通信情報保護學會誌
第5卷 第4號, 1995. 12

디지탈 이동통신 시스템에 적합한 세션 키 분배 및 가입자 인증 프로토콜+

A Session Key Distribution and Subscriber Authentication Protocol for the Digital Mobile Communication Systems+

박 창 섭*

요 약

본 논문에서는 디지탈 이동통신 시스템을 위해 제시된 기존의 세션 키 분배 및 가입자 인증 프로토콜을 소개하고, 선형대수에 기반을 둔 새로운 프로토콜의 제안 및 이의 안전성을 분석한다. 기존의 제안된 프로토콜들이 단말기의 하드웨어적 제약성을 고려하여 작은 지수를 이용하는 RSA 시스템이나 Modular Square Root 기법을 이용한 공개키 암호 체계에 기반을 둔 반면에 새로이 제시되는 세션 키 분배 프로토콜은 세션 키 분배상의 계산 복잡도가 단지 유한 체 상의 행렬과 벡터의 곱 계산이라는 측면에서 디지탈 이동통신 시스템에 적합한 방식이다.

1. 서 론

고도의 정보화 사회로의 발전에 일익을 담당하고 있는 무선 이동통신 시스템은 언제, 어디서나, 또한 누구와도 통화가 가능토록 하기 위한 필수적인 시스템으로, 그 궁극적인 목표는 그 사용자에게 장소와 이동성에 무관하게 어느 순간에도 가입자가 전체 통신망의 기능을 사용할 수 있도록 하는데 있다. 무선 기술은 매체를 유선통신과는 달리 전파를 이용하여 신호를 전달하고, 수신하므로 그 자원이 유한하다. 현재 우리나라에서 사용되고 있는 '제 1 세대' 아날로그 이동통신 시스템은 셀룰러(cellular) 통신 시스템 기술의 개발로 주파수 재사용에 의한 전파 자원의 이용 효율을 높이고, 동적 채널 할당기술 등 운영 기술의 확보에도 불구하고 폭발적인 가입자의 증가에 따른 한정된 주파수 자원의 고갈에 따라 서비스 용량의 한계에 이르게 되었다. 이에 따라 각 기지국 당, 주파수 대역 당 더 많은 가입자를 수용할 수 있으며, 따라서 고밀집의 지역에서도 더 경제적으로 서비스를 제공할 수 있는 '제 2 세대' 디지탈 이동통신 시스템의 출현을 가져왔다. 디지탈 이동통신 시스템의 장점으로는, 먼저 저속 음성 부호화기의 사용으로 인한 추가용량 증대, 디지탈화된 유선 망

* 단국대학교 전자계산학과 부교수
+ 이 논문은 1995년도 정보통신부, 한국통신의 후원으로 연구되었음.

(ISDN 망)과의 접속 용이, 음성 및 데이타의 혼합 통신 가능, RF(radio frequency)송신 전력의 감소로 인한 단말기의 배터리 수명 연장, 통화 도청 방지를 위한 암호화 기법의 사용 가능 등을 들 수 있다[9]. 제 2 세대 디지탈 이동통신 시스템은 주요 국가마다 이미 개발이 완료되어 일부는 상용 서비스 중에 있다. 유럽에서 개발되어 서비스 중에 있는 GSM(Global System for Mobile Communications)디지탈 셀룰라 시스템은 1994년도 기준으로 유럽 전역에 200만 가입자를 수용하고 있다[8].

디지탈 이동통신 시스템에 있어서 가입자의 이동성(mobility of subscriber)과 통신망에의 무선 접속(wireless access)이라는 특성은 보안적인 측면에서 여러가지 문제점들을 내포하고 있다. 첫째는 무선 채널을 통한 사용자 데이타의 전달은 유선 채널의 경우보다 제 3 자에 의한 도청에 쉽게 노출되어 진다. 둘째, 유선 통신 망과는 달리, 다른 가입자의 ID(identiy)를 도용하여 요금을 물지 않고 서비스를 받을 수 있는 가능성이 매우 높다. 마지막으로, 가입자 위치는 항상 이동하고 있기 때문에 가입자의 현재 위치는 경우에 따라 보안적인 측면에서 보호할 가치가 있는 정보라 할 수 있다. 그러므로, 디지탈 이동통신 시스템에서 제공되어야 할 보안 서비스는 먼저, 사용자 데이타의 비밀성을 보장하기 위한 암호화 기능, 서비스 가입자 신분 확인을 위한 가입자 인증, 그리고 가입자의 현재 위치 정보를 보호하기 위한 임시 ID할당 등이 있다.

