2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

M-Commerce를 위한 고액지불시스템

임수철*, 김선형*, 강혁*, 김태윤*
*고려대학교 컴퓨터학과
e-mail:causal@netlab.korea.ac.kr

A Macropayment for M-Commerce

Soo-Chul Lim*, Sun-Hyoung Kim*,
Hyeok Kang*, Tai-Yun Kim*
*Dept of Computer Science & Engineering, Korea University

요약

현재 m-commerce를 위한 지불시스템 연구는 인터넷에서 사용하는 소액지불기법을 무선환경에서 사용할 수 있도록 하는 연구가 주를 이루고 있다. 그러나 다양한 서비스 제공을 위해서는 소액지불기법 뿐만이 아닌 고액지불기법도 필요하다. 본 논문에서는 m-commerce에서 상품 구매나 다양한 서비스를 제공할 수 있도록 고액지불시스템을 제안한다. 고액지불 수행을 위해 신용카드를 사용한다. 또한 안전한 지불을 수행할 수 있도록 공개키 암호 시스템을 사용한다.

1. 서론

m-commerce는 무선인터넷상에서 무선 또는 이동 단말기를 사용해 서비스를 제공받거나 상품을 구매하는 것이다[1]. 인터넷을 사용하는 전자상거래에 비해 m-commerce는 이동 통신의 장점인 이동성을 가지고 다양한 서비스를 제공할 것이다. m-commerce에서 다양한 서비스를 제공받기 위해서는 서비스의 특성에 알맞은 지불시스템이 필요하다.

현재 m-commerce를 위한 지불시스템 연구는 인터넷에서 사용하는 소액지불기법을 무선환경에서 사용할 수 있도록 하는 연구가 주를 이루고 있다[2]. 그러나 다양한 서비스 제공을 위해서는 소액지불기법 뿐만이 아닌 고액지불기법도 필요하다.

본 논문에서는 m-commerce에서 상품 구매나 다양한 서비스를 제공할 수 있도록 고액지불시스템을 제안한다. 고액지불 수행을 위해 신용카드를 사용한다. 또한 안전한 지불을 수행할 수 있도록 공개키 암호 시스템을 사용한다.

본 논문의 구성은 다음과 같다. 2장에서는 소액지불시스템인 PayWord를 기술하고 3장에서는 고액지불시스템은 신용카드 지불시스템을 제안한다. 4장에서는 성능평가를 하고, 마지막 5장에서는 결론 및 향후 연구과제를 기술한다.

2. PayWord

PayWord[3]는 공개키 연산의 서명과 해쉬체인을 응용한 대표적인 소액지불시스템이다. PayWord는 공개키 연산의 최소화, 온라인 인증의 사용을 지양하여 연산의 효율성을 얻을 수 있어 m-commerce를 위한 소액지불시스템 연구에 기초가 되는 소액지불시스템이다.

PayWord 해쉬체인은 사용자 U가 생성한다. 이를 생성하기 위해서 U는 n번째 PayWord로 나머지 PayWord 체인을 생성하기 위한 값 w_n을 랜덤하게 생성하며, 이를 사용하여 PayWord 체인을 아래와 같이 생성한다.

$$w_{i-1} = h(w_i),\ where\ i = 1, , , , , n$$

여기에서 사용된 함수는 해쉬함수(one-way and collosion-resistent)이다.

마지막으로 계산되는 w_0값은 해쉬체인의 "Root" 값으로 해쉬체인을 검증하는 값으로 체인에 포함되지 않고, U가 V에게 위탁하는 값 M에 포함된다. M은 U의 비밀키에 의해 서명된 값으로 w_0, 상점

신분 id_V, 사용자 인증서 $Cert_U$, 사용만료시간 D, 기타정보 I_M로 구성된다.

$$M = Sig_U\{w_0, id_V, Cert_U, D, I_M\}$$

U는 V와의 거래를 위하여 사전에 브로커로부터 인증서 $Cert_U$를 받아야 한다.

PayWord의 지불 프로토콜 흐름은 그림 1과 같다.

