타원곡선 기반의 이동 통신 환경에서의 인증 및 키 합의 프로토콜

정선영*, 김동휘**, 최영근**, 김순자**

*경북대학교, 정보통신학과, **경북대학교, 전자전기공학부

Authentication and Key Agreement Protocol based on ECC in Mobile Communication

Seon-Yeong Jeong*, Dong-Hwee Kim**, Young-Geun Choe**, Soon-Ja Kim**

*Dept. of Information and Communication, Kyung-pook National Univ.

**Dept. of Electronics Engineering, Kyung-pook National Univ.

요 약

이동 통신의 급격한 발달로 다양한 부가가치서비스가 등장하고, 이러한 서비스를 좀더 편리하고 안전하게 사용하고 싶어하는 사용자와 부가가치서비스를 제공하는 VASP(Value -Added Service Provider) 사이의 보안이 필수적인 것이 되었다. 이를 위하여 이동 통신 환경의 한계인 제한된 자원과 제한된 계산력을 극복할 수 있도록 적은 키 길이를 가지고 보다 안전한 서비스를 제공할 수 있는 타원곡선 암호시스템(ECC)를 기반으로 하여 부가가치서비스에 효율적인 인증 및 키 합의 프로토콜을 제안하고, 차세대 이동통신시스템에 적용해본다.

I. 서론

이동통신기술의 급격한 발달로 단순한 이동통신서비스뿐 만 아니라 모바일 컴퓨팅, 이동 멀티미디어 서비스 등 이동통신 시스템을 이용한 부가가치서비스(Value-Added Services)들의 개발과 제공이 늘어나고 있으며, 사용자와 부가가치서비스를 제공하는 VASP(Value-Added Service Provider)간의 인증과 지불 초기화(API: Authentication and Payment Initialization)과정이 안전한 서비스의 기초가 된다.

이동통신은 그 특성상 무선접속구간에서의 이용자 신분 및 위치 정보의 노출, 송수신되는 데이터의 도청 및 변조, 불법적 서비스 이용 등이 보안문제의 쟁점이 되어왔다 [1, 2]. 최근에 제안된 이동통신환경에서의 서비스와 관련한 인증 및 키 합의 프로토콜들 중 일부는 2세대 무선시스템의 보안을 더욱 강화시키는 방향으로 제안되었고 [3], 많은 부분들이 차세대 무선 시스템의 인증 프로토콜로 제안되었다 [4-6]. 보안 메카니즘에 적용되는 암호 알고리즘의 형태를 보면 대칭키 암호 알고리즘 방식, 공개키 암호 알고리즘 방식과 대칭키와 공개키를 결합한 혼합형 방식 등으로 나뉘어진다. 공개키 암호알고리즘은 대칭키 알고리즘에 비해 강한 보안성과 키 관리의 측면에서 장점이 있지만 계산량이 많고 키 길이가 길어 효율성이 떨어지는 면이 있다.

최근에는 작은 키값으로 안전하고 빠른 연산이 가능한 타원곡선 암호기술의 발달로 무선통신구간에서의 공개키 알고리즘의 적용이 훨씬 용이해졌다 [6].

본 논문에서는 타원곡선 암호기술 기반으로 API 프로토콜의 목표를 만족하는 인증 및 키 합의 프로토콜을 제안하고 차세대 이동통신시스템에 적용해본다.

II. 이동통신에서의 인증 프로토콜

이동 통신 사용자는 통신장소와 이동성에 무관하게 편리하고 안전한 서비스의 제공을 원한다. 보안에서 가장 중요한 부분은 호 설정(call setup) 절차의 초기에 수행하는 인증 및 키 합의 프로토콜을 설계하는 것이다. 이것의 보장이 이후 세션에서의 안전성의 바탕이 된다. 부가가치망에서 API 프로토콜은 사용자가 VASP에 접속함으로부터 시작되며 각 상대방은 인증된 자신의 공개키를 가지고 상대방의 비밀키를 필요로 하게된다. 그러나 통신 상대방은 상호간의 인증과 공유키의 합의, 지불 스킴의 초기화가 필요하다.

1. API 프로토콜의 보안목표

① 무선접속구간에서 세션키 합의 프로토콜 수행 시 상대방을 가장하는 것을 방지하기 위한 상호 개체 인증.

② 모든 공개키 기반 인증 및 키 설정 프로토콜을 지원하기 위해서 사용된 공개키의 정당성에 대한 확인을 위한 공개키 인증서의 상호 교환.

③ 세션키는 두 당사자의 정보 모두를 사용하여 각각 생성하여야 한다는 세션 키의 상호 키 합의.

