IMT-2000 이동통신시스템의 보안기능 요구 분석 및 설계

권 수 근, 신 경 철*, 김 진 업*, 김 대식*
경주대학교 컴퓨터전자공학부, *ETRI
전화 : 054-770-5176 / 핸드폰 : 016-863-5176

Analysis and Design of Security Feature in IMT-2000

Sookun Kwon, Kyongchul Shin, Jinup Kim, Daesik Kim
Dept. of Computer and Communication, Kyungju University
E-mail : skkwon@kyungju.ac.kr

Abstract

Security-related issues in mobile communications are increasing. The security requirements of mobile communications for the mobile users include authentication of the mobile user, the data confidentiality, the data confidentiality and the location privacy of mobile user. These services require security features compatible with the wireline networks. However, wireless networks have many restrictions compare to wireline networks such as the limited computational capability of mobile equipment and limited resource(bandwidth) between a mobile user and a fixed network. So, security features for IMT-2000 are designed to meet the limited capacity. In this paper, we analyze the required security features and mechanism, and design network access security feature effective for IMT-2000 Systems. The design includes security functions allocation to each system. Finally, discuss the computational power of each system based on allocated functions to it.

I. 서론

이동통신은 공간의 제약을 받지 않는 서비스의 이점으로 인하여 수요가 폭발적으로 증가하고 있다. 2세대 이동통신 시스템인 CDMA방식의 Digital Cellular System(DCS)과 Personal Cellular System(PCS)의 경우 우리나라가 세계최초로 상용화 개발에 성공하였으며, 현재 CDMA 이동통신 세계시장에서의 점유율도 세계 1위이다. 현재의 2세대 이동통신시스템은 음성 서비스는 충분히 제공하고 있으나 점차 수요가 증대되고 있는 영상서비스, 인터넷 등 멀티미디어 서비스의 제공에는 한계를 가지고 있다. 이동멀티미디어 서비스를 제공하기 위해 3세대 이동통신시스템인 International Mobile Telecomm-unications-2000 (IMT-2000)이 개발되고 있다. IMT-2000의 무선접속 국제표준으로 광대역 CDMA 방식이 채택되었다. 유럽, 일본 등은 W-CDMA 방식 중 비동기 방식을 사용한 무선접속방식이 채택되어 3GPP 표준화기구에서 각종 규격에 대한 표준화를 진행시키고 있으며 우리나라도 ETRI를 중심으로 세계시장으로의 진출 및 국내 서비스를 위하여 비동기방식 IMT-2000을 연구개발 중이다. 비동기 방식을 적용한 IMT-2000 이동통신시스템의 연구개발에서 기본통신기능은 상당한 정도의 연구가 진행되어 본격적인 개발이 진행중이다. 그러나 가입자가 수시로 위치를 변경하는 이동통신에서 절대적으로 요구되며, 또한 기존의 음성통신위주에서 WAP를 적용한 무선인터넷수요가 음성서비스를 능가하게 될 차세대이동통신의 경우 가입자에 대하 인증 및 보안에 대한 연구는 매우 중요한 기술이나 국내외적으로 활발한 연구가 진행되고 있지 않고 있다. 본 연구에서는 비동기 방식의 IMT-2000에서의 인증 및 보안 기능에 대한 요구사항을 분석하고 또한 이를 바탕으로 한 무선 프로토콜을 설계한다. 또한 각 구성요소별 기능할당을 수행하고 각 구성요소의 처리 성능을 분

석한다.

II. IMT-2000 인증 및 보안서비스 요구 사항

2.1 엑세스 관련 요구사항
- IMT-2000 party 모방의 어려움
- 서비스 가용성 제한 불가
- 사용중인 트래픽채널의 hijacking 어려움
- 전송된 사용자 정보, 제어정보의 수정 어려움
- 사용자의 저장된 가입정보에 엑세스, read, 수정하기 어려움
- 인증 증명 메커니즘 요구

2.2 무선접속관련 요구사항
- 무선링크 통신 내용의 복호의 어려움
- 사용자 위치 추적의 어려움
- 특정통신과 연관된 사용자 확인의 어려움
- 무선접속과 관련된 신호 정보, 제어 정보의 비밀 보장

2.3 터미널 관련 요구사항
- 도난 단말기의 식별 가능, 그것을 통한 엑세스 제한
- UIM human 사용자 직간접 인증 가능
- UIM의 사용자 보안 관련 정보 방어