암호화 기법을 사용하기 위해서는 먼저 당사자간에 공통된 세션 키(session key)의 공유가 우선되어야 한다. 비록, 기존의 여러 유형의 세션 키 분배 프로토콜이 제시되어 지고 있지만 디지탈 이동통신 시스템 하에서는 단말기의 하드웨어적인 제약성이 고려되어야 한다. 그러므로 상당히 큰 finite field 상에서의 계산이 요구되는 Diffie-Hellman 유형의 지수형 키 교환(expronential key exchange)프로토콜은 적당하지가 않다. 특히, 키 분배 및 사용자 인증에 있어서 고려되야 할 사항은 모든 통신이 네트워크 센타를 통해 이루어 진다는 사실이다. 이 부분은 보안 관련 서비스를 설계하는데 있어서 매우 유리한 환경이라고 할 수 있다.

본 논문에서는 디지탈 이동통신 시스템을 위해 제안된 기존의 세션 키 분배 및 가입자 인증 프로토콜을 분석하고 선형대수에 기반을 둔 새로운 프로토콜을 제안하고자 한다. 먼저 2절에서는 유럽의 GSM 시스템에 적용되어 사용되고 있는 보안 관련 서비스들을 소개한다. 기반을 이루는 구체적인 암호화 알고리즘은 공개적으로 발표가 되어 있지 않기 때문에 개략적인 세션 키 및 가입자 인증 프로토콜의 운영방식만을 논의의 대상으로 한다. 제 3 절에서는 Tatebayashi[3]등에 의해 제시된 RSA 공개 키 암호체계에 기반을 둔 프로토콜과 Beller[4]등에 의해 제시된 Modular Square Root기법을 이용한 프로토콜을 분석한다. 선형대수에 기반을 둔 세션키 및 가입자 인증 프로토콜을 제 4절에서 새로이 제시하고 그 안전성을 분석한다. 여기서 제시되는 세션 키의 분배는 단말기와 네트워크 센타간의 통신 보안만을 고려한 키의 분배가 아니라 네트워크 센타의 중계를 통한 호(call)요구 단말기와 호출 단말기간의 직접적인 세션 키의 공유를 의미한다.

2. GSM시스템의 보안 서비스

유럽의 디지탈 셀룰라 이동통신 시스템인 GSM(Global System for Mmobile Communication)은 무선을 통해 전달되는 음성 및 데이타의 비밀성을 보장함과 동시에, 정당한 단말기 사용자의 시스템에의 안전한 접속을 가능하게 하는 여러 가지 보안 관련 서비스를 제공하고 있다[5]. GSM시스템의 서비스를 제공받

는 각각의 가입자들은 가입자 정보와 보안 관련 파라메타들이 내장된 SIM(subscriber identity module)이라는 가입자 카드를 발급 받는다. 가입자는 먼 지역으로 이동 시에 자기의 단말기(MS : mobile station)를 가지고 이동 할 필요가 없이 단지 그의 SIM을 사용 가능한 ME(mobile equipment)에 삽입한 후 사용함으로써 이동통신 서비스를 받게 된다. 그러므로, ME는 SIM이 없는 단말기(MS)를 의미한다.

SIM에는 가입자의 ID인 IMSI(international mobile subscriber identiy)와 128 비트의 가입자 비밀키 K_i, 그리고 세션 키 생성 알고리즘인 'A8'과 가입자 인증 알고리즘 'A3'가 내재되어 있다.

GSM시스템에서는 MS와 기지국간의 무선 채널을 비화하기 위한 'A5'라는 암호화 알고리즘이 ME와 기지국에 실리콘 칩의 형태로 내재되어 있고, 이 알고리즘은 약 3,000개의 트랜지스터를 이용해 실행되어 질 수 있다. 그림 1에서와 같이 GSM 시스템에서 사용되는 암호체계는 스트림 암호로서 결국 'A5'는 키 스트림을 생성시키는 알고리즘이다.

