글로벌 로밍 환경에서 시간 동기화 OTP를 포함한 티켓 기반 AAA 메커니즘에 관한 연구

문 종 식[†] · 이 임 영[††]

요 약

AAA(Authentication, Authorization, Accounting) 프로토콜은 유선망뿐만 아니라 무선망과 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 사용자 인증, 인가, 과금 기능을 체계적으로 제공하는 정보보호 기술이다. 현재 IETF(Internet Engineering Task Force) AAA 워킹 그룹에서도 AAA 프로토콜에 관하여 중요하게 다루고 있으며, 활발히 연구 중 이다. 최근 사용자의 익명성과 프라이버시 침해 측면에서 많은 문제점을 드러내고 있어 본 연구에서는 모바일 디바이스가 홈 인증 서버로부터 인증을 받고 난 후에 외부 네트워크로 이동하더라도 홈 인증 서버로부터 발급받은 티켓을 이용하여 홈 인증 서버로 접근 하지 않고 외부 네트워크에서의 인증을 제공하여 서비스를 받을 수 있게 한다. 또한 서비스를 이용하는데 있어 사용자의 프라이버시 및 익명성을 제공할 수 있는 방안에 초점을 맞춘다. 본 방식은 인증, 인가, 과금 중 인증과 인가에 초점을 두고 시간 동기화 OTP를 사용함으로써 제 3자의 공격에 안전하며, 안전하고 효율적인 인증방식을 제공한다. 또한 티켓을 사용함으로써 정당한 사용자만이 서비스를 제공받을 수 있고 교환되는 메시지 및 지연을 줄이며 지속적인 서비스를 제공받을 수 있어 안전성과 효율성을 높일 수 있다.

키워드 : AAA, 인증, 시간 동기화, 원타임 패스워드, 익명성, 프라이버시

A Study on Ticket-Based AAA Mechanism Including Time Synchronization OTP in Global Roaming Environment

Jong-Sik Moon[†] · Im-Yeong Lee[††]

ABSTRACT

AAA(Authentication, Authorization, Accounting) protocol is an information security technology that offer secure and reliable user Authentication, Authorization, Accounting function systematically in various services, protocol and wireless network as well as wire network. Currently IETF(Internet Engineering Task Force) AAA Working Group deal with about AAA protocol and studying with activity. But, recently it exposing much problems side to user's anonymity and privacy violation. Therefore, in this paper, AAAH(Home Authentication Server) authenticates Mobile device. after that, use ticket that is issued from AAAH even if move to outside network and can be serviced offering authentication in outside network without approaching by AAAH. Also, we study mechanism that can offer user's privacy and anonymousness to when use service. Our mechanism is using Time Synchronization OTP and focusing authentication and authorization. Therefore, our mechanism is secure from third party attack and offer secure and effective authentication scheme. Also only right user can offer services by using ticket, can reduce signal and reduce delay of message exchanged, can offer persistent service and heighten security and efficiency.

Key Words : AAA, Authentication, Time Synchronization, One-Time Password, Anonymity, Privacy

1. 서 론

인터넷 및 휴대용 디바이스의 발전으로 인해 사용자들은 다양한 서비스를 제공받고 있으며, 이동하면서도 동일한 서비스를 지속적으로 제공 받기를 원한다. 현재 다양한 서비스와는 반대로 보안에는 많은 취약점을 드러내고 있으며, 이러한 문제점들을 해결하는 방안으로 안전하고 효율적으로 사용자를 인증하고 인가하는 기술인 IETF 표준안으로 삼고 있는 AAA (Authentication, Authorization, Accounting) 기술이 있다. AAA 프로토콜은 기존의 유선망뿐만 아니라 비약적으로 발전하고 있는 무선망의 WiBro, Mobile IP 등과 같은 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 인증, 인가, 과금 기능

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원 사업의 연구결과로 수행되었음.
† 준 회 원 : 순천향대학교 컴퓨터학과 석사과정
†† 종신회원 : 순천향대학교 컴퓨터학부 교수
논문접수 : 2006년 10월 26일, 심사완료 : 2007년 2월 28일

을 체계적으로 제공하는 정보보호 기술이다. 현재 무선망에서의 모바일 사용자를 위한 인증, 인가, 과금 표준화를 목표로 다양한 응용 서비스에 대한 표준화 작업을 진행하고 있으며, 이기종망 간의 로밍 서비스 및 모바일 IPv6 네트워크망에서의 AAA를 이용한 다양한 연구가 진행 중 이다. AAA기술은 보안의 심각한 문제를 일으키는 IPv4/IPv6기반 유/무선에서의 안전한 인증을 제공하고 이동에 따른 사용자에 대한 인증에서도 적용 가능함으로 인해 사용자의 편의성 및 보안 측면에서의 해결책을 가져다 주고 있다.

모바일 디바이스를 이용하여 네트워크 서비스를 제공받고자 접근하는 사용자를 인증, 인가, 과금하는 기술로는 여러 방식이 있으나, 본 연구에서는 티켓을 기반으로 사용자 익명성과 프라이버시에 초점을 맞추어 편의성을 증대시키면서 안전하고 효율적인 방식을 제안한다. 2장에서는 기존 연구에 대하여 알아보며 3장에서는 제안 방식에 대하여 설명한다. 4장에서는 1장의 보안 요구 사항으로 제안 방식을 분석하고 마지막으로 5장에서는 결론 및 향후 연구방향으로 마치도록 한다.

1.1 보안 요구 사항

모바일 사용자에게 다양한 서비스를 제공하는데 있어 접근하는 사용자가 정당한 사용자이며 서비스를 이용할 수 있다는 것을 확인할 수 있어야 한다. 그러나 무선 네트워크의 특성으로 인해 사용자는 다양한 외부의 네트워크를 통해 접근할 수 있으며, 외부의 공격에 매우 취약하고 통신에 있어서 많은 제약사항이 뒤따르고 있다. 또한 서비스를 이용하는 방안에 있어 접근 시 마다 인증을 제공하는 방안을 제시하고 있으나 이러한 방식은 매번 외부의 네트워크에서 홈 네트워크의 인증 서버에 인증을 요청하여 오버헤드가 발생하는 문제가 있다. 이에 따라 초기 인증을 받은 사용자는 홈 인증 서버로부터 티켓을 발급받아 외부 네트워크로 이동하였을 때, 티켓을 이용하여 인증을 수행하는 방안에 대해서 논의가 되어져 왔다. 우선 외부의 네트워크에서 홈 인증 서버에 접근하는 데이터는 다음과 같은 보안 사항이 제공되어야 한다.

