개인 통신망에서 적용가능한 인증 및 키분배 프로토콜

송 희 삼°, 전 문 석*
숭실대학교 전자계산학과

An applicable Key Distribution and Authentication Protocol in Personal Communication Networks

Hee-Sam Song°, Moon-Seog Jun*
Dept. of Computer Science, Soongsil Univ.

Abstarct

In this paper, We present that protocols have already proposed an applicable key distribution and authentication protocol based discrete logarithm and prime-factorization problem in PCN(Personal Communication Network) is anaysised. We newly propose identiity-based protocol using smart card. This proposed potocol is that Fiat-Shamir identification scheme and a new key distribution scheme based on Fiat-Shamir identification scheme are joined. Proposed protocol is compared with exiting protocols with respect to security and efficiency to evalate performance, so its calculation is reduced in key distribution and authentication to evaluate performance.

1. 서 론

개인 통신망은 개인에게 부여된 고유의 개인번호를 이용한 사용자 위주의 이동통신 서비스로써 PSTN과 가입자 단말간의 유선접속을 무선화함으로써 가입자는 단말기로부터 자유로운 이동성을 보장받을 수 있고 지능화된 통신 처리기능과 연동을 가능케 함으로써 고부가가치 서비스를 제공할 수 있다. 이동통신 시스템은 언제, 어디서, 누구와도 어떤 종류의 통신을 가능하도록 하는 것을 목적으로 구축되고 있다. 현재 우리나라는 차세대 디지틀 이동통신 표준 방식으로 미국에서 제안하고 있는 CDMA 방식을 Qualcomm사의해 데이터의 보호 시스템을 도입하고 있다. 이동통신에 암호시스템을 적용하기 위해서는 몇가지 고려사항이 있다. 첫째로 연산처리 능력이 제한되어 있는 단말기로써는 이상적인 시간내에 세션키를 얻을 수 있어야 한다는 것이고 두번째로 무선을 이용하기 때문에 정보의 노출이나 불법 수정에 대해 안전한 것과 다른 사람의 단말기를 무단 사용하면 그 단말기 소지자의 ID로 요금이 부과되기 때문에 부단한 과금에 대한 대비책등이 있어야한다. 이런 점을 고려하여 개인 통신 시스템에서는 단말기와는 별도로 사용자에게 스마트 카드를 발급하여, 스마트 카드내에서 암호화 연산처리를 수행하고 사용자 개인 식별방식도 수행하도록하여 단말기와는 별도로 과금을 할 수 있도록 하는 것이다.[3] 본 논문에서는 제안한 프로토콜에서 사용자 인증시에 이용되는 인증 방식은 기존의 프로토콜보다 단말기에서의 연산처리량을 크게 줄일 수 있는 ID를 기본으로 하는 인증 방식이다. 특히 각 사용자의 키분배에 대한 안전성을 높이기 위하여 인증센타에서 사용자를 인증할 때 사용자의 비밀정보가 노출되지 않는 인증 방식을 키분배 프로토콜에 적용시키고자 한다. 제안하는 프로토콜은 Fiat-Shamir의 개인식별 방식과 Fiat-Shamir의 개인식별 방식을 변형시킨 새로운 키

분배 방식을 결합하여 구성하는 프로토콜이다.

본 논문에서는 2장에서는 기존의 PCN에 적용 가능한 인증 및 키 분배 프로토콜에 대해 고찰하고, 3장에서는 이 키분배 프로토콜에 대한 문제점을 보완할 수 있는 새로운 키분배 프로토콜을 제안한다. 그리고 지금까지 제안되었던 대표적인 인증 및 키분배 프로토콜을 분석하고, PCN에 적합한 변형된 Fiat-Shamir을 이용한 인증 및 키분배 프로토콜을 새롭게 제안하고 제안한 방법에 대한 안전성과 효율성에 관해 비교,검토한다.

2. 지금까지 제안된 PCN에 적용가능한 인증 및 키분배 프로토콜에 대한 고찰

공개키 암호시스템[6]을 이용하여 인증 기능을 수행하는 경우, 통신 상대방의 공개 암호키를 획득하는 방법은 각각의 사용자가 통신 가능성이 있는 모든 통신 상대의 공개키를 저장하는 방법, 비밀 통신에 앞서 상대방과 미리 통신하여 암호키를 얻는 방법, 그리고 키 인증 센타에게 상대의 공개키를 조회하는 방법등이 있다. 이러한 방법은 암호 통신을 하기 위해서 비밀 세션키를 키분배센타(key distribution center)에서 제공받거나 자신이 직접 관리해야 하며 공개키의 경우도 공개화일을 유지하거나 KDC에서 제공 받아야한다는 문제점이있다. 통신 상대의 암호키 보관시에 어려운 문제를 해결하기 위해서 ID에 의한 방식에 대한 연구가 널리 수행되고 있다.