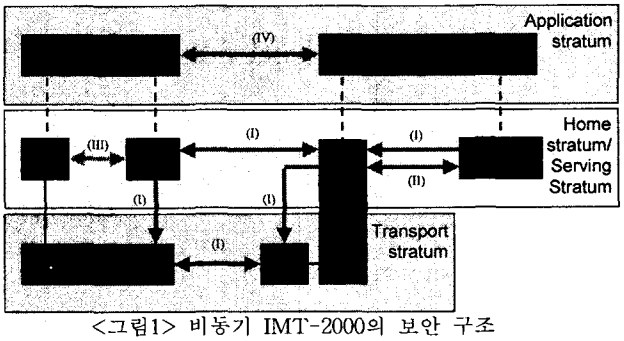
2.4 망 운용 요구사항
- 도난 단말기의 식별 가능, 그것을 통한 엑세스 제한
- UIM human 사용자 직간접 인증 가능
- UIM의 사용자 보안 관련 정보 방어

2.5 보안 관리 요구사항
- 보안 키, UIM secure 관리 갱신
- 가입자 연관 사건 기록을 위한 보안 메커니즘 요구
- 보안 메커니즘의 버전 관리 갱신 가능

III. 비동기 방식의 보안 구조

그림1은 비동기 IMT-2000의 보안 구조를 보여준다. 비동기 방식 IMT-2000 보안 서비스 제공을 위해서는 아래의 5개의 기능군으로 정의할 수 있다.

- 망 접속 보안(Network access security, I): 3G 서비스에 보안 엑세스를 제공하는 기능군으로 특히 무선접속구간에서 침입을 방지한다.
- 망영역 보안(Network domain security, II) : 서비스 제공자 영역에서 각 노드들간의 신호정보들의 안전한 교환을 제공하는 기능군으로 유선망에서의 침입을 방지한다.
- 사용자 영역 보안(User domain security, III) : 이동국 접속시 보안을 제공하는 기능군
- 응용영역 보안(Application domain security, IV) : 사용자 및 서비스제공자의 영역에서 응용부의 메시지 교환의 보안을 지원하는 기능군
- 보안기능의 가시성 및 구성능력(Visibility and configurability of security, V) : 사용자가 보안기능이 수행되고 있는지 여부를 알 수 있는지 여부와 서비스의 사용 및 제공이 보안기능에 따라 제공되는 기능군



<그림1> 비동기 IMT-2000의 보안 구조

IV. 비동기 IMT-2000 보안 기능 특성

4.1 망 접속 보안

가. 사용자 신원의 비밀성

아래의 사용자신원 비밀성(user identity confidentiality)과 관련된 보안기능이 제공된다.
- 사용자신원 비밀성 (user identity confidentiality): 서비스 대상 사용자의 permanent user identity (IMUI)이 무선링크 상에서 노출되지 않아야 한다.
- 사용자위치 비밀성 (user identity confidentiality): 사용자가 어떤 지역에 위치하는지 무선링크 상에서 노출되지 않아야 한다.
- 사용자 비추적성(user untraceability): 침입자가 무선링크를 통해 동일사용자에게 다른 서비스가 전달되는지 추적할 수 없어야 한다.

위의 목적을 달성하기 위해 사용자는 일반적으로 방문 서비스망에 알려진 temporary identity에 의하여 확인되거나 암호화된 permanent identity에 의하여 확인된다. 사용자 신원의 야기하는 사용자의 추적을 피하기 위해 오랜 시간 동안 동일한 temporary or encrypted identity를 사용하지 않아야 한다. 위의 보안기능을 위해 추가적으로 사용자 신원을 노출시킬 수 있는 신호 및 사용자 정보는 무선 링크 상에서 암호화되어야 한다.

Temporary identity에 사용자 신원을 제공하는 방식은 위치등록, 서비스요청, detach 요청, 연결설정 요청 등에

무선 링크 상에서 사용되어야 한다.

Temporary identity를 방문 서비스 제공망이 알지 못하는 경우 USIM과 HE간의 transparent channel을 통해 encrypted permanent identity을 사용하여 제공된다. 방문서비스 제공망은 encrypted permanent identity을 HE로 전달하여 복호된 사용자의 user's permanent identity를 수신한다. 선택적으로 사용자가 permanent identity를 사용하여 자신을 확인할 수 있도록 허용할 수 있다.

나. 인증(authentication)

인증과 관련된 아래의 보안기능이 제공된다.

- 인증 메커니즘 동의(authentication mechanism agreement): 사용자와 서비스제공망은 안전하게 인증 및 이후에 사용될 키를 협상할 수 있는 특성이다.
- 사용자 인증(user authentication):서비스망이 사용자와 협의하여 사용자의 신원을 확인하는 특성이다.
- 망 인증(network authentication): 사용자가 서비스망이 HE에 의하여 인증된 망인지를 확인하는 특성이다.

