디지탈 셀룰라 네트워크에서의 안전성에 관한 연구

임 병렬, 김 병규, 고 정훈, 이 원호, 김 희진, 김 동규
아주대학교 전자계산학과

A Study on the Security of Digital Cellular Network

Byungryul Lim, Byunggyu Kim, Jeonghoon Koh,
Wonho Lee, Heejin Kim, Dongkyoo Kim
Dept. of C.S A-Jou University

요 약

네트워크 가입자 부분을 무선화하여 사용자에게 이동성을 제공하는 셀룰라 무선통신은 현대사회의 개인화, 이동성 및 정보화 추세에 부응해 상당한 발전을 거듭하고 있으나, 전송매체로 전파를 사용함으로 인해 생기는 정보보호의 취약성은 많은 문제점을 유발시키고 있다. 본 연구에서는 이런 문제를 해결하기 위해 셀룰라 망의 특성을 분석하고 안전성에 관해 논한다.

I. 서론

현 사회의 다양하고도 복잡함 속에 우리가 접해야 하는 정보의 양은 실로 많아 고도 정보화 사회가 도래 하였음을 느끼게 한다. 각종 업무 처리에 있어서 편리성과 생산성 향상을 위한 각종 이동 데이타, FAX, 영상 데이

타 등에 대한 통신 요구와 기존 유선망의 선로 유지 보수 및 증설, 장비 이전등의 어려운 문제점으로 인해 무선 및 이동 통신 서비스가 점차 중요시되고 있는 추세이다. 이러한 가입자 부분을 무선화한 무선통신은 현대사회의 개인화(personalization), 이동성(mobility) 및 정보화 추세에 부응해 상당히 발전하고 있으나, 각 가입자당 별개의 선로가 할당되어 있는 유선접속에 비해 여러 가입자가 한 주파수 대역의 전파를 공유해야 하는 무선접속에 있어 보안성은 매우 취약하다고 할 수 있다. 정보화 사회의 도래에 따라 정보의 보호대책은 심각한 문제로 대두되고 있으며, 특히 전송매체로서 전파를 사용하는 무선 통신에 있어 정보의 불법적인 도청, 변조, 또는 삭제가 유선통신에 비해 대단히 용이할 뿐 아니라, 불법적 자원 액세스의 사취(fraud)로 인한 과금등의 문제가 발생하게 된다. 따라서 보안성의 유지, 구체적으로 정보의 프라이버시 유지와 부당한 자원 사용의 방지를 무선통신 서비스 품질의 주요 관건으로 처리하여 사용자가 안심하고 이용할 수 있어야 한다. 서비스 측면에서의 이러한 요소는 통신 시장 개방을 앞서 대외 경쟁력과 수요 창출에 하나의 디딤돌이 될 것이다.

Ⅱ. 셀룰라 무선통신

1. 셀룰라 네트워크 구조(Architecture)

셀룰라 네트워크는 자체적 특성에 의해 허용가능한 수행도(Acceptable-performance)를 위해 내장된 프로그램 컨트롤(Stored Program Control)과 공통 채널 시그널링(Commom Channel Signalling)을 요구한다. 따라서 완전한 셀룰라 네트워크는 다양한 종류의 전송 설비로 연결된 무선 영역들 내에서 셀룰라 RF 액세스를 지원하기 위해 스위칭 디바이스들로 이루어진 전송 네트워크(Transmission network)와 메세지 라우팅 Capabilities에 의해 제공되는 데이타 링크들로 이루어진 시그널링 네트워크(Signalling network)로구성된다. 전송네트워크는 사용자의 트래픽 전송과 연결들(connections)을 위한 기본 메카니즘들을 제공한다.[6] 이것은 하나 이상의 스위칭 계층 구조를 갖는다. 시그널링 네트워크는 제어 신호들의 효율적이고 신뢰성 있는 통신을 위해 제공된다. 그림 1은 IS-41에 기초한 네트워크 참조 모델(Network Referance Model)을 보여준다. 이는 CCITT MAP 표준(Standard)과근본적으로 동일하다. 참조 모델 구조의 구성 요소들은 다음과 같다.

MS : 셀룰라 가입자(subscriber)의 MOBILE STATION. 이것은 Potable & Vehicular 장비 모두를 포함한다.

BS : 한 장소에 위치하여 MS들에게 무선 액세스를 제공하기 위해 사용되는 BASE STATION.

MSC : 무선 액세스 설비들과 공중 교환 (public switched network)들 또는 다른 MSCs와의 사이에 인터네트워킹과 회선 접속(circuit switching)을 제공하는 MOBILE SWITCHING CENTER.

