제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

이동 통신에서의 효율적인 인증 프로토콜 구현

강상승*, 최영근**, 김순자**
*한국전자통신연구원 전자거래연구부
**경북대학교 전자전기컴퓨터학부
e-mail:sskang@econos.etri.re.kr

Implementation of an Efficient Authentication Protocol for Mobile Communications

Sang-Seung Kang*, Yeong-Geun Choe**, Soon-Ja Kim**
*Electronic Commerce Department, ETRI
**School of EECS, Kyungpook National University

요 약

이동 통신 환경에서의 서비스 영역이 전자거래 분야로 확대됨에 따라 이동 통신 환경에 적합한 인증 기술의 도입이 필수조건이 되고 있다. 본 논문에서는 이동 통신에서의 보안 요구조건을 만족하고, 제한된 자원과 대역폭 등을 갖는 이동 단말기의 연산량을 줄일 수 있도록 XTR 암호 기법을 적용하고, 통신 패스 수와 연산 부하의 최소화라는 측면에서 효율성을 제공할 수 있는 인증 프로토콜을 제안한다. 제안한 프로토콜은 J2ME를 기반으로 구현하여 플랫폼에 독립적이며 사용이 용이하고 종단간 보안을 제공한다.

1. 서론

최근 이동 통신 가입자의 무선 인터넷 서비스 이용률이 급속히 증가함에 따라 뱅킹, 증권거래, 쇼핑과 같은 비즈니스 응용분야까지 그 서비스 영역이 확장되고 있다. 이러한 비즈니스 응용분야 서비스로 인해 사용자에게는 많은 편의를 제공하지만 비합법적인 접근에 따른 피해의 가능성도 커지게 된다. 따라서 이를 예방하기 위한 인증 기술의 도입이 요구된다.

일반적인 사용자 인증 기술은 사용자 ID와 패스워드에 의해 이루어지는데 이것은 도청, 재전송 공격 등에 매우 취약하므로, 안전하고 효율적인 인증 프로토콜의 설계가 필요하다. 무선 인터넷에서 사용되는 인증 프로토콜의 목적은 통신에 참여하는 개체들을 인증하고 그들 사이에서 주고받을 데이터를 암호화 및 복호화할 세션키를 설정하는데 있다. 이러한 인증 및 키 합의 프로토콜을 구현하고자 할 때 기존 유선 인터넷 환경은 데스크톱 이상의 컴퓨터와 높은 대역폭을 제공할 수 있는 네트워크를 기반으로 하지만, 이동 통신 환경에서는 현재의 데스크톱 기준으로 접근하기에는 전력 소모량, 메모리 크기, 디스플레이 크기, 전송속도, 안정성 등에서 많은 어려움이 있다. 따라서 제한된 자원과 낮은 연산 처리 능력을 가지는 시스템에서 사용하기 위해서는 특별히 설계된 효율적인 인증 프로토콜이 필요하다.

본 논문에서는 이동 통신 서비스에 적합한 공개키 기반의 인증 프로토콜을 제안한다. 제안한 프로토콜은 이동 통신 환경에서의 보안 요구 조건 및 제한점을 고려하여 이동 단말기의 연산량을 줄일 수 있도록 XTR 암호 기법을 적용하고 통신 패스 수와 연산 부하의 최소화라는 측면에서 효율성을 제공하도록 설계하였다. 또한 프로토콜의 구현에 있어서 J2ME를 사용함으로써 이기종인 이동 단말기들에 대하여 독립적이며 사용이 용이하도록 하고 여러 무선 인터넷 표준들의 보안상 약점을 극복할 수 있도록 하였다. 즉 응용계층에서 WPKI 구조를 사용하여 단말기에서 서버까지 하나의 암호화된 정보가 복호 과정과 변환 과정 없이 전달되므로 종단간 보안 문제를 해결하였다. 이는 기존 PKI와도 호환이 되며, 인터넷 전자상거래 보안의 필수 요소인 기밀성, 무결

성, 인증, 부인 방지, 접근 제어 등을 제공한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 이동 통신 환경에 따른 요구조건과 고려사항을 기술하고, 3장에서는 효율적인 인증 프로토콜을 제안하며, 4장에서는 제안한 프로토콜을 구현하고 성능을 분석한다. 마지막으로 5장에서는 결론을 맺는다.