인증은 사용자와 단말사이에 각 연결 설정 시 마다 일어나야 한다고 가정한다. 인증은 두가지의 메커니즘이 제공된다. 하나는 HE에 의하여 서비스망에 전달된 authentication vector를 사용하는 방식 이고, 다른 하나는 이전에 수행된 인증 및 키 설정 절차에 따라 사용자와 서비스망간에 설정된 integrity key를 사용하여 로컬 인증을 하는 방법이다.

인증 및 키 설정은 로컬인증에 사용되는 derived integrity key 의 최대수가 수행된 경우 서비스망에 첫번째 위치 등록 후, 서비스 요청 후, 위치 수정 요청 후, detach request 또는 연결 재설정 요구 후에 서비스망에 의하여 요청된다.

로컬 인증은 사용되는 derived integrity key 의 최대 수에 도달되지 않은 경우 서비스망에 첫번째 위치등록후, 서비스요청후, 위치수정요청후, detach request 또는 연결 재설정요구후에 서비스망에 의하여 요청된다.

다. 기밀성(Confidentiality)

아래의 보안기능이 데이터의 비밀성 유지를 위해 망 엑세스 링크에서 제공된다.

- 암호 알고리즘 합의(cipher algorithm agreement) : MS와 SN이 사용할 암호 알고리즘을 협상할 수 있는 특성
- 암호 키 합의(cipher key agreement) : MS와 SN이 사용할 암호키를 협상할 수 있는 특성
- 사용자 데이터의 기밀성(confidentiality of user data): 사용자 데이터가 무선링크상에서 노출 되지 않는 특성
- 신호 데이터의 기밀성(confidentiality of signalling data): 사용자 데이터가 무선링크 상에서 노출 되지 않는 특성

암호키 합의는 인증 및 키합의를 위한 메키니즘의 수행으로 실현되며, 암호 알고리즘의 합의는 사용자와 망간의 보안모드 협상에 의하여 실현된다.

라. 데이터 무결성 (Data integrity)

아래의 보안기능이 망 엑세스 링크에서 데이터의 무결성을 위해 제공된다.

-무결성 알고리즘 합의(integrity algorithm agreement) : MS와 SN이 안전하게 무결성 알고리즘을 협의할 수 있는 특성

-무결성 키 합의(integrity key agreement): MS와 SN이 사용할 무결성 키를 합의하는 특성

-데이터 무결성 및 신호데이타의 인증(data integrity and origin authentication of signalling data): 수신엔티티(MS or SN)가 수신한 신호정보가 도중에 허가되지 않은 방법으로 변경되지 않았음을 확인할 수 있는 특성 및 수신한 신호 데이터의 데이터 origin이 요구한것임을 확인 할 수 있는 특성.

무결성 키(Integrity Key) 합의는 인증 및 키합의를 위한 메키니즘의 수행으로 실현되며, 무결성 알고리즘의 합의는 사용자와 망간의 보안모드 협상에 의하여 실현된다.

V. 시스템별 기능 할당

일부 보안기능은 아주 높은 처리능력을 요구하며, 시스템간의 신호교환은 시스템별 기능할당에 많이 좌우되기 때문에 필요로 하기 때문에 각 시스템으로의 기능할당은 매우 중요한 사항이다[2][3]. 본 연구에서는 기능할당에 3개의 주요한 요소를 고려하였다.

i) 신호메세지 전달의 최소화 : 무선링크상의 제한된 대역폭 고려
ii) 무선대역폭의 효율성 : 무선구간 대역폭의 고비용 부담
iii) 낮은 계산 부하 이동단말기의 제한된 계산 능력

5.1 각 시스템의 처리능력 및 링크 특성분석

o UIM<->MT

User Interface Module과 Mobile Terminal간은 동일 장소에 위치하는 시스템으로서 연결상의 통신제약사항은 없다. MT는 이동성 위해 소형화, 경량화, 저전력등의

요구 특성에 따라 처리용량의 제한을 가진다.

o MT<->RNC

MT와 RNC간은 무선으로 연결되는 부분으로서 무선 자원의 제한으로 인한 통신용량의 제한이 가장크며 또한 무선전송상의보안에 대해 가장 취약한 부분이다.

