IMT-2000 시스템의 보안 위협요소 분석 및 이의 적용에 따른 무선링크 트래픽 분석

정회원 권 수 근*

Analysis of Security Threats and Air Interface Traffic Performance for IMT-2000 Mobile Systems

Soo-kun Kwon* *Regular Member*

요 약

IMT-2000 이동통신시스템에서는 빠른 전송속도의 지원으로 무선인터넷, 전자상거래 등 많은 응용서비스의 제공이 예상된다. 이들 서비스는 인증, 데이터 무결성, 데이터 암호화, 부인방지 등 높은 수준의 보안기능을 요구한다. 본 논문에서는 IMT-2000의 새로운 보안위협 요소를 분석하고 이에 따른 이동국과 기지국간 무선링크의 성능 분석을 수행하였다. 망 접속보안서비스의 지원에 필요한 무선구간의 신호트래픽은 평균메시지의 길이가 256~768bits, 기본서비스 대비 보안서비스 발생율이 0.2~1.0, 기본서비스의 발생율이 0.2~1.0서비스/호 인 조건에서 최소 0.2kbps에서 최대 4.5kbps로 분석되었다.

ABSTRACT

IMT-2000 mobile system will provide many application services such as mobile internet, wireless electronics commerce applications using air interface with high data rate. These applications require high data integrity, data confidentiality, user authentication, user identity confidentiality and non-repudiation. In this study, we analyze new security threats and air interface traffic performance for IMT-2000 mobile systems. Signal traffic for network access security services requires 0.2kbps~4.5kbps with the conditions of 246~768bits/message, 0.2~1.0 basic services/sec and the security services of the rate of 0.2~1.0 times compared with basic services.

Ⅰ. 서 론

이동통신은 공간의 제약을 받지 않는 서비스의 이점으로 인하여 수요가 폭발적으로 증가하고 있다. 2세대 이동통신시스템인 CDMA방식의 Digital Cellular System(DCS)과 Personal Cellular System (PCS)의 경우 우리나라가 세계최초로 상용화 개발에 성공하였으며, 현재 광범위하게 서비스되고 있다. 2세대 이동통신시스템은 음성서비스는 충분히 제공하고 있으나 점차 수요가 증대되고 있는 영상서비스, 무선인터넷 등 멀티미디어 서비스의 제공에는 한계를 가지고 있다. 이동멀티미디어 서비스를 제공하기 위해 3세대 이동통신시스템인 IMT-2000이 개발되고 있다. IMT-2000의 무선접속 국제표준으로 광대역 CDMA 방식이 채택되었으며 3GPP, 3GPP2등의 국제표준기구에서 동기 및 비동기방식에 대한 표준화를 진행하고 있으며, 국내에서도 많은 연구가 진행되고 있다[1,2,3,4].

보안에 취약한 무선구간을 포함하는 이동통신에서 절대적으로 요구되며, 또한 기존의 음성통신위주에서 무선인터넷서비스, 전자상거래 등의 수요가 음성서비스를 능가하게 될 차세대이동통신의 경우 가입자에 대한 인증 및 보안에 대한 연구는 매우 중요한 기술이다[5,6,7,8]. 보안을 요구하는 응용서비스를

* 경주대학교 컴퓨터전자공학부(skkwon@kyongju.ac.kr)
논문번호 : K01172-0730, 접수일자 : 2001년 7월 30일

지원하기 위해 IMT-2000 이동통신시스템에서도 유선에서와 동일한 수준의 사용자 인증, 데이터 무결성 및 기밀성 유지, 부인방지 등의 보안절차가 요구된다. 그러나 IMT-2000과 같은 이동통신시스템에서는 무선링크상의 제한된 대역폭을 고려한 신호메세지 전달의 최소화, 무선자원의 고비용 부담을 고려한 무선대역폭의 효율적인 사용, 이동단말기의 제한된 계산능력 등의 제한요소를 가지며 이에 대한 고려가 필요하다. 지금까지 이동통신을 위한 인증 및 키 설정방식, 암호화, 무결성, 부인방지 등의 서비스시 이동국과 무선링크의 부하를 감소시키기 위한 많은 연구가 진행되고 있다[9,10,11]. 그러나 셀 설계, 효율적인 무선 프로토콜 설계, 신호채널 설계 등에 필수적으로 요구되는 보안서비스 처리에 따른 무선링크에서의 성능분석에 대한 연구가 미흡하다. 본 논문에서는 IMT-2000에서 요구되는 보안위협요소를 분석하고, 보안 기능의 적용에 따른 무선링크상의 신호트래픽을 분석한다. 본 논문은 다음과 같이 구성된다. II장에서는 IMT-2000의 보안기능의 목표를 살펴보고, III장에서는 IMT-2000의 보안 위협요소를 분석한다. IV장에서는 망접속 보안기능 적용에 따른 무선링크 성능을 분석하고 끝으로 V 장에서 결론을 내린다.

