무선인터넷에서의 사용자 익명성을 제공하는 신용카드 기반 지불 프로토콜

임수철° 김정범 김선형 박복녕 김태윤
고려대학교 컴퓨터학과
{causal°, qston, shaklim, happy, tykim}@netlab.korea.ac.kr

A Payment Protocol Based on Credit Card Assuring User Anonymity of Wireless Internet

Soo-Chul Lim° Jeong-Beom Kim Sun-Hyoung Kim Bok-Nyong Park Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

무선인터넷에서 다양한 서비스를 지원하기 위해서는 서비스의 특성에 알맞은 지불 프로토콜이 필요하다. 본 논문에서는 신용카드를 사용한 지불 프로토콜의 익명성 제공을 위한 임시 사용자 인증서를 사용하여 신용카드 지불 프로토콜을 제안하였다.

1. 서 론

무선인터넷의 발달과 사용자들의 증가로 인해 서비스의 종류가 다양해졌으며, 서비스의 질 또한 향상되고 있다. 서비스 종류의 다양화로 서비스에 적합하도록 많은 지불 프로토콜들이 연구되고 있다. 다양해지는 서비스로 인해 지불 프로토콜이 만족시켜야할 요구사항들도 달라지고 있다. 요구되는 여러 사항 중에 사용자의 익명성은 보안과 개인 정보 노출이라는 양면성을 지니고 있다.

따라서 사용자의 익명성은 제공받는 서비스의 종류에 따라서 부분적으로 제공하는 방법을 사용한다. 무선인터넷을 이용하여 상품을 구매한다면, 상품을 받을 수 있는 주소를 알려야하므로 사용자의 개인 정보가 서비스 제공자에게 노출된다. 그러나 실질적인 상품이 아닌 디지털 컨텐츠나 서비스를 받는다면 사용자의 개인 정보를 노출시킬 필요는 없다.

[1]에서 제안한 지불 프로토콜은 무선인터넷에서 신용카드를 이용하여 상품 구매 또는 서비스를 받을 수 있도록 하였다. [1]의 지불 프로토콜은 상품 구매와 서비스 제공을 모두 고려한 프로토콜로써 이를 사용하여 서비스 제공을 받을 때에는 불필요한 개인 정보가 노출될 우려가 있다.

따라서 본 논문에서는 [2]에서 제안한 임시 이동 사용자 인증서를 사용하여 디지털 컨텐츠나 서비스 제공시에 사용자 익명성을 제공하는 무선인터넷에서의 사용자 익명성을 제공하는 신용카드 지불 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로써 [1]에서 제안한 신용카드 기반의 지불 프로토콜과 임시 사용자 인증서에 관하여 기술하고, 3장에서는 임시 사용자 인증서를 사용하여 익명성을 제공하는 신용카드 기반 지불 프로토콜을 제안한다. 4장에서는 제안한 지불 프로토콜의 성능을 평가하고, 마지막 5장에서는 결론을 기술한다.

2. 관련연구

2.1 신용카드 기반 지불 프로토콜

무선인터넷에서 신용카드 기반 지불 프로토콜은 사용자 U와 서비스 제공자 V가 상호 인증을 수행하여 세션키를 공유한 후, U가 V에게 신용카드 지불 정보를 전송한다.

표 1. 신용카드 지불 프로토콜에서 사용한 데이터 요소

데이터 요소	설명
id_X	X의 신원
x	X의 공개키
g^x	X의 개인키
K_{XY}	X와 Y가 공유하는 세션키
TX	X에 의해 생성된 타임스탬프
ch_{data}	지불 정보
$card_{data}$	신용카드 정보

V는 지불 게이트웨이 PG(Payment Gateway)에게 U가 전송한 신용카드 지불 정보를 전달하여 지불요청을 하고 지불이 이루어졌다는 메시지를 PG에게 전송받은 후, U에게 서비스를 제공하는 것으로 구성되어 있다.

신용카드 지불 프로토콜에서 사용한 데이터 요소와 프로토콜이 표 1과 그림 1에 나타나있다.

