이동통신망에서 개선된 키분배 방식을 이용한 암호화 문제로의 접근

조장관*, 전문석

Approach to Security Problem Using Improved Key Distribution Method in Mobile Communication Network

Jang Gwan Cho, Moon Seog Jun
Dept. of Computer Science, Soongsil University

요 약

이동통신에서의 암호화 문제는 최근 많은 통신관련 범죄가 증가함에 따라 그 중요성과 필요성의 인식이 증대되고 있다. 하지만 기존의 시스템에서는 MSC(Mobile Switch Center)가 모든 정보를 관장하므로 MSC을 통한 정보유출이 발생하면 모든 이동국에 대한 정보가 가로채기를 당하거나 하는 여러가지 정보보호 위협을 당할 소지가 있으므로 이러한 문제를 해결하기 위해서 본 논문에서 중점적으로 다루는 부분은 기존의 방법에서 제공하지 못하는 두개의 이동국 사이에서만 정보를 공유하기 위한 세션키를 형성하는 방법으로 기지국에서의 정보유출을 막기위해서 이러한 방법이 연구되어 오고 있으나 실제로 세션키를 형성하는 방법이 속도면에 문제를 가지고 있어서 적용에 문제점을 가지고 있는 형편이다. 이에 본 논문에서 이러한 Diffie-Hellman의 방법을 기초한 세션키를 간단히 생성하며 적용하는 방법과 이것을 실제 시스템인 EIA/TIA/IS-95 권고안에 근거한 방법에 적용하는 것을 보이고자 한다.

1. 서 론

암호화를 통해 보안을 기하는 것이 공용화된 시스템 상에서 전송되는 정보를 보호하기 위한 가장 적합하고 효과적인 방법이다. 이러한 방법은 암호화된 메세지가 키를 파라메타로 하는 함수에 의해 만들어지고 암호문을 복호화하는데에는 오직 정당한 수신자만이 알고있는 복호화 키가 필요하게 된다. 이 복호화 키들은 통신시에는 읽을 수 없는 형태로 전달될 필요가 있으며 여기서 키분배 문제가 발생한다. 또한 인증이란 상대방과 통신을 하고 있는 당사자를 식별하기 위해 검사하는 것을 의미한다. 일반적으로 만약 송신지의 인증이 수행되지 않는다면 침입자가 실제 송신지를 가장하여 잘못된 정보를 어떤 목적지에 보내는 일이 발생할 수 있으며 또한 목적지 인증이 수행되지 않는다면 아마도 침입자가 정당한 수신자로 가장하여 권한이 부여되지 않은 정보를 받아보게 될 것이다.

이러한 문제점을 해결하기 위해 제안된 여러가지 키 분배와 인증 프로토콜이 있다. 이러한 기초적인 문제점은 세션의 인증과 세션 암호를 위한 키 분배라는 두개의 프로토콜로 불리해서 생각해 볼 수 있다. 금지되었거나 위조된 메세지를 사용할 수 있는 가능한 침입자는 인증된 자료를 교체하지 않고 전송할 것이다. 그러나 침입자는 세션키를 가로채려고 할 것이다. 그래서 인증이 나타난 이 키에 의해

금지되거나 위조된 자료를 암호화하게 된다.

