M-Commerce 사용자를 위한 효율적인 패스워드 기반 인증 및 키교환 프로토콜

(An Efficient Password-based Authentication and Key Exchange Protocol for M-Commerce Users)

박 수 진 † 서 승 현 †† 이 상 호 †††
(Soo-Jin Park) (Seung-Hyun Seo) (Sang-Ho Lee)

요 약 M-Commerce 사용자가 다양한 서비스를 안전하게 제공받으려면 통신하려는 상대방을 인증해야 하고, 통신하는 개체들 사이에 설정한 세션키를 사용하여 통신 메시지를 암호화하여야 한다. 하지만 M-Commerce 환경은 유선통신 환경에 비해 제약점이 있으므로 이를 고려한 효율적인 인증 및 키교환 프로토콜의 제안이 요구된다. 본 논문에서는 타원곡선 암호시스템을 사용한 효율적인 인증 및 키교환 프로토콜을 제안한다. 제안하는 프로토콜은 무선통신 사업자가 계산과정 일부를 대신 수행함으로써 이동통신 사용자의 계산량을 줄였고, 무선통신 구간에서 효율적으로 사용자를 인증할 수 있도록 패스워드 기반 인증방식을 사용하였다. 또한 M-Commerce 호스트에게 사용자의 신원을 직접 드러내지 않음으로써 이동통신 사용자의 익명성을 보장하며, 사용자와 호스트 사이의 통신내용을 무선통신 사업자를 포함한 제 3자가 알지 못하게 함으로써 통신정보의 기밀성을 보장한다.

키워드 : 키 교환 프로토콜, 인증, 타원곡선 암호시스템, 무선통신 환경

Abstract Wireless access always has to include the authentication of communication partners and the encryption of communication data in order to use secure M-Commerce services. However, wireless systems have limitations compared with the wired systems, so we need an efficient authentication and key exchange protocol considering these limitations. In this paper, we propose an efficient authentication and key exchange protocol for M-Commerce users using elliptic curve crypto systems.

The proposed protocol reduces the computational load of mobile users because the wireless service provider accomplishes some parts of computations instead of the mobile user, and it uses the password-based authentication in wireless links. Also, it guarantees the anonymity of the mobile user not to reveal directly the real identity of the user to the M-Commerce host, and preserves the confidentiality of communication data between the M-Commerce host and the user not to know the contents of communication between them to others including the wireless service provider.

Key words : key exchange protocol, authentication, elliptic curve crypto system, mobile environments

1. 서 론

최근 보편화된 무선 단말기의 보급과 이동통신 네트워크의 고속화 등에 힘입어 이동통신 사용자의 수가 빠르게 증가함에 따라, M-Commerce 환경에서 무선 인터넷 서비스 제공업자들은 이동통신 사용자들의 요구를 충족시키기 위해서 다양한 서비스를 제공하려고 노력하고 있다. M-Commerce란 휴대폰이나 PDA 등의 이동통신 단말기의 무선 네트워킹으로 이루어지는 모든 비즈니스를 말하며 게임, 전자쿠폰, 모바일 광고, 온라인 예약 등이 이에 속한다. 이와 같은 M-Commerce 서비스들은 사용자들에게 이동성을 보장하고 시·공간의 제약을 받지 않고 필요한 정보를 얻을 수 있게 하며, 좀더 개인화된 맞춤 서비스를 가능하게 한다는 점에서 이동통신 사용자들에게 각광받고 있다. 그러나 무선통신 환경에서 제공되는 서비스들은 유선통신 환경에 비해 저

† 비 회 원 : 삼성SDS
moviefree@empal.com
†† 비 회 원 : 이화여자대학교 컴퓨터학과
seosh@ewhain.net
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
shlee@ewha.ac.kr
논문접수 : 2004년 4월 9일
심사완료 : 2004년 11월 30일

속의 서비스를 제공하고 어플리케이션이 빈약하며 불안정한 통신품질을 가지기 때문에 실시간 공격 또는 도청으로 인한 평문의 노출, 다양한 사용자의 인증방식 부족 등 보안상 많은 문제점들이 발생한다[1].

무선통신 환경에서 이와 같은 보안 문제점들을 해결하고 안전한 통신을 보장하려면 통신하는 개체들이 주고받는 메시지가 암호화되어 전송되어야 하고, 이를 위해서 통신하는 두 개체들 간의 세션키 설정이 필요하다. 그러나 이동통신 단말기들은 좁은 화면과 적은 메모리, 낮은 처리속도 등의 제약점을 가지고 있으므로 유선 환경에서 제공되는 암호시스템이나 키교환 프로토콜을 그대로 적용하는 것은 오버헤드가 크고 계산시간도 오래 걸려서 이동통신 사용자의 요구에 적합하지 못하다. 그러므로 M-Commerce 환경에 적합하도록 이동통신 단말기의 한계점들을 고려한 효율적이고 안전한 키교환 프로토콜이 필요하다.

