3 세대 이동 통신을 위한 티켓 기반 인증 및 지불 기법

(A Ticket based Authentication and Payment Scheme for Third Generation Mobile Communications)

이 병 래 † 장 경 아 † 김 태 윤 ††
(Byung-Rae Lee) (Kyung-Ah Chang) (Tai-Yun Kim)

요 약 UMTS와 같은 제 3세대 이동 통신 시스템에서의 value-added 서비스를 위한 중요한 점은 이동 사용자로부터의 지불을 받을 수 있는 지의 여부를 검사하는 것이다. 기존의 value-added 서비스를 위한 인증 및 지불 프로토콜은 사용자의 인증 기관의 역할을 해주는 온-라인(on-line) TTP에 의존하고 있다. 그러나 3 세대 이동 통신 시스템에서의 수많은 서비스 제공자들, 다양한 종류의 서비스들, 그리고 넓은 사용자 계층 등을 고려할 때 온-라인 TTP에 기반한 인증과 지불 기법은 실용적이지 못하다. 본 논문에서는 3 세대 이동 통신 시스템에서의 value-added 서비스를 위하여 티켓(ticket)을 이용하여 인증 및 지불 프로토콜을 제안한다. 제안한 티켓 기반 인증 및 지불 프로토콜은 온-라인 TTP와의 통신 없이 사용자의 비용 지불 여부를 확인할 수 있는 효율적인 방법을 제공한다. 또한 티켓에 기반한 제안된 프로토콜은 이동 사용자의 서비스 사용에 대한 익명성을 보장 할 수 있다.

키워드 : 인증, 지불, 티켓, UMTS, 이동 통신, ASPeCT

Abstract In the third generation mobile telecommunication systems such as UMTS, one of the important problems for value-added services is to check the recoverability of costs used by a mobile user. Previous authentication and payment schemes for value-added services by a mobile user across multiple service domains, rely on the concept of the on-line TTP, which serves as the users certification authority. In the third generation systems with many service providers, a wide range of services, and a diverse user population, authentication mechanisms with the on-line TTP provide a far from ideal solution. In this paper we present an efficient public-key protocol for mutual authentication and key exchange designed for value-added services in the third generation mobile telecommunications systems. The proposed ticket based authentication and payment protocol provides an efficient way for VASP to check the recoverability of costs without communication with the on-line TTP. Furthermore, the proposed ticket based protocol can provide anonymous service usage for a mobile user.

Key words : Authentication, Payment, Ticket, UMTS, Mobile Communications, ASPeCT

1. 서 론

UMTS(Universal Mobile Telecommunications System)[1]와 같은 3세대 이동 통신 시스템에서는 사용자들이 네트워크를 통하여 지불을 함으로써 제공받을 수 있는 다양한 종류의 수많은 value-added 서비스들이 존재할 것이다. UMTS 서비스 제공자는 이동 사용자들에게 인증서를 발급함으로써 사용자가 서비스를 사용할 수 있는 신용과 전자적으로 지불을 할 수 있는 방법을 제공한다. 사용자가 자신의 서비스 사용에 대한 지불을 완료하지 않으면 인증서는 취소되며 재발급 되지 않는다[2].

3 세대 이동 통신 시스템에서 중요한 점 중의 한 가지는 사용자의 서비스 사용과 지불에 대한 문제이다. 사용자가 서비스를 이용하기 전에 VASP(Value-Added Service Provider)는 사용자의 서비스 사용에 대한 지불 가능성을 확신할 필요가 있다. ASPeCT(Advanced

† 정 회 원 : 삼성전자 소프트웨어센터 연구원
byungrae.lee@samsung.com
kachang@samsung.com
†† 종신회원 : 고려대학교 컴퓨터학과 교수
tykim@netlab.korea.ac.kr
논문접수 : 2001년 6월 21일
심사완료 : 2002년 5월 8일

Security for Personal Communications Technologies) [3]에서는 UMTS에서의 사용자와 VASP간에 인증과 지불을 위한 AIP (Authentication and Initialization of Payment) 프로토콜을 제시하고 있다[2,4]. AIP 프로토콜에서 VASP는 사용자의 비용에 대한 지불을 확신하기 위하여 사용자의 온-라인 TTP(Trusted Third Party)에 접근하여 서비스 사용을 원하는 사용자의 인증서 취소 여부를 확인한다[4].