II. IMT-2000 보안기능의 목표

보안의 목적은 사용자 정보 및 이와 관련된 정보, 망에 의해 제공되는 서비스나 자원이 오용되거나 잘못 사용되는 것을 방지하는 것이다. 특히 이동망에서는 보안에 취약한 무선접속구간에서의 정보보호, 다른 망으로의 로밍 서비스 제공시의 보안기능, 표준 암호화 알고리즘 제공에 의한 단말의 이동성 제공 기능 등이 추가적으로 요구된다.

IMT-2000에서의 보안은 새로운 위협이나 서비스를 위해 확장된 기능과 메커니즘 제공을 요구하며 또한 기존 2세대 이동통신시스템과의 호환성이 고려 되야한다. 이를 고려하여 IMT-2000의 보안기능은 2세대 이동통신시스템의 보안을 기본으로 하여 GSM, CDMA 및 다른 2세대 시스템에서 필요성 및 안정성이 증명된 기능은 IMT-2000에서도 적용되며, 2세대시스템 보안기능의 취약점을 개선하고 새로운 기능 및 서비스의 제공을 특징으로 한다.

먼저 IMT-2000에서도 유지되야할 2세대의 보안기능으로는 선택적 인증 및 이의 암호화에 대한 기능을 강화한 엑세스 가입자에 대한 인증 기능, 암호화의 세기가 2세대보다 강화되고 빠른 처리 능력을 가진 새로운 장비들에 대한 위협에 대처를 고려한 무선접속 구간의 암호화, 좀더 안전한 방식을 제공하는 무선상의 가입자 신원 기밀성 유지 등이 있다. 또한 보안기능에 따른 단말의 변화를 방지하기 위한 움직일 수 있는 하드웨어 보안 모듈 등을 사용한 보안기능과 단말의 독립성, SIM (Subscriber Interface Module)과 망 계층 서버 사이의 보안 응용계층 제공, 보안기능을 위한 서비스망(SN:Serving Network)에서의 역할 최소화 등이 IMT-2000에서도 지속적으로 유지되야 한다[2,3].

2세대 이동시스템의 보안기능 중에서 IMT-2000에서 보완되야할 요소로는 비인가 기지국에 의한 active attacks의 가능성, 암호 키와 인증 데이터의 망 내 비암호상태로 전달, 암호화가 핵심망에 까지 확장되지 않으며 결과적으로 사용자 정보와 신호 데이터가 마이크로웨이브 링크상에 비암호화 문서로 전달되는 문제, 기존에 생성된 암호 키를 사용하는 사용자 인증과 채널상의 하이제킹 방지가 사용자 암호화에 의존하는 점들이다. 또한 암호화가 일부 망내에서는 사용되지 않아 기만의 가능성이 있으며 데이터 무결성(integrity)이 제공되지 않아 잘못된 기지국의 공격을 가능하게 하며 암호화가 없는 경우 채널 하이제킹이 가능한 점, IMEI가 보안되지 못하며 SN간을 로밍하는 가입자에 대해 SN이 어떻게 인증 파라메터를 사용하는지 관리하는지 HE ((Home Environment)가 알지 못하는 점, 보안기능의 업그레이드를 위한 유연성이 없는 점등의 문제점이 3세대 이동통신시스템인 IMT-2000에서는 보완되야 한다[4].

