안전한 모바일 결제 프로토콜을 위한 위임기관을 사용한 인증과 키 동의

(Authentication and Key Agreement using Delegating Authority for a Secure Mobile Payment Protocol)

성 순 화 †
(Soonhwa Sung)

요 약 모바일 결제 시스템은 모바일 장치의 특성과 모바일 결제 과정의 안전성 때문에 실제 모바일 결제 네트워크에 많은 문제점을 가지고 있다. 특히 이전에 제안된 모바일 결제 프로토콜에서는 결제 기관인 발행 은행의 신뢰 검증을 할 수 없다. 따라서 본 논문에서는 발행 은행의 신뢰성을 높이기 위한 발행 은행 검증 위임 기관을 제안하여, 모바일 결제 효율성을 분석하였다. 그 결과 은행의 결제 검증 위임 기관을 둔 모바일 결제 프로토콜은 키 동의 계산 시간과 통신 신뢰성 회복에서 향상을 보였다.

키워드 : 모바일 결제 프로토콜, 결제 위임 기관, 키 동의, 결제 인증

Abstract Mobile payment system has many problems in real mobile payment networks because of the characteristics of mobile device and the security of mobile payment process. Specially, the previous suggested mobile payment protocol can not verify a trust of issuing bank. Therefore, this paper has analyzed the efficiency of a mobile payment with a delegating authority for an issuing bank to trust issuing bank. As a result, the mobile payment protocol with a delegating authority for a payment verification of an issuing bank has improved the time complexities for key computation and communication resilience.

Key words : mobile payment protocol, delegating authority for payment, key agreement, payment verification

1. 서 론

모바일 거래는 사용자가 가는 곳은 어디든지 거래를 할 수 있는 모바일 장치를 위한 중요한 응용 영역이다. 이러한 모바일 거래의 장점은 언제 어디서나 이용할 수 있는 접근성, 위치 시스템을 사용한 지역 정보 서비스를 포함하는 지역성, 모바일 장치의 크기와 무게의 편리성, 사용자의 필요와 요구를 조정하는 개인성 등이다[1]. 한편 모바일 거래의 단점은 모바일 장치의 제한된 성능, 이기종 장치와 네트워크 기술이 단일 사용자 플랫폼에 부적합한 점, 모바일 장치의 분실 파괴 위험성, 그리고 모바일 장치와 네트워크 사이의 통신 도청 등이다. 이러한 단점 중 모바일 통신 도청은 특히 모바일 결제 서비스에서는 아주 중요한 이슈이다.

뿐만 아니라 다른 금융 기관 사이의 모바일 상거래를 위한 표준화 부족, 단 대 단 시큐리티 이슈, 소매상인 거래 센터 통합 문제, 많은 거래 수용 능력 부족, 결제 기반 구조의 부족 등이다. 그리고 새로운 기술 도전과 이슈를 제공하기 위한 지역적 차이, 각각의 시장 원동력, 안정된 가격 효율성 등도 고려해야만 한다.

최근, 모바일 결제에서 비즈니스 시장, 결제 과정, 결제 방법 및 표준에 관하여 많은 논문들이 발표되었다[2-5]. 그러나 아직 프로토콜, 디자인 이슈, 안전성 해결책을 포함한 모바일 결제 시스템을 어떻게 수립할 것인가에 대해 논의되지 않고 있다[6-9]. 특히 Li Xi, Hu Han-ping이 발표한 논문[10]은 안전한 모바일 결제 시스템을 위한 안전한 모바일 결제 프로토콜을 제안하였

† 종신회원 : 충남대학교 공과대학 전기정보통신공학부 BK전임교수
shsung@cnu.ac.kr
논문접수 : 2009년 8월 25일
심사완료 : 2010년 1월 20일

정보과학회논문지: 정보통신 제37권 제2호(2010.4)

다. 이는 모바일 결제 시스템 전체 구성을 모바일 장치, 콘텐츠 제공자, 결제 서비스 제공자로 나누어 본다면 모바일 장치와 콘텐츠 제공자인 상인이 서로 거래를 동의한다는 가정에서 시작된다. 또한 결제 서비스인 은행을 완벽한 신뢰 기관으로 전제한 결제 거래 프로토콜이다. 그러나 실제의 모바일 결제에서는 이러한 결제 서비스를 제공하는 전체 은행을 신뢰할 수 있는 안전한 웹 서비스가 필요하다.

따라서 본 논문에서는 Li Xi, Hu Han-ping이 제안한 모바일 결제 프로토콜[10]이 더 효율적이고 안전하기 위해, 결제 검증 위임 기관을 제안하여 전체 은행을 인증하며 키 동의하는 프로토콜을 제시한다.