본 논문에서는 타원곡선 암호시스템을 사용한 인증 및 키교환 프로토콜을 제안한다. 타원곡선 암호시스템은 다른 암호시스템에 비해 짧은 키 길이로 동일한 보안강도를 제공하므로 제한된 자원을 가지는 무선통신 환경에 효율적으로 이용될 수 있다[2,3]. 제안하는 프로토콜은 무선통신 구간의 인증방식으로 사용자와 무선통신 사업자 사이에 미리 공유된 패스워드를 사용한다. 인증방식은 기반 기술요소에 따라 생체인증, 스마트카드, 인증서, ID카드 등의 다양한 형태가 있으나, 무선 통신 환경에서는 무선 PKI기반의 인증서를 이용하여 상대방의 공개키 정보를 확인함으로써 상대방을 인증하는 방식과 무선통신 사업자사이에 공유한 패스워드를 이용하여 인증하는 방식이 많이 사용되고 있다[1,4-6]. 그러나 무선 PKI 기반의 인증서를 사용할 경우, 적은 메모리를 갖는 이동통신 단말기에 사용자의 인증서를 발급 받아 저장해야하고, 무선통신 사업자와 통신을 하여 인증을 받고자 할 때, 인증서를 전송해야 하는 부담이 있다. 반면 패스워드를 이용한 인증방식은 무선통신 사업자와 통신하고자 할 때, 사용자가 기억하기 쉬운 패스워드를 이용하여 인증을 수행하기 때문에, 인증서를 저장하거나 전송해야 하는 부담없이 편리하게 사용할 수 있어 무선통신 환경에 더 적합하다.

또한, 본 프로토콜에서는 무선통신 사업자가 사용자의 계산과정 일부분을 대신 수행하게 함으로써 사용자의 계산량을 줄이고 효율성을 높였으며, 무선통신 사업자가 M-Commerce 호스트와 이동통신 사용자 사이에 설정된 세션키를 계산할 수 없게 함으로써 통신내용의 기밀성을 제 3자로부터 보장하였다. 더불어 M-Commerce 호스트가 한번의 통신 이후에 해당 사용자의 신분정보를 악용하는 일을 방지하기 위해, 무선통신 사업자를 통한 사용자 인증으로 M-Commerce 호스트에게 이동통신 사용자를 인증함으로써 사용자의 익명성을 보장하였다.

본 논문의 구성은 다음과 같다. 2장에서 인증 및 키교환 프로토콜의 요구사항과 안전성 기반이 되는 암호학적으로 어려운 문제들에 대해 정의하고, 3장에서 제안하는 프로토콜을 설명한다. 4장에서 안전성 및 효율성을 분석하며 5장에서는 구현 결과를 보여주고, 마지막으로 6장에서 결론을 맺는다.

2. 개 요

M-Commerce 환경은 그 특성상 무선통신 구간에서 사용자의 신분 정보 및 위치 정보의 노출, 송·수신되는 데이타의 도청 및 변조 등의 보안 문제점들이 발생한다. 이러한 문제점들을 해결하고 무선시스템의 보안을 강화시키기 위하여 안전한 인증 및 키교환 프로토콜들이 필요하다. 지금까지 여러 암호 기술들을 사용한 인증 및 키교환 프로토콜들이 제안되었지만, 기존 연구들은 두 명의 참가자가 유한체 기반의 연산을 사용하여 키교환을 수행하는 프로토콜들이다. 이들은 유·무선 환경에서 모두 적용되지만, 이동통신 단말기들이 가지는 저장 공간 및 계산능력의 한계점을 고려해볼 때 이들을 무선환경에서 사용하는 것은 비효율적이다. 또한 현재 M-Commerce 서비스가 제공되는 현실적인 환경을 살펴보면 무선통신 사업자와 M-Commerce 호스트는 기존의 유선 네트워크(wired network)를 이용하여 통신하고, 이동통신 사용자는 무선통신 사업자가 제공하는 무선 네트워크(wireless network)를 이용하여 통신하기 때문에, M-Commerce 환경에서의 통신 참가자들은 이동통신 사용자와 M-Commerce 호스트, 무선통신 사업자로 구성된다. 따라서 기존의 두 명의 통신 참가자를 대상으로 하는 키교환 프로토콜들을 실제 M-Commerce 환경에서 사용하는 것은 적절하지 못하며 실제 M-Commerce 환경에 맞는 인증 및 키교환 프로토콜이 필요하다.

이 절에서는 M-Commerce 환경에 적합한 인증 및 키교환 프로토콜을 설계하기 위해서 필요한 요구사항을 분석하고, 이러한 프로토콜의 안전성에 기반이 되는 암호학적 문제들을 기술한다.

2.1 요구사항

인증 및 키교환 프로토콜에 필요한 보안 요구사항들은 다음과 같다[2,7,8].

(1) 개체 인증(entity authentication) 제공
: 키교환 프로토콜에 참여하고 있는 상대방의 신원을 확인할 수 있어야 한다.

