중소기업정보기술융합학회논문지 제1권 제1호 pp.67~73, 2011

Mobile WiMAX에서 부분암호화 방식을 적용한 안전하고 신속한 핸드오버 기법

김기수[1], 김윤철[2], 이상호[3*]
[1](주)한국아이티평가원, [2](주)유앤비테크, [3]충북대학교 컴퓨터과학과

A Handover Scheme based on Partial Encrypton Method to Support Security and Rapidity of Mobile WiMAX

Ki-Su Kim[1], Yon-Cheol Kim[2] and Sang-Ho Lee[3]
[1]KSEL Co., [2]U&B Tech., [3]Chungbuk National University

요 약 고속 이동 통신 서비스에서의 핸드오버, 특히 Mobile WiMAX는 120km/h의 속도에서도 이동성을 효과적으로 지원한다. 하지만 한 셀 안에서 증가하는 사용자의 수를 수용하기 위해 무선 네트워크의 각 셀의 크기를 줄임으로써 대역폭을 할당하는 방법으로 마이크로셀, 피코셀이 점점 늘어나고 있다. 이러한 결과로 핸드오버가 발생하게 되고, 그에 따라 연결 실패 비율이 증가하였다. IEEE 802.16 표준안에서는 핸드오버 최적화 기법을 통해 Seamless 한 연결성을 제공하지만 인증절차를 생략함으로써 네트워크 취약성이 노출되었다. 본 논문은 VoIP, 화상통신, Streaming Data Service 같은 실시간서비스를 지원하면서 보안성이 우수한 부분암호화 방식의 핸드오버를 제안한다. 평가결과, 제안 기법은 기존 방법에 비해 처리시간이 20%이상 향상됨을 입증하였다.

키워드 : WiMAX, 핸드오버, 부분 암호화, IEEE 802.16

Abstract Handover in high speed mobile communication service, in particulary mobile WiMAX is supported efficiency mobility to 120km/h speed. But, in order to accommodate number of user increment in a cell, wireless network is increment to microcell and picocell by allocate bandwidth and by decrease cell size. handover is occurrent and increment connection failure ratio In this result. IEEE 802.16 standard is support seamless connection through handover optimization scheme. But because authentication process is abbreviate, network weakness is exposure. In this paper, we propose handover scheme for support realtime service as VoIP, Picure communication, Streaming Data Service in order to support partially encryption method. In experiment, proposed scheme is proof which process time is increment 20% more than previous scheme.

Key Words : WiMAX, Handover, Partial Encryption, IEEE 802.16

1. 서론

정보통신 기술의 발전으로 통신과 방송이 융합된 다양한 서비스가 출현하고, 언제 어디서나 이용할 수 있는 환경으로 바뀌어 가고 있으며, 이는 전송용량의 광대역화, 고속의 이동성, MS의 개인화라는 특성을 가지고 있다. 이러한 특성을 가장 잘 제공하는 서비스 중 하나가 Mobile WiMAX이다.

IEEE 산하의 Broadband Wireless Access(BWA)를 담당하는 802.16 Working Group에서 표준화 작업을 수

*교신저자(shlee@chungbuk.ac)
접수일(2011년 10월 2일), 심사완료일(2011년 11월 4일)

행한 Mobile WiMAX는 단순히 고속으로 이동 중에 인터넷을 이용할 수 있는 기본적인 인터넷접속 서비스를 넘어, 언제 어디서나 무선IP기반의 각종 데이터, 커뮤니케이션, 멀티미디어 서비스를 즐길 수 있는 환경을 제공한다.

성공적인 Mobile WiMAX 서비스 제공을 위해서 다양한 보안위협으로부터 MS과 네트워크 장비들을 보호하고, 네트워크를 통하여 전송되는 정보를 보호할 수 있는 기술이 필수적으로 요구된다.