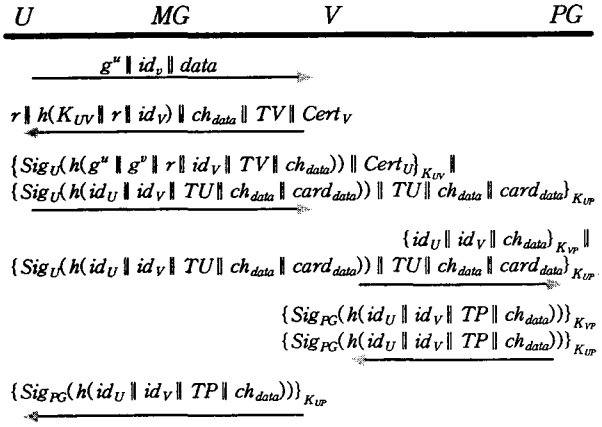

그림 1. 신용카드 지불 프로토콜

그림 1의 프로토콜은 U가 V에게 지불 정보로써, 신용카드 정보를 전송하기 전에 상호 인증을 수행한다. 이 과정에서 U는 V에게 자신의 신분을 밝혀야 한다. U가 받은 서비스가 상품 구매를 하여 U가 상품을 배달받아야 하는 경우가 아닌 단순한 서비스를 받을 경우까지 사용자의 신원을 밝혀야 한다.

2.2 임시 이동 사용자 인증서

[2]에서 제안한 임시 이동 사용자 인증서는 ASPeCT의 AIP(Authentication and Initialization of Payment) [3] 프로토콜에서 이동 사용자가 외부 도메인의 서비스 제공자에 인증서를 검증할 수 있는 공개키를 보다 효율적으로 공유할 수 있도록 한 것이다. 임시 이동 사용자 인증서 발급은 다음과 같은 단계로 이루어진다.

그림 2에서 U는 사용자, N은 네트워크 운영자, TN은 네트워크 운영자의 신뢰기관, TU는 사용자의 신뢰기관이다.

그림 3의 프로토콜을 수행한 후, U는 TN이 발급한 임시 이동 사용자 인증서를 사용하여 N의 도메인에서 서비스를 받을 수 있다.

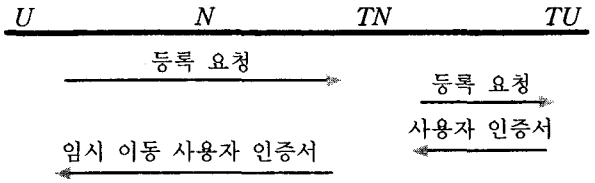

그림 2. 임시 이동 사용자 인증서 발급 프로토콜 모델

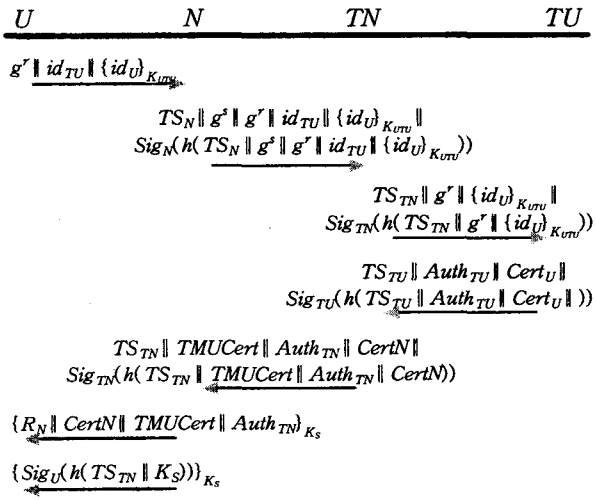

그림 3. 임시 이동 사용자 인증서 발급 프로토콜

3. 익명성을 제공하는 신용카드 기반 지불 프로토콜

신용카드 기반 지불 프로토콜에 사용자의 익명성을 제공하기 위해 임시 이동 사용자 인증서를 발급받아 서비스 제공자와의 상호 인증을 수행한다.

제안한 지불 프로토콜은 임시 이동 사용자 인증서를 발급 받기 위해 그림 3과 같이 수행한다. 제안한 프로토콜에서 MG(Mobile Gateway)가 임시 이동 사용자 인증서 프로토콜에서는 N처럼 동작한다. 따라서 U는 MG를 통해 등록 요청을 하고, MG의 신뢰기관인 TN (TMG)이 사용자의 신뢰기관에게 확인 요청을 수행하여 $TMUCert$라는 임시 이동 사용자 인증서를 발급받는다.

신용카드 지불 프로토콜을 수행하기 전에 사용자는 외부 도메인의 신뢰기관으로부터 임시 인증서를 발급받아야한다.

임시 인증서를 사용하여 사용자의 익명성을 제공하는 신용카드 지불 프로토콜은 그림 4와 같다.