그러나 온-라인 TTP에 의존하여 사용자의 인증서 취소 여부를 확인하는 것은 원거리에서의 인증 프로토콜 수행과 그에 따른 시간 소비라는 단점이 존재한다. 또한 이러한 방식은 VASP가 있는 외부 도메인과 TTP가 존재하는 사용자의 홈 도메인과의 신뢰 관계를 필요로 한다. 적은 서비스 제공자가 존재하는 환경에 있어서는 이동성 계약에 의하여 온-라인 TTP에 기반한 인증과 지불 프로토콜의 수행이 가능하나 3 세대 이동 통신 환경과 같이 수많은 서비스 제공자들과 다양한 서비스들이 존재하는 환경에서는 비효율적인 방법이다.

본 논문에서는 3세대 이동 통신을 위한 AIP 프로토콜에서 온-라인 TTP에 의존하는 방식을 개선하고자 티켓을 이용한 인증 및 지불 프로토콜을 제안한다. 티켓은 사용자가 서비스를 사용할 수 있는 권리를 나타내게 된다[5,6]. 사용자는 원하는 서비스에 대한 티켓을 제공받고 VASP에게 티켓을 제출하므로 온-라인 TTP에 의한 인증서 검증 절차가 필요 없어지는 장점을 가지게 된다. 본 논문에서는 기존의 AIP 프로토콜을 티켓을 이용한 인증 및 지불 프로토콜로 변형하여서 3세대 이동 통신 시스템에 적합하면서 동시에 티켓 기반 서비스로 인한 개선된 효율성의 장점을 가지도록 하였다.

그러나 티켓에 기반한 인증 및 지불 프로토콜은 자원의 접근에 대한 제한를 다루고 있기 때문에 사용자와 서비스 제공자에 있어서 안전성이 보장되어야 한다. 사용자는 티켓을 획득할 때 공인된 기관에서 획득하는 것에 대한 확인을 필요로 한다. 또한 사용자들은 공격자에 의해서 티켓이 불법적으로 수정되거나 위조되지 않았음을 확신하여야 한다. VASP는 서비스를 제공하기 전에 티켓이 위조가 아니고 원본임을 확인하여야 한다. 또한 티켓의 이중 사용의 문제 또한 해결되어야 한다[5,6].

제안한 인증 및 지불 프로토콜은 티켓을 사용함으로써 사용자의 인증서 취소 여부를 검사하기 위해 온-라인 TTP에 접근하는 과정을 없애고 VASP는 단지 티켓을 검증하고 사용자가 정당한 티켓의 소유주임을 확인한다. 제안된 기법은 AIP 프로토콜을 기반으로 하여 3세대 이동 통신 시스템에서의 보안 요구 사항을 만족하면서 티켓을 이용함으로써 AIP 프로토콜과 비교하여 통신과 계산 비용을 개선하였고 익명성과 차별화된 서비스 등을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 사용자의 서비스 사용에 대한 지불을 확인할 수 있는 온-라인 TTP를 이용한 AIP 프로토콜에 대하여 설명한다. 3장에서는 본 논문에서 제안한 티켓에 기반한 인증과 지불 모델에 대하여 기술한다. 4장에서는 새로운 티켓의 구조와 티켓 획득 프로토콜을 제안하고 5장에서는 티켓에 기반한 인증 및 지불 프로토콜을 제시한다. 6장에서는 제안된 프로토콜에 대한 정성적 분석을 한다. 마지막으로 7장에서는 결론을 제시한다.

2. ASPeCT AIP 프로토콜

ASPeCT에서의 AIP(Authentication and Initialization of Payment) 프로토콜은 사용자와 VASP간에 인증과 지불 초기화를 수행하며 두 단계로 구분되어져 있다. 처음 단계에서는 사용자와 VASP는 상호 인증과 세션키를 설정하고 지불 초기화 정보를 교환한다. 다음 단계에서 사용자는 서비스를 제공 받는 동안 VASP에게 Pederson의 소액 지불 기법[7]을 이용하여 지불을 수행하게 된다. AIP 프로토콜은 다음과 같은 요구 조건을 만족시켜야 한다[2,4].

- 사용자와 VASP간의 명확한 상호 인증;
- 사용자와 VASP간의 상호 함축적 키 인증을 통한 세션키 K의 성립;
- 사용자와 VASP간의 상호 키 확인;
- 상호간의 새로운 키의 확신;
- VASP에게 전송되는 사용자 데이타의 부인 방지;
- 사용자와 VASP 인터페이스에서의 사용자 신원의 기밀성.

