韓國 컴퓨터情報學會 論文誌
第14卷 第1號, 2009. 1.

2009-14-1-3-1

WiMAX 환경에서 내부 공격의 안전성을 향상시킨 분산 키 관리 프로토콜

정 윤 수*, 김 용 태**, 박 길 철***

A Distribution Key Management Protocol for improving Security of Inner Attack in WiMAX Environment

Yoon-Su Jeong*, Yong-Tae Kim**, Gil-Cheol Park***

요 약

WiMAX 환경에서 사용되는 암호학적 키는 베이스 스테이션의 통신 범위안에 위치하는 이동 노드(노트북, PDA, 휴대폰 등)들에 의해 일정기간동안 사용되어지며, 이 때 이동 노드에 의해 사용되어지는 키는 이동 노드가 베이스 스테이션의 통신 범위를 벗어날 때까지 사용된다. 그러나 이동 노드가 베이스 스테이션의 통신 범위를 벗어나거나 이동 노드가 베이스 스테이션과 통신하기 위해 통신범위안에 진입하려고 할 때 이동 노드와 베이스 스테이션 사이의 통신구간은 무선으로 동작되기 때문에 man-in-the-middle 공격과 같은 내부 공격에 매우 취약한 문제점을 가지고 있다. 이 논문에서는 이동 노드가 베이스 스테이션과 통신하려고 할 때 베이스 스테이션에서 발생되는 암호학적 보안 공격위험과 통신 오버헤드를 줄이기 위해서 이동 노드들이 사용하는 키를 재사용할 수 있는 분산 키 설립 프로토콜을 제안한다. 제안된 분산 키 설립 프로토콜은 통신과정 중에 발생되는 키의 재사용을 통해 베이스 스테이션과 이동 노드 사이에서 발생되는 오버헤드를 줄일 수 있을 뿐만 아니라 상호 인증에 필요한 공유키를 노드 자신이 생성한 난수 값을 통해 생성하여 IEEE 802.16 표준보다 안전성을 향상시키고 있다.

Abstract

The cryptological key which is used in WiMAX environment is used at regular intervals by mobile nodes(laptop computer, PDA, cell-phone) which is in the range of base station coverage. But it is very weak at local attack like man-in-the-middle when the mobile node is off the range of base station or enters into the range to communicate with base station because the communication section is activated wirelessly. This paper proposes a distribution key building protocol which can reuse security key used by nodes to reduce cryptological security attack danger and communication overhead which occurs when mobile node tries to communicate with base station. The proposed distribution key establishing protocol can reduce overhead which occurs between base station and mobile node through key reusing which occurs during the communication process and also, makes security better than IEEE 802.16 standard by creating shared key which is required for inter-certification through the random number which node itself creates.

• 제1저자 : 정윤수 교신저자 : 김용태
• 투고일 : 2008. 9. 4, 심사일 : 2008. 11. 10, 게재확정일 : 2008. 12. 20.
* 충북대학교 전자계산학과 ** 한남대학교 멀티미디어학부 강의전담 교수 *** 한남대학교 멀티미디어학부 교수

▸ Keyword : 이동 와이맥스(Mobile WiMAX), 분산 관리(Distribution Management), 보안(Security), 키 설립(Key Establishment)

Ⅰ. 서 론

IEEE 802 그룹 중 IEEE 802.16 표준은 광대역 무선 접속 표준으로써 현재 WiMAX(Worldwide Interoperability for Microwave Access)라 불리는 고정 및 저속 이동접속에 대한 광대역 무선 통신 지원 기술이 포함되어 있다[5,16]. 802.16e-2005 표준인 Mobile WiMAX는 이동성을 지원하지 않는 IEEE 802.16 표준에 비해 키 관리 뿐만 아니라 EAP 기반의 인증과 트래픽 암호화 등의 다양한 보안 기능을 지원한다.

IEEE 802.16e 표준안이 개정된 이후에 IEEE 802.16e 기반 네트워크에 존재할 수 있는 보안 취약성 및 공격 가능성에 대해서 많은 연구가 수행되었다[10,11]. 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[12,13,14].

최근 WiMAX 환경에서 노드의 보안을 일정 수준으로 유지하기 위해 사용되는 다양한 암호학적 기술들은 애드혹, 센서 네트워크 그리고 메쉬 네트워크 등에 많이 활용되어지고 있다[1,2,3,4]. 그러나 암호학적 기술 중 키 동의와 관련된 기술은 WiMAX 환경에서 내부 보안과 관련하여 많은 문제가 발생되고 있다. WiMAX와 같은 분산환경에서는 기존 키 동의와 관련된 기술이 적합하지 않으며 통신 패턴에서도 제약사항이 많다. 이러한 문제점을 해결하기 위해서는 WiMAX 환경에서 사용되는 키의 설립과 재생성 방법을 안전하게 생성할 필요가 있다. 특히, WiMAX 환경에서는 WiMAX를 구성하는 노드들이 이동성을 가지고 있기 때문에 베이스 스테이션의 통신 범위에 노드들이 존재하는 일정 시간동안 노드들이 예상치 못한 일을 수행하거나 베이스 스테이션의 통신 범위를 벗어날 경우 자동적으로 노드에 대한 위치 정보, 키 정보 등의 노드정보 등을 갱신하여야 한다.

