情報保護學會論文誌
第17卷 第5號, 2007. 10

익명성을 지원하는 ID기반 티켓을 이용한 AAA 메커니즘*

문 종 식,[1†] 백 창 현,[2] 이 임 영[1‡]
[1]순천향대학교 컴퓨터학부, [2]한국전자통신연구원 부설 연구소

An AAA Mechanism using ID-based Ticket offer Anonymity

Jong-Sik Moon,[1†] Chang-Hyun Paek,[2] Im-Yeong Lee[1‡]
[1]Division of Computer Science and Engineering,Soonchunhyang University,
[2]Electronics & Telecommunications Research Institute

요 약

AAA는 기존의 유선망뿐만 아니라 비약적으로 발전하고 있는 무선망의 WiBro, Mobile IP 등과 같은 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 인증, 인가, 과금 기능을 체계적으로 제공하는 정보보호 기술이다. 현재 무선망에서의 모바일 사용자를 위한 인증, 인가, 과금 표준화를 목표로 다양한 응용 서비스에 대한 표준화 작업을 진행하고 있으며, 이기종망간의 로밍 서비스 및 모바일 IPv6 네트워크에서의 AAA를 이용한 다양한 연구가 진행 중 이다. 본 논문에서는 유비쿼터스 환경에서 모바일 디바이스를 사용하는 사용자 인증을 위해 *OTP*와 ID기반 티켓을 사용하며, 홈 네트워크에서 외부 네트워크로 이동하더라도 티켓을 이용하여 서비스를 지속 받을 수 있다. 또한 외부 네트워크에서 티켓을 갱신하여 홈 인증 서버의 오버헤드를 줄일 수 있으며, 익명 ID를 통해 사용자가 이용한 서비스에 대한 익명성을 보장하는 방안에 대하여 제안한다.

ABSTRACT

AAA protocol is an information protection technology which systematically provides authentication, authorization and accounting function not only in the existing wire network but also in the rapidly developing wireless network, various services and protocol. Nowadays, standardization of the various application services is in progress with the purpose of AAA standardization for the mobile user in the wireless network. And various researches are being conducted for using AAA in the roaming service and mobile IPv6 network between heterogeneous networks. In this paper uses OTP and ID-based ticket for user authentication in the mobile device under the ubiquitous environment, and service is seamlessly provided even though the mobile device moves from the home network to the foreign network. In addition, with the ticket renewed from the foreign network, the overhead of the home authentication server can be reduced, and provides anonymity of service through the anonymity ID.

Keywords : *AAA, ID-based, Ticket, Anonymity, OTP*

접수일: 2007년 5월 29일; 채택일: 2007년 8월 13일
* 본 연구는 한국전자통신연구원 부설 연구소의 위탁 연구 과제 지원으로 수행되었음
† 주저자, jsmoon@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

Ⅰ. 서 론

인터넷 및 네트워크의 발전과 유비쿼터스 환경이 도래함에 따라 모바일 디바이스(PDA, Mobile Phone, Notebook, etc.)를 이용하여 서비스를 제공받고자 하는 수요는 급속도로 증가하고 있다. 사용자들은 현재 다양한 서비스를 제공받고 있으며, 이동하면서도 동일한 서비스를 지속적으로 제공 받기를 원한다. 그러나 무선 환경의 특성으로 인해 모바일 디바이스를 이용해 서비스를 제공받는 방법에는 많은 취약점이 존재하며, 그 취약점으로 인해 사용자의 프라이버시가 그대로 노출 된다. 유비쿼터스 환경에서 모바일 디바이스를 이용해 안전하게 서비스를 제공받기 위해 AAA(Authentication, Authorization, Accounting)는 기존의 유선망뿐만 아니라 비약적으로 발전하고 있는 무선망의 WiBro, Mobile IP 등과 같은 다양한 서비스 및 프로토콜 상에서 안전하고 신뢰성 있는 인증, 인가, 과금 기능을 체계적으로 제공하는 정보보호 기술이다. 현재 무선망에서의 모바일 사용자를 위한 인증, 인가, 과금 표준화를 목표로 IETF(Internet Engineering Task Force) AAA 워킹그룹에서는 다양한 응용 서비스에 대한 표준화 작업을 진행하고 있으며, 이기종망간의 로밍 서비스 및 모바일 IPv6 네트워크에서의 AAA를 이용한 다양한 연구가 진행 중이다.