AIP 프로토콜은 사용자와 온-라인 TTP의 존재 여부에 따라서 두 가지 종류의 프로토콜로 구분이 된다. 온-라인 TTP가 관여하지 않는 프로토콜은 사용자와 VASP간에 이루어지는 것으로 프로토콜이 간단한 장점이 있지만 사용자의 인증서 취소 여부를 파악할 수 없는 단점이 있다. 따라서 VASP는 제공한 서비스에 대해 사용자가 지불을 완료할 것인지에 대한 검증을 할 수가 없다. 온-라인 TTP를 이용한 AIP 프로토콜에서 VASP는 온-라인 TTP와 프로토콜 수행을 통해 사용자의 인증서의 취소 여부를 파악함으로써 제공한 서비스에 대한 지불 가능 여부를 검사할 수 있다. 그러나 온-라인 TTP와의 원거리 통신에 따른 문제점이 있으며 인증서 체인(certificate chain)을 이용하여 검증을 수행

하므로 계산량이 많아지게 된다. 또한 AIP 프로토콜은 사용자의 인증서가 VASP에게 전달이 되므로 사용자의 신원이 VASP에게 파악이 되어 익명 서비스 사용이 보장되지 않는 단점이 있다.

사용자의 서비스 사용에 대한 지불 여부를 파악 할 수 있는 온-라인 TTP를 이용하는 AIP 프로토콜은 <그림 1>에 기술되어 있다. AIP 프로토콜은 유한체(finite field)의 곱셈군(multiplicative group) 또는 타원 곡선의 부분군(subgroup)과 같은 유한군 G와 생성원 g에서 이산 대수 문제(discrete logarithm problem)[8,9]에 기반하고 있다. <그림 1>에서 U는 사용자, V는 VASP, T는 온-라인 TTP를 의미한다. U는 V와 Diffie-Hllman 키 설정[8] 방식에 의하여 세션키를 생성하고 U와 T는 ElGamal 방식[9] 에 의하여 세션키를 만들어 낸다. $CertChain(X, Y)$는 X가 Y의 인증서를 검증할 수 있도록 생성된 인증서 체인을 나타낸다. 메시지 M을 세션키 K로 암호한 경우는 $\{M\}_K$와 같이 표기한다. U와 T의 서명은 각각 Sig_U와 Sig_T와 같이 나타낸다. T의 타임스탬프는 TT로 표기한다. U와 V의 신원은 각각 idU와 idV로 표기한다. $h1, h2, h3$는 [2,4]에 정의된 해쉬 함수이다.

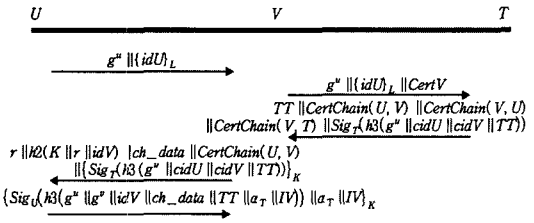

그림 1 온-라인 TTP를 이용한 AIP 프로토콜

프로토콜이 시작되면 U는 난수 u를 생성하고 키 설정용 공개키 g^u를 계산해낸다. 그리고 T의 공개키 g^t를 이용하여 세션 키 $L = g^{tu}$를 생성한다. U는 공개키 g^u와 자신의 신원 idU를 생성한 세션키 L로 암호화하여 V에게 보낸다.

V는 U로부터 메시지를 받아 자신의 인증서 $CertV$와 같이 온-라인 TTP 인 T에게 전송하게 된다.

T는 V로부터 받은 메시지에서 $CertV$를 이용하여 U가 V의 공개키를 검증할 수 있도록 $CertChain(U, V)$를 생성하고 V가 U와 TTP의 인증서를 검증할 수 있도록 각각 $CertChain(V, U)$와 $CertChain(V, T)$를 생성해서 V에게 전송한다.

V는 $CertChain(V, U)$를 통하여 U의 키 설정용 공개키를 얻어서 U와의 세션키 $K = h(g^{uv} \| r)$을 생성한다. 그리고 $CertChain(V, T)$를 이용하여 T의 서명을 검증할 수 있는 공개키를 얻게 되며 T로부터 받은 g^u, $cidU$, $cidV$, TT에 대한 서명을 U에게로 전달해 주게 된다.

