다중 지불이 가능한 PayWord 기반의 소액 지불 프로토콜

(A Micro-Payment Protocol based on PayWord for Multiple Payments)

김 선 형 † 김 태 윤 ††
(Sun-Hyoung Kim) (Tai-Yun Kim)

요 약 본 논문에서는 대표적인 소액 지불 프로토콜 중의 하나인 PayWord를 개선한 효율적인 지불 프로토콜을 제안한다. 기존의 PayWord 시스템은 사용자가 해쉬 체인 연산을 수행하여 생성된 payword를 하나의 지정된 판매자에게만 지불할 수 있도록 설계되어 있다. 즉 사용자는 인터넷상의 수많은 판매자들과 거래를 하기 위해서 각 판매자에 대한 해쉬 체인 값을 새로 생성해야 한다. 본 논문에서는 이러한 결점을 보완하기 위해 사용자가 한 번 생성하는 해쉬 체인 값으로도 다른 판매자들과 거래를 할 수 있는 효율적인 방법을 제안한다. 제안한 시스템에서는 브로커가 사용자의 인증서 발급 요청에 대하여 인증서와 함께 새로운 해쉬 체인 값을 생성한다. 이 인증서에는 사용자에게 payword를 생성할 수 있는 권한을 부여하기 위해 브로커의 전자 서명이 되어 있다. 브로커가 생성하는 새로운 해쉬 체인 값은 사용자가 한 번의 해쉬 체인 연산의 수행으로 여러 판매자들과 거래할 수 있는 수단을 제공한다.

키워드 : 공개키 암호 시스템, 다중 지불, 소액 지불, 해쉬 체인, PayWord

Abstract In this paper, we propose an efficient payment protocol by improving PayWord, which is one of the representative micropayment protocols. The original PayWord system is designed for a user who generates paywords by performing hash chain operation for payment to an only designated vendor. In other words, a user has to create new hash chain values in order to establish commercial transactions with different vendors on the Internet. Therefore, we suggest an efficient scheme that is able to deal with business to different vendors by using only one hash chain operation to supplement this drawback. In this proposed system, a broker creates a new series of hash chain values along with a certificate for the user's certificate request. This certificate is signed by a broker to give authority enabling a user to generate hash chain values. New hash chain values generated by a broker provide means to a user to do business with multiple vendors.

Key words : public key cryptography, multiple payments, micro-payment, hash chain, PayWord

1. 서 론

인터넷 보편화의 가장 주된 이유는 인터넷 사용의 편리성에 있다. 네트워크에 연결되어 있는 컴퓨터만 있으면 '정보의 바다'인 인터넷에서 원하는 정보를 쉽게 검색하고 사용할 수 있기 때문이다. 전자상거래는 결국 인터넷 기술을 통해 편리한 방법으로 자신이 원하는 정보나 상품을 구입하고자 하는 욕구로부터 생겨난 것이라 할 수 있다. 현재 인터넷상에는 다양한 컨텐츠를 갖춘 수많은 서비스 제공자나 판매자들이 존재한다. 이러한 판매자들과 사용자간의 안전하고 신뢰적인 통신을 보장하기 위해 전자 지불 시스템이 구축되었다.

전자 지불 시스템은 사용자에게 인터넷상의 판매자로부터 컨텐츠를 구입할 수 있는 방법을 제공하며 사용자는 지불 수단으로서 전자 화폐를 사용한다. 1982년 David Chaum[1]이 은닉 서명을 기반으로 하는 추적 불가능한 전자 화폐 프로토콜을 제안한 이래로 다양한

† 비 회 원 : 고려대학교 컴퓨터학과
shaklim@netlab.korea.ac.kr
†† 종신회원 : 고려대학교 컴퓨터학과 교수
tykim@netlab.korea.ac.kr
논문접수 : 2002년 10월 29일
심사완료 : 2002년 12월 9일

기법의 지불 프로토콜들이 제안되었다[2]. Chaum의 은닉 서명 기법을 이용한 전자 화폐 프로토콜은 익명성, 불추적성, 이중 사용 방지, 위조 불가 등의 기능을 제공하지만 신뢰기관이 온라인으로 지불 과정에 직접 참여하기 때문에 소액 지불 시스템에는 적합하지 못하다. 소액 지불 시스템은 유료 정보를 제공하는 사이트의 접속, AOD(Audio on Demand)나 VOD(Video on Demand)와 같이 시간 당 혹은 페이지 당 요금이 부과되는 서비스, 전자 책이나 전자 신문, 네트워크 게임과 같은 소액 가치의 정보에 대한 지불을 위해 제안되었다.