AAA 기술은 보안의 심각한 문제를 일으키는 IPv4/IPv6기반 유/무선에서의 안전한 인증을 제공하고 이동에 따른 사용자에 대한 인증에서도 적용 가능함으로 인해 유비쿼터스 환경에서 사용자의 편의성 및 보안 측면에서 해결책을 가져다주고 있다. 모바일 디바이스를 이용하여 네트워크 서비스를 제공받고자 접근하는 사용자를 인증, 인가, 과금하는 AAA 기술은 여러 방식이 있으나, 본 연구에서는 ID기반 티켓으로 사용자 편의성을 증대시키면서 안전하고 효율적인 방식을 제안한다. 또한 익명 ID를 통해 서비스를 이용할 때 사용자가 어떠한 서비스를 제공받았는지 알 수 없게 하여 익명성을 보장해준다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 연구 배경에 대하여 알아보며 Ⅲ장에서는 기존 방식에 대하여 알아본다. Ⅳ장에서는 제안 방식에 대하여 설명하며, Ⅴ장에서는 Ⅱ장의 보안 요구 사항, 공격에 따른 요구 사항 및 통신에 따른 효율성으로 제안 방식을 분석하고 마지막으로 Ⅵ장에서는 결론 및 향후 연구 방향으로 마치도록 한다.

Ⅱ. 연구 배경

본 장에서는 보안 요구 사항에 대하여 알아보고, AAA와 티켓 방식 그리고 ID기반 방식의 개요에 대하여 살펴본다.

2.1 보안 요구 사항

기존의 유선 네트워크와는 다르게 무선 네트워크에서의 통신은 다양한 취약점이 존재할 수 있으며, 제 3자가 쉽게 접근할 수 있다. 이에 따라 사용자가 네트워크에 접근하여 서비스를 제공받을 때 전송되는 메시지 및 통신은 다음과 같은 보안 요구 사항을 만족해야 한다.

- 기밀성(Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 한다. 데이터의 출처와 목적지, 횟수, 길이, 또는 통신 선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다.
- 무결성(Integrity) : 통신 채널에서 전송되는 데이터는 중간에 위조, 삭제 및 변조 되지 않았음을 확인할 수 있어야 한다.
- 인증(Authentication) : 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어(Access Control) : 정당하지 않은 사용자는 서비스를 이용할 수 없어야 한다.
- 익명성(Anonymity) : 사용자가 이용한 서비스에 대해서 제 3자가 알 수 없어야 한다.

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

- 도청 공격(Eavesdropping Attack) : 통신 채널에서 전송되는 데이터가 제 3의 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다.
- 재전송 공격(Replay Attack) : 통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로

써 인증 받는 것을 막을 수 있어야 한다.

- 패스워드 추측 공격(Password Guessing Attack) : 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야한다.
- 위장 공격(Impersonation Attack) : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다.

2.2 AAA의 개요

IETF의 AAA 워킹그룹에서 진행하고 있는 AAA 표준은 Diameter 프로토콜에 해당되며, 기존의 RADIUS (Remote Authentication Dial In User Service) 프로토콜에 대한 제한사항 및 근본적인 문제점을 보완하지 않고, 새로운 차세대 로밍 환경에 적합한 AAA 프로토콜을 제정하기에 이르렀다. 이러한 프로토콜 표준을 위하여 1998년 12월에 정식 워킹그룹이 형성되었고, 해당 AAA 프로토콜을 Diameter로 명명하여 현재까지 표준화를 진행하고 있다. Diameter의 기본 구조는 SCTP(Stream Control Transmission Protocol)를 포함하는 전송 프로토콜과, 과금 기능을 포함한 Base 프로토콜, 그리고 상위의 다양한 응용 프로토콜들로 나눌 수 있다.