HLR : 신분확인과 자격유무에 대한 파라메타, 서비스 프로파일, 현재 네트워크의 위치 등과같은 각 가입자의 현행 작동 데이타에 관한 영구적 기록을 유지하는 HOME LOCATION REGISTER.

VLR : HLR과 다른 위치에서 관련된 가입자의 작동 데이타에 관한 일시적 기록을 유지하는 VISITOR LOCATION REGISTER.

AC : 신분확인과 비밀 응용들(applications)을 위한 Key Management Capabilities를 제공하기 위해 추정된 AUTHENTICATION CENTER.

EIR : 가입자 장비 식별 기록을 유지하는 EQUIPMENT IDENTITY REGISTER.

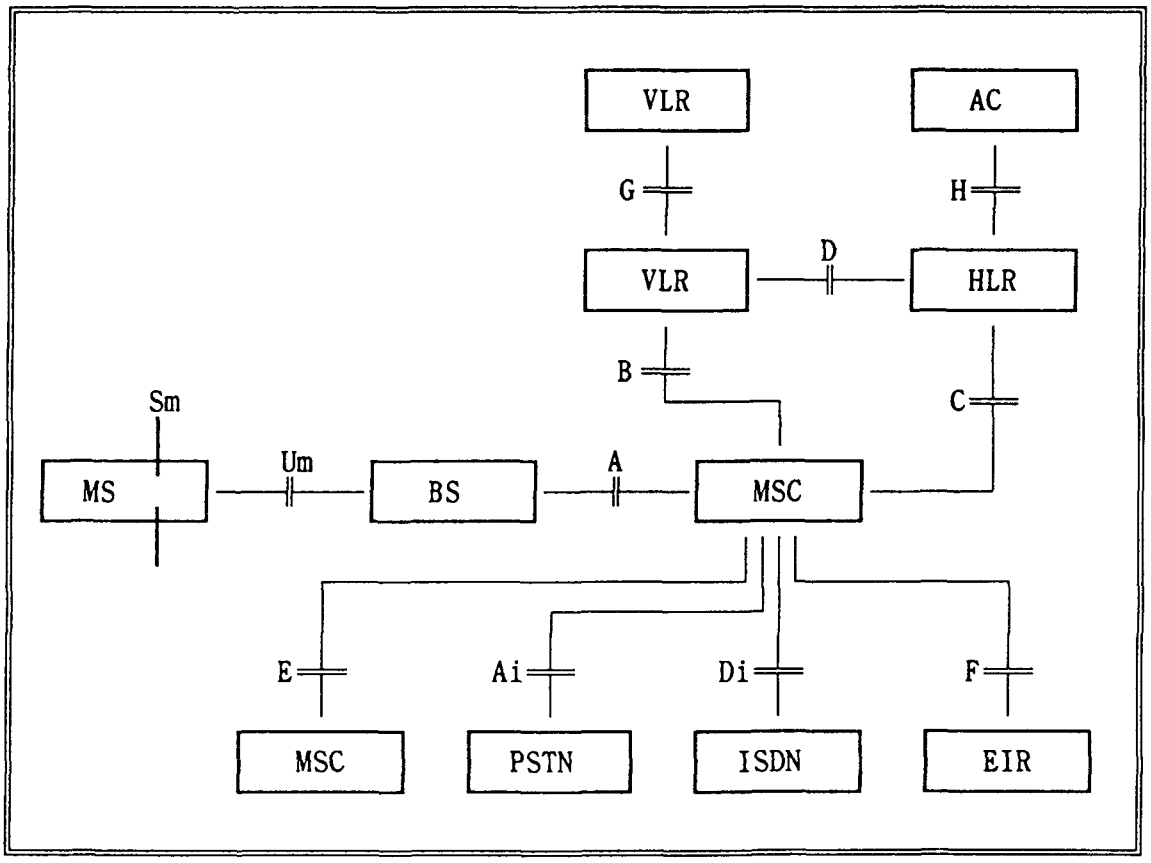

그림 1. 네트워크 참조 모델

2. 셀룰라 네트워크의 프로토콜

이동성 관리를 위해 IS-41은 특별히 정의된 트랜잭션에 사용될 시그널링 메세지들의 집합을 정의한다. 이들은 OSI 참조 모델(Open System Interconnection Reference Model)에 따라 계층화된 하나의 응용 프로토콜(Application Protocol)을 구성한다.