대부분의 소액 지불 시스템에서는 MD5와 같이 암호학적으로 강한 일방향 해쉬 함수[3]를 반복해서 수행하는 해쉬 체인 기법을 사용한다[4]. 이는 공개키 암호 연산에 비해 수행 속도가 빠르고 비용이 저렴하기 때문이다. 일반적으로 해쉬 함수는 RSA 방식으로 서명을 수행하는 시간보다 10,000 배 정도 빠르고, 이를 검증하는 시간도 100 배 정도 빠르다고 알려져 있다[5]. 따라서 소액 지불 시스템에서는 공개키 암호 알고리즘의 사용을 최소화하고 처리 속도와 비용을 고려하여 해쉬 함수와 같은 암호 알고리즘을 사용하도록 설계되어야 한다. iKP, MicroMint, Milicent, MPTP, Netcard, PayWord [5,6,7,8,9] 등과 같은 대부분의 소액 지불 프로토콜에서 해쉬 체인 기법을 사용하는 것은 바로 이와 같은 이유에서이다.

Rivest와 Shamir는 1996년에 해쉬 체인 기법을 이용하여 사용자가 컴퓨터 네트워크 상에서 소액의 정보나 상품을 구입할 수 있는 PayWord 소액 지불 시스템[5]을 제안하였다. PayWord 시스템에서는 사용자가 인터넷 판매자에게 지불하는 수단으로 해쉬 체인 값인 payword를 사용한다. 그러나 PayWord 시스템에서는 생성된 payword가 하나의 지정된 판매자에게만 사용되어야 한다. 즉 사용자가 다른 판매자와 거래를 하기 위해서는 새로운 payword를 다시 생성해야 하는 문제점이 있다[10].

본 논문에서는 기존 PayWord 시스템의 이러한 결점을 보완한 효율적인 소액 지불 시스템을 제안한다. 제안하는 소액 지불 기법은 사용자에 의한 한 번의 해쉬 체인 연산의 수행으로 여러 판매자들과 거래할 수 있는 방법을 제공한다. 브로커는 사용자가 생성하는 payword와는 별도의 새로운 해쉬 체인 값을 생성하여 사용자에게 전달한다. 사용자는 지불의 root 값으로 브로커가 생성한 해쉬 값을 연동함으로써 사용자가 지불하고 남은 payword를 다른 판매자와의 거래에 사용할 수 있다. PayWord 시스템에서 공개키 암호화 연산이 필요한 인증서 요청 단계의 횟수를 사용자가 거래할 판매자의 수만큼 감소시킬 수 있으며 이를 통해 효율적인 소액 지불 시스템을 구축할 수 있다.

본 논문은 다음과 같은 순서로 구성되어 있다. 2 장에서는 대표적인 소액 지불 시스템인 PayWord에 대해 살펴보고 이의 문제점을 고찰한다. 3 장에서는 본 논문에서 제안하는 개선된 소액 지불 시스템에 대하여 설명한다. 제안한 프로토콜은 인증서 획득 단계, 지불 단계, 결제 단계로 나뉜다. 4 장에서는 제안하는 소액 지불 프로토콜의 안전성을 분석하고, 5 장에서는 기존의 PayWord와 제안하는 프로토콜의 효율성을 비교한다. 6 장에서 결론을 맺고 향후 연구 과제를 제시한다.

2. PayWord

PayWord는 1996년에 Rivest와 Shamir가 제안한 소액 지불 시스템이다. PayWord 시스템에서는 매 거래마다 요구되는 공개키 암호화 연산을 최소화하고 비교적 계산 복잡도가 낮은 해쉬 함수를 사용한다. PayWord 시스템은 사용자, 판매자, 브로커로 구성되어 있으며 모든 사용자와 판매자는 기본적으로 브로커와 신용 계좌를 수립하고 있어야 한다.

- 사용자 : 브로커로부터 자신의 신용카드를 기반으로 한 PayWord 인증서를 발급받고, 해쉬 함수를 수행하여 생성된 payword로 컨텐츠를 구입한다.
- 판매자 : 사용자가 지불한 payword에 대하여 컨텐츠를 제공하고, 만료 날짜 내에 획득한 payword에 해당하는 금액을 브로커에게 요구한다.
- 브로커 : 모든 사용자와 판매자의 신용 계좌 정보를 유지하며 신뢰기관의 역할을 한다. 사용자에게는 지불에 필요한 PayWord 인증서를 발급하고, 판매자의 결제 요청을 처리하는 역할을 한다.

Payword 시스템은 사용자가 브로커로부터 인증서를

표 1 프로토콜에 사용되는 기호

기 호	설 명
X	프로토콜에 참여하는 X의 신원
PK_X	X의 공개키
SK_X	X의 개인키
$\{M\}_{SK_X}$	메시지 M을 X가 서명
A_U	사용자의 주소
C_U	사용자의 공개키 인증서
M_U	사용자의 위임 메시지(commitment)
E_C	C_U의 만료 날짜
E_M	M_U의 만료 날짜

발급받는 단계, 사용자가 상품을 구매하고 이를 판매자에게 payword로 지불하는 단계, 판매자가 사용자로부터 획득한 payword를 브로커에게 전달하여 결제가 이루어지는 단계로 구분할 수 있다. 표 1은 프로토콜에서 사용되는 기호들을 나타낸다.