Mobile WiMAX에서는 향상된 보안기능을 제공하기 위해 PKM(Privacy Key Management)라 불리는 Security Sub-layer를 가지고 있으며, PKMv2를 통해 EAP(Extensible Authentication Protocol)인증[7], AES(Advanced Encryption Standard)기반 기밀성 제공 알고리즘, CMAC/HMAC(Cipher/Hashed Message Authentication Code)을 사용한 메시지 인증 기능 제공 등을 지원한다. 하지만 작은 셀 크기를 갖는 환경에서 고속 이동은 빈번하게 핸드오버를 초래하게 되며, 이는 PKM인증과정에서의 지연으로 인하여 VoIP, 화상통신, Streaming Data Service같은 실시간 서비스에서 일시적인 서비스 단절이 발생할 수 있다. 이러한 문제는 핸드오버 과정에서 PKM인증단계와 TEK생성단계를 생략함으로써 MS(Mobile Station)의 이동성 및 QoS(Quality of Service)을 보장하여 해결할 수 있다. 그러나 이 방법은 치명적인 네트워크 취약성이 존재한다. 따라서 신속한 MS의 이동성을 지원하면서 인증과 기밀성을 제공할 수 있는 안전한 핸드오버 방안이 필요하다.

본 논문에서는 Mobile WiMAX에서 부분암호화 방식을 적용한 안전하고 신속한 핸드오버 기법을 제안한다. 키 교환과정에서 필연적으로 발생하는 지연은 수용하되, 암호화, 복호화에 걸리는 시간을 단축시킴으로써 실시간 서비스의 단절현상을 막고자 하는데 의의가 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 빠른 핸드오버를 위한 기존의 관련 연구들을 살펴본다. 제 3장에서는 본 논문에서 제안하는 모델을 설명하며, 제 4장에서는 기존 기법들과의 성능평가를 통해 제안방식의 우수성을 입증한다. 마지막으로 제 5장에서는 결론과 향후 연구과제를 제시한다.

2. 관련연구

IEEE 802.16 표준안[3]이 2004년에 제정된 이후로 Mobile IP기반 핸드오버에 대해서 많은 연구가 수행되어져 왔다. 2장에서는 먼저 신속하고 끊김없는 이동성을 지원하기 위해 표준안에 포함되어있는 핸드오버 최적화 기능을 설명을 하고, 그 후 가장 최근 연구에서 제안된 Pre-authentication 기반의 핸드오버 방안을 언급한다.

2.1 핸드오버 최적화 기법

Mobile WiMAX는 끊김없는 이동성 서비스를 위하여 다양한 핸드오버 기법[4][5][6]을 제공한다. IEEE 802.16 표준에는 Hard handover(HHO), Optimized hard handover(OHHO), Fast base station switching(FBSS), Macro diversity handover (MDHO)의 4가지 핸드오버가 정의되어 있다. 그러나 WiMAX Forum이 Mobile WiMAX 인증을 위하여 정의한 시스템 프로파일에는 HHO와 OHHO만으로도 우수한 핸드오버 성능을 얻을 수 있기 때문에 이 두 종류의 핸드오버만을 필수 기능으로 포함하고 있다. Mobile WiMAX는 완벽한 이동성을 제공하는 것을 강점으로 내세우고 있기 때문에 빈번한 핸드오버가 발생하는 경우에도 끊김없는(seamless) 서비스를 제공하여야 한다.

따라서 핸드오버 과정에서의 지연을 최소화하기 위해, IEEE 802.16e 표준안은 표 1에서 기술한 바와 같이 RNG-RSP 메시지 안에 핸드오버 Opti- mization bit #1과 #2 를 통한 보안설정을 제공한다.

표 1. 핸드오버 최적화 옵션
Table 1. Options of Handover Optimization

옵션	내용
Bit #1	Mobile WiMAX 네트워크에 단말이 재진입시 인증절차 생략
Bit #2	Mobile WiMAX 네트워크에 단말이 재진입시 암호화키 생성 생략

핸드오버 최적화 옵션 기능은 표 1에서 보는 것처럼 Mobile WiMAX에서 효율적인 핸드오버 지원을 위하여 부가적인 기능으로 제공되며 총 8종류로 구성되어 있고 핸드오버가 발생했을 때 네트워크 재진입과정이나 재인증 과정에서의 최소화된 절차를 지원한다. Bit #1와 Bit #2는 각각 PKM 인증절차 생략, TEK생성단계 생략을 의미한다. 만일 이 두 종류의 기능이 핸드오버 과정에서 적용된다면, PKM인증단계와 TEK생성단계가 생략됨으로써 핸드오버 지연 시간을 최소화하여 끊김없는 서비스를 제공할 수 있다.