2. 본 론

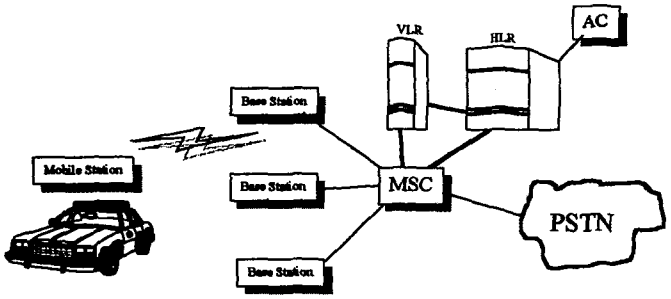
전형적인 방법에서는 모든 통화의 수락과 거절의 절차가 거의 실시간에 이루어져야 하는 통신시스템에서 인증하는데 시간적인 문제가 중요하게 인식되어져 왔다. 또한 이러한 개념에서 기존의 IS-95를 근간으로 한 CDMA방식의 무선통신망에서의 인증절차는 매우 간단하게 구성되어있으며 보다 신속하게 계산하기 위해서 여러가지 알고리즘들을 사용하여 인증에 이용하고 있다. 본 논문에서는 여기서 발생하는 여러 문제점 중에서 사용자가 기지국을 신뢰할 수 없어 통화의 절절한 두 당사자간에만 통화를 위한 보안을 요구하는 경우에 기지국은 이 통화의 내용이나 이에 관련된 자료를 가지고 있지 않고 다만 이동국만이 상호간에 세션키를 형성하여 통화하게 하여 주는 경우를 생각하여 적용한 것이다.

속도적인 문제를 감안하여 일반적인 경우에는 일반모드로 기존의 방법을 지속적으로 이용하며 특별한 요구가 있을 때에만 특수모드로 하여 제안된 프로토콜을 적용하므로써 사용자에 요구에 민감하게 적용될 수 있다. 또한 Diffie-Hellman의 방법에 기초한 방법으로 여기서 사용되는 시스템 공용으로 이용되는 p를 솟수, g를 GF(p)의 원시근이라고 하면 $y \neq 0 (\mathrm{mod}\, p)$인 임의의 y에 대해서 $y \equiv g^x (\mathrm{mod}\, p)$의 관계를 만족하는 $x \in Z_{p-1}$이 존재한다고 하면 y를 계산된 공개 기록집에 두어 계산을 하므로써 속도의 문제를 해결할 수 있겠다.

2.1 기존의 방법에 대한 분석

IS-95는 인증 파라메타는 ESN, MIN, CHARi의 기본적인 데이타와 SSD의 비밀데이타가 있다. IS-95에서는 발호이동국과 기지국, 기지국과 착호이동국간의 모든 인증을 제공하는 인증서비스와 트래픽 채널상의 시스템 데이타와 음성데이타를 보호하는 기밀성 서비스에 모두 대칭키 암호 기법을 채택하고 있다.

기존 EIA/TIA/IS-95 권고안에 근거한 방식은 등록 인증 절차와 발/착호 인증 절차 그리고 시도 응답 절차에 따른 분리하여 설명된다. 이러한 인증을 통해서 비도는 다른 일련의 방법들 보다 낮지만 속도가 빠른 이동교환국 측면에서 판장하는 중앙집중형의 형태로 이루어져 있다. 그러므로 기존의 방법은 중앙인 교환국에서는 모든 정보에 대한 신뢰성있는 보판이 필요하게 되며 그 책임이 있다고 하겠다. 하지만 이러한 경우에 교환국에 있는 정보가 누출된다면 모든 사용자에 대한 정보를 알 수 있는 문제점이 있으며 Tatebayashi가 제안한 프로토콜과 같은 문제점을 가지게 된다.



< 그림 1 > CDMA 이동통신 시스템의 개략

2.2 제안된 방법의 효용성

제안된 방법은 세션키를 생성하는 부분을 특수모드로 두고 정확한 보안이 요구되는 경우에 어느 정도의 호 설정 시간에 대해 감수할 수 있을 때 선택하도록 한다. 그렇게 하므로써 사용자에게 보다 적절한 서비스를 제공한다.