U는 $CertChain(U, V)$를 이용해서 V의 인증서를 검증할 수 있으며 V와 동일한 세션키 $K = h(g^{uv} \| r)$을 생성한다. 그리고 U는 지불에 관련된 ch_data, a_T, 그리고 지불 초기화 벡터 IV를 공개키 g^u와 g^v와 같이 서명을 하여서 V에게 전송한다.

마지막으로 V는 U로부터의 서명을 검증하고 지불에 관련된 파라미터들을 전송 받게 된다. 검증에 성공하게 되면 V는 U에게 서비스를 제공하기 시작한다.

3. 티켓에 기반한 인증과 지불 모델

본 논문에서 고려하고 있는 티켓 기반 인증 및 지불 모델에서의 각 참여자들 간의 관계는 아래 <그림 2>와 같다. 티켓에 기반한 서비스 이용과 지불의 참여자는 사용자와 VASP 그리고 티켓 서버로 구성되어 있다. 티켓 서버는 일종의 인증 기관의 역할을 하는 특별한 TTP이다. 티켓을 이용한 서비스 제공자와의 인증 및 지불 메커니즘은 두 단계로 구분되어 진다. 우선 각 사용자는 티켓 서버에 등록되어 있다. 이동 사용자는 티켓 서버와 티켓 획득 프로토콜을 수행시킴으로써 티켓을 얻게 된다. 티켓 획득 단계는 사용자와 티켓 서버간에 이루어지는 것으로 서비스의 선별 그리고 티켓의 획득으로 이루어진다. 이 단계에서 사용자는 티켓 서버에게 획득한 티켓에 대한 지불을 수행한다.

티켓 획득 과정 다음에 수행되는 티켓 사용 단계에서는 사용자는 VASP에게 티켓 획득 과정에서 얻은 티켓을 VASP에게 전송한다. 그러면 VASP는 티켓의 불법적인 수정과 위조 여부를 검증하고 사용자가 티켓의 정당한 소유주임을 확인하기 위한 인증 과정을 수행한다. 만약 티켓의 검증이 성공적이면, 티켓의 조건에 따라서 사용자에게 서비스를 제공한다.

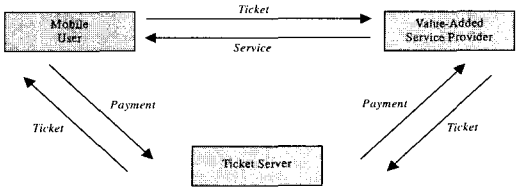

그림 2 티켓 기반 지불 모델

사용된 티켓은 VASP에게 저장이 되어서 나중에 티켓 서버에게 제출이 된다. 티켓 서버는 티켓을 제출한 VASP에게 서비스 제공에 대한 지불을 한다.

4. 티켓 획득 프로토콜

본 장에서는 사용자와 티켓 서버간에 수행되는 티켓 획득 프로토콜을 제시한다. 티켓 획득 프로토콜에서는 사용자는 VASP와의 익명 서비스 사용을 위해서 티켓 서버로부터 임시로 사용할 수 있는 서명을 위한 비밀키와 검증을 위한 공개키 그리고 VASP와의 세션키를 설정하는데 사용할 새로운 공개키와 비밀키를 얻게 된다.

4.1 티켓 구조

티켓은 사용자가 서비스를 이용하는데 있어서 사용하는 특별한 인증서이다. 티켓은 일련 번호 sn, 사용자의 키 설정용 공개키 g^u, 사용자의 서명을 검증할 수 있는 검증용 공개 키 PK_U, 티켓이 발행된 시간을 나타내는 티켓 서버의 타임스탬프 TT, 그리고 기타 정보에 대한 $data$를 가지고 있다. 이러한 파라미터들은 해쉬 함수 h로 처리되고 티켓 서버의 서명으로 이루어진다.

$$Ticket = \{sn, idT, g^u, PK_U, TT, data, Sig_T (h(sn, idT, g^u, PK_U, TT, data))\}$$

g^u는 VASP와의 세션 키 설정에 사용될 공개키로서 티켓에 포함되며 비밀키 u와 같이 사용자는 티켓 획득 프로토콜 수행 단계에서 티켓 서버로부터 전송 받게 된다. 익명 서비스 사용을 위해서 티켓 서버는 VASP와의 티켓 사용 단계에서 사용할 서명용 비밀키 SK_U를 생성하여 사용자에게 전송하고 대응되는 서명 검증용 공개키 PK_U를 티켓에 포함하여 사용자에게 전송하게 된다.