(2) 키 확인(key confirmation) 제공

: 키교환 프로토콜에 참여한 사용자가 자신이 의도한 상대방과 동일한 세션키를 실제로 공유하였음을 확인할 수 있어야 한다.

(3) 묵시적 키 인증(implicit key authentication) 제공
: 세션키의 소유 여부가 알려져 있지 않은 경우라도 키교환 프로토콜에 참여한 사용자 이외에 어느 누구도 세션키를 계산할 수 없음을 보장해야 한다.

(4) 키 신규성(key freshness) 제공
: 세션마다 새로운 키를 설정해야 한다.

(5) 능동적 위장 공격(active impersonation attack) 불가
: 공격자가 자신을 임의의 다른 사용자로 위장하여 프로토콜에 참여한 후, 정당한 사용자와 키교환을 성공적으로 수행하는 공격이 불가능해야 한다.

(6) 완전한 전향적 보안성(perfect forward secrecy) 제공
: 키교환 프로토콜에 참여하는 두 사용자의 장기간 비밀키(long term secret key)가 노출되거나 분실된 경우라도 공격자가 두 사용자 사이에 설정된 과거 및 현재의 세션키를 유추할 수 없어야 한다.

(7) 알려진 키에 대한 안전성(known key security) 제공
: 키교환 프로토콜에 참여하는 두 사용자들 사이의 과거 세션키가 노출되어도 현재 세션키의 안전성에는 아무런 영향을 미치지 않아야 한다.

위와 같이 인증 및 키교환 프로토콜에 필요한 기본적인 요구사항 이외에도, 사용자의 신원 정보나 거래 정보가 노출되기 쉬운 M-Commerce 환경의 특징을 고려하여 추가적으로 필요한 요구사항은 다음과 같다.

(8) 이동통신 사용자의 익명성(anonymity of mobile user) 제공
: M-Commerce 호스트가 이동통신 사용자의 신원을 직접적으로 확인하지 못하게 한다.

(9) 통신정보의 기밀성(confidentiality)과 무결성(integrity) 제공
: 키교환을 하는 두 사용자 사이의 통신내용을 무선통신 사업자를 포함한 제 3자가 알지 못하게 하고, 다른 사람에 의해 통신내용이 변경되지 않음을 보장해야 한다.

2.2 안전성 기반 문제

타원곡선 암호시스템을 사용하는 인증 및 키교환 프로토콜은 다음에서 설명하는 두 문제에 기반하여 안전성을 제공한다[2,7].

[정의 1] 타원곡선 이산대수 문제(elliptic curve discrete logarithm problem : ECDLP):

위수가 n인 타원곡선 위의 한 점 G와 $Q = aG$인 타원곡선 위의 점 Q를 알 때, 점 G를 몇 번 더해야 점 Q가 되는지 a값을 알아내는 문제

위의 문제는 n이 충분히 클 경우, a와 G를 알면 Q를 구하는 것이 쉬우나, 점 Q와 점 G를 알고 있어도 a값을 알아내긴 힘들다는 어려움에 근거하여 안전성을 제공한다[2].

[정의 2] 타원곡선 Diffie-Hellman 문제(elliptic curve Diffie-Hellman problem : ECDHP):

타원곡선 위의 기본 점 G를 알고 랜덤수 a, b에 대하여 aG와 bG가 주어졌을 때, abG를 구하는 문제

aG와 bG를 알아도 a 또는 b 어느 것도 알지 못한다면 abG를 알기 힘들다는 ECDHP의 어려움은 대부분 유한체 상에서 정의된 Diffie-Hellman 문제보다 어렵다고 알려져 있어 키 비트당 보다 많은 안전성을 보장한다[2]. 만약 공격자가 G와 aG 혹은 bG로부터 a 또는 b를 계산한다면 이 암호시스템은 깨지지만 이 문제는 위에서 언급한 타원곡선 이산대수 문제를 풀어야 하는 것이므로 불가능하다.

3. 제안하는 인증 및 키교환 프로토콜

무선통신 환경의 제약점을 고려하여 타원곡선 암호시스템을 사용한 효율적이고 안전한 인증 및 키교환 프로토콜을 제안한다.

3.1 용어 정의

제안하는 프로토콜에서 사용되는 용어들은 아래와 같다.