2.1 소인수 분해 문제에 바탕을 둔 인증 및 키분배 프로토콜[1]

본 절에서는 이동통신 시스템에 적용가능한 Tatebayashi등이 제안한 인증 및 키분배 프로토콜을 기술한다. 이 프로토콜은 센타가 사용자 인증과 키분배에 직접적으로 관여하여 사용자 터미날의 암호화 연산처리를 분담하는 프로토콜이다. 이것의 키 분배 프로토콜은 (그림 1)과 같다. 이 프로토콜은 세션키 분배 방식을 사용자의 인증기능과 세션키 분배 기능을 동시에 수행하며, 타임스탬프 t_A의 유효성을 검증함으로 재생공격을 방지할 수 있는 효율적인 방식이다. 따라서 매우 빠른 암호화가 수행되지만 통신 상대방의 두 가입자인 A와 B가 세번만 통신하게 되면 B는 $(C_A \| t_A \| R_A)$(여기서,C_A는 센타만이 알고 있는 일방향함수,R_A는 랜덤수)으로부터 A의 C_A를 구할 가능성이 높아서 해당 사용자를 가장할 수 있어 비도가 그리 높지다는 단점이 있고 네트워크 센타가 가입자간의 세션키를 모두 알고 있기 때문에 모든 가입자의 통신 내용을 쉽게 도청할 수 있다는 단점이 있다.

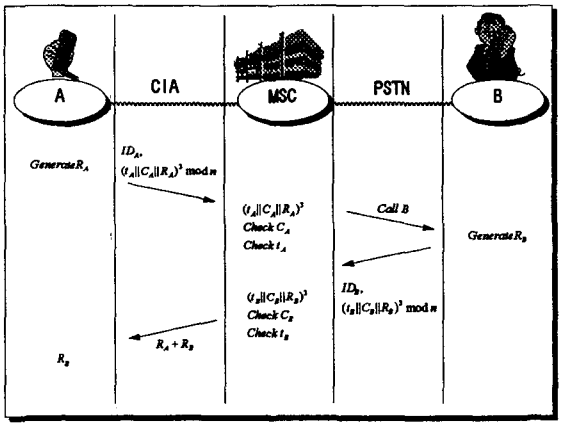


그림 1) 소인수 분해에 문제에 바탕을 둔 인증 및 키분배 프로토콜

2.2 이산대수 문제에 바탕을 둔 인증 및 키분배 프로토콜[3]

이산대수(discrete logarithm)의 계산의 어려움의 정도에 따라 비도가 결정되는 Diffie-Hellman / ElGaman의 혼합된 공개키 암호화 시스템은 p가 소수일 경우, GF(P)상의 이산 대수 문제를 푸는 것이 어렵다는 사실에 근거를 두고 있는 인증방식을 이용한 프로토콜이다. 키 발행 센타 인증 및 세션키키 분배에 이용되는 각 사용자의 비밀정보를 발급하여 스마트 카드 형식으로 전달하며, 이 비밀정보에 대응되는 공개정보를 키 인증 센타의 데이타 베이스에 저장하도록한다. 키 분배 및 인증의 주체는 인증 센타, 통신을 원하는 두 사용자들이다. 따라서 키 운영 센타는 사용자의 비밀정보 S_i를 유도할 수 없으므로 사용자간의 세션키를 구할 수 없다. 즉, 키 인증 센타는 암호된 트래픽에 대한 정보을 불법도청 및 접근할 수 없게된다. 이것의 키 분배 프로토콜은(그림 2)와 같다.

이 방식은 사용자 측면에서 계산량을 최소화한 개인 통신망에 적용 가능한 효율적인 인증 및 키분배 방식이다. 인증 센타가 사용자에 대한 공개정보를 저장하고 인증시 데이타 베이스와 접속해야 하며 인증 센타에서 계산량이 많다는 단점이 있다.