Diameter의 기반 프로토콜은 응용에서 필요로 하는 세션 또는 과금에 대한 관리 등의 기본적인 서비스를 제공하고, AVP(Attribute Value Pair)의 전달, 노드의 능력(Capabilities)에 대한 협상 및 에러 통보, 전송 프로토콜 제어 및 watch dog 기능을 부가적으로 수행한다. Diameter 프로토콜 계층과 응용 프로토콜 표준을 보면, 기존의 전통적인 PAP/CHAP(Password Authentication Protocol/Challenge Authentication Protocol) 등의 유선 기반 네트워크 액세스 인증 및 범용적인 접근제어를 위한 NASREQ(Network Access Service Requirements) 응용과 무선랜 환경 등에서 보안기능을 강화하고, EAP(Extensible Authentication Protocol) 워킹그룹에서 제공하는 다양한 인증방식을 수용하여 인증하기 위한 EAP 응용, 이동 로밍환경을 지원하기 위한 Mobile IPv4 응용이 있다. 또한 선불 및 후불 카드 서비스를 위한 Credit Control 응용, SIP(Session Initiation Protocol) 프로토콜에 기반한 VoIP(Voice over IP) 서비스 사용자 인증을 위한 SIP 응용이 있으며, Mobile IPv6 표준이 마무리됨에 따라 Mobile IPv6를 위한 bootstrapping과 관련된 AAA 응용에 대한 제안이 계속적으로 이어 지고 있다. IP 기반의 인터넷이 보편화 되면서 무선 이동 환경에서 네트워크에 접근하려는 요구가 증가되고 있으며, 무선 환경에서도 QoS 제공, 또는 선불카드 등 사용자의 서비스 환경이 다양해지고 있다. 이러한 사용자의 요구를 충족하기 위하여 유무선 또는 유비쿼터스 통신 사업자는 적법한 사용자에 대하여 안전한 고도의 서비스를 제공하여야 할 것이다. 이러한 안전한 네트워크 접근 및 이동 서비스를 위하여 사용자 인증, 인가 및 과금 처리를 수행하는 AAA 프로토콜은 필수적인 요소라 할 수 있다. 1991년 AAA 프로토콜은 리빙스톤사에 의해 RADIUS 프로토콜이 제안되어 하나의 관리 도메인 내에서 SLIP(Serial Line Internet Protocol)이나 PPP(Point-to-Point Protocol) 연결 서비스에 대한 AAA 서비스를 제공하는 것이 초기 모델이었으나, 현재에는 서비스 네트워크도 개방형으로 그리고 다중 도메인 환경으로 점차 변화되고 있다. 따라서 IETF의 AAA 워킹그룹에서는 로밍 환경에 적합한 AAA 서비스를 제공하기 위하여 Diameter 프로토콜에 대한 표준화를 진행하고 있다. 국내의 경우에도, 최근 휴대인터넷 사업자 선정을 앞두고, 후보 사업자들은 이동환경에서 이동 네트워크 서비스를 제공하는 Mobile IPv4, Mobile IPv6 서비스를 서두르고 있다. 이러한 이동환경을 위하여 도메인간 AAA 서비스가 반드시 적용되어야하며, 이러한 환경에서 실제적인 서비스를 위해서는 기존의 표준에 따른 기술 개발도 필요하지만, 개발된 제품이 표준에 적합한지를 시험하는 표준 적합성 시험과 제품들 사이에 상호 연동이 가능한지를 시험하는 상호 운용 시험을 위한 기술 개발이 병행되어야 할 것이다. 국내외 표준화 단체들로부터 Diameter 프로토콜 표준이 완성되고, 이동 인터넷 환경이 보편화되면 Diameter 프로토콜의 사용이 급속도로 확대될 것이며, 이에 대한 시장도 급성장할 것으로 기대된다.[5][11]

2.3 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 소요시간이 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 신용정보를 바탕으로 인증 과정과 권한 설정 과정을 거친 후 이동 노드에게 발급된다.[9] 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.