2.1 인증서 발급 단계

사용자가 계정과 인증서를 요청하는 메시지를 브로커에게 보내고, 브로커는 이에 대한 PayWord 인증서를 사용자에게 발급해주는 단계이다. 사용자와 브로커 사이에는 SSL(Secure Sockets Layer)[11]의 Handshake 프로토콜을 이용하여 이미 세션키(long-term session key)가 성립되어 있다고 가정한다. 사용자는 이와 같은 안전한 채널로 브로커에게 신용카드 번호, 공개키 PK_U, 주소 A_U를 전송하고, 브로커는 다음과 같은 형식을 갖는 인증서를 사용자에게 발급한다.

$$C_U = \{B, U, A_U, PK_U, E_C, I_U\}_{SK_U}$$

판매자는 인증서의 만료 날짜 E_C전에 사용자들로부터 받은 지불 정보 즉, payword를 인증서와 함께 브로커에게 제시함으로써 정당한 지불 요청을 할 수 있다. 인증서는 일정 기간을 주기로 갱신되어야 하며 만료 날짜가 지난 인증서는 유효하지 않다.

2.2 지불 단계

사용자가 웹 사이트를 방문하여 상품을 구입하거나 유료 웹 페이지를 방문하여 이를 이용하고자 할 경우, 해쉬 함수를 수행하여 소액의 화폐 가치를 지닌 n 개만큼의 payword를 생성해야 한다. 즉 사용자는 n 번째 payword w_n을 임의로 생성하고 $i = n-1, \ldots, 0$에 대하여 다음과 같이 해쉬 함수를 수행한다.

$$w_i = h(w_{i+1})$$

사용자는 payword의 root 값 w_0, 판매자의 신원, 사용자의 인증서 C_U, 만료 날짜 E_M, 해쉬 체인의 길이 n과 같은 기타 정보 I_M으로 구성된 다음과 같은 위임 메시지(commitment)를 생성한다.

$$M_U = \{V, C_U, w_0, E_M, I_M\}_{SK_U}$$

이 위임 메시지에 포함된 payword의 root 값은 사용자가 지불할 나머지 payword를 인증하는 역할을 한다. 위임 메시지는 사용자의 인증서 C_U와 함께 사용자의 비밀 서명키 SK_U로 서명되어 있으므로 판매자는 인증서의 만료 날짜 E_C 이전에 결제 단계에서 브로커에게 정당한 지불 요청을 할 수 있다.

이후부터 사용자가 판매자에게 지불하는 payword는 암호화되지 않은 데이타로 전송되며 판매자는 받은 payword의 개수만큼 해쉬 함수를 수행한 결과가 w_0와 일치하는지를 검사한다. 예를 들어 각 payword가 1 센트의 값어치를 지닌다고 가정하고 사용자가 구입한 물품의 값이 5 센트라면 사용자는 모든 payword를 전송하지 않고 w_5와 인덱스 값 5의 쌍으로 이루어진 $P_5 = (w_5, 5)$를 전송한다. 판매자는 해쉬 함수를 5 번 수행하여 전달받은 payword가 w_0와 일치하는지를 검증한다. 이러한 지불 과정이 완료되면 판매자는 위임 메시지 M_U와 마지막 payword 값인 $P_l = (w_l, l)$을 저장한다. 그림 1은 이러한 PayWord 프로토콜의 개략적인 흐름을 보여준다.

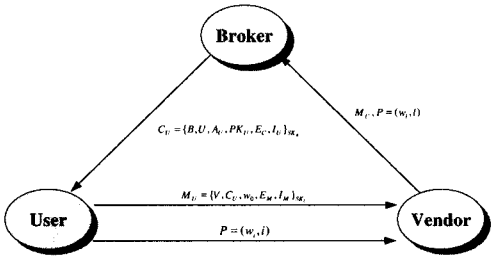

그림 1 PayWord 프로토콜

2.3 결제 단계

판매자는 브로커에게 M_U와 P_l을 전송하여 지불 요청을 한다. 브로커는 사용자의 공개키를 이용하여 M_U에 적용된 사용자의 서명을 검증하고, 마지막 payword인 P_l이 l번 해쉬 함수 수행 후에 w_0가 되는지를 확인한다. 모든 과정이 정상적으로 이루어진다면 브로커는 사용자의 계정에서 판매자의 계정으로 해당 금액을 이체한다.

