通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

이동 시스템에서의 효율적인 인증 및 키 교환 프로토콜

최 영 근*, 김 순 자**

An efficient Authentication and Key Agreement Protocol in Mobile Systems

Yeong-Geun Choe*, Soon-Ja Kim**

요 약

본 논문은 휴대폰, 개인 휴대단말기 등과 같은 낮은 연산 처리 능력을 가지는 시스템에서 사용하기 위해 설계된 인증 및 키 교환 프로토콜을 제안한다. Rabin 암호시스템에 기반한 프로토콜의 구현은 무선 통신에 있어서 통신 패스수와 연산 부하의 최소화라는 측면에서 효율성을 제공한다.

또한 기존의 인증 및 키 교환 프로토콜을 소개하고 제안한 프로토콜을 다양한 측면에서 분석하고 비교할 것이다.

ABSTRACT

In this paper we propose an efficient authentication and key agreement protocol which has been designed specifically for use with low powered computationally weak equipment such as Cellular phone and PDA(Personal Digital Assistant). Implementing the protocol based on the Rabin cryptosystem provides the efficiency requirements for mobile communications including minimum number of passes and low computational load.

The paper outlines the new protocol, examines its various aspects, and compares them to those of the representative authentication and key agreement protocols.

keyword : Authentication, Key Agreement, Key exchange

Ⅰ. 서 론

최근 이동통신의 가입자의 확대와 더불어 전자우편, 게임, 채팅 등의 서비스를 제공하는 무선 인터넷 서비스가 매우 각광받고 있다. 이동통신의 휴대성, 개인성과 인터넷 서비스의 폭발적 요구로 인해 '언제, 어디서나' 인터넷 접속의 실현이 가능하도록 여러 단체나 기업에서 무선 인터넷 표준안들을 제시하고 있다. 에릭슨, 노키아 등이 주도하는 WAP (Wireless Application Protocol), 마이크로소프트사의 ME (Mobile Explorer), SUN의 J2ME (Java2 Micro Edition) 등이 바로 그것이다. 이러한 무선 인터넷을 위한 표준들은 기존의 음성 서비스에 국한되지 않고 좀더 고급서비스들을 제공하여 사용자들의 욕구를 충족시키고 있다.

현재 무선 인터넷은 게임, 전자우편, 채팅 등의 서비스가 주를 이루고 있지만, 점차 뱅킹, 증권거래, 쇼핑과 같은 비즈니스 응용분야까지 영역을 확장하고

* 경북대학교 전자전기공학부 컴퓨터 통신망 연구실(ind@palgong.knu.ac.kr)
** 경북대학교 전자전기공학부 컴퓨터 통신망 연구실(snjkim@ee.knu.ac.kr)

있는 추세이다.

특히 음성 위주의 무선 통신에서는 도청 및 복제 단말기를 사용한 통화도용 등이 문제가 되지만, 증권, 쇼핑, 뱅킹 등과 같은 단순한 정보 서비스를 뛰어넘는 상거래 활동이 진행되는 비즈니스 응용 서비스에서는 사용자 인증, 데이터 기밀성 보장 등의 정보보호 서비스가 필요하다.

또한 무선 인터넷에서의 보안은 무선 네트워크 환경을 충분히 고려해 이뤄져야 하며, 단순히 무선 네트워크에만 그치는 것이 아니라 유선 네트워크와의 연동을 반드시 고려해야한다.

일반적인 사용자 인증기술은 사용자 ID와 패스워드에 의해 이뤄지며 이것은 도청, 재전송 공격 등에 매우 취약하여 그대로 사용하기에는 문제점이 많다.

무선 인터넷에 사용되는 사용자(또는 가입자) 인증 프로토콜의 목적은 통신에 참여하는 개체들을 인증하고 그들 사이에서 주고 받을 데이터를 암/복호화할 세션키(session key)를 설정하는 데 있다.

2세대 시스템의 인증 프로토콜들은 비밀키 방식의 인증 프로토콜로 사용자와 홈 네트워크간의 미리 설정된 마스터 키를 통하여 세션키의 분배와 인증을 수행한다. 이는 초기 설정시 홈 네트워크가 온라인으로 관여해야 하고 사용자와의 마스터 키를 관리하기 위한 secure database를 유지해야 한다. 이러한 많은 수의 secret-key를 유지하는 database는 시스템 자원에 많은 부하를 가져다 준다.

이러한 문제점을 해결하기 위한 공개키 방식의 인증 프로토콜은 크고 복잡한 통신 네트워크에서 확장성과 키 관리가 용이하면서 온라인 인증서버가 필요하지 않는 장점을 가진다. 그러나 비밀키 방식의 인증 프로토콜과 비교해서 공개키 방식 인증 프로토콜은 더 복잡한 연산량을 가진다.

