WiMAX 환경에서 악의적 노드 예방을 위한 보안 기법

정윤수*, 김용태**, 박길철***, 이상호****

Security Scheme for Prevent malicious Nodes in WiMAX Environment

Yoon-Su Jeong*, Yong-Tae Kim**, Gil-Cheol Park*** and Sang-Ho Lee****

이 논문은 2008년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음

요 약

이동 단말기의 사용이 일반화되면서 최근 WiMAX 기술의 다양한 서비스 요구가 점점 증가하여 보안의 중요성이 점점 대두되고 있다. 이러한 보안 요구사항을 충족시키기 위해서 WiMAX에 전통적인 1 홉 네트워크 보안 기법이 적용되더라도 이동 WiMAX에서는 이웃 링크 설립과정과 TEK 교환 과정사이에 비연결적으로 동작이 이루어져서 악의적인 공격에 쉽게 공격당할 수 있는 문제점을 가지고 있다. 이 논문에서는 이동 WiMAX의 보안 요구사항을 충족하기 위해 IEEE 802.16e 표준에서 제공하는 기본 기능이외에 WiMAX의 이웃 링크 설립 과정과 TEK 교환 과정사이를 안전하게 연결하는 보안 연계 메커니즘을 제안한다. 제안 메커니즘에서는 SS와 BS가 생성한 임의의 난수와 비밀값을 이웃 링크 설립과 TEK 교환 과정의 공개키에 적용하여 SS와 BS에 대한 보안기능을 강화하였다. 또한 이웃 링크 설립과정과 TEK 교환 과정의 암호학적 연결을 통해 TEK 요청에서 발생할 수 있는 man-in-the-middle 공격과 같은 내부 공격을 예방할 수 있다.

ABSTRACT

As the use of mobile device is popularized, the needs of variable services of WiMAX technique and the importance of security is increasing. There is a problem that can be easily attacked from a malicious attack because the action is achieved connectionlessly between neighbor link establishing procedure and TEK exchange procedure in mobile WiMAX even though typical 1 hop network security technique is adapted to WiMAX for satisfying these security requirement. In this paper, security connected mechanism which safely connects neighbor link establishing procedure of WiMAX and TEK exchange procedure additional to the basic function provided by IEEE 802.16e standard to satisfy security requirement of mobile WiMAX is proposed. The proposed mechanism strengthens the function of security about SS and BS by applicating random number and private value which generated by SS and BS to public key of neighbor link establishing procedure and TEK exchange procedure. Also, we can prevent from inside attack like man-in-the-middle which can occur in the request of TEK through cryptographic connection of neighbor link establishing procedure and TEK exchange procedure.

키워드

WiMAX, 키 관리(Key Management), 보안 협상(Security Association)

* 충북대학교 전자계산학과(제1저자)

** 한남대학교 멀티미디어학부 강의전담 교수

*** 한남대학교 멀티미디어학부 교수

**** 충북대학교 전기전자 컴퓨터공학부 교수(교신저자)

접수일자 2008. 08. 14

Ⅰ. 서 론

최근 이동 단말기(ex. 노트북, PDA)의 사용이 일반화되면서 인터넷 기반의 다양한 서비스와 애플리케이션의 요구가 점차 증가하고 있다. 이와 같은 추세에 맞추어 IEEE 802.16 워킹 그룹은 저속 이동성과 사용자들의 요구를 충족시키기 위한 IEEE 802.16 표준안을 2004년과 2005년에 제정하였다[7,8].

IEEE 802.16e-2005 표준안이 개정된 이후에 IEEE 802.16e 기반 네트워크에 존재할 수 있는 보안 취약성 및 공격 가능성에 대해서 많은 연구가 수행되었다[12,13]. 이동 WiMAX(World wide Interoperability for Microwave Access)는 이동성을 지원하지 않는 IEEE 802.16 표준에 비하여 다양한 보안 기능을 지원하지만 무선 네트워크 환경의 보안 요구사항을 완벽하게 지원하지 못하는 문제점 있다[9,10,11].