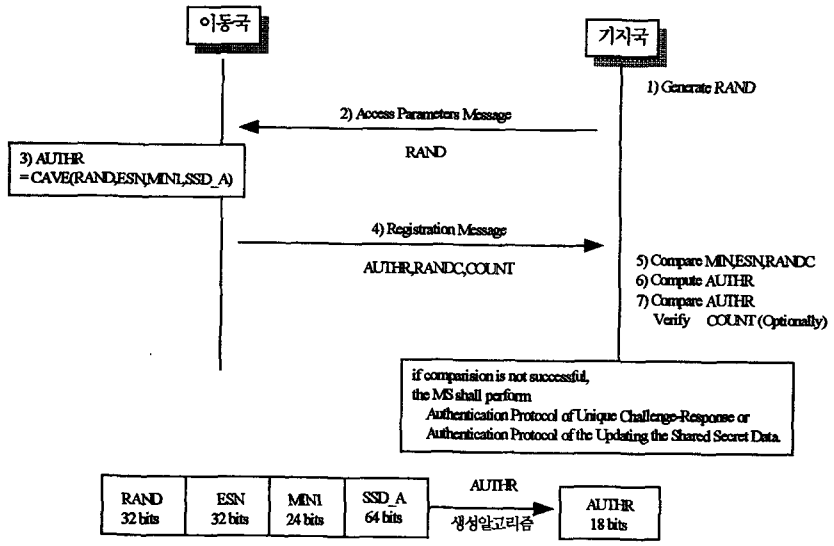
2.3 기존의 방법에 추가된 세션키 생성 방법

제안된 시스템은 세션키 생성 부분을 추가한 방법이다. 이것은 일반 모드와 특수 모드로 구분하여 일반 모드인 경우에는 사용자가 중앙교환국이 정보를 가지는 것을 허용하는 경우로 설정하지 않은 경우에도 같은 효과로 기대한다. 특수모드란 세션키를 형성하여 기지국이 통신하는 상호 이동국에 대한 정보를 가질 수 없게 하는 형태로 구성된다.

3. 이동통신 시스템에의 적용

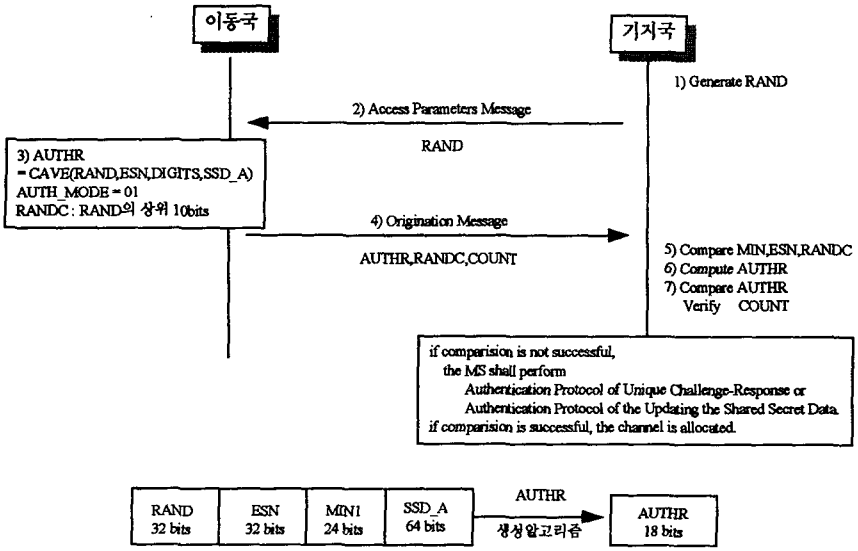
3.1 기존의 방법의 인증시스템

제안된 인증시스템은 현재 셀 안에서 이동국을 커므로 발생하는 등록인증은 동일한 형태로 사용하고 단지 전화통화를 요구하는 호인 발신/착신에 관한 경우에만 두가지의 일반/특수 모드를 두어 제안하였다. 인증 시스템의 분석을 위해서 IS-95에서 권고하는 알고리즘을 사용하였다. [3]



