무선인터넷에서의 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜

(A Credit Card based Payment Protocol Assuring End-to-End Security in Wireless Internet)

임 수 철 † 강 상 승 †† 이 병 래 ††† 김 태 윤 ††††

(Soo-Chul Lim) (Sang-Seung Kang) (Byung-Rae Lee) (Tai-Yun Kim)

요 약 WPP 지불 프로토콜은 WAP 프로토콜을 이용하여 무선인터넷에서 신용카드 지불을 수행한다. 그러나 WPP 지불 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용함으로써 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 본 논문에서는 공개키 암호 시스템과 Mobile Gateway를 사용하여 특정 무선인터넷 플랫폼과 독립적인, 종단간 보안이 제공되는 지불 프로토콜을 제안한다. 제안한 지불 프로토콜은 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써, 이동성이 많은 무선단말기가 다른 도메인에 존재하는 서비스 제공자에게도 서비스를 받을 수 있다.

키워드 : 지불 프로토콜, 무선인터넷, 종단간 보안, 공개키 암호 시스템, 신용카드

Abstract The WPP payment protocol uses the WAP protocol to enable credit card payment on the wireless internet. Since the security of the WAP protocol is based on the WTLS security protocol, there exists an end-to-end security weakness for the WPP payment protocol. This paper is suggesting a payment protocol, which is making use of the Public-Key Cryptosystem and the Mobile Gateway, so assuring end-to-end security independently of specific protocols. As the on-line certification authority is participating on the authentication process of the payment protocol, the suggested payment protocol enables wireless devices to get services from service providers on other domains.

Key words : Payment Protocol, Wireless Internet, End-to-End Security, Public-Key Cryptosystem, Credit Card

1. 서 론

무선인터넷의 발달과 사용자 증가로 무선인터넷 전자상거래 시장이 급속하게 커지고 있으며, 제공되는 서비스가 다양해질 것으로 예상된다[1]. 다양한 서비스를 제공하기 위해서는 안전한 지불 프로토콜이 반드시 요구되며, 이를 수용하기 위해 무선인터넷의 전자상거래를 위한 지불 프로토콜이 활발하게 연구되고 있다. 이러한 연구 중, 유선환경에서 사용하는 지불시스템을 무선인터넷에서도 사용할 수 있도록 하는 연구가 가장 활발하게 진행된다.

유선환경에서 사용되는 지불 프로토콜 중, 대표적인 신용카드 지불 프로토콜인 SET(Secure Electronic Transaction)[2]는 지불에 사용되는 신용카드 정보가 안전하도록 프로토콜이 구성되어 있으며 시스템 또한 구축되어 있다. 그러나 제한적 요소가 많은 무선인터넷에는 적합하지 않다[3].

제한적 요소가 많은 무선환경에서 신용카드를 사용하여 지불 수행을 하기 위해 제안된 WPP(Wireless Payment Protocol)[3] 지불 프로토콜은 스마트카드 기술과 WAP(Wireless Application Protocol)[4]의 WTLS(Wireless Transport Layer Security)[5]를 사용한다.

WTLS를 사용하는 WAP 프로토콜 스택은 인터넷

† 학생회원 : 고려대학교 컴퓨터학과
causal@netlab.korea.ac.kr
†† 비 회 원 : 한국전자통신연구원 전자거래연구부 연구원
kss@etri.re.kr
††† 정 회 원 : 삼성전자 CTO전략실 소프트웨어센터 연구원
byungrae.lee@samsung.com
†††† 종신회원 : 고려대학교 컴퓨터학과 교수
tykim@netlab.korea.ac.kr
논문접수 : 2002년 3월 8일
심사완료 : 2002년 9월 26일

프로토콜과 서로 다르기 때문에 사용자가 직접 원하는 서버와 통신할 수 없다. 따라서 WAP에서는 무선단말기와 유선상의 서버를 연결해 줄 수 있는 다리로써 WG(WAP Gateway)를 사용한다. 그러나 WG에서 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 메시지가 노출되는 위험성을 가지고 있다[6]. WAP의 WTLS를 사용하는 WPP 지불 프로토콜은 종단간 보안을 제공하지 못해 사용자의 신용카드 정보를 보호할 수 없다.

ASPeCT(Advanced Security for Personal Communications Technologies)에서는 UMTS(Universal Mobile Telecommunications System)에서 사용자와 VASP(Value-Added Service Provider)간에 인증과 지불을 위한 AIP(Authentication and Initialization of Payment) 프로토콜을 제안하였다[7,8,9]. AIP 프로토콜은 참여자간의 안전한 세션을 제공하기 위해 공개키 암호 시스템을 사용하여 종단간 보안을 제공한다. 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[7,8].