본 논문에서 제안하는 인증 및 키 교환 프로토콜은 Rabin 암호시스템에 기반한 공개키 방식의 프로토콜이다. 제안하는 프로토콜은 유럽의 차세대 이동통신 표준인 UMTS(Universal Mobile Telecommunications Systems)의 보안 서비스 제공을 위해 ASPeCT(Advanced Security for Personal Communications Technologies) 프로젝트에서 제시한 인증 및 키 교환 프로토콜을 위한 보안 요구조건[1]을 대부분 만족시키고 공개키 암호 시스템으로 Rabin 암호시스템을 사용하여 멱승으로 인한 과도한 연산량을 줄임으로서 휴대폰, 개인 휴대단말기(Personal Digital Assistant) 등과 같은 낮은 연산 처리 능력을 가지는 시스템에 적합하도록 설계되었다.

본 논문을 개략적으로 살펴보면 다음과 같다. 2절에서 인증 및 키 교환 프로토콜에서 고려해야 할 보안 특성과 요구 조건들을 살펴볼 것이다. 3절에서 기존의 인증 프로토콜들을 비교하고 4절에서 효율적인 인증 프로토콜을 제안할 것이다. 또한 제안한 프로토콜에 대한 보안 특성들에 대해 살펴볼 것이다. 5절에서 기존 프로토콜들과 보안 특성과 요구조건을 비교하고 6절에서 결론을 내릴 것이다.

II. 고려해야 할 보안 특성

2.1 인증 및 키 교환 프로토콜에 관한 보안 요구조건

유럽의 차세대 이동통신 표준인 UMTS의 보안 서비스 제공을 위해 ASPeCT 프로젝트에서 연구된 인증 및 키 교환 프로토콜에서 고려해야 할 보안 특성과 요구 조건은 아래와 같다. 본 논문에서 제안하는 프로토콜 또한 이러한 요구조건들을 대부분 만족시키도록 설계되었다.[1]

(1) 상호 개체 인증(mutual entity authentication)
실시간으로 통신에 참여하고 있는 두 개체가 서로 상대방의 신분을 확인하는 과정으로 서로 다른 개체에 대한 가장(masquerade)을 방지하기 위하여 필요하다.

(2) 공개키 인증서의 상호 교환(exchange of certified public keys)
공개키 기반 인증 및 키 설정 프로토콜을 지원하기 위해서는 사용된 공개키의 정당성에 대한 확인 과정이 반드시 필요하다. 이를 해결하기 위한 방법으로 공개키 인증서를 상호 교환한다.

(3) 세션키에 대한 상호 동의(mutual agreement of a secret key)
이동국과 기지국사이에 교환되는 데이터를 보호하기 위해서 세션키는 이동국과 기지국이 상대방과 자신의 정보 모두를 사용하여 각각 생성하여야 한다.

(4) 세션키의 상호 제어(joint control of the secret key)
다른 한 개체가 우연히 또는 고의적으로 약한(weakened) 키를 선택하는 것을 방지하기 위해 이동국과 기지국이 세션키에 영향을 미치는

정도가 동일하여야 한다. 즉, 세션키 생성에 사용되는 이동국과 기지국의 정보가 세션키에 미치는 영향이 동일하여야 한다.

(5) 키 인증(key authentication)
키 인증은 함축적 키 인증(implicit key authentication)과 명확한 키 인증(explicit key authentication)의 두 가지 형태로 구분될 수 있다.
- 함축적 키 인증 : 통신에 참여하지 않는 다른 개체가 설정된 세션키를 얻을 수 없도록 하기 위해 대응되는 키를 가능한 한 참여하는 개체만이 계산할 수 있어야 한다.
- 명확한 키 인증 : 대응되는 키를 가능한 한 참여하는 개체만이 계산할 수 있어야 하고 실제로도 계산되어야 한다.

(6) 키 신규성에 대한 상호 확신(mutual assurance of key freshness)
이전 메시지의 재사용으로 이전의 키를 재 설정하는 공격(replay attack)을 방지하기 위해 필요한 요구조건이다.

(7) 사용자 신분의 기밀성(confidentiality of the user identity)
사용자의 신분이나 특정 사용자의 위치를 추적하기 위해 주고 받는 데이터를 가로채는 것을 방지하기 위해서 주고 받는 데이터를 암호화해서 보내야 한다.

(8) 부인 봉쇄(non-repudiation)
중요한 데이터나 사용자의 요금에 관련된 부인할 수 없는 증거가 보장되어야 한다.

2.2 프로토콜 설계에 있어서의 제한점

유선 네트워크와 비교해서 이동국은 제한된 계산능력, 전력 소모량, 메모리 크기, 전송속도, 안정성, 제한된 대역폭 등 무선환경에 따르는 여러 가지 고려해야 할 것이 많다. 따라서 다음과 같은 효율성에 관한 성질을 고려해야 한다.

(1) 통신 패스의 최소화 : 교환되는 트랜잭션 수를 가능한 줄여야 한다.
(2) 대역폭 사용의 효율화 : 프로토콜 메시지를 가능한 짧게 유지해야 한다.
(3) 연산 부하의 최소화 : 사전계산 단계를 두어 온라인 계산을 오프라인 계산으로 하여 실시간 실행시의 연산량을 줄일 수 있다.