2세대 이동통신시스템에서의 유지 및 보완되어야 할 기능과는 별개로 새로운 서비스 제공 및 환경을 가지는 IMT-2000에서는 추가적인 보안요구 기능들이 고려 되야 한다. 다양한 컨텐츠 제공, 멀티미디어 서비스 제공, HLR only 서비스 제공 등의 새로운 서비스 제공에 따른 보안기능, 유선에 비해 우선하는 서비스 선호도, prepaid 및 pay-as-you-go 서비스에 대한 변형 제공, 서비스 프로파일 및 단말기의 능력에 대한 사용자의 증가된 제어, 장치가 네트워크의 일부인 것처럼 동작하는 active attack의 증가 등에 대한 대처가 필요하다. 또한 단말기가 e-commerce나 다른 응용서비스의 플랫폼으로 사용가능하다. 즉 다중응용 스마트카드가 단말기와 같이 사용가능하며 스마트카드나 단말기가 이것을 허용하기 위해 Java와 같은 가상환경을 지원하여야 하며

바이오 메트릭 방법을 사용하여 개인 인증을 지원할 수도 있다.

Ⅲ. IMT-2000 보안위협요소 분석

1. 보안 위협요소의 분류

IMT-2000의 보안위협요소로는 민감한 데이터에 대한 비인증 장치로부터의 접근을 방지하는 기밀성 유지, 민감한 데이터에 대한 허가되지 않은 조작을 방지하는 무결성 유지, 망이 제공하는 서비스에 대한 비허가 사용자의 접근 및 남용방지, 사용자나 망이 수행한 사건에 대하여 부인하는 행위 방지 등으로 분류할 수 있다[4].

민감한 데이터에 기밀성 및 무결성을 유지하기 위해서는 침입자가 방지 없이 메시지를 취하는 도청(eavesd -ropping), 침입자가 가입자의 기밀성 있는 정보를 얻기 위해 그들이 합법적인 시스템인 것처럼 하거나 시스템의 정보를 얻기 위해 인증된 가입자처럼 하는 가장(masquerading), 침입자가 사용자의 위치를 알거나 주요한 일이 일어나는지를 알기 위해 메시지의 시간, 속도, 길이, 소스, 목적지 등을 얻는 트래픽 분석, 침입자가 민감한 정보를 위해 데이터 스토리지를 찾는 브라우징, 침입자가 query나 신호를 시스템으로 보내 시스템으로부터 반응을 조사하는 추정(Inference) 등이 방지 되야 한다. 망의 가용성 감소를 방지한 기능으로 침입자가 사용자의 트래픽, 신호, 제어데이타를 재밍하여 인가된 사용자의 사용을 방해하는 Intervention, 침입자가 인가된 서비스에 과부하를 주어 인가된 사용자의 서비스를 방해하는 자원고갈, 사용자나 망이 인가되지 않은 서비스나 정보를 얻기 위해 특권을 오용하는 행위, 침입자가 특수서비스나 시설을 남용하거나 망의 혼란(disruption)을 야기하는 행위, 침입자가 사용자의 망 요소를 가장한 접근, 사용자나 망 요소가 접근 권한을 오용하여 허가되지 않은 서비스에 접근하는 행위 등이 방지 되야 한다. 또한 사용자나 망이 수행한 사건에 대하여 부인하는 행위, 침입자에 의해 메시지의 변경, 삽입, 재연, 삭제 등의 메시지의 조작이 방지 되야 한다.

2. 접속요소별 보안위협요소 분류

IMT-2000 시스템은 단말기, 엑세스 망, 타 망과의 접속을 통하여 서비스가 수행되며 이들 접속구간 및 시스템별로 다양한 보안 위협요소를 가진다. 먼저 무선접속구간에 관련된 보안 위협요소는 데이터에 대한 비인증 접근, 기밀성 위협, 서비스 부인, 서비스에 비인증 접근 등의 카테고리가 있다. 데이터 비인증 접근으로는 사용자 트래픽의 도청, 신호 및 제어정보의 도청, 통신상대로서 가면, 수동적인 트래픽 분석, 능동적인 트래픽 분석 등이 있다. 무결성(Integrity) 위협요소로는 사용자 트래픽 조작, 신호 및 제어 데이터의 조작 등이 가능하다. 서비스 공격의 부인으로는 물리적인 간섭, 프로토콜 간섭, 통신파트너를 가장한 서비스의 부인 등이 가능하며 침입자가 다른 사용자를 가장하여 망에 접근하거나 처음에 침입자가 기지국을 가장하여 가입자에 접근하여 인증이 성립된 후 그의 연결을 하이제킹하는 등의 보안위협 요소들이 존재한다.