이 논문에서는 노드가 베이스 스테이션과 통신하려고 할 때 발생되는 암호학적 보안 공격위험과 통신 오버헤드를 줄이기 위해서 노드들이 사용하는 보안 키를 재사용할 수 있는 키 설립 프로토콜을 제안한다. 제안된 프로토콜은 통신과정 중에 발생되는 키의 재사용을 통해 베이스 스테이션과 노드 사이에서 발생되는 오버헤드를 줄일 수 있을 뿐만 아니라 상호 인증에 필요한 키를 Pseudo 랜덤 함수를 통해 생성하도록 한다. Pseudo 랜덤 함수를 통해 생성한 임의의 난수와 비밀값을 통해 이웃 링크 설립과 TEK 교환 과정에 사용되는 제안 프로토콜의 공개키에 적용하여 가입자와 베이스 스테이션에 대한 보안을 강화하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 이동 WiMAX의 개념 및 보안에 대해서 분석한다. 3장에서는 이동 WiMEX 환경의 링크 키 설립과정과 TEK 키 생성사이에서 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. 관련연구

2.1 Mobile WiMAX

IEEE 802.16 표준에서 WiMax는 (그림 1)처럼 현실적으로 동일 주파수 대역과 출력에서 서비스가 되는 경우 전송속도, 커버리지 측면에서 Wi-Fi서비스와 전반적으로 대등한 것으로 알려져 있으며, OFDM/x-QAM 방식의 변조를 채택하고 있어 전체적으로 유사한 기술로 분석된다. 하지만 Wi-Fi가 멀티셀 환경에서 복수 사업자가 사업에 참여하는 경우 상호간섭의 문제로 인해 사업에 부적절한 측면이 존재하는 데 비해 WiMax는 프레임 동기 설정을 바탕으로 간섭문제가 해결 가능하여 상대적으로 우월하며 주파수 효율에 있어서도 Wi-Fi에 비해 일반적으로 우수한 것으로 알려져 있다. 또한 상대적으로 서비스 QoS보장에 상당한 강점을 가지고 있으며, WiMax 포럼의 주장에 따르면 정책 환경을 배제한 순수한 기술적 차원에서는 30마일, 약 50킬로미터의 커버리지와 70Mbps의 전송속도를 구현할 수 있으며, 음성과 데이터를 모두 구현할 수 있는 것으로 되어 있다.

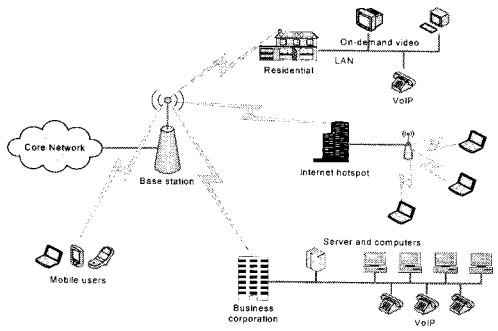

그림 1. 이동 WiMAX 환경
Fig. 1. Mobile WiMAX Environment

최근 이동 장치(PDA, 노트북, 휴대폰 등) 기술의 발달로 고정 WiMAX보다는 이동 WiMAX 기술 연구가 활발히 진행되고 있다. 이동 WiMAX는 IEEE 802.16e 표준으로 정의되어 있으며 고정 WiMAX 기술을 기반으로 이동성 기능을 지원하고 있다. 이동 WiMAX는 크게 3가지 기능을 가지고 있다. 첫째, 이동 중에도 최대 30Mbps의 속도로 데이터를 주고받을 수 있고 둘째 기지국간 이동을 원활하게 하기 위한 핸드오버 기능을 지원하며 마지막으로 핸드오버 지연시간을 50ms 미만으로 낮추어 VoIP와 같은 실시간 서비스도 품질의 저하없이 제공할 수 있다.

2.2 Mobile WiMAX의 사전인증 기법

이동 WiMAX 환경에서는 안전한 통신을 위해 키 관리 및 인증 기법에 대해서 많은 연구가 진행되고 있다[6,15,17]. Kassab는 사전적 키 분배를 기반으로 802.11 네트워크를 위한 빠른 사전 인증 기법을 제안했으며, MS와 BS사이에 사전 계산된 키 정보와 EAP-TLS의 단계를 줄임으로써 핸드오버 지연을 줄이는 장점을 가지지만 MS가 이웃 지역으로 로밍할 때는 PMK가 적용되지 않는 단점을 가진다[8,9]. WiMAX에서 사용되는 사전 인증 기법은 대표적으로 IAPP 캐싱을 이용한 PKD(Pro-active Key Distribution) 방법과 4 방향 핸드쉐이크를 사용하는 PKD가 있다. IAPP에서 캐싱을 이용하는 방법은 PTK(Pairwise Transient Key)와 TIME_AUTH 값이 협력되기 위해서 이웃 AP들에게 IAPP 교환을 실행한다[9]. 이 기법은 단지 한번만 그룹 키 핸드쉐이크가 실행된다. 또 다른 기법은 4방향 핸드쉐이크 방법으로 PTK 이웃 처리과정이 사전 인증 과정으로 동작된다. 따라서 핸드오버 동안 MS는 인증을 끝내기 위해 새로운 AP와 함께 그룹 키 핸드쉐이크 교환을 실행한다.