2. 관련 연구

2.1 모바일 결제 시스템

모바일 결제가 대부분의 무선 정보 서비스와 모바일 거래 응용의 중요한 부분을 차지하고 있기 때문에 안전한 모바일 결제 시스템을 어떻게 구성해야 하는가가 연구의 관심이다. 따라서 Li Xi, Hu Han-ping이 제안한 모바일 결제 프로토콜[10]에서는 안전하지 않은 모바일 환경에서 모바일 장치를 사용하여 효율적인 모바일 결제 시스템을 제안하였다. 이러한 모바일 결제 시스템은 그림 1과 같은 구조로 이루어지며, 이러한 모바일 결제 시스템의 프로토콜은 결제 거래 프로토콜과 세션 키 생성 프로토콜로 구성된다.

2.2 모바일 결제 거래 프로토콜

① 모바일 폰과 발행 은행은 각 세션의 데이터의 암호화 복호화를 위해 사용될 공유 세션 키를 생성한다.

② 결제자는 결제 정보를 입력한다.

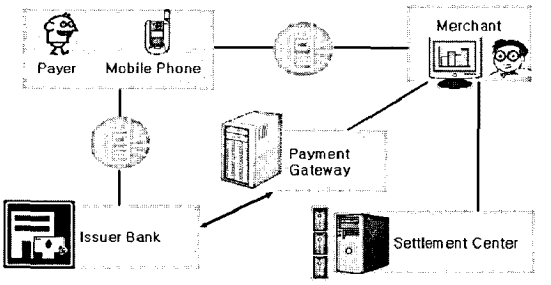

그림 1 모바일 결제 시스템 구조

③ 결제자의 주문, 결제 패스워드와 같은 민감한 데이터는 암호화한다.

④ 모바일 폰은 암호화된 결제 데이터의 메시지를 상인에게 보낸다.

⑤ 결제 거래에서 주문에 대한 상인 정보가 필요하면 상인은 은행 ID와 메시지에 대한 주문을 취득해야만 한다.

⑥ 모바일 결제 메시지는 결제 게이트웨이를 통해 발행 은행에게 보내어진다.

⑦ 결제 데이터를 복호화한 뒤 발행 은행은 그 유효성과 인증을 검증한다. 동시에 시스템은 결제자의 잔액을 체크한다.

⑧ 발행 은행은 결제에 대한 인증을 결제 게이트웨이를 통해 상인에게 보낸다.

⑨ 결제 거래 결과는 결제자에게 보내지고 거래가 성공적이면 잔액과 새로운 체크가 수반된다.

⑩ 주기적으로, 전날 모든 거래를 바탕으로 한 결산 과정이 은행들 사이에서 이루어진다.

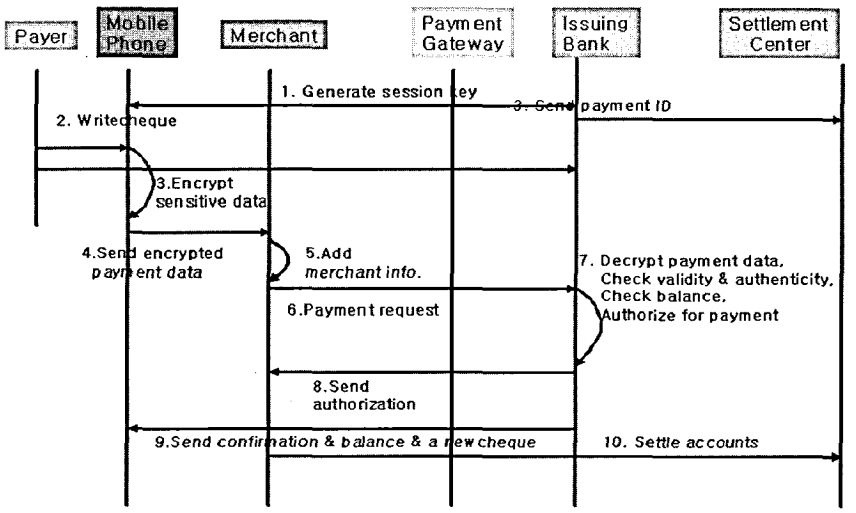

그림 2 모바일 결제 거래 프로토콜

2.3 세션 키 생성 프로토콜

결제가 이루어지기 전에 모바일 폰과 발행 은행이 세션 키 K_s와 보전 키 K_i를 생성한다. 이들 키는 난수열(Random Sequence Number)에 의해 오프라인으로 생성되며, 이러한 과정은 결제자에게 보여지지 않는다.