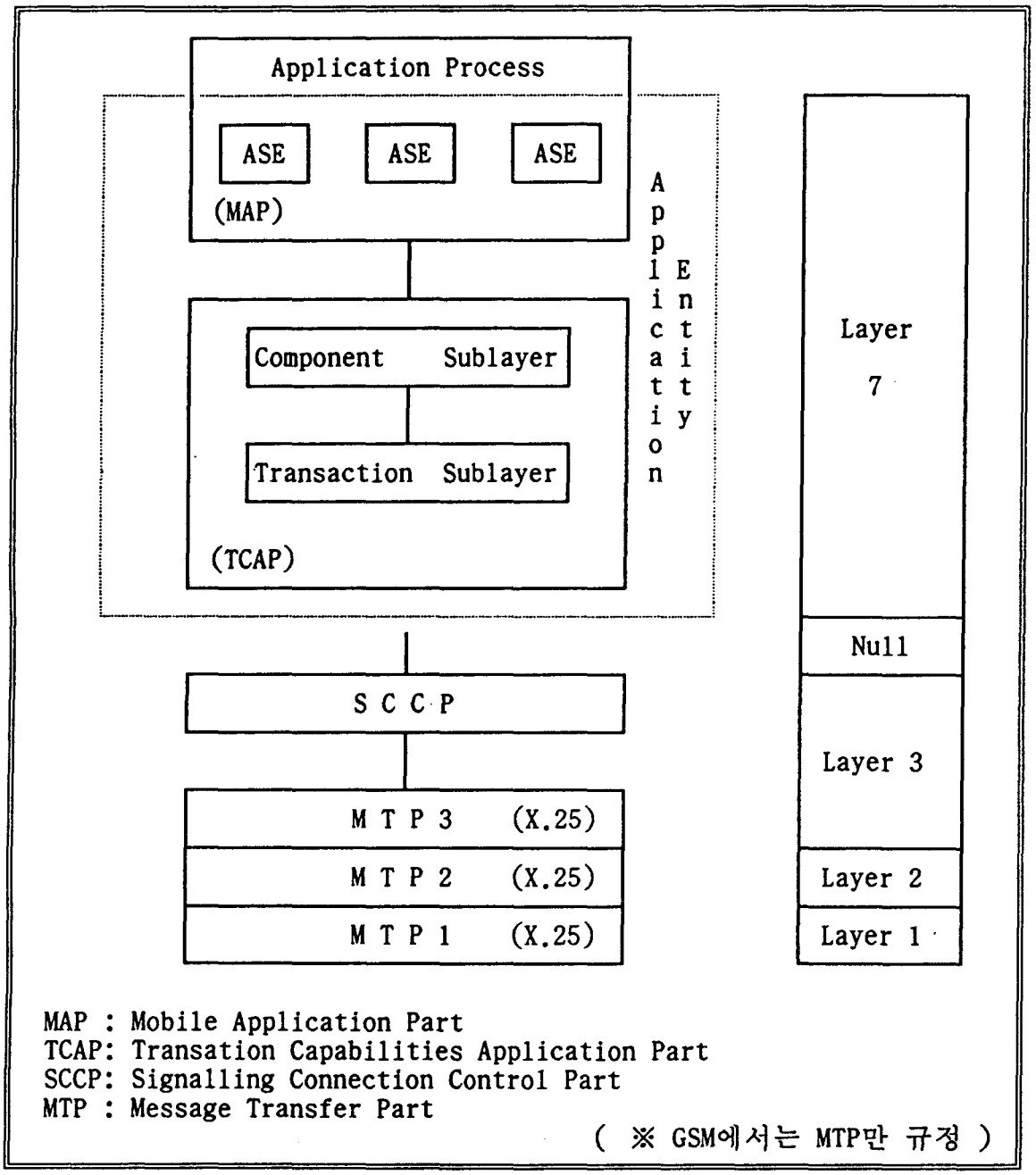

그림 2. OSI 참조 모델에 따른 MAP 프로토콜 구조

상위 프로토콜 계층들은 ANSI Standard T1.114-1988 Signalling System Number 7 - TCAP(Transaction Capabilities Application Part)에 따라 구조화 된다. 운반서비스(Carriage Service)를 형성하는 하위 계층(Lower layers)들을 위해서는, CCITT X.25 나 ANSI Signalling System 7 - SCCP(Signalling Connection Control Part)와 MTP(Message Transfer Part) - 중 어느하나가 적합하게 설정될(specified) 수 있다. TCAP은 표준형식 메세지 구조를 가지고 다른 원격 프로세스에 의한 동작(Operation)을 요청할 수 있는 하나의 응용 프로세스내의 트랜잭션 프로토콜 환경을 제공한다. MAP(Mobile Application Part) 프로토콜 구조는 그림 2와 같으며, 초기 요구(initial request)를 구성하는 메세지는 호출(INVOKE)과 같이 쓰여진다. 응답 메세지는 시도된 동작의 결과에 따라 RETURN RESULT, RETURN ERROR, 또는 REJECT를 보내게 된다.[3,6]

2-1 자동 로밍(Automatic Roaming)

자동 로밍이란 어떤 MSC의 제어하에 서비스를 제공받는 MS가 다른 영역의 MSC 제어하에서도 서비스를 제공받을 수 있도록 해주는 기능적 절차를 말한다.