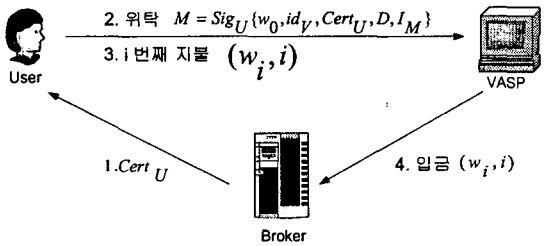

그림 1. PayWord 지불 처리 흐름

PayWord는 그림 1과 같이 지불을 수행하기 위해 전송하는 데이터 횟수가 적고, 전송하는 데이터의 용량도 적다. 따라서 PayWord를 m-commerce에서 사용할 수 있도록 많은 연구를 한다.

그러나 PayWord의 안전성은 공격자의 공격 비용이 실제 거래량보다 비싼 경우 효용이 없음을 기본으로 하고 있다. 따라서 거래량이 공격자의 공격 비용보다 비싼 고액지불의 경우에는 안전성에 위험이 있다.

본 논문에서는 m-commerce에서 고액지불이 가능하도록 신용카드를 사용하고, 전송되는 신용카드 정보를 보호하기 위해서 공개키 암호 시스템을 사용한다.

3. 제안하는 신용카드 지불 프로토콜

제안한 지불 프로토콜은 고액지불을 위해 신용카드를 사용한다. 무선환경에서 신용카드 정보를 보호하기 위해서 공개키 암호 시스템을 사용한다. 공개키 암호 시스템은 무선 이동 통신에 적합하지 않았으나, 적은 비트 수와 빠른 계산 속도를 보장하는 타원 곡선 공개키 암호 시스템으로 인하여 무선 이동 통신에 공개키 암호 시스템을 사용할 수 있게 되었다[4].

제안한 지불 프로토콜의 안전성은 유한체(finite field)의 곱셈군(multiplicative group) 또는 타원 곡선의 부분군(subgroup)과 같은 유한군 G와 생성원 g에서 이산 대수 문제(discrete logarithm problem)[5]가 어렵다는 가정을 근거로 한다. 또한 각 참여자와의 세션키(session key) 설정은 Diffie-Hellman 키 설정[6] 방식을 사용한다. 제안한 프로토콜에서 U는 사용자, V는 상품/서비스 제공자(VASP), CA는 인증기관, PG는 Payment Gateway를 의미한다. $h(\cdots)$은 일방향 해쉬함수이고, $Sig_X(\cdots)$은 X의 개인키를 사용하여 메시지를 서명한 것이다. $\{\cdots\}_K$은 X와 Y가 공유하는 세션키(K)를 사용하여 암호화한 것이다. 사용한 데이터 요소는 표1과 같다.

표 1. 제안한 지불 프로토콜에서 사용한 데이터 요소

데이터 요소	설 명
id_X	X의 신원
x	X의 개인키
g^x	X의 공개키
K_{XY}	X와 Y가 공유하는 세션키
TX	X에 의해 생성된 타임스탬프
ch_{data}	지불정보를 의미하며, 상품이나 서비스 명칭과 수량이 포함된다.
$card_{data}$	신용카드 정보를 의미한다.

각 참여자는 프로토콜에서 사용되는 알고리즘을 알고 있어야 하며, U는 PG와 공유하는 세션키를 가지고 있어야 한다. 또한 무선단말기의 스마트카드에 저장되어 있는 신용카드 정보는 무선환경에서 사용할 수 있도록 신용카드사와 미리 협정한 정보이다.

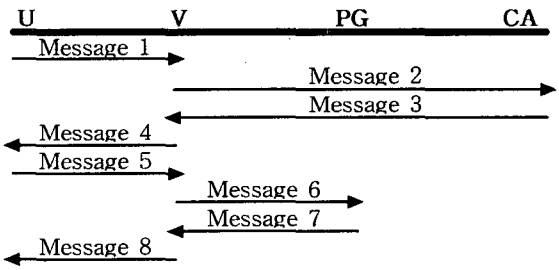

그림 2. 제안한 신용카드 지불 프로토콜의 흐름도

그림 2는 제안한 신용카드 지불 프로토콜의 흐름도이다.