III. 안전성을 향상시킨 분산 키 관리 프로토콜

이 절에서는 WiMAX 환경에서 게이트웨이 역할을 하는 베이스 스테이션의 오버헤드를 줄이기 위해 링크 키와 그룹 키 설립과정에서 생성된 키를 재사용하는 분산 키 관리 프로토콜을 제안하고 있다. 다수의 노드들이 무선 구간을 안전하게 이동하면서 베이스 스테이션의 인증 오버헤드를 줄이기 위해서 제안 프로토콜에서는 분산 키 프로토콜을 사용한다. 특히 링크 키 설립과정에서 사용되는 사용자의 키는 데이터 트래픽 상의 기밀성과 인증을 제공하기 위해 사용되며 그룹 키 설립과정에서 생성되는 그룹 키는 공개키 암호기법을 사용하여 메시지의 무결성과 인증을 검증하기 위해 사용된다.

3.1 용어

제안 프로토콜에서 사용되는 용어는 〈표 1〉에서 정의하고 있다.

표 1. 파라미터
Table 1. Parameter

용 어	설 명
A, B	노드 A와 B
NM	베이스 스테이션 역할을 하는 네트워크 관리자
N_A	A에 의해 생성된 난수
PK_{NM}	네트워크 관리자의 공개키
SK_{NM}	네트워크 관리자의 개인키
K_{NMA_1}	A와 NM 사이에서 사전 동의된 공유키
h(x,y)	x와 y를 해쉬한 one-way 해쉬 함수
E_k(M)	키 K를 사용하여 메시지 M을 암호
MAC_k(M)	키 K를 사용하여 메시지 M의 메시지 인증 계산
SIG_{SK}(M)	개인키 SK를 사용하여 메시지 M의 표시

3.2 이동 노드와 베이스 스테이션 사이의 키 재사용 설립 과정

베이스 스테이션과 이동 노드 사이의 안전한 통신을 위해서는 키 설립 과정에서 생성되는 키를 이동 노드와 베이스 스

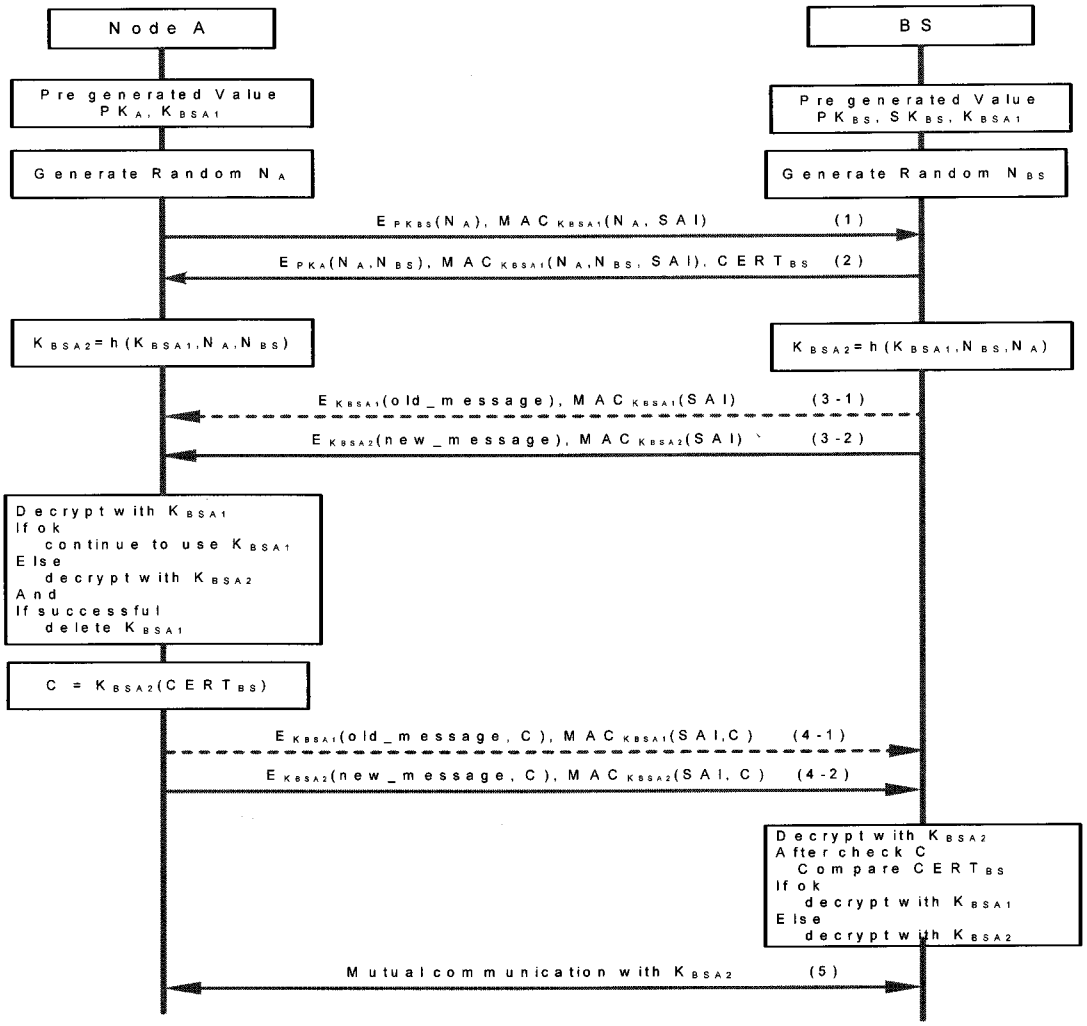

그림 2. 이동 노드와 베이스 스테이션간 키 재사용 동작과정
Fig. 2. Key Reuse Process between Mobile Node and Base Station