이동 WiMAX 환경에서는 사용자가 고정되어 있지 않고 네트워크간 이동이 수시로 이루어지기 때문에 이때마다 사용자를 인증하여 통신을 수행하기에는 베이스 스테이션과 ASN의 부하가 증가하는 문제점이 있다. 이동 WiMAX의 보안 문제점을 해결하기 위해서 IEEE 802.16e 표준에서는 가입자(SS:Subscriber Station)와 베이스 스테이션(BS : Base Station) 사이의 안전한 통신을 지원하기 위해 기본(Primary), 동적(Dynamic) 그리고 고정(Static) SA의 보연연관(Security Association:SA)을 제공한다. SA는 가입자와 베이스스테이션 사이에 데이터 보안 협상을 위해 CID(Connection ID)와 SAID(Security Association ID)가 사용되지만 CID와 SAID만으로는 무선 환경에서 발생될 수 있는 보안공격에 안전하지 않으며 IEEE 802.16e 표준에서 제공하는 기본 보안기능 이외에 보안 공격에 안전한 보안 메커니즘이 추가적으로 필요하다.

이 논문에서는 WiMAX 표준에서 제공하는 이웃 링크 설립과 TEK 교환 과정 사이에서 생성되는 보안 파라미터의 비연관성으로 인해 발생되는 보안 문제를 해결하기 위해서 이웃 링크 설립과정과 TEK 교환 과정을 연관지울 수 있는 보안 연관 메커니즘을 제안한다. 제안 메커니즘에서는 SS와 BS가 생성한 임의의 난수와 비밀값을 이웃 링크 설립과 TEK 교환 과정에 사용되는 공개키에 적용하여 가입자와 베이스 스테이션에 대한 보안을 강화하고 있다. 또한 이웃 링크 설립과정과 TEK 교환 과정의 암호학적 연결을 통해 TEK 요청에서 발생할 수 있는 man-in-the-middle 공격과 같은 내부 공격을 예방할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 이동 WiMAX의 개념 및 보안에 대해서 분석한다. 3장에서는 이동 WiMEX 환경의 링크 키 설립과정과 TEK 키 생성 사이에서 발생할 수 있는 보안 문제점을 해결하기 위한 보안 연관 메커니즘을 제시하고, 4장에서는 제안 메커니즘에 대해서 발생가능한 보안 공격유형에 따른 보안평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련 연구

2.1 이동 WiMAX

이동 WiMAX는 고정 WiMAX에 이동성을 추가한 IEEE 802.16e 표준 기반의 광대역 무선 네트워크 기술이다[1,3]. 802.16e 표준은 유선에서 제공하는 xDSL, ISDN, CATV등의 기술을 대신하여 도심 지역에서 이동성을 가지는 사용자에게 무선 서비스를 제공하기 위한 표준이다[2]. 이동 WiMAX 네트워크 참조 모델은 그림 1과 같다.

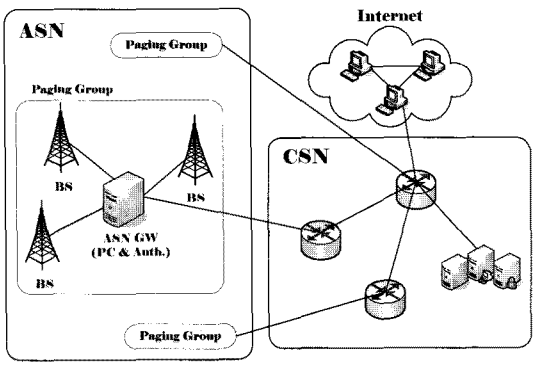

그림 1. 이동 WiMAX 네트워크 참조 모델
Fig. 1 Mobile WiMAX Network Reference Model

그림 1의 이동 WiMAX 네트워크는 액세스 서비스 네트워크(ASN: Access Service Network), 연결 서비스 네트워크(CSN: Connectivity Service Network)로 구성된다. BS와 ASN 게이트웨이로 구성된 액세스 서비스 네트워

크는 이동 가입자에게 주파수 접근을 제공하고 연결 서비스 네트워크는 이동 가입자(Mobile Subscriber)의 IP 연결 서비스를 제공한다. BS는 셀의 중앙에 위치하며 각각의 이동 가입자에게 직접적인 주파수 연결을 제공한다.