Ⅲ. 기존의 인증 및 키 교환 프로토콜

이 절에서는 기존에 발표된 인증 및 키 교환 프로토콜을 비교하고자 한다. 이후 논문에서 사용될 기호와 그 의미들은 [표 1]과 같다.

3.1 개선된 BCY(Beller-Chang-Yacobi) 프로토콜

BCY프로토콜[2]은 비밀키 방식과 공개키 방식의 조합을 도입한 최초의 방법들 중 하나로 처음 발표된 이후 많은 개선이 있었다.[3,4,5] Carlsen은 BCY 프로토콜과 Diffie-Hellman의 키 교환 프로토콜을 결합해서 개선된 MSR+DH 프로토콜을 제안하였고[6] Varadharajan과 Mu는 Carlsen의 MSR+DH 프로토콜을 개선하여 현재의 표준 프로토콜과 비슷한 구조를 가지는 프로토콜을 제안했다.[7] 개선된 BCY프로토콜에서 MSR 시스템은 인증서를 생성하는데 사용되고 Diffie-Hellman 기법은 공통된 세션키를 설정하는데 사용된다.

개선된 BCY 프로토콜을 살펴보면 아래와 같다.

1. B → M : $r_B \| Cert_B^*$
2. M → B : $x \| E_{r_M}(r_B, ID_M, g^m, Cert_M^*)$
   여기서 $x = r_M^2 \pmod{N_B}$, $KK = (g^b)^m$, $K = E_{KK}(r_M)$이고 B는 기지국(Base Station), M은 이동국(Mobile Station)이다. 앞으로 논문에서는 B와 M으로 표시할 것이다.

이 프로토콜은 2절에서 살펴본 여러 보안 요구조건들을 많이 만족시키지 못한다([표 3] 참조). 보안

[표 1] 사용된 기호의 정의

기 호	정 의
ID_E	개체 E의 ID
e	개체 E의 비밀키
$P_E = g^e$	개체 E의 공개키
$Cert_E$	개체 E의 인증서
r_E	개체 E가 생성한 임의의 Nonce
TS	기지국이 생성하는 타임스탬프(timestamp)
RT	실시간(realtime)
K	이동국과 기지국 사이에 설정되는 세션키
$E_K(x)$	K를 사용해 x를 암호함
$h(x)$	일 방향 해쉬 함수
$Sig_E(x)$	개체 E의 서명

요구조건 중 단지 공개키 인증서의 상호교환, 세션키에 대한 상호 동의, 사용자 신분의 기밀성만 만족시키고 있으므로 다소 비현실적인 프로토콜이라 할 수 있다.

누구나 다른 개체에게 사용자나 기지국의 역할을 대신할 수 있기 때문에 어느 방향으로나 개체 인증이 없다. 또한 기지국이 단지 사용자만이 r_M을 알고 있다는 확신을 가질 수 없기 때문에 상호 함축적인 키 인증 뿐 만 아니라 키 확신을 할 수 없다.

3.2 PACS(Personal Access Communications System) 프로토콜

PACS 프로토콜은 선택적으로 공개키 기반 인증 프로토콜을 지원한다.[8] 프로토콜의 흐름은 아래와 같다.

1. B → M : $Cert_B \| RT$
2. M → B : $E_{P_u}\{K \| ESN \| TID_M \| RT\} \| E_K\{Cert_M\}$

기지국이 인증서 $Cert_B$와 실시간 RT를 broadcast channel을 이용해 전송하면 이동국은 기지국이 보내온 정보를 이용하여 세션키 K를 다음과 같이 계산한다.

$$K = Sig_M\{RT \| ID_B \| TID_M \| ESN\}$$

그런 다음 ESN, TID_M 그리고 RT와 같은 파라미터들을 기지국의 공개키로 암호화하고 이동국의 인증서는 세션키 K로 암호화해서 기지국으로 보낸다. 기지국은 복호화 과정을 통해 세션키 K를 얻고 이동국의 인증서와 서명을 검증하게 된다.

PACS 프로토콜은 키 교환 프로토콜이 아니라 키 분배 프로토콜이며 세션키는 두 개체 사이에서 서명의 역할을 담당하며 일반적인 서명으로는 사용되지 않는다.

3.3 Zheng의 1.5-move 프로토콜

Zheng은 일명 1.5-move 프로토콜을 제안했다.[9] Zheng의 1.5-move 프로토콜을 요약하면 아래와 같다.