2.4 ID기반 방식의 개요

공개키 암호알고리즘의 개념이 1976년 Diffie와 Hellman에 의해 처음으로 소개된 이후 많은 공개키 암호알고리즘이 연구되었는데 일반적으로 공개키 기반 암호기법 사용 시에는 공개키 사이즈가 비밀키 통신에 비해 엄청나게 커지게 되어 키의 문제라든지, 키를 따로 관리해야 하는 3자 개입의 문제가 발생된다. 이와 관련하여 ID기반의 암호기법은 이 같은 문제점을 해결할 수 있는 시스템으로 1984년 Shamir에 의해 처음 제기 되었다.[1]

ID기반의 암호기법은 어떻게 누구나 개인 식별정보에 있는 본인임을 식별 할 수 있는 임의의 스트링으로 공개키를 대처하느냐는 것이 기본 아이디어로 e-mail 주소, 네트워크 주소 등이 이런 공개키로 사용될 수 있는데 이런 공개키들의 관리가 CA(Certificate Authority)를 이용하는 인증서 기반의 공개키 등의 관리보다 용이해질 수 있으며 그에 대응되는 비밀키는 키생성 센터에서 생성하여 처음 사용자 등록 시 사용자에게 안전하게 전달하여 사용하도록 할 수 있다. ID기반의 암호기법의 가장 큰 장점은 공개키에 대한 인증서가 필요 없다는 것으로 인증서의 부담을 줄일 수 있다. 또한 공개키가 갱신될 경우 갱신된 공개키에 대한 인증서를 재발급 받아야 하는데 ID기반의 암호기법을 사용하면 공개키를 ID에 갱신할 년도와 개월을 연접시켜 쉽게 갱신할 수 있다.[7] 본 논문에서는 통신에 사용되는 비밀 값을 ID기반으로 생성하여 안전성을 증가 시킨다.

Ⅲ. 기존 연구

기존 ID기반의 연구 중 패스워드 인증 방식, 사용자 인증 방식, 키 교환 방식에 대하여 알아보고 각 방식별 특징 및 장/단점에 대하여 알아본다.

3.1 ID기반 패스워드 인증 방식

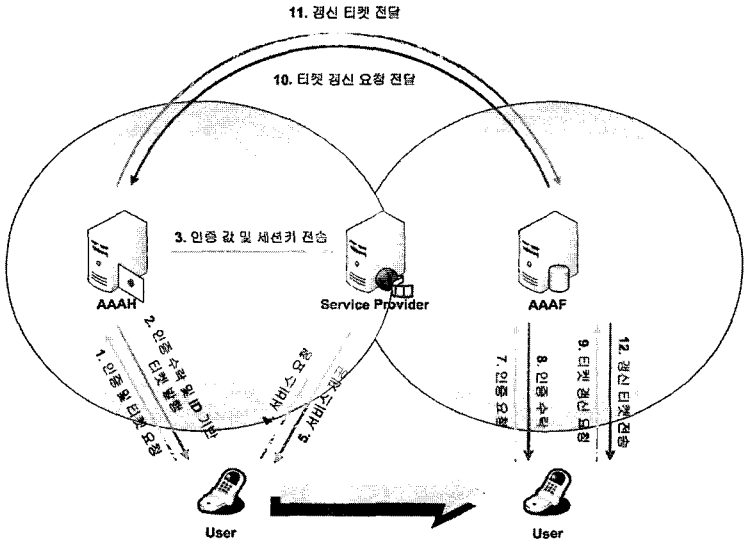
ID기반 패스워드 인증 방식은 타임스탬프 기반 방식과 난수 기반 방식의 2가지 ID기반 패스워드 인증 방식을 제안 하였으며, 다른 ID기반 방식들과는 달리 사용자들이 그들의 패스워드를 자유롭게 변경할 수 있다. 또한 시간 동기화가 되지 않는 네트워크를 위해 제안된 Nonce 기반 인증 방식은 메시지 재전송 공격에 안전하다.[2] 본 방식은 합법적인 사용자들을 인증 할 수 있고, 패스워드 추측 공격, 메시지 재전송 공격, 위장 공격으로부터 안전하다. 제안된 2가지 방식은 시스템에서 각 사용자의 알고 있는 것, 소유하고 있는 것 그리고 생물학적 측정에 의한 각 사용자를 인증하는 것을 요구한다. 이와 같은 특징은 본 방식의 신뢰성을 높여준다고 하고 있으나, 지문 정보가 없더라도 비밀 값을 알 수 있으며, 소극적 공격에 대한 취약점이 존재한다.[4]