o RNC<->MSC/VLR

RNC와 MSC/VLR간은 위치적으로 멀리 떨어져서 존재하며 하나의 MSC는 많은 RNC와 상대한다. 두 시스템은 유, 무선으로 모두 연결 가능하나 일반적으로 유선으로 연결되며 광케이블 등 기존의 초고속통신 미디어를 사용할 수 있어 통신용량에는 큰 제한이 없다.

o MSC/VLR<->HLR/AuC

MSC/VLR와 HLR/AuC은 위치적으로 멀리 떨어져서 존재하며 하나의 HLR/AuC은 많은 MSC/VLR한다. 두 시스템은 유으로 연결되며광케이블 등 기존의 초고속통신 미디어를 사용할 수 있어 통신용량에는 큰 제한이 없다. MSC/VLR은 각종 하드웨어를 제어하기 위해 임베디드 시스템으로 구성되며 HLR은 데이터처리위주의 기능을 수행하여 상용 컴퓨터를 사용하다. HLR은 이동성 제공 등을 위해 많은 가입자의 정보변화를 관리해야 하므로 처리용량의 제한을 가진다.

5.2 시스템별 기능할당

o 가입자 신원의 기밀성

가입자신원의 기밀성을 유지하기 위해 TMSI를 운용하는 기능으로 MSC/VLR에서 TSMI를 할당하고 저앗하며 MT에도 이를 통보하여 일정기간동안 TMSI를 통하여 통신한다.

o 인증 및 키 합의

인증 및 키 합의는 보안의 가장 핵심부분으로 보안성이 가장 우수한 HLR/AuC의 주관하에 기능이 수행되야 한다. HLR/AuC는 전체가입자의 정보를 관리하므로 처리능력의 한계를 가지며 서비스시 지연시간등을 고려하며 실제적인 인정 키관리 및 인증처리기능은 각 MSC/VLR로 분산하여 처리한다. 따라서 MSC/VLR는 관리하는 정보에 대하여 확실한 보안대책이 마련되야 한다. HLR/AuC에서 인증벡터를 발생시키고 이 데이터를 전달받아 MSC/VLR에서 인증정보를 보관하며 서비스 시 MT와 연동하여 인증기능을 수행한다.

o 엑세스 링크 데이타 무결성 및 기밀성

엑세스 링크 데이타 무결성 및 기밀성은 무선링크의 종단이 되는 RNC와 MT에서 수행한다. 이를 위해 RNC와 MT는 각 종 키 값과 sequence number, dircetion bit, random number 등을 관리해야 한다.

VI. 결 론

IMT-2000은 여러 무선접속을 통한 멀티 환경과 높은 접속용량을 통해 멀티미디어 서비스를 제공할 수 있어야 한다. 유선 멀티미디어통신에서와 마찬가지로, IMT-2000 서비스의 주된 서비스 대상은 무선인터넷 서비스, 무선을 통한 전자상거래 등이 될 것이다.

이들 서비스는 고정망에서와 동일한 정도의 보안서비스를 요구한다. 그러나 이동망은 고정망에 비해 단말기의 제한된 계산 능력, 단말기와 망간의 제한된 무선전송대역 등 여러 가지 제한된 특성을 가진다. 따라서 IMT-2000에서 위와 같은 제한된 자원을 극복하고 효과적인 서비스를 위한 보안기능 설계를 요구한다.

본 논문에서는 IMT-2000에서 요구하는 보안기능과 메카니즘을 분석하고 이를 기준으로한 효과적인 인 보안 기능구조를 제시하였다. IMT-2000을 구성하는 각 단말기, RNC, MSC, HLR, VLR AuC 등 각 시스템의 부하능력과 전체기능을 고려한 기능할당을 수행하였다.

참고문헌

1. N. Joshi etc., cdma-2000 Evloution of cdmaone to IMT-2000, Bell Labs Tech. J., 1998
2. UMTS 30.03, Universal Mobile Telcom. System
3. 3G TS 33.102 version 3.4.0 Release 1999, Security Architecture
4. Lee CH, Hwang MS, Yang WP, Enhanced privacy and authentication for the global system for mobile communications, *Wireless Networks* , Vol.5 No.4 , pp. 231-243 , 1999.
5. Lo CC, Chen YJ, Secure communication mechanisms for GSM networks, *IEEE Transactions on Consumer Electronics*, Vol.45 No.4, pp. 1074-1080 , 1999.
6. Boyd C, Mathuria A, Key establishment protocols for secure mobile communications: a critical survey, *Computer Communications*, Vol.23 No.5-6, p. 575-587 , 20000
7. Park C.S., ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS, *IEEE Network* , Vol.11 No.5 , 50-55 , Sep. 1997.