1. B → M : $Cert_B \| TS$
2. M → B : $g^{r_M} \| E_{K_1}\{K \| TS \| Cert_M \| tag\}$

Zheng의 1.5-move 프로토콜은 기지국의 비밀키 x_B를 아는 내부 공격자가 이동국의 비밀키 x_M를 알지 않고도 이동국을 가장할 수 있는 심각한 문제점을 가지고 있다. 내부 공격자에 의한 공격은 Xu와 Wang에 의해 제안되었다.[10]

기지국의 비밀키 x_B와 이동국에 의해 계산된 유효한 (c_1, c_2)을 알고 있는 내부자가 있다고 가정하고 (c_1, c_2)를 다음과 같이 정의한다.

$$c_1 = g^{r_M} \bmod p$$
$$c_2 = E_{K_1}\{K \| TS \| Cert_M \| tag\}$$

공격자는 다음과 같은 방법으로 이동국의 비밀키 x_M없이 다른 유효한 (c_1', c_2')를 만들 수 있다.

$$K_1 = c_1^{x_B} \bmod p$$
$$Cert_M = D_{K_1}\{c_2\}$$
$$c_1' = g^{x'} \bmod p$$
$$K_1' = (c_1')^{x_M} \bmod p$$
$$c_2' = E_{K_1'}\{K' \| TS' \| Cert_M \| tag'\}$$
$$tag' = hash(K' \| TS' \| Cert_M \| (P_M \cdot c_1')^{x_B} \bmod p)$$

또한 1.5-move 프로토콜은 부인봉쇄(non repudiation)를 제공하지 않고 PACS 프로토콜과 마찬가지로 키 교환 프로토콜이 아니라 키 분배 프로토콜이다.

3.4 Signcryption을 이용한 LM 프로토콜

LM 프로토콜[11]은 Zheng이 제안한 signcryption[12]을 사용하여 연산량을 줄인 효율적인 AKA (authentication and key agreement)프로토콜로 2절에서 설명한 보안 요구조건들을 대부분 만족시킨다. 이동통신에서 서명자의 익명성을 제공하기 위해 signcryption을 수정하였다. 주요 아이디어는 두 통신 개체가 초기에 전송측의 정보 데이타를 보호하는 암호화 키를 설정하고 복호화된 데이타와 수신측의 비밀키를 사용하여 복호화 키를 생성하는 것이다. 수정된 signcryption 기법은 Zheng이 제안한 최초의 singcryption 기법보다는 다소 연산량이 증가하지만 서명자의 익명성을 제공하고 기존의 암호 시스템과 서명기법을 따로 사용하는 것보다는 연산량이 작다.

프로토콜의 흐름을 개략적으로 요약하면 아래와 같다.

1. B → M : $r_B \| Cert_B \| RT$
2. M → B : $T \| RT \| c$

여기서 $T = g^{r_M} \bmod p$, $r = KH_T(m)$,
$s = r_M/(r + x_M) \bmod q$,
$c = E_{K_{tm}}\{m \| r \| s\}$이다.

Ⅳ. 제안한 인증 및 키교환 프로토콜

4.1 Rabin 기반 암호 기법

공개키 암호 기법은 일방향(one-way) 함수나 트랩도어(trapdoor) 함수에 기반하고 있다. 그러한 구조를 가진 효율적인 것들 중 하나가 Rabin 함수이다.[13] 휴대 장비를 위한 Rabin 기반의 암호시스템은 에서 처음 제안되었다.[2] BCY 프로토콜은 내부적으로 Rabin 함수가 그 자체로서 안전한 암호기법이라는 것을 가정했다. 그러나 Rabin 함수가 암호시스템을 위해 사용되기 위해서는 더 많은 보안 요건을 갖춰야 한다.[14]

암호 기법에서 보안은 단순한 트랩도어 함수 이상의 것을 필요로 한다. 특히, 주어진 암호문으로부터 평문을 얻기가 어려워야 할 뿐 아니라 공격자가 어떠한 메시지에 관한 정보를 일부 알고 있다 할 지라도 암호화된 메시지의 정보를 얻을 수 없다는 것이 보장되어야 한다. 이러한 보안 개념을 *semantic security*라 한다.[14,15] 키 교환에 있어서 이것은 (1)세션키에 관한 어떠한 정보도 주어진 암호문으로부터 얻을 수 없고 (2)공격자가 세션키를 추측할 수 있다 할 지라도 그것을 증명할 수 없다는 것을 의미한다.

또한 암호문을 생성하는 개체가 암호문이 포함하고 있는 내용을 알고 있어야 한다는 것을 보장해야 한다. 즉, 공격자가 어떤 임의의 암호문을 생성하여 복호를 요구하는 것을 방지해야 한다. 이것은 Rabin 기반의 암호 기법이 선택적 암호문 공격에 깨어지기 쉽기 때문에 필요한 요건이다. 선택적 암호문 공격은 Davida에 의해 처음 소개되었고,[16,17] Naor와 Yung에 의해서 증명되었다.[18] 여기서는 Bellare와 Rogaway에 의해 제안되었고,[19] Carrol 등에 의해 도입된 *plaintext awareness*의 개념을 사용하였다.[15] 이것은 공격자가 임의의 메시지를 선택하는 것을 제공하지 않을 뿐 아니라 전체 메시지를 알아야 한다는 것을 필요로 한다.

Rabin 함수 R에 기반한 random oracles와 같이 동작하고, semantic security 개념에서 안전하고 plaintex-taware한 암호를 다음과 같이 가정한다.

$$E(m) = R[(m, F(m)) \oplus G(t),\ t \oplus H\{(m, F(m)) \oplus G(t)\}]$$

여기서 t는 임의의 값이다.