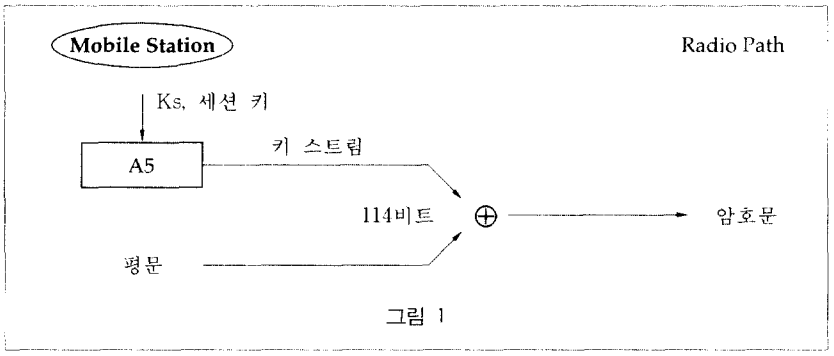

그림 1

평문은 114 비트의 블럭들로 구성되어 키 스트림과 XOR(⊕) 되어진다. 114 비트의 블럭으로 구성되는 이유는 GSM시스템의 무선 접속 방식은 시분할 다중 접속(TDMA : time division mulitple access)으로 한 개의 time slot에 114 비트가 전송되기 때문이다. 가입자에 대한 네트워크 센타의 인증 절차는 MS와 네트워크 센타가 공유하고 있는 'A3' 알고리즘과

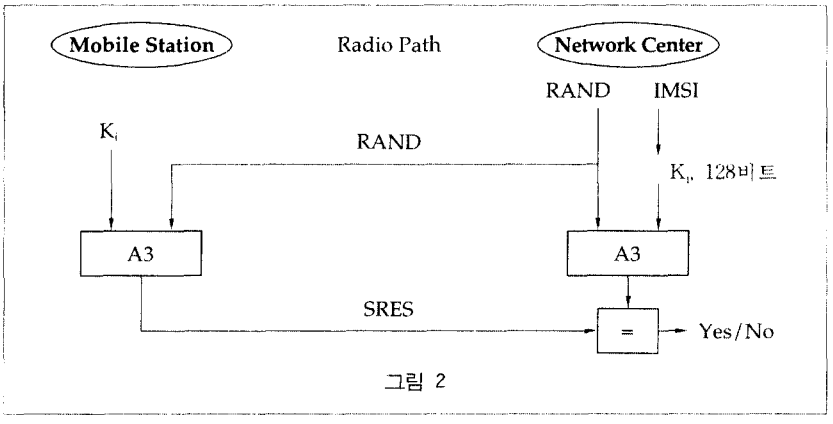

그림 2

가입자의 비밀 키 K_i를 이용해 challenge - response형태로 이루어진다. 그림 2 에서와 같이 네트워크 센타에서 보내 온 non-predictable number RAND에 자신의 비밀 키 K_i를 'A3' 알고리즘에 적용한 결과인 SRES를 네트워크 센타에 재전송하여 인증 절차를 마친다.

그림 2에서와 같이 네트워크 센타에서의 가입자의 비밀 키 도출은 가입자의 IMSI로 부터 도출하는 알고리즘을 채택하기 때문에 네트워크 센타는 각 가입자의 비밀 키를 저장하는 추가의 데이타 베이스를 구축할 필요는 없다. 그 도출 알고리즘으로 사용할 수 있는 것으로 DEA(Data Encryption Algorithm)를 들 수 있다. 각 가입자의 IMSI는 4비트씩 부호화된 15자리 수로 구성되는데 이를 16자리 수로 확장한 UD를 DEA의 입력 자료로 사용하고, 센타의 128비트 Master키 MK를이용하여 다음과 같이 128 비트의 K_i를 도출한다. '‖'는 2개의 64비트를 연결하는 작업을 의미한다.

$$K_i = DEA_{MK_{left}}(UD) \parallel DEA_{MK_{right}}(UD)$$

MS와 네트워크 센타간의 세션 키의 공유는 그림 3에서와 같이 'A8' 알고리즘을 통해 이루어 진다. 결국 가입자 인증과 세션 키의 분배는 동일한 challenge 값인 RAND를 이용해 이루어 질 수 있다.