2-2 핸드오프(Handoff)

핸드오프란 어떤 셀의 영역에서 통신을 하는 MS가 다른 셀의 영역으로 이동할때 통신 상태를 계속 유지하도록 하여주는 기능적 절차를 말하며, 한 MSC 제어하에서 이루어 지는 핸드오프와 MSC간 이루어 지는 핸드오프로 구분할 수 있다.

Ⅲ. 셀룰라 네트워크에서의 안전성

현재의 아날로그 음성 시스템에서도 정보 보호 서비스가 있으나, 그 방식이 제한되어 있고(scrambling 방법등), 또한 처리시간 측면이나 서비스의 질 등을 고려할 때 비교적 간단한 보호 기능 밖에 실현할 수 없으므로 정보의 안전성을 완전하게 보장하지는 못한다. 그러나 디지탈 셀룰라로의 전환기에 처해 있는 이 시점에서 앞으로의 디지탈 셀룰라 서비스가 상용화됨에 따라 정보에 대한 보호는 훨씬 유연하게 될 것이다. 디지탈 셀룰라의 도래로 음성뿐만 아니라 무선 데이타 통신 서비스도 본격적으로 시작될 것

이며, 음성/데이타 겸용 터미널이나 데이타 전용 터미널의 등장도 예상된다. 이러한 데이타 전용 터미널은 지금의 pager 시장과 mobitex와 같은 무선 패킷통신 시장의 상당한 수요를 대치하게 될 것이다. 그러나, 정보보호에 대한 취약성이 매우 높다고 할 수 있다. 이러한 보안성 유지를 위해, 사용자가 안전한 통신 확립을 할 수 있도록 신분확인(Authentication)이 수행되어야 하며, 전송데이타(음성/ 데이타)에 대한 암호화를 이용한 보호는 여러 응용의 안전성 서비스를 제공 하는데 근간이 된다.

1. 디지탈 셀룰라에서 신분확인과 대화키 분배

현재 셀 방식의 시스템이나 기타 이동 무선 시스템에서는 주로 음성 서비스가 위주이나 가까운 장래에는 데이타 서비스의 수요가 증가될 것이다. 무선이동 데이타 통신은 셀룰라 데이타 통신과 패킷 무선 서비스로 나눌 수 있으며, 회선교환방식인 셀룰라 네트워크는 이동성을 충분히 지원하고 사용시간으로 요금이 결정되므로, 전송당 데이타 밀도가 높고 전송빈도가 낮은 EDI, 데이타 베이스 액세스, FAX, Video등이 유리하다. 반면 패킷무선교환망은 짧은 bursty 데이타 통신에 효율적이고 경제적이다. 향후 무선 데이타 서비스는 하부구조가 광범위한 기존의 셀룰라 망을 통하여 회선교환방식의 데이타 서비스를 제공하다가 새로운 패킷 교환망을 구축하게 될 것이다. 이에 따라 셀룰라 이동 통신망에서의 신분확인 및 대화키 생성과 분배 과정을 전화 망에 기초해 연구하고 향후 셀룰라 망을 이용한 데이타 통신에도 적용할 수 있게 하고자 한다.

1) 디지탈 셀룰라 망에서의 신분확인 및 정보 보호

현행의 차량 전화나 휴대폰에 적용할 수 있는 정보 보호 대책으로는 무선채널 할당전에 통신자 상호간(Peer-to-Peer)이 아닌 무선접속 요청자 신분에 대한 망 제공자의 입장에서 인증(Authentication)이 수행되어야 하며, 통신자 상호간 안전한 통신을 위한 대화키(Session Key) 생성 및 분배 기능을 갖도록 하여야 할 것이다. 이것은 부당한 액세스 요청과 무선 채널에 대한 도청과 같은 위협 요소에 대응하여 부정한 MS의 호 설정, 위치등록 및 갱신으로 인해 정당한 MS에게 부당한 과금을 가하게 하거나 무선 채널의 도청으로 생기는 프라이버시 등의 문제점을 해결할 수 있게 된다. 이를위해 우선 셀룰라 망의 호 설정 절차를 그림 3과 같이 나타낼수 있다.

셀룰라 네트워크에서의 안전성을 위해 다음과 같은 점을 고려해야 한다.