2.4 PayWord 시스템의 결점

Rivest와 Shamir가 제안한 PayWord 시스템은 암호 연산 속도가 빠르고 비용이 낮은 해쉬 체인 연산을 사용한다. 이러한 해쉬 함수의 특성은 소액 지불 프로토콜에 적합하므로 대부분의 소액 지불 시스템에서 이를 도입하여 사용하고 있다. 그러나 PayWord 시스템은 다음과 같은 몇 가지 결점을 지니고 있다[10].

- 사용자가 생성한 해쉬 체인 값은 하나의 판매자에게만 사용될 수 있다. 즉 사용자는 거래하고자 하는 판매자 수만큼의 해쉬 연산을 매번 수행해야 한다.
- 사용자가 새로운 해쉬 체인 값을 생성할 경우 브로커로부터 이에 해당하는 새로운 인증서를 발급받아야 한다. 따라서 사용자가 새로운 해쉬 체인 값을 생성할 때마다 브로커로부터 새로운 인증서를 발급받기 위한 공개키 암호 연산을 매번 수행해야 한다.
- 사용자는 각 판매자에 해당하는 서로 다른 해쉬 체인

값과 거래에 사용되었던 마지막 인덱스 값을 모두 저장하고 있어야 한다.

이러한 특성은 인터넷 기반의 전자상거래에서 수행되는 소액 지불 프로토콜로서 비효율적이다. 본 논문에서는 기존의 PayWord 시스템에서 나타나는 이러한 문제점을 해결하고자 PayWord 시스템을 기반으로 하여 개선된 소액 지불 프로토콜을 제안한다. 제안한 시스템에서는 사용자가 수행하는 한 번의 해쉬 체인 연산으로 여러 판매자와 거래할 수 있는 효율적인 방법을 제공한다.

3. 제안한 프로토콜

본 논문에서는 저렴한 비용과 빠른 속도의 장점을 갖고 있는 해쉬 함수를 이용하여 높은 비용을 요구하는 공개키 암호 연산을 최대한 배제함으로써 기존의 PayWord 시스템보다 개선된 소액 지불 프로토콜을 제안한다. 시스템을 구성하는 각 참여자들은 사용자, 판매자, 브로커로서 PayWord 시스템의 구성원과 같다.

제안한 시스템에서는 브로커가 사용자의 다중 지불 거래를 가능하게 하기 위하여 사용자가 생성하는 해쉬 체인 값과는 별도의 새로운 해쉬 체인 값을 생성한다. 브로커가 생성하는 해쉬 체인 값은 인증서 발급 단계에서 인증서와 함께 사용자에게 전달되며 사용자는 해쉬 체인 개수만큼의 판매자들과 거래를 할 수 있다. 제안한 시스템은 프로토콜이 시작되기 전에 기본적으로 각 구성원 사이에 다음과 같은 사항을 가정하고 있다.

- 사용자와 판매자는 거래하기 전에 미리 브로커와의 계좌를 수립하고 있다고 가정한다. 브로커는 사용자와 판매자에 대한 신뢰기관의 역할을 하며 두 구성원 사이에서 전자상거래 수행 시 발생되는 지불을 처리한다.
- 사용자와 브로커 사이에는 이미 안전한 채널이 형성되어 있다고 가정한다. 사용자는 사전에 브로커와 SSL의 handshake 프로토콜을 수행하여 비밀 세션키 K를 공유하고 있으며 이를 이용하여 데이타를 암호화하여 전송할 수 있다.

제안하는 소액 지불 프로토콜은 사용자가 브로커로부터 인증서를 획득하는 인증서 획득 단계, payword를 사용하여 판매자에게 지불하는 지불 단계, 판매자가 각 사용자로부터 획득한 인증서와 payword를 이용하여 브로커와 지불 처리를 수행하는 결제 단계로 나뉜다.

3.1 인증서 획득 단계

사용자는 브로커에게 미리 설정된 안전한 통신 채널을 통해 자신의 개인 정보를 전송함으로써 인증서의 발급을 요청하고 브로커는 이에 대한 응답으로 올바른 사용자임을 보장해주는 인증서 C_U와 지불 시에 root 값으로 사용될 S_U를 사용자에게 전송한다. 인증서를 획득한 사용자만이 해쉬 체인 연산을 수행하여 payword를 생성할 수 있는 권한을 갖는다. 판매자는 지불 단계에서 인증서를 통해 거래 중인 사용자가 정당한 거래를 수행하고 있는 사용자임을 보장받는다. 그림 2는 사용자가 브로커로부터 인증서 C_U와 root 값 S_U를 발급받는 과정을 나타낸다.