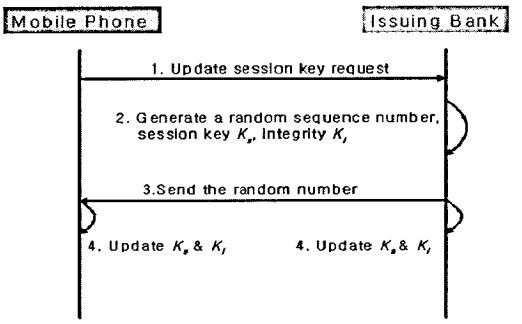

그림 3 세션 키 생성 프로토콜

3. 제안한 모바일 결제 프로토콜

모바일 결제가 시작될 때, 서비스 제공자의 거래 명세서에는 서비스 제공자 ID, 주문 번호, 거래 계좌와 금액 등을 설명하는 최소한의 명세를 소비자에게 제시한다. 이러한 제시는 인터넷과 같은 웹 서비스로 이루어진다.

최근 발표된 Li Xi, Hu Han-ping의 프로토콜[10]에서는 모바일폰과 발행 은행 사이 안전성을 위해 세션 키를 생성하였다. 그러나 이 프로토콜에서는 발행 은행 자체를 신뢰할 수 있는 어떠한 검증 절차가 없다. 따라서 제안한 모바일 결제 프로토콜은 Li Xi, Hu Han-ping이 제안한 프로토콜[10]의 발행 은행 신뢰성을 높이기 위하여 발행 은행 검증을 위한 위임 기관을 둔다. 이러한 위임 기관은 인증 기관과 같은 제 3의 신뢰 기관으로 가정하며, 제안한 프로토콜은 Li Xi, Hu Han-ping 프로토콜[10]의 결산 센터를 따로 둘 필요가 없어 부가적인 서버가 필요 없다.

모바일 결제 거래 프로토콜은 그림 4와 같은 단계로 이루어진다.

① 결제자는 구입하고자 하는 쇼핑몰의 상인에게 결제 ID를 생성한다.
② 상인은 결제자가 보낸 결제 ID에 동의한다.
③ 결제자는 발행 은행과 결제 ID 검증 위임 기관에게 결제 ID를 보낸다.
④ 모바일 폰과 발행 은행은 각 세션을 위해 생성된 데이터의 암, 복호화를 위해 사용되는 공유 세션 키를 생성한다.
⑤ 결제자는 결제 정보를 입력한다.
⑥ 결제자의 계좌, 결제 패스워드등과 같은 민감한 데이터는 암호화된다.
⑦ 모바일 폰은 암호화된 결제 데이터를 가진 메시지를 상인에게 보낸다.
⑧ 결제 거래에서 상인 계좌 정보가 필요하다. 그래서 상인은 결제 전에 취득 은행 ID와 그 메시지의 계좌 정보를 취득해야만 한다.
⑨ 모바일 결제 메시지는 결제 게이트웨이의 발행 은행에게 보내어진다.

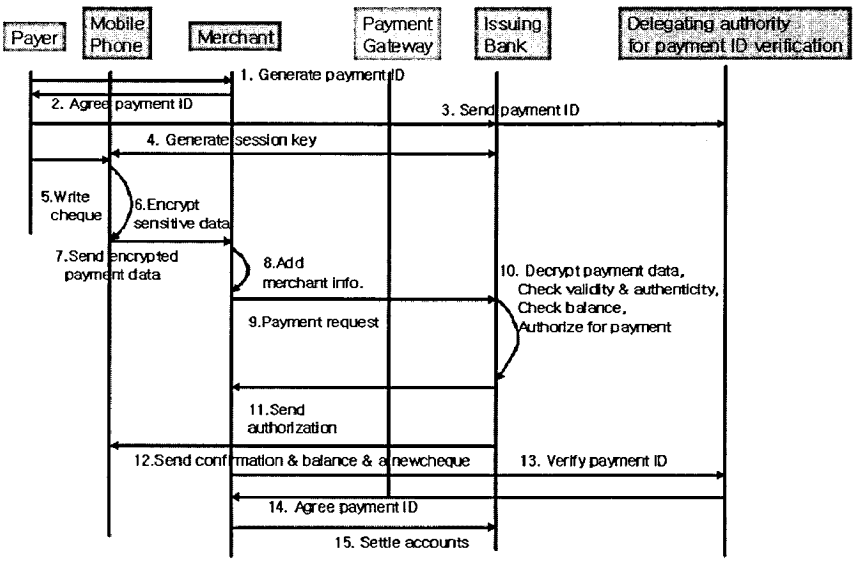

그림 4 모바일 결제 거래 프로토콜

⑩ 결제 데이터를 복호화한 후, 발행 은행은 그 유효성과 확실성을 검증한다. 동시에 시스템은 결제자의 계좌 잔액을 확인한다. 발행 은행은 결제 정보가 정확하고 결제자의 충분한 액수가 확인되면 거래를 계속한다.

