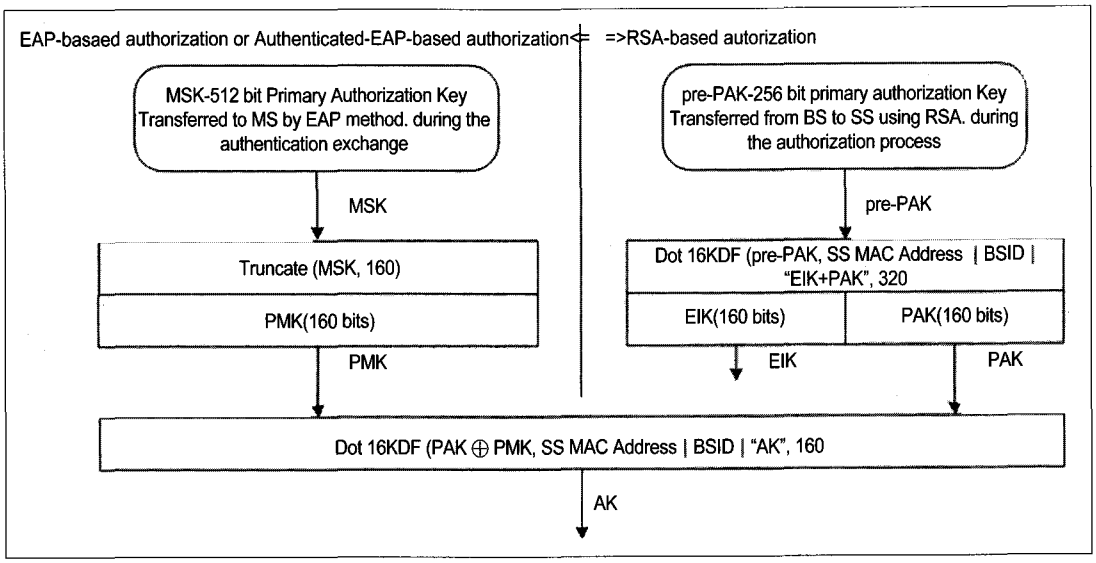
PKMv2에서는 다양한 인증 정책을 정의하고 있다. 제 2장에서 언급한 바와 같이, SBC-REQ/RSP 메시지에 포함된 인증 정책 지원 필드를 통해 단말과 기지국은 인증 정책을 협상하게 된다. 이런 협상 과정을 통해 단말과 기지국은 다양한 조합의 인증 방식으로 이루어진 인증 절차를 수행하게 된다. WiBro 시스템에서 정의되고 있는 다양한 조합의 인증 방식에는 RSA 기반 인증 정책만을 지원하는 인증 방식, EAP 기반 인증 정책만을 지원하는 인증 방식, RSA 기반 인증 정책 수행 후 EAP 기반 인증 정책 또는 인증된 EAP 기반 인증 정책을 수행하는 인증 방식, EAP 기반 인증 정책 수행 후 인증된 EAP 기반 인증 정책을 수행하는 인증 방식 그리고 인증 정책을 생략하는 인증 방식들이 존재한다.

1) PKMv2에서 인증키 체계 구조

이처럼 다양한 인증 방식을 통해 단말과 기지국이 갖게 되는 하나 이상의 기본키를 (Root Key) 통해 인증키 (AK: Authorization Key)를 공유하게 된다. 이 인증키를 생성하는 방법, 즉 인증키에 대한 키 체계 구조를 그림 1)에 도시하였다.

그림 1)에서 오른쪽 부분이 RSA 기반 인증 정책을 통해 단말과 기지국이 키 (pre-PAK: pre Primary Authorization Key)를 얻게 되었을 때 인증키를 도출하는 방법이고 왼쪽 부분은 EAP 기반 인증 정책 또는 인증된 EAP 기반 인증 정책을 통해 단말과 기지국이 키 (MSK: Master Session Key)를 얻게 되었을 때 인증키를 도출하는 방법이다. 여기에서, MSK는 단말과 인증 서버에 존재하고 있는 상위 EAP 인증 프로토콜로부터 생성되어 MAC(Medium Access Control)으로 전달되는 키이다.