4.2 제안한 티켓 획득 프로토콜

아래에서 사용자와 티켓 서버는 각각 U와 T로 표현된다. 제안한 티켓 획득 프로토콜 수행 전에 U와 T는 비밀 세션키 L을 소유하고 있다고 가정한다. T의 신원은 idT로 나타내며 타임스탬프는 TT로 표시한다. 티켓 획득 프로토콜은 아래의 그림과 같이 수행된다.

사용자는 난수 r을 생성하여 자신의 신원 idU와 같이 T와의 비밀 세션키 L을 이용하여 암호화하고 T에게 전송한다.

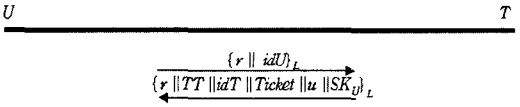

그림 3 티켓 획득 프로토콜

T는 U로부터 메시지를 받아 복호화를 하여 티켓을 요청하는 U의 신원과 난수 r을 획득한다. U의 신원을 파악한 T는 U의 인증서 취소 여부를 파악한다. 인증서가 취소되지 않았으면 T는 U가 VASP와의 통신에서의 세션키 설정에 사용될 새로운 난수 u를 생성하고 그에 대응되는 키 설정용 공개키 g^u를 생성한다. 또한 U가 VASP에게 전송할 서명에 사용될 비밀 서명키 SK_U와 그에 대응되는 서명 검증키 PK_U를 생성하여 4.1절에서와 같이 티켓을 계산해낸다. T는 티켓과 자신의 신원 idT, 난수 r, 타임 스탬프 TT 그리고 비밀키 u와 SK_U를 비밀 세션키 L을 이용하여 암호화 한 후 U에게 전송한다.

U는 T로부터의 메시지를 받아 복호화 한 후 티켓을 획득하고 T의 서명을 검증하게 된다. 티켓을 획득한 U는 T에게 지불을 수행한다. U는 VASP와의 세션키 설정에 사용할 키 설정용 키 쌍인 u와 g^u를 얻는다. 또한 서명에 사용될 임시 서명용 키 쌍인 SK_U와 PK_U를 얻어서 훗날 VASP와의 통신에 사용을 하게 된다.

5. 티켓 기반 인증 및 지불 프로토콜

본 장에서는 사용자와 VASP간에 티켓을 이용한 인증 및 지불 프로토콜을 제안한다. 5.1절에서는 티켓에 기반한 새로운 프로토콜을 제시하며 5.2절에서는 안전성 분석을 한다.

5.1 인증 및 지불 프로토콜

티켓 획득 프로토콜을 성공적으로 수행하게 되면, 사용자는 티켓 서버로부터 티켓을 전송받게 된다. 본 장에서는 티켓을 이용한 인증 및 지불 프로토콜을 제안한다. 제안된 프로토콜은 서비스 사용에 대한 비용 지불 가능 여부를 검사하기 위해 사용자의 온-라인 TTP에 접근하는 것이 아니라, VASP는 단지 티켓의 정당성과 사용자가 티켓의 소유주임을 확인하면 된다. 또한 티켓을 이용하여 익명 서비스 사용을 보장해줄 수 있다.

아래의 프로토콜에서 U는 사용자 그리고 V는 VASP를 나타낸다. $CertV$는 V의 신원을 나타내고 TV는 V가 생성한 타임스탬프를 의미한다. ch_data는 V가 U에게 보내주는 지불에 관련된 정보이다. h는 해쉬 함수이다.

제안된 인증 및 지불 프로토콜의 목적은 다음과 같다.

- U와 V간에 명확한 상호 인증;
- U와 V간에 상호 키 인증과 세션키 K의 성립;
- U와 V간에 상호 키 확인;

- 새로운 키에 대한 상호 확신;
- U의 티켓 사용에 대한 부인 방지.

제안된 프로토콜 시작전의 가정은 다음과 같다.

- U는 T로부터 부여받은 정당한 $Ticket$을 소유하고 있다;
- V는 T에 의해서 할당된 키 설정을 위한 공개키에 대한 인증서가 있다;
- U는 T의 공개된 서명 검증키를 가지고 있다.