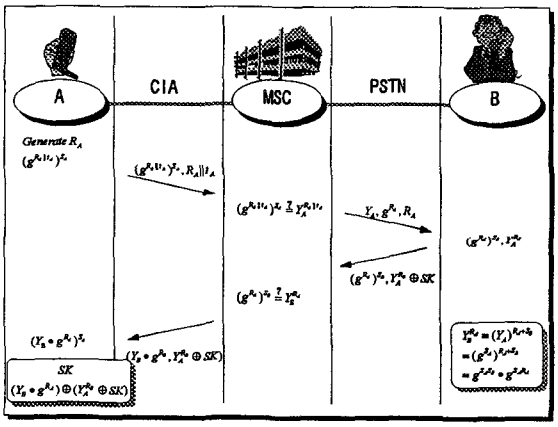


그림 2)이산대수 문제에 바탕을 둔 인증 및 키분배 프로토콜

3. 새로운 제안한 키분배 프로토콜

Fiat-Shamir 개인식별방식[8]은 개인식별 정보 ID의 평방 잉여 s_i를 계산하여 가입자의 비밀키로 사용하였다. 이 방식의 안전성은 충분히 큰 두 소수 p,q의 곱인 n의 소인 수 분해를 모를 때, 제곱근을 구하는 문제는 어려운(NP 문제)라는 것에 근거한다.

사전 준비 과정에서 신뢰 센타는 소수 p,q를 선택하여 비밀리에 보관하고, 그 곱인 n을 공개한다. 카드 발급 과정에서 센타는 합법적인 사용자에게 카드를 발급할 때, 그 사용자에 관한 개인정보(이름,ID번호,주소,주민등록번호 등)와 카드에 관한 정보(유효기간 등)를 담고 있는 ID를 준비하고, mod n상에서 ID_i의 평방근을 계산하여 그 역수 S_i를 각 가입자의 비밀키로 한다.

사실, 모든 ID_i가 mod n상에서 평방근을 갖지는 않으므로, 이 문제의 해결의 해결책으로 임의의 스트링을 [0,n] ($2^{511} < n < 2^{512}$인 양의 정수)으로 사상하는 의사 랜덤함수 f를 선택하여 공개하여 아래와 같이 비밀키를

생성한다.

① $v_j = f(ID_i, k_j)(j = 1,2,\cdots,m)$ 을 구한다.

✦ 의사 랜덤 함수 $f: Z_n \times Z \rightarrow \{1,\cdots,2^k - 1\}$

② 이 중에서 평방 잉여를 갖는 k개의 v_j를 선택한 후 각 v_j^{-1}의 가장 작은 제곱근 S_j를 갖는 k개를 구한다.

✦ 공개키 $v_i(i = 1,\ldots,k)$, $v_j^{-1} \equiv s_i^2 (\mathrm{mod}\, n)$

③ID_i와 k개의 S_j 단, 평방 잉여성 여부는 Jacobi심볼을 이용하여 판단될 수 있다.

✦ 비밀키 $s_i \in Z_n, (i = 1,\cdots,k)$

각각의 j값을 카드에 담아 사용자에게 발급한다.

3.1 PCN에 적용 가능한 새롭게 제안하는 키분배 방식을 이용하는 키분배 프로토콜

키 분배 프로토콜에 Fiat-Shamir의 인증 방식을 이용하는데 알맞은 키분배 방식이 없기 때문에 각 사용자의 비밀키와 공개키로 구성되는 키분배 방식을 이용하는 새로운 키분배 프로토콜을 제안한다. Fiat-Shamir의 개인식별 방식을 사용자 인증 방식으로 하고, Fiat-Shamir의 개인식별 방식을 변형시킨 키분배 방식을 결합시켜서 다음과 같은 키분배 프로토콜을 구성한다.

단계 1) 사용자 A는 0과 n-1사이의 임의의 난수 R_A 을 생성하여 $f(R_A{}^2 (\mathrm{mod}\, n), ID_A \| ID_B \| t_A) = E_A$ 를 계산하고, 개인식별은 $P_A = R_A \prod_{j=1}^{k} S_{Aj}^{e_{Aj}}$ 을 계산한다. (1.1)

단계2) 사용자 A는 $ID_A \| ID_B \| t_A, E_A, P_A$ 을 센타에게 전송한다.)1.))

단계 3) 센타는

$f(P_A{}^2 \prod_{j=1}^{k} v_{Aj}{}^{e_{Aj}}, ID_A \| ID_B \| t_A)$ 와 E_A 가 같은지를 확인하여 A가 정당한 사용자인가를 확인하고, 사용자 B에게 E_A 을 전송한다. (1.3)

단계 4) 사용자 B 는 R_B 을 생성하여

$f(R_B{}^2 (\mathrm{mod}\, n), ID_B \| ID_A \| t_B) = E_B$ 을 계산하고,

개인식별 $P_B = R_B \prod_{j=1}^{k} S_{Bj}^{e_{Bj}}$ 을 계산한다. (1.4)

단계 5) 사용자 B는 랜덤수 E_A 을 이용하여 $E_{AB} = E_A E_B$ 을 계산하고, $R_{SK} = R_B \prod_{j=1}^{k} (v_{Aj} S_{Bj})^{e_{ABJ}}$ 을 계산한다.