Setup : k, k_0, k_1는 security 파라미터이다. k는 모듈라의 크기, k_0는 메시지에 덧붙여지는 인증서의 크기이고 k_1은 해쉬함수의 출력 크기이다.
N_M는 $k \cdot bit$의 큰 blum integer이다. 즉, $N_M = p_M q_M$이다.
여기서 p_M, $q_M = 3 \bmod 4$이고 $|p_M| = |q_M| = k/2$이다.
$F : \{0, 1\}^* \rightarrow \{0, 1\}^{k_0}$,
$G : \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k-k_0}$,
$H : \{0, 1\}^{k-k_1} \rightarrow \{0, 1\}^{k}$은 "random oracles"처럼 행동하는 해쉬함수이다.

4.2 Rabin 기반 서명 기법

사용된 서명 기법 또한 Rabin 함수에 기반한 것이다. 서명 기법은 공격자가 임의의 메시지의 서명을 요청하는 것이 허용된다 할지라도 어떤 메시지의 서명을 생성하는 것이 실행 불가능하다는 것이 보장되어야 한다. 이 논문에서는[15,20]에서 사용한 프로토콜을 적용한다. 이것은 "random oracle model"아래서 선택적 메시지 공격에 안전하다는 것이 증명되어 있다.[21]

Setup : k, k_1을 security 파라미터이다. k는 모듈라의 크기이고 k_1은 해쉬함수의 출력 크기이다.
$H : \{0, 1\}^* \rightarrow \{0, 1\}^{k_1}$,
$G_1 : \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k_1}$,
$G_2 : \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k-2 \cdot k_1}$는 "random oracles"처럼 행동하는 해쉬함수이다.

4.3 제안하는 프로토콜

제안한 프로토콜을 살펴보면 3단계로 나뉘어진다.

(1) 초기화 단계(initialization stage)
(2) 사전계산 단계(precomputation stage)
(3) 실 시행 단계(real-execution stage)

휴대폰 또는 휴대용 단말기 구입시 이루어지는 초기화 단계에서 이동국은 비밀키 p_M, q_M를 생성하고 공개키 N_M를 계산한다. 계산된 N_M를 AC(Authentication Center)로 전송을 하면, AC는 이동국에 대한 인증서 $Cert_M$를 생성하여 이동국에게 전송한다.

이동국은 전송된 인증서를 저장하게 된다. 이때 저장하는 매체는 휴대폰 단말기나 스마트카드와 같은 장치를 사용한다.

다음으로 사전계산 단계이다. 오프라인 상에서 이루어지는 단계로 온라인으로 접속시에 연산 부하량과 시간을 단축시킬 수 있다.

이동국은 휴대용 단말기를 사용하지 않을 때 즉, 무선 네트워크를 사용하지 않거나 음성 통화를 하지 않는 빈 시간(idle time)에 임의의 수 r_M, t를 선택하고 x를 계산한다.

■ **암호문 생성 :**

· $r_M \in_R \{0, 1\}^{k-k_0-k_1}$
· $t \in_R \{0, 1\}^{k_1}$
· $x=((r_M, F(r_M)) \oplus G(t),$
$t \oplus H((r_M, F(r_M)) \oplus G(t)))$

계산된 r_M, t, x를 이동국의 메모리에 저장한다.

마지막 단계인 실 시행 단계는 실제로 온라인으로 접속하여 세션키를 설정하는 단계이다.

이동 네트워크는 동기화 매개변수, 가능한 서비스, 시간, 기지국 ID 등 다양한 형태의 제어 정보를 기지국으로부터 이동국에게 연속적으로 전파하기 위해 broadcast channel을 사용한다. 이러한 broadcast channel의 한 부분을 사용하여 기지국이 임의의 수 r_B와 인증서 $Cert_B$를 이동국에게 전파한다.

동기화 데이터, 서비스 형태, 시간, 기지국의 공개키, 인증서 등과 같은 다양한 제어정보를 계속 유지하기 위해 이동국은 broadcast channel을 계속 모니터링 해야 한다.

이동국이 네트워크에 서비스 요청을 하게 될 때 사전계산 단계에서 저장한 x, r_M을 이용하여 y, K를 계산하고 RT, 인증서와 서명값을 K로 암호화 해서 y와 함께 기지국으로 전송한다.

$y=x^2 (\bmod N_B)$
$K=h(r_M \| r_B)$
$E_K\{RT, Cert_M, Sig_M[h(K \| ID_M \| ID_B \| r_B)]\}$

■ **서명 생성 :**

· 임의의 수 $i \in_R \{0, 1\}^{k_1}$을 선택하고 s, v를 계산한다.
$s=H(h(K \| ID_M \| ID_B \| r_B), i),$
$v=(s, G_1(s) \oplus i, G_2(s) \oplus$
$[h(K \| ID_M \| ID_B \| r_B)]_{[1, k-2 \cdot k_1]})$
v가 quadratic residue modulo N_M가 될 때까지 반복한다.
· $v (\bmod N_M)$의 4개의 square root 값($u^2 \equiv v (\bmod N_M)$) 중 하나를 임의로 선택한다.
$h(K \| ID_M \| ID_B \| r_B)$의 서명값이 u이다.