테이션이 신뢰할 수 있는 공유키의 역할을 수행할 수 있여야 한다. (그림 2)는 이동 노드와 베이스 스테이션 사이의 키 재사용 설립을 위한 프로토콜 과정을 보여주고 있다. (그림 2)에서 이동 노드는 베이스 스테이션의 공개키를 사용하여 암호화된 랜덤 수를 베이스 스테이션에게 보냄으로써 베이스 스테이션과 함께 일정 주기동안 사용될 재사용 키를 초기화 한다. 이 때 공개키를 가지고 랜덤 수를 암호화하는 것은 공격자가 공유키를 계산할 수 없게 하고 랜덤 수를 복호화할 수 없도록 수동적 공격에 대해서 forward secrecy를 지원하기 위해서이다.

(그림 2)에서 사용되는 모든 메시지는 페이로드와 현재 사용중인 공유키를 사용하여 MAC을 계산한다. 제안 프로토콜에서는 재사용 키를 초기화하기 위해서 베이스 스테이션의 공개키를 이용하여 암호화한 랜덤수를 페이로드에 삽입함으로써 이동 WiMAX 환경에서 많이 발생되는 impersonation 공격을 예방하고 있다. (그림 2)에서 이동 노드가 베이스 스테이션에게 전달하는 메시지 형식은 식 (1)과 같다. 식 (1)에서 사용되는 키 K는 이동 노드와 베이스 스테이션에 사전 동의된 공유키를 의미한다. 제안 프로토콜에서는 재사용 키가 설립되기 전에 공격자로부터 키 K가 안전하다고 가정한다.

페이로드, MAC_K(페이로드) ..... (1)

(그림 2)의 단계 1에서는 재사용 키를 생성하기 위해서 이동 노드 자신이 생성한 난수 N_A와 SAI(Secure Authentication Information)을 베이스 스테이션에게 전달한 후 베이스 스테이션은 단계 2를 통해 베이스 스테이션 자신이 생성한 난수 N_B와 함께 전달받은 이동 노드의 난수 N_A, 베이스 스테이션의 인증서 $CERT_{BS}$를 이동노드에게 전달한다. 단계 2 과정 이후에 이동 노드와 베이스 스테이션은 현재 사용중인 공유키 K_{BSA_1}와 랜덤수(N_A, N_{BS})를 one-way 해쉬 함수에 적용하여 이동 노드와 베이스 스테이션 사이의 새로운 공유키 K_{BSA_2}를 생성한다. 이 과정에서 공격자가 송·수신되는 메시지를 가로챈 후 사용중인 키를 타협하더라도 새로 생성되는 키 K_{BSA_2}는 one-way 해쉬 함수의 특성으로 인하여 공격자가 초기 키(k-1, k-2, k, ..., k-n) 정보만을 가지고서는 암호화된 메시지를 복호화할 수 없다.

단계 2 이후에 제안 프로토콜의 이동 노드와 베이스 스테이션은 모든 메시지를 암·복호화 할 때 2가지의 키(old 키(K_{BSA1})와 new 키(K_{BSA2})) 선택과정을 수행한다. 이 때 2가지의 키를 선택하는 이유는 이동 노드와 베이스 스테이션 사이에서 키 K_{BSA2}를 생성하기 전에 키 K_{BSA1}를 MAX에 적용할 경우가 발생할 수 있기 때문이다. 수신된 메시지를 복호화하는 과정에서 단계 3는 2개의 공유키 중 우선 먼저 old 키를 이용하여 수신된 메시지를 복호화하고(단계 3-1) 만약 복호화하가 실패할 경우 새로 생성된 new 키로 교체하여 메시지 복호화 과정을 수행한다(단계 3-2). 단계 3-1에서 old 키를 사용하는 경우에는 이동 노드가 보낸 재사용 키 요청 메시지를 베이스 스테이션이 수신하지 못하였거나 지연된 이전 메시지를 처리해야 하는 경우에 사용되며 단계 3-2에서 new 키를 사용하는 경우에는 베이스 스테이션이 이동 노드로부터 재사용 키 요청 메시지를 정확하게 수신한 경우에 사용된다. 단계 3-1에서 이동 노드는 복호화가 실패할 때까지 old 키를 사용하며 복호화가 실패할 경우 단계 3-2과정을 통해 이동 노드는 MAC을 사용하여 메시지를 검증한 후 old 키를 삭제하고 전달받은 new 키를 사용하게 된다. 이동 노드는 새로 생성된 new 키를 이용하여 베이스 스테이션에게 전달받은 인증서 $CERT_{BS}$를 암호화한 후 단계 4를 통해 베이스 스테이션에게 전달한다. 단계 4에서는 베이스 스테이션이 이동 노드에게 전달 받은 메세지를 new 키로 복호화하기 전에 인증서 $CERT_{BS}$를 검증한다. 인증서 검증이 완료되면 new 키로 메시지를 복호화한 후 old 키를 삭제한다. 이 때, 베이스 스테이션은 메시지를 복호화하는 과정에서 단계 4-1처럼 우선 먼저 이전에 사용한 old 키를 사용하여 메시지 복호화를 시도한 후 복호화가 이루어지지 않으면 단계 4-2의 새로운 메시지부터는 new 키를 사용하여 복호화를 시도한다. 단계 4에서 old 키를 삭제하는 기간에는 무선 장비의 특성으로 인하여 링크상에 평균 지연이 발생하게 되다. 마지막으로 단계 5에서는 새로 생성한 new 키를 이용하여 이동 노드와 베이스 스테이션 사이에 안전한 상호 통신을 수행한다.