먼저, RSA 기반 인증 정책을 지원하여 단말과 기지국이 pre-PAK를 가지게 된 경우에 있어서, EIK (EAP Integrity Key)와 PAK (Primary Authorization Key)들은 Dot16KDF (pre-PAK, SS_MAC_Address | BSID | "EIK+PAK", 288)를



〈그림 1〉 PKMv2에서 인증키 체계 구조

통해 도출할 수 있다. 여기에서 SS_MAC_Address는 단말의 MAC(Medium Access Control) 주소로서 단말의 식별자 역할을 하고, BSID는 기지국의 식별자 역할을 한다. 이 방법을 통해 얻어진 키의 상위 128비트가 EIK이고 하위 160비트가 PAK이다. 이 Dot16KDF의 정확한 사용 방법은 IEEE Std 802.16-2005 규격서의 7.5.4.6.1절을 참조하면 된다 [2]. EIK는 RSA 기반 인증 절차를 수행한 후 인증된 EAP 기반 인증 절차를 수행할 시 메시지 인증을 위해 사용되는 키이다. PAK를 가지고 Dot16KDF (PAK, SS_MAC_Address | BSID | "AK", 160)을 통해 인증키를 도출할 수 있다.

EAP 기반 인증 정책 또는 인증된 EAP 기반 인증 정책을 지원하여 단말과 기지국이 MSK를 가지게 된 경우에 있어서, PMK (Pairwise Master Key)는 Truncate (MSK, 160)를 통해 도출할 수 있다. 즉, MSK의 최상위 160비트가 PMK이다. 인증키는 Dot16KDF (PMK, SS_MAC_Address | BSID | "AK", 160)을 통해 도출할 수 있다. 현재 WiBro 시스템에서 고려하고 있는 PISIM을 이용한 AKA 프로토콜을 지원하는 EAP기반의 인증 정책이 여기에 해당된다.

마지막으로, RSA 기반 인증 정책과 EAP 기반 인증 정책 또는 인증된 EAP 기반 인증 정책을 공히 지원하여 단말과 기지국이 pre-PAK와 MSK를 가지게 된 경우에 있어서, 그림 1)과 같이 PAK와 PMK를 도출할 수 있다. 이 PAK와 PMK를 Dot16KDF (PAK⊕PMK, SS_MAC_Address | BSID | "AK", 160)의 입력으로 사용하여 인증키를 도출할 수 있다.

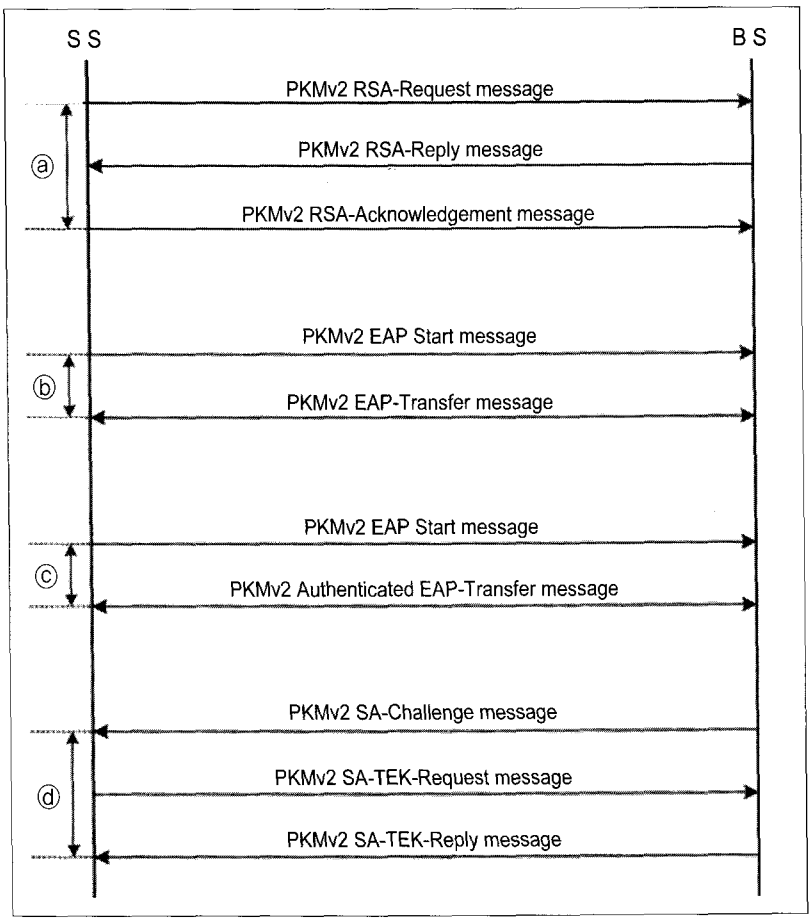
이처럼 다양한 인증 정책을 통해 도출된 인증키는 단말 인증 절차 후에 단말과 기지국 사이에 교환되는 모든 제어 메시지에 대한 메시지 인증을 위해 사용되는 메시지 인증키 (예: CMAC_Key_D, CMAC_Key_U 등등)의 입력키가 된다. 게다가, 단말과 기지국 사이의 무선 링크에서 송·수신되는