기지국은 y와 암호문을 받은 시간(T')을 기록하고, y를 다음과 같은 방법으로 복호화한다.

〔표 2〕 제안한 프로토콜

이동국		기지국
	r_B, RT, $Cert_B$ ◀	
· compute $y=x^2 (\bmod N_B)$ $K=h(r_M \| r_B)$	y, $E_K\{RT, Cert_M, Sig_M[h(K \| ID_M \| ID_B \| r_B)]\}$ ▶	· compute $\sqrt{y} (\bmod p_B q_B)$ · compute $K=h(r_M \| r_B)$

〔표 3〕 프로토콜의 비교

보안 특성	제안한 프로토콜		개선된 BCY		PACS		1.5-move		LM	
	M→B	M←B	M→B	M←B	M→B	M←B	M→B	M←B	M→B	M←B
Entity authentication	Y	N	N	N	Y	N	Y	N	Y	N
Certificate exchange	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Key agreement	Y	Y	Y	Y	N	N	N	N	Y	Y
Key authentication	YE	YI	YI	YI	YE	YI	YE	YI	YE	YI
Key freshness	Y	Y	N	N	N	N	N	N	Y	Y
Anonymity	Y	N	Y	N	Y	N	Y	N	Y	N
Non-repudiation	Y	N	N	N	Y	N	N	N	Y	N

■ **Notation** : $[a]_{[m_1, m2]}$는 a의 m_1 *bit*에서 m_2 *bit* 까지 라는 표시이다.

■ **암호문 복호 :**

· y의 4개의 square root값을 계산한다.

$\{x_1, x_2, x_3, x_4\} \equiv y^{1/2} \pmod{N_B}$

· y의 square root중 적어도 하나가 올바르게 복호화되었는지 검증한다.

즉, 각 x_i에 대해서

- $a_i = [x_i]_{[1, k-k_1]}$, $b_i = [x_i]_{[k-k_1+1, k]}$
- $t_i = b_i \oplus H(a_i)$, $r_i^* = a_i \oplus G(t_i)$
- 만약 $r_i^* = (r_i, F(r_i))$이라면 암호문 y는 유효한 것이 된다. 이때 암호화된 값은 r_i이다. 만약 어떠한 x_i도 정확히 복호화되지 않는다면 그 때 y는 무효가 되어 프로토콜을 중단하게 된다.

복호화된 r_i와 자신이 보낸 r_B를 사용하여 세션키 K를 계산한다. 계산된 K를 이용하여 암호문을 복호화해서 timestamp(RT)를 다음과 같이 검증한다. 검증이 만족되지 않으면 접근 요청을 거절한다.

$$T - RT \leq \triangle T$$

여기서 $\triangle T$는 채널의 최대 지연시간이다.

복호화된 것으로부터 인증서를 구한다. 인증서에서 이동국의 공개키를 구하여 서명을 검증하게 된다.

이때 서명의 검증이 만족되지 않는다면 접근 요청을 거절하고 검증이 만족된다면 접근요청을 받아들이게 된다.

■ **서명 검증 :**

· $v = u^2 \pmod{N_M}$를 계산한다.

$s = [v]_{[1, k_1]}$, $j = [v]_{[k_1+1, 2 \cdot k_1]}$,

$m = [v]_{[2 \cdot k_1+1, k]}$

즉, s는 v의 첫 k_1비트, j는 다음 k_1비트, m은 나머지 비트이다.

· $i = j \oplus G_1(s)$,

$M = [h(K \| ID_M \| ID_B \| r_B)]_{[1, k-2 \cdot k_2]}$

$= m \oplus G_2(s)$

· $H(M, i) = s$이라면 서명을 받아들이게 된다.

실 시행 단계를 요약하면 〔표 2〕와 같다.

4.4 제안한 프로토콜의 security 특성

4.4.1 Semantic Security

앞에서 설명한 암호 $E(M) = R[M \oplus G(t), t \oplus H\{M \oplus G(t)\}]$를 살펴보자. 위의 것에서 $(m, F(m))$은 M으로 대체되었다. M에 관한 정보가 $G(t)$와 XOR되어 있기 때문에 공격자가 M에 관한 어떤 부분 정보를 얻기 위해서는 $G(t)$에 관한 것을 얻어야 한다. G가 random oracle이기 때문에 $G(t)$를 얻기 위해서는 입력 t 전체를 알아야 한다. 그러나 t를 얻기 위해서는 t가 $H(M \oplus G(t))$와 XOR되어 있으므로 전체 메시지를 알아야 한다. 이것에 대한 증명은[19]를 참고하기 바란다.

4.4.2 Plaintext Awareness

공격자가 메시지의 암호문을 구성하는 것을 가정하면 M은 $(m, F(m))$의 형태로 되어야 한다. 그러나 이것을 임의로 구성하는 것은 어렵다. 그러므로 공격자가 $(m, F(m))$을 모르고서 합법적인 암호문을

구성하는 것은 어렵다.