3.3 베이스 스테이션의 통신 범위내에 있는 이동 노드들의 그룹 키 설립

이 절에서는 베이스 스테이션의 통신 범위내에 위치하는 이동 노드간에 통신 그룹을 형성하기 위해서 베이스 스테이션이 이동 노드들과 멀티캐스팅을 위한 그룹 키를 설립하는 과정을 나타낸다. 베이스 스테이션은 그룹 키를 분배하기 위해서 3.2절에서 생성한 베이스 스테이션과 이동 노드 사이에 공유된 공유키 K_{BSA}로 그룹키를 암호화하여 전달하며 제안 프로토콜의 그룹 키를 설립 과정은 (그림 3)과 같다.

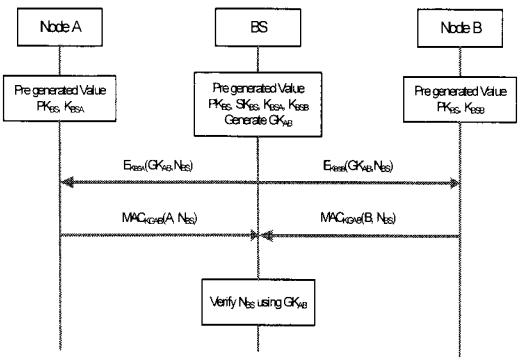

그림 3. 베이스 스테이션 통신 범위 내 노드들의 그룹 키 설립 과정
Fig. 3. Group Key Establishment Process of Nodes within Communication Range of Base Station

(그림 3)에서 베이스 스테이션은 그룹을 원하는 이동 노드들에게 전달할 그룹키 GK_{AB}를 생성한 후 베이스스테이션의 난수 N_{BS}와 함께 이동 노드들간에 공유된 공유키 K_{BSA}와 K_{BSB}로 각각 암호화하여 노드들에게 분배한다. 이동 노드들은 베이스 스테이션과 공유된 공유키 K_{BSA}와 K_{BSB}를 이용하여 그룹키를 복호화한 후 그룹키를 사용하여 수신된 난수 N_{BS}와 함께 이동 노드의 인식자를 HMAC을 사용하여 베이스 스테이션에게 전달한다. 마지막으로 이동 노드는 전달된

HMAC 값을 분석 한 후 그룹키 GK_{AB}를 정확하게 소유하였는지를 검증한다.

3.4 이동노드의 인증 정보 업데이트

WiMAX에서 동작되는 이동 노드들은 서로 다른 타입으로 동작되며 이동 노드들이 그룹으로 형성되기 위해서는 그룹 구성요소인 이동 노드들의 인증 정보를 주기적으로 업데이트할 필요가 있다. 제안 프로토콜에서는 (그림 4)와 같이 멀티캐스팅 방법을 사용하여 패킷을 그룹키로 암호화하여 이동 노드들에 대한 인증 정보를 업데이트한다. 이동 노드의 인증 정보를 업데이트하기 위해서 베이스 스테이션은 데이터를 N개로 분할한 후 역순으로 데이터를 해쉬하여 데이터들을 체인화하도록 한다. 제안 프로토콜에서는 이동 노드 정보 X와 함께 H1을 베이스 스테이션의 개인키로 서명함으로써 이동 노드의 인증과 무결성을 검증한다. CBC 생성 과정에서 난수 N을 포함한 목적은 두 번째 사전이미지 공격을 수행하는 공격자를 예방하기 위해서이며 이동 노드들에게 전달된 암호문 C1은 이전 암호문 C0와 함께 평문 D1와 H2로부터 계산되어진 패킷을 통해 검증하게 된다.

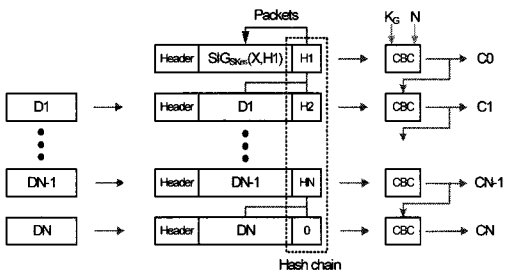

그림 4. 멀티캐스팅을 이용한 키 인증 업데이트
Fig. 4. Key Authentication Update using Multicasting

IV. 평가

이 절에서는 인터 도메인간 이동 노드의 핸드오프 지연과 베이스 스테이션의 오버헤드를 통해서 제안 프로토콜의 성능을 평가하고 있다. 평가 결과의 객관성을 위해서 제안 프로토콜은 인터 도메인 인증 솔루션 IEEE802.1x 인증 기법, RSA 인증 기법 그리고 ECC 인증 기법과 성능비교 평가한다.