본 논문에서는 공개키 암호 시스템을 사용하여 종단간 보안이 제공되는 신용카드 기반의 지불 프로토콜을 제안한다. 제안하는 지불 프로토콜은 종단간 보안을 제공하는 AIP 프로토콜을 기초하여 참여자간의 인증을 수행하고 신용카드 지불을 수행하기 위한 세션키(session key)를 생성한다. 생성된 세션키는 단 한 번만 사용되어야하며 이전에 사용된 세션키가 노출되어도 지불에 관련된 정보는 안전하게 보호되어야 한다. 제안하는 지불 프로토콜을 위한 시스템은 유선구간에서는 인터넷에서 신용카드 지불을 수행하기 위해 구축되어 있는 시스템을 사용하며, WPP의 WG 문제점을 극복하기 위해 지불 프로토콜에 직접 참여하지 않고 무선구간과 유선구간의 연결 기능만을 수행하는 MG(Mobile Gateway)를 사용한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 기술하고, 3장에서는 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜을 제안한다. 4장에서는 제안한 지불 프로토콜의 안전성을 분석하고, 5장에서는 제안한 지불 프로토콜의 성능 평가를 한다. 마지막으로 6장에서는 결론을 기술한다.

2. 관련연구

본 장에서는 SET 프로토콜, WPP 지불 프로토콜, API 프로토콜을 기술하고, WPP 지불 프로토콜에서 사용하는 WAP의 보안 프로토콜인 WTLS를 기술한다.

2.1 SET 프로토콜

SET는 인터넷에서 안전한 신용카드 기반의 전자상거래를 위하여 개발된 지불 프로토콜이다. SET는 안전한 지불을 수행할 수 있도록 공개키 암호 방식을 사용하며 암호 알고리즘으로 RSA와 DES를 사용한다[2].

SET는 사용자와 상품/서비스 제공자, 지불게이트웨이, 인증기관, 신용카드사로 구성된다. 프로토콜을 수행하기 전에 사용자, 상품/서비스 제공자, 지불게이트웨이는 인증기관에게 인증서를 발급 받아야 한다. SET 프로토콜은 사용자와 상품/서비스 제공자가 인증과정을 수행한 후에 그림 1과 같이 지불 과정을 수행한다.

SET 프로토콜은 공개키 암호 방식을 사용하여 종단간 보안이 제공되는 안전한 거래를 수행한다. 그러나 종단간 보안이 제공되는 안전한 거래를 하기 위해서는 프로토콜의 참여자에게 많은 저장공간과 계산량을 요구한다. 따라서 SET 프로토콜은 저장공간과 계산량, 통신량 등과 같은 사항들에 제약성을 가지고 있는 무선환경에는 적합하지 않다[3].

2.2 WPP 프로토콜

본 절에서는 WPP 프로토콜에서 사용하는 WAP의 보안 프로토콜인 WTLS와 WPP 프로토콜을 기술한다.

2.2.1 WTLS

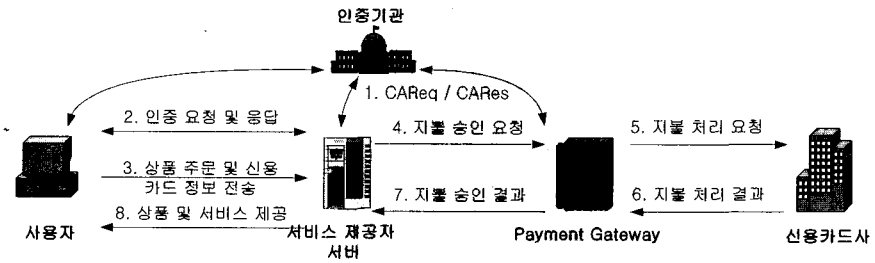

그림 1 SET 프로토콜 구성도 및 프로토콜 흐름도

WTLS는 WAP의 보안 프로토콜로서 인터넷 프로토콜에서 TCP의 보안을 위해 사용하는 TLS를 무선환경에 맞도록 최적화한 것이다. WTLS는 TLS와 마찬가지로 인증, 암·복호화, 무결성 검증 기능의 보안을 제공한다.

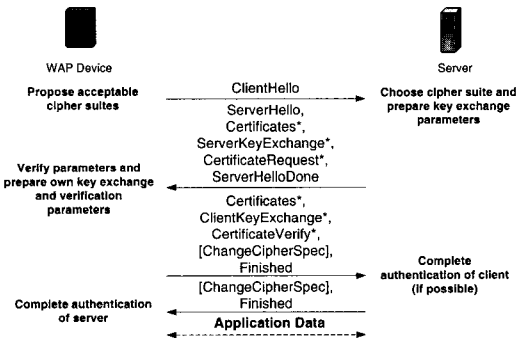

그림 2 Handshake 프로토콜

WAP 단말기와 서버가 WTLS를 이용해 지불과 관련된 메시지를 전송할 경우, 먼저 핸드쉐이크 프로토콜(Handshake Protocol)[5]을 수행하여 메시지를 안전하게 전송하는데 사용되는 세션키, 암호 알고리즘, 인증서 등과 같은 암호 매개변수를 서로 공유하게 된다. 새로운 세션을 생성하기 위해 WAP 단말기와 서버가 서로 4번의 메시지 전송을 수행해야 한다. 또한 암·복호화에 사용할 키를 생성하기 위해 master_secret을 생성한다. master_secret은 키 교환 알고리즘으로 생성된 pre_master_secret과 난수를 사용하여 생성한다[5,10,11]. 핸드쉐이크 프로토콜에서 생성된 세션 정보는 레코드 프로토콜(Record Protocol)[5]에서 안전한 메시지 전송을 제공하는데 이용된다.