ASN 게이트웨이는 ASN의 가장자리에 위치하며 연결 서비스 네트워크와 BS들을 연결해주는 게이트웨이 역할을 한다. 또한 ASN 게이트웨이는 인증자(Authenticator)와 페이징 제어(PC: Paging Controller)의 역할을 한다. ASN 게이트웨이의 인증자는 각 가입자의 PMK(Primary Master Key)를 저장하고 BS를 위해 PMK로부터 생성된 AK 문맥(context)을 제공한다. 페이징 제어 역할을 하는 ASN 게이트웨이는 정지(idle) 모드의 이동 가입자 목록을 저장하고 이동 가입자들을 페이지하기 위해 BS과 직접 통신을 한다.

2.2 이동 WiMAX 보안 분석

2004년 IEEE 802.16 표준이 발표된 이후 WiMAX 환경에서 발생 가능한 보안 문제점을 [4]에서 언급하고 있다. [4]에서 언급한 WiMAX의 문제점은 데이터 패킷과 인증 패킷을 위한 메시지 무결성 코드 부족, 베이스 스테이션에서의 인증 부족 그리고 TEK와 AK 키 생성및 라이프타임의 불안정 등이다. [4]에서 언급한 보안 문제점을 해결하기 위해서 [5]는 난수와 타임스탬프를 PKM 프로토콜에 적용하였고 [6]은 형식적 보안 분석을 통해 이동 WiMAX의 보안이 무선 환경에서 매우 취약함을 증명하였다.

이동 WiMAX의 인증을 수행하기 위해서는 SS가 중앙 서버와 인증을 수행하도록 접근제어 기능을 수행하는 BS와 같은 노드가 필요하다. 만일 BS가 직접적으로 도달할 수 없다면 네트워크에 진입한 SS는 BS에 도달하기 위해 멀티 홉 연결을 사용해야 한다.

Ⅲ. 이웃 링크 설립 과정과 TEK 교환 과정 사이의 보안 연계 메커니즘

이 절에서는 이웃 링크 설립과정과 TEK 교환 과정의 보안 연계를 구축하기 위해 그림 2와 같이 인증 정보에 대한 키 정보를 이웃 링크 설립과정과 TEK 교환과정에 적용하는 보안 연계 메커니즘을 제안한다. 이웃 링크 설립 과정에서는 네트워크에 진입한 노드들의 상호인증을 통해 노드간링크 설립을 수행하는 과정을 나타내며, TEK 교환 과정에서는 이웃 링크 설립과정에서 생성한 보안 파라미터와 AK 키를 이용하여 TEK 키를 생성하는데 필요한 정보를 BS에게 요청한 후 수신된 정보를 이용하여 SS가 TEK를 생성하는 과정을 보여주고 있다.

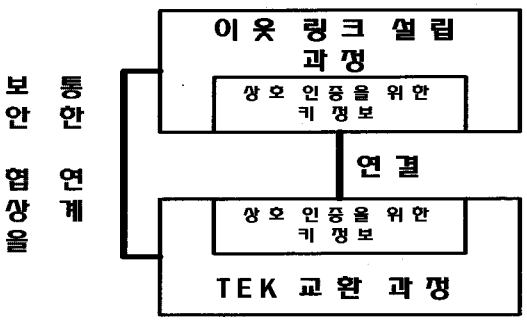

그림 2. 키 정보에 의한 연결 협상 모델
Fig. 2 Connection Association Model for Key Information

3.1 용어 정의

제안 메커니즘에서 사용하는 주요 용어를 정의하면 표 1와 같다.