- 기밀성 : 사용자가 전송한 메시지는 통신 객체들만이 알 수 있어야 한다.
- 무결성 : 전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며, 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다.
- 인 증 : 접근하는 사용자가 정당한 사용자라는 것을 즉시 확인할 수 있어야 한다.
- 접근제어 : 정당하지 않은 사용자는 서비스를 이용할 수 없어야 한다.
- 익명성 : 사용자가 이용한 서비스에 대해서 제 3자가 알 수 없어야 한다.
- 프라이버시 : 사용자의 사적인 정보는 공개되지 않고 간섭받지 않아야 한다.

위의 보안 요구 사항 외에도 제 3자가 다음과 같은 공격을 할 수 있다.

- 재전송 공격 : 제 3자가 메시지를 재전송하여 인증 받는 것을 막을 수 있어야 한다.
- 위 장 : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다.
- 위조/변조 : 제 3자가 메시지를 변경하거나 생성하여 인증을 받을 수 없어야 한다.

또한 티켓을 이용함으로써 티켓의 요구 사항은 다음과 같다.

- 위 조 : 검증된 티켓으로 받아들일 수 있는 티켓의 생성이 불가능해야 한다.
- 복 제 : 티켓은 하나만 존재하여야 하며 복사본이 존재해서는 안 된다.
- 변 경 : 티켓의 내용을 변경할 수 없어야 한다.
- 재판매 : 다른 사용자에게 티켓이 양도될 수 있는가의 여부를 판단해야 한다.

그러므로 제안하는 방식은 티켓을 이용하여 인증을 수행함으로 위에서 언급한 모든 요구 사항을 고려해야 한다.

1.2 AAA 개요

본 절에서는 AAA에 대한 전반적인 설명이 아닌 DIAMETER의 개요를 설명함으로써 AAA의 활용에 대해 살펴보고, 제공하는 서비스 및 운용 형태에 따른 관리에 대해 살펴본다. DIAMETER AAA 프로토콜은 CDMA2000 1x/EVDO, IMT-2000, Wireless LAN, 휴대인터넷(WiBro), 유선 PPP 등의 다양한 액세스 망이 연동되는 유/무선 이동인터넷 환경에서 가입자에 대한 안전하고 신뢰성 있는 인증(Authentication), 인가(Authorization) 그리고 과금(Accounting) 등의 서비스를 제공하는 정보보호 프레임워크(Framework)이다[6][12].

DIAMETER 프로토콜의 구조는 구조적인 확장을 위해 메시지 생성 및 전송, 보안, 장애 처리 등 모든 AAA 응용에서 요구되는 기본사항과 과금 기능을 포함하고 있는 'DIAMETER Base Protocol'과 다양한 AAA 서비스를 제공해줄 수 있는 DIAMETER 응용 그리고 안전하고 신뢰성 있는 메시지의 전송을 위한 하부 전송계층으로 나누어진다. DIAMETER 응용서비스에는 단말의 이동성 지원을 위한 'DIAMETER Mobile IP 응용', 단말의 Link Layer 인증을 위한 'DIAMETER EAP (Extensible Authentication Protocol) 응용', 유선 PPP와 역 호환성(Backward Compatibility) 지원을 위한 'DIAMETER NASREQ(Network Access Server Requirement) 응용' 그리고 멀티미디어 서비스 인증을 위한 'DIAMETER SIP(Session Initiation Protocol) 응용'과 선불제(Pre-Paid) 과금 서비스를 위한 'DIAMETER CC(Credit Control) 응용' 등으로 구성되어 있다. DIAMETER 프로토콜의 특징은 다음과 같다.

첫째, 확장성이 뛰어난 차세대 인증 프로토콜로써 DIAMETER 프로토콜은 Base 프로토콜 위에 새로운 응용, Command 및 AVPs(Attribute Value Pairs)의 추가를 통하여 확장성을 제공하며, 사업자 망의 확장성을 위해 다양한 Agents(Relay/Redirect/Proxy/Translation Agent)를 통하여 망간 접속을 지원한다. 또한 Broker 서버를 통하여 사업자간 로밍 컨소시엄

구성 및 관리 기능을 제공한다.

둘째, 한층 더 강화된 보안 기능 제공할 수 있으며, 이를 위하여 TLS(Transport Layer Security) 및 IPSec(IP Security)를 이용하여 전송 계층의 Hop-by-Hop 보안을 제공하고, End-to-End간의 보안까지 제공하여 서버 간 메시지의 안전한 전송을 보장한다.

셋째, 신뢰성 있는 전송계층 프로토콜 사용할 수 있다. 신뢰성 기반의 전송 프로토콜인 TCP(Transport Control Protocol) 또는 SCTP(Stream Control Transmission Protocol) 사용으로 안전하고 신뢰성 있는 메시지 전송이 가능하며, 종량제 과금의 99%까지 회수가 가능하다.

넷째, 강화된 장애 복구 및 재전송 기능을 제공하는데 전송계층의 Peer 관리 기능을 통하여 전송계층의 실패(Failure)에 대한 검출(Detection) 및 복구(Failover) 기능을 제공하고, 복구 시 Proxy 서버가 자동적으로 메시지를 Next-Hop의 Peer로 재전송 하도록 되어 있어서 Proxy 분산 환경에 아주 적합하다.

마지막으로 향상된 세션관리 및 호환성을 제공하는데 이것은 서버 Initiate 메시지를 통하여 AAA 서버가 NAS(Network Access Server)에게 특정 세션의 종료나 재인증/재인가 및 다양한 과금정책 적용을 할 수 있는 향상된 세션관리를 지원하고, 기존 RADIUS 프로토콜의 변환(Conversion)을 통한 호환성을 제공한다.

1.3 티켓 방식의 개요

티켓이란 사용자가 어떤 권리를 부여받았다는 것을 보여주는 한 조각의 데이터를 말한다. 티켓 기반 모델(Ticket Based Model)이란 이러한 티켓을 사용하는 인증 모델이며, 도메인간의 인증(Cross-domain Authentication) 방법의 대표적인 것 중의 하나가 바로 티켓 기반 모델이다. 서비스를 요구하는 사용자는 신용정보(Credential)로써 티켓을 서비스 공급자에게 제출하고, 서비스 공급자는 티켓을 확인하여 티켓에 맞는 서비스를 제공하게 된다.