- p : 사용되는 기반 유한체 F_p의 크기 (p는 소수)
- E : a와 b($a, b \in F_p$)에 의해 정의된 F_p상의 타원곡선 ($E : y^2 = x^3 + ax + b,\ 4a^3 + 27b^2 \neq 0 \pmod p$)
- G : 타원곡선위의 기본점
- n : G의 위수
- U : 이동통신 사용자
- M : M-Commerce 호스트
- S : U와 M의 통신을 연결시켜주는 무선통신 사업자
- ID_M : 사용자 M의 식별자
- pwd : U와 S사이에 미리 공유된 패스워드
- Q, Q^{-1} : 패스워드 pwd로부터 계산하는 정수와 그의 역수
- r_U : U가 구간 [2, n-2]에서 선택한 랜덤수
- R_U : r_U의 공개값(public value), $R_U = r_U * G$
- c : 구간 [2, n-2]에서 선택한 랜덤수
- K : U와 M이 설정하는 세션키(session key)
- PK_M / SK_M : M의 공개키/비밀키
- $E_K[\ ]$: 키 K를 사용한 대칭키 암호 알고리즘
- $\{\ \}_{PKM}$: 공개키 PK_M을 사용한 공개키 암호 알고리즘
- $H(\ )$: 암호학적 일방향 해쉬 함수(strong one-way hash function)

3.2 프로토콜 환경

이동통신 사용자가 M-Commerce 호스트로부터 서비

스를 제공받기 위해서는 무선통신 사업자를 통하여 M-Commerce 호스트 사이트에 접속해야 한다. 이때, 이동통신 사용자와 무선통신 사업자 사이는 무선 네트워크(wireless network)로 연결되어 있고, 무선통신 사업자와 M-Commerce 호스트는 유선 네트워크(wired network)로 연결되어 있다.

본 논문에서는 이동통신 사용자와 무선통신 사업자 사이에 미리 공유된 패스워드가 있음을 가정하고 이를 사용하여 서로를 인증하도록 한다. 이 패스워드는 일정 기간 후, 무선통신 사업자가 이동통신 사용자에게 패스워드를 변경해야 함을 알리는 메시지를 전송하여 이동통신 사용자가 패스워드를 주기적으로 변경하도록 한다. 또한 M-Commerce 호스트와 무선통신 사업자는 상대방을 확인할 수 있는 서로의 공개키를 포함한 인증서(certificate)를 가지고 있다고 가정한다.

제안하는 프로토콜의 환경은 그림 1과 같다. 이동통신 사용자는 무선 구간을 지나 무선통신 사업자에게 접속한 후, 서비스 제공업자인 M-Commerce 호스트에게 연결된다. 현재 M-Commerce 서비스를 제공하는 환경은 M-Commerce 호스트들이 직접 이동통신 사용자와 연결을 설정할 수 없고, 무선통신 사업자가 M-Commerce 호스트와 이동통신 사용자 사이에 존재하여 이 둘을 연결해 주는 형태만이 가능하다. 따라서 M-Commerce 호스트는 반드시 무선통신 사업자를 거쳐야만 이동통신 사용자에게 서비스를 제공할 수 있다.

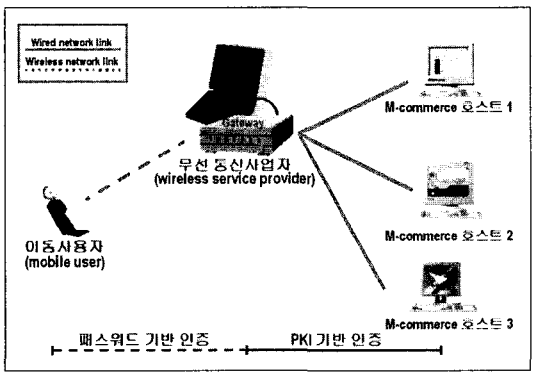

그림 1 프로토콜 환경

3.3 프로토콜

패스워드 인증을 위해서 이동통신 사용자 U와 무선통신 사업자 S는 미리 공유된 패스워드 pwd로부터 계산된 정수값 $Q= H(pwd)$를 공유하고, 무선통신 사업자는 이동통신 사용자가 M-Commerce 호스트와의 접속을 요청해올 경우 사용자 DB에서 검색한 해당 사용자의 패스워드를 가지고 프로토콜을 시작한다. 모든 연산은 유한체 F_p에서의 연산이므로 mod p는 생략한다. 제안하는 프로토콜은 다음 단계들로 구성되며, 그림 2에 요약되어 있다.

[이동통신 사용자 U => 무선통신 사업자 S]

Step 1. U는 구간 [2, n-2]에서 랜덤수 c와 r_U를 선택한다. U는 S와의 패스워드 인증을 수행하기 위해 다음과 같이 x_U를 계산한 후, 이것의 공개값 P_U를 계산한다.

$$x_U = r_U * Q$$
$$P_U = x_U * G$$

Step 2. U는 통신하려는 M-Commerce 호스트 M의 URL을 담은 req와 패스워드 인증을 위한 공개값 P_U, 랜덤수 c값을 S에게 전송한다.

[무선통신 사업자 S => M-Commerce 호스트 M]

Step 3. S는 U와 미리 공유한 패스워드 pwd를 이용하여 계산한 정수값 Q로부터 역수 Q^{-1}을 계산한 후, Q^{-1}와 전송받은 P_U값을 사용하여 Val_1을 계산한다.

$$Q= H(pwd)$$
$$Val_1 = Q^{-1} * P_U$$

Step 4. S는 req로부터 M의 URL을 확인하여 Step 3에서 계산한 Val_1을 포함하는 메시지 $\{ID_S, Val_1, c\}$를 M의 공개키 PK_M으로 암호화하여 $\{ID_S, Val_1, c\}_{PKM}$를 M에게 전송한다.