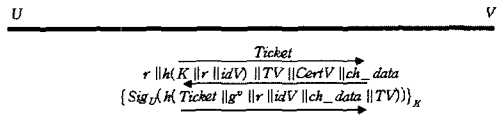

그림 4 티켓 기반 인증 및 지불 프로토콜

프로토콜(<그림 4>)이 시작되면 U는 티켓 획득 프로토콜에서 얻은 $Ticket$을 V에게 전송한다.

V는 $Ticket$으로부터 얻은 g^u와 자신의 키 설정용 비킬키 v를 이용하여 세션키 $K=h(g^{uv}||r)$을 계산한다. V는 난수 r을 생성하여 세션키 K와 자신의 신원 idV을 해쉬 함수 h로 처리하고 r과 타임 스탬프 TV 그리고 자신의 키 설정 공개키인 g^v에 대한 인증서 $CertV$와 같이 U에게 전송한다.

두 번째 메시지를 전송 받은 후, U는 $CertV$를 이용하여 V와 동일한 세션키 $K=h(g^{vu}||r)$ 를 계산한다. 그리고 해쉬 값을 검사한 후 V가 실제로 세션 키 K을 소유하고 있다는 것을 확인하게 된다. U는 150 $Ticket||g^u||r||idV||ch_data||TV$에 해쉬 함수 h를 취하고 생성된 값에 전자 서명을 하여 V에게 전송한다.

마지막 세 번째 메시지를 받은 후, V는 세션키 K를 이용해서 전달받은 메시지를 복호화 하고 사용자의 서명을 검증한다. 검증에 성공하면 U에게 서비스 제공을 시작한다. V는 티켓 서버에게 U의 서명을 제출하고 제공한 서비스에 대한 지불을 받게 된다.

5.2 안전성 분석

V의 키 확인과 인증: 두 번째 메시지에 $h(K||r||idV)$을 첨가하는 것은 V에서 U에게 키 확인과 함축적 키 인증 그리고 신원 인증을 해준다.

U의 키 확인과 인증: 세 번째 메시지의 티켓 $Ticket$을 세션키 K로 암호화하는 것은 키 확인을 해준다. 세 번째 메시지의 서명된 부분에 $Ticket||g^v||r$을 첨가하는 것은 $Ticket$의 소유주인 U를 확인하며 g^u는 g^v와 r에 연관되어서 U에서 V에게 키 인증을 해준다. V로부터 생성된 난수 r을 세 번째 메시지의 서명된 부분에 첨가하는 U에 대한 인증을 제공한다.

익명 서비스 사용: V에게 전송되는 티켓은 U의 신원 정보를 가지고 있지 않다. 또한 프로토콜 수행 중에 U는 서비스 사용을 위해 새로이 생성한 비밀 서명키를 이용하여 서명을 수행하므로 서비스 사용에 대한 익명성이 보장된다.

티켓 사용의 부인 방지: 마지막 메시지의 티켓 $Ticket$과 V의 신원 idV, 난수 r 그리고 타임스탬프 TV를 포함한 U의 전자서명은 티켓에 대한 서비스 사용의 부인 방지를 해준다.

서명의 암호화: 마지막 메시지의 티켓을 포함한 U의 전자서명은 세션키 K로 암호화된다. 이를 통하여 U가 세션키 K를 알고 있다는 것을 보여줄 수 있다. 또한 signer verification 공격[10] 그리고 content verification 공격[11] 을 방지할 수 있다.

새로운 키의 사용: 세션키 K는 V로부터 생성된 난수 r로부터 만들어진다. 이는 예전의 세션키 K가 재사용되는 것을 방지하기 위함이다. 또한 이것은 새로이 생성된 난수 u와 같이 U와 V 양쪽에 새로운 키라는 것을 제공한다. 이것은 각 세션마다 세션키 K가 같지 않으므로 제안한 프로토콜은 K를 알아내기 위한 code-book 공격[12]에 취약하지 않다.

두 번째 메시지에서의 idV: 이것은 source-substitution 공격[13]을 방지하기 위해서 필요하다. 또한 해쉬된 난수 r과 같이 K를 알아내기 위한 time-memory tradoeoff 공격[14]을 방지할 수 있다.