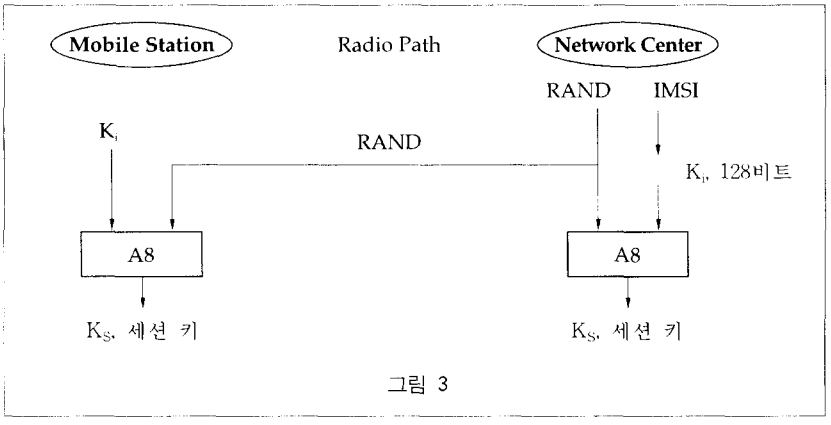

그림 3

3. 공개키 암호체계에 기반을 둔 프로토콜

여기서는 공개키 암호체계에 기반을 두고 디지탈 이동통신 시스템을 위해 제안된 기존의 두 가지 세션 키 분배 및 가입자 인증 프로토콜을 소개한다. Tatebayashi[3]등에 의해 제시된 방식은 RSA 시스템에 그 기반을 두고 있고, 반면 Beller[1]등에 의해 제안된 방식은 Rabin[1]에 의해 제시되고 Williams[2]에 의해 개선된 modular square square root 기법을 이용하고 있다. 두 개의 프로토콜 모두 단말기의 계산 능력이 제한적이라는 사실을 고려하여 단말기에서의 encryption에 이용되는 공개키 exponent를 각각 3과 2로 제한하고 있다. Tatebayashi 등에 의한 세션 키 분배 프로토콜은 네트워크 센타의 중계에 의한 단말기 사용자들간의 직적적인 세션 키의 분배인 반면, Beller등이 제안한 세션 키 분배 프로토콜은 단말기와 네트워크 센타간의 세션 키 분배를 다룬다.

3.1 RSA시스템에 기반을 둔 프로토콜

Tatebayashi등은 Crypto'89에서 RSA공개키

암호체계를 이용한 세션 키 분배 및 가입자 인증 프로토콜을 제시하였다. 그들의 제안은 기본적으로 단말기의 하드웨어 특성을 고려하고 또한 네트워크 센타의 키 관리 문제를 해결하는데 초점을 맞추고 있다. 먼저 네트워크 센타는 공개키로 사용되는 exponent가 e = 3이고 modulus가 n = p·q인 RSA시스템 $E(M) = M^e \bmod n$과 pseudorandom 함수인 f()를 생성한다. 이때, 공개키 e에 대한 개인키 d와 두개의 prime number인 p와 q, 그리고 f()는 센타의 비밀정보가 된다. 가입자 A와 B는 네트워크 서비스 가입 시에 네트워크 센타로 부터 그들의 ID에 기반을 둔 비밀 키 $S_a = f(ID_a)$와 $S_b = f(ID_b)$를 각각 부여 받는다. 그림 4는 가입자 A(MS_a : mobile station A)와 B(MS_b : mobile station B) 간의 세션 키 분배 및 각 가입자에 대한 네트워크 센타에 의한 인증 프로토콜을 보여 주고 있다.