1) 신분확인과 관련한 트래픽의 최소화로 시간적 오버헤드의 감소
2) 호 설정 요구시 발신 및 착신 MS에 대한 정확한 신분확인,
3) 신분확인후 무선채널 암호화 키 분배
4) 위치 등록 및 갱신시 MS에 대한 신분확인
5) 무선 채널 암호화 키는 통신시 새로이 생성
6) 암·복호화에 소요되는 시간이 적어야 함

위와같은 고려사항을 토대로하여 설계한 신분확인과 키 생성 및 분배 과정은 두 가지 형태(그림 4,그림 5)로 구분될 수 있다.

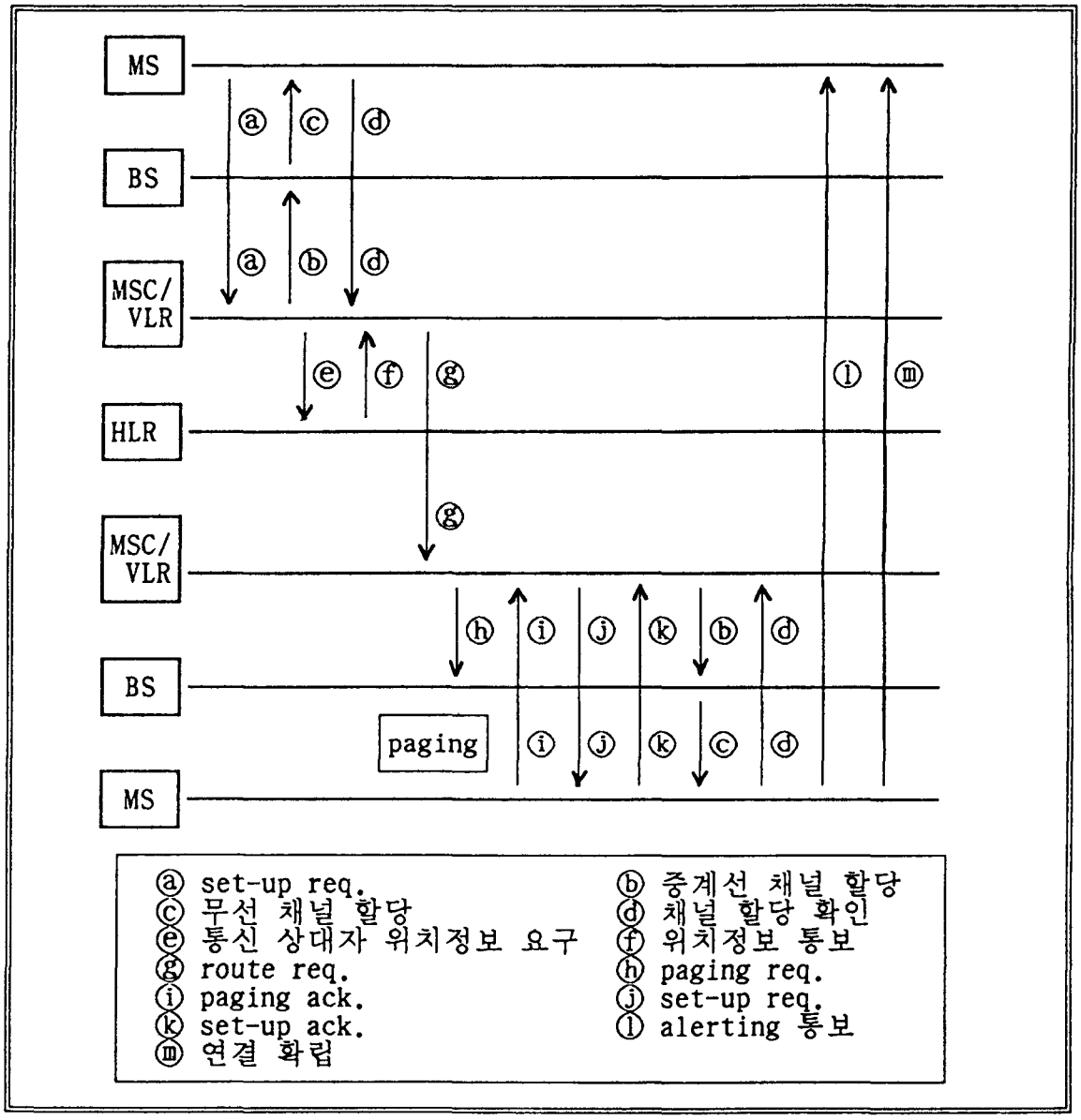

그림 3. 호 설정 절차

2) TYPE A

- 조건 및 상황

1) 신분확인 센터는 철저한 신뢰성과 보안성(Trusty Party)을 갖는다.
2) 실시간 처리를위해 단일 키 암호화 기법(예:DES나 FEAL)을 사용한다.
3) 각 MS는 초기 등록시 자신의 비밀 키를 신분확인 센터에 등록한다.
4) 신분확인 센터는 모든 MS의 비밀 키를 관리하며 호설정 요구시 무선 채널에 대한 암호화 키를 생성 분배하여 준다.
5) MS와 BS는 무선채널 암·복호화에 사용하게되는 같은 알고리즘을 갖는다
6) 각 MS는 신분확인 파라메터를 생성키위해 신분확인 센터와 같은 알고리즘을 갖는다.