다른 시스템 요소와 관련된 위협요소로는 시스템 요소에 저장된 데이터의 비인증 접근, 가입자위치 정보의 노출, 응용부나 데이터로 가장하여 터미널이나 USIM의 동작 조작을 통한 악의적으로 다운로드 행위, 시스템에 저장된 정보의 변경, 과금의 부인, 착,발신 트래픽의 부인 등이 가능하다. 또한 비인증 서비스 접근으로 침입자가 다른 사용자를 가장하여 다른 가입자에게 허가된 서비스를 이용하는 행위, 다른 서비스 망 가장, HE 가장, 사용자 특권의 오용, 서비스망 특권의 오용 등의 행위에 대한 대처가 필요하다.

단말기 및 USIM(User Services Identity Module)과 관련된 위협요소로는 분실된 단말기와 USIM의 사용하는 행위, 빌린 단말기를 사용하여 계약이상으로 사용하는 행위, 유효한 USIM을 분실된 단말기와 사용하는 경우, 단말기 ID를 조작하는 행위, 침입자가 단말기에 저장된 데이터를 수정하거나 추가 삭제하는 처리, 침입자가 USIM에 저장된 데이터를 수정하거나 추가 삭제하는 처리, USIM과 단말기 접속간의 도청 등의 행위가 가능하다.

Ⅳ. 보안기능 적용에 따른 무선링크 성능 분석

본 장에서는 암호화, 인증 등 망접속 보안기능 제공에 따른 무선링크의 성능 분석을 수행한다. 보안기능의 추가에 따라 모든 구성 시스템간의 링크에서 관련 메시지 전송에 따라 부하가 증가하나 추가되는 용량의 처리가 쉽게 해결 가능한 유선구간에서의 성능분석은 제외하고 메시지 증가에 가장 민감한 구간인 무선링크에 대한 성능에 미치는 영향을 분석한다. 이를 위해 먼저 앞에서 연구된 각 시스템별 할당기능을 바탕으로 무선링크상에서 발생되

는 보안 관련 메세지를 분석하고 이를 토대로 신호 및 트래픽 채널에 대한 모델을 설정하고 시뮬레이션을 통하여 보안기능이 무선채널에 미치는 영향을 분석한다.

1. 보안 기능별 메시지용량 분석

망접속 보안 기능인 사용자 신원의 기밀성, 인증 및 키 합의절차, 데이터 무결성, 주기적인 지역 인증을 위한 신호 절차, 국부 인증 및 연결 설정 보안 제어 명령 등을 위해 무선구간을 통하여 전달되어야 하는 메시지에 대하여 분석한다.

사용자 신원의 기밀성을 위해 IMT-2000에서는 각 단말에 대한 암호화 초기화 이후 임시 이동국가입자식별자(TMSI/P-TMSI)를 할당하여야 한다. 그림 1에서 본 바와 같이 이 기능은 단말의 UE와 망요소의 RNC사이에서 수행되며 할당요청 및 할당처리를 위해 무선구간 양방향에서 하나의 메시지가 필요하다. 인증 및 키 합의는 가입자에 대한 인증 수행 및 암호키 변경시 필요한 절차로서 매 호마다 필수 사항은 아니나 운용자가 지정한 시간 경과 시, 최소한 24시간 내 한번은 반드시 수행되어야 하며 무선구간을 포함하는 VLR과 UE 사이에서 신호채널을 통해 양방향 하나의 메시지가 필요하다. IMT-2000에서는 무선구간을 통과하는 모든 신호전달메시지는 전송상의 데이터 무결성을 보장하기 위한 메커니즘이 필수적으로 요구되며 국제표준 절차에 따른 메커니즘 수행시 모든 신호메세지는 원래의 정보에 각 32비트의 정보가 추가된다.