④ 세션키 생성에 사용되는 두 당사자의 정보가 세션키에 미치는 영향이 동일하여야 하는 세션 키의 키 조절.

⑤ 프로토콜에 참여한 양쪽만이 세션키를 가지고 있을 것이라는 확신을 가지는 상호 묵시적 키 인증.

⑥ 프로토콜 과정에서 양쪽 당사자 모두가 같은 세션키를 공유했다는 확신을 가지는 상호 키 확신.

⑦ 전송정보 재사용에 대한 검사를 위한 상호 키 갱신 보증.

⑧ 무선접속구간에서 사용자 신분의 비밀성.

⑨ 부가가치서비스를 위한 지불 메카니즘의 초기화.

⑩ 중요한 데이터나 사용자의 요금에 관련된 부인할 수 없는 지불 초기화 데이터의 부인봉쇄.

위 목표 중 ①~⑧은 사용자와 네트워크간 인증 프로토콜이 적합하다. ⑨와 ⑩은 네트워크 인증 프로토콜에 약간의 조건을 추가해서 충족시킬 수 있다 [7].

2 타원곡선 암호시스템

먼저 Diffie-Hellman 문제에 안정성을 둔 프로토콜을 타원곡선 상의 프로토콜로 확장하여 프로토콜에 포함되는 양 실체가 공통적으로 사용하는 타원곡선 매개변수와 각 실체의 키 쌍에 대해 간단히 설명한다.

매개변수는 표수(characteristic)가 p인 유한체 F_q상에서 정의된 타원곡선 E와 위수가 n인 기저점 $P \in E(F_q)$로 구성된다. 실체의 개인키는 $[1, n-1]$에서 임의로 선택한 d이고, 공개키는 타원곡선 상의 점 $Q = dP$이며, 키 쌍은 (Q, d)가 된다.

기지점 P에 대하여 aP와 bP가 주어졌을 때 abP를 구하는 것이 타원곡선 상에서 Diffie-Hellman 문제라 할 수 있다.

타원곡선 암호시스템은 기존 공개키 암호시스템과 같은 안전도를 제공하는데 더 작은 길이의 키로도 가능하다. 예를 들어 RSA 1024 비트 키와 ECC 160 비트 키를 갖는 암호시스템이 같은 안전도를 갖는 것으로 알려져 있다. 또한 타원곡선에서의 디하기 연산은 유한체에서의 연산을 포함하므로, H/W와 S/W로 구현하기가 용이하다 [8-10].

3 ASK 프로토콜

이 프로토콜은 Aydos, Sunar, Koc가 1998년에 제안한 ASK 프로토콜로 공개키 교환이 Diffie-Hellman 키 교환 방법으로 이루어진다 [8].

이 프로토콜은 다른 2세대 이동통신시스템에서와 같이 무선접속구간(air interface)의 사용자와 네트워크간 보안서비스만을 고려하였으며, 중간의 유선네트워크 구간은 안전하다고 가정하였다. 먼저 off-line에서 CA (Certification Authority)와 서버, CA와 사용자의 초기화가 이루어지고, 사용자(U)와 서버(S)는 실시간으로 프로토콜이 진행된다.

① S는 자신의 공개키 Q_s를 U로 보낸다.

② U는 Q_u를 S로 보내고, $Q_k = d_u Q_s = (d_u d_s)P$를 계산한다. Q_k의 x축 좌표가 상호 합의된 키이다.

③ S는 $Q_k = d_s Q_u = (d_s d_u)P$를 계산하고 랜덤 수 g를 생성한 후, 랜덤 수 g와 인증서 $(Cert_s)$를 Q_k로 암호화하여 U로 보낸다.

④ U는 인증서 $Cert_u$와 받은 랜덤 수 g를 Q_k로 암호화하여 S로 보낸 후, $k_m = Q_k \cdot x + g$을 계산한다

⑤ S는 $k_m = Q_k \cdot x + g$를 계산한다.
$Q_k \cdot x$는 Q_k의 x축 좌표이다.

⑥ k_m은 이후 사용하는 유일한 비밀키이다

이 프로토콜은 제안자의 주장에도 불구하고 다음과 같은 문제점이 있다 [7]. 첫째로 사용자는 서버 즉 VASP에 인증되지만, VASP는 사용자에게 인증되지 않는다. 둘째로 묵시적 키 인증 및 키 확신을 가질수 없고 셋째로 키 갱신을 확인할 수 없다. 넷째로 이 프로토콜에 서명이 사용되지 않았기 때문에 부인봉쇄 서비스가 제공되지 않고 다섯째 사용자의 익명성이 지켜지지 않는다.