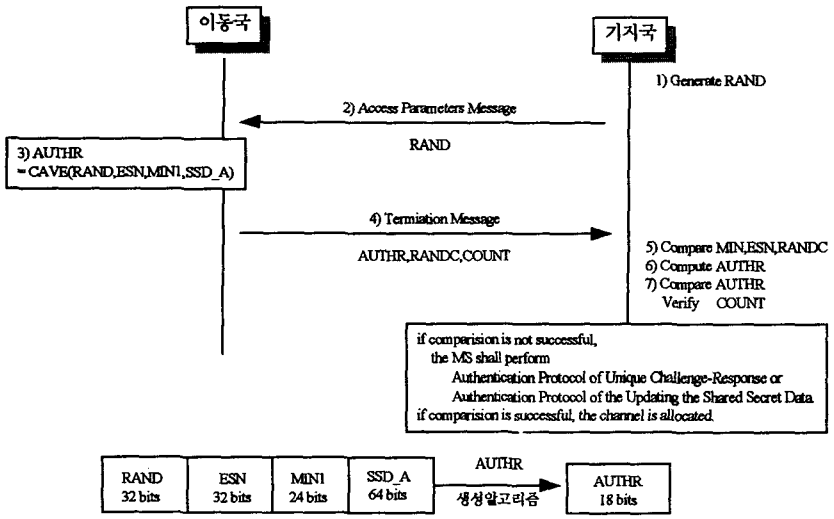
< 그림 2 > 이동국의 등록 인증

이동국의 등록 인증 절차는 기지국에서 발송한 액세스 파라메타 메시지의 AUTH가 *01*로 설정되었을 때 수행한다.



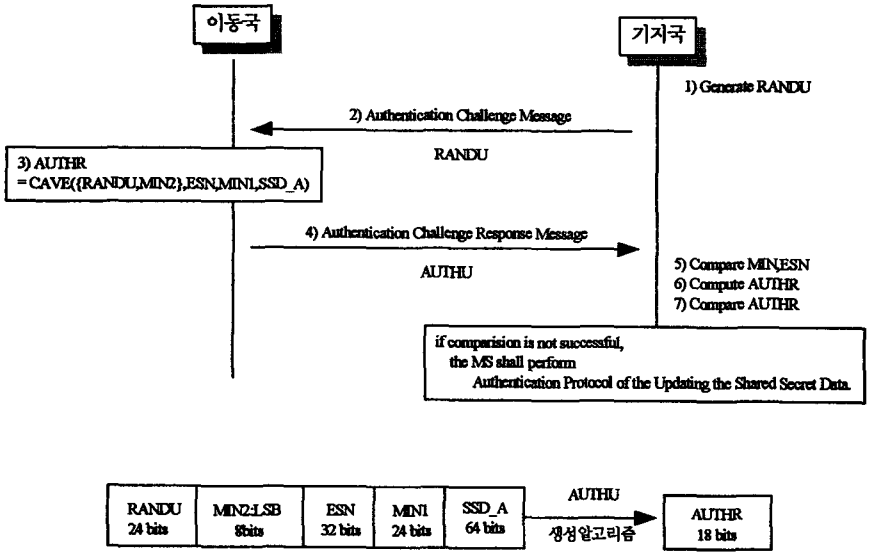
< 그림 3 > 이동국의 발호 인증

시스템 파라메타 추가 메시지의 정보요소인 AUTH가 1로 설정되어 있고 이동국이 호를 액세스 할 경우, 발호 인증 절차가 수행된다.