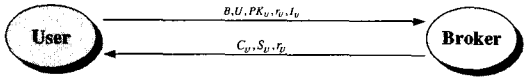

그림 2 인증서 획득 단계

각 사용자는 프로토콜을 개시하기 전에 자신의 공개키 PK_U와 개인키 SK_U의 쌍을 생성하여 이를 자신의 신원과 브로커의 신원, 기타 정보 I_U와 함께 브로커에게 전송한다. I_U에는 사용자의 신용카드 정보를 비롯한 개인 정보와 최대 판매자의 수 N, 해쉬 체인의 수 n과 같은 정보 포함되어 있다. 브로커에게 전송되는 공개키 PK_U는 브로커가 서명하는 사용자의 공개키 인증서에 포함되기 때문에 이 키를 이용하려는 사람은 사용자를 신뢰할 수 있게 된다.

브로커는 사용자의 인증서 발급 요청에 따라서 인증서와 사용자가 지불의 root 값으로 사용할 해쉬 체인 값을 생성한다. 브로커는 인증서와 해쉬 체인 값을 생성하기 전에 해쉬 체인의 키 값으로 다음과 같은 T_U를 생성한다. T_U는 사용자의 신원 U와 브로커가 생성한 난수 R_B, 사용자와 브로커 사이에 공유된 비밀 세션키 K를 해쉬 함수로 처리하여 생성된다.

$$T_U = h(U, r_B, K)$$

T_U는 브로커 이외에는 생성할 수 없으며 브로커가 생성하는 해쉬 체인이 어느 사용자에게 발급되는 것인지를 분명히 하기 위해서 사용된다. 앞서 언급되었듯이 기존의 PayWord 프로토콜에서는 사용자가 해쉬 체인 연산을 수행하여 생성된 payword를 하나의 지정된 판매자에게만 지불해야 한다. 이러한 문제점을 보완하기 위해서 브로커는 사용자가 수행하는 해쉬 체인 연산과 유사한 방법으로 새로운 해쉬 체인 값을 생성한다. 즉 브로커는 N에 대하여 임의의 s_N을 선택하고, $i = N-1, \ldots, 0$에 대하여 해쉬 체인 값을 생성한다. S_U를 다음과 같이 정의한다.

$$S_U = \{ s_i \mid s_i = h(s_{i+1}, T_U), i = N-1, \ldots, 0 \}$$

브로커는 생성된 T_U와 전송받은 사용자의 공개키 PK_U, 각각의 신원과 사용자의 개인 정보 I_U, 인증서의

만료 날짜 E_C를 이용하여 사용자의 인증서를 만든다. 인증서는 다음과 같이 브로커의 개인키로 전자 서명이 되어 있기 때문에 이를 발급받는 사용자는 payword를 생성할 수 있는 권한을 부여받게 되며 판매자에게 정당한 사용자임을 증명할 수 있다.

$$C_U = \{B, U, PK_U, T_U, I_U, E_C\}_{SK_B}$$

브로커는 이와 같이 생성된 인증서 C_U와 사용자로부터 전송받은 난수 r_U, 새로이 생성된 해쉬 체인 S_U를 사용자에게 전송한다.

3.2 지불 단계

사용자는 판매자와 거래를 시작하기 전에 PayWord과 같은 방식으로 해쉬 체인 연산을 수행하여 payword를 생성하고, 위임 메시지(commitment)를 생성한다. PayWord 프로토콜과 다른 점은 payword의 root 값이 브로커로부터 받은 s_i가 함께 사용된다는 점이다. 즉 브로커가 생성한 각 해쉬 값은 사용자가 각 판매자와의 거래에 사용하는 지불의 root 값과 해쉬 함수로 처리됨으로써 나머지 payword를 계속해서 지불할 수 있도록 한다.

인증서를 발급받은 사용자는 payword를 생성하고 최초로 거래를 시작하는 판매자에 대하여 위임 메시지를 생성한다. 위임 메시지는 판매자의 신원 V, 사용자의 인증서 C_U, payword의 root 값으로 사용되는 w_0와 $h(w_0, s_1)$, 위임 메시지의 만료 날짜 E_M, 그리고 기타 지불 정보를 나타내는 I_M으로 구성되어 있으며 이를 사용자의 개인키 SK_U로 서명한 것이다.

$$M_U = \{V, C_U, w_0, h(w_0, s_1), I_M, E_M\}_{SK_U}$$

사용자는 생성된 M_U를 처음으로 거래하고자 하는 판매자에게 제공한다. 판매자는 전달받은 M_U를 통해 사용자가 앞으로 지불할 payword에 대한 정당성을 보장받게 된다. 사용자가 판매자에게 payword를 지불하는 과정은 PayWord 프로토콜과 같다. 즉 사용자는 정보나 서비스를 구매하기 위해 해당되는 payword를 지불하며 판매자는 해쉬 함수를 수행하여 그 값이 w_0와 일치하는지를 확인함으로써 지불받은 payword가 유효함을 보장받는다. 그림 3은 첫 번째 판매자와의 지불 과정을 나타낸다.