3.2 ID기반의 사용자 인증 방식

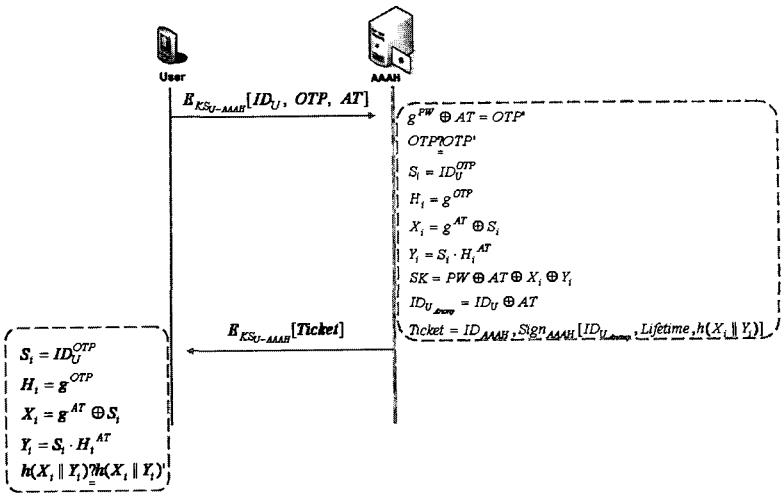
스마트카드를 이용한 ID기반의 사용자 인증 방식은 패스워드와 스마트카드를 이용하여 다양한 공격에 대항할 수 있을 뿐만 아니라 안전성과 효율성을 제공한다.[8] 본 논문에서 제안한 프로토콜을 패스워드 추측공격, 메시지 재전송 공격, 그리고 위장 공격의 세 가지 측면에서 분석한 결과 패스워드는 스마트카드에 저장되어 있어서 소유자 인증 없이는 직접적으로 접근 할 수 없기 때문에 불가능하다. 또한 시스템 클럭을 사용하기 때문에 메시지 재전송 공격에 안전하며, 이산대수의 어려움에 근거하여 위장 공격에도 안전하다. 기존의 방식들에서 발생하는 오버헤드를 줄였으며 결함을 해결하였다. 그러나 시스템 클럭의 동기화가 필요하며 스마트카드의 안전성에 절대적으로 의존하고 있다.

3.3 ID기반의 키 교환 방식

사용자의 식별 정보를 이용하여 두 시스템 간에 인증과 키 교환을 스마트카드를 이용하여 수행하는 ID기반의 키 교환 프로토콜을 제안하였다.[10] 제안한 프로토콜은 사용자의 스마트카드와 입력 지문 특징점 정보를 이용하여 스마트카드와 시스템 간에 세션키를 교환한다. 제안한 프로토콜의 안전성은 이산 대수 문제와 Diffie-Hellman 문제의 어려움에 기반하며 완전한 전방향 보안은 세션키 생성을 위해 입력 지문 정보로부터 난수 값을 조합하여 제공한다. 가장 공격은 만약 공격자가 다른 적합한 사용자로 가장할 수 있다면 공격자에 의한 공격이 가능하다. 따라서 프로토콜은 가장 공격을 방지하기 위해 매우 중요한 중간 레이어를 제시했다. 잠재적인 재전송 공격은 난수를 사용함으로써 방지 할 수 있다. 그러나 연산량의 증가와 사용자의 편리성에 문제가 있으며 효율성이 떨어진다.