사용자 B는 세션키 $SK = R_B \prod_{j=1}^{k} S_{Bj}^{e_{ABJ}}$ 을 생성한다. (1.5)

단계 6) 사용자 B는 $ID_B \| ID_A \| t_B, P_B, P_{SK}, E_B, E_{AB}$ 을 센타에게 전송한다. (1.6)

단계 7) 센타는 $f(P_B^2 \prod_{j=1}^{k} v_{Bj}^{e_{Bj}}, ID_B \| ID_A \| t_B) = E_B$ 을 확인하여 B가 정당한 사용자인가를 확인하고, 사용자 A에게 R_{SK}, E_{AB} 을 전송한다. (1.7)

단계 8) 사용자 A는

$$SK = R_{SK} \prod_{j=1}^{k} S_{Aj}^{2e_{ABj}} = R_B \prod_{j=1}^{k} v_{Aj}^{e_{ABj}} \bullet S_{Aj}^{2e_{ABj}} \bullet S_{Bj}^{e_{ABj}} = R_B \prod_{j=1}^{k} S_{Bj}^{e_{ABj}}$$ 을 계산하여 세션키를 생성하게 된다. (1.8)

단계 9) 위와 같은 각 사용자 인증은 t회, 키분배 방식은 S회 반복한다.

다음 (그림 3)는 제안하는 Fiat-Shamir방식 키분배 프로토콜이다.

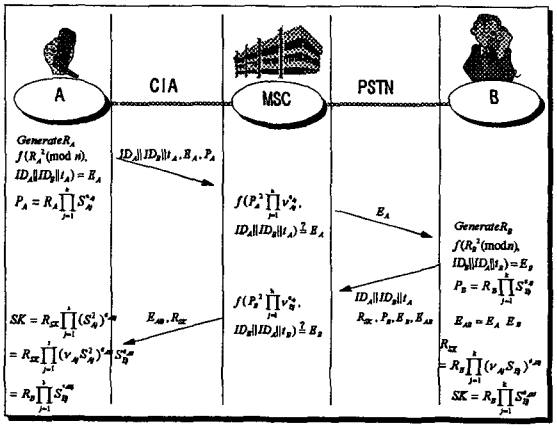


그림 3) 제안하는 Fiat-Shamir방식 키분배 프로토콜

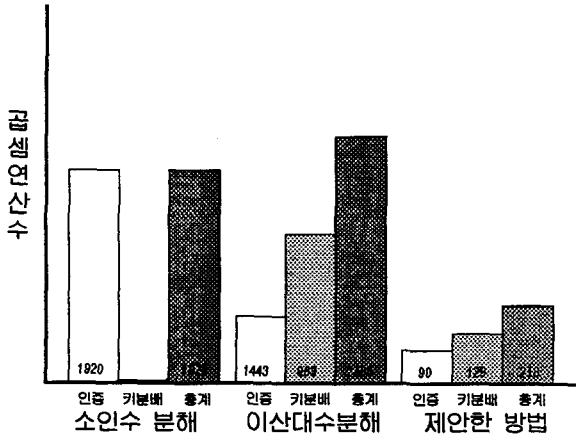
4. 제안하는 키분배 프로토콜에 대한 안전성과 효율성 분석

Fiat-Shamir의 개인식별 방식을 이용하는 프로토콜은 평방 잉여 제곱근 분배의 어려움에 근거하는 키분배 프로토콜이다. 이 프로토콜에서 사용자A의 지식이 사용자 B에게 전송되지 않으므로 영지식이며 안전성은 매개변수(Security Parameter) k, t에 의존한다. 제 3자인 침입자가 A인척 위장하려면 식(1-5)를 정확히 t회 생성해야 한다. 침입자가 식(1-5)를 1회 정확히 생성할 확률은 2^{-k}이며 e_{ij}를 t회 정확히 생성할 확률은 2^{-kt}이므로 k와 t를 적정 크기로 하면, 침입자가 A인척 할 수 있는 확률은 무시할 수 있을 정도의 확률이라고 할 수 있다. 따라서 사용되는 키분배 방식은 송신자 자신의 비밀키와 수신자의 공개키를 이용하기 때문에 자신의 비밀키가 공개키에 의해 노출되지만 않는다면 키분배 방식은 안전하다. 재생공격에 대비해서는 Time-stamp를 이용하여 공격을 대비했으며, 특히 센터에서 사용자의 비밀정보가 노출되지 않기 때문에 센터와의 협작과 센터의 부정방지 등에 대해서는 기존 프로토콜에 비해 매우 안전하다. 다음 표는 <표 1>은 본 논문에서 제안하는 프로토콜과 기존의 프로토콜에 대해서 여러 가지 공격에 대한 안전성을 비교한 것이다.