표 1. 제안 메커니즘의 용어 정의
Table 1. Parameter of Proposed Mechanism

Notaion	Definitions
SS	가입자
BS	베이스 스테이션
$E_{PU_A}(X)$	A의 공개키를 가지고 X를 암호화
$S_{PR_A}(X)$	A의 개인키를 통해 메시지 X에 대한 시그너처 생성
$Cert(x)$	x의 인증서
ID_x	x의 인식자
$SAID$	보안협력 인식자
SN_x	x의 sequence number
R_x	x의 난수
$M_1 \| M_2$	M_1과 M_2의 연접

3.2 보안 연계 메커니즘

제안 메커니즘에서 사용되는 키는 IEEE 802.16 표준에서 정의된 것과 같이 안전한 통신을 위해 AK, KEK, downlink HMAC key, uplink HMAC key, TEK 등의 5개 키를 사용한다. AK는 인증 처리과정동안 BS에 의해 활성화되며 SS와 BS 사이에 공유된 비밀키로써, AK는 PKMv1에 정의된 안전한 키 교환을 위해 사용한다.

제안 메커니즘에 사용되는 128-bit AK는 BS에 의해 128-bit KEK을 생성하기 위해 사용된다. 식 1에 의해 생성되는 KEK는 TEK 암호화와 분배를 위해 사용한다.

$$KEK = Truncate\_128\{SHA1[(AK|0^{44}) \oplus 53^{64}]\} \quad (1)$$

식 1에서 AK는 $(AK|0^{44}) \oplus 53^{64}$처럼 0^{44}과 XOR한 53^{64}로 연접한다. 식 1에서 사용되는 해쉬 함수는 가장 일반적으로 사용되는 해쉬 알고리즘 SHA1를 사용한다. 식 1의 Truncate_128(.)는 KEK와 비트의 나머지를 버림으로써 해쉬 결과의 처음 128 비트를 검색한다.

TEK 교환과정에 사용되는 다운링크 HMAC키와 업링크 HMAC 키는 SS와 BS 사이에서 키 분배 메시지의 데이터 인증을 제공한다. TEK 교환 과정은 교환하는 메시지를 안전하게 송·수신하기 위해 다운링크 HMAC 키와 업링크 HMAC 키에 의존한다.

3.2.1 이웃 링크 설립 과정

이동 WiMAX 환경의 메쉬 모드에서 A는 단일 활성 링크보다도 더 많은 링크를 유지하여야 한다. 802.16 표준에서는 노드 A와 B 사이의 이웃 링크 설립(Neighbor Link Establishment)을 3 방향 핸드쉐이크로 정의하고 있지만 이웃 링크 설립과 TEK 교환의 연관성 부족으로 인하여 내부에 존재하는 악의적인 공격에 취약한 문제점을 가지고 있다. 제안 메커니즘에서는 802.16 표준의 이웃 링크 설립과정에서 발생되는 연관성 부족 현상을 해결하기 위하여 그림 3와 같이 노드 A와 노드 B가 링크 설립을 할 경우 노드 A와 노드 B가 BS에게 BS의 공개키로 암호화한 임의의 랜덤 값을 부여받도록 한 후 랜덤 값을 TEK 교환에 사용하도록 한다. 제안 메커니즘의 이웃 링크 설립 과정을 위해 8개의 과정으로 동작되는 그림 3은 BS의 랜덤값을 노드들에게 전달함으로써 BS 인증을 수행하도록 하고 있으며 메시지 부인 방지를 위하여 자신이 생성한 랜덤 값을 송·수신하여 비교하는 방식을 사용하고 있다. 또한, 내부 공격에 따른 피해를 줄이기 위하여 노드 자신이 생성한 랜덤 값을 상호 인증에 사용하고 있다.