4.1 실험 환경

제안 프로토콜에서는 인터 도메인간 이동 노드의 평균 인증 지연 시간을 객관적으로 평가하기 위해서 [7]에서 제시한 인터 도메인간 평균 인증 지연 평가 방법을 적용하였다. 인터 도메인간 핸드오프 수의 확률 밀집 함수(Probability density function)를 구하는 식은 식 (2)와 같다.

$$\alpha(j)=\begin{cases}1-1/\rho_{BS}[1-f^{*}_{BS}(t)], & \text{if } j=0,\\ 1/\rho_{BS}[1-f^{*}_{BS}(t)]^{2}*[f^{*}_{BS}(t)]^{i-1}, & \text{if } j>0\end{cases} \cdots (2)$$

식 (2)에서 $\alpha(j)$는 인터 도메인간 핸드오프 수 j의 확률 밀집 함수를 의미하고 ρ_{BS}는 베이스 스테이션의 확률 밀집률을 의미한다. 이동 노드의 잔존시간은 $1/(\rho_{BS})$의 분산 값으로 구해지고 확률 밀집 함수는 $f_{BS}(t)$로 표현한다. 식 (2)에서 $f^{*}_{BS}(t)$는 베이스 스테이션의 Laplace 전송을 의미한다 [7]. 네트워크 도메인에 진입하는 이동 노드의 인터 도착 시간은 $1/\lambda$와 $\rho_{BS}=\lambda/\mu_{BS}$의 평균을 가지는 지수분포를 따른다. 인터 도메인간 인증 기법에 대한 평균 인증 지연은 식 (3)으로 정의한다.

$$T_{inter}(i)=\sum_{j}\vec{d_i}\bullet\vec{t}\bullet j\bullet\alpha(j),$$
$$\forall i=1,2,3,4,5 \cdots (3)$$

인증지연은 인증 사용자가 인증 요청을 보냈을 때 인증 응답을 수신받을 때까지의 시간으로 정의한다. 식 (3)에서 $\vec{t}$는 인증 지연에 따른 인증 동작의 벡터값을 의미하며 $\vec{d}$는 각 시간에 대한 벡터값을 의미한다. 〈표 2〉는 제안 프로토콜의 성능을 평가하기 위해 IEEE 802.1x, RSA, ECC, 제안 프로토콜 등의 홉 당 전송지연 시간을 유추한 결과이다.

표 2. 홉 당 평균 전송지연 시간
Table 2. Average Transsmision Delay Time per Hop

	IEEE 802.1x	RSA	제안 프로토콜
Delay/hop (ms)	19.6	1.68	0.5
Delay (ms)	17.2	28.75	7.2

4.2 성능 평가

(그림 5)는 평균 인증 지연상에 각 이동 사용자가 베이스 스테이션의 통신 범위내에 잔존하는 이동 노드들의 시간 변화를 보여주고 있다. X축에 있는 잔존시간(Resident time)은 이동 노드가 다른 베이스 스테이션의 통신 범위에 이동하지

않고 현재 베이스 스테이션에 머무르는 시간을 의미하며 1/Resident Time은 이동 노드가 다른 베이스 스테이션의 통신 범위에 진입하지 않고 현재 베이스 스테이션에 머무르는 시간을 비율로 표현한 것이다. Y축은 이동 노드의 평균 인증 지연시간을 의미한다.

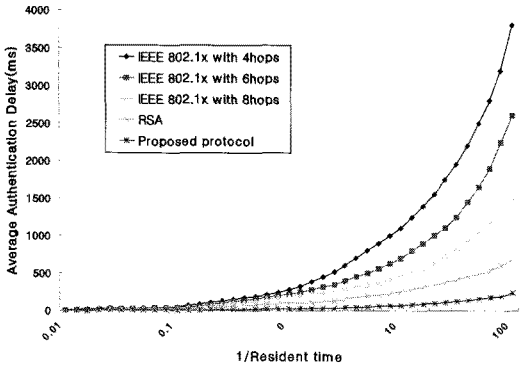

그림 5. 도메인에 잔존하는 이동 노드의 평균 인증 지연 시간
Fig. 5. Average Authentication Delay Time of Resident Mobile Node in Domain

(그림 5)의 결과처럼 이동 노드가 현재 베이스 스테이션의 통신 범위 상에 머무르는 시간이 높을수록 평균인증 지연 시간은 낮아지며 반대로 현재 베이스 스테이션의 통신 범위 상에 머무르는 시간이 낮을수록 평균 인증 지연 시간은 높아진다. WiMAX 환경에서 이동 노드 인증과 관련해서 많이 사용하는 IEEE 802.1x, RSA 그리고 제안 프로토콜을 비교한 결과 이동 노드 잔존시간이 길어질 경우 평균인증 지연시간은 거의 차이가 없지만 이동 노드의 잔존시간이 짧을수록 IEEE 802.1x, RSA, 제안 프로토콜 순으로 평균 인증 지연시간이 낮아졌다. IEEE 802.1x의 경우 홉 수가 클수록 평균인증 지연시간이 낮아지는 것을 알 수 있다. 이러한 결과는 공개키의 사용방법에 따라 결과의 차이를 가져왔으며 제안 프로토콜은 공개키와 비밀키를 혼용해서 사용하는 혼합방식을 사용하여 이동 노드의 인증 부하를 줄여졌기 때문에 다른 알고리즘에 비해 평균 인증 지연시간이 낮았음을 알 수 있다.