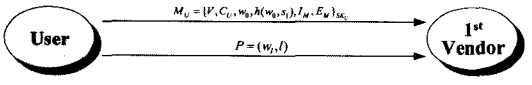

그림 3 첫 번째 판매자와의 지불 단계

사용자는 지불하고 남은 나머지 payword를 이후에도 계속해서 사용하기 위해서 payword의 root 값으로 브로커로부터 받은 해쉬 값 S_U를 함께 사용한다. 예를 들어 사용자가 이전까지의 거래에서 w_{j-1} 만큼의 payword를 사용했다면 k번째의 판매자와 거래를 하기 위해 사용자는 w_j와 s_k를 $h(w_j, s_k)$와 같이 해쉬 함수로 처리하여 다음 거래의 root 값으로 이용한다. 사용자가 w_j와 s_k에 대하여 l개 만큼의 payword를 사용했다면 다음 $k+1$ 번째의 판매자에 대한 root 값은 w_{j+l+1}과 s_{k+1}을 해쉬 함수로 처리한 $h(w_{j+l+1}, s_{k+1})$이 된다. 이와 같은 방법으로 사용자는 자신이 생성한 payword를 다른 여러 판매자에게도 지불할 수 있으며 최대 거래 한계인 N까지 사용한 payword가 w_n을 초과하지 않는다면 정상적인 거래가 이루어지게 된다. 그림 4는 k번째 판매자와의 지불 과정을 나타낸다.

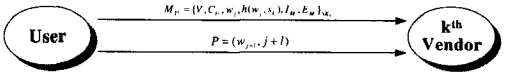

그림 4 k번째 판매자와의 지불 단계

판매자는 사용자로부터 마지막 지불받은 $P_{j+l} = (w_{j+l}, j+l)$과 M_U를 저장하고 사용자와의 거래를 종료한다.

3.3 결제 단계

판매자는 일정 마감 기한이 되기 전에 브로커와 결제 단계를 진행한다. 브로커는 사용자에게 발급한 인증서를 검증함으로써 판매자가 요구하는 지불에 대한 정당성을 확인할 수 있다. 그림 5는 판매자와 브로커 간에 수행되는 결제 과정을 나타낸다.

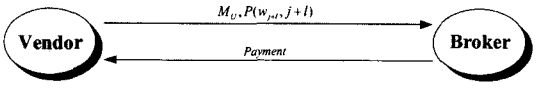

그림 5 결제 단계

판매자는 사용자의 위임 메시지와 지불 정보를 브로커에 전송하여 결제를 요청한다. 브로커는 사용자의 인증서 C_U에 수행된 자신의 서명을 검증하고, 판매자가 요청한 P_{j+l}에 해당하는 금액을 판매자의 계좌로 이체시킨다. 브로커는 판매자가 전송한 s_k에 대하여 w_j에서 w_{j+l}까지만 검증할 수 있다. 즉 s_k에 해당하는 root 값은 w_j가 되고 마지막 받은 w_{j+l}에 해쉬 함수를 l번 적용하여 w_j와 일치하는지에 대해서만 확인하면 된다. 브로커는 만료 기한까지 N개 이하의 판매자에 대한 결제 요청을 처리하고, 마지막 받은 w_l이 사용자가 생성한 해

쉬 체인의 최대 값인 w_n보다 작은지를 검사함으로써 결제 과정을 완료한다.

4. 안전성 분석

인터넷 기반의 전자상거래 환경에서는 사용자가 자신의 지불 데이타를 네트워크 상으로 전송하므로 안전성에 대한 보안 대책이 철저히 이루어져야 한다. 소액 지불 시스템은 온라인 기반의 지불 시스템과 비교하여 상대적으로 화폐 단위가 작고 위험성이 낮은 편이나 다음과 같은 기본적인 보안 요구 사항을 만족시켜야 한다[12].

4.1 이중 지불 탐지(Double spending detection)

사용자는 거래를 시작하기 전에 브로커로부터 발급받은 인증서 C_U와 지불의 root 값으로 사용되는 w_j, $h(w_j, S_k)$이 포함된 위임 메시지를 판매자에게 제공한다. 위임 메시지는 결제 과정에서 브로커에게 전달되기 때문에 사용자가 자신이 생성한 payword를 이중으로 사용하였을 경우 브로커가 이를 탐지하게 된다.

4.2 위조 방지(Forgery prevention)

소액 지불 시스템에서는 위조 방지와 관련한 다음의 두 가지 사항을 고려해야 한다. 제안하는 프로토콜은 다음과 같이 전자 화폐에 대한 위조와 결제 정보에 대한 위조에 대한 공격으로부터 안전하다.