그림 3에서 사용되는 frame number는 링크 설립이 시작되기 전에 A와 B사이에서 가져온 프레임의 흐름에서 프레임의 인식자로써 사용된다. 프레임의 무결성을 검증하기 위해서 B는 IEEE 802.16 표준에 명세화되지 않은 범위에서 현재 프레임 수로써 사용되는 다중 해쉬를 계산한다. 노드 ID는 터미널의 인식자이고 링크 ID는 설립 후 링크를 인식하기 위한 최신 값을 의미한다. HMAC() 함수는 인증된 해쉬 알고리즘을 의미한다. 그림 3의 핸드쉐이크는 B가 네트워크에 포함될 경우 A에게 보장받아야 한다. 그림 3의 과정에서 A와 B는 개인적으로 공유된 비밀값을 가지고 있지 않다.

- Step 1 : A, B ← BS
  $PU_A\{R_{BS}\}$, $PU_B\{R_{BS}\}$
- Step 2 : A, B
  Generate Cert(A. Manufacturer), Cert(B. Manufacturer),
  $PR_A\{\text{Random number}\}$, $PR_B\{\text{Random number}\}$
- Step 3 : A → B
  $HMAC\{\text{Operator Shared Secret, frame number, Node ID of Node A, Node ID of node B}\}||PU_B\{R_A\}||PU'_B\{R_{BS}\}||SAID$
- Step 4 : B
  Compare $PU_B\{R_{BS}\}$ and $PU'_B\{R_{BS}\}$
- Step 5 : A ← B
  $HMAC\{\text{Operator Shared Secret, frame number, Node ID of node B, Node ID of Node A}\}||PU_B\{R_B\}||PU'_A\{R_{BS}\}||SAID$
- Step 6 : A
  Compare $PU_A\{RBS\}$ and $PU'_A\{RBS\}$
- Step 7 : A → B
  Accept, Random unused link ID
- Step 8 : A,B → BS
  $PU'_A\{R_{BS}\}||PU'_B\{R_{BS}\}||Lifetime||SN_A||SN_B||SAIDList||S_{PR_{BS}}(A)||S_{PR_{BS}}(B)$

그림 3. 이웃 링크 설립 처리과정
Fig. 3 Process of Neighbor Link Establishment

3.2.2 TEK 교환 과정

다운링크 HMAC 키와 업링크 HMAC 키에 의존하는 TEK 교환 과정은 SS와 BS사이에서 동작된다. 제안 메커니즘에서 TEK 교환 과정의 세부적인 동작과정은 그림 4과 같다.

그림 4는 SS와 BS사이의 TEK 교환 과정을 보여주고 있다. 그림 4의 과정을 통해서 인증된 SS는 각각의 SAID에 대해 TEK 처리를 분할한다. 그림 4의 TEK 과정은 keying material의 최신성을 요청하도록 주기적으로 BS에게 TEK 키 요청 메시지를 보낸다. BS는 BS의 활성화된 keying material을 얻어 TEK 키 응답 메시지와 함께 메시지를 요청하여 TEK 키에 응답한다. TEK은 AK로부터 유도된 적당한 KEK를 사용하여 암호화한다. TEK 키 응답 메시지는 keying material의 잔존 라이프타임을 SS에게 요청하여 제공한다. 수신하는 SS는 BS가 일부 TEK을 무효화하고 향후 TEK 키 요청을 스케쥴링할 때 평가할 수 있다. TEK 과정은 SS가 명확한 AK를 가능한 오래 가지고 있을 때 활성화하고 BS는 SS가 요구할 때 최신의 keying material를 제공한다. TEK 최신 메커니즘은 SS가 BS와 함께 암호화된 트래픽을 계속적으로 교환할 수 있도록 한다.