트래픽 데이터를 암호화하기 위해 사용되는 트래픽 암호화 키 (TEK: Traffic Encryption Key)를 기지국이 생성하고 이를 단말에게 전달하는데, 이 때 트래픽 암호화 키를 안전하게 전달하기 위해서 트래픽 암호화 키 자체도 키 암호화 키 (KEK: Key Encryption Key)를 통해 암호화한다. 여기에서, 키 암호화 키를 생성할 때에 인증키를 입력키로 사용한다. 이로써, 권한 검증이 된 단말과 기지국 사이에는 안전한 제어 메시지 교환 뿐만 아니라 트래픽 데이터 전송도 가능한 것이다.

2) PKMv2에서 인증 절차

인증 정책 필드를 통해 협상된 다양한 인증 정책에 따라 사용되는 단말 인증 절차와 그 때 사용되는 메시지들에 대하여 그림 2)에 도시하였다.

RSA 기반의 인증 정책을 지원할 경우, ⓐ부분과 같이 PKMv2 RSA-Request 메시지, PKMv2 RSA-Reply 메시지와 PKMv2 RSA-Acknowledgement 메시지들을 사용한다. RSA 기반 인증을 시작하기 위해서 단말이 전송하는 PKMv2 RSA-Request 메시지에는 단말의 인증서가 포함되어 있



〈그림 2〉 PKMv2에서 단말 인증 흐름

다. 이 PKMv2 RSA-Request 메시지를 수신한 기지국은 해당 단말에 대한 장치 인증을 수행한 후 성공하였을 경우, 해당 단말에게 기지국의 인증서와 단말의 공개키 (public key)로 암호화된 pre-PAK가 포함된 PKMv2 RSA-Reply 메시지를 전송한다. PKMv2 RSA-Reply 메시지를 수신한 단말은 기지국의 인증서를 검증하고 성공하였을 경우, 기지국에게 PKMv2 RSA-Acknowledgement 메시지를 전송하면서 RSA 기반 인증 절차가 완료되는 것이다. 이 절차를 통해 단말과 기지국은 pre-PAK를 공유할 수 있게 된다.

EAP 기반의 인증 정책을 지원할 경우, ⓑ부분과 같이 PKMv2 EAP-Start 메시지와 PKMv2 EAP-Transfer 메시지가 사용된다. 단말이 망의 EAP 프로토콜에게 EAP 기반 인증 절차의 시작을 통보하기 위하여 기지국으로 PKMv2 EAP-Start 메시지를 전송한다. 이를 수신한 기지국은 망의 EAP 프로토콜에 EAP 인증 절차 시작을 통보한다. 이후, 상위 EAP 인증 프로토콜의 절차에 따라 여러 번의 PKMv2 EAP-Transfer 메시지가 단말과 기지국 사이에 교환된다. 즉, 단말과 기지국의 MAC (Medium Access Control)은 PKMv2 EAP-Transfer 메시지를 통해 상위 EAP 인증 프로토콜에서 사용되는 EAP 데이터 (EAP payload)만을 단순하게 상대 기지국 또는 단말에게 전달한다. 사용하는 상위 EAP 인증 프로토콜이 키를 생성하는 프로토콜 (예: TLS 또는 AKA)인 경우에는, 이 절차를 통해 단말과 기지국은 MSK를 공유할 수 있게 된다.

인증된 EAP 기반의 인증 정책을 지원할 경우, ⓒ 부분과 같이 PKMv2 EAP-Start 메시지와 PKMv2 Authenticated-EAP-Transfer 메시지가 사용된다. 이 인증된 EAP 기반의 인증 절차는 RSA 기반의 인증 절차 (ⓐ)나 EAP 기반의 인증 절차 (ⓑ)가 선행되어야 한다. 왜냐하면, PKMv2 Authenticated-EAP-Transfer 메시지는 PKMv2 EAP-Transfer 메시지와 달리 메시지 인증 기능이 추가된 메시지이고 메시지 인증 시 필요한 EIK는 미리 수행된 RSA 기반의 인증 절차나 EAP 기반의 인증 절차를 통해 도출되는 키이기 때문이다. 인증된 EAP 기반 인증 절차를 통해서도 단말과 기지국은 상위 EAP 인증 프로토콜 특성에 따라 MSK를 공유할 수 있다.