V. Security 특성과 연산량 분석

5.1 security 특성분석

기존의 인증 프로토콜과 제안한 인증 프로토콜의 security 특성을 2절에서 살펴본 보안 요구조건에 맞추어 분석한다([표 3] 참조).

(1) 개체 인증(entity authentication) : 기지국이 보낸 임의의 수 r_B에 이동국이 서명을 하게 되므로 검증자인 기지국은 이동국을 인증할 수 있다. 반면에 이동국은 기지국을 인증할 수 없다.

(2) 키 인증(key authentication) : 기지국 측으로는 명확한(explicit) 키 인증이 되고 이동국 측으로는 함축적(implicit) 키 인증이 된다. p_M, q_M을 아는 사람만이 K를 서명할 수 있으므로 검증자인 기지국은 세션키 K가 서명자인 이동국으로부터 실제로 계산된 것임을 확신할 수 있다. 또한 기지국의 비밀키 p_B, q_B를 아는 사람만이 이동국이 보낸 r_M을 복호하여 세션키 K를 계산할 수 있으므로 이동국은 함축적 키 인증을 가질 수 있다.

(3) 키 교환(key agreement)과 키 신규성(key freshness): 키는 기지국과 이동국에 의해 선택된 r_B와 r_M에 의해서 계산되어진다.

(4) 익명성(anonymity of mobile user) : 이동국에서 기지국으로 가는 모든 정보가 암호화되어서 전송되므로 익명성이 보장된다.

(5) 부인 봉쇄(non-repudiation) : 이동국에서 기지국으로 가는 정보에 서명을 하므로 이동국은 기지국에 보낸 정보를 부인할 수 없게 된다.

5.2 연산량 분석

앞에서 소개한 기존의 인증 및 키 설정 프로토콜들은 대부분 D-H (Diffie-Hellman) 프로토콜에 기반하여 세션키를 설정하므로 연산량이 많게 된다. 해쉬, 비밀키 암호화, 인증서 검증에 관련된 시간은 무시할 만큼 작기 때문에 연산에 필요한 시간의 대부분은 서명 생성/검증, 공개키 암호/복호와 키 생성을 위한 모듈라 멱승에서 주로 소요된다. 3세대 이동통신 시스템에서는 성능이 좋은 CPU와 메모리를 사용하므로 연산에 소요되는 시간이 줄어들겠지만 휴대용 단말기에서의 연산량이 많으므로 실시간 인증을 필요로 하는 이동 통신 시스템에서는 실현이 어렵게 된다.

본 논문에서 제안한 프로토콜은 모듈라 곱셈이 1번뿐이므로 이동국에서의 연산량이 대폭 감소하게 된다. Rabin 암호시스템과 Rabin 서명기법에 기반한 이 프로토콜은 낮은 연산처리 능력을 가진 휴대용 단말기 등의 사용에 적합하다.

[표 4]는 이동국에서의 각 프로토콜의 연산량을 비교 분석한 것이다.

VI. 결 론

무선 통신 시스템은 고정망에 비교했을 때 다른 특성이 많다. 이동국은 cell로부터 cell로 이동을 하게 되므로 인증 속도가 실시간 통신의 요건을 만족해야 하며 기존 유선 네트워크와는 달리 계산자원이 비대칭적이다. 이동국측은 낮은 연산처리 능력을 가지는데 비해 네트워크측은 큰 규모의 컴퓨터를 사용함으로서 연산 처리 능력이 뛰어나다.

또한 3세대 이동통신 시스템에서는 여러 부가 서비스 사업자들이 많이 생겨 네트워크의 비합법적인 접근이 큰 관심사가 될 것이다.

이 논문에서 제안하는 프로토콜은 Rabin 암호시

[표 4] 각 프로토콜의 연산량 비교

		제안한 프로토콜	개선된 BCY	PACS	1.5-move	LM
이 동 국	서명 생성	[39M]	-	[39M]		
	PK 암호화	1M	1M	[78M]		
	키 생성		[78M]		[78M]	[78M]
	기 타				[39M]	
	합계	[39M]+1M	[78M]+1M	[117M]	[117M]	[78M]

여기서, M : 1024 × 1024, [·] : 오프라인 연산

스템에 기반한 효율적으로 실현 가능한 프로토콜이다. 기존의 MSR+DH 프로토콜이 가지는 보안 특성들을 보완하였으며 복잡한 모듈라 멱승 연산을 Rabin 암호시스템과 오프라인에서의 사전계산(precomputation)을 통하여 감소시킴으로써 휴대폰, 개인 휴대단말기 등과 같은 낮은 연산 처리 능력을 가지는 시스템에 적합하도록 설계되었다. 또한 무선 통신에 있어서 통신 패스수와 연산 부하의 최소화라는 측면에서 효율성을 제공한다.

그러나, 제안한 프로토콜은 대역폭 사용의 효율화라는 측면에서 키 사이즈가 크다는 문제점을 내포하고 있기 때문에 이를 해결하기 위해 향후 발전 과제로 타원곡선(elliptic curve)상으로의 변환에 대한 추가 연구가 필요하다.