(그림 1) 제안 방식 전체 흐름도



〔그림 2〕 인증 및 티켓 요청 단계

Ⅳ. 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. 제안 방식은 사용자가 홈 인증 서버에 접근하여 인증 후 티켓을 발급받고 나서 외부 네트워크로 이동하더라도 티켓을 제시함으로써 인증을 받아 서비스를 지속적으로 제공 받을 수 있다. 또한 익명성을 제공받고자 하는 서비스를 이용할 때 익명 ID를 통해서 사용자의 익명성을 보장해 준다. 이와 같은 방식을 사용하면 인증 절차에서 일어나는 지연을 감소시킬 수 있으며, 안전성과 효율성을 높일 수 있다.

4.1 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
- $ID_{U_{Anony}}$: 익명 아이디
- PW : 사용자의 패스워드
- g : 곱셈군 Z_n^*의 생성자
- $h(\ )$: 충돌성이 없는 안전한 일 방향 해쉬 함수
- OTP : One-Time Password
- AT : Authentication Time
- $E_*[\ ]$: *의 키로 암호화
- KS_{U-*} : 사용자와 * 사이에 공유한 대칭키
- SK : 사용자와 서비스 제공자 사이의 세션키
- KU_* : *의 공개키
- $Sign_*$: *의 개인키로 서명
- $Lifetime$: 티켓의 유효시간

4.2 제안 프로토콜

제안 프로토콜을 총 4단계로 이루어진다. 사용자 패스워드와 통신에 사용되는 대칭키는 사전에 분배 되었다고 가정하며, 각 단계는 인증 및 티켓 요청, 서비스 요청, 외부 네트워크에서의 인증, 외부 네트워크에서의 티켓 갱신 단계로 이루어진다.

4.2.1 인증 및 티켓 요청 단계

인증 및 티켓 요청 단계는 사용자가 홈 인증 서버와 공유한 대칭키로 인증 값을 전송하여 인증을 요청한다. 인증은 OTP로써 제공하며, 홈 인증 서버는 사용자를 인증한 후, 티켓과 사용자와 서비스 제공자 사이에 사용될 세션키를 발행하고 사용자는 발급받은 티켓을 검증한다.

• Step 1. 사용자는 자신의 패스워드와 AT(Aut- hentication Time)을 XOR 연산하여 OTP를 생성하고 사전에 공유한 대칭키로 자신의 ID, OTP 그리고 AT를 암호화 하여 전송한다. AT를 기반으로 하여 OTP를 생성하기 때문에 인증 값은 랜덤하게 생성되며, 재전송 공격에 안전하다.

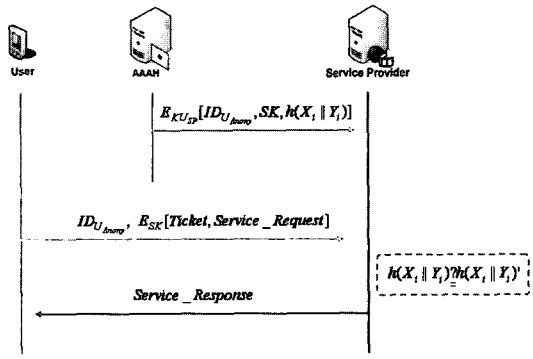
$$OTP = g^{PW} \oplus AT \quad (1)$$
$$E_{KS_{U-AAAH}}[ID_U,\ OTP,\ AT]$$