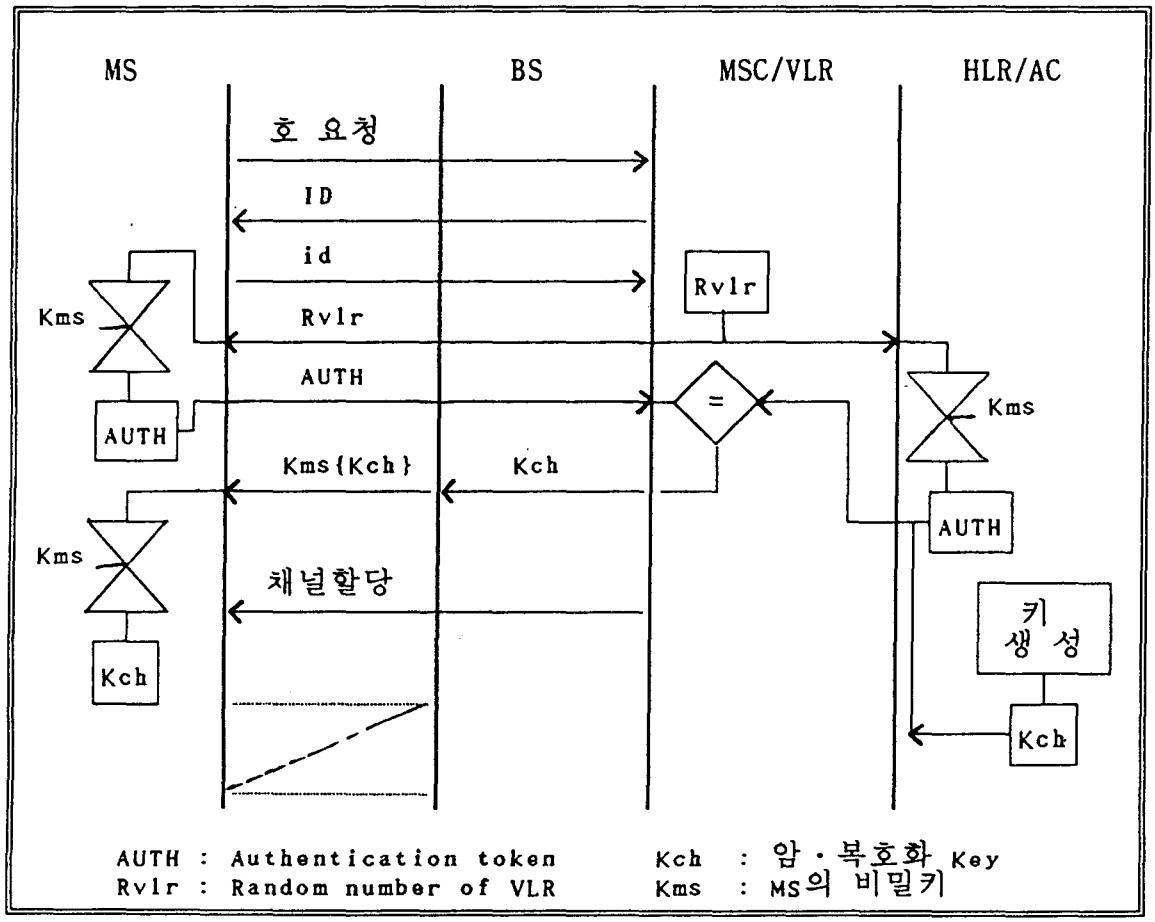

그림 4. TYPE A의 신분확인 및 암·복호화 키 분배 과정

- 과정 및 절차

1) 호 설정 요청은 MSC/VLR로 전송되어 MS의 ID를 요구한다.
2) MS는 자신의 id를 전송한다.
3) MSC/VLR은 자신의 id,MS의 id, 그리고 random number Rvlr을 생성시켜 AC에게 전송한다.
4) MSC/VLR은 또 한편으로 MS에게 Rvlr을 전송한다.
5) MS는 Rvlr을 자신의 비밀키로 AUTH를 생성후 MSC/VLR에 전송한다.
6) AC 또한 MS의 id에 근거한 비밀 키로 AUTH 생성후 MSC/VLR로 전송한다.
7) AC는 암·복호화에 쓰일 Kch를 {Kms(Kch),Kch} 형태로 전송한다.
8) MSC/VLR은 AUTH가 같으면 Kch를 BS로, Kms(Kch)를 MS로 보내고 BS에게 무선통신 채널 할당을 명한다.
9) 통신시 Kch를 이용하여 무선 채널에 대한 보안을 취한다.