Ⅲ. 제안하는 프로토콜

앞의 ASK프로토콜과 마찬가지로 기지국을 서비스제공자로, 사용자를 이동통신사용자로 보고 이동통신환경의 전자상거래에 활용하고 있다.

서버(S)의 인증서가 방송채널(broadcast channel)을 통해 전송되고 있다는 가정 하에 서버

와 사용자 사이의 안전한 키 합의 과정을 수행한다. 앞에서와 같이 CA (Certification Authority)와 서버, CA와 사용자의 초기화가 off-line에서 이루어진다. 사용자(U)와 서버(S)는 실시간으로 프로토콜이 진행된다.

1. 초기화 단계

① U는 $d_u \in [2, n-2]$를 선택하여 $Q_u = d_u P$를 계산하여 CA와 초기화 작업을 한다.

② S는 $d_s \in [2, n-2]$를 선택하여 $Q_s = d_s P$를 계산하여 CA와 초기화 작업을 한다.

2 실행 단계

초기화가 된 상태에서 이동통신 사용자는 서비스 제공자로부터 이동통신을 통한 서비스를 제공받고자 할 때, 먼저 서비스제공자에게 서비스 요구를 한다. 그 뒤에 그림 1과 같이 프로토콜이 이루어지게 된다.

1) 1단계

사용자는 서버로부터 방송되는 인증서로부터 공개키 Q_s를 추출해 $Q_k = d_u Q_s = (d_u d_s)P$ 계산한다. Q_k의 x축의 좌표가 임시 합의 키이다. 그 다음 사용자는 랜덤 수 r_u를 생성하고 인증서 $(Cert_u)$와 r_u를 Q_k로 암호화한 다음 사용자의 공개키 Q_u와 함께 서버로 보낸다.

2) 2단계

서버는 $Q_k = d_s Q_u = (d_s d_u)P$를 계산한다. 그 다음 서버는 랜덤 수 r_s를 생성한 후 $K = H(r_u, r_s)$를 계산하고, K와 서버의 ID ID_s를 해쉬한 후 r_s화 함 께 Q_k로 암호화하여 사용자에게 보낸다.

3) 3단계

사용자는 $K = H(r_u, r_s)$를 계산한다. 그 다음 랜덤수 r_s와 r_u 그리고 ID_u에 서명한 후 K로 암호화하여 서버로 보낸다

3. 확인 단계

서버는 사용자로부터 받은 메시지인 C_2 $(E_K\{Sig_u(r_s, r_u, ID_u)\})$를 전 단계에서 계산한 K를 이용해서 복호화 한다. 이로인해 얻어지는 $Sig_u(r_u, r_s, ID_u)$를 사용하여 사용자를 인증하고, $Sig_u(r_u, r_s, ID_u)$의 유효성을 확인한다.

Ⅳ. 보안특성 및 적용

1. 보안 특성 및 안전성 분석

제안된 프로토콜은 작은 키 길이에도 보안성이 뛰어난 ECC방식을 Diffic -Hellman 문제에 안전성을 둔 프로토콜에 적용시켰으며, 랜덤하게 선택한 랜덤 수를 이용하는 도전-응답(challenge-response)방식을 이용한 Diffic-Hellman 기반의 키 교환 프로토콜이다.

1) 상호 개체 인증

사용자가 서버에 보내는 첫 번째 메시지에서 서버는 Q_u를 이용하여 Q_k를 계산해 내고 이를 이용하여 C_0를 복호화하여 $(Cert_u)$와 r_u를 찾아내고 이것을 통해 사용자의 신분을 확인한다. 서버가 보내는 C_1을 받은 사용자는 Q_k로 복호화하여 $H(K, ID_s)$와 r_s를 찾아내고 이것을 통해 서버의 신분을 확인한다. 이로써 이동통신 사용자와 서비스를 제공하는 서버간의 신원 확인이 가능하다

2) 갱신키 확인

사용자와 서버는 공유키 K를 갖는다. 이 값은 사용자가 임의로 선택한 r_u와 서버가 선택한 r_s를 이용하여 얻어진다. 세션마다 임으로 선택하기 때문에 공유키가 다름을 알 수 있다.

3) 전송된 정보의 부인 봉쇄

사용자가 서버가 보내준 C_1을 복호화하여

Mobile User		Server
$Q_k = d_u Q_s = (d_u d_s)P$ 랜덤 수 r_u 생성 $C_0 = E_{Q_k}\{r_u, Cert_u\}$	Q_u, C_0 →	$Q_k = d_s Q_u = (d_s d_u)P$
$K = H(r_u, r_s)$	← C_1	랜덤 수 r_s생성 $K = H(r_u, r_s)$ $C_1 = E_{Q_k}\{r_s, H(k, ID_s)\}$
$C_2 = E_K\{Sig_u(r_s, r_u, ID_u)\}$	C_2 →	

그림 1: 제안한 프로토콜.