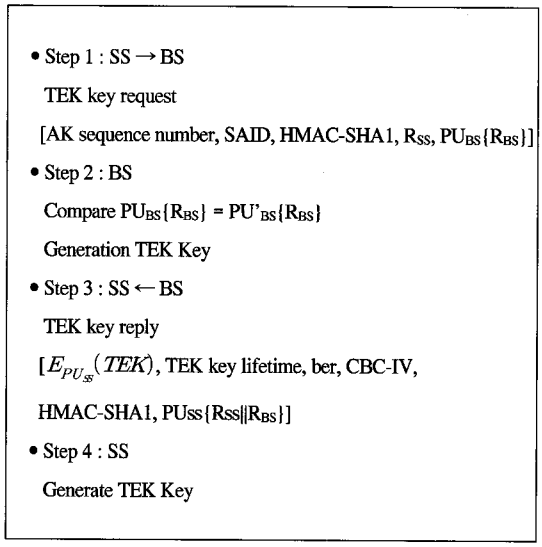

그림 4. TEK 교환 처리과정
Fig. 4 Process of TEK Exchange

그림 4의 동작과정은 크게 4가지 단계로 구성된다. 1단계에서는 SS가 BS에게 TEK 키 요청 메시지를 보낸다. 이 메시지에는 그림 3의 과정에서 생성된 BS의 랜덤값을 BS의 공개키로 암호화하여 BS에게 전달한다. 2단계는 BS가 생성한 PU_{BS} {Random number}값과 BS가 저장하고 있는 랜덤 값을 비교한 후 TEK 키를 생성한다. 단계 3에서는 그림 3에서 생성한 SS의 랜덤값과 BS의 랜덤값을 XOR하여 SS에게 전달한다. 마지막으로 단계 4에서는 SS가 가지고 있던 BS의 $PU_{BS}\{R_{BS}\}$값을 비교 후 TEK 사용 권한을 부여한다. 제안 메커니즘의 TEK 교환 과정에서 SS와 BS는 메시지의 무결성 검증을 통해 메세지 부인방지 및 내부에 존재하는 노드의 악의적인 공격을 예방할 수 있다.

Ⅳ. 평가

이 절에서는 제안 메커니즘의 보안성능을 평가하기 위해 IEEE 802.16 표준에서 지원하고 있는 알고리즘과 제안 메커니즘을 공격유형 및 인증방법에 따른 보안 평가를 수행한다.

① SS 인증 과정

제안 메커니즘의 *SS* 인증 과정에서는 *SS*와 *BS*의 상호 인증을 통해 *SS*와 *BS* 자신이 생성한 인증서를 메시지에 포함하도록 하고 있다. *SS*와 *BS*의 무결성을 보장하기 위해서 제안 메커니즘에서는 *SS*와 *BS* 자신이 생성한 난수를 권한 요청 메시지와 권한 응답 메시지에 사용한다.

② BS 인증 과정

BS 인증은 IEEE 802.16 표준에서 지원하지 않지만 제안 메커니즘에서는 *BS*의 인증서와 BS의 랜덤 값을 권한 응답 메시지에 추가하여 BS의 인증을 수행한다. 권한 응답 메시지에 포함된 타임스탬프는 *SS*를 보장하기 위해 추가되었으며, 권한 응답 메시지에 포함된 *BS*의 시그너처는 초기 메시지 인증과 부인방지를 위해 사용된다. 제안 메커니즘에서는 *BS*의 권한 요청 메시지가 이미 이전에 보낸 메시지인지를 판별하기 위해 이웃 링크 설정과 TEK 교환과정에서 BS가 생성한 임의의 랜덤수를 이용하여 무선 네트워크환경에서 가장 많이 발생하는 내부공격인 replay 공격을 예방하고 있다.