위 열거한 절차 (ⓐ나 ⓑ 또는 ⓒ)들을 통해 단말과 기지국은 공유한 pre-PAK 또는 MSK를 가지고 그림 1)과 같은 인증키 생성 방법을 통해 인증키를 공유한다. 하지만, 인증키에 대한 일련번호, 유효시간 그리고 SA-ID (Security Association Identifier)와 각각의 SA마다 사용될 알고리즘들을 단말과 기지국이 공유해야 하는데, 이를 위해 ⓓ부분과 같이 3-Way SA-TEK 절차를 사용한다. SA에 대한 설명은 다음 3.3절에 설명한다. 인증키를 도출한 기지국은 단말로 인증키의 일련번호와 유효시간이 포함된 PKMv2 SA-TEK-Challenge 메시지를 전송한다. 이를 수신한 단말은 기지국으로 단말 자신이 지원 가능한 암호화 알고리즘들을 알려주기 위해서 PKMv2 SA-TEK-Request 메시지를 전송한다. PKMv2 SA-TEK-Request 메시지를 수신한 기지국은 단말에게 제공 가능한 primary SA와 다수개의 static SA들에 해당하는 SA-ID와 각 SA에 해당하는 암호 알고리즘을 PKMv2 SA-TEK-Response 메시지를 통해 알려줌으로써 3-Way SA-TEK 절차가 완료된다. 이로써, 단말 또는 기지국에 대한 장치 인증이나 사용자 인증 절차가 최종적으로 완료되는 것이다.

3) 메시지 인증과 트래픽 데이터 암호화

WiBro 시스템에서 기지국과 인증된 단말 사이에 송·수신되는 메시지에 대한 인증 기능과 트래픽 데이터에 대한 암호화 기능들이 존재한다. 메시지 인증과 트래픽 데이터 암호화를 위해 다양한 알고리즘들을 사용한다. 이 때 사용되는 알고리즘들과 사용 방법들은 IEEE 802.16 규격서들을 참조한다[1][2]. 현재 WiBro 시스템에서는 정의된 다양한 암호 알고리즘들 중에서 가장 강력한 AES (Advanced Encryption Standard)알고리즘을 사용하기를 권고하고 있다.

단말과 기지국 사이에 전달되는 신호 메시지에 대한 인증을 위해 PKMv2에서는 협상된 메시지 인증 코드 방식 필드값에 따라 HMAC, CMAC 또는 다양한 short-HMAC들 중 하나의 메시지 인증 방식이 사용된다. 물론, WiBro 시스템 서비스 사업자 정책에 따라 시스템 성능 향상을 위해 신호 메시지에 대한 인증 기능을 생략할 수도 있다. 단말 또는 기지국은 협상되지 않은 메시지 인증 코드 방식이 포함된 메시지를 수신하거나 틀린 메시지 인증 코드 값이 포함된 메시지를 수신하였을 경우에는 해당 메시지를 폐기한다.

단말과 기지국 사이에 통신되는 트래픽 데이터에 대한 암호화를 실행할 수 있다. 이를 위해 한 단말당 한 개 이상의 SA (Security Association)를 관리한다. 여기에서 SA는 트래픽 데이터를 암호화하는데 사용되는 트래픽 암호화 키 관련 정보들의 집합을 의미하고 이 SA에는 SA의 식별자인 SA-ID, 해당 SA에 사용되는 암호화 알고리즘, 트래픽 암호화 키 (TEK), CBC-IV (Cipher Block Chaining - Initial Vector), PN (Packet Number) 등이 포함되어 있다.

SA들을 단말과 기지국 사이에 공유하기 위해서 트래픽 암호화 키 생성 및 분배 절차를 수행한다. 트래픽 암호화 키 생성 및 분배 절차에는 PKMv2 Key-Request 메시지와 PKMv2 Key-Reply 메시지가 정의된다. 단말은 PKMv2 Key-Request 메시지를 기지국으로 전송하여 특정 SA에 대한 트래픽 암호화 키 생성을 요청하고 이 메시지를 수신한 기지국은 트래픽 암호화 키를 생성하여 해당 단말에게 트래픽 암호화 키가 포함된 PKMv2 Key-Reply 메시지를 송신함으로써 트래픽 암호화 키 생성 및 분배 절차가 완료된다.

모든 트래픽 연결 (traffic connection)에는 하나의 SA에 매핑 (mapping)된다. Secondary connection은 primary SA에 매핑되고, MBS (Multicast and Broadcast Service)와 같은 멀티캐스트 서비스 연결 (multicast service connection)은 static SA나 dynamic SA에 매핑되며, 유니캐스트 서비스 연결 (unicast service connection)은 기 정의된 SA에 매핑된다. 서비스 사업자 정책에 따라 모든 트래픽 연결은 단 하나의 SA에 매핑시킬 수 있거나 보다 안전성을 고려하여 각각의 트래픽 연결을 서로 다른 SA에도 매핑시킬 수도 있다. 또한, 트래픽 데이터에 대한 암호화 기능도 생략할 수 있다.