예를 들어 설명하자면, 다양한 놀이기구 시설을 갖춘 놀이공원을 생각해 보았을 때 놀이기구들을 이용하기 위해서는 우선 놀이공원에 대한 입장권을 구매해야 한다. 놀이공원의 입장권은 성인, 청소년, 미취학 아동 등과 같은 고객에 대한 세분화되어져 있다. 고객들은 자신이 성인인지 청소년인지 혹은 미취학 아동인지를 증명할 수 있는 증명 자료를 제시함으로써 서로 다른 형태의 입장권을 발급 받게 된다. 놀이공원 관계자들은 입장권을 소지한 고객에 대해서만 놀이공원의 입장을 허용하게 되는 것이다. 이제 이렇게 발급 받은 입장권을 제시하고 놀이공원에 입장해 본다. 다양한 종류의 흥미진진한 놀이기구들이 펼쳐질 것이다. 한 종류의 놀이기구를 선택하여 놀이기구에 탑승하려 했더니 놀이공원 관계자의 제지를 받게 된다. 이유는 이용권을 보여 달라는 것이다. 모두 알고 있듯이 놀이공원에서 입장권과 별도로 놀이기구 이용을 위한 탑승권을 다시 구매해야만 한다. 각 놀이기구마다 입장권 구매 시와 같이 성인, 청소년, 미취학 아동과 같은 고객 구분에 따라 서로 다른 종류의 이용권을 구매해야 하는 것이다. 하지만 이렇게 이용자들은 각 놀이기구마다의 입장권 구매를 위해 대기해야 하는 불편을 겪게 되는데, 이러한 문제를 해결할 수 있는 방법이 자유 이용권을 고객이 입장권 구매하는 시기에 함께 구매하는 방법이다. 이는 놀이기구별로 이용권을 발급 받는 데 걸리는 대기시간을 훨씬 줄일 수 있다. 또한 입장권 발급 초기단계에서 고객들은 자신의 신분을 증명할 수 있는 증명 자료를 한번 만 제시하면 되기 때문에 중요한 자료를 여러 번 펼쳐 보일 필요가 없는 점에서도 훨씬 효율적이다. 물론 입장권과 자유 이용권의 발급에 따른 소요 시간이 두 배로 걸리기는 하나 이는 각 놀이기구에 따른 개별 이용권발급에 따른 시간에 비교해볼 때 간과할 만하다.

티켓의 개념은 위의 현실모델에서 제시한 입장권과 자유이용권의 기능을 모두 가지고 있다고 이해하면 정확할 것이다. 새롭게 정의되는 AAA 모델에서 사용되는 티켓은 이동 노드가 제시하는 신용정보(Credential)를 바탕으로 인증 과정과 권한 설정 과정을 거친 후 이동 노드에게 발급된다. 사용자는 티켓만으로 어느 곳에서나 서비스를 요청하고 제공받을 수 있기 때문에, 티켓 기반 모델은 많은 사용자의 이동성 서비스에 적합한 모델이며, Kerberos 시스템이 대표적인 티켓 기반 인증 모델이다[7].

티켓기반 모델은 티켓의 안전성 여부가 전체 모델의 안전성에 큰 영향을 미치므로 티켓 기반 모델을 사용하기 위해서는 다음과 같은 문제점들을 해결하여야 한다[5].

- 복제(Duplication) : 티켓은 하나만이 존재하여야 하며 복사본이 존재해서는 안 된다. 티켓의 복제는 악의적인 사용자와 도청하는 사람에 의해서 이루어질 수 있다. 이 문제는 암호화나 nonce를 이용하는 방법으로 해결할 수 있다.
- 위조(Forgery) : 네트워크가 검증된 티켓으로 받아들일 수 있는 티켓의 생성이 불가능해야 한다. 이것은 암호화나 비밀정보를 티켓에 삽입함으로써 방지할 수 있다.
- 변경(Modification) : 클라이언트는 티켓의 내용을 변경할 수 있어서는 안 된다. 이것은 클라이언트가 티켓의 범위를 넘어서는 서비스를 받을 수 없다는 것을 말한다. 이것은 일방향 해쉬 함수를 사용하여 쉽게 해결할 수 있다.
- 재판매(Re-sale) : 티켓이 다른 이용자에게 양도될 수 있는가를 말한다. 이것이 문제인가는 아직 논란 중이다. 티켓 발급자는 원 소유주 이외의 사람이 티켓을 사용하는 것을 원하지 않을 수도 있지만, 티켓의 재판매는 티켓의 시장을 활성화할 수도 있다.

2. 기존 연구

기존 연구로 대표적인 중앙집중식 인증 방식과 AAA에서 티켓을 이용한 인증 방식에 대하여 알아보고 각 방식별 특징 및 장/단점에 대해서 언급한다.

2.1 Kerberos

가장 대표적인 티켓 방식으로 사용자에게 서비스를 안전하게 이용할 수 있도록 인증 서비스를 제공하고 있는 Kerberos가 있

다[10]. Kerberos는 중앙 집중식 인증 서버를 사용하고, 암호화 방식은 대칭키 암호화 방식을 사용하여 인증을 수행한다. 사용자가 서비스를 제공받기 위해서는 인증 서버에서 티켓-승인 티켓을 발급 받고, 티켓 발행 서버에서 서비스-승인 티켓을 발행받아 서비스를 이용하게 된다. 각각의 Kerberos 구성요소에 접근하기 위해서는 사전에 약속된 패스워드를 기억하고 있어야 한다. 현재 Kerberos 프로토콜은 버전 4에서 버전 5까지 개발되었으며 이는 IETF RFC 4120에 표준화 되어 있다. 이러한 Kerberos 프로토콜의 경우 패스워드의 취약점을 안고 있으며, 티켓 발행 서버가 세션키를 분배해주기 때문에 사용자와 서비스 제공 서버 사이에 전송되는 메시지 정보를 알 수가 있어 익명성과 프라이버시를 제공하지 않는다. 또한 Kerberos 서버가 인증 서버와 티켓 발행 서버로 분리되어 있어 인증 요청 시 지연이 발생할 수 있는 문제점을 안고 있다[9].

2.2 Mobile IP 네트워크에서 티켓기반 AAA 메커니즘에 관한 방식

본 방식은 Mobile IP기반 이동성을 가지는 AAA에 대하여 제안하였으며, 특히 ISP(Inter Service Provider)와 모바일 무선 사용자들을 위해 보안 문제 및 효과적인 이동성 서비스에 대해 제안하였다. 본 방식에서는 MIPv6(Mobile IPv6)에서 모바일 노드를 인증하는데 지연 및 위험을 줄이고 서비스를 제공하는데 있어 사용자에게 인증과 인가를 제공 할 수 있는 티켓 방식의 새로운 AAA 서비스 메커니즘을 제안하였다. 또한 바인딩 업데이트에서 지연을 줄이기 위해 확장된 AAA 구조와 AAA 브로커 모델을 제안하였다[2].