③ 키 교환 과정

제안 메커니즘의 이웃 링크 설립과정을 통해 인증과정이 수행된 후 SS는 데이터 암호화를 위해 BS에게 키 정보(TEKs)를 요청한다. 이 정보는 주기적으로 *SAID* 중에 하나를 참조하여 키 요청 메시지를 보낸다. 키 교환 구문 과정에서 발생할 수 있는 응답 공격은 2비트 길이를 가지는 *TEK*의 키 연속 변호에 의해 가능하다. 연속적인 번호는 키 응답 메시지내의 *TEK* 파라미터에 포함된다. 제안 메커니즘에서 이러한 공격을 예방하기 위해 키 교환 과정에 $Life\,Time_{AK}$를 포함하여 공격자가 *TEK* 메시지를 캡처하여 데이터 트래픽을 복호화하기 위해 필요한 정보를 획득할 수 있는 시간을 제한하고 있다.

④ 메시지 응답(message replay)/DoS 공격

메시지 응답 공격은 인증과 인증되 키 설립 프로토콜 상에서 가장 일반적인 공격중에 하나이다. 만일 인증 프로토콜에서 교환된 메시지들이 적당한 최신 인식자를 수행하지 않는다면 공격자는 쉽게 합법적인 인증 세션으로부터 복사한 메시지를 응답하여 공격자 자신을 쉽게 인증할 수 있다.

제안 메커니즘에서는 SS의 시그너처와 함께 타임스탬프의 권한 요청 메시지를 제공한다. 이렇게 추가된 파리미터들은 제안 메커니즘에서 메시지 인증을 보장하는데 사용된다. 메시지에 사용된 시그너처는 메시지 내 중요 정보를 예방하기 위해 SS의 개인키를 사용한다.

제안 메커니즘에서는 replay 공격에 노출되는 것을 막기 위해 BS는 pre-AK를 AK로 변경하여 SS게 보낸다. SS와 BS는 pre-AK로부터 AK를 추출할 수 있다. 제안 메커니즘에서는 pre-AK가 타협되는 것을 막기 위해 BS는 $Life\,Time_{AK}$를 생성하여 SS에게 전달하여 $Life\,Time_{AK}$는 주기적으로 갱신되기 때문에 공격자가 동일한 알고리즘으로 AK를 추출하더라도 공격자는 AK를 사용할 수 없다.

⑤ Man-in-the-Middle 공격

Man-in-the-Middle 공격의 경우, 공격자는 자신이 생성한 AK을 획득하여 권한 응답 메시지를 생성하고 공격한 SS의 통신과정에서 제어할 수 있다. 이러한 결과는 SS가 권한 구문 메시지를 신뢰할 수 있는 BS로부터 생성된 것인지를 판단할 수 없기 때문이다. 제안 메커니즘에서는 이러한 문제점을 해결하기 위해 SS와 BS의 상호인증과정에서 SS와 BS 자신이 생성한 임의의 ID와 난수를 수신한다.

⑥ 위조 공격

위조 공격의 경우, 공격자는 SS와 BS 사이에 위치하여 SS를 인증하기 위해 SS를 위조하고 AK를 SS에게 전달함으로써 세션을 초기화 할 수 있다. 이러한 문제를 해결하기 위해 제안 메커니즘에서는 이웃 링크 설정과 TEK 교환과정에서 SS의 임의의 랜덤 수를 BS에게 상호 인증과정 중에 등록하여 일정 시간동안 SS의 무결성을 보장받게 되어 위조 공격을 사전에 예방할 수 있도록 하였다.

⑦ 기타

WiMAX 환경에서는 이동 장비의 가장 큰 제약성으로 파워 절약 모드를 지적하고 있다. 제안 메커니즘에서는 IEEE 802.16 표준에서 지원하는 것과 같이 파워 절약 모드에서 SS는 대역폭 요청에서 휴지 모드로 설정하고 인증하지 않은 휴지 제어 메시지를 업 링크한다. 만일 공격자가 피해자 SS의 인식자와 함께 대역폭 요청과 업링크 제어 메시지를 보내면 BS는 DoS 공격을 막기위해 SS에게 메시지 전송을 멈추도록 지시한다. 이 때, 관리 프레임은 CMP-CLK 메시지와 같은 DoS 공격을 만들기 위해서 공격자에 의해 인증되지 않도록 안전하게 보낸다. Auth Invalid 메시지나 RNG-RSP 메시지는 네트워크 엔트리나 인증을 반복적으로 SS에게 사용하거나 비동기(desichronize) 클럭을 사용한다.