2. 요구 분석

이동 통신 사용자에게 보다 편리하고 안전하게 서비스를 제공하기 위해 이동 통신에서의 인증 프로토콜의 보안 요구조건을 기술하고, 환경적 제약사항을 극복하고 효율성 확보를 위한 방안을 분석한다.

유럽의 차세대 이동통신 표준인 UMTS의 보안 서비스 제공을 위해 ASPeCT 프로젝트에서 연구된 인증 및 키 합의 프로토콜에 관한 보안 요구조건등은 1) 상호 개체 인증, 2) 공개키 인증서의 상호교환, 3) 세션 키에 대한 상호 동의, 4) 세션 키에 대한 상호 제어, 5) 키 인증, 6) 키의 신규성에 대한 상호 확인, 7) 사용자 신분의 기밀성, 8) 부인 봉쇄 등과 같다. 이러한 보안 조건들을 만족시키면서 트랜잭션의 효율성을 실현하도록 설계가 필요하다.

한편 이동 통신망은 고정망에 비해 전송 속도, 디스플레이 크기, 인터페이스, 통신 에러율, 접근 형태, 메모리 크기, 계산 능력, 전력 소모량, 제한된 대역폭 등의 면에서 제약 사항이 많다. 사용자는 셀에서 셀로 이동을 하게 되므로 인증 속도가 실시간 통신의 요건을 만족해야 하며 기존 유선망과는 달리 계산 자원이 비대칭이다. 즉 사용자 측은 낮은 연산처리 능력을 가지는데 비해 서버 측은 큰 규모의 컴퓨터를 사용함으로써 연산 처리 능력이 뛰어나다. 이와 같은 이동 통신 환경의 제약사항으로 인해, 1) 통신 패스의 최소화, 2) 대역폭 사용의 효율화, 3) 연산 부하의 최소화를 고려해야 한다. 즉 교환되는 트랜잭션 수를 가능한 줄이고, 프로토콜 메시지를 가능한 짧게 유지하며, 사전 계산 단계를 두어 온라인 계산의 연산 부하를 줄이고 오프라인 동안 사전 계산을 수행하여 사용자측의 연산량이 가능한 작도록 설계해야 한다.

또한 제한된 자원을 사용하는 이동 단말기의 효율성 향상을 위해 키 길이를 줄일 수 있는 새로운 암호 시스템의 도입이 필요하다. 이에 각광받고 있는 것이 타원 곡선 암호시스템인데, 이는 기존의 다른 공개키 스킴과 동일한 안전도를 제공하는 데에 더 작은 키 길이를 가지고 가능하며 구현이 용이하다는 장점을 가진다. 그러나 여전히 키 생성에 많이 시간이 소요되는 단점이 있는데, 이를 해결하기 위해 더 빠른 암호 시스템에 대한 연구가 이루어지고 있다. 그 예로 격자 줄임에 기반을 둔 NTRU와 유한체 승법군의 부분군을 사용하는 XTR 등을 들 수 있다. XTR의 보안성은 p^2-p+1을 나누는 위수의 $GF(p^6)^*$의 부분군에서 이산 대수 문제에 기반하는데, 암호학적 프로토콜에서 XTR의 응용은 보안성을 손상시키지 않으면서 통신 및 연산 오버헤드에서 실질적인 절약을 가져온다. 따라서 기존에 사용되던 암호 프로토콜을 XTR을 이용해서 이동 통신 환경에 적용할 수가 있다.