착신 MS에 대해서도 Paging의 응답후 위와같은 절차를 취하며, 위치 등록 및 갱신시는 MSC/VLR에서 신분확인을 하여 인증이 되면 위치 등록 및 갱신 절차를 행한다.

3) TYPE B

- 조건 및 상황

1) 신분확인 센터는 철저한 신뢰성과 보안성(Trusty Party)을 갖는다
2) 실시간 처리를위해 단일 키 암호화 기법(예:DES나 FEAL)을 사용한다
3) 각 MS는 초기 등록시 자신의 비밀 키를 신분확인 센터에 등록한다
4) 신분확인 센터는 모든 MS의 비밀 키를 관리하며 호설정 요구시 전체 통신 채널에 대한 암호화 키를 생성 분배하여 준다
5) 통신 상호간의 MS는 무선 채널 암·복호화에 사용하게되는 같은 알고리즘을 갖는다
6) 각 MS는 신분확인 파라메터를 생성하기 위해 신분확인 센터와 같은 알고리즘을 갖는다

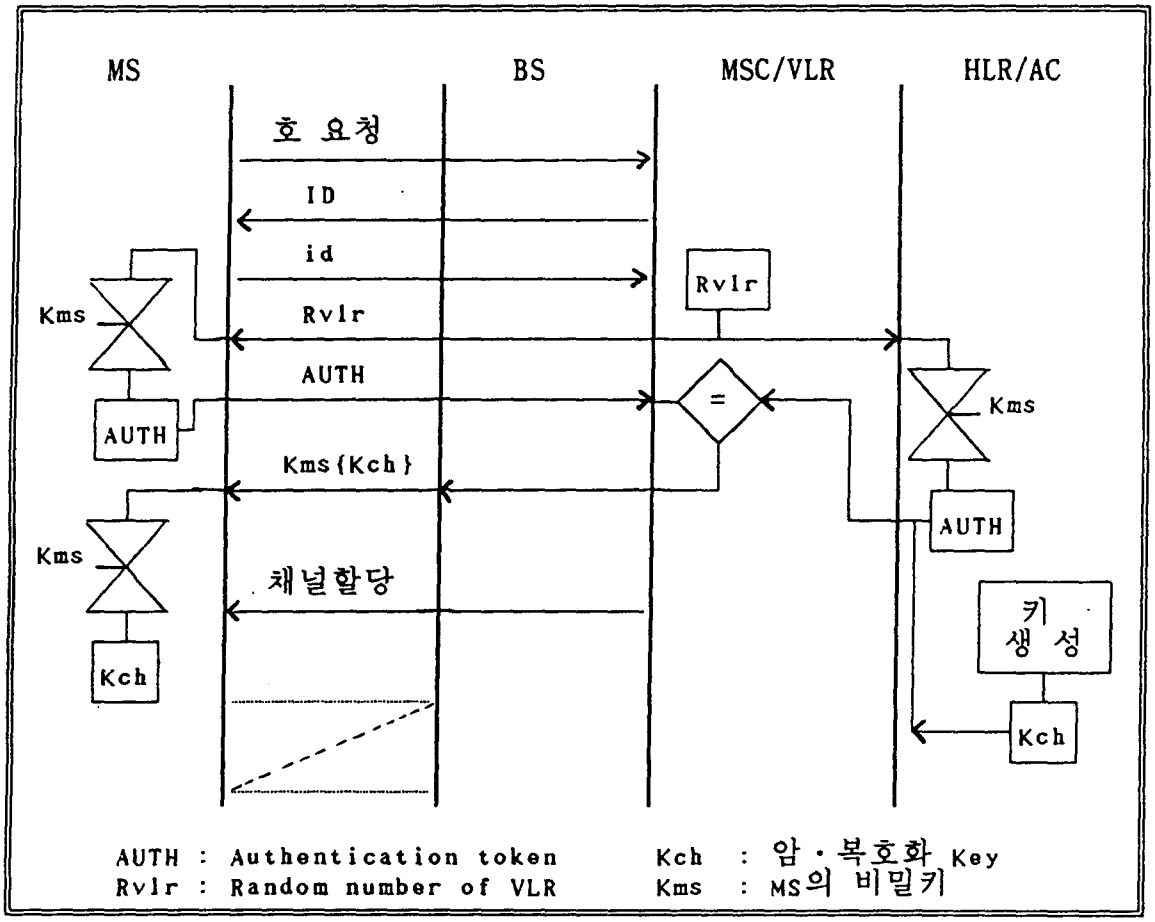

그림 5. TYPE B의 신분확인 및 암·복호화 키 분배 과정

- 과정 및 절차

1) 호 설정 요청은 MSC/VLR로 전송되어 MS의 ID를 요구한다.
2) MS는 자신의 id와 상대의 id를 전송한다.
3) MSC/VLR은 자신의 id,발,착신 MS의 id, 그리고 random number Rvlr을 생성 시켜 AC에게 전송한다.
4) MSC/VLR은 또 한편으로 MS에게 Rvlr을 전송한다.
5) MS는 Rvlr을 자신의 비밀키로 AUTH를 생성후 MSC/VLR에 전송한다.
6) AC 또한 MS의 id에 근거한 비밀 키로 AUTH 생성후 MSC/VLR로 전송한다.
7) AC는 암·복호화에 쓰일 Kch를 생성후, {Kms(Kch)} 형태로 MSC/VLR로 전송한다. 또한 AC는 Kch를 보관하여 착신 MS의 인증시 같은 절차를 취한다.

8) MSC/VLR은 AUTH가 같으면 Kms(Kch)를 MS로 보내고 BS에게 무선통신 채널 할당을 명한다.
9) 통신시 Kch를 이용하여 양단간 데이타에 대한 보안을 취한다.

위치 등록 및 갱신시는 MSC/VLR에서 신분확인을 하여 인증이 되면 위치 등록 및 갱신 절차를 행한다.

4) TYPE A 와 TYPE B의 비교

TYPE A	TYPE B
통신망 사업자가 다를때 유리	통신망 사업자가 다를때 불리
AC간 제어 프로토콜 필요없음	AC간 제어 프로토콜 필요
선택적 암호화 기능 (무선구간)	전체적 암호화 기능
암·복호화에 따른 시간 낭비	암·복호화에 따른 시간 절약