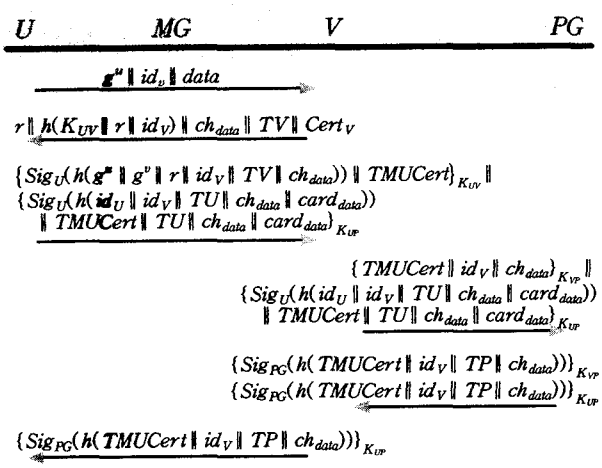

그림 4. 익명성을 제공하는 신용카드 지불 프로토콜

제안한 사용자 익명성을 제공하는 프로토콜은 *TMUCert*를 사용하여 [4]에서 제안한 익명성 단계 중 제 2단계에 해당하는 익명성을 제공할 수 있다. 그림 4에 나타나 있는 지불 프로토콜은 컨텐츠를 제공받거나 서비스를 제공받을 때 서비스 제공자가 사용자의 신원을 알 수 없다. 다만, 사용자가 서비스 제공자의 신뢰기관으로부터 받은 임시 이동 사용자 인증서를 통해 정당한 사용자임을 확인 할 수 있게된다.

4. 성능 평가

본 장에서는 제안한 사용자 익명성을 제공하는 신용카드 지불 프로토콜의 성능을 평가한다. 성능 평가는 제안한 지불 프로토콜과 [1]에서 제안한 지불 프로토콜을 비교한다. 성능 평가 비교 결과는 표 2와 같다.

표 2. 신용카드 지불 프로토콜의 성능 비교

	익명성 제공하지 않는 프로토콜	익명성 제공하는 프로토콜
임시 인증서	×	○
로밍 지원	○	○
익명성 제공	×	○
메시지 횟수	6	6

(○ : YES, × : NO)

두 프로토콜은 동일한 메시지 횟수의 메시지를 전송하여 지불을 수행한다. 또한 로밍을 지원한다. [1]에서 제안한 지불 프로토콜은 ASPeCT의 AIP 프로토콜과 같이 인증 과정에 온라인 신뢰기관이 참여하는(인증 체인을 사용하여 인증하는 방식) 방법을 사용하여 로밍을 지원할 수 있다. 또한 제안한 지불 프로토콜은 임시 사용자 인증서를 사용하여 익명성을 제공하지만, 서비스 제공자에게 서비스를 받고 지불을 수행하기 위해서는 임시 사용자 인증서를 받는 전처리 과정이 필요하다는 문제점을 가지고 있다.

5. 결론

무선인터넷에서 다양한 서비스를 지원하기 위해서는 서비스의 특성에 알맞은 지불 프로토콜이 필요하다. 본 논문에서는 신용카드를 사용한 지불 프로토콜에 익명성을 제공하기 위해 임시 사용자 인증서를 사용하여 신용카드 지불 프로토콜을 제안하였다. 제안한 지불 프로토콜은 이동성이 많은 무선인터넷 사용자에게 적합하도록 로밍 서비스를 제공한다. 그러나 서비스 제공자에게 서비스를 받기 위해서 임시 사용자 인증서를 발급받는 전처리 과정이 필요하다는 문제점이 있다.

참고 문헌

[1] 임수철, 김정범, 이윤정, 김태윤, "무선인터넷에서의 안전한 신용카드 지불 프로토콜 설계", 한국정보과학회 봄 학술발표논문집 Vol.29, No.1, 2002.

[2] Byung-Rae Lee, Kyung-Ah Chang, Tai-Yun Kim, "Temporary Mobile User Certificate for Mobile Information Services in UMTS", IEICE TRANS. COMMUN. Vol.E83-B, No.8, 2000

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

[4] D. Samfat, R. Molva and N. Asokan, "Anonymity and Untraceability in Mobile Networks", ACM International Conference on Mobile Computing and Networking, November 1995.

[5] K. M. Martin, B. Preneel, C. J. Mitchell, H. J. Hitz, G. Horn, A. Policková, P. Howard, "Secure Billing for Mobile Information Services in UMTS", LNCS 1430, Springer-Verlag, IS&N May. 1998.