3. 프로토콜 설계

인터넷 전자상거래에서는 본인을 입증하는 인증서와 거래부인을 방지하는 전자서명, 그리고 타인으로부터의 통신보호를 위한 암호화가 필요하다. 이는 이동 통신 환경에서 무선 인터넷을 기반으로 전자거래 시에도 동일하게 지원되어야 한다. 즉 사용자는 인증기관으로부터 자신의 인증서를 받게 되고, 인증서를 획득한 사용자는 자신의 인증을 통해 서비스 제공자가 제공하는 서비스를 받을 수 있게 된다.

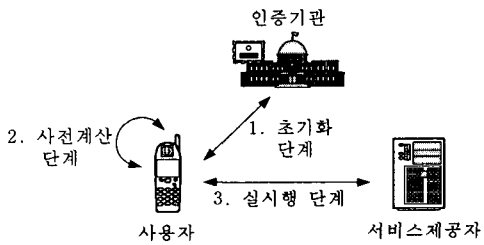

그림 1. 전체 시스템 구성도

전체 인증 프로토콜은 그림 1과 같이, 초기화 단계, 사전 계산 단계, 실시행 단계로 구성된다. 초기화 단계에서는 사용자와 인증기관 사이에 공개키와 인증서를 교환하고, 사전 계산 단계에서는 실시행 단계에서의 연산량을 줄이기 위해서 이동 단말기가 사용되지 않는 시간을 이용하여 필요한 값들을 계산한다. 실시행 단계에서는 사용자와 서비스 제공자 사이의 구체적인 인증 프로토콜이 실행된다.

먼저, 초기화 단계는 사용자 단말기와 인증기관의 통신을 통해 사용자가 인증서를 획득하는 과정이다. 즉 사용자 단말기에서 공개키와 비밀키를 생성

하여 사용자의 공개키와 인증서 신청 정보를 인증기관으로 전송하면, 인증기관은 사용자로부터 받은 공개키와 인증서 신청 정보로부터 사용자의 인증서를 생성하여 사용자 단말기로 전송한다.

사전 계산 단계는 실시행 단계의 연산 부하를 줄이기 위해 이동 단말기가 사용되지 않을 때 필요한 값들을 계산하는 과정이다.

실시행 단계는 사용자 단말기와 서비스 제공자 서버 간의 구체적인 인증 및 키 합의 프로토콜이 실행되는 과정이다. 세부적인 프로토콜 수행 절차는 그림 2와 같다.

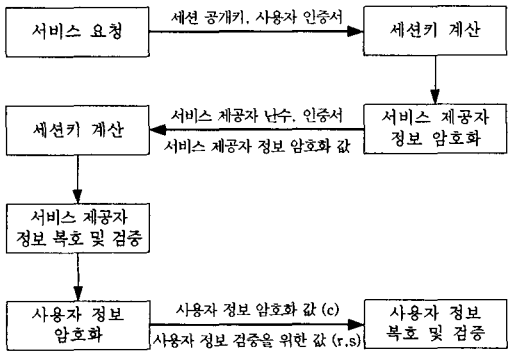

그림 2. 실시행 단계의 프로토콜 흐름도

서비스 요청 과정에서, 사용자 단말기는 인증서와 사전 계산 단계에서 계산된 난수(r_U)로부터 세션 공개키($y=g^{r_U}$)를 계산하여 서비스 사용에 대한 요청 메시지로 서비스 제공자 서버로 전송한다.

서비스 제공자의 세션키 계산 과정에서, 수신된 g^{r_U}와 자신이 생성한 난수(r_V)를 이용하여, 사용자와 동일하게 암호화된 정보를 복호화하기 위한 서비스 제공자의 세션키($K_V=h(r_V \| (g^{r_U})^{x_V})$)를 생성한다.

서비스 제공자 정보 암호화 과정에서, 서비스 제공자는 생성된 자신의 세션키를 이용하여 자신의 세션키, ID, 난수로 구성된 서비스 제공자의 정보 ($z=E_{K_V}\{h(K_V \| ID_V \| r_V)\}$)를 암호화하고, 암호화된 정보와 서비스 제공자의 난수, 인증서를 사용자 단말기로 전송한다.