주기적인 로컬 인증을 위한 신호절차는 망접속 보안에 사용되는 COUNT값이 한계치에 도달 시 RNC에 의해 시작되며 COUNT 확인 요청 및 응답을 위해 순방향, 역방향 각 방향별 하나의 무선구간 통과 메시지가 필요하다. 국부 인증 및 연결 설정 절차는 가입자로부터 초기 계층3 메세지 수신 후(첫번째 위치등록후, 서비스요청후, 위치수정요청후, detach request 또는 연결 재설정 요구 후에 서비스망에 의하여 요청) 가입자와 망은 가입자인증 및 키 설정을 위한 절차가 필요하며 이를 위해 순방향, 역방향 각 방향별 하나의 무선구간 통과 메시지가 필요하다. 보안제어 명령절차는 암호절차가 필요한 경우 가입자로부터 초기 계층3 메세지 수신 후 가입자와 망간에 보안 모드 요청 및 응답을 위해 각 방향 하나의 무선구간 메시지가 필요하다. 데이터 기밀성의 경우는 암호화하는 경우 plain text와 cipher text의 메시지 길이가 동일하므로 별도의 추가되는 정보나 메시지는 필요하지 않다. <표1>은 망접속보안을 위한 무선구간의 신호메세지를 보여준다.

표 1. 망접속보안을 위한 무선구간의 신호메세지

서비스 종류	메세지 용도	무선구간의 신호트래픽
기본서비스 처리메세지	· 위치등록 · 서비스요청 · 위치수정 요청 · detach request · 연결 재설정요구	· 서비스 절차에 따름
망접속보안 서비스 처리 메세지	· 사용자정보 기밀성	· 2개 메세지/서비스
	· 인증 및 키 설정	· 2개 메세지/서비스
	· 신호정보 무결성을 위한 정보	· 32bit/메세지
	· 주기적인 로컬 인증	· 2개 메세지/서비스
	· 국부 인증 및 연결 설정 절차	· 2개 메세지/서비스 (인증 및 키 합의시 외 L3엑세스시 발생)
	· 보안제어명령(서비스에 사용될 보안기능 협상)	· 2개 메세지/서비스 (L3 엑세스시 발생)
	· 데이터 기밀성	· 없음

2. 무선신호채널 구조 및 트래픽 모델

본 절에서는 보안기능의 추가에 따른 무선링크상의 신호전송채널의 성능을 분석한다. 무선링크상의 채널은 일반적으로 신호전송과 트래픽 전송이 공유되는 inband 방식과 신호전송과 트래픽 전송이 분리되는 outband 방식으로 나눌 수 있다. 본 성능분석에서는 비동기 방식인 3GPP의 무선접속 규격에 따라 outband 방식을 적용한다. 보안에 관련된 모든 신호메세지는 하나의 uplink 신호채널과 downlink 신호채널로 전달된다고 가정하였다. Uplink 및 downlink의 신호채널속도는 14.4, 32, 64kbps로 가정하였다.

그림 1은 무선구간 신호채널 성능분석을 위한 채널 모델을 보여준다. 신호채널을 통하여 전달되는 신호메시지는 기본서비스를 위한 메시지와 보안기능을 위한 메시지로 분류하였다. 보안관련 메시지는 사용자신원 기밀성 처리 메시지, 인증 및 키 설정 메세지, 로컬인증 처리 메시지, 보안제어 메시지, 주기적인 로컬인증 메시지가 독립적인 메시지로 무선구간을 통해 전달되며 기본서비스를 포함한 메시지

의 무결성을 수행하기 위한 추가 데이터가 모든 메시지에 필요하다. 신호정보는 메시지별로 크기는 다르나 분석의 편의성을 위하여 일반서비스 관련 메시지와 보안관련 메시지 모두 평균 메세지 크기를 256, 512, 768 bits인 경우로 가정하였다. 각 셀에 대해 발, 착신호를 포함한 기본서비스의 발생은 평균이 λ 서비스/초 인 포아손 분포를 가지며, 보안서비스는 서비스 특성에 따라 도달율을 달리하였으며 모두 포아손 분포로 도달한다고 가정하였다.