2.2.2 WPP 프로토콜

WPP[3] 프로토콜은 SET을 기초하여 무선인터넷에서 신용카드 지불을 할 수 있도록 제안된 지불 프로토콜이다. WPP는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP의 WTLS를 사용하였다.

WPP는 사용자와 사용자의 은행(신용카드사), 서비스 제공자(상점) 서버, 서비스 제공자의 은행으로 구성되며, 사용자와 은행, 서비스 제공자 서버를 연결해 주는 WG가 필요하다. 그림 3은 WPP 지불 프로토콜의 구성도와 지불 흐름도를 나타낸 것으로써 WAP 프로토콜 스택을 인터넷 프로토콜로 변환하는 WG를 생략하였다.

WPP 지불 프로토콜은 WAP의 WTLS를 사용하여 무선구간의 보안을 제공한다. 이 때문에 WAP에서는 무선단말기와 유선환경에 존재하는 서버를 연결해 줄 수 있는 다리로써 WG를 사용한다. WG에서는 WTLS-SSL 프로토콜 변환 시 암호화된 메시지가 복호화되어 원본 메시지가 노출될 위험성을 가지고 있어 종단간 보안을 제공하지 못한다는 단점을 가지고 있다[6].

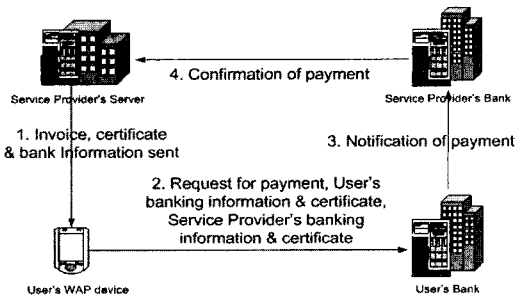

그림 3 WPP 지불 프로토콜 구성도 및 지불 흐름도

본 논문에서는 무선인터넷에서 안전한 신용카드 지불을 수행할 수 있도록 종단간 보안을 제공하는 지불 프로토콜을 제안한다.

2.3 AIP 프로토콜

ASPeCT의 AIP 프로토콜은 무선 이동 통신 환경에서 사용자와 VASP간에 인증과 지불 초기화를 수행 가능하게 해주는 프로토콜이다. AIP 프로토콜은 사용자와 VASP가 상호 인증과 세션키를 설정하고 지불 초기화 정보를 교환한 후 Pederson의 소액 지불 기법을 사용하여 지불을 수행한다. 종단간 보안을 제공하는 AIP 프로토콜은 다음과 같은 조건을 만족시켜야 한다[7,9].

- 사용자와 VASP간의 명확한 상호 인증
- 사용자와 VASP간의 합축적 키 인증성을 가진 세션키의 성립
- 사용자와 VASP간의 상호 키 확인
- 상호간의 새로운 키의 확신
- VASP에게 전송되는 사용자 데이타의 부인 방지
- 사용자와 VASP 인터페이스에서의 사용자 신원의 기밀성

공개키 암호 시스템은 무선 이동 통신에 적합하지 않았으나, 적은 비트 수와 빠른 계산 속도를 보장하는 타원 곡선 공개키 암호 시스템으로 인하여 무선 이동 통신에서 사용할 수 있게 되었다[7,8,12]. AIP 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)[12,13,14]가 어렵다는 가정을 근거로 한다.