• Step 2. 홈 인증 서버는 데이터베이스에 저장된 사용자의 패스워드와 사용자에게 전송받은 AT를 XOR 연산하여 OTP'를 생성하고 전송된 OTP와 비교한다. 값이 일치하면 홈 인증 서버는 S_i, H_i, X_i, Y_i을 생성하고 티켓을 발행한다. 티켓의 구성요소는 사용자의 익명 ID와 비밀 값 그리고 티켓의 유효시간을 홈 인증 서버가 서명을 한 값과 홈 인증 서버의 ID로 구성된다. 그 후 사용자와 서비스 제공자 사이에 사용될 세션키를 생성하고 사용자의 익명성을 위해 익명 ID를 생성한 후 티켓을 대칭키로 암호화 하여 전송한다. 티켓에 X_i, Y_i를 포함함으로써 외부 네트워크의 인증 시에 지역 인증서버는 사용자를 인증할 수 있다.

$$OTP' = g^{PW} \oplus AT \quad (2)$$
$$OTP \stackrel{?}{=} OTP'$$
$$S_i = ID_U^{OTP},\ H_i = g^{OTP}$$
$$X_i = g^{AT} \oplus S_i,\ Y_i = S_i \cdot H_i^{AT}$$
$$SK = PW \oplus AT \oplus X_i \oplus Y_i$$
$$ID_{U_{Anony}} = ID_U \oplus AT$$
$$Ticket = ID_{AAAH},\ Sign_{AAAH}[ID_{U_{Anony}},\ Lifetime,\ h(X_i \| Y_i)]$$
$$E_{KS_{U-AAAH}}[Ticket]$$

• Step 3. 사용자는 전송받은 값을 복호화 하고 S_i, H_i, X_i, Y_i을 생성한 후 티켓에 포함되어 있는 비밀 값과 비교하여 티켓의 정당성 여부를 검증한다.

$$S_i = ID_U^{OTP},\ H_i = g^{OTP} \quad (3)$$
$$X_i = g^{AT} \oplus S_i,\ Y_i = S_i \cdot H_i^{AT}$$
$$h(X_i \| Y_i) \stackrel{?}{=} h(X_i \| Y_i)'$$



〔그림 3〕 서비스 요청 단계

4.2.2 서비스 요청

서비스 요청 단계는 사용자가 티켓을 발급받고 서비스를 이용하고자 할 때, 홈 인증 서버에게 발급받은 티켓을 서비스 제공자에게 제시하여 인증을 받고 서비스를 제공 받을 수 있다. 티켓에 포함되어 있는 익명 ID로 사용자가 어떤 서비스를 제공받았는지 익명성을 제공받을 수 있다.

• Step 1. 홈 인증 서버는 사용자 인증 후 티켓 발급 시 생성한 사용자의 익명 ID, 세션키와 비밀 값을 서비스 제공자의 공개키로 암호화 하여 서비스 제공자에게 전송한다.

$$E_{KU_{SP}}[ID_{U_{Anony}},\ SK,\ h(X_i \| Y_i)] \quad (4)$$

• Step 2. 사용자는 서비스 이용하고자 할 때, 서비스 제공자에게 홈 인증 서버로부터 발급받은 티켓과 서비스 요청메시지를 세션키로 암호화 하여 익명 ID와 함께 전송한다.

$$ID_{U_{Anony}},\ E_{SK}[Ticket,\ Service\_Request] \quad (5)$$

• Step 3. 서비스 제공자는 홈 인증 서버에게 전송받은 값을 자신의 개인키로 복호화 하여 사용자의 익명 ID, 세션키, 비밀 값을 획득한다. 그 후 사용자에게 전송받은 값을 홈 인증 서버에게 받은 세션키로 복호화 하여 티켓에 포함되어 있는 비밀 값과 전송받은 비밀 값을 비교하여 사용자를 인증한다. 인증이 완료되면 사용자에게 서비스를 제공한다. 이 단계에서 서비스 제공자는 사용자의 실제 ID는 알 수 없고

익명 ID만 알고 있기 때문에 어떠한 사용자가 서비스를 제공받았는지 알 수 없어 사용자의 익명성을 제공한다.