⑪ 발행 은행은 결제 게이트웨이의 상인에게 결제에 대한 권한 부여를 한다.

⑫ 결제 거래 결과는 결제자에게 보내어지고, 거래가 성공이면 계좌 잔액과 새로운 체크가 필요하다.

⑬ 상인은 결제 ID 검증 위임 기관에게 결제 ID 검증을 요청한다.

⑭ 결제 ID 검증 위임 기관은 결제 ID에 동의한다.

⑮ 주기적으로, 전날 모든 거래를 바탕으로 한 결산 과정이 은행들 사이에서 이루어진다.

세션 키 생성 프로토콜의 과정은 Li Xi, Hu Hanping 프로토콜[10]에서와 같으며 결제자에게 보여지지 않는다.

이때 모바일 폰과 발행 은행이 세션 키 K_s와 보전 키 K_i를 생성하기 이전 누군가가 발행 은행이 신뢰할 수 있는 은행인지를 인증해야만 한다. 따라서 본 논문은 은행을 인증할 수 있는 위임 기관을 두어 안전한 결제를 위한 인증과 키 동의 프로토콜을 제시한다.

4. 위임기관에서 인증과 키 동의

4.1 인증 및 키 동의 프로토콜

제안한 위임 기관은 신뢰된 제3기관으로 가정하였으므로 위임 기관의 비밀키를 이용하여 은행과의 공유키를 생성한다. 또한 은행의 ID_{Bi}를 알면 은행의 비밀키도 생성할 수 있다. 결제자가 다른 은행으로 이동할 경우 키 갱신이 필요하며 이때 키 갱신은 등록 센터에서만 수행하도록 가정한다. 위임 기관 D_k와 등록 센터 R은 비밀키 $\delta_k = h(x \| ID_{Dk})$를 공유하며, 마스터 키 x는 등록 센터 R에 의해 안전하게 보호된다.

인증과 키 동의에 필요한 기호는 다음과 같다.

B_i: 은행 i

D_k: 위임 기관 k

ID_{Bi}: B_i의 ID

P_{Bi}: B_i의 패스워드

ID_{Dk}: D_k의 ID

N_i: 신규성(freshness)을 위한 파라미터

K_R: 키 요구 메시지

SK_n: 세션키

R_{n1}, R_{n2}: 랜덤값

h: 일방향 함수

x: 센터의 마스터 키

R: 등록 센터(Registration Center)

K_{update}: 키 갱신 요청

$\oplus$: XOR 연산자

$\|$: 연접(concatenation) 연산자

δ_k : D_k의 비밀키, $h(x \| ID_{Dk})$

α_i : B_i의 비밀키, $h(\delta_k \| ID_{Bi})$

μ_{ik} : B_i와 D_k의 공유키, $h(\alpha_i \| ID_{Dk})$

λ_{ijk} : B_i와 B_j의 공유키, $h(\mu_{ik} \| ID_{Bj})$

1) 등록 단계

은행 B_i는 자신의 ID_{Bi}와 패스워드 P_{Bi}를 R에 보내 등록을 요청한다. R은 B_i의 비밀키 정보 $\alpha_i = h(\delta_k \| ID_{Bi})$와 $\beta_i = \alpha_i \oplus P_{Bi}$를 계산한다. 은행 B_i는 ID_{Bi}, P_{Bi}, 그리고 ID_{Dk}를 저장하고 α_i를 계산하여 둠으로써 초기화 과정을 마무리한다.

2) 공유키 설정 단계

은행과 위임 기관간의 공유 키 설정은 위임 기관이 은행으로부터 ID_{Bi}를 받아 자신의 비밀키를 이용하여 공유키 μ_{ik}를 계산할 수 있다. 은행 B_i와 은행 B_j가 안전한 통신을 원한다면, B_i와 B_j는 인증과 키 동의를 위해 비밀키 λ_{ijk}를 공유해야 한다. B_i는 자신의 비밀키와 ID_{Bi} 정보만으로 공유키 $\lambda_{ijk} = h(\mu_{ik} \| ID_{Bj})$를 만들 수 있다. 한편, B_j가 공유키 λ_{ijk}를 가지고 있지 않다면 D_k에 요청을 한다. D_k는 δ_k를 이용하여 B_i의 비밀키 $\alpha_i = h(\delta_k \| ID_{Bi})$와 $\lambda_{ijk} = h(\mu_{ik} \| ID_{Bj})$를 생성할 수 있다.

위임 기관 D_k는 은행 B_j에게 공유키 λ_{ijk}를 α_j로 암호화하여 전송하면 은행 B_j는 자신의 비밀키 α_j로 복호화하여 은행 사이의 공유키 λ_{ijk}를 얻을 수 있다. 그 단계는 다음과 같다.