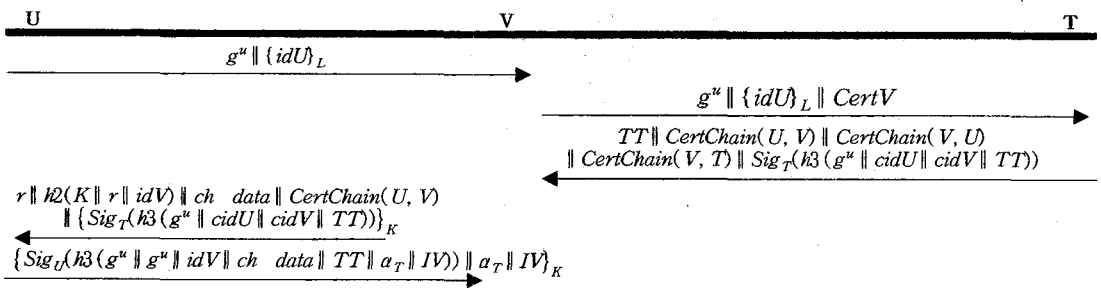

그림 4 온라인 TTP가 참여한 AIP 프로토콜

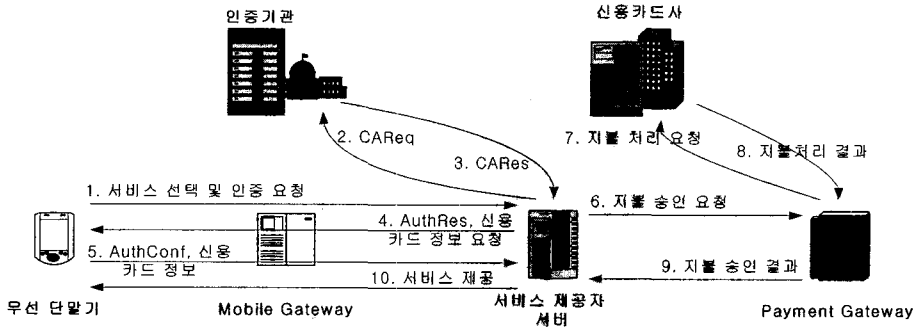

그림 5 제안하는 지불 프로토콜을 위한 시스템 구성도와 프로토콜 흐름도

AIP 프로토콜은 프로토콜 참여자에게 인증서를 제공하는 온라인 TTP(Trusted Third Party)의 참여 여부에 따라 두 가지 종류의 프로토콜로 구분된다. 그림 4는 온라인 TTP가 참여한 경우의 AIP 프로토콜이다. 그림 4에서 U는 사용자, V는 VASP, T는 온라인 TTP를 의미한다. U는 V와 Diffie-Hellman 키 설정[14] 방식에 의하여 세션키를 생성하고 U와 T는 Elgamal 방식[13]에 의하여 세션키를 만들어낸다. 생성한 세션키를 사용해서 인증을 수행한 후 지불을 수행하기 위한 초기화 정보를 교환한다.

3. 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜

본 장에서는 제안한 지불 프로토콜에 적합한 시스템과 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜을 제안한다. 제안하는 지불 프로토콜은 인증과정에 온라인 인증기관이 참여하는 경우와 참여하지 않는 경우로 나누어 기술한다.

3.1 제안하는 지불 프로토콜을 위한 시스템

제안하는 지불 프로토콜을 위한 시스템은 현재 인터넷에서 신용카드 지불을 수행하기 위해 구축되어 있는 지불 시스템을 도입한다. 따라서 유선환경의 PG(Payment Gateway)와 신용카드사는 이미 구축되어 있는 시스템을 사용한다. 또한 유선환경에서의 지불 흐름은 SET에서 사용한 전통적인 지불 흐름을 사용한다[2].

시스템은 그림 5와 같이 사용자의 무선 단말기, MG, 서비스 제공자 서버, PG, 인증기관, 신용카드사로 구성된다. 지불 프로토콜의 흐름은 사용자가 무선 단말기로 서비스 제공자 서버에 접속하여 원하는 상품 및 서비스를 선택하는 것으로 시작한다. 이후 인증과정을 수행하고 서비스 제공자 서버에게 지불 정보를 전송하여 PG가 지불을 수행한다. PG가 지불이 성공적으로 처리되었다는 메시지를 서비스 제공자 서버에 전송하는 것으로 프로토콜은 종료한다.

제안하는 지불 프로토콜을 위한 시스템에서, 사용자의 무선 단말기는 각 참여자와 공개키 암호 시스템을 수행할 수 있도록 스마트 카드를 장착한다. WPP 프로토콜에서 WG 문제점을 극복하기 위해 프로토콜에 직접 참여하지 않고 무선구간과 유선구간을 연결만을 제공해주는 MG를 사용한다. 또한 사용자의 이동성을 보장할 수 있도록 온라인 인증기관이 참여한다.

3.2 종단간 보안을 제공하는 신용카드 기반의 지불 프로토콜

제안하는 지불 프로토콜은 신용카드 지불을 안전하게 수행할 수 있도록 공개키 암호 시스템을 사용하여 종단간 보안을 제공하는 AIP 프로토콜을 기초하였다. 또한 AIP 프로토콜의 안전성을 따른다. 제안한 프로토콜에서 U는 사용자, V는 상품/서비스 제공자(VASP), CA는 인증기관, MG는 Mobile Gateway, PG는 Payment Gateway를 의미한다. 각 참여자와의 세션키 설정은 Diffie-Hellman 키 설정[14] 방식을 사용한다. 제안한 프로토콜에서 사용한 알고리즘과 데이타 요소는 표 1과 2에 나타나 있다.

표 1 제안한 지불 프로토콜에서 사용한 알고리즘

알고리즘	설 명
$h(\cdots)$	일 방향 해쉬 함수
$Sig_X(\cdots)$	X의 개인키를 사용하여 메시지를 서명
$\{\cdots\}_{K_{XY}}$	X와 Y가 공유하는 세션키(K)를 사용하여 암호화

제안하는 지불 프로토콜이 종단간 보안을 제공하기 위해서는 다음과 같은 조건을 만족시켜야 한다[7,9].