하지만, 이런 장점에도 불구하고 핸드오버 최적화 옵션의 사용은 핸드오버 과정에서의 인증 및 기밀성과 같은 보안기능의 생략을 의미하므로 결국 치명적 네트워크 취약성을 노출시킬 수 있다. 즉, 보안키가 현재 BS에서 다음 BS로 전달되는 것을 뜻하며, 이런 접근은 네트워크에서 인증키가 공유되는 것을 뜻하므로 매우 위험하다.

2.2 Pre-authentication 기반 메커니즘

PKMv2의 보안 취약성을 개선하며 Pre-authentication 기반 메커니즘을 적용한 안전하고 신속한 핸드오버 방안을 논문[1]에서 나타낸다. 이 방안은 기존의 IEEE 802.16 표준에서의 핸드오버 최적화 옵션의 문제점을 지적하고, PKMv2의 키교환절차를 보다 안전하게 개선함으로써 보안성을 향상시켰다. 그리고 이웃한 모든 BS과 pre-authentication procedure를 거침으로써 사전에 해당 셀에서 사용하게 될 인증키, 무결성 검사키, 데이터 암호화키를 생성하였다. 이를 통해 해당 망 진입 후 발생하게 될 인증 및 키 교환 절차로 인한 지연을 현저히 감소시켰으므로 빠른 핸드오버를 지원한다.

그림 1은 논문[1]에서 제안하는 소프트 핸드오버에서의 메시지 교환 및 키 교환방식이다.

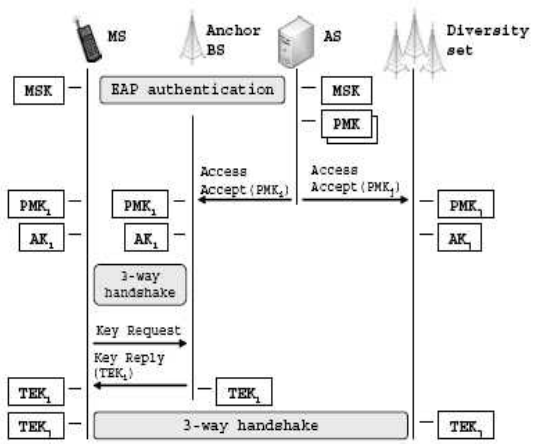

그림 1. 제안 기법의 메시지 교환 방식
Fig 1. Message change method of proposed scheme

기존 PKMv2 키교환절차에서는 MSK(Master Session Key)를 AS(Authenticaion Server)에서 생성하여 BS에게 전달하였다. MSK는 BSID와 MS의 MAC Address를 숨길 수 없으므로 어느 BS나 MSK를 수신하고 BSID와 MS의 MAC Address를 안다면 이를 통해 PMK (Pairwise Master Key), AK(Authorization Key), KEK (Key Encryption Key), TEK(Traffic Encryption Key)를 모두 만들 수 있는 문제가 있다. 논문[1]은 MSK대신 PMK를 전달함으로써 MSK 노출로 인한 문제를 막았으며, MS와 인접한 모든 BS와 키교환과정을 거쳐 미리 통신에 사용될 키를 생성함으로써 핸드오버를 통해 해당 망에 진입했을 때 소요되는 지연을 현저히 줄였다. 하지만 이 경우 불필요한 키 생성 과정을 거치게 되어 과도한 계산에 따른 부하와 키를 저장하기 위한 메모리가 낭비되는 문제점이 있다.

3. 부분암호화를 이용한 핸드오버 기법

기존 논문들은 PKMv2의 인증 및 키교환 방식에서의 지연을 단축시키는데 중점을 두었지만 암호화, 복호화에 걸리는 시간을 간과하였다. 아무리 인증 및 키교환을 빨리 수행하였다하더라도 데이터의 암호화, 복호화에서 지연이 많아진다면 빠른 핸드오버를 통한 실시간 서비스는 지원할 수 없다. 따라서 데이터의 암호화, 복호화시의 시간을 단축시켜야 한다.