시뮬레이션 결과 티켓을 사용함으로 인해 교환되는 메시지의 횟수를 줄임으로써 AAA 브로커 모델의 응답속도를 최소화 하고 보안의 효율성을 높이며, AAA 모델의 응답속도가 줄어듦을 보여준다. 티켓은 안전성을 개선하기 위해 사용자 정보의 노출을 최소화 하고 티켓의 유효시간 내에 서비스의 재인증이 요구되지 않기 때문에 효율성을 제공한다. 그러나 티켓 발행 단계에서 인증과 티켓 발행의 분리로 지연을 발생시킨다.

2.3 익명성과 프라이버시 보장을 위한 인증 방식

본 방식에서는 인터넷을 통해 다양한 콘텐츠 서비스를 사용자가 편리하게 이용할 수 있도록 EAP-TLS 인증 방식과 SKKE(Symmetric-Key Key Establishment) 방식을 이용하여 보다 효율적인 인증 메커니즘을 설계하였다. 제안하는 메커니즘에서는 사용자가 인증서 방식을 통해 AAA 서버로부터 인증을 받으면 인증 서버와 가맹 관계에 있는 콘텐츠 제공자에는 별도의 로그인 과정 없이 서비스를 이용할 수 있는 SSO(Single Sign On) 서비스, 사용자 익명성 및 프라이버시를 제공한다. 사용자가 익명성을 필요로 하는 콘텐츠 서비스를 이용할 경우 사용자의 익명성을 보장 해주며 사용자와 콘텐츠 제공자가 안전하게 데이터를 전송하기 위해 사용 할 세션키를 인증 서버에게 노출시키지 않고 교환한다. 콘텐츠 제공자 마다 다른 세션키를 사용함으로서 사용자의 프라이버시를 보장해 준다[9].

2.4 실시간 서비스를 위해 티켓에 기반 AAA 프로토콜에 관한 방식

무선 통신 서비스의 수요가 급격히 증가함에 따라 무선 주파수의 부족이 무선 네트워크 발전의 걸림돌이 되고 있다. 최근 주파수 대역이 충분히 활용되고 있지 않음을 보여주고 있으며, 이 문제에 대해서 본 방식에서는 주 사용자가 사용하지 않는 주파수를 일시적으로 이차 사용자에게 허가를 해주는 실시간 Secondary Market Service 개념을 소개하였다. 또한 AAA 시스템 구조를 제안하고 이차 사용자를 인증, 인가하는 메커니즘과 다중의 이차 장치 간 동기화를 제공하면서 Secondary Market Service를 관리하는 방식을 제안하였다. 본 방식에서는 공개키를 이용하여 티켓을 브로드캐스트 하여 모든 단말기들이 자신의 티켓인지 확인하는 과정이 필요하며, 특히 티켓에 대한 안전성은 난수에 의존하고 있다.

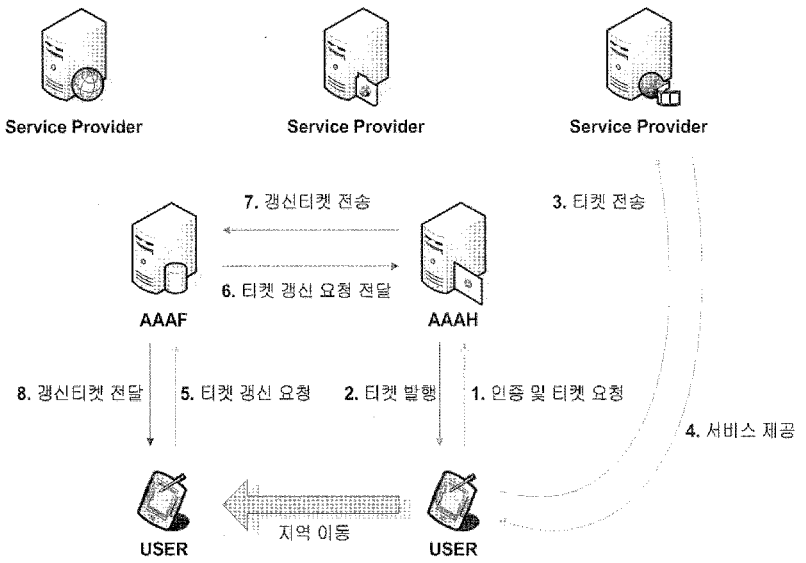
3. 제안 방식

기존 방식은 사용자가 외부 네트워크로 이동하였을 때 티켓을 새로 발급 받거나 재인증을 요청하여 지연 및 오버헤드가 발생하였으며, 또한 연산량이 많아 모바일 환경에 적용하기 적합하지 않았다. 이에 본 제안 방식은 모바일 디바이스를 사용하는 사용자가 홈 인증 서버에 접근하여 인증을 받고 티켓을 발급받은 후에 서비스 제공자에게 티켓을 제시함으로써, 서비스를 제공 받을 수 있다. 또한 외부 네트워크로 이동하더라도 티켓을 이용하여 인증을 제공 받을 수 있으며, 외부 네트워크에서도 티켓을 갱신하여 사용할 수 있다. 이와 같은 방식을 이용하면 인증 절차에서 발생하는 지연을 감소시킬 수 있으며, 사용자가 외부 네트워크로 이동하더라도 티켓을 이용하여 인증을 제공 받을 수 있다. (그림 1)에서와 같이 사용자는 홈 인증 서버에서 티켓을 발행 받아 서비스 제공자에게 전송하여 서비스를 제공받는다. 그 후 사용자가 이동하여 외부 네트워크에 위치해 있더라도 티켓을 갱신할 경우 홈 네트워크로 이동하여 티켓을 갱신할 필요 없이 외부 네트워크의 지역 인증 서버를 통해서 티켓을 갱신하여 서비스를 지속할 수 있다. 이때 티켓에 포함된 구성요소 중 익명 아이디를 사용함으로 인해 사용자의 익명성을 제공하며 홈 인증 서버에 통신 내용이 노출되지 않아 프라이버시가 제공된다.

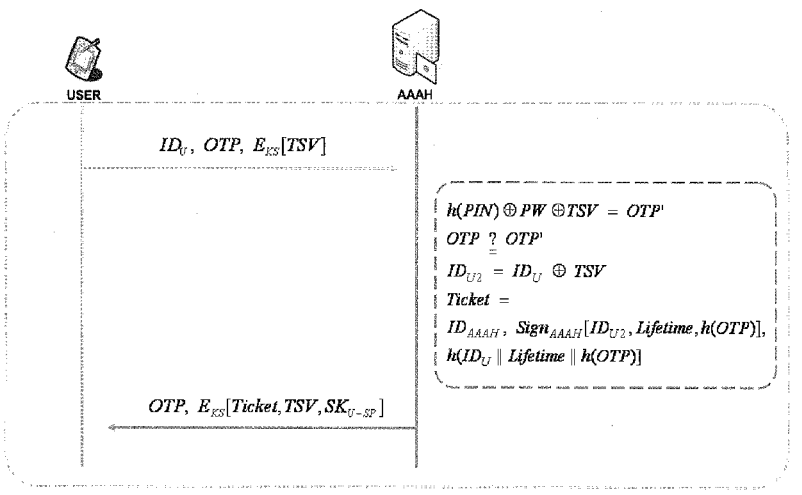
3.1 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수이다.