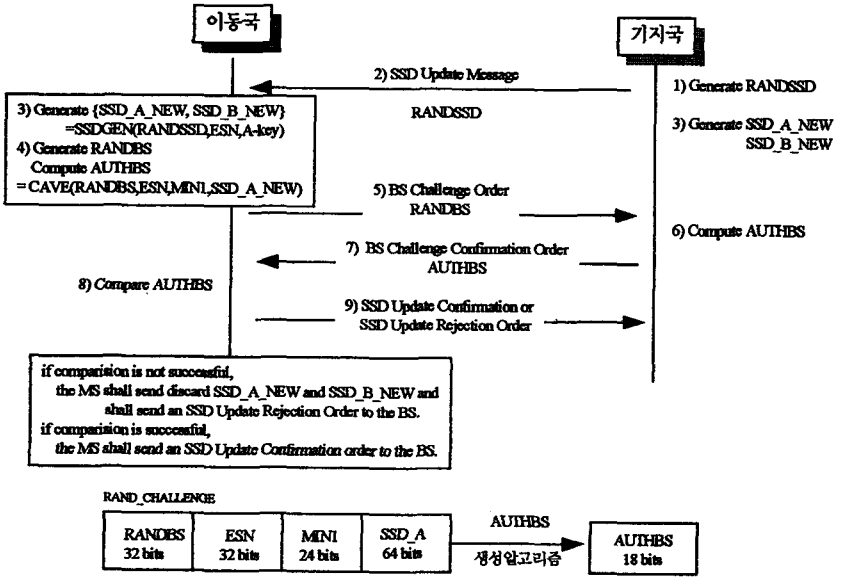
< 그림 4 > 이동국의 착호 인증

이동국의 착호 인증 절차는 기지국에서 호출채널로 전송한 액세스 파라메타 메시지의 AUTH가 *01*로 설정되어 있다면 이동국이 기지국으로 부터 호출에 호출 응답 메시지로 응답한다면 수행된다.



< 그림 5 > 시도 응답의 인증

시도 응답 절차는 기지국에서 시작되는 순방향 통화채널(FVC) 또는 역방향 통화채널(RVC)과 관련하여 페이징과 액세스 채널 중에서 수행할 수 있다.

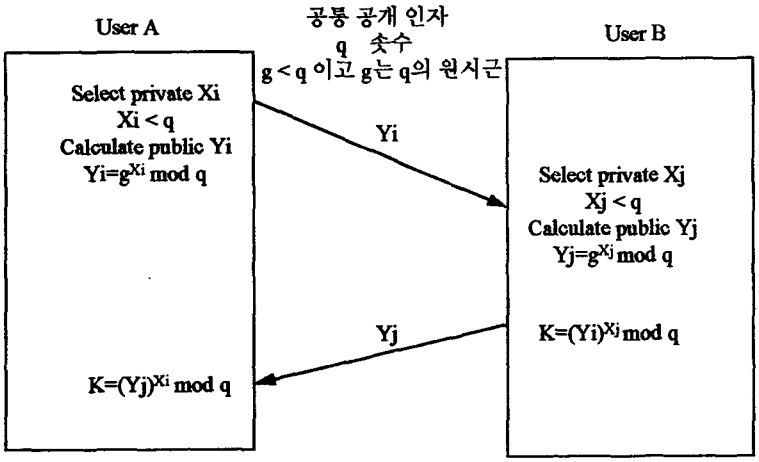


< 그림 6 > 공유 비밀 데이타 갱신

SSD의 갱신은 이동국 특유의 정보와 랜덤 데이터 그리고 이동국의 A-Key를 초기화 시키는 SSD생성 절차로 구성된다. A-Key는 64비트 길이로 이동국에 의해 규정되고 이동국 장치 내부의 영구적인 보안(Security) 및 식별(Identification) 기억장소에 기록된다. 이와 관련된 위치 레지스터/승인센터(HLR/AC)에만 알려진다. 따라서 SSD의 갱신은 단지 이동국과 이와 관련된 HLR/AC에 의해 수행된다.

3.2 Diffie-Hellman의 키분배 방식

Diffie-Hellman의 키분배 방식은 아래의 < 그림 7 >과 같이 설명될 수 있다.