1단계: $B_j \rightarrow D_k$: N_1, ID_{Bi}, ID_{Bj}

2단계: $D_k \rightarrow B_j$:

$$E_{\alpha_j}\left(\lambda_{ijk}, h\left(ID_{B_i} \| ID_{D_k} \| K_R \| N_1 \| \lambda_{ijk}\right)\right)$$

3) 은행 B_i와 위임 기관 D_k 사이의 인증 및 세션키 동의

은행 B_i와 위임 기관 D_k 사이에는 α_i와 랜덤값 R_{n1}, R_{n2}을 이용하여 세션키 $SK_n = h(R_{n1} \| R_{n2} \| \alpha_i)$을 생성할 수 있다. 그 단계는 3단계로 위임 기관에서 α_i를 구할 때, 등록 센터 R에 문의하지 않고 바로 구할 수 있다.

1단계: $B_i \rightarrow D_k$: N_2 , ID_{Bi}

$$E_{\alpha_i}\left(R_{n1}, h\left(N_2 \| ID_{B_i} \| ID_{D_k} \| R_{n1}\right)\right)$$

2단계: $D_k \rightarrow B_i$: N_3

$$E_{\alpha_i}\left(R_{n2}, h\left(N_2 \| N_3 \| ID_{B_i} \| ID_{D_k} \| R_{n2}\right)\right)$$

3단계: $B_i \rightarrow D_k : E_{SK_n}(N_3+1)$

4) 은행 B_i와 은행 B_j 사이의 인증 및 세션키 동의

은행 B_i와 은행 B_j 사이의 세션키를 만들기 위해 공유키 λ_{ijk}를 이용하기 앞서 랜덤값 R_{n1}, R_{n2}를 인증해야 한다. 그 과정은 다음과 같다.

1단계: $B_i \rightarrow B_j : N_4, ID_{Bi}\ ID_{Bj}$

$$E_{\lambda_{ijk}}\left(R_{n1}, h\left(N_4 \| ID_{B_i} \| ID_{B_j} \| R_{n2}\right)\right)$$

2단계: $B_j \rightarrow B_i : N_5$

$$E'_{\lambda_{ijk}}\left(R_{n2}, h\left(N_4 \| N_5 \| ID_{B_i} \| ID_{B_j} \| R_{n2}\right)\right)$$

3단계: $B_i \rightarrow B_j \quad E_{SK_n}(N_6+1)$

이러한 인증 과정을 마친 후, 세션키 $SK_n = h(R_{n1} \| R_{n2} \| \lambda_{ijk})$을 계산한다.

4.2 비밀키 갱신 프로토콜

결제자가 이전의 은행 B_i 영역에서 은행 B_j 영역으로 옮겼다고 가정하면, 이전에 사용했던 은행과 위임 기관과의 비밀키를 갱신해야만 한다. 키 갱신이 필요한 은행 B_i가 위임기관 D'_k에 키 갱신 정보 K_{update}와 함께 ID_{Bi}, ID_{Dk}를 비밀키 α_i로 암호화하여 전송한다. 전송 받은 위임 기관은 비밀키 α_i로 복호화 할 수 있고 공유키와 세션키를 생성할 수 있다. 만약 ID_{Dk}가 틀린 경우, D'_k는 등록 센터 R에 재등록을 요청한다. 등록 센터 R은 $\alpha_i' = h(\delta_k' \| ID_{Bi})$를 계산하여 은행의 이전 비밀키 α_i로 암호화한다. 위임 기관 D'_k에게는 δ_k'로 암호화하여 전송한다. D'_k는 δ_k'로 복호화한 후 다음과 같은 메시지를 B_i에게 전송한다.

$$E_{\alpha_i}(\alpha_i', ID'_{Dk}, h(ID_{Bi} \| ID'_{Dk} \| N_1 \| \alpha_i'))$$

은행 B_i는 비밀키 α_i로 복호화 한 뒤 새로운 α_i'와 ID'_{Dk}를 얻어 이 메시지를 갱신할 수 있다. 그 과정은 다음과 같다.