3. 성능 분석 및 검토

성능분석을 위한 모델로서 각 기지국은 하나의 신호채널을 가지는 것으로 가정하였으며 기본서비스 메시지와 보안기능 관련 신호메세지는 동일한 채널을, 동일한 우선권을 가지는 것으로 가정하였다. 새로운 TMSI 할당, 인증, 암호화 키 및 무결성 키의 갱신 주기는 신호 트래픽 부하에 가장 많은 영향을 미치는 변수이나 각 운용시스템에서 운용자에 의하여 변경이 가능한 요소이다. 본 연구에서는 기지국 단위에서 발생하는 보안기능요구는 기본서비스에 비례하여 발생하는 것으로 가정하였으며 기본서비스 발생율 대비 총 보안기능 발생비율 β 는 0.2에서부터 1까지 변화하는 조건에서 실험하였다

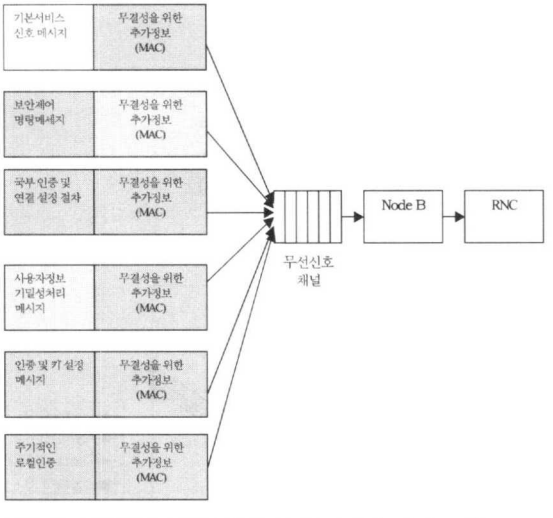

그림 1. 무선구간 신호채널 성능분석을 위한 채널 모델

$$\beta = \frac{\text{보안서비스 발생빈도}}{\text{기본서비스 발생빈도}}$$

성능분석은 기본서비스의 발생율이 0.2~1.0 서비스/초이고 기본서비스에 대한 보안서비스의 발생비율 β가 0.2~1.0인 경우에 대하여 수행하였다. 기본서비스의 경우 호 당 uplink, down 링크 각 방향에 대해 신호메시지 수는 10개로 가정하였다. 여기서 기본서비스는 위치등록, 서비스요청, 위치수정 요청, detach request, 연결 재설정요구 등을 포함하며 보안서비스는 사용자신원 기밀서비스, 인증, 데이터 기밀성, 데이터 무결성 서비스와 주기적인 주기적인 로컬인증 서비스를 고려하였다.

그림 2는 메시지의 평균 메시지 길이를 256bits로 가정한 경우 망접속 보안기능 처리에 소요되는 신호메세지의 무선구간에서의 단방향 전송율을 보여준다. 기본서비스의 발생율 및 기본서비스에 대한 보안서비스의 발생비율의 증가에 따라 거의 선형적으로 증가되며 최대 1.75kbps정도의 전송율이 필요한 것으로 나타났다. 그림 3, 4는 메시지의 평균길이가 512, 768kbps인 경우를 보여주며 기본서비스의 발생율 및 기본서비스에 대한 보안서비스의 발생비율에 따른 증가는 그림 2와 동일하며 이들의 증가에 따라 거의 선형적으로 증가함을 보여준다.

그림 5, 6, 7은 각, 각 uplink 및 downlink의 신호채널 전송속도가 14.4, 32, 64kbps인 경우의 신호메시지 차단 확률이다. 기본서비스는 0.2~1.0서비스/초의 발생율로 포아손 분포를 가지고 발생하며 기본호당 신호메시지는 10개로 가정하였으며 메시지의 평균길이는 256bits로 가정하였다. 기본서비스에 대한 보안서비스의 발생비율 β 는 0.2~1.0 범위에서 변화시켰다. 여기서 기본서비스는 위치등록, 서비스요청, 위치수정 요청, detach request, 연결 재설정요구 등을 포함한다. 보안서비스는 사용자신원 기밀서비스, 인증, 데이터 기밀성, 데이터 무결성 서비스와 주기적인 로컬인증 서비스를 포함한다. 그림에서 보는 바와 같이 보안 기능의 추가에 따라 무선신호채널의 블록킹 확률이 증가하며 셀의 부하와 신호채널의 용량에 상관없이 기본서비스 대비 보안서비스의 발생비율에 따라 거의 선형적으로 증가함을 볼 수 있다. 기본서비스 대비 보안서비스의 발생비율이 0.2인 조건에서 보안서비스의 제공에 따른 신호채널 블록킹 확률의 증가는 신호채널의 속도가 14.4kbps인 경우 1%, 신호채널의 속도가 32kbps인 경우 0.5%, 신호채널의 속도가 64kbps인 경우 0.25% 정도 증가하였다.