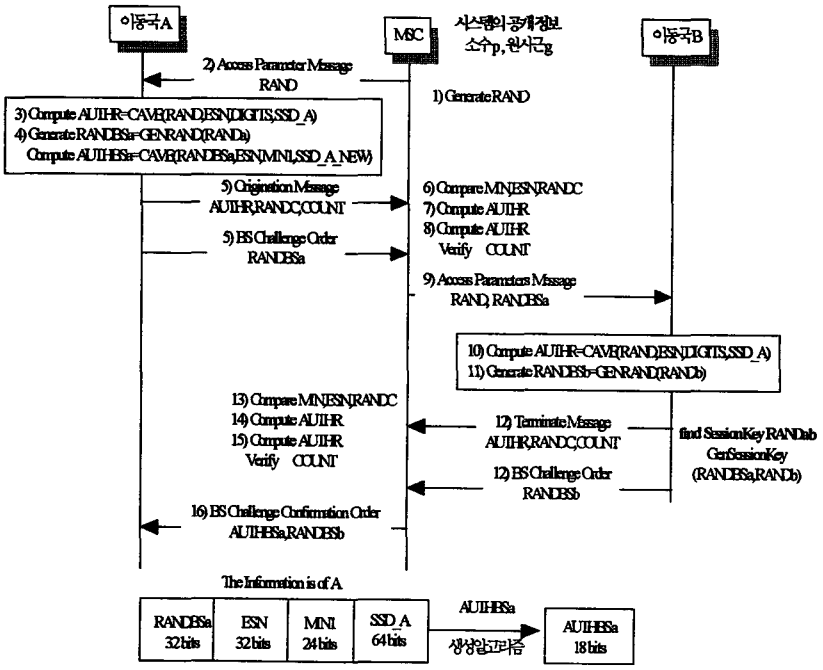
< 그림 7 > Diffie-Hellman의 키분배 방식

3.3 제안된 방법의 인증시스템

제안된 방법은 이동국의 발호 및 착호 인증에 있어서는 기존의 방법과 같은 방법을 사용한다. [6]

이동국은 기지국이 보낸 RAND에 의해서 AUTHR을 생성한 후에 기지국 측으로 보낸다. 제안된 방법에서는 여기에 RANDBS을 생성하여 AUTHBS를 생성한 후에 같이 보내게 된다. 기지국 측에서 발호 메시지(Origination Message)를 수신하면 수신된 RANDC, ESN, MIN값을 기지국 내부 저장값과 비교한다. 그리고 선택적으로 COUNT를 비교할 수도 있다. 기지국내에 저장되어 있는 SSD_A를 이용하여 이동국과 같은 방법으로 AUTHR값을 계산하고, 수신된 AUTHR값과 비교한다. 기지국에서 비교사항들이 기본적인 조건에 만족하면 적절한 채널 할당 절차가 개시된다. 제안된 방법에서는 기지국이 통화하고자 하는 발신 이동국에게서 수신하게 되는 RANDBS를 RAND와 함께 착신 이동국에게 보내게 된다. 착신 이동국은 수신된 RAND로 AUTHR값을 생성하며 AUTHR, RANDC 그리고 COUNT를 보내며 또한 RANDBS를 생성하여 세션키를 만들고 RANDBS를 착신 메세지를 기지국에게 보내게 된다. 기지국은 기지국내에 저장되어 있는 SSD_A를 이용하여 이동국과 같은 방법으로 AUTHR값을 계산하고, 수신된 AUTHR값과 비교한다. 기지국에서 비교사항들이 기본적인 조건에 만족하면 적절한 채널을 할당하게 된다. 마지막으로 기지국은 발신 이동국에 AUTHBS와 착신 이동국으로 부터 수신된 RANDBS를 발신

이동국에 보내게 되며 발신 이동국은 세션키를 생성하게 된다.



< 그림 8 > 제안된 세션키를 이용한 인증방법

3.3 비교분석한 결과

시뮬레이션에 사용된 기종은 SUN 기종을 사용하였으며 프로세스는 SPARC processor(32bits)를 이용하였고 clock speed는 25 MHz이며 사용된 OS는 UNIX를 이용하였으며 데이타 수형의 범위는 integer은 2 Bytes, long integer는 4 Bytes, float형은 8 Bytes 그리고 double형은 8 Bytes를 사용되며 사용된 언어는 C++로 구현되었다.