[M-Commerce 호스트 M => 무선통신 사업자 S]

Step 5. M은 구간 [2, n-2]에서 랜덤수 r_M을 선택하여 r_M의 공개값 R_M을 계산하고, 전송 받은 암호문 $\{ID_S, Val_1, c\}_{PKM}$을 자신의 비밀키 SK_M로 복호화한다. 복호화된 메시지 중 Val_1을 이용하여 U와의 세션키 K를 계산하고, S에게 자신이 S로부터 전송 받은 Val_1값을 사용하였음을 알려주는 동시에, 자신이 전송한 R_M이 정당한지 확인시켜주는 값인 v를 계산한다.

$$R_M= r_M * G$$
$$K= r_M * Val_1$$
$$v= \mathrm{H}(Val_1 \| R_M)$$

Step 6. M은 전송 받은 c를 세션키 K로 암호화하여 암호문 $E_K[c]$를 포함하는 메시지 $\{ID_M, E_K[c], v, R_M\}$을 S의 공개키 PK_S로 암호화하여 $\{ID_M, E_K[c], v, R_M\}_{PKS}$를 S에게 전송한다.

[무선통신 사업자 S => 이동통신 사용자 U]

Step 7. S는 비밀키 SK_S를 사용하여 M으로부터 받은 암호문을 복호화한 후, 아래와 같이 v'을 계산한다.

$$v' = \mathrm{H}(Val_1 \| R_M)$$

v'은 M이 Step 3에서 생성된 Val_1을 사용하였는지 확인하고 M이 전송한 R_M이 정당한지 검증하기 위해서 계산한 값으로 이 값을 M에게서 전송 받은 v와 비교한다. $v' = v$인 경우, M이 Val_1을 사용하여 U와 공유한

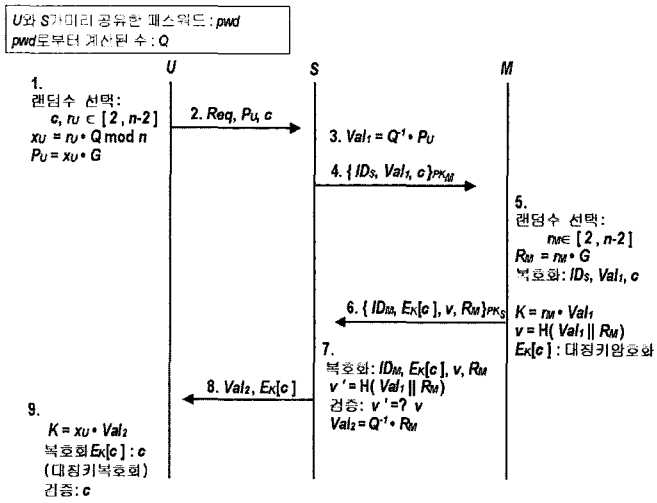

그림 2 프로토콜 흐름도

세션키 K를 계산하고 M으로부터 전송 받은 R_M이 올바른지 확인된 것이므로 계속 다음 단계를 수행한다.

$v' \neq v$인 경우 프로토콜 수행을 종료한다.

Step 8. S는 R_M을 전송할 때 패스워드 인증을 위해 Q^{-1}을 사용하여 Val_2를 계산하고, 이 값을 M으로부터 받은 암호문 $E_K[c]$와 함께 U에게 전송한다.

$$Val_2 = Q^{-1} * R_M$$

[이동통신 사용자 U]

Step 9. U는 Val_2를 사용하여 세션키 K를 계산하고, K로 $E_K[c]$를 복호화한 후, 복호화된 메시지가 자신이 생성한 랜덤수 c와 맞는지 검증함으로써 세션키 K가 올바른지 확인한다.

$$K = x_U * Val_2$$

4. 안전성 및 효율성 분석

제안한 프로토콜의 안전성과 효율성에 대하여 살펴보겠다.

4.1 안전성 분석

제안한 프로토콜은 다음과 같이 9개의 요구사항을 만족한다.

(1) 개체 인증 제공

: 이동통신 사용자 U와 무선통신 사업자 S는 미리 설정한 패스워드 pwd를 사용하여 서로를 인증하며, 각각 ID_M와 ID_S을 확인함으로써 M-Commerce 호스트 M과 무선통신 사업자 S는 서로를 인증한다. 또한 M-Commerce 호스트는 사용자를 무선통신 사업자를 통해 간접적으로 인증한다.

(2) 키 확인 제공

: 이동통신 사용자 U는 전송받은 암호문 $E_K[c]$을 복호화 하였을 때 얻은 메시지가 자신이 생성한 랜덤수 c임을 검증함으로써 자신이 세션키 K를 올바로 계산하였고, 자신과M-Commerce 호스트 사이에 세션키 K가 올바로 공유되었음을 확인할 수 있다.