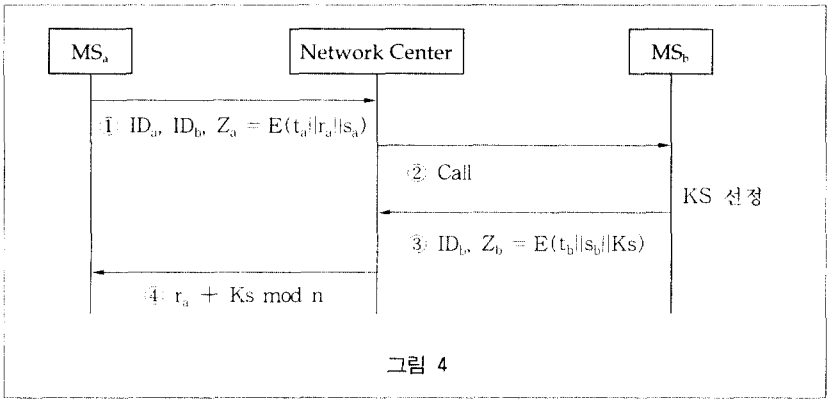

그림 4

'||'는 concatenation, t_a와 t_b는 timestamp, r_a는 가입자 A가 임의로 생성한 random number를 의미한다. 위의 세션 키 분배 방식은 결국 호출된 가입자가 세션 키 Ks를 선정하여 네트워크 센타의 중계에 의해 이루어진다. 가입자 A와 B에 대한 네트워크 센타에 의한 인증은 네트워크 센타의 개인키 d를 이용한 복호화 과정을 통해 얻은 S_a, S_b를 $f(ID_a)$, $f(ID_b)$과 각각 비교함으로써 ① 단계와 ③ 단계에서 각각 행해진다. t_a와 t_b를 포함하는 이유는 제 3자에 의한 replay 공격을 방지하기 위해서 이다. ([3] 참조). 하지만 최근 park[7]등에 의해 Tatebayashi 방식의 취약점이 지적되었다.

3.2 Modular Square Root에 기반을 둔 프로토콜

공개키 암호체계의 기본 구조로서 MSR (modular square root)의 사용은 Rabin[11]과 williams[12]에 의해서 제시되었다. MSR을 이용한 공개키 암호체계에서의 공개키는 modulus n = p·q이고 개인키는 두 개의 prime number인 p와 q이다. 송신자가 메시지 M을 수신자에게 보내기 위해 수신자의 공개키 n을 이용하여 $C = M^2 \bmod n$ 을 보낸다. p와 q를 알고 있는 수신자는 복호화 과정을 통해, 즉 C의 modular square root를 취함으로써 M을 얻을 수 있다. MSR을 이용한 공개키 암호체계의 안전성은 소인수 분해의 어려움에 그 기반을 두고 있다. 그림 5는 단말기와 네트워크 센터 간의 키 분배 방식을 보여 주고 있다. 단말기는 네트워크 센타 측에서 방송되는 시스템 정보에 포함된 공개키 n = p·q을 이용해 임으로

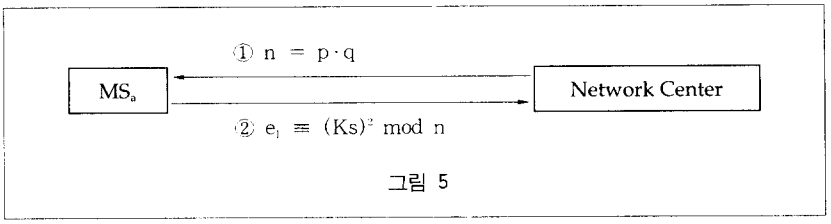

그림 5

선정한 Ks를 암호화한 e_1을 보낸다. p와 q를 알고 있는 센타는 e_1으로 부터 세션 키 Ks를 도출하여 공유하게 된다.

단말기 또는 가입자에 대한 인증은 네트워크 서비스 가입 시에 가입자가 부여 받은 certificate를 통해 이루어 진다. g()를 공개된 one-way function, f()를 DES나 FEAL-32와 같은 관용 암호화 알고리즘 $n_u = p_u q_u$를 또 하나의 공개키 modulus라 할때, 가입자 A는 ID_a에 근거한 증명서 c를 발급 받는다. 즉, $c^2 \equiv g(ID_a) \bmod n_u$. 세션 키 Ks의 공유가 이루어진 직후 가입자 단말기는 $e_2 = f(Ks,m), m = (ID_a,c)$를 센타측에 보내고 센타측은 $m = f^{-1}(K_S, e_2)$을 계산한 후 $g(ID_a)$와 c^2을 비교하여 인증 절차를 마친다.