V. 결 론

현재의 2세대 이동통신시스템은 음성 서비스는

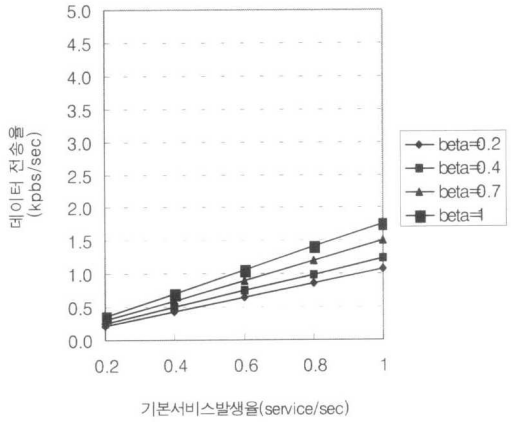

그림 2. 보안서비스를 위한 신호메세지 전송율
(평균 메시지 길이 : 256bits)

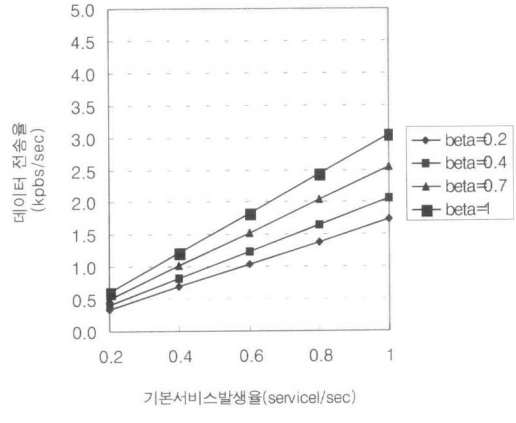

그림 3. 보안서비스를 위한 신호메세지 전송율
(평균 메시지 길이 : 512bits)

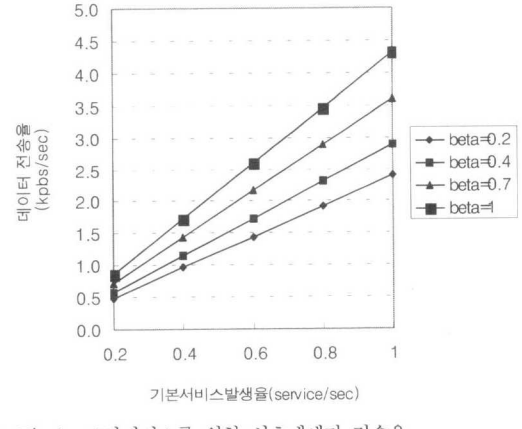

그림 4. 보안서비스를 위한 신호메세지 전송율
(평균 메시지 길이 : 768bits)

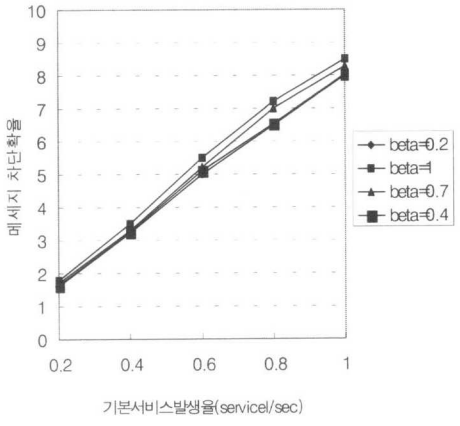

그림 5. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 14.4kbps)

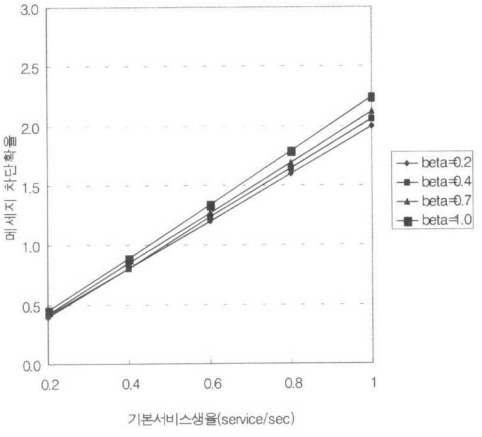

그림 6. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 32kbps)