3.1 부분암호화 방안

적용되는 부분 암호화 방법은 그림 2에서처럼 전송하려는 데이터를 16,000바이트씩 메시지 블록으로 나누고 다시 80바이트로 작게 세분화한다. 세분화된 메시지 블록의 순번과 부분 암호화용 랜덤 비트열(비트 '0'과 비트 '1'의 전체 개수는 각각 100개)을 이용하여 비트 값이 '1'인 블록에 대하여 암호화를 수행한다. 논문에서 적용하는 부분암호화 방법은 데이터를 전체적으로 암호화하는 경우보다 보안성은 떨어지지만 메시지의 암호화가 그 만큼 덜 수행되어지기 때문에 암호화 시간을 줄여주며 단말의 부하도 낮출 수 있는 장점을 가지고 있다.

SSL에서의 레코드 프로토콜은 전송하는 응용 메시지를 취해서 관리하기 쉬운 블록으로 데이터를 분해하여 데이터를 압축한다. 이때 압축은 214바이트의 크기로 적용된다. 제안시스템 역시 동일한 방식을 적용하여 한 번에 읽어올 수 있는 데이터의 크기를 16,000바이트로 제한하였다. 입력데이터는 부분암호화를 위해 각각 8,000바이트씩 2블록으로 나뉘어 지며, 메시지 인증을 위해 MAC

이 더해진다. 핸드쉐이크 과정을 거쳐 선택된 해쉬 알고리즘에 따라 MAC의 크기는 가변적으로 변하게 되어 MD5일 경우 16바이트, SHA일 경우 20바이트가 추가적으로 더해진다. 총 전송데이터는 16,000바이트 이상이므로 수신측에서는 부분복호화를 위해 MAC의 크기에 관계없이 비암호화 데이터 8000바이트를 제외한 부분을 복호화 대상 데이터로 판단할 수 있다.