4. 선형대수에 기반을 둔 프로토콜의 제안

본 절에서는 선형대수에 기반을 둔 단말기 사용자들 간의 세션 키 분배 프로토콜 및 가입자에 대한 네트워크 센타의 인증 프로토콜을 새로이 제시한다. 단말기에서의 세션 키 분배와 관련된 계산 복잡도는 단지 finite field 상의 벡터와 행렬간의 multiplication에만 기인하고, 가입자 인증은 challenge-response 방식으로 분배된 세션키를 이용해 이루어 진다. 세션 키 분배 방식에 있어서 일반적인 두 개의 square 행렬 간에는 곱셈상의 교환법칙이 성립하지 않지만 두개의 diagonal행렬간에는 성립한다는 사실이 본 연구의 기본적인 동기가 된다.

q를 power of prime, k와 n을 positive integers, $Q = GF(q)$, 그리고 Q^k를 Q상의 모든 k-tuple들로 이루어진 vector space라 할때, 다음의 용어를 먼저 정의한다.

- $\mathbf{ID}_i$: 집합 I에 속하는 가입자 i의 ID
- **S** : GF(q) 상의 n-by-n nonsingular 행렬
- **P** : GF(q) 상의 n-by-n nonsingular 행렬
- $\mathbf{m}_j$: 세션 j에 사용될 GF(q)상의 n-tuple
- **u** : 해밍 가중치가 $0 < wt(\mathbf{u}) < n-k$인 GF(q)상의 (n-k)-tuple
- g() : I로 부터 Q^k로의 injection을 수행하는 pseudorandom함수
- f(M,Ks) : 매세지 M을 세션 키 Ks로 암호화하는 관용 암호화 알고리즘

■ 시스템 생성 단계

네트워크 센타는 먼저 두개의 행렬 **S**와 **P**, 그리고 diagonal 행렬 $\mathbf{D}_i$를 각 가입자의 ID_i를 기반으로 생성한다. 즉, $\mathbf{D}_i$의 diagonal elements들은 '$g(ID_i) \| \mathbf{u}$'로 구성된다. 이때, '$\|$'는 concatenation을 의미한다. '$g(ID) \| \mathbf{u}$'의 해밍 가중치는 항상 n보다 작고 0보다는 크다. 각 가입자 i는 네트워크 서비스 가입 시에 자기의 비밀정보 $\mathbf{S} \cdot \mathbf{D}_i \cdot \mathbf{P}$를 부여 받는다. 네트워크 센타의 비밀정보는 **S**,**P**,**u** 그리고 g()이다.

다음의 프로토콜과 그림 6은 단말기 사용자 A와 B간의 네트워크 센타의 중계를 통한 세션 키 분배 및 인증 프로토콜의 절차를 설명한다.

■ 세션 키 분배 및 가입자 인증 프로토콜

① 가입자 A는 $\{ID_a, ID_b\}$를 네트워크 센타에 보낸다.

② 네트워크 센타는 random한 $\mathbf{m}_j$를 선정한 후, $\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}$와 $\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}$를 가입자 A와 B에게 각각 전송한다.

③ 가입자 A와 B는$(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}) \cdot (\mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{P})$.와 , $(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{S}^{-1}) \cdot (\mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{P})$를 각각 계산함으로써 공통된 세션 키 $Ks = \mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{D}_b \cdot \mathbf{P}$를 공유하게 된다.

④ 가입자 A와 B는 $f(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}, Ks)$ $f(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{S}^{-1}, Ks)$를 네트워크 센타에 전송하면 센타는 자기의 계산 결과와 비교하여 가입자에 대한 인증 절차를 마친다.