- $*$: 각각의 개체 (U : 사용자, $AAAF$: 지역 인증 서버, $AAAH$: 홈 인증 서버, SP : 서비스 제공자)
- ID_* : $*$의 아이디
- PW : 사용자의 패스워드
- PIN : 사용자가 소지한 모바일 디바이스의 일련번호
- $h()$: 충돌성이 없는 안전한 일방향 해쉬 함수
- OTP : One-Time Password
- TSV : Time Synchronization Value



(그림 1) 제안 방식 전체 흐름도



(그림 2) 티켓 및 인증 요청 단계

- $E_*[\,]$: *의 키로 암호화
- R_* : *이 선택한 랜덤수
- $Sign_*$: *의 개인키로 서명
- KS : 사용자와 홈 인증 서버가 공유한 대칭키
- SK_{U-SP} : 사용자와 서비스 제공자 사이의 세션키
- KU_* : *의 공개키
- KR_* : *의 개인키
- $Lifetime$: 티켓의 유효시간

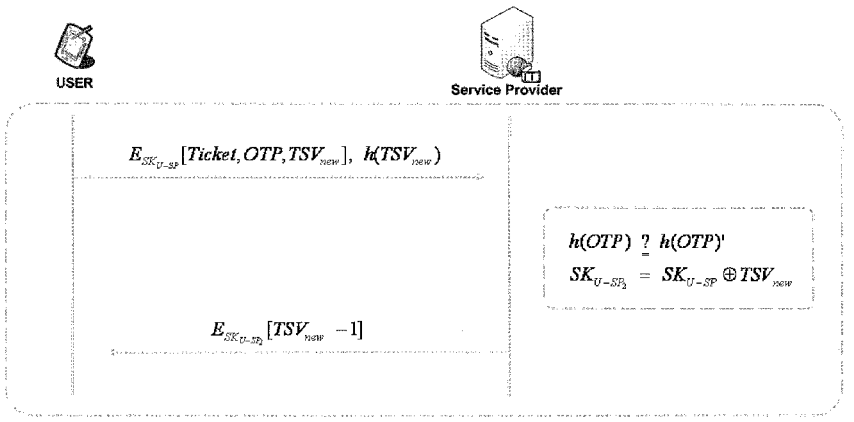
3.2 제안 프로토콜

제안 프로토콜은 총 3단계로 이루어진다. 사용자 패스워드와 통신에 사용되는 대칭키는 사전에 분배되었다고 가정하며, 각 단계는 인증 및 티켓 요청 단계, 서비스 요청 단계, 외부 네트워크에서 티켓 갱신 단계로 이루어진다.

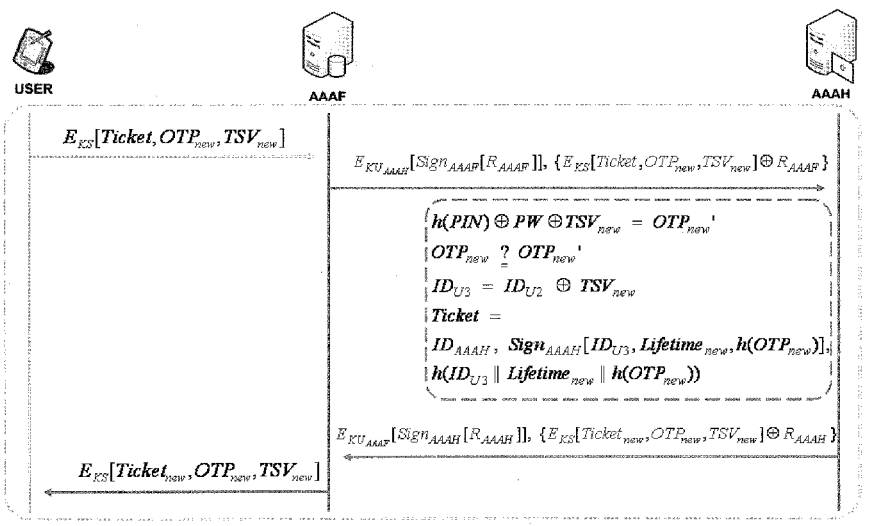
가. 인증 및 티켓 요청

인증 및 티켓 요청 단계는 사용자가 사전에 공유된 대칭키를 이용하여 데이터를 암호화 하고 인증을 요청한다. 인증은 시간 동기화 *OTP*(One-Time Password)를 이용하여 제공하며, 정당하게 인증 받은 사용자는 홈 인증 서버로부터 티켓 및 서비스 제공자와 통신에 이용될 세션키를 발행받게 된다.

Step 1. 사용자는 자신이 소유한 모바일 디바이스의 일련번호 해쉬 값(모바일 디바이스의 일련번호는 비트가 동일하지 않기 때문에 해쉬 연산을 하여 비트자리를 동일하게 한다.)과 패스워드, *TSV*(시간 동기화 값)을 XOR 연산 한 *OTP*를 생성한다. 그 후, 사용자는 홈 인증서버에 자신의 아이디와 *OTP*, *TSV*를 사전에 공유한 대칭키로 암호화한 값을 전송한다. *OTP*는 *TSV*를 기반으로 하기 때문에 값이 랜덤하게 발생하여 반복되지 않으며, 재전송 공격에 안전하다.