1단계: $B_i \rightarrow D'_k : N_1, ID_{Bi}, ID_{Dk}, K_{update}$

$$E_{\alpha_i}(ID_{Bi}, ID_{Dk})$$

2단계: $D'_k \rightarrow R : N_1, N_2, ID_{Bi}, ID_{Dk}, ID'_{Dk}, K_{update}$

$$E_{\delta'_k}(E_{\alpha_i}(ID_{Bi}, ID_{Dk}), ID'_{Dk})$$

3단계: $R \rightarrow D'_k : E_{\delta'_k}(K_{update}, h(ID'_{Dk} \| N_2))$

$E^{-1} = E_{\alpha_i}(\alpha_i', ID'_{Dk}, h(ID_{Bi} \| ID'_{Dk} \| N_1 \| \alpha_i'))$

4단계: $D'_k \rightarrow B_i :$

$E^{-1} = E_{\alpha_i}(\alpha_i', ID'_{Dk}, h(ID_{Bi} \| ID'_{Dk} \| N_1 \| \alpha_i'))$

5단계: $B_i : \alpha_i \leftarrow \alpha_i', ID_{Dk} \leftarrow ID'_{Dk}$

은행 B_i가 안전하게 키를 갱신할 수 있는 것은, 은행 B_i가 보낸 ID_{Bi}, N_1 정보를 인증할 수 있는 α_i를 가진 등록 센터 R과 이전의 D_k이다. 그러나 키 갱신 이전에는 은행 B_i와 위임기관 D_k와는 통신이 되지 않으므로 등록 센터 R 만이 키를 갱신할 수 있다. 따라서 D'_k 조차도 α_i를 알지 못하므로 인증된 α_i'를 전송할 수 없다. 그리고 D'_k도 자신이 보낸 ID'_{Dk}, N_2 정보를 인증할 수 있는 $h(ID'_{Dk} \| N_2)$를 만들 수 있는 유일한 객체는 δ_i'를 가진 R 뿐이므로 R에 대한 인증을 할 수 있다.

5. 성능 분석

Li Xi, Hu Han-ping 프로토콜[10]에서는 안전하고 편리한 결제 메커니즘을 제공할 뿐만 아니라 모바일 결제 프로토콜과 안전성 문제를 고려하였지만 모바일 결제를 위한 은행들간의 인증이 제시되지 않았다. 따라서 본 논문에서는 은행들을 인증할 위임 기관을 두어 인증 및 키 동의 프로토콜과 비밀키 갱신 프로토콜을 제시하였다. 이러한 프로토콜을 분석하면 다음과 같다.

5.1 안전성 분석

정보 보호 서비스는 기밀성, 인증, 무결성, 신규성 등으로 나누어 볼 수 있으며, 이러한 서비스들은 도청에 의한 비밀키 공격[11], 중간자 공격[12]에 의한 인증 침해, 변조 공격[13] 등에 의한 무결성 침해, 그리고 재전송 공격[14] 등에 의한 신규성 침해를 받을 수 있다. 따라서 제안된 프로토콜의 저항성을 분석하면 다음과 같다.

- 도청에 의한 비밀키 공격

공격자는 도청 정보로부터 공유키인 α_i와 λ_{ijk}를 계산할 수 없으며, 이를 알지 못하면 암호화되어 전송되는 R_{n1}, R_{n2}을 알지 못한다. 그러므로 은행들간의 설정된 세션키를 사용하여 데이터를 암호화하면 기밀성을 제공할 수 있다.

- 중간자 공격

중간자 공격은 제 3자가 두 통신자를 속여 인증하거나 비밀 정보를 획득하거나 변조된 정보를 전송하는 공격이다. 제안 방식의 세션 키 설정 과정은 ID와 랜덤값 R_{n1}, R_{n2}을 각각 해쉬한 후 공유키로 인증하여 사용함으로 불법적인 중간자 공격은 불가능하다.

- 변조 공격

변조 공격은 공격자가 데이터를 변조하는 공격으로서, 공격자는 은행과 위임 기관간의 공유키 α_i나 은행간의 공유키 λ_{ijk}를 계산할 수 없어 암호화되어 전송되는 메시지를 변조할 수 없다.

- 재전송 공격

재전송 공격은 공격자가 이전에 사용된 정보들을 다시 사용하여 인증 및 키 동의를 얻는 공격이다. 공격자는 은행과 위임 기관 혹은 은행들간 통신에서 사용된 신규성을 위한 파라미터 N_i가 암호화된 메시지를 매번 다르게 전송하므로 재전송 공격을 할 수 없다.

5.2 시뮬레이션 분석

은행들을 신뢰할 수 있는 위임 기관을 둠으로써 이들을 인증하는 키 동의에 필요한 시간 복잡도(time complexities)와 통신 장애 허용성(communication resilience)을 구하기 위한 시뮬레이션을 시행하였고, 이를 위하여 NS-2 시뮬레이터[15]를 사용하였다. 제안한 위임 기관은 은행 인증 뿐만 아니라 결제 ID에 대한 검증도 수행한다. 이러한 위임 기관은 한번의 결제 거래 프로토콜에서 상인이 결제 ID 검증 요청 시, 이미 발행 은행 인증을 마친 후 발행 은행이 결제 게이트웨이의 상인에게 결제에 대한 권한 부여를 하였으므로 결제 ID에 동의만 하면 된다. 따라서 본 시뮬레이션은 위임 기관의 발행 은행 인증만을 분석하였다.