- 사용자와 VASP간의 명확한 상호 인증
- 사용자와 VASP간의 함축적 키 인증성을 가진 세션키의 성립
- 사용자와 VASP간의 상호 키 확인
- 상호간의 새로운 키의 확신
- VASP에게 전송되는 사용자 데이타의 부인 방지
- 사용자와 VASP 인터페이스에서의 사용자 신원의 기밀성

표 2 제안한 지불 프로토콜에서 사용한 데이타 요소

데이타 요소	설 명
id_X	X의 신원
cid_X	X의 인증서용 신원
x	X의 개인키
g^x	X의 공개키
K_{XY}	X와 Y가 공유하는 세션키
$Cert_U$	서명 확인용 U의 공개키 인증서
$Cert_V$	세션키 생성용 V의 공개키 인증서
$CertChain(X, Y)$	X가 Y의 인증서를 검증할 수 있도록 생성된 인증서 체인
TX	X에 의해 생성된 타임스탬프
ch_{data}	지불 명세서를 의미하며, 상품이나 서비스 명칭과 수량, 가격이 포함된다.
$card_{data}$	신용카드 정보를 의미한다.

- 사용자의 신용카드 정보에 대한 안전성 제공

제안하는 프로토콜 시작전의 가정은 다음과 같다.

- 각 참여자는 프로토콜에서 사용되는 알고리즘을 알고 있다.
- U는 CA와 공유하는 세션키를 가지고 있다.
- U는 PG와 공유하는 세션키를 가지고 있다.
- U의 무선단말기의 스마트카드에 저장되어 있는 신용카드 정보는 무선환경에서 사용할 수 있도록 신용카드사와 미리 협정한 정보이다.

3.2.1 인증과정에 온라인 인증기관이 참여하지 않는 경우

그림 6은 U와 V가 동일한 도메인에 존재하고, 인증서를 가지고 있는 경우에 해당하는 지불 프로토콜이다.

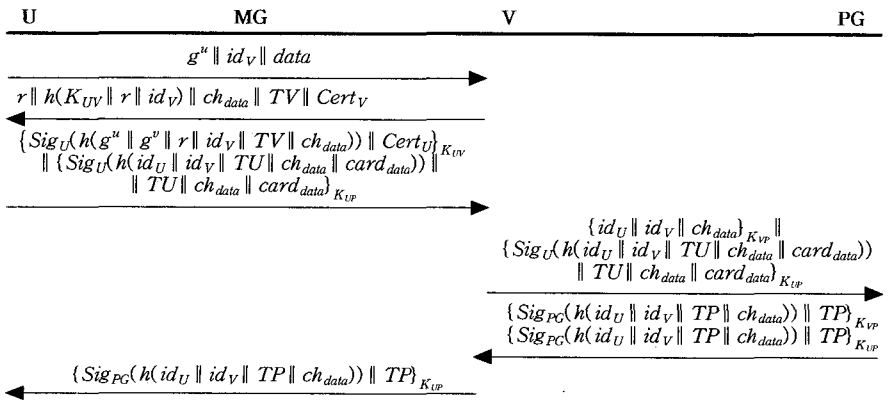

그림 6 인증과정에 온라인 인증기관이 참여하지 않은 지불 프로토콜

프로토콜의 수행은 U가 V의 서버에 접속하는 것으로 시작한다. U는 난수 u를 생성하여 키 설정용 임시 공개키 g^u를 계산한 후, V의 신원과 선택한 상품이나 서비스 정보 $data$를 V에게 전송한다.

V는 난수 r을 생성한 후 첫 번째 메시지에서 받은 U의 키 설정용 임시 공개키를 사용하여 U와 공유하는 세션키 $K_{UV}=h((g^u)^v \| r)$을 생성하고 계산한 해쉬값과 지불 명세서 ch_{data}를 전송한다.

두 번째 메시지를 받은 U는 세션키 생성에 필요한 V의 공개키를 $Cert_V$에서 구해서 V와의 세션키 $K_{UV}=h((g^v)^u \| r)$을 생성한 후 해쉬값을 계산하여 전송받은 해쉬값 $h(K_{UV} \| r \| id_V)$과 동일한지를 비교한다. 비교한 값이 동일하면 인증 확인 메시지와 $Cert_U$를 전송한다. 또한 지불을 위해 신용카드 정보 $card_{data}$가 들어있는 메시지를 PG와의 세션키를 사용해서 암호화하여 V에게 전송한다.

V는 U가 보낸 메시지의 $Cert_U$를 사용하여 서명을 확인한다. V는 PG에게 지불승인 요청을 하기 위해 id_U, id_V, ch_{data}를 암호화한 메시지와 U가 생성한 지불정보를 전송한다.

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 지불이 성공적으로 처리되면 거래에 참여한 참여자 id_U, id_V,와 지불처리가 수행된 시간 TP, 지불 명세서 $card_{data}$의 해쉬값에 서명하여 암호화한 메시지를 V에게 전송하고, V를 통하여 U에게도 전송된다. 이 과정이 수행되면 V는 U가 선택한 상품이나 서비스를 제공하게 된다.