(3) 묵시적 키 인증 제공

: ECDLP의 어려움에 근거하여 비밀 랜덤수 r_M 또는 r_U를 아는 사람만이 세션키 $K=r_M*r_U*G$를 계산할 수 있음을 확신하므로 이동통신 사용자와 M-Commerce 호스트는 서로에게 묵시적인 키 인증을 제공한다.

(4) 키 신규성 제공

: 매 세션마다 새로운 랜덤수 r_M과 r_U를 사용하므로 매번 새로운 세션키를 설정한다.

(5) 능동적 위장 공격 불가

: 이동통신 사용자는 무선통신 사업자와 패스워드 pwd를 공유하고 이로부터 계산된 Q^{-1}값을 사용하여 암호화된 메시지를 전송하므로 패스워드 pwd를 모르는 다른 사람이 해당 이동통신 사용자 U로 위장할 수 없다. 또한, M-Commerce 호스트와 무선통신 사업자 사이의 통신내용은 공개키 암호 알고리즘을 이용하여 암호화가 되어 있기 때문에, 두 개체의 비밀키 SK_S , SK_M를 모르는 공격자는 암호화된 통신 내용을 복호화할 수 없으므로 복호화된 메시지를 이용하여 해당 무선통신 사업자나 M-Commerce 호스트로 위장할 수 없다.

(6) 완전한 전향적 보안성 제공

: 공격자가 이동통신 사용자의 장기간 비밀키(long term secert key)인 패스워드 pwd를 알아냈을 경우, 공격자는 pwd로부터 계산된 정수값 Q와 Q^{-1}을

알게 되고, 통신과정을 통하여 쉽게 노출될 수 있는 값 P_U와 Val_2로부터 R_U나 R_M값을 알아낼 수 있지만, ECDHP의 어려움에 근거하여 세션키를 계산할 수 없다. 그리고 M-Commerce 호스트의 비밀키 SK_M과 무선통신 사업자의 비밀키 SK_S를 알아냈을 경우라도 둘 사이의 통신내용은 드러나지만 ECDHP의 어려움에 근거하여 세션키 K는 계산할 수 없다.

(7) 알려진 키에 대한 안전성 제공
: 매 세션마다 새로운 랜덤수 r_M 또는 r_U를 사용하여 세션키 K를 생성하므로, 과거 세션키의 노출이 현재 세션키의 안전성에는 아무런 영향을 미치지 않는다.

(8) 이동통신 사용자의 익명성 제공
: M-Commerce 호스트는 이동통신 사용자를 직접 인증하지 않고 무선통신 사업자를 통해 간접적으로 인증하여 세션키 K를 설정하기 때문에 M-Commerce 호스트에게 사용자 의 신원이 노출되지 않으므로 M-Commerce 호스트에게 사용자의 익명성이 보장된다.

(9) 통신정보의 기밀성과 무결성 제공
: 무선통신 사업자는 ECDHP의 어려움에 근거하여 두 키 재료값 r_M 또는 r_U를 안다 하더라도 이동통신 사용자와 M-Commerce 호스트 사이의 세션키 K를 계산할 수 없으므로 무선통신 사업자를 포함한 제 3자로부터 M-Commerce 호스트와 이동통신 사용자 사이의 통신내용의 기밀성이 보장된다. 또한, 무선통신 사업자는 세션키 K를 모르기 때문에 사용자와 M-Commerce 호스트 사이의 세션키로 암호화된 통신내용을 위·변조 할 수 없으므로 통신정보의 무결성이 보장된다.

4.2 효율성 분석

제안하는 프로토콜은 이동통신 사용자와 무선통신 사업자간의 인증과정에서 효율성을 위하여 패스워드 기반의 인증방식을 사용했다. 따라서 적은 비트 길이를 갖는 패스워드를 이용한 인증방식들의 공통적인 취약점인 온라인 패스워드 추측공격에는 약하지만, 무선통신 사업자가 올바른 패스워드 입력 시도의 실패 횟수를 제한함으로써 최소화할 수 있다.

또한 이동통신 사용자의 계산량을 고려해볼 때, 제안하는 프로토콜에서 많은 계산량이 요구되는 스칼라 곱셈 연산의 횟수는 P_U와 K를 계산할 때 2회이다. 그러나 P_U는 오프라인 상에서 계산이 가능하기 때문에 온라인상에서는 K의 계산 1회만 스칼라 곱셈 연산을 수행하면 되므로 이동통신 사용자의 계산량을 줄일 수 있어 효율적이다. 그밖에 무선통신 사업자가 M-Commerce 호스트에게 이동통신 사용자를 대신하여 서비스를 요청하기 때문에 M-Commerce 호스트의 신원을 무선통신 사업자가 대신 확인하고, 프로토콜 수행과정 중 v와 v'의 비교를 통해서 M-Commerce 호스트가 전송한 값이 정당한지 여부를 검증하기 때문에, 이동통신 사용자의 계산량을 줄일 수 있어 무선 환경에 적합하다.