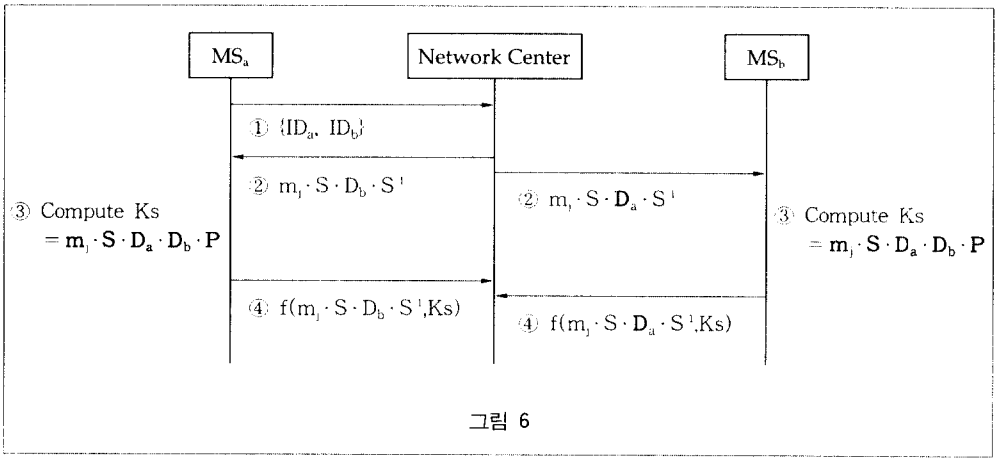

그림 6

본 논문에서 제시하는 프로토콜은 네트워크 센타측에서 보내는 하나의 challenge값 RAND를 통해 세션 키 생성과 가입자 인증을 수행하는 GSM 시스템의 프로토콜과 동일하다. ② 단계에서 네트워크 센타는 매 세션마다 random한 $\mathbf{m}_j$를 선택하기 때문에 서로 다른 두 세션에서 두 가입자가 동일한 세션 키를 공유할 가능성은 매우 희박하다. 가입자에 대한 인증은 GSM 시스템[5]에서와 같이 challenge-response 방식을 통해 이루어진다. 호(call)요구 가입자와 호출 가입자 간의 세션 키 분배를 위해 네트워크 센타가 전송하는 $\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}$와 $\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{S}^{-1}$가 challenge 값으로 이용되고, ④단계에서 가입자가 전송하는 $f(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_b \cdot \mathbf{S}^{-1}, Ks)$와 $f(\mathbf{m}_j \cdot \mathbf{S} \cdot \mathbf{D}_a \cdot \mathbf{S}^{-1}, Ks)$가 response 값이 된다. 네트워크 센타도 세션 키 Ks를 알고 있기 때문에 response 값을 자기가 계산한 것과 비교함으로써 가입자 A와 B에 대한 인증을 수행하게 된다.

■ 제안된 프로토콜에 대한 안전성 분석

Diagonal 행렬 $\mathbf{D}_i$의 diagonal elements의 해밍 가중치는 이미 언급한 바와 같이 0보다 크고 n보다는 작아야 한다. 그것을 보장하기 위해서 diagonal elements는 해밍 가중치가 0 보다는 크고 (n-k)보다는 작은 (n-k)-tuple $\mathbf{u}$와 $g(ID_i)$을 연결하여 구성한다. 해밍 가중치에 대한 그러한 제약 조건의 필요성은 두 가지 이다. 즉, 가입자들이 네트워크 센타의 비밀정보

S를 도출하지 못하게 하고, 또한 Ks = 0와 같이 유효성이 없는 세션 키의 생성을 방지하기 위해서 이다. 첫째, 만약 D_b가 nonsingular, 즉 diagonal elements들의 해밍 가중치가 n이면, 네트워크 센타의 비밀정보 S가 다음과 같이 노출되어 질 수 있다. 가입자 A와 B가 공모를 하면 $(S \cdot D_a \cdot P) \cdot (S \cdot D_b \cdot P)^{-1}$을 계산 함으로서 $C = S \cdot D_a \cdot D_b^{-1} \cdot S^{-1}$를 얻을 수 있다. 이때, $D = D_a \cdot D_b^{-1} = S^{-1} \cdot C \cdot S$인 nonsigular행렬 S가 존재하기 때문에 n-by-n 행렬 C는 "diagonalizable"하다. 그러므로, C와 연관된 n개의 eigenvalues와 eigenvectors를 구함으로써 S를 도출해 낼 수 있다. 둘째, $g(ID_a)$와 $g(ID_b)$간의 해밍 가중치가 k이고 u의 해밍 가중치가 0 이라 하자. 결국, $D_a \cdot D_b$는 zero행렬이 될 수가 있고 $Ks = m_j \cdot S \cdot D_a \cdot D_b \cdot P = 0$가 된다.