3.2.2 인증과정에 온라인 인증기관이 참여하는 경우

U가 인증서를 가지고 있지 않거나 V와 다른 도메인에 속하면 제안한 지불 프로토콜을 수행하기 위해 온라인 인증기관인 CA가 인증과정에 참여한다. 인증과정에 온라인 인증기관이 참여한 경우의 지불 프로토콜은 그림 7과 같다.

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.

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

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

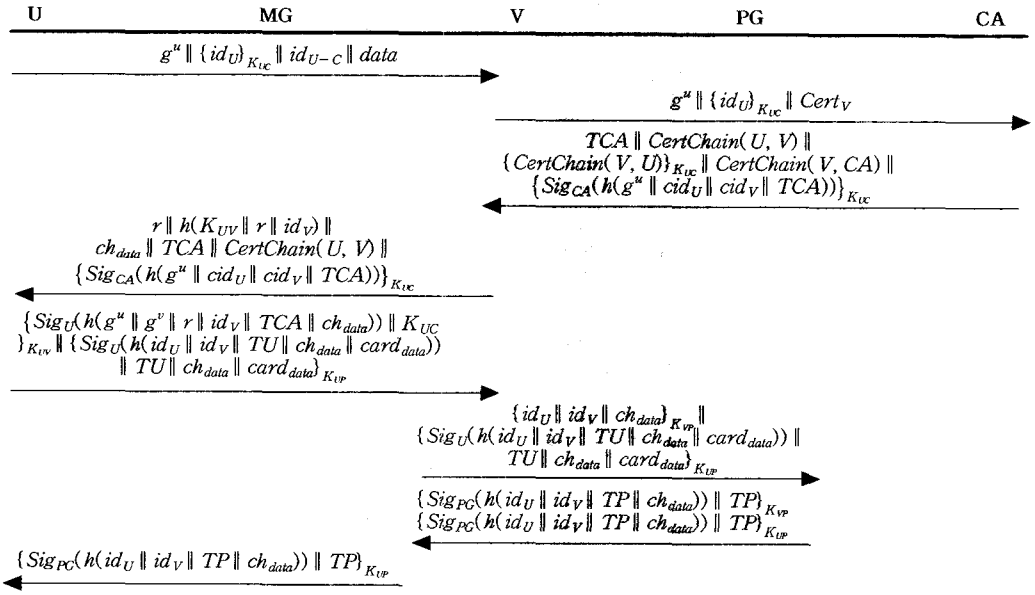

그림 7 인증과정에 온라인 인증기관이 참여한 지불 프로토콜

세션키를 사용하여 암호화해서 전송하는데 이는 악의적인 VASP 재전송 공격[7,9]을 막기 위해서이다.

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 데이타를 함께 전송한다.

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 인증 확인 메시지와 CA와의 세션키를 전송한다. 또한 서비스에 대한 지불로써 신용카드 정보 $card_{data}$가 포함되어 있는 메시지를 PG와의 세션키를 사용하여 암호화하여 V에게 전송한다.

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

이후의 과정은 그림 6의 인증과정에 온라인 인증기관이 참여하지 않은 지불 프로토콜과 동일하다. 모든 프로토콜의 과정이 끝나면 U는 V에게 자신이 선택한 서비스를 받을 수 있다.

4. 안전성 분석

본 장에서는 제안한 지불 프로토콜이 무선인터넷에서 안전한 지불을 수행하기 위해 필요한 안전성을 분석한다. 또한 악의적인 참여자가 제안한 지불 프로토콜을 수행하려 할 때 프로토콜이 안전한지를 분석한다.