5. 구현 결과

본 장에서는 논문에서 제안한 프로토콜을 구현하여 수행한 결과를 보인다.

5.1 프로토콜 구현 환경

본 논문에서 제안한 프로토콜의 구현 환경과 사용한 암호 기법들은 표 1, 표 2와 같다.

제안하는 프로토콜에서는 대칭키 암호 알고리즘으로 RC4[9,10]를 선택하고, 공개키 알고리즘으로는 ElGamal [9,10]을 사용하며, 암호학적 해쉬 함수는 128비트를 생성하는 MD5[9,10]를 선택한다. 또한, 본 프로토콜의 사용자의 수행부분을 SK-VM 에뮬레이터를 사용하여 테스트하였다.

표 1 구현 환경

운영 체제	Window 2000
암호 라이브러리	Bouncy Castle
개발 언어	Java, SK-VM

표 2 사용하는 암호기법

대칭키 암호 알고리즘	RC4
공개키 암호 알고리즘	ElGamal
해쉬 함수	MD5

본 논문에서 사용하는 타원곡선을 선택하기 위한 도메인 파라미터 값들인 필드 F_p를 생성하는 192비트 소수 p, F_p상의 타원 곡선 $E : y^2 = x^3 + ax + b \pmod p$를 정의하는 값인 a와 b, 타원 곡선 위의 기본점인 G와 G의 위수 n을 정의한다[11,12]. 이들은 "ANSI X9.62[7]에 정의된 값을 사용하였다.

5.2 구현 결과

이동통신 사용자가 무선통신 사업자에게 M-Commerce 호스트와의 통신을 요청하는 것으로 프로토콜을 시작한다.

이동통신 사용자는 그림 3과 같이 오프라인 연산을 통하여 통신 준비를 하고, 초기 연산이 완료되면 그림 4와 같은 입력화면에 서비스를 받으려는 호스트의 이름인 "ewha"를 입력하여 화면 하단의 "OK"버튼을 눌러 무선통신 사업자에게 M-Commerce 호스트와의 연결을 요청한다. 그 후 무선통신 사업자는 이동통신 사용자의

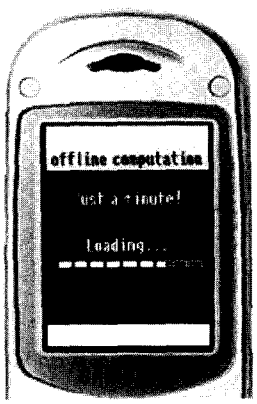

그림 3 초기화면

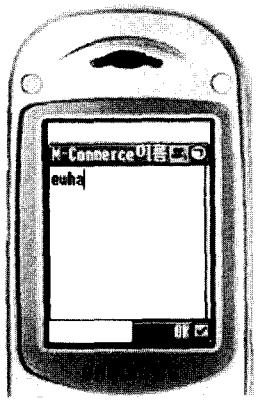

그림 4 입력화면

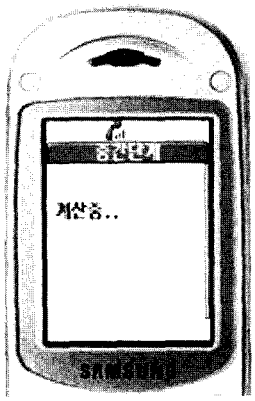

그림 7 중간단계

그림 8 키교환

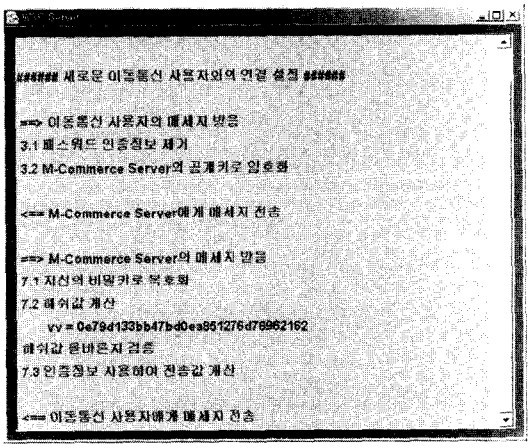

그림 5 무선통신 사업자의 처리 과정

통신 요청을 받아 전송받은 값을 사용하여 사용자가 M-Commerce 호스트와 세션키를 설정하도록 M-Commerce 호스트와 무선통신 사업자 사이의 통신을 그림 5와 그림 6과 같이 수행한다.