특정가입자, 예를 들어 가입자 B의 비밀정보 $S \cdot D_b \cdot P$를 도출하기 위한 가입자 A의 가능한 공격 방법을 분석해 보자. 가입자 A가 가입자 B와의 연결을 n번 시도함으로써 얻을 수 있는 정보는 $m_j \cdot S \cdot D_a \cdot S^{-1}$와 $m_j \cdot S \cdot D_a \cdot D_b \cdot P$(where j = 1, 2, ···, n)이다. X와 Y를 각각 $m_j \cdot S \cdot D_a \cdot S^{-1}$와 $m_j \cdot S \cdot D_a \cdot D_b \cdot P$(where j = 1, 2, ···, n)의 n개의 row vector들에 의해 구성된 n-by-n square 행렬이라고 하자. 만약 X의 rank가 n이면 $S \cdot D_b \cdot P$은 다음의 방정식의 해를 구함으로서 구할 수 있다.

$$X \cdot w_l = y_l \text{ for } l = 1,2, \cdots, n$$

위의 식에서 w_l은 $S \cdot D_b \cdot P$의 l번째 column vector이고, y_l은 l번째 column vector이다. 하지만, $m_j \cdot S \cdot D_a \cdot S^{-1}$에서 D_a의 diagonal elements의 해밍 가중치가 n보다 작기 때문에 X의 rank도 역시 n 보다 작게 된다. 따라서, 가입자 B의 비밀정보를 도출해 내는 것은 불가능하다.

5. 결 론

본 논문에서는 디지탈 이동통신 시스템을 위해 제안된 기존의 세션 키 분배 및 가입자 인증 프로토콜의 특성을 분석하고, 선형대수에 기반을 둔 새로운 프로토콜을 제안하였다. 공개키 암호체계에 그 기반을 둔 기존의 프로토콜과는 달리 새로이 제안된 프로토콜의 계산 복잡도는 단지 유한 체 상의 벡터와 행렬의 곱에만 기인한다. 또한, GSM 시스템에서와 같이 네트워크 센타에 의해서 주도되는 challenge-response 방식을 통해 세션 키의 분배와 가입자에 대한 인증이 동시에 이루어 진다.

현재의 이동통신 단말기 사용자의 통화는 네트워크 센타의 중계를 통한 유선 전화망 가입자와의 통화가 대부분을 차지하지만 가까운 장래에 실현될 개인휴대통신(PCS:personal communication system) 시대에는 단말기 사용자들간의 통화가 빈번해 질 것이다. 이와 관련하여 본 논문에서 새로이 제시되는 세션 키 분배 프로토콜은 Tatebayashi 등이 제시한 방식에서 처럼 단말기 사용자들 간의 직접적인 세션 키의 분배를 다루었다.

참 고 문 헌

[1] Rabin,M.O., 'Digitalized Signatures and Public Key Functions as Intractable as Factorization', MIT Laboratory for Computer Science, TR 212, January 1979.

[2] Willams, H.C., 'A Modification of RSA Public-Key Encryption', IEEE Trans. on Inform. Theory, vol.IT-26, no.6, November 1980.

[3] Tatebayashi, M., Matsuzaki, N., and Newman, Jr,. DB., 'Key Disribution

Protocol for Digital Mobile Communication Systems', Advances in Cryptology, Proeedings of Crypto'89, 1989, pp. 324-334.

[4] Beller, M.,J., Chang, L.F., and Yacobi, Y., 'Privacy and Authentication on a Portable Communication Systam', IEEE GLOBECOM'91 Conference, 1991, pp. 1922-1927.

[5] ETSI-GSM, Technical Specification GSM 03.20, 'Security Related Network Functions', Version 3.3.2 (Release 92, phase 1)

[6] Vedder, K, 'Security Aspects of Mobile Communications',Computer Security and Industrial Crytography, Lecture Notes in Computer Science 741, Springer-Verlag, Berlin,1993, pp. 193-210.

[7] Park, Choonsik., K., and Okamoto, T., and Tsujii, S., 'On Key Disribution and Authentication in Mdbile Radio Networks', Advances in Cryptology, Proceedings of Eurorypt'93, 1994, pp. 461-465.

[8] 전자신문사, 95년 판 정보통신연감.

[9] Fehrer, K., Wireless Digital Communications, Prentice-Hall, 1995.

□ 著者紹介

박 창 섭

1958년생
연세대학교 경제학과 졸업
미국 Lehigh 대학 전자계산학과 석사
미국 Lehigh 대학 전자계산학과 박사
현재 단국대학교 전자계산학과 부교수

※ 관심분야 : 부호이론 및 암호이론