4.1 제안한 지불 프로토콜의 안전성 분석

- V에 대한 키 확인과 인증 : 그림 6의 지불 프로토콜 메시지 중 두 번째 메시지에 $h(K_{UV} \| r \| id_V)$를 첨가하는 것은 V가 U에게 키 확인과 V의 함축적 키 인증과 개체 인증을 제공한다.
- U에 대한 키 확인과 인증 : 세 번째 메시지의 인증서 $Cert_U$를 세션키 K_{UV}로 암호화하는 것은 키 확인을 제공한다. 또한 해쉬함수에 $g^u \| g^v \| r$의 첨가는 U에서 V에게 함축적 키 인증을 제공한다. 난수 r의 첨가는 U에 대한 개체 인증을 제공한다.
- 새로운 키 제공 : 세션키 K_{UV} 생성에 V로부터 생성된 난수 r이 포함된다. 이는 이전에 사용되었던 K_{UV}가 재 사용되는 것을 방지하기 위함이다. 또한 난수 r과 U로부터 생성된 난수 u는 세션키가 새로운 키(key freshness)임을 증명한다. 이는 이전에 사용되었던 세션키와 다르므로 제안한 지불 프로토콜은 세션키 K_{UV}을 알기 위한 code-book 공격[9]에 취약하지 않다.
- 부인 방지 : U의 전자 서명은 서명된 데이타의 부인 방지를 제공한다. 또한 제안한 프로토콜의 맨 마지막 메시지는 거래와 지불에 대한 부인 방지를 제공한다.
- 서명의 암호화 : 신용카드 정보를 포함한 U의 전자 서명은 세션키 K_{UV}로 암호화된다. 이를 통하여 U가 세션키 K_{UP}를 알고 있다는 것을 보여줄 수 있다. 또한 signer verification 공격[9] 그리고 content verification 공격[9] 을 방지할 수 있다.
- V의 신원을 두 번째 메시지에 포함 : 그림 6의 지불 프로토콜의 두 번째 메시지에 V의 신원을 포함하는 것은 근원지 대체 공격(source-substitution attack)[7,9]을 방지하기 위함이다.
- V의 신원을 세 번째 메시지에 포함 : 이는 서명의 정당한 수신자를 나타내기 위하여 id_V를 포함하는 것이다.
- U의 신용카드 정보에 대한 안전성 : U의 신용카드 정보는 PG와의 세션키 K_{UP}를 사용하여 암호화를 한다. 또한 U의 신원과 타임스탬프 TU를 신용카드 정보 $card_{data}$가 포함되어 있는 메시지에 첨가하는 것으로써 신용카드 정보를 보호한다. $card_{data}$는 일정 기간의 거래에 사용한 후 신용카드 사와 재 협약한다.

4.2 악의적인 참여자에 의한 안전성 분석

- 악의적인 사용자의 경우 : 사용자가 신용 불량자이거나 자신의 신용카드 정보가 아닌 타인의 신용카드 정보를 이용하는 경우를 악의적인 사용자라 한다. 이 경우에 제안한 프로토콜은 다음과 같이 수행된다. V가 PG에게 악의적인 U의 신용카드 정보를 전송하고, PG가 신용카드사에게 지불 처리 요청을 하였을 때 신용카드사는 지불 처리 결과로 지불 처리 실패 메시지를 전송한다.
- 악의적인 서비스 제공자의 경우 : V가 이전에 사용되었던 지불 정보를 다시 사용하려 하거나, U가 지불할 금액보다 많은 금액을 요청할 때 악의적인 서비스 제공자의 경우에 속한다. V가 이전에 사용되었던 지불 정보를 다시 사용하려 할 때, PG는 U가 생성한 메시지에 포함되어 있는 타임스탬프 TU를 확인하여 사용할 수 없는 데이타임을 알고 V에게 지불 처리 요청 실패 메시지를 전송한다. 또한 V가 거래 금액보

표 3 지불 프로토콜의 특성 비교

종단간 보안성 제공	○	×	○
인증과 지불 통합 여부	×	×	○
키 교환 알고리즘	RSA / DES	RSA / Diffie-Hellman	Diffie-Hellman
무선인터넷 플랫폼	-	WAP	독립적
지불 수행 개체	Payment Gateway	사용자와 서비스제공자의 은행	Payment Gateway
유무선 연결 수행 개체	-	WAP Gateway	Mobile Gateway

(○ : Yes × : No)

다 많은 금액을 요청하였을 때는 *PG*가 *V*로부터 전송받은 메시지 중 *U*가 서명한 메시지와 *V*가 서명한 메시지를 비교하는 것으로 악의적인 서비스 제공자임을 알 수 있다.

5. 성능 평가 및 분석

무선인터넷에서 신용카드를 사용하여 지불을 수행하기 위해서는 프로토콜 참여자만이 지불 정보를 볼 수 있어야 한다. 제안한 지불 프로토콜은 종간간 보안을 위해 상품/서비스 제공자와 안전한 세션을 생성한 후, 신용카드 정보를 PG와의 세션키를 사용해서 암호화하여 PG만이 지불 정보를 볼 수 있다. WPP의 WG 문제점을 극복하기 위해 유·무선 구간을 연결시켜주는 역할만을 수행하는 MG를 사용하였다. 또한 유선구간은 인터넷에서 신용카드 지불을 위해 구축되어 있는 PG를 사용한다. 표 3은 SET, WPP, 제안한 지불 프로토콜의 특성을 비교하고 있다.

WPP가 WAP에만 제한적으로 사용되지만 제안한 지불 프로토콜은 무선인터넷 플랫폼에 독립적이다. SET과 같이 종단간 보안을 제공하지만, 인증서를 받은 후 인증과정을 수행하는 SET과는 달리 무선인터넷의 이동성을 보장하기 위해 온라인 인증기관이 제공하는 인증체인을 사용한다. SET과 WPP는 인증과정을 수행한 후 지불과정을 수행하지만, 제안한 지불 프로토콜은 인증과정을 수행하면서 지불 정보를 전송하는 방법을 통해 인증과정과 지불과정을 통합하였다.