V. 결 론

Mobile WiMAX는 기존 이동통신 시스템에 비해 월등한 성능, 낮은 지연 시간, all-IP 핵심망 연동 가능, 그리고 진보된 QoS 및 보안 기능을 제공한다. 그러나 이와 같은 많은 장점에도 불구하고 Mobile WiMAX는 보안 관점에서 몇몇 취약성을 내포하고 있다. 이 논문에서는 IEEE 802.16e 표준에서 제공하는 기본 보안 기능이외에 SS

의 인증 부하를 줄이면서 무선 환경에서 발생하는 보안 공격(reply 공격과 man-in-the-middle 공격)에 안전한 보안 메커니즘을 제안했다. 제안된 메커니즘은 SS와 BS가 생성한 난수와 비밀값을 이용하여 TEK과 데이터 암호에 필요한 키 정보를 교환하고 SS의 초기 인증정보와 인증서를 이용하여 BS의 추가 인증 과정을 제거하여 BS의 성능 부하를 줄였다. 향후 연구에서는 무선 환경에서 발생할 수 있는 여러 보안 공격에 안전한 보안 구조 및 정책 연구를 수행할 계획이다.

참고문헌

[1] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures", 2007.

[2] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", 2006.

[3] D. Sweeney, "WiMax Operator Manual: building 802.16 Wireless Networks", Apress, 2005.

[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," IEEE Security & Privacy, vol. 2, no. 3, pp. 40-88, May/June 2004.

[5] S. Xu, M. M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in ACM Southeast Regional Conference, R. Menezes, Ed. ACM, pp. 113-118, 2006.

[6] M. Barbeau, "Wimax/802.16 threat analysis," in Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks. New York, NY, USA: ACM Press, pp. 8-15, 2005.

[7] A. Ghosh, D. R. J. Wolter, G. Andrews, and R. Chen, "Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential", IEEE Communications Magazines, vol. 43, issue 2, pp. 129~136. Feb. 2005.

[8] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", 2006.

[9] IETF RFC 4285, "Authentication Protocol for Mobile IPv6", 2006.

[10] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures", 2007.

[11] S. Xu and C.-T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions", Proceedings of the 3rd International Symposium on Wirelesss Comunication Systems (ISWCS 2006), Sep. 2006.

[12] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.

[13] S. Xu, M. Mattews and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16", Proceedings of the 44th ACM Southeast Conference(ACMSE 2006), Mar. 2006.

저자소개

정 윤수(Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2008.3 ~ 현재 충북대 및 한남대 시간강사
※관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용태(Yong-Tae Kim)

1984. 한남대학교 계산통계학과 학사.
1988. 숭실대학교 전자계산학과 석사.
1995. 충북대학교 전산학과 박사수료.
2002. 12. ~2005.2 (주)가림정보기술 이사
2006.3 ~ 현재 한남대학교 멀티미디어학부 강의전담 교수
※관심분야 : 멀티미디어, 모바일 웹서비스, Real-time Multimedia Communication

박 길철(Gil-Cheol Park)

1983. 한남대학교 전자계산학과 학사.
1986. 숭실대학교 전자계산학과 석사.
1998. 성균관대학교 전자계산학과 박사.
2006. UTAS, Australia 교환교수
1998. 8.~ 현재 한남대학교 멀티미디어학부 교수
2005. 2. 한국정보기술학회 이사 멀티미디어 분과 위원장
※관심분야 : multimedia and mobile communication, network security

이 상호(Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사.
1981. 숭실대학교 전자계산학과 석사.
1989. 숭실대학교 전자계산학과 박사.
1981. 3. ~ 현재 충북대학교 전기전자 컴퓨터공학부 교수
※관심분야 : 네트워크보안, Protocol Engineering Network Management,