- 전자 화폐에 대한 위조 방지 : 브로커가 발급하는 인증서 C_U는 다른 사용자가 획득할 수 없는 브로커의 개인키로 서명되어 안전한 채널로 전송되기 때문에 이를 변경할 수 없으며 C_U를 소유하고 있는 정당한 사용자만이 화폐 가치를 지닌 payword를 생성할 수 있으므로 이를 위조하는 것이 불가능하다.
- 결제 정보에 대한 위조 방지 : 판매자가 브로커와 올바른 결제 과정을 수행하기 위해서는 사용자의 인증서 C_U, payword의 root 값으로 사용되는 w_j와 $h(w_j, s_k)$, 지불 정보를 알고 있어야 한다. 그러나 판매자가 이를 위조하기 위해서는 브로커의 비밀 서명키와 사용자의 비밀 서명키, T_U에 사용된 브로커의 난수 γ_B 와 세션키 K를 알고 있어야 하는데 사실상 이들 중 하나라도 알아내는 것이 불가능하다.

4.3 부인 방지(Non-repudiation)

부인 방지는 비밀 서명키를 이용한 전자 서명을 통해 제공될 수 있다. 시스템의 각 구성원들은 자신의 공개키와 개인키의 쌍을 생성하여 부인 방지가 필요한 메시지에 대하여 서명 알고리즘을 적용해야 한다. 제안하는 프로토콜에서는 사용자가 지불 단계에서 공개키 인증서 C_U를 포함하는 위임 메시지를 판매자에게 전송하며 이 위임 메시지는 사용자의 비밀 서명키로 서명되어 있다. 따라서 사용자는 이후부터 지불할 지불 정보에 대하여 부인할 수 없으며 판매자는 사용자에게 제공하는 서비스에 대하여 부인할 수 없다.

4.4 과옹 지불 방지(Overspending prevention)

사용자는 브로커에게 인증서 발급 요청 시 생성할 해쉬 체인의 크기에 대한 정보를 같이 전송해야 한다. 또한 판매자가 해쉬 체인의 한도를 검증할 수 있도록 인증서 내에 해쉬 체인의 크기가 포함되어 있어야 한다. 제안한 프로토콜에서는 사용자가 인증서 발급 단계에서 신용카드 정보, payword의 최대 길이 n과 브로커가 생성할 해쉬 체인의 최대 길이 N을 포함하는 개인 정보 I_U를 전송한다. 위임 메시지의 I_M에는 payword의 최대 길이 n과 같은 지불 정보가 포함되어 있기 때문에 사용자가 이를 초과하여 지불하는 것을 방지할 수 있다.

5. 효율성 분석

기존의 PayWord 시스템의 경우 사용자는 판매자와 거래를 시작하기 전에 매번 브로커로부터 인증서를 발급받고 payword를 생성해야 한다. 생성된 payword는 하나의 판매자에게만 사용될 수 있으며, 사용자는 payword를 생성할 때마다 브로커로부터 인증서 발급받기 위해 공개키 암호 연산을 수행해야 한다.

본 논문에서는 소액 지불 시스템에서 사용자가 한 번의 해쉬 체인 연산을 수행함으로써 여러 판매자들과의 거래를 할 수 있는 효율적인 방법을 제안하고 있다. 표 2는 PayWord 시스템과 제안하는 시스템의 효율성을 비교하여 나타낸다. 사용자가 N 개의 판매자와 거래를 하고, 생성된 해쉬 체인의 최대 길이는 n이라고 가정한다.

표 2 제시된 소액 지불 시스템의 효율성 비교

소액 지불 시스템 / 항 목	PayWord 시스템	제안하는 시스템
사용자가 생성하는 해쉬 체인의 수	$\sum_{i=1}^{N} l_i$	n
브로커가 생성하는 해쉬 체인의 수	0	N

PayWord 시스템에서는 사용자가 각 판매자에 대하여 매번 payword를 새로이 생성해야 한다. 각각의 판매자 V_i에 대하여 사용자가 생성하는 마지막 payword의 인덱스 값을 l_i라고 하면, 사용자가 생성해야 하는 payword의 총 개수는 $l_1+l_2+\ldots,l_N$이다[13]. 반면 제안하는 시스템에서는 사용자가 N 개의 판매자에 대하여 n 개의 해쉬 체인

값을 한 번만 생성해도 되므로 payword의 총 개수는 n이 된다.

PayWord 시스템에서 payword가 생성될 때마다 매번 n개씩의 payword가 생성된다면 각 l_i의 값은 n이 되므로 생성되는 총 payword의 수는 $N \times n$이다. 따라서 사용자 측면에서의 효율성은 제안하는 시스템이 기존의 PayWord 시스템보다 N배만큼 높다.

반면에 PayWord 시스템에서는 오직 사용자만이 해쉬 체인 연산을 수행하지만 제안하는 시스템에서는 인증서 발급 과정에서 브로커가 N개의 해쉬 체인 값을 생성하여 이를 사용자에게 전달한다.