사용자의 세션키 계산 과정에서, 서비스 제공자 서버의 정보로부터 사용자 정보의 암호화에 사용할 세션키($K_U=h(r_V \| (g^{x_V})^{r_U})$)를 생성한다.

서비스 제공자 정보 복호 및 검증 과정에서, 사용자 단말기는 생성한 세션키로 서비스 제공자의 암호화된 정보를 복호화하고, 생성키를 확인한다. ($D_{K_U}\{E_{K_V}\{h(K_V \| ID_V \| r_V)\}\} = h(K_V \| ID_V \| r_V)$ 확인)

사용자 정보 암호화 과정에서, 사용자의 인증을 위한 정보($m=Cert_U \| h(g^{x_V} \| r_V \| K_U \| ID_U \| ID_V)$)를 생성 및 암호화($c=E_K\{m\}$)하고, 검증을 위한 값 (r,s)을 계산한 후, 사용자 인증을 위한 정보에 대한 사용자의 사인크립션 (c,r,s)을 서비스 제공자 서버로 전송한다. 여기서, r값의 계산 과정은 $r=h(y,c)$, s값의 계산 과정은 $s=r_U+x_U \cdot r-r \bmod q$ 이다.

마지막으로 사용자 정보 복호 및 검증 과정에서, 서비스 제공자 서버는 사용자의 올바른 인증을 위해 사용자가 전송한 정보를 분석하고 검증한다. 서비스 제공자 서버는 사용자 단말기로부터 전송된 정보 (c,r,s)가 악의적인 공격자에 의해 위조나 변경이 되었는지를 검증할 필요가 있다. 서비스 제공자 서버는 사용자로부터 수신한 s값과 r값의 검증을 통하여 복호화된 정보 m에 대한 검증을 수행한다. 여기서, s값 검증의 경우는, 먼저 $0 \le s < q$인지 확인하여 s가 범위를 벗어날 경우에 인증이 실패하고, m의 정보 중 사용자의 인증서로부터 g^{x_U}와 ID를 추출하고, $y_V=g^{s+r} \cdot (g^{x_U})^{-r}$의 값이 y값과 같은지를 확인한 후 동일하지 않은 경우에는 인증이 실패한다. r값 검증의 경우는, s값을 검증할 때 계산한 y_V와 c를 해시한 값($h(y_V,c)$)과 r값과 비교하여 동일하지 않은 경우에는 인증이 실패한다.

4. 구현 및 성능 분석

제안한 프로토콜은 자바를 기반으로 구현하였다. 사용자 즉 서비스 요청자는 J2ME MIDP를, 서비스 제공자는 JDK와 Apache Tomcat 자바 서블릿 컨테이너를 이용하였다.

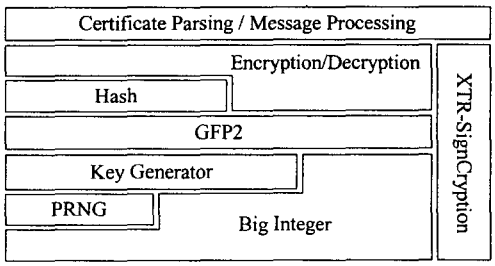

그림 3. 구현 모듈 구성도

본 논문에서 구현된 모듈은 프로토콜의 기본적인 설정 기능을 수행하는 하위 레벨의 모듈과 프로토콜의 핵심 기능을 수행하는 XTR-SignCryption 모듈과 서명된 데이터의 전송에 필요한 상위 레벨의 모듈로 구성된다. 구현 모듈의 구성도는 그림 3과 같다.