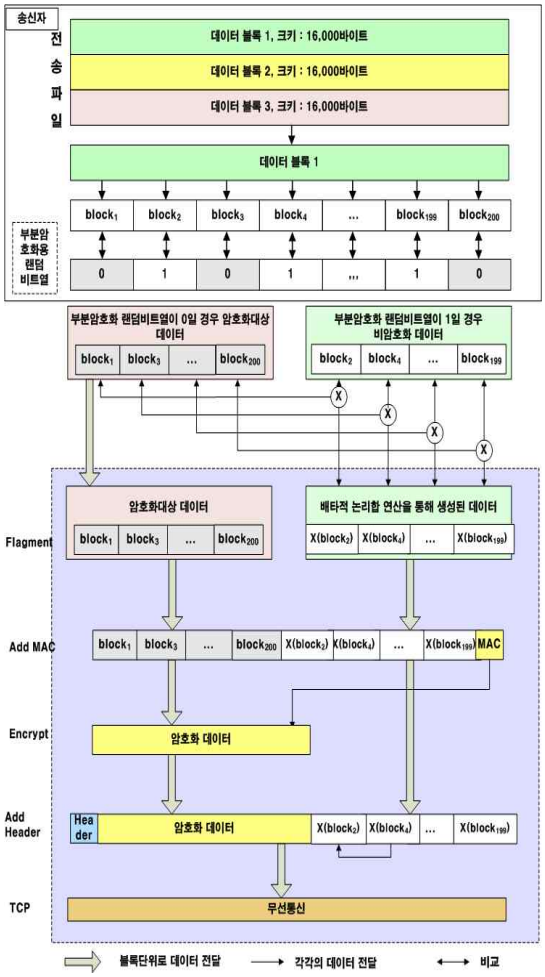

그림 2. 제안기법의 복호화 방안
Fig 2. Partially cryption method of proposed scheme

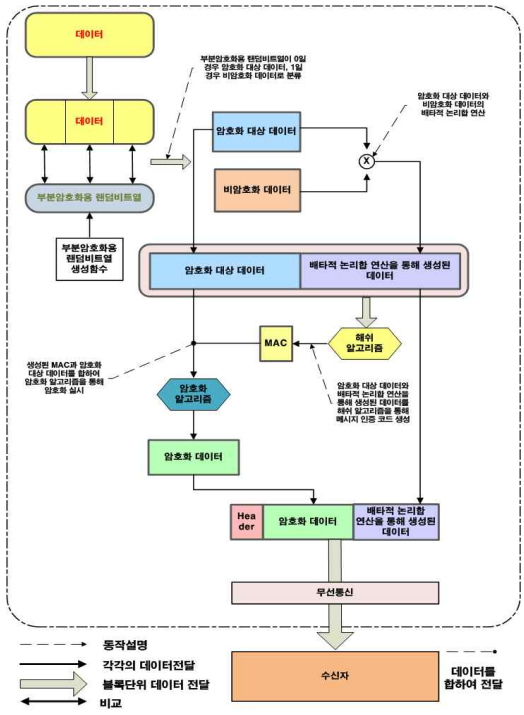

그림 3. 데이터 송신 알고리즘
Fig 3. Data sending algorithm

16,000 바이트 크기의 데이터를 버퍼에 저장한 후 사전에 생성한 200개의 부분암호화용 랜덤 비트열(암호화를 위한 100개의 패턴과 비암호화를 위한 100개의 비암호 패턴)을 80 바이트 크기로 각각 적용하여 8,000 바이트의 암호화될 메시지와 8,000 바이트의 비암호화될 메시지로 비트열을 구분한다. 암호패턴에 의해 선택된 8,000 바이트의 메시지는 암호 알고리즘을 통해 메시지를 암호화하고 8,000 바이트의 비암호화될 메시지는 암호화되기 전의 8,000 바이트 메시지와 배타적 논리합 연산을 수행한 후 암호화된 8,000 바이트의 메시지와 결합하여 수신자에게 전달한다.

3.2 부분 복호화 방안

제안하는 부분복호화 방법은 그림 4을 통해 알 수 있다. 무선을 통해 전달받은 데이터는 뒷부분의 배타적 논리합 연산을 통해 생성된 8,000 바이트의 데이터와 MAC을 포함한 8,000 바이트 이상의 암호화 데이터로 구성된다.

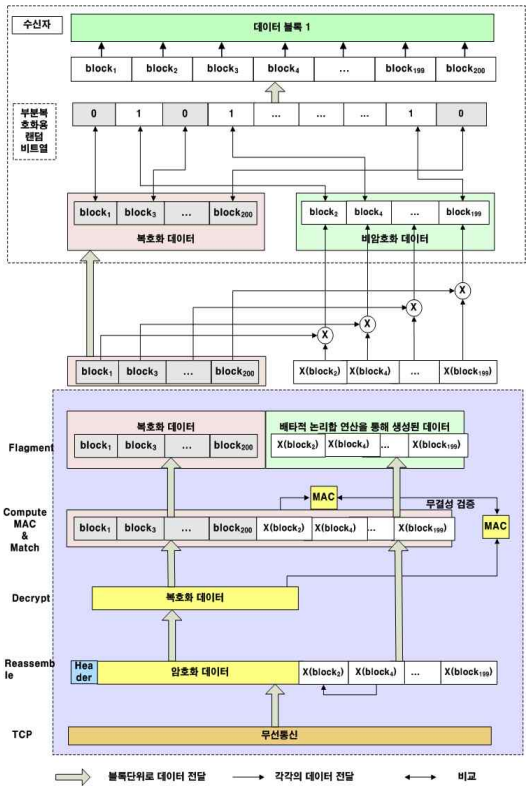

그림 4. 제안기법의 복호화 방안
Fig 4. Partially decryption method of proposed scheme

암호화 데이터는 송신자와 수신자가 사전에 정의된 복호화 알고리즘을 통해 암호화 데이터를 복호화 한다. 복호화 과정이 끝나면 전달받은 데이터의 무결성을 검증하기 위해 배타적 논리합 연산을 통해 생성된 데이터와 복호화 데이터를 결합한 후 해쉬 알고리즘을 적용하여 MAC을 계산한다. MAC을 통해 무결성을 검증받은 데이터는 복호화 데이터와 배타적 논리합 연산을 통해 생성된 데이터를 각각 80바이트로 세분화한 후 복호화 데이터와 배타적 논리합 연산을 통해 생성된 데이터를 순서대로 서로 배타적 논리합 연산을 수행한다. 배타적 논리합 연산을 통해 생성된 비암호화 데이터와 복호화 데이터는 부분복호화용 랜덤 비트열을 이용하여 평문 데이터를 생성한다. 생성된 평문 데이터는 부분암호화용 랜덤 비트열의 비트를 0과 1로 읽어 들여 비트가 0일 경우는 복호화 데이터에서 80바이트를 불러 버퍼에 저장하고, 비트가 1일 경우는 비암호화 데이터에서 80바이트의 데이터를 버퍼에 저장한다.