참 고 문 헌

[1] G. Horn, K. M. Martin, and C. J. Mitchell, "Authentication Protocols for Mobile Network Environment Value-Added Services", draft, available at http://isg.rhbnc.ac.uk/cjm/Chris_Mitchell.htm.

[2] M. J. Beller, L. F. Chang, and Y. Yaboci, "Privacy and Authentication on a Portable Communications System", *Proceedings of GLOBECOM'91*, pp. 1922~1927, IEEE Press, 1991.

[3] M. J. Beller, L. F. Chang, and Y. Yacobi, "Security for Personal Communication Services: Public-Key vs. Private Key Approaches", *Proceedings of Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'92)*, pp. 26~31, IEEE Press, 1992.

[4] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and Authentication on a Portable Communications Systems", *IEEE Journal on Selected Areas in Communications*, Vol. 11, pp. 821~829, Aug. 1993.

[5] M. J. Beller and Y. Yacobi, "Fully-Fledged two-way Public Key Authentication and Key Agreement for Low-Cost Terminals", Electronics Letters, 29, pp. 999~1001, May 1993.

[6] U. Carlsen, "Optimal Privacy and Authentication on a Portable Communications System", *ACM Operating Systems Review*, Vol. 28(3), pp. 16~23, 1994.

[7] V. Varadharajan, Y. Mu, "On the Design of Security Protocols for Mobile Communications", *Australasian Conference, ACISP '96 Conference*, pp. 134~145, Springer-Verlag, 1996.

[8] JTC, "PACS(Personal Access Communications System) Air Interface Standard," J-STD-014, Jun. 1995.

[9] Y. Zheng, "An Authentication and Security Protocol for Mobile Computing", proceedings of IFIP, pp. 249~257, Sep. 1996.

[10] S. Xu and X. Wang, "Cryptanalysis and two Authentication and Key Distribution Protocols in Portable Communications Systems", *1996 IEEE International Symposium on Information Theory and Its Application*, pp. 347~350, Sep. 1996.

[11] KookHeui Lee and SangJae Moon, "AKA Pro tocols for Mobile Communications", *Australasian Conference. ACISP 2000, LNCS 1841*, pp. 400~411, Brisbane, Australia, Jul. 2000.

[12] Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) << Cost(Signature) + Cost(Encryption)," *Advances in Cryptology, Proceedings of CRYPTO '97*, pp. 165~179, Aug. 1997.

[13] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization", Technical report, Massachusetts Institute of Technology Technical Report MIT/LCS/TR-212, Cambridge, Massachusetts, Jan. 1977.

[14] S. Goldwasser, S. Micali, "Probabilistic encryption", *Journal of Computer and System Sciences*, Vol. 28(2), pp. 270~299, Apr. 1984.

[15] C. Carroll, Y. Frankel, Y. Tsiounis, "Efficient key distribution for slow computing

devices : achieving fast over the air activation for wireless systems. Security and Privacy", *Proceedings of 1998 IEEE Symposium*, pp. 66~76, 1998.

[16] G. I. Davida, "Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem", Tech. Report TR-CS-82-2, University of Wisconsin-Milwaukee, Oct. 1982.

[17] G. I. Davida, "Further results on the chosen signature cryptanalysis of the RSA cryptosystem", Tech. Report, University of Wisconsin-Milwaukee, 1987.

[18] M. Naor, M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attack", *Proceedings of the twenty second annual ACM Symp, Theory of Computing, STOC*, pp. 427~437, May 1990.

[19] M. Bellare, P. Rogaway, "Optimal asymetric encryption -- how to encrypt with RSA", *Advances in Cryptology, Proceedings of Eurocrypt '94*, Springer-Verlag, Perugia, Italy, May 1994. Current version available at http://www-cse.ucsd.edu/ users/ mihir.

[20] M. Bellare, P. Rogaway, "The exact security of digital signatures -- how to sign with RSA and Rabin", In U. Maurer, editor, *Advances in Cryptology, Proc. of Eurocrypt '96*, pp. 399~416, Springer-Verlag, Zaragoza, Spain, May 1996.

[21] S. Goldwasser, S. Micali, R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks", *Siam J. Comput.*, Vol. 17(2), pp. 281~308, Apr. 1988.

〈著者紹介〉

최 영 근 (Yeong-Geun Choe) 학생회원
1994년 2월 : 경북대학교 전자공학과 졸업
1995년 3월~2001년 2월 : 경북대학교 전자공학과 석사 졸업
2001년 3월~현재 : 경북대학교 전자공학과 박사
〈관심분야〉 전자상거래 및 보안기술, 정보보호 응용기술

김 순 자 (Soon-Ja Kim) 종신회원
1975년 2월 : 경북대학교 수학과 졸업
1977년 2월 : 경북대학교 수학과 석사 졸업
1988년 2월 : 계명대학교 수학과 박사 졸업
1993년~현재 : 경북대학교 공과대학 전자공학과 교수
〈관심분야〉 전자상거래 및 보안기술, 정보보호 응용기술, 공학 수학