6. 결론 및 향후 연구 과제

본 논문에서는 대표적인 소액 지불 시스템 중의 하나인 PayWord 소액 지불 시스템을 개선한 효율적인 프로토콜을 제안하였다. 본 논문에서는 기존의 PayWord 시스템이 판매자와 거래할 때마다 해쉬 함수를 새롭게 생성해야 하는 결점을 보완하기 위해 payword의 root 값을 다중 지불에 적합한 방식으로 변형하였다. 즉 PayWord 시스템에서는 payword의 첫 번째 값인 w_0을 root 값으로 설정하여 나머지 payword를 지불하는 방식이었지만 제안하는 시스템에서는 브로커로부터 전달받은 새로운 해쉬 값을 payword의 root 값과 연동함으로써 지불하고 남은 나머지 payword를 다른 판매자에게도 사용할 수 있도록 하였다.

제안한 프로토콜은 이중 지불 탐지, 위조 방지, 부인 방지, 그리고 과용 지불 방지와 같은 소액 지불 프로토콜의 기본적인 보안 요구 사항들을 충분히 만족시킴으로써 인터넷상에서 이루어지는 안전한 전자상거래의 실현에 공헌할 거라 생각한다.

최근에는 무선 인터넷을 이용한 M-commerce가 활성화됨에 따라 이동 통신 환경에서도 지불과 결제가 가능한 지불 시스템이 연구되고 있다[14,15]. 이동 단말기의 전력 소비량과 무선 네트워크 환경의 특성을 고려할 때 비교적 위험성이 낮은 소액 지불 시스템의 개발이 가능하리라 생각한다. 향후에는 차세대 이동 통신 시스템에서 적용될 수 있는 지불 시스템의 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology - Proceedings of CRYPTO'82, pp.199-203, 1983.

[2] H. W. P. Beadle, R. Gonzalez, R. Safavi-Naini and S. Bakhtiari, "A Review of Internet Payments Schemes," In Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC'96), September 1996.

[3] R. Rivest, "The MD5 Message-Digest Algorithm," Internet RFC 1321, April 1992.

[4] T. P. Pederson, "Electronic Payments of Small Amounts," Security Protocols, LNCS 1361, pp.59-68, Springer-Verlag, 1997.

[5] R. Rivest and A. Shamir, "PayWord and MicroMint: Two simple micropayment schemes," Security Protocols, LNCS 1189, pp.69-87, Springer-Verlag, 1996.

[6] R. Hauser, M. Steiner and M. Waidner, "Micro-Payments based on iKP," Research Report RZ 2791(#89269), IBM Research, February, 1996.

[7] M. S. Manasse, "The Milicent Protocol for Electronic Commerce", In Proceedings of the 1st USENIX Workshop on Electronic Commerce, 1995.

[8] Philip M. Hallam-Baker, Micro Payment Transfer Protocol (MPTP) Version 0.1. W3C Working Draft, Novembar 1995.

[9] R. Anderson, C. Manifavas and C. Sutherland, "NetCard-A Practical Electronic Cash System," Technical Report, Computer Laboratory, Cambridge University, UK, 1995.

[10] M. H. Lee, H. R. Lee and K. G. Kim, "A Micro-payment System for Multiple-Shopping," SCIS 2002, Vol.1/2, pp.229-234, January-February 2002.

[11] A. Freier, P. Karlton and P. Kocher, The SSL Protocol Version 3.0, Internet Draft, Novermber 1996.

[12] Ellis Chi, "Evaluations of Micropayment Schemes," Technical Reports, HP Laboratory, 1997.

[13] C. T. Wang, C. C Chang and C. H. Lin, "A New Micro-Payment System Using General Payword Chain," Electronic Commerce Research Journal, Vol.2, No.1-2, pp.159-168, 2002.

[14] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," In Computer Security - ESORICS'98 LNCS 1485, pp.277-293, 1998.

[15] D. G. Park, C. Boyd and Ed Dawson, "Micropayments for Wireless Communications," ICISC 2000, LNCS 2015, pp.192-205, 2000.

김 선 형

2001년 성공회대학교 정보통신학과 학사 2003년 고려대학교 컴퓨터학과 석사 2003년~현재 고려대학교 컴퓨터학과 박사 과정 재학 중. 관심분야는 전자상거래, 암호 프로토콜, 이동 통신 보안

김 태 윤

1981년 고려대학교 산업공학과 학사 1983년 미국 Wayne State University 전산과학과 석사. 1987년 미국 Auburn University 전산과학과 박사. 1988년~2002년 고려대학교 컴퓨터학과 교수. 관심분야는 전자상거래, 컴퓨터 네트워크, EDI, 이동 통신, 멀티미디어 등