분류 / 프로토콜	사용자 확인	키 분배	재생 공격	불법 조작	센타 부정방지
소인수분해 문제	❑	❑	❑		
이산대수분해 문제	❑	❑	❑	❑	❑
제안한 방식	❑	❑	❑	❑	❑

<표 1> 제안하는 프로토콜과 기존의 프로토콜에 대한 안전성 비교

연산 처리량을 비교하기 위해서 소인수 프로토콜에 이용하는 키분배 프로토콜에서 e=3, n=512 을 사용하고 이산대수의 방식을 이용하는 프로토콜에서 p=512,q=600 을 사용하고 Fiat-Shamir 방식을 이용하는 방식에서는 k=9, t=8, n=512 로 사용하였다. RSA 방식에서는 Trustered Center 는 불필요하고 인증시에 M(750)정도의 곱셈 연산에 해당되는 1 회의 지수계산과 확인과정에서 M(2)가 필요하다. 이산대수문제와 Fiat-shamir 은 Trustered Center 가 필요하고 Fiat-shamir 은 인증과정에서 M(45)정도의 곱셈 연산과 확인과정에서 M(45)의 곱셈 연산 과정을 필요로 한다.



<표 2> 제안한 프로토콜의 인증, 키분배의 연산 처리량 비교

5. 결 론

본 논문에서는 PCN 에 적용 가능한 여러 가지 인증 및 세션키 분배방식을 살펴보고 Fiat-Shamir 의 ID 를 기본으로 하는 개인식별 방식을 사용자 인증 방식으로 하고, Fiat-Shamir 의 개인식별 방식을 변형시킨 키분배 방식을 결합시켜 새로운 키분배 프로토콜을 제안하였다. 이 프로토콜은 기존에 제안된 소인수 분해 문제에 바탕을 둔 RSA 과 이산대수 문제에 바탕을 둔 인증 및 키분배 프로토콜과 비교했을 때, 인증과 키분배에서 연산 처리량을 많이 줄일 수가 있었다. 따라서 PCN 의 환경에서는 가입자 단말에는 전력이 제한되어 있으므로 전력적인 면에서 연산량을 적게함으로 전력을 적게 소비하면서 안전성을 보장할 수 있는 효율적인 프로토콜임을 볼 수 있었다. 그러나 프로토콜에서 수행되는 데이타량이 다른 프로토콜에 비해 많다는 단점이 있다. 따라서 데이타의 저장 능력이

큰 스마트 카드일 경우 이 프로토콜이 효과적이라 할 수 있다.

6.참 고 문 헌

[1] Choonsik Park, Kaoru KUROSAWA and Shigeo TSUJII, "Key Distribution Protocol for Mobile Communication Systems", IEICE Trans. Fund., vol. E78-A, No.1, Jan,1995.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. on Information Theory, vol. IT-22, pp. 644-654, 1978.

[3] 염흥렬, 이만영, 김재공, "이동통신에 적용가능한 인증 및 세션키 분배방식과 키스트림 생성기에 관한 연구", 통신정보보호학회지 제4호 제3권 1994.9

[4] "정보보호를 위한 디지탈서명 표준 워크샵 자료집" 1994.4.25

[5] A. Fiat and A. Shamir, "How to prove youself : Practical solution to identification and sinnature problem." Proc. Crypo 86, pp. 186-194. 1986

[6] GNANESH COOMARASWAMY and SRIKANTA P. R. KUMAR, "A Novel Method for Key Exchange and Authenticfication with Celluliar Network Applications." IEEE Con93, pp. 186-190, 1993.

[7] R . Akiyama, S. sasaki, " Authentication and encrytion in mobile communication system," Proc. 43th IEEE VT Conference, pp 927-930, 1993.

[8] "현대 암호학" , 한국 전자 통신 연구소. 1991.

[9] 원동호, "암호방식과 키분배", 통신정보보호학회지 제14호 제1권 1991.4