WPP와 제안한 지불 프로토콜과의 성능 분석한 결과가 표 4와 5에 나타나 있다. SET 프로토콜은 유선환경에서 사용되므로 제안한 지불 프로토콜과의 성능 분석은 제외하였다. 성능 분석은 무선인터넷의 제한적 요소 중 많은 영향을 끼치는 통신량과 계산량을 비교하였다. 통신량은 전송되는 메시지 횟수로, 계산량은 세션키나 공개키 생성을 위해 일어나는 멱승(exponentiation)의 횟수를 계산하였다.

WPP는 WAP 단말기와 서버가 안전하게 정보를 전송하기 위해 핸드쉐이크 프로토콜을 통해 암호 매개 변수를 교환한다. 암호 매개 변수를 교환하기 위해 WAP 단말기는 상품/서비스 제공자(상품/서비스 제공자측의 WG)와 4번, 사용자의 은행(사용자의 은행측의 WG)와 4번, application data 전송을 위해 각각 1번씩, 즉 10번의 메시지 교환을 수행한다. 또한 pre_master_secret와 공개키를 생성하기 위해 3번의 멱승을 수행한다[5,10,11]. WAP의 WTLS는 암호 매개 변수를 교환할 때 많은 선택사항을 가지고 있다. 표 4와 5에서는 선택사항에서 추가되는 멱승 횟수는 제외하였다.

표 5는 제안한 프로토콜 중 인증과정에 온라인 인증기관이 참여하는 경우와 WPP 프로토콜을 서비스 제공자 측면에서 비교하였다.

제안한 지불 프로토콜과 WPP 프로토콜을 비교한 표 4와 5를 보면 계산량에서는 두 프로토콜이 비슷하나, 통신량에서는 제안한 지불 프로토콜이 향상된 성능을 보인다.

표 4 사용자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 지불 프로토콜
메시지 교환 횟수	10	4
멱승 횟수	3	4

표 5 서비스 제공자 측면에서의 통신량과 계산량 비교

	WPP 프로토콜	제안한 지불 프로토콜
메시지 교환 횟수	10	8
멱승 횟수	3	3

6. 결론 및 향후 연구 과제

WPP 지불 프로토콜은 WAP 프로토콜을 이용하여 무선인터넷에서 신용카드 지불을 수행할 수 있도록 하

였다. 그러나 WPP 지불 프로토콜은 WAP의 보안 프로토콜인 WTLS를 사용함으로써 종단간 보안을 제공하지 못하는 문제점을 가지고 있다. 본 논문에서는 MG와 공개키 암호 시스템을 사용하는 AIP 프로토콜를 기초하여 특정 무선 플랫폼과 독립적인 종단간 보안이 제공되는 지불 프로토콜을 제안하였다. 제안한 지불 프로토콜은 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써 이동성이 많은 무선단말기가 다른 도메인에 존재하는 서비스 제공자에게도 서비스를 받을 수 있다.

향후 연구 과제로는 사용자가 직접 신용카드 정보를 입력하여 사용할 수 있도록 전자지갑 기법을 연구할 것이다.

참 고 문 헌

[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] VISA & Mastercard, "SET Electronic Transaction Specification," 1997.

[3] J. Hall, S. Kilbank, M. Barbeau, and E. Kranakis, "WPP: A Secure Payment Protocol for Supporting Credit- and Debit-card Transactions Over Wireless Networks," IEEE International Conference on Telecommunications (ICT), Bucharest, June, 2001.

[4] WAP Forum, "WAP White Paper," 2000.

[5] WAP Fourm, "Wireless Application Protocol Wireless Transport Layer Security Spectification version 18-FEB-2000," 2000.

[6] Eun-Kyeong Kwon; Yong-Gu Cho; Ki-Joon Chae, "Integrated transport layer security: end-to-end security model between WTLS and TLS," Information Networking, 2001. Proceedings. 15th International Conference on , pp.65-71, 2001.

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

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

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

[10] T. Dierks, C. Allen, "The TLS Protocol version 1.0," IETF RFC 2246, Jan. 1996.

[11] A. Freier, P. Karlton, P. Kocher, "The SSL Protocol version 3.0," Internet Draft, Nov. 1996.

[12] M. Aydos, B. Sunar, and C. K. Koc., "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication," 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October 30, 1998.

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

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

[15] W. Rankl, W. Effing, "Smart Card Handbook," JOHN WILEY & SONS, LTD, 2000.

임 수 철

2001년 고려대학교 정보공학과 학사
2001년 ~ 현재 고려대학교 컴퓨터학과 석사 과정 재학중. 관심분야는 이동 통신 보안, 암호 프로토콜, 네트워크.

강 상 승

1997년 경북대학교 전자공학과 학사
1999년 경북대학교 전자공학과 석사
1999년 ~ 현재 한국전자통신연구원 전자거래연구부 연구원. 관심분야는 전자상거래, 정보보호, 무선 인터넷, 비지니스 지식처리 기술

이 병 래

정보과학회논문지 : 정보통신
제 29 권 제 4 호 참조

김 태 윤

정보과학회논문지 : 정보통신
제 29 권 제 1 호 참조