데이타 전송시 안전성 미비	모든 비밀 응용 서비스 가능

표 1. TYPE A 와 TYPE B의 비교

표 1에서 살펴본바와 같이 TYPE A는 무선구간만을 암호화 함으로써, 유선구간의 안전성이 별로 요구되지 않는 응용에 적용할 수 있고 독립적 망 운용이 가능하다. 반면 TYPE B는 셀룰라 망을 이용한 데이타의 전송을 고려할때 ISO IS 7498-2에서 제안한 다섯가지의 비밀 응용을 수용할 수 있다. 따라서 응용 서비스의 형태 특성에 맞도록 선택함이 바람직 하다 하겠다.

Ⅳ. 결론

본 연구에서는 통신에 이동성의 부여로 편리함을 제공하고 있는 셀룰라 네트워크에 관해 역기능의 요소로 부각되는 안전성 문제에 대한 연구를 진행하였다. 우선적으로 셀룰라 네트워크의 구조 및 기능을 분석 하였고 유

선 통신에 비해 그 보안성이 열등한 무선채널상의 보안 대책에 대해 디지탈 셀룰라 망에 기초하여 연구 하였다. 특히 무선채널에서의 도청 및 부당한 자원 액세스를 방지하기 위한 신분확인과 암호화 키의 생성 및 분배 과정에 대해 두가지 형태로 논했다. 앞으로 셀룰라 네트워크에서의 안전성을 보장하기 위해 신분확인 센터(AC)의 명확한 기능 설계와 구현이 이루어 져야 할 것이며, 이에따른 많은 연구가 수행 되어야 할 것이다.

참고 문헌

[1] EIA/TIA IS-54A, "*Cellular System Dual-Mode Mobile Station - Base Station Compatibility Standard*", 1991. 3

[2] EIA/TIA IS-41, "*Cellular Radiotelecommunications System Operations*", 1988

[3] EIA/TIA IS-20A, "*Digital Cellular Systems*", 1990. 12

[4] Communications & Marketing Systems, "*Wireless Access & PCN*", Vol.1-4, 1991. 1

[5] 대한 전자 공학회, "텔레콤", 제 8 권, Vol.1, 1992. 6

[6] Bijan Jabbari, "*Cellular Network Architecture & Operations*", 1991

[7] ISO IS 7498-2, "*Security Architecture*", 1989

[8] 김동규 외, "OSI 통신망 구조에서의 네트워크 안전 체제 연구 ", 과학기술처 최종 연구 보고서, 1991. 5