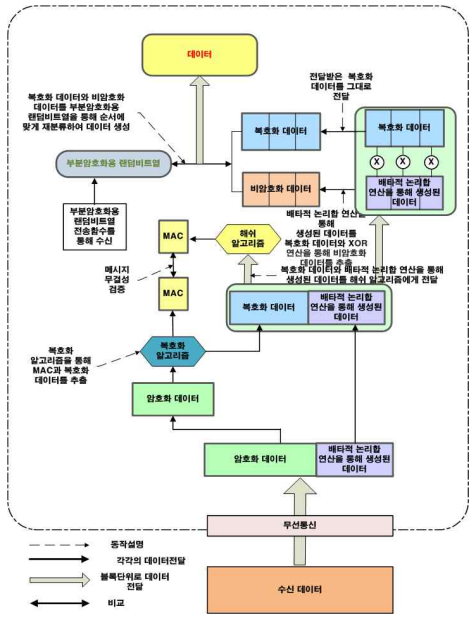

그림 5. 데이터 수신 알고리즘
Fig 5. Data receiving algorithm

그림 5를 통해 송신자로부터 전송받은 부분암호화용 랜덤 비트열을 생성하여 수신 비트열들을 부분 복호화 패턴을 이용하여 평문 비트열을 얻어 텍스트 파일로 출력하는 과정을 알 수 있다. 16,000 바이트의 데이터를 수신한 후 암호 패턴정보에 의해 8,000 바이트의 암호화 데이터와 8,000 바이트의 배타적 논리합 연산에 의해 생성되었던 비암호화 데이터로 비트열을 구분한다. 구분된 데이터 중 암호화된 8,000 바이트의 데이터는 암호화 알고리즘을 통해 복호화 되고 배타적 논리합 연산을 통해 생성된 8,000 바이트의 데이트는 복호화된 데이터와 배타적 논리합 연산과정을 통해 비암호화된 데이터를 생성한다. 생성된 복호화 데이터와 비암호화된 데이터는 암호화 패턴 정보에 의해 소스 데이터로 통합된다.

4. 평가

성능 평가는 파일 형식과 크기에 따라 데이터를 전체 암호화하는 방식과 부분 암호화의 암·복호화 처리시간을 서로 비교하여 효율성을 측정하였다.

4.1 고려사항

① 클라이언트에서 서버로 데이터가 전송될 때 네트

워크의 상태에 따라 전송속도가 다르기 때문에 네트워크를 통해 전송되는 과정에서의 전송 처리시간은 배제한다.

② 전체 암호화와 부분암호화 부분을 제외한 모든 부분이 동일하기 때문에 데이터 전송 처리시간은 전체 암호화와 부분암호화만을 고려하여 측정

③ 부분암호화는 데이터를 분리하고, 분리된 하나의 데이터는 암호화되며 또 다른 데이터는 배타적 논리합(XOR)을 수행 후 두개의 데이터를 결합되는 4가지 처리과정을 포함한다.

4.2 수행결과

그림 6은 20Mbyte 텍스트에서의 전체 암호화와 부분암호화의 시간 비교를 보여주고 있다.