(그림 3) 서비스 요청 단계



(그림 4) 외부 네트워크에서 티켓 갱신 단계

$$OTP = h(PIN) \oplus PW \oplus TSV \quad (1)$$

$$ID_U,\ OTP,\ E_{KS}[TSV] \quad (2)$$

Step 2. 홈 인증 서버는 사용자로부터 받은 암호화된 TSV를 복호화 한 다음 자신의 데이터베이스에 저장된 사용자가 소지한 모바일 디바이스의 일련번호 해쉬 값과 패스워드 그리고 전송받은 TSV를 XOR 연산하여 $OTP'(h(PIN) \oplus PW \oplus TSV)$를 생성하고 전송된 OTP와 비교한다. 값이 동일하면 사용자의 아이디에 TSV를 XOR 연산하여 갱신 아이디와 티켓을 생성한다. 티켓은 사용자의 갱신 아이디, 티켓의 유효시간, 해쉬함수를 적용한 OTP를 홈 인증 서버의 개인키로 서명한 값 그리고 홈 인증 서버의 아이디, 무결성 검증 값으로 구성되어 있다. 홈 인증 서버는 OTP, 티켓, TSV, 사용자와 서비스 제공자 사이에 사용될 세션키를 사전에 공유한 대칭키로 암호화하여 전송한다. 이 단계에서 사용자의 아이디와 TSV를 XOR 연산하여 갱신 아이디를 생성하는 것은 사용자가 서비스를 이용하는데 있어 익명성을 제공하기 위해서이다.

$$h(PIN) \oplus PW \oplus TSV = OTP' \quad (3)$$

$$OTP \stackrel{?}{=} OTP' \quad (4)$$

$$ID_{U_2} = ID_U \oplus TSV \quad (5)$$

$$Ticket = ID_{AAAH},\ Sign_{AAAH}[ID_{U_2},\ Lifetime,\ h(OTP)],\ h(ID_{U_2} \| Lifetime \| h(OTP)) \quad (6)$$

$$OTP,\ E_{KS}[Ticket,\ TSV,\ SK_{U-SP}] \quad (7)$$

나. 서비스 요청

사용자가 서비스를 이용하고자 할 때, 홈 인증 서버로부터 발급받은 티켓을 서비스 제공자에게 전송하여 인증을 받고 서비스를 제공 받을 수 있다. 이 단계에서 티켓에 포함된 갱신 아이디로 익명성이 제공되고, 사용자와 서비스 제공자가 세션키를 갱신함으로써 프라이버시를 제공한다.

Step 1. 사용자는 홈 인증 서버로부터 전송받은 세션키로 발행받은 티켓, OTP, TSV_{new}(새로운 시간 동기화 값)를 암호화

하여, 무결성 검증 값과 서비스 제공자에게 전송한다.

$$E_{SK_{U-SP}}[Ticket,\ OTP,\ TSV_{new}],\ h(TSV_{new}) \quad (8)$$

Step 2. 서비스 제공자는 세션키로 전송받은 메시지를 복호화 한다. 메시지에 포함된 티켓을 홈 인증 서버의 공개키로 복호화 하여 사용자의 갱신 아이디와 유효시간, 해쉬함수를 적용한 OTP를 획득한다. 사용자로부터 전송받은 메시지안의 OTP를 해쉬하여 $h(OTP)'$를 생성하고 티켓에 포함된 $h(OTP)$와 비교 한다. 비교 값이 올바르면, TSV_{new}를 이전 세션키($E_{SK_{U\ SP}}$)와 XOR 연산하여 세션키를 갱신($E_{SK_{U-SP_2}}$)한다. 그 후 정당한 서비스 제공자라는 것을 증명하기위해 전송받은 TSV_{new}에 연산 ($TSV_{new}-1$)을 하고 갱신된 세션키로 암호화 하여 전송한다. 이 단계에서 서비스 제공자는 사용자를 인증하더라도 신원은 확인할 수 없다. 이는 갱신된 아이디를 티켓에 포함하였기 때문에 사용자가 어떠한 서비스를 이용하더라도 신원을 확인할 수 없어 익명성을 제공한다. 또한 세션키에 TSV_{new}를 XOR 연산하여 세션키를 갱신하여 통신에 사용하기 때문에 홈 인증 서버는 통신 내용을 알 수 없으므로 프라이버시를 제공한다.

$$h(OTP) \stackrel{?}{=} h(OTP') \quad (9)$$

$$SK_{U-SP_2} = SK_{U-SP} \oplus TSV_{new} \quad (10)$$

$$E_{SK_{U-SP_2}}[TSV_{new} - 1] \quad (11)$$

다. 외부 네트워크에서 티켓 갱신

사용자가 홈 네트워크에서 외부 네트워크로 이동하여 티켓을 갱신하고자할 경우, 사용자는 외부 네트워크에서 티켓을 갱신하여 서비스를 지속적으로 제공 받을 수 있다.

Step 1. 사용자는 지역 인증 서버에게 티켓과 OTP_{new}, TSV_{new}를 홈 인증 서버와 공유한 대칭키로 암호화 하여 전송한다. 이 메시지는 티켓 갱신 요청메시지 이다.

$$E_{KS}[Ticket,\ OTP_{new},\ TSV_{new}] \quad (12)$$

Step 2. 지역 인증 서버는 사용자가 전송한 값에 자신의 랜덤수(R_{AAAF})를 XOR 연산하고 랜덤수를 서명하여 홈 인증 서버의 공개키로 암호화한 값과 함께 홈 인증 서버에 전송한다.

$$E_{KU_{AAAH}}[Sign_{AAAF}[R_{AAAF}]],\ \{E_{KS}[Ticket,\ OTP_{new},\ TSV_{new}]\oplus R_{AAAF}\} \quad (13)$$

Step 3. 홈 인증 서버는 자신의 개인키로 복호화 하여 지역 인증 서버의 랜덤수(R_{AAAF})를 획득한다. 획득한 랜덤수로 티켓 갱신 요청 메시지가 포함된 메시지를 XOR 연산하여 메시지를 획득한다. 티켓 갱신 요청 메시지를 공유한 대칭키로 복호화 하여 티켓을 확인하고 사용자로부터 받은 TSV_{new}를 자신의 데이터베이스에 저장된 사용자가 소지한 모바일 디바이스의 일련번호 해쉬 값과 패스워드를 XOR 연산하여 OTP_{new}'를 생성하고 전송된 OTP_{new}와 비교하여 사용자를 인증한다. 인증이 완료되면 이전에 사용하던 갱신 아이디에 사용자로부터 받은 TSV_{new}를 XOR 연산하여 새로운 갱신 아이디를 생성하고 티켓을 갱신한다. 갱신된 티켓을 OTP_{new}, TSV_{new}와 사용자와 공유한 대칭키로 암호화한다. 그 값에 홈 인증 서버의 랜덤수(R_{AAAH}) XOR 연산한다. 랜덤수를 서명하고 지역 인증 서버의 공개키로 암호화 하여 갱신된 티켓 갱신 응답 메시지에 랜덤수를 XOR 연산한 값과 함께 전송한다.