이전 프로토콜의 시뮬레이션을 위하여 SK_n, R_{n1}, R_{n2}, N_i, x, K_R에 각각 64bits, h를 위하여 256bits를 할당하고 제안한 프로토콜 시뮬레이션을 위하여 ID_{Bi}, ID_{Dk}, P_{Bi}, S_{Kn}, R_{n1}, R_{n2}, N_i, x, K_R에 각각 64bits, δ_k, α_i, μ_{ik}, λ_{ijk}를 위하여 160bits, h를 위하여 256bits를 할당한다. 인증 키 계산을 위한 데이터 전송 간격을 0.2초, 0.4초, 0.6초, 0.8초, 1초로 변경하면서 600초 동안 시행하여 한번의 결제 시 가상 은행 노드 수를 시뮬레이션한 결과의 평균 시간 복잡도를 나타낸 것이 그림 5이다.

제안한 프로토콜의 인증과 키 동의에 필요한 비트 할당 요소보다 많지만 평균 시간 복잡도는 이전 프로토콜 시간 복잡도보다 낮은 것으로 나타났다. 이는 위임 기관을 둠으로써 신뢰할 수 있는 은행을 찾을 때 시간이 단축된다는 의미로 위임 기관이 없는 경우 신뢰할 수 없는 은행과 연결되면 신뢰할 수 있는 은행을 찾을 때까지 걸리는 시간이 비트 할당 요소를 찾아 진행하는 시간보다 더 많이 걸린다는 것을 알 수 있다.

제안한 프로토콜의 통신 장애 허용성은 그림 6에서 위임 기관을 둔 프로토콜과 위임 기관을 두지 않은 프

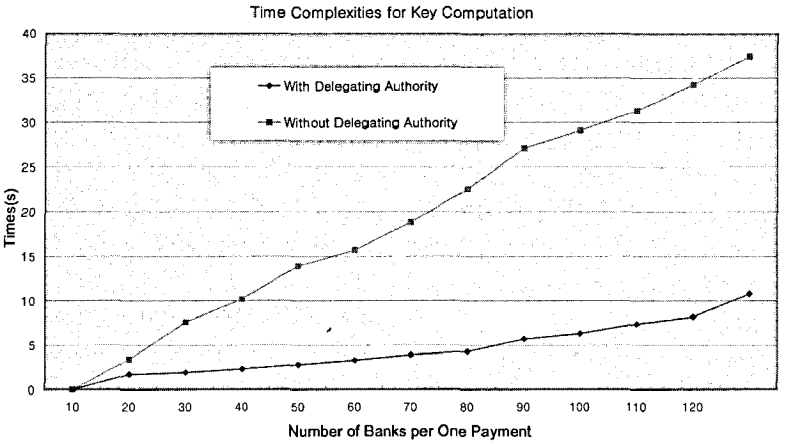

그림 5 Time Complexities for Key computation

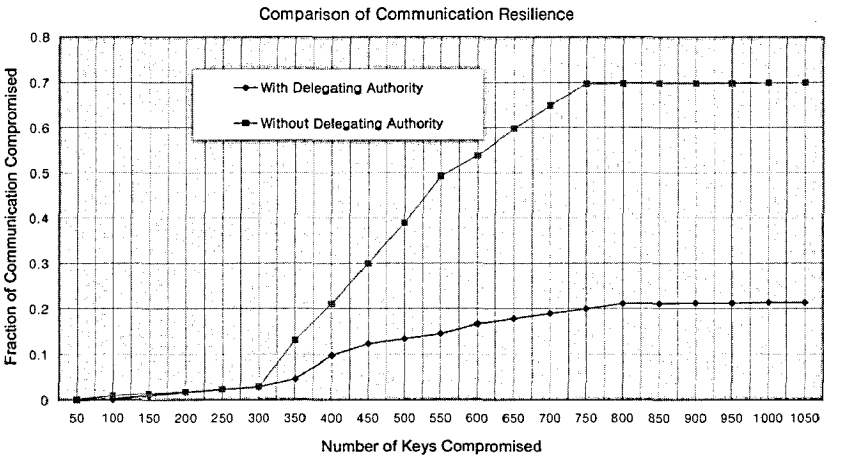

그림 6 Comparision of Communication Resilience

로토콜을 비교한 결과, 손상된 키가 300개 이상일 때 현저한 차이를 보이기 시작하다가 손상된 키가 800개 이상일 때 손상된 통신 비율이 일정 비율로 수렴함을 보이며, 위임 기관을 둔 프로토콜의 통신 장애 허용성이 위임 기관을 두지 않은 프로토콜의 통신 장애 허용성보다 높은 결과를 보인다.