$H(K, ID_s)$와 r_s를 알고 난 후 r_s, r_u 그리고 ID_u에서명하여 서버에 보내줌으로써 부인봉쇄가 이루어 진다.

4) 함축적 키 인증성과 명시적 키 인증성

서버와 사용자 각각의 비밀키를 알고 있는 사람만이 임시 키 Q_k를 생성할 수 있으므로 서로에게 함축적 키인증성을 가진다. 마지막단계에서 사용자는 새롭게 생성된 세션키 K로 암호화한 메시지를 전달하므로 서버는 사용자가 생성한 공유키를 확인할 수 있다. 따라서 서버는 서버는 사용자에 대한 명시적 키 인증성을 가지게 되지만 사용자는 서버에 대해 명시적 키 인증성을 갖지 않는다.

5) 사용자의 익명성 보장

첫 번째 메시지에서 보내지는 사용자의 공개키 Q_u는 CA와 사용자사이의 초기화단계에서 일회용 키 쌍 즉 (d_u, Q_u)을 사용함으로써 익명성을 보장할 수 있다.

6) 전향적 보안성

사용자와 서버의 비밀키를 모두 알더라도 각 세션 마다 새롭게 생성된 랜덤 수를 사용하기 때문에 이전에 공유된 공유키는 알 수 없다

2. 차세대 이동시스템에 적용한 프로토콜

2세대 이동통신시스템에서는 중간 유선구간은 안전하다고 가정하고 설계 시 유선구간의 네트워크 실체들을 부분적으로 고려했으며 유선네트워크영역에서 이용자 데이터와 신호데이터는 암호화되지 않는 평문형태로 전송되었다. 차세대 이동통신시스템에서 이용자 데이터의 기밀성을 보장하는 안전한 통신을 위해서는 무선접속구간 뿐만 아니라 두 단말이용자간(end-to end) 데이터가 안전하게 전송될 수 있는 보안 메카니즘과 프로토콜 구성이 필요하다 [11, 12].

여기에서는 프로토콜의 실체를 사용자, 네트워크, 그리고 제3의 신뢰기관(TTP:Trusted Third Party) 세 가지로 한정한다. TTP는 상호 인증이 필요한 실체들에 대한 공개키 인증서 발급 및 검증에 관여하지만 이동통신시스템의 보안 프로토콜에는 직접 참여하지 않는다.

이동 통신 사용자가 홈 네트워크에 있는 경우와 방문 네트워크에 있는 경우가 있을 수 있는데, 예에서는 이동 통신 사용자가 홈 네트워크에 있는 경우를 가정한다.

다음은 프로토콜에 새로이 사용되는 기호들이다.

- MS:이동통신시스템 사용자
- VN, HN: 방문네트워크, 홈네트워크
- UID, NID:사용자와 네트워크의 고유신분
- TID:사용자의 초기 임시신분
- TID′:프로토콜 수행후 새로 생성된 임시신분
- d_A, Q_A:A의 공개키 인증서의 개인키, 공개키
- $Cert_A$:A의 공개키 인증서
- K_{AB}:실체 A와 실체 B간에 합의된 세션키

1) 1단계

이동통신사용자(MS)는 홈네트워크(HN)에서 방송되는 공개키 Q_H를 수신하여 $Q_K = d_M Q_H = (d_M d_H)P$를 계산한다. 그 다음 사용자(MS)는 랜덤 수 r_M을 생성한 후 인증서 $(Cert_M)$, r_M, 그리고 TID를 Q_K로 암호화 한 다음 MS의 공개키 Q_M와 함께 HN으로 보낸다.

$$MS \rightarrow HN : \ Q_M, \ Q_K\{Cert_M, \ r_M, \ TID\}$$

2) 2단계

HN은 $Q_K = d_H Q_M = (d_H d_M)P$를 계산한 후 HN은 NID와 TID를 이용하여 데이터베이스를 검색하여 MS가 정당한 가입자인가 확인 후 프로토콜 계속 수행한다. HN은 랜덤 수 r_H를 생성한 다음 $K_{MH} = H(r_M, \ r_H)$와 $TID' = H(UID, Q_K)$를 계산하고, r_H, TID'와 $H(K_{MH}, \ TID', \ NID)$를 Q_K로 암호화하여 MS에게 보낸다.