4. 핸드오버에서의 인증 기능

WiBro 시스템은 이동하는 단말들에 대한 끊임없는 서비스 제공을 목적으로 하고 있다. 이러한 목적을 만족시키기 위해서 단말의 핸드오버 (Handover) 상황에서의 효율적인 인증 기능을 지원해야 한다.

핸드오버를 시도하는 단말에 대한 인증 시나리오는 단말과 현재 서비스를 제공하는 기지국 사이에 수행될 핸드오버 절차인 MOB_BSHO-REQ 메시지와 MOB_BSHO-RSP 메시지 그리고 단말과

단말이 핸드오버를 시도하려는 새로운 기지국 사이에 수행될 레인징 절차인 RNG-RSP 메시지에 포함된 핸드오버 프로세스 최적화 (HO Process Optimization) 필드와 핸드오버 인증 정책 지원 (HO Authorization Policy Support) 필드에 의해 정해진다.

여기에서, 핸드오버 프로세스 최적화 필드를 통해 단말이 새로운 기지국으로 핸드오버하였을 경우, 단말과 새로운 기지국 사이의 단말 인증 절차의 생략 여부와 트래픽 암호화 키 생성 및 분배 절차 생략 여부를 결정하게 된다. 만약, 이 두 가지 절차를 모두 생략하게 된다면, 단말의 새로운 기지국으로 빠른 핸드오버가 수행될 수 있다.

또한, 핸드오버 인증 정책 지원 필드를 통해 단말과 새로운 기지국과의 주기적인 재 인증을 위해 사용될 인증 정책과 단말과 새로운 기지국 사이에 교환될 제어 메시지에 대한 메시지 인증을 위해 사용되는 메시지 인증 코드 방식을 협상한다.

핸드오버 상황에서의 위와 같은 인증 시나리오를 통해 단말이 끊임없는 트래픽 데이터 서비스를 제공받을 수 있는 것이다.

5. 결 론

차세대 통신 시스템으로서 각광받고 있는 WiBro 시스템의 다양한 서비스를 안전하게 제공하기 위해서 강력한 보안 기술은 필수적인 사항이다.

WiBro 시스템을 이용하는 각각의 사용자들에 대한 인증을 수행하기 위해 PISIM을 이용한 AKA 프로토콜을 지원하는 EAP 기반의 인증 정책을 지원해야 한다. 권한 검증된 사용자들이 사용하는 단말과 기지국 사이에 인증키를 공유하게 되고 이러한 인증키를 통해 두 노드 간에 제어 메시지 뿐만 아니라 다양한 트래픽 데이터를 안전하게 교환할 수 있게 된다.

또한, 이동하는 단말들에 대해서 끊임없이 WiBro 서비스를 제공하기 위해서 단말의 핸드오버 상황에서도 효율적인 인증 기능을 지원하고 있다.

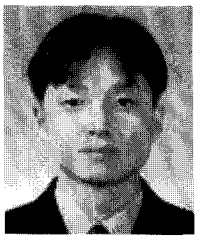
WiBro 시스템에 대한 표준화 규격 작업이 완료되었기 때문에 이젠 한국에서 곧 서비스할 WiBro 서비스가 사용자들에게 안전하게 제공되기를 기대하는 바이다.

참 고 문 헌

[1] IEEE Std 802.16-2004, "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," 2004. 10

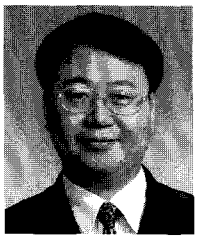
[2] IEEE Std 802.16-2005, "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," 2006. 2

필 자 소 개



조 석 헌

- 2000. 2 전북대학교(학사)
- 2002. 2 광주과학기술원 대학원(석사)
- 2002. 2~현재 ETRI 이동통신연구단 WiBro 표준 연구팀
- 2004. 11~ IEEE 802.16 표준화 활동, WiBro 시스템 TTA 규격서 작성 (보안 기술 부분)
- E-mail:chosh@etri.re.kr



윤 철 식

- 1988. 2 서울대학교(학사)
- 1990. 2 포항공대 대학원(석사)
- 2000. 2 서강대학교 대학원 (박사수료)
- 1993. 2~현재 ETRI 이동통신연구단 휴대인터넷표준연구팀장
- E-mail:csyoon@etri.re.kr