• Message 1

$$g^u \| \{id_U\}_{K_{UC}} \| id_{U\_C} \| data$$

제안한 지불 프로토콜은 U가 V에 접속하는 것으로 시작된다. U는 난수 u를 생성하고 키 설정용 임시 공개키 g^u를 계산한다. 그리고 CA의 공개키 g^c를 이용하여 세션키 $K_{UC}=(g^c)^u$를 생성한다. U는 자신의 공개키와 세션키를 사용하여 암호화한 신원 id_U, U의 CA 신원 id_{U_C}, 선택한 서비스의 정보 $data$를 V에게 전송한다.

• Message 2

$$g^u \| \{id_U\}_{K_{UC}} \| Cert_V$$

V는 U가 전송한 메시지와 자신의 인증서 $Cert_V$를 온라인 인증기관인 CA에게 전송한다.

• Message 3

$$TCA \| CertChain(U, V) \| \{CertChain(V, U)\}_{K_{UC}} \| CertChain(V, CA) \| \{Sig_{CA}(h(g^u \| cid_U \| cid_V \| TCA))\}_{K_{UC}}$$

CA는 V에게 받은 메시지에서 $Cert_V$를 사용하여 U가 V의 공개키를 검증할 수 있도록 $CertChain(U, V)$를 생성한다. 또한 V가 U와 CA의 공개키를 확인할 수 있도록 $CertChain(V, U)$와 $CertChain(V, CA)$을 생성하여 V에게 전송한다. 이때 $CertChain(V, U)$은 U와의 세션키를 사용하여 암호화해서 전송하는데 이는 악의적인 VASP 재전송 공격[4]을 막기 위해서이다.

• Message 4

$$r \| h(K_{UV} \| r \| id_V) \| ch_{data} \| TCA \| CertChain(U, V) \| \{Sig_{CA}(h(g^u \| cid_U \| cid_V \| TCA))\}_{K_{UC}}$$

V는 난수 r을 생성한 후 첫 번째 메시지에서 받은 U의 키 설정용 임시 공개키를 사용하여 세션키를 생성한다. 세션키는 Diffie-Hellman 키 교환 방법을 변형한 형태인 $K_{UV}=h((g^u)^v \| r)$으로 생성한다. 그리고 해쉬값을 계산하여 지불 명세서와 CA가 서명한 데이터를 함께 전송한다.

• Message 5

$$\{Sig_U(h(g^u \| g^v \| r \| id_V \| TCA \| ch_{data})) \| K_{UC}\}_{K_{UV}} \| \{Sig_U(h(id_U \| id_V \| TU \| ch_{data} \| card_{data})) \| TU \| ch_{data} \| card_{data}\}_{K_{UP}}$$

U는 $CertChain(U, V)$를 통해서 V의 공개키를 얻고, 이를 사용하여 V와의 세션키를 계산한다. 그리고 해쉬값을 계산하여 V에게 전송받은 해쉬값과 비교한다. 지불 명세서와 타임스탬프 TCA를 확인한 후 V에게 인증확인 메시지와 CA와의 세션키를 전송한다. 또한 서비스에 대한 지불로써 신용카드 정보 $card_{data}$가 포함되어 있는 메시지를 PG와의 세션키를 사용하여 암호화하여 V에게 전송한다.

• Message 6

$$\{id_U \| id_V \| ch_{data}\}_{K_{VP}} \| \{Sig_U(h(id_U \| id_V \| TU \| ch_{data} \| card_{data})) \| TU \| ch_{data} \| card_{data}\}_{K_{UP}}$$

V는 U가 전송한 메시지에서 K_{UC}을 구하여 $CertChain(V, U)$을 확인한다. 그리고 U가 서명한 메시지를 확인하고, PG에게 전송할 메시지 $\{id_U \| id_V \| ch_{data}\}_{K_{VP}}$를 생성하여 신용카드 정보가 포함되어 있는 U가 서명한 메시지를 PG에게 함께 전송한다.

• Message 7

$$\{Sig_{PG}(h(id_U \| id_V \| TP \| ch_{data}))\}_{K_{VP}} \{Sig_{PG}(h(id_U \| id_V \| TP \| ch_{data}))\}_{K_{UP}}$$

PG는 U와 V가 보낸 메시지를 확인하여 지불 명세서 ch_{data}를 비교하고 동일하면 신용카드 정보 $card_{data}$를 사용하여 지불처리를 행한다. U가 보낸 신용카드 정보로 성공적으로 지불이 처리되면 거래에 참여한 참여자 id_U, id_V와 지불처리가 수행된 시간 TP, 지불 명세서 ch_{data}의 해쉬값에 서명하여 암호화한 메시지를 V에게 전송하고, V를 통하여 U에게도 전송된다.