$$h(PIN) \oplus PW \oplus TSV_{new} = OTP_{new}' \quad (14)$$

$$OTP_{new} \stackrel{?}{=} OTP_{new}' \quad (15)$$

$$ID_{U_3} = ID_{U_2} \oplus TSV_{new} \quad (16)$$

$$Ticket_{new} = ID_{AAAH},\ Sign_{AAAH}[ID_{U_3},\ Lifetime,\ h(OTP_{new})],\ h(ID_{U_3} \| Lifetime \| h(OTP_{new})) \quad (17)$$

$$E_{KU_{AAAF}}[Sign_{AAAH}[R_{AAAH}]],\ \{E_{KS}[Ticket_{new},\ OTP_{new},\ TSV_{new}]\oplus R_{AAAH}\} \quad (18)$$

Step 4. 지역 인증 서버는 자신의 개인키로 복호화 하여 홈 인증 서버의 랜덤수(R_{AAAH})를 획득한다. 획득한 랜덤수로 메시지를 XOR 연산하여 티켓 갱신 응답 메시지를 획득하고 사용자에게 전송한다.

$$E_{KS}[Ticket_{new},\ OTP_{new},\ TSV_{new}] \quad (19)$$

Step 5. 사용자는 이후 서비스 요청 단계와 동일하게 갱신된 티켓을 이용하여 서비스를 제공 받을 수 있다.

4. 제안 방식 분석

제안 방식의 프로토콜을 1장에서 언급한 안전성과 제 3자의 공격 및 티켓의 보안 요구 사항에 맞추어 분석하고 통신에 따른 효율성을 분석하면 다음과 같다.

가. 기밀성

사용자가 전송한 메시지는 통신 객체들만이 알 수 있다. 홈 인증 서버와 사용자 사이에는 공유한 대칭키(E_{KS})로 메시지를 암호화 하여 전송하고, 홈 인증 서버와 지역 인증 서버 사이에는 공개키($E_{KU_{AAAF}}$, $E_{KU_{AAAH}}$)를 이용하여 암호화하기 때문에 대칭키와 공개키로써 기밀성을 제공한다. 또한 사용자와 서비스 제공자 사이에 이용되는 세션키($E_{SK_{U-SP}}$)는 초기 홈 인증 서버로부터 제공되나 통신 중에 갱신하여 사용한다.

나. 무결성

전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며, 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다. 제안 방식에서는 각 메시지마다 해쉬 값($h(TSV_{new})$)과 $OTP(h(PIN)\oplus PW\oplus TSV)$를 검증함으로써

〈표 1〉 통신에 따른 효율성 분석표

	2.1	2.2	2.3	2.4	제안 방식
총 통신 횟수	7회	14회	14회 (EAP-TLS 포함)	13회 (티켓 갱신 포함)	8회 (티켓 갱신 포함)
초기 인증 통신 횟수	2회 (상호인증)	4회 (상호인증)	6회 (EAP-TLS)	1회 (단일인증)	2회 (상호인증 및 티켓 발행)
홈 네트워크 티켓 갱신	제공 안함	4회	제공 안함	3회	2회
외부 네트워크 티켓 갱신	제공 안함	4회	제공 안함	제공 안함	4회
메시지의 암호화 연산	대칭키 : 8회	대칭키 : 6회	대칭키 : 4회 공개키 : 4회	대칭키 : 6회 공개키 : 1회	대칭키 : 6회 공개키 : 2회
해쉬 연산	0회	0회	0회	3회	3회
키 갱신 횟수	제공 안함	제공 안함	1회	1회	1회
보유 키 개수 (사용자 측면)	3개	3개	3개	2개	2개

제공한다.

다. 인증

접근하는 사용자가 정당한 사용자라는 것을 즉시 확인할 수 있어야 한다. 제안 방식에서는 Time Synchronization *OTP* ($h(PIN) \oplus PW \oplus TSV$)를 이용하여 인증을 제공한다. 정당한 사용자라면 자신이 소유한 디바이스의 일련번호, 패스워드, 시간 동기화 값을 이용해 바로 검증할 수 있다.

라. 접근제어

정당하지 않은 사용자는 서비스를 이용할 수 없어야 한다. 정당하게 인증을 받은 사용자만이 티켓을 획득할 수 있기 때문에 티켓을 획득하지 못한 사용자는 서비스를 제공받을 수 없다.

마. 익명성, 프라이버시

사용자가 이용한 서비스에 대해서 제 3자가 알 수 없어야 하며, 사용자의 사적인 정보는 공개되지 않고 간섭 받지 않아야 한다. 사용자가 홈 인증 서버로부터 인증을 받은 후에 홈 인증 서버는 사용자의 아이디와 시간 동기화 값을 XOR 연산하여 아이디를 갱신($ID_{U_2} = ID_U \oplus TSV$)함으로써 서비스 제공자는 사용자의 실제 아이디를 알 수 없다. 또한 사용자와 서비스 제공자 사이에 세션키(SK_{U-SP_2})를 갱신함으로써 홈 인증 서버는 통신 내용을 알 수 없어 사용자의 프라이버시가 제공된다. 그러나 프라이버시 측면에서 AAAH가 세션키를 생성하여 분배하므로 악의적인 목적을 가진 AAAH라면 통신의 모든 데이터를 도청하였을때 내용을 볼 수 있다는 문제점이 있다.

바. 재전송 공격, 위조, 변조

제 3자의 공격에 대하여 안전하여야 한다. 시간 동기화 *OTP*와 통신 메시지에 사용되는 시간 동기화 값(*TSV*), 홈 인증 서버의 랜덤수(R_{AAAH}), 지역 인증 서버의 랜덤수(R_{AAAF})를 이용하여 제 3자의 재전송 공격으로부터 안전하다. 또한 홈 인증 서버의 서명($Sign_{AAAH}$)과 각 메시지의 암호화로 위조 및 변조로부터 안전하다.

사. 효율성

티켓을 사용함으로써 사용자는 매번 홈 인증 서버로부터 인증을 요청하지 않고 서비스를 제공받을 수 있다. 이는 인증 지연 및 홈 인증 서버의 오버헤드를 감소시킴으로써 효율성을 제공한다. 티켓의 발행에서 소요되는 시간은 매번 홈 인증 서버로부터 인증을 요청하는 시간에 비하여 매우 미비하기 때문에 문제시 될 수 없다. 본 제안 방식을 사용자가 이동하여 서비스를 이용할 때, 서비스 제공자와 세션키를 갱신함으로 메시지 교환 횟수가 증가되나 프라이버시를 제공한다는 측면에서 효율성을 제공한다. 또한 사용자와 서비스 제공자 사이의 통신에서 프라이버시를 위한 목적으로 세션키를 갱신하나 모바일 디바이스의 특성을 고려하였을 때 비효율적이라는 문제점이 있다.