(그림 6)은 이동 노드 속도에 따른 베이스 스테이션의 전체 인증 저장 계산량을 보여주고 있다. (그림 6)의 결과처럼 이동 노드의 속도가 높을 경우 이동 노드의 속도가 낮을 때보다 전체 인증 저장 계산량이 낮았으며 이 같은 결과는 이동 노드의 속도가 높을수록 베이스 스테이션의 통신 범위를 빠르게 벗어나기 때문이다. 그리고 이동 노드의 속도가 높을 경우가 이동 속도가 낮을 때보다 전체 인증 저장 계산량이 일정 비율을 유지하였으며 다른 알고리즘에 비해 IEEE 802.1x가 높은 인증 저장 계산량을 보이고 있다. 반면 RSA, ECC, 제안 프로토콜은 인증 저장 계산량이 RSA, ECC, 제안 프로토콜 순으로 낮았으며 RSA, ECC, 제안 프로토콜은 인증 저장 계산량 차이가 5% 이내로 나타났다.

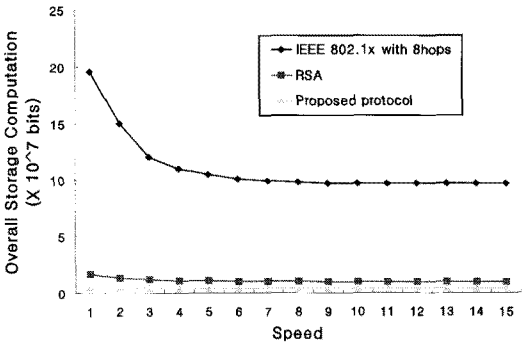

그림 6. 베이스 스테이션의 전체 저장 계산량
Fig. 6. Overall Storage Computation of Base Station

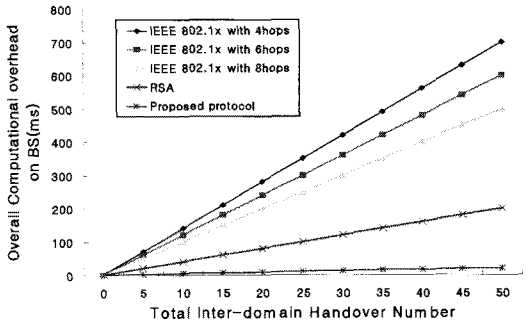

그림 7. 인터 도메인간 핸드오버 수에 따른 베이스 스테이션의 전체 계산 오버헤드
Fig. 7. Overall Computation Overhead Base Station through Handover Number of Inter-domain

(그림 7)은 인터 도메인간 핸드오버 수에 따른 베이스 스테이션의 전체 계산 부하량를 보여주고 있다. (그림 7)의 결과처럼 인터 도메인간 핸드오버 수가 증가함에 따라 각각의 알고리즘에 대한 베이스 스테이션의 전체 계산 로드 시간이 비례적으로 증가하고 있다. 이 같은 결과는 각 알고리즘에 대한 처리시간에 따른 결과로써 제안 프로토콜이 다른 암호 알고리즘에 비해 베이스 스테이션의 전체 계산 부하량이 낮은 결과를 얻을 수 있었다.

4.3 보안 평가

이 절에서는 WiMAX 환경에서 가장 많이 발생되는 BS 인증 취약, 메시지 응답 공격, Man-in-the-Middle 공격 등의 3가지 보안 위협에 대해서 제안 프로토콜을 평가한다. 2004년 제정된 WiMAX 표준에서는 베이스 스테이션의 인증 방법을 지원하고 있지 않아서 무선에서 발생할 수 있는 보안 위협에 매우 취약하였지만 제안 프로토콜에서는 권한 응답 메시지에 베이스 스테이션의 인증서와 랜덤값을 추가하여 베이스 스테이션의 보안을 향상시키고 있다. 특히 베이스 스테이션이 생성한 랜덤 값은 무선 네트워크 환경에서 많이 발생하는 reply 공격을 예방할 수 있다. 또한 베이스 스테이션이 이동 노드에게 전달하는 권한 응답 메시지에는 타임스탬프가 있어 이동 노드의 무결성을 보장하도록 하고 있으며 권한 응답 메시지에 포함된 베이스 스테이션의 시그너처는 초기 키 설립 과정에서 메시지의 인증과 부인방지를 제공하고 있다.

WiMAX의 키 설립과정에서 가장 많이 발생하는 공격 중 하나가 바로 메시지 응답 공격이다. 이 공격을 예방하기 위해서는 인증과정에서 교환되는 메시지들의 인식자를 최신으로 유지할 수 있어야 한다. 제안 프로토콜에서는 베이스 스테이션이 시그너처와 함께 타임스탬프를 권한요청 메시지에 추가함으로써 메시지 응답 공격을 예방하고 있다. 메시지에 사용되는 시그너처는 메시지 내 중요 정보를 예방하기 위해 이동 노드의 개인키를 사용한다.

Man-in-the-Middle 공격은 자신이 생성한 권한 키를 획득하여 권한 응답 메시지를 생성하고 통신과정에서 이동 노드를 제어할 수 있게 하는 공격유형이다. 이 공격이 WiMAX 환경에서 가능한 이유는 이동 노드가 베이스 스테이션으로부터 생성된 권한 구문 메시지를 신뢰할 수 없기 때문에 발생된다. 제안 프로토콜에서는 이러한 문제를 해결하기 위해 베이스 스테이션과 이동 노드 사이에 키 설립과정에서 상호인증을 수행할 수 있도록 임의의 난수를 서로 교환하여 검증 메시지를 서로 송·수신하도록 하고 있다.