• Message 8

$$\{Sig_{PG}(h(id_U \| id_V \| TP \| ch_{data}))\}_{K_{UP}}$$

이 과정이 수행되면 V는 U가 선택한 상품이나 서비스를 제공하게 된다.

4. 프로토콜 분석

- V에 대한 키 확인과 인증 : 네 번째 메시지에 $h(K_{UV} \| r \| id_V)$를 첨가하는 것은 V가 U에게 키 확인과 V의 함축적 키 인증성과 개체인증을 제공하기 위함이다.
- U에 대한 키 확인과 인증 : 다섯 번째 메시지의 인증서 $Cert_U$를 세션키 K_{UV}로 암호화하는 것은 키 확인을 제공한다. 또한 해쉬함수에 $g^u \| g^v \| r$을 첨가하는 것은 U에서 V에게 함축적 키 인증성을 제공하기 위함이다. 난수 r의 첨가는 U에 대한 개체인증을 제공한다.
- 재전송 방지 : V로부터 생성된 난수 r은 K_{UV}의 생성에 필요한 하나의 요소이다. 이는 이전에 사용되었던 K_{UV}가 재 사용되는 것을 방지하기 위함이다. 난수 r과 U로부터 생성된 난수 u는 세션키가 새로운 키(key freshness)임을 증명한다.
- 부인 방지 : U의 전자 서명은 서명된 데이터의 부인 방지를 제공한다. 또한 제안한 프로토콜의 맨 마지막 메시지는 거래와 지불에 대한 부인 방지를 제공한다.
- 서명의 암호화 : 전자 서명은 두 가지 이유에 의해서 암호화가 된다. 첫째, 서명자가 세션키를 알고 있다는 것을 보장하기 위함이다. 둘째, 사용자의 익명성을 보장하기 위함이다. 만약 서명이 암호화되지 않는다면, 공격자는 서명을 검증함으로써 U의 신원을 파악할 수 있다. 만약 공격자가 사용자들의 공개키에 접근이 가능하고 서명자가 충분히 작은 그룹에 속한다는 것을 알 수 있다면 이 같은 공격은 가능하다.
- V의 신원을 두 번째 메시지에 포함 : 두 번째 메시지에 V의 신원을 포함하는 것은 근원지 대체 공격(source-substitution attack)[4,7]을 방지하기 위함이다.
- V의 신원을 세 번째 메시지에 포함 : 이는 서명의 정당한 수신자를 나타내기 위하여 id_V를 포함하는 것이다.

5. 결론

본 논문에서는 m-commerce에서 고액지불을 할 수 있도록 공개키 암호 시스템을 사용한 신용카드 지불 프로토콜을 제안하였다. 제안한 지불 프로토콜은 현재 사용중인 이동통신 단말기에는 적합하지 않으나, 충분한 저장공간과 연산량을 가지고 있는 무선단말기나 스마트 카드를 장착한 이동통신 단말기에는 적합하다.

참고문헌

[1] Lyytinen, K., "M-commerce - mobile commerce: a new frontier for E-business", System Sciences, Proceedings of the 34th Annual Hawaii International Conference on, pp.3509 -3509, 2001.

[2] 이만호, 김광조, "이동컴퓨팅 환경을 위한 소액지불시스템", 한국정보보호학회 종합학술발표회 논문집, Vol.11, No.1, pp.181-184, 2001.

[3] R. Rivest, A. Shamir, "PayWord and MicroMint : Two Simple Micropayment Schemes", Proc. of 1996 Int. Workshop on Security Protocols, LNCS 1189, pp.69-87, 1996.

[4] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems", ESORICS, LNCS 1485, pp.277-293, 1998.

[5] A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.

[6] W. Diffie, M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp.472-492, Nov. 1976.

[7] ACTS AC095, "ASPeCT Deliverable D20, Project final report and results of trials", Dec. 1998