인증 프로토콜의 실시행 단계에서 사용자와 서비스 제공자간의 메시지 처리를 담당하는 모듈에서는 통신 프로토콜이 필요하다. J2SE에서는 java.net 패키지의 소켓을 이용하여 TCP 네트워크를 구현하지만, 이는 충분한 자원을 가진 일반 컴퓨터를 기준으로 설계된 것이기 때문에 제한된 환경을 가진 무선 이동 장치에서 사용하기에는 부적절하다. 따라서 J2ME는 다양한 네트워크 환경과 장치들을 지원하는 유연성을 만족시키기 위해 MIDP에서 필수적으로 HttpConnection을 지원하는데, 이를 이용하여 구현함으로써 네트워크에 독립적이며 애플리케이션 이식성이 높고 데이터의 전환이나 처리가 용이하다.

구현한 모듈 검증을 위해서는 GUI 환경을 제공하는 J2ME Wireless Toolkit을 사용하였다. 이는 컴파일, 사전검증, manifest 파일과 애플리케이션 디스크립터 파일 생성, JAR 파일 생성이 한번에 실행된다. 검증 단계 이후, 프로토콜 실시행 단계에서 사용되는 연산 모듈 및 전체 프로토콜에 대해 성능 측정을 수행하였는데, 프로그램의 반복 실행 횟수와 입력 값의 길이 변화를 통한 프로토콜 수행 시간 평가에 중점을 두었다.

제안한 프로토콜에서 사용한 공개키 암호 시스템인 XTR은 RSA의 1/6 키 크기로 RSA와 비슷한 보안성을 제공한다. 따라서 RSA의 64, 128, 256, 512, 1024bit의 키 크기에 해당하는 XTR의 10, 20, 40, 80, 170bit 키 값을 입력으로 주고 키 길이 변화에 따른 전체 프로토콜의 수행시간을 측정하였다. 프로토콜의 수행시간은 사용자가 요청 메시지를 서비스 제공자 서버로 보내는 것부터 최종적으로 서버로부터 인증 성공 혹은 실패 메시지를 받는 것까지 측정하였으며, 시험 시스템(366MHz CPU, 256MB RAM)에서의 측정 결과는 표1과 같다.

표 1. 전체 프로토콜 수행시간

키 길이(bit)	10	20	40	80	170
수행시간(ms)	166	417	833	1250	1676

가장 널리 사용되는 공개키 암호 시스템인 RSA의 1024bit 키 길이와 동일한 보안강도를 갖는 XTR의 170bit 키 길이를 가지고 테스트한 결과, 전체 프로토콜이 실행되는데 약 1.6초 정도의 시간이 소요되었다.

5. 결론

이동 통신 환경은 제한된 자원과 대역폭, 낮은 연산 처리 능력 등으로 인한 제약사항이 따른다. 따라서 짧은 키 길이, 빠른 키 생성, 적은 양의 메모리를 사용하면서도 강한 보안성이 보장되어야 한다.

본 논문에서는 이동 통신 환경에서의 보안 요구조건 및 제한점을 고려하여 이동 단말기의 효율성을 높일 수 있는 인증 프로토콜을 제안하였다. 제안한 프로토콜은 키 길이를 줄이고 보다 빠른 키 생성을 위해 XTR 암호 기법을 적용하였고 통신 패스 수와 연산 부하의 최소화라는 측면에서 효율성을 제공한다. 또한 J2ME를 기반으로 구현함으로써 이기종인 이동 단말기에 대하여 독립적이며 사용이 용이하고 응용계층에서 WPKI 구조를 사용하여 종단간 보안 문제를 해결하였다.

참고문헌

[1] A. Mehrotra and L. S. Golding, "Mobility and Security Management in the GSM System and some Proposed Future Improvements," *Proceedings of the IEEE*, Vol.86, pp. 1480-1497, July 1998.

[2] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," *ESORICS'98*, pp. 277-293, 1998.

[3] J. Hoffstein, J. Pipher, J. Silverman, "NTRU: A Ring Based Public Key Cryptosystem," *ANTS III*, June 1998.

[4] A. Lenstra, E. Verheul, "The XTR public key system," *CRYPTO 2000*, pp. 1-19, 2000.

[5] J2ME, http://java.sun.com/j2me/

[6] Apache Tomcat, http://jakarta.apache.org/tomcat/

[7] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.