6. 결 론

모바일 결제 시스템은 크게 모바일 사용자, 콘텐츠 제공자, 결제 서비스 제공자로 이루어진다. 이러한 모바일 결제 시스템의 안전한 결제 프로토콜을 위한 발행 은행 결제 검증을 위한 위임 기관을 제안하였다. 그 결과 Li Xi, Hu Han-ping 프로토콜[10]에서 제안한 모바일 결제 프로토콜보다 안전성과 효율성이 향상되었을 뿐만 아니라 부가적인 서버가 필요 없게 되었다. 또한 모바일 전자 거래를 위한 인터넷 결제, 카드 없는 결제 시스템 등에 응용될 수 있다.

그러나 제안한 위임 기관이 여러 개일 경우, 신뢰된 제 3기관으로서의 키 동의 문제점을 해결해야 한다.

참 고 문 헌

[1] T. Weitzel, W. Konig, "Vom E-zum M-Payment" (in German), http://much-magic.wiwi.unifrankfurt.de/profs/mobile/infos.html

[2] Jean-Michel sahut and Malgorzata Galuszewska, "Electronic payment market:A non-optimal equilibrium," *Proceedings of the 2004 International Symposium on Applications and the Internet Workshops(SAINTW'04)*, pp.3-8, 2004.

[3] Antovski, L. and Gusev, M., "M-payments," *Proceedings of the 25th International Conference information Technology Interfaces(ITI'03)*, pp.95-100, 2003.

[4] Agnieszka Zmijewska, "Evaluating wireless technologies in mobile payments-A customer centric approach," *Proceedings of the International Conference on Mobile Business(ICMB'05)*, pp.354-362, 2005

[5] Ondrus, J. and Pigneur, Y., "A distruption analysis in the mobile payment market," *Proceedings of the 38th Hawaii International Conference on System Sciences(HICSS-38'05)*:84c-84c, 2005.

[6] Ashutosh Saxena, Manik Lal Das and Anurag Gupta, MMPS: "A versatile mobile-to-mobile payment system," *Proceedings of the International Conference on Mobile Business(ICMB'05)*, pp.400-405, 2005.

[7] Delic, N. and Vukasinovic, Ana., "Mobile payment solution-symbiosis between banks, application service providers and mobile network operators," *Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06)*, pp.346-350, 2006.

[8] Ondrus, J., Camponovo, G., Pigneur, Y., "A proposal for a multi-perspective analysis of the mobile payment environment," *Proceedings of the International Conference on Mobile Business(ICMB'05)*, pp.659-662, 2005.

[9] Nambiar, S. and CHANG T. L., "M-payment solutions and m-commerce fraud management," Available at: http://europa.nvc.cs.vt.edu/~ctlu/Publication/M-Payment-Solutions.pdf, September 9, 2004.

[10] Li Xi, Hu Han-ping, "A secure mobile payment system," *Computer Technology and Application*, ISSN1934-7332, vol.1, no.1, June 2007.

[11] S. Bellovin and M. Merritt, "Encrypted Key Exchanged: Password-Based Protocols Secure Against Dictionary Attacks," In *Proc. of IEEE Symposium on Research in Security and Privacy*, pp.72-84, 1992.

[12] W. Stallings, Cryptography and Network Security, 4th Edition, Prentice Hall International, 2007.

[13] C. Yang, T. Chang and M. Hwang, "Cryptanalysis of Simple Authenticated Key Agreement Protocols," *IEICE Trans. Fundamentals*, vol.E87-A, no.8, pp. 2174-2176, 2004.

[14] P. Syverson, "A Taxonomy of Relay Attacks," In *Proc. of Computer Security Foundations Workshop VII*, pp.187-191, 1994.

[15] S. McCanne and S. Floyd, "NS network simulator," URL: http://www.isi.edu/nsnam/ns

성 순 화

1983년 경북대학교 전자공학과(전산학)(공학사). 2000년 한남대학교 컴퓨터공학과(공학석사). 2005년 충남대학교 컴퓨터공학과(공학박사). 2000년~2004년 대덕대학 겸임교수. 2002년~2005년 충남대학교 시간강사. 2006년 충남대학교 부설 정보통신연구소 연구원. 2006년~현재 충남대학교 차세대통신인력양성사업단 BK전임교수. 관심분야 정보 보안, 유비쿼터스 컴퓨팅 보안, 유무선 인터넷 보안, 유무선 인터넷 트래픽 솔루션, 차세대 인터넷을 위한 사용자 인증 시스템