기존의 인증시스템과 제안된 인증시스템[1]을 비교한다.

호착신 프로토콜 : Torgi / 호발신 프로토콜 : Tterm
1) Tm(CAVE) : 이동국 측에서의 CAVE의 계산시간
2) Tb(CAVE) : 기지국 측에서의 CAVE의 계산시간
3) Tma(GENRAND) : 이동국 A측에서의 GENRAND의 계산시간
4) Tmb(GENRAND) : 이도국 B측에서의 GENRAND의 계산시간
5) T(m-b) : 이동국에서 기지국 측으로 신호 전송시간
6) T(b-m) : 기지국에서 이동국 측으로 신호 전송시간

단일하게 호의 발신과 착신에 의해 이루어는 간단한 경우에 대해서만 비교하여 보면 기존의 경우으로 기술할 수 있으며

Torgi = Tterm = {T(b-m)+Tm(CAVE)} + {T(m-b)+Tb(CAVE)}

호의 발신과 착신에서 걸리는 시간은 전체적으로
Ttota = Torgi + Tterm
라고 쓸 수 있다.

제안된 방법은 아래와 같이 기술할 수 있다.
Torgi = Tterm = {T(b-m)+Tm(CAVE)} + {T(m-b)+Tb(CAVE)}
호의 발신과 착신에서 걸리는 시간은 아래와 같이 전체적으로 설명될 수 있다.
Ttota = {Torgi + Tterm} + {Tma(GENRAND)+Tmb(GENRAND)} +T(b-a)
기존의 방법보다 제안된 특수모드의 상태에서 {Tma(GENRAND)+Tmb(GENRAND)}+T(b-a) 만큼의 시간이 더 소요된 것으로 나타난다.

4. 결 론

기존의 시스템이 MSC에 의해 모든 정보가 관장되므로 발생하므로 MSC에서 정보가 유출된 경우에 심각한 문제를 유발할 수 있다. 여기서 통화당사자들의 의견에 따라 보다 신뢰성있는 통신이 보장되어야만 한다. 이러한 기존의 시스템이 가지고 있는 문제점을 보완하기 위해서 Diffie-Hellman의 키분배 방식을 이용한 간단한 프로토콜을 제안한다. 본 논문에서는 기존의 EIA/TIA/IS-95 권고안을 기초로 하여 보다 강력한 인증을 하기 위해서 세션키를 형성하여 인증하는 방법을 제안하였으며 이것은 부분적으로 속도적인 문제를 감안하여 일반/특수 모드로 사용을 제안하였다. 또한 이 방법은 사용자에게 보다 신뢰할 수 있는 시스템을 제공하기 위해서 EIA/TIA/IS-95에 적용하여 실제적인 부분을 고려하여 보았다.

참 고 문 헌

1) 홍기용, 김동규
IS-95에 기반한 CDMA 이동통신망을 위한 인증 프로토콜의 정확성에 관한 연구,
통신정보보호학회논문지, 제5권 2호, 1995.6

2) 암호학 입문, 한국전자통신연구소, 1987.10.

3) *Tatebayashi, M., Matsuzaki, N. and Newman, Jr., D.B.,*
Key Distribution Protocol for Digital Mobile Communication Systems, Advances in Cryptology, Proceedings of Crypto*89, pp. 324-334, 1989.

4) Diffie. W., and Hellman, M. E., New Direction in Cryptography, IEEE Trans. on Information Theory, Vol 22, No.6, Nov. 1976, pp.644-654.

5) Dorothy E. Denning, Cryptography and Data Security, Addison-Wesley, 1983.

6) Qualcomm Inc., "TIA/EIA Interm Standard(IS-95): Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Celluar System", Feb, 1993

7) Proposed TR45 Standard, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Celluar System", Feb. 1993.