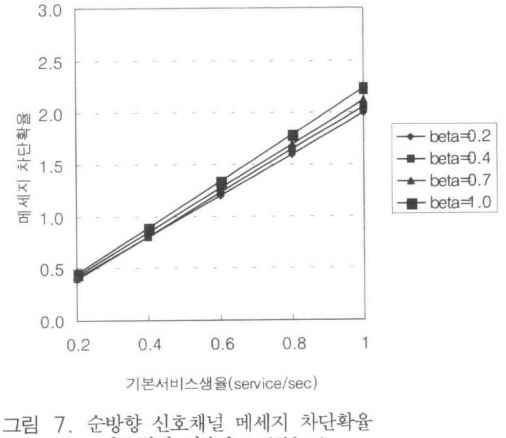

그림 7. 순방향 신호채널 메세지 차단확율
(신호채널 전송율 : 64kbps)

충분히 제공하고 있으나 점차 수요가 증대되고 있는 영상서비스, 무선인터넷 등 멀티미디어 서비스의 제공에는 한계를 가지고 있다. 이동멀티미디어 서비스를 제공하기 위해 3세대 이동통신시스템인 IMT-2000이 개발되고 있다.

대역폭의 확장에 따라 데이터 전송속도가 증가되는 차세대이동통신에서는 무선전자상거래 등 새로운 응용서비스가 급격히 증가될 것이다. 이들 서비스의 경우 데이터 무결성과 기밀성 보장, 부인방지(Non-repudiation), 가입자신원 익명성 등 엄격한 보안 특성을 요구한다. 그러나 IMT-2000과 같은 이동통신 시스템에서는 무선링크상의 제한된 대역폭을 고려한 신호메세지 전달의 최소화, 무선자원의 고비용 부담을 고려한 무선대역폭의 효율적인 사용, 이동단말기의 제한된 계산능력 등의 제한을 가지며 이에 대한 고려가 필요하다.

본 논문에서는 IMT-2000의 보안기능별 위협요소와 시스템 구성요소별 보안위협요소를 분석하고, 망 접속 보안기능을 지원하기 위해 추가적으로 요구되는 무선구간에서의 신호트래픽의 성능을 분석하였다. 망 접속 보안서비스의 지원에 필요한 무선구간의 신호트래픽은 평균메시지의 길이가 256~768bits, 기본서비스 대비 보안서비스 발생율이 0.2~1.0, 기본서비스의 발생율이 0.2~1.0서비스/호 인 조건에서 최소 0.2kbps에서 최대 4.5kbps로 분석되었다. 신호채널의 블록킹 확률은 평균메시지의 길이가 256~768bits이고 기본서비스 대비 보안서비스의 발생비율이 0.2인 조건에서 신호채널의 속도가 14.4kbps인 경우 1%, 신호채널의 속도가 32kbps인 경우 0.5%, 신호채널의 속도가 64kbps인 경우 0.25% 정도 증가됨을 확인하였다.

본 연구의 결과는 IMT-2000시스템의 무선신호채널의 전송율 결정, 효율적인 무선 프로토콜 설계와 이동국, 기지국 등 시스템 구성 요소의 설계 및 구현에 기여할 것으로 기대된다.

참 고 문 헌

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2] s3-99005: UMTS 33.23, version 0.2.0: "Security architecture".

[3] s3-99010: Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[4] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[5] 3G TS 23.003: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".

[6] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[7] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements"

[8] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[9] Chichun Loand Yu-Jen Chen, Secure communication mechanism for GSM networks, *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 4, 1999.

[10] AshaMehrotra etc, Mobility and Security Management in the GSM System and Some Proposed Future Improvements , *Proceeding of THE IEEE*, Vol. 86, No. 7, July 1998

[11] C. Boyd, A. Mathuria, Key establishment protocols for secure mobile communication: a critical survey , *Computer Communicatons* 23 (2000)

[12] Zao, J., etal., A Public-Key Based Secure Mobile IP, *MOBICOM97*, September 1997

권 수 근(Kwon-soo Kwon) 정회원

한국통신학회 논문지 제22권 제5호 참조