아. 티켓의 위조, 복제, 변경, 재판매

티켓의 복제는 암호화와 서명($Sign_{AAAH}$)으로 위조 및 변조는 갱신 아이디(ID_{U2})와 티켓의 유효시간(*Lifetime*), 홈 인증 서버의 서명으로 안전하다. 티켓의 재판매에 대한 사항은 고려하지 않았다.

〈표 2〉 제안 방식 분석표

		2.1	2.2	2.3	2.4	제안 방식
기밀성		○	○	○	○	○
		대칭키	대칭키	공개키/대칭키	공개키/대칭키	공개키/대칭키
무결성		X	X	△	○	○
		무결성 검증 단계 없음	무결성 검증 단계 없음	묵시적인 무결성 제공	해쉬함수	해쉬함수
인증		○	○	○	○	○
		공유패스워드	인증자	EAP-TLS	공개키/증명서	OTP/티켓
접근제어		○	○	○	○	○
익명성		X	X	○	X	○
		ID 노출	ID 노출	임의의 ID	ID 노출	갱신 ID
프라이버시		X	X	○	X	△
		서버가 생성한 세션 키를 그대로 사용하여 통신 내용을 서버가 모두 알 수 있음	홈 서버와 외부 서버가 동일한 키를 사용하여 이동 노드와 통신하므로 모든 서버는 통신 내용을 볼 수 있음	인증서버 모르게 사용자와 콘텐츠 제공자(CP) 사이에 세션 키를 교환하고 CP마다 다른 세션 키를 사용함으로써 제공	서버가 생성한 세션키를 그대로 사용하여 통신 내용을 서버가 모두 알 수 있음	AAAH가 세션 키를 생성하여 분배하므로 악의적인 목적을 가진 AAAH라면 통신의 모든 데이터를 도청하였을 때 내용을 볼 수 있음
재전송 공격		○	○	○	○	○
		Authentication/nonce	Timestamp/ Lifetime	Timestamp/ Lifetime	nonce	OTP/TSV
효율성	비 이동 시	△	△	○	X	○
		인증·티켓 서버의 분리	인증·티켓 서버의 분리	SSO 서비스, 익명성, 프라이버시 제공	지속적인 모니터링 필요/ 디바이스 연산량 증가	익명성 및 프라이버시 제공
	이동 시	△	△	X	△	△
		인증·티켓 서버의 분리	인증·티켓 서버의 분리	이동성을 고려하지 않음	그룹 티켓을 발행하여 각 디바이스마다 티켓 발행 필요 없음	세션 키 갱신 횟수 증가
티켓	복제	○	○	○	○	○
	위조	○	○	○	○	○
	변경	X	X	X	○	○
	재판매	•	•	•	•	•

[○ : 제공, 안전함 △ : 보통 X : 제공 못함, 안전하지 않음 • : 고려하지 않음]

5. 결 론

최근 모바일 디바이스를 이용하여 서비스를 제공 받는 방안이 많이 모색되고 있으며, 그에 따른 안전성도 중요시 되고 있다. 따라서 본 제안 방식은 모바일 디바이스를 이용하는 사용자 인증을 위해 시간 동기화 *OTP* 티켓을 기반으로 하여 홈 네트워크에서 외부 네트워크로 이동하더라도 지속적인 서비스를 제공하는 방안에 대하여 연구를 진행하였다. 또한 티켓의 유효기간이 만료되더라도 홈 네트워크로 이동하지 않고, 외부 네트워크에서 티켓의 갱신으로 서비스를 지속할 수 있다. 이와 같은 방식으로 통신 횟수를 줄임으로써 지연을 감소시키고 홈 인증 서버의 오버헤드를 줄임으로써 효율성을 가져다주며, 최근 이슈가 되고 있는 사용자의 프라이버시 및 익명성을 제공 할 수 있다.

향후 유비쿼터스 사회가 도래됨에 따라 디바이스의 경량화, 소형화 및 이동성을 고려하여 보다 안전하고 효율적인 보안 프로토콜에 관한 연구가 필요할 것으로 사료되며, 사용자의 이동으로 키 관리의 어려움이 예상되고 있다. 따라서 안전하고 효율적인 모바일 디바이스의 키 관리에 대한 연구가 필요하다.

참 고 문 헌

[1] Bhrat Patel and Jon Crowcroft, "Ticket based service access for the mobile user," *In Third annual ACM/IEEE internaional conference on Mobile computing and networking*, pp.223-233, 1997.

[2] Jung-Min Park, Eum-Hui Bae, Hye-Jin Pyeon, and Kijoon Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network," *ICCSA*, pp. 210-219, 2003.

[3] Markus Hillenbrand, Joachim G¨otze, Jochen M¨uller, and Paul M¨uller, "Role-based AAA for Service Utilization in Federated Domains," *DFN Arbeitstagung Düsseldorf*, pp.205-219, 2005.

[4] Yihong Zhou, Dapeng Wu, and Scott M. Nettles, "On the Architecture of Authentication, Authorization, and Accounting for Real-Time Secondary Market Service," *IJWMC*, 2005.

[5] 김동현, "Mobile IP를 위한 티켓 기반 AAA 서비스에 대한 연구," *연세대학교 대학원*, 2002.

[6] 김봉주, "차세대 인증 프로토콜 DIAMETER AAA 기술 동향." *TTA 기술표준이슈*, 2001.

[7] 배은희, "IPv6 이동 네트워크에서의 티켓 기반 AAA 서비스 모델에 관한 연구," *이화여자대학교 과학기술대학원*, 2002.

[8] 서승현, 조태남, 이상호, "OTP-EKE : 원-타임-패스워드 기반의 키 교환 프로토콜," *한국정보과학회논문지*, pp.291-298, 2002.

[9] 이동명, 최효민, 이옥연, "익명성과 프라이버시 보장을 위한 효율적인 인증 메커니즘 설계," *한국정보처리학회 추계학술발표대회*, pp.941-944, 2005.

[10] C. Neuman, T. Yu, S. Hartman, and K. Raeburn, "The Kerberos Network Authentication Service," RFC 4120, 2005.

[11] J, Vollbrecht, P. calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruihjn, C.de Laat, M. Holdrege and D.Spence, "AAA Authorization Framework," RFC 2904, 2000.

[12] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," RFC 3588, 2003.

문 종 식

e-mail : comnik528@sch.ac.kr

2006년 순천향대학교 정보기술공학부 졸업

2006년~현재 순천향대학교 컴퓨터학과 석사 과정

관심분야 : AAA, 키 분배

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과 졸업

1986년 오사카대학 통신공학전공 석사

1989년 오사카대학 통신공학전공 박사

1985년~1994년 한국전자통신연구원 선임연구원

1994년~현재 순천향대학교 컴퓨터학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안