V. 결론

WiMAX 환경에서 사용되는 암호학적 키는 베이스 스테이션의 통신 범위안에 위치하는 이동 노드들이 베이스 스테이션의 통신 범위를 벗어날 때까지 사용된다. WiMAX 환경에서는 이 때 이동 노드가 베이스 스테이션의 통신 범위를 벗어나거나 진입하려고 할 때 베이스 스테이션의 인증과정이 없어 man-in-the-middle 공격과 같은 내부 공격에 매우 취약한 문제점을 가지고 있다. 이 논문에서는 노드가 베이스 스테이션과 통신하려고 할 때 발생되는 암호학적 보안 공격위험과 통신 오버헤드를 줄이기 위한 키 설립 프로토콜을 제안했다. 제안된 프로토콜은 통신과정 중에 발생되는 키의 재사용을 통해 베이스 스테이션과 노드 사이에서 발생되는 오버헤드를 줄일 수 있을 뿐만 아니라 상호 인증에 필요한 키를 Pseudo 랜덤 함수를 통해 생성하도록 하였다. 제안 프로토콜은 성능 측면에서 IEEE 802.1x, RSA와 함께 도메인에 잔존하는 이동 노드의 평균 인증 지연 시간, 베이스 스테이션의 전체 저장 계산량 그리고 인터 도메인간 핸드오버 수에 따른 베이스 스테이션의 전체 계산 오버헤드 등에 대해서 향상된 성능을 보였으며 보안 측면에서는 베이스 스테이션 보안 문제, 메시지 응답 공격, Man-in-the-Middle 공격 등에 대해서 제안 프로토콜이 안전성을 향상시켰음을 평가하였다. 향후 연구에서는 제안 프로토콜에서 사용되는 재사용 키를 이용하여 무선 환경에서 발생할 수 있는 다른 보안 공격에 대해서 안전한 보안 구조 및 정책 연구를 수행할 계획이다.

참고문헌

[1] C. Beaver, D. Gallup, W. Neumann, and M. Torgerson, *"Key Management for SCADA,"* Technical Report, Sandia National Laboratories, 2002.

[2] S. A. Camtepe and B. Yener, *"Key Distribution Mechanisms for Wireless Sensor Netowrks: A Survey,"* Technical Report, Rensselaer Polytechnic Institute, 2005.

[3] B. Dutertre, S. Cheung, and J. Levy, *"Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust,"* Technical Report, SRI International, 2004.

[4] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," In CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41-47, New York, NY, USA, 2002. ACM Press.

[5] 손태식, 최욱, 최효현, "Mobile WiMAX 보안 이슈와 해결 방안," 한국통신학회지, 제 24권, 제11호, 5-13쪽, 2007년 11월

[6] W. Liang and W. Wang, "A Quantitative Study of Authentication and QoS in Wireless IP

Networks," in Proc. of IEEE INFOCOM'05, Miami, FL, USA, Mar. 2005.

[7] S. Baek, S. Pack, T. Kwon and Y. Choi, "A Localized Authentication Authorization, and Accounting (AAA) Protocol for Mobile Hotspots," in WONS 2006, 2006.

[8] M. Zhao, S. W. Smith and D. M. Nicol, "Aggregated Path Authentication for Efficient BGP Security," in Proc. of CCS 2005, pp. 128-138, Nov. 2005.

[9] F. R. Henriquez, C. E. Lopez-Peza and M. A. Leon-Chavez, "Comparative Performance Analysis of Public-key Cryptographic Operations in The WTLS Handshake Protocol," in Proc. of IICEEE'04, pp. 124-129, 2004.

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

[11] S. Xu, M. Mattews and C.-T. Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 02.16," Proceedings of the 44th ACM Southeast Conference(ACMSE 2006), Mar. 2006.

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

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

[14] 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.

[15] 정윤수, 김용태, 이상호,. "ECC 기반의 클러스터간 노드들의 안전한 인증 프로토콜," 한국컴퓨터정보학회논문지, 제13권, 제2호, 167-175쪽, 2008년 3월.

[16] 박종현, 강지훈, "디지털 방송을 위한 Set-Top Box기반 TV-Anytime 메타데이터 관리 시스템," 한국컴퓨터정보학회논문지, 제13권, 제4호, 71-78쪽, 2008년 7월.

[17] 이상렬,"RFID 시스템의 개선된 인증 프로토콜," 한국컴퓨터정보학회논문지, 제12권, 제6호, 193-200쪽, 2007년 12월.

저 자 소 개

정 윤 수

2000년 2월 : 충북대학교 대학원 전자계산학 이학석사

2008년 2월 : 충북대학교 대학원 전자계산학 박사

관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태

1988년 숭실대학교 석사

2008년 2월 충북대학교 전자계산학 이학박사

2006.3 ~ 현재 한남대학교 멀티미디어 학부 강의전담교수

관심분야: 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신보안, 멀티미디어

박 길 철

1986년 숭실대학교 전자계산학과 석사.

1998년 성균관대학교 전자계산학과 박사.

2006년 UTAS, Australia 교환교수

1998년 8월~현재 한남대학교 멀티미디어학부 교수

(관심분야) multimedia and mobile communication, network security