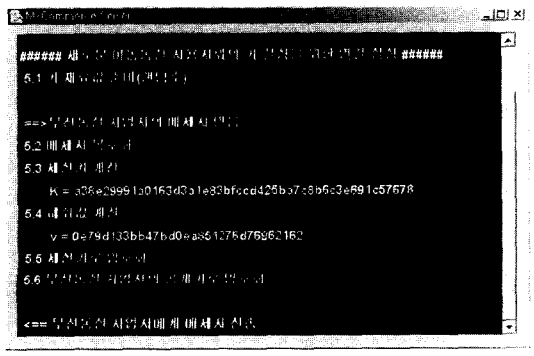

그림 6 M-Commerce 호스트의 처리 과정

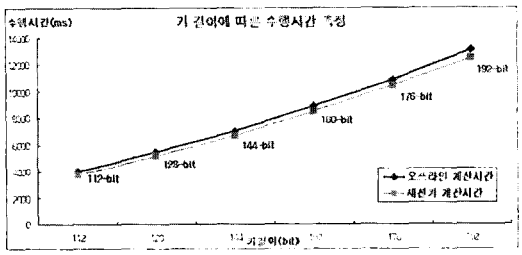

그림 9 수행결과

무선통신 사업자와 M-Commerce 호스트 사이의 통신이 수행되는 동안 사용자의 휴대폰에는 그림 7과 같은 메시지가 보이고, 모든 키교환 과정이 완료되면 그림 8과 같은 화면을 확인할 수 있다. 키의 길이가 증가함에 따라 오프라인 연산의 수행시간과 온라인상에서 세션키 연산의 수행시간을 측정하였고, 그 결과는 그림 9의 그래프와 같다.

6. 결 론

M-Commerce 환경에서 안전한 서비스를 제공하기 위해서는 전송되는 메시지들을 암호화해야하며, 이를 위해 세션키의 설정이 요구된다. 그러나 유선통신 환경과 비교해 볼 때 M-Commerce 환경은 연산 속도나 저장 공간 등에 제약점이 있어 이를 고려한 키교환 프로토콜 설계가 필요하다.

본 논문에서는 이러한 제약점들을 고려하여 M-Commerce 환경에서 이동통신 사용자가 안전한 통신을 하기 위한 인증 및 키교환 프로토콜을 제안하였다. 제안하는 프로토콜은 M-Commerce 환경에 적합하고 이동통신 사용자의 익명성을 보장하는 효율적인 인증 및 키교환 프로토콜이다. 또한, 온라인상에서 사용자의 계산량을 최소화함으로써 M-Commerce 환경의 한계점을 보완하

고, M-Commerce 호스트가 무선통신 사업자를 통하여 이동통신 사용자를 간접 인증하는 방식을 택하여 사용자의 익명성을 제공하였다.

제안하는 프로토콜은 이동통신 사용자의 정보를 보호하면서 안전하고 빠른 서비스를 제공할 수 있어 M-Commerce 환경에서 유용하게 적용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 조병선, 하영욱, "국내 무선인터넷 산업 동향 분석", ETRI 전자통신동향분석, 제 17권 4호, pp. 29-38, 2002.

[2] ANSI X9.63, "ANSI X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography," ANSI Working Draft, 2000.

[3] M. Aydos, B. Sunar, and D. Koc, "An Elliptic Curve Cryptography Based Authentication and Key Agreement Protocol for Wireless Communication," International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, USA, 1998.

[4] M. Bellare, D. Jablon, H. Krawczyk, P. MacKenzie, P. Rogaway, R. Swaminathan and T. Wu, "Proposal for P1363 study group on password-based authenticated-key-exchange methods," 2000.

[5] T. Kwon, "Authentication and key agreement via memorable password," NDSS 2001 Symposium Conference Proceedings, 2001.

[6] T. Wu, "Secure remote password protocol," NDSS, 1998.

[7] ANSI X9.62, "ANSI X9.62 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," ANSI, X9.62-1998, 1999.

[8] T. Satoh, K. Araki and S. Miura, "Overview of elliptic curve cryptography," PKC'98, LNCS 1431, pp. 29-49, 1998.

[9] 이민섭, 현대 암호학, 교우사, 2000.

[10] D. Stinson, Cryptography - Theory and Practice, CRC Press, ISBN 0-8493-5821-0, 1995.

[11] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes," Journal of Cryptology, Vol. 14, No. 4, pp. 255 - 293, 2001.

[12] SEC2, "SEC 2 - Recommended Elliptic Curve Domain Parameters," Standards for Efficient Cryptography Group, Ver. 1.0, 2000.

박 수 진

2002년 이화여자대학교 컴퓨터학과 학사 2004년 이화여자대학교 과학기술대학원 컴퓨터학과 석사. 2004년~현재 삼성 SDS. 관심분야 정보보호, 암호프로토콜 설계, 무선 이동통신 보안

서 승 현

2000년 이화여자대학교 수학과 학사. 2002년 이화여자대학교 과학기술대학원 컴퓨터학과 석사. 2002년~현재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정 관심분야 정보보호, 암호프로토콜 설계, 홈 네트워크 보안

이 상 호

1979년 서울대학교 계산통계학과 학사 1981년 한국과학기술원 전산학과 석사 1987년 한국과학기술원 전산학과 박사 1983년~현재 이화여자대학교 컴퓨터학과 교수. 관심분야 알고리즘 설계, 정보보호, 바이오인포매틱스