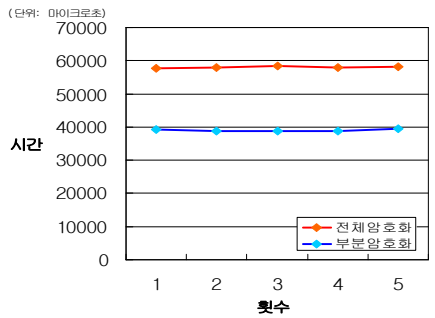

그림 6. 20Mbyte 텍스트에서의 전체 암호화와 부분암호화 시간 비교

Fig 6. Time comparison of whole and partial encryption with 20Mbyte text file

표 2. 파일크기에 따른 비교

Table 2. Comparison by file size

단위 : ms

	텍스트파일	워드파일	이진파일
16KB	257	255	255
2MB	58076	61164	59306
20MB	689590	680328	669479

4.3 분석

① 부분암호화는 전체 암호화의 처리시간보다 20 - 30% 단축하였다.

② 데이터를 100% 암호화한 전체 암호화에 비해 부분암호화는 데이터가 50% 암호화된 상태이기 때문에 전체 암호화보다 50%의 시간이 단축되었다.

③ 데이터 분리, 배타적 논리합(XOR) 연산, 데이터 결합 등의 처리시간이 전체 암호화보다 25%의 시간이 소요되었다.

④ 분리, XOR, 암호화, 결합의 4가지 과정을 포함하고 있는 부분 암호화는 전체 암호화보다 처리시간이 적게 소요됨을 보여 주고 있다.

5. 결론

본 논문에서 제안하는 부분암호화 기반 핸드오버는 기존의 PKMv2를 상속하므로 EAP인증, AES기반 기밀성 제공 알고리즘, CMAC/HMAC을 제공하며, TEK를 통한 데이터 암·복호화를 부분적으로 하므로 전체를 암호화했을 때보다 시간이 단축된다. 따라서, 핸드오버시 인증 및 키교환 단계를 거친 후 빠른 데이터 전송시 유리하므로 핸드오버에 따른 지연이 현저히 줄어들게 되어 VoIP, Video Streaming Service같은 실시간 서비스들을 충분히 지원한다. 관련자료[2]에 따르면 VoIP는 약 50ms , Video Streaming Service는 100ms의 지연을 넘어선 안된다. 그러므로 본 제안모델을 이용할 경우 신속한 핸드오버를 통한 QoS를 유지할 수 있다. 평가를 통해 핸드오버 지연시간을 줄이고 보안성을 유지시켜 본 모델의 우수성이 입증되었음을 확인하였다.

참 고 문 헌

[1] J. B. Hur, et al., "Security Considerations for handover Schemes in Mobile WiMAX networks", IEEE Wireless Communications and networking Conference, 2008. pp. 2531~2536, March 31 2008

[2] WiMAX Forum, "Mobile WiMAX - Part I : A Technology Overview and Performance Evaluation", February 2006.

[3] IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005, "Amendment2 for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", November 2005.

[4] H. J. Jang, et al., "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks", draft-ietf-mishop-fh80216e-01.txt, Jan. 2007.

[5] R. Koodli, Ed., "Fast Handovers for Mobile IPv6", IETF,

RFC 4068, July 2005.
[6] D. H. Lee, et al., “Fast Handover algorithm for IEEE 802.16e Broadband Wireless Access System”, 1st IEEE Symposium on Wireless Pervasive Computing, 2006.
[7] J. Arkko, et al., "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement", IETF, RFC 4187, Jan. 2006.

저 자 소 개

김 기 수 (Kim Ki Soo)

- 2007 : 충북대학교 정보통신공학 학사
- 2009 : 충북대학교 전자계산학 석사
- 2009 ~ 현재 : 한국아이티평가원

<관심분야> : Mobile WiMAX, HandOver, 네트워크보안

김 윤 철 (Kim Yoon Chul)

- 1988 : 한국산업기술대학교 컴퓨터 공학과 졸업.
- 1988 ~ 1996 : 삼보컴퓨터
- 1996 ~ 2005 : 두루넷
- 2006 : 하나로 텔레콤
- 2008 ~ 현재 : ㈜유앤비테크

<관심분야> : 그리드컴퓨팅, 클라우드보안, 네트워크보안

이 상 호(Sang-Ho Lee) [정회원]

- 1976년 2월 : 숭실대학교 전자계산학과 학사
- 1981년 2월 : 숭실대학교 전자계산학과 석사
- 1989년 2월 : 숭실대학교 전자계산학과 박사
- 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> : 네트워크보안, Protocol Engineering Network Management