세 번째 메시지에서의 idV: idV 는 서명의 정당한 수신자를 지칭하기 위하여 반드시 서명 메시지에 첨가가 되어야 한다.

6. 정성적 분석

티켓에 있어서 문제가 되는 점은 불법적인 수정과 위조, 복제 그리고 재사용이다. 정당하지 못한 사용자는 티켓을 복제하여 사용할 수 있다. 그러나 티켓 사용 프로토콜에서의 서명을 생성해낼 수가 없으므로 티켓의 복제 사용은 방지될 수 있다. 티켓 서버이외의 엔티티로부터의 티켓의 수정과 위조는 가능하지 않다. 왜냐하면 사용자나 정당하지 못한 티켓의 사용은 티켓 서버의 서명을 생성해낼 수 없기 때문이다. 사용자가 티켓을 재사용 하면 티켓 서버는 동일한 티켓에 대한 사용자의 서명(제안한 프로토콜의 세 번째 메시지)을 중복해서 받게 된다. 따라서 티켓 서버는 사용자의 티켓 재사용 여부를

파악할 수 있으므로 티켓 재사용은 검출 될 수 있다.

<표 1>은 온-라인 TTP가 관여하는 AIP 프로토콜과 제안한 티켓 기반의 인증 및 지불 프로토콜의 특성을 비교하고 있다. 제안한 티켓 기반 프로토콜은 사용자의 지불 가능성을 검사하기 위하여 온-라인 TTP의 관여가 필요하지 않는다. 또한 티켓의 특성으로 사용자의 서비스 사용에 대한 익명성이 보장된다. 사용자는 티켓 서버에게 티켓을 획득하고 그에 대한 지불을 하기 때문에 기본적으로 선-지불(pre-paid) 방식이다. 하지만 티켓 안에 지불 초기화 파라미터 등을 포함하고 실제 서비스 이용 중에 소액 지불 기법을 수행하는 후 지불(post-paid) 방식으로도 변형될 수 있다. 사용자는 자신의 요구에 맞는 적절한 티켓을 구입함으로써 다른 사용자와의 차별화된 서비스 프로파일의 적용이 가능하다. 또한 사용자들은 원하는 서비스를 선택할 수 있으며 서비스 제공자와의 장기간에 걸친 계약을 할 필요가 없다.

표 1 AIP 프로토콜의 특성 비교

	온-라인 TTP의 AIP 프로토콜	제안한 프로토콜
사용자의 지불 가능성 검증	○	○
온-라인 TTP의 관여 여부	○	×
익명 서비스 사용	×	○
키 설정 알고리즘	ElGamal/Diffie-Hellman	Diffie-Hellman
지불 방식	선-지불	선-지불/후-지불
차별화된 서비스 프로파일	×	○
서비스 계약 기간	중기/장기	일회용/단기/중기/장기

○: 가능 ×: 불가능

AIP 프로토콜과는 다르게, 제안한 기법은 티켓 획득의 추가적인 단계가 필요하다. 그러나 대개의 경우, 티켓 획득 프로토콜은 이동 단말이 휴지 상태 일 때 수행 될 수 있다. 그리고 이동 단말의 제한된 능력을 고려할 때, n-times 티켓 (최대 n번 사용할 수 있는 티켓)[6] 또는 subscription (주어진 기간 동안 계속해서 사용할 수 있는 티켓)[6]이 매우 유용할 수 있다.

온-라인 TTP 기반 AIP 프로토콜과 제안된 인증 및 지불 프로토콜간의 사용자 측면에서의 성능 평가가 <표 2>와 <표 3>에 나와 있다. 프로토콜 비교에서 전처리는 프로토콜 시작 전에 수행할 수 있는 세션 키 생성 또는 공개키 생성을 위해 멱승(exponentiation)이 일어나는 횟수를 의미한다. 온-라인 처리는 프로토콜 수행 중에 세션 키 생성 또는 공개키 생성을 위해 멱승이 일어나는 횟수를 나타낸다. 서명 생성은 서명을 생성하는 횟수를 나타내며, 검증의 경우는 서명 또는 인증서의 검증 횟수를 의미한다. 암호화, 복호화는 세션키로 수행한 각각의 암호화, 복호화 횟수를 의미한다.