$$MS \leftarrow HN : \ Q_K\{r_H, \ H(K_{MH}, \ TID', \ NID)\}$$

3) 3단계

MS는 $K_{MH} = H(r_M, \ r_H)$와 TID'를 계산하고 $H(K_{MH}, \ TID', \ NID)$를 확인한 다음 랜덤수 r_H, r_M와 TID'에 서명한 후 K_{MH}로 암호화하여 HN으로 보낸다.

$$MS \rightarrow HN : \ E_{K_{MH}}\{sig_M(r_M, \ r_H, \ TID')\}$$

프로토콜 초기에 임시신분 TID에 의해 네트워크가 이용자를 확인하고, 프로토콜 실행중 UID와 임시 공유키 Q_K를 사용하여 새로운 임시 신분 TID'을 상호 계산하며, 새로운 임시 신분 TID'를 다음 세션의 인증 프로토콜에 이용하여 임시신분의 세션별 갱신을 보증한다. 또한, 이용자의 고유신분 UID이 무선접속구간 프로토콜 메시지 교환과정에서 알 수 없기 때문에 이용자의 익명성을 보장한다.

V. 결론

보편화되고 다양화되고 있는 부가가치서비스를 좀 더 편리하고 안전하게 사용하기 위하여 보안

요건의 강화가 요구되고 있다.

본 논문에서는 이동통신의 특성이 주는 한계점을 극복하기 위하여 적은 키 사이즈로 높은 보안 요건을 충족하는 타원곡선 암호시스템을 기반으로 하는 이동통신에서 부가가치서비스의 안전성을 높일 수 있는 인증 및 키 합의 프로토콜을 제안하였다. 또한 이를 두 단말이용자간 통신이 중요시되는 차세대이동통신환경에 적용시킨 예를 제안하였다.

차후 두 이용자간의 방문네트워크간 안전한 메시지 전달을 위한 네트워크시스템상의 보안에 대한 연구가 필요하며 통신로 상의 범죄와 같은 문제발생 시 합법적 기관에 의한 합법적인 보안해제를 할 수 있는 체제의 형성에 대한 연구가 필요하다 하겠다.

참고문헌

[1] M. J. Beller, L. F. Chang, and Y. Yaboci, "Privacy and Authenticationon a Portable Communications System", Proceedings of GLOBECOM '91, pp. 1922-1927, IEEE Press, 1991.

[2] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and Authenticationon a Portable Communications Systems", IEEE Journal on Selected Areasin Communications, vol.11, pp. 821-829, Au g. 1993.

[3] A. Mehrotra, Golding, L. S, "Mobility and security management in the GSM system and some proposed future improvements", Proceedings of the IEEE , Vol 86 Issue 7, pp. 1480 -1497, July 1998.

[4] Min Xu; Upadhyaya, S, "Secure communication in PCS ", Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd , pp.2193 -2197 Vol.3, 2001.

[5] D. G. Park, C. Boyd and S. J. Moon, "Forward Secrecy and Its Application to Future Mobile Communications Security", PKC 2000, Springer -Verlag, pp. 433-445, 2000.

[6] C. S. Park, "On Certificate-based Security Protocols for Wireless Mobile Communication Systems", IEEE Network Vol. 11 Issue 5, pp. 50-55, Sept.-Oct, 1997.

[7] Horn, G., Martin, K.M.; Mitchell, C.J, "Authenti -cation protocols for mobile network environment value-added services", Vehicular Technology, IEEE Transactions on , Vol. 51 Issue 2 , pp. 383-392, March 2002.

[8] M. Aydos, B. Sunar, and D. K. Koc, "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication", presented at the 2nd Int. Workshop Discrete Algorithms and Methods for Mobility(DIAL M'98), Dallas, TX, Oct, 1998.

[9] 김 덕수, 이 은정, 심 상규, 이 필중, "유한체 GF(p^m)에서 정의된 타원곡선 암호 시스템의 효율적 구현," 한국통신정보보호학회 종합학술발표회 논문집 제8권, pp.455-468, 12월 1998.

[10] 이민섭, "현대암호학", 교우사, pp.361-382, 1999.

[11] C. Boyd and A. Mathuria, "Key Establishment Protocols for Secure Mobile Communications: A Selective Survey", Information Security and Privacy, LNCS 1438, Springer-Verlag, pp.344-355, 1998.

[12] 고재승, 김광조, "차세대 이동통신시스템에 적용되는 보안 프로토콜의 구성 방식 (Constructing security protocols suitable for next generation mobile system)", KIISC 종합학술발표회(CISC2000), 종합 학술발표 논문집, Vol. 10, No. 1, pp.172-186, 성균관대학교, Nov. 25, 2000.