표 2 사용자 측면에서의 계산량 비교

	온-라인 TTP의 AIP 프로토콜	제안한 프로토콜
전처리	1	0
온-라인 처리	2	1
서명 생성	1	1
검증	2	1
암호화	2	0
복호화	1	1

제안된 프로토콜은 전처리, 온-라인 처리, 검증, 암호화, 복호화 등에 있어서 개선된 효율성을 보여주고 있다. VASP 측면에서의 성능 개선은 <표 3>에 나와 있다.

표 3 VASP 측면에서의 계산량 비교

	온-라인 TTP의 AIP 프로토콜	제안한 프로토콜
전처리	1	0
온-라인 처리	1	1
서명 생성	0	0
검증	3	2
암호화	0	0
복호화	1	1

7. 결 론

본 논문에서는 제 3세 이동 통신 시스템인 UMTS에서의 value-added 서비스를 위하여 티켓을 이용한 효율적인 인증과 지불 프로토콜을 제안하였다. 제안된 프로토콜은 티켓을 이용하여 사용자의 온-라인 TTP와의 통신 없이도 사용자의 지불 가능 여부를 VASP가 검증할 수 있으며 VASP는 단지 티켓의 정당성과 사용자가 티켓의 소유주임을 확인한다. 제안한 프로토콜은 온-라인 TTP가 관여하는 AIP 프로토콜과 비교하여 계산량과 통신 비용에 있어서 우수하며 또한 서비스 사용에 대한 사용자의 익명성이 보장된다.

참 고 문 헌

[1] UMTS Forum, "A Regulatory Framework for UMTS," Report no. 1, 1997.

[2] K. M. Martin et al, "Secure Billing for Mobile

Information Service in UMTS," IS&N LNCS 1430, pp.535-548, Springer-Verlag, May. 1998.
[3] ACTS AC095, ASPeCT Deliverable D02, Initial Report on Security Requirements, Feb. 1996.
[4] Gunter Horn and Bart Preneel, "Authentication and Payment in Future Mobile Systems," ESORICS, LNCS 1485, pp.277-293, 1998.
[5] B. Patel and J. Crowcroft, "Ticket Based Service Access for the Mobile User," pp.223-233, Mobicom, 1997.
[6] L. Buttyán and J-P. Hubaux, "Accountable and Access to Services in Mobile Communication Systems," Symposium on Reliable Distributed Systems, pp.384-389, 1999.
[7] T. P. Pedersen, "Electronic Payments of Small Accounts," Security Protocols, LNCS vol.1361, pp.59-68, Springer-Verlag, 1997.
[8] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, 1976.
[9] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Transactions on Information Theory, Vol. IT-31, No.4, pp.469-472, 1985.
[10] ISO/IEC 9796-2: 1997. Information Technology - Security techniques - Digital Signature giving message recovery - Part 2: Mechanisms using a hash-function.
[11] G. Horn, K. M. Martin and C. J. Mitchell, "Authentication Protocols for Mobile Network Environment Value-Added Services," submitted.
[12] W. Diffie, P. C. van Oorschot and M. J. Wiener, "Authentication and Authenticated Key Exchanges," Designes, Codes and Cryptography, vol.2, pp.107-125, 1992.
[13] J. Borst, B. Preneel and J. Vandewalle, "On the Time-Memory Tradeoff between Exhaustive Key Search and Precomputation," Symposium on Information Theory, Benelux, Veldhoven, Netherlands, pp.111-118, 1998.
[14] M. Hellman, "A Cryptanalytic Time-Memory Tradeoff," IEEE Transactions on Information Theory, vol.22, pp.644-654, 1976.

이 병 래

1998년 고려대학교 컴퓨터학과 학사. 2000년 고려대학교 컴퓨터학과 석사. 2002년 고려대학교 컴퓨터학과 박사. 2002년 ~ 현재 삼성전자 CTO전략실 소프트웨어센터 선임연구원. 관심분야는 이동 통신 보안, 암호 프로토콜, 네트워크 시스템

장 경 아

1997년 동덕여자대학교 전자계산학과 학사. 1999년 고려대학교 컴퓨터학과 석사. 2001년 고려대학교 컴퓨터학과 박사. 2002년 ~ 현재 삼성전자 CTO전략실 소프트웨어센터 선임연구원. 관심분야는 DRM, 분산 시스템 보안, 암호프로토콜, 그리드 컴퓨팅 시스템

김 태 윤

정보과학회논문지 : 정보통신
제 29 권 제 1 호 참조