$h(X_i \| Y_i) \stackrel{?}{=} h(X_i \| Y_i)'$ (6)

Service_Response

4.2.3 외부 네트워크에서의 인증

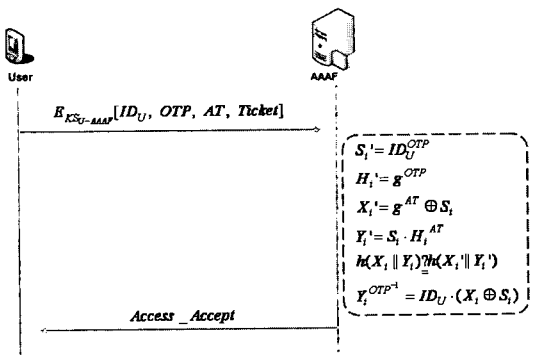
외부 네트워크에서의 인증 단계는 사용자가 홈 네트워크에서 서비스를 제공받다가 외부 네트워크로 이동하였을 때 지역 인증 서버에게 티켓을 제공하여 인증을 받고 서비스를 지속적으로 제공 받을 수 있다.

티켓을 이용함으로써 홈 인증 서버에게 접근하지 않고 외부 네트워크에서 인증을 받을 수 있어 인증 지연 및 홈 인증서버의 오버헤드를 줄일 수 있다.

- Step 1. 사용자는 홈 네트워크에서 외부 네트워크로 이동하였을 때 지역 인증 서버에게 자신의 ID, OTP, AT 그리고 티켓을 대칭키로 암호화 하여 전송한다.

$E_{KS_{U-AAAF}}[ID_U, OTP, AT, Ticket]$ (7)

- Step 2. 지역 인증 서버는 S_i, H_i, X_i, Y_i와 $h(X_i \| Y_i)'$ 생성하고 티켓에 있는 비밀 값을 비교하여 티켓을 검증한다. 그 후 사용자에게 전송받은 값을 연산하여 사용자를 인증한다. 인증을 받은 사용자는 외부 네트워크에서 지속적으로 서비스를 제공받을 수 있다. 이 단계에서 지역 인증 서버는 X_i, Y_i를 통하여 인증을 할 수 있다.



〔그림 4〕 외부 네트워크에서의 인증 단계

$S_i' = ID_U^{OTP}$, $H_i' = g^{OTP}$ (8)

$X_i' = g^{AT} \oplus S_i'$, $Y_i' = S_i' \cdot H_i^{AT}$

$h(X_i \| Y_i) \stackrel{?}{=} h(X_i \| Y_i)'$

$Y_i^{OTP^{-1}} = ID_U \cdot (X_i \oplus S_i)$

Access_Accept

4.2.4 외부 네트워크에서의 티켓 갱신

사용자가 외부 네트워크로 이동 하였을 때 티켓의 유효기간이 만료 되었거나, 티켓이 손상 되었을 경우 홈 네트워크로 이동하지 않더라도 외부 네트워크에서 티켓을 갱신하여 서비스를 지속 받을 수 있다.

- Step 1. 사용자가 외부 네트워크에서 티켓을 갱신할 경우 OTP_{new}, AT_{new}, 티켓 갱신 요청 메시지를 지역 인증 서버와 공유한 대칭키로 암호화 하여 지역 인증 서버에게 전송한다.

$E_{KS_{U-AAAF}}[OTP_{new}, AT_{new}, Ticket\_Renewal\_Req]$ (9)

- Step 2. 지역 인증 서버는 사용자에게 전송받은 값을 복호화 하여 OTP_{new}와 AT_{new}를 홈 인증 서버의 공개키로 암호화 하고 자신의 개인키로 서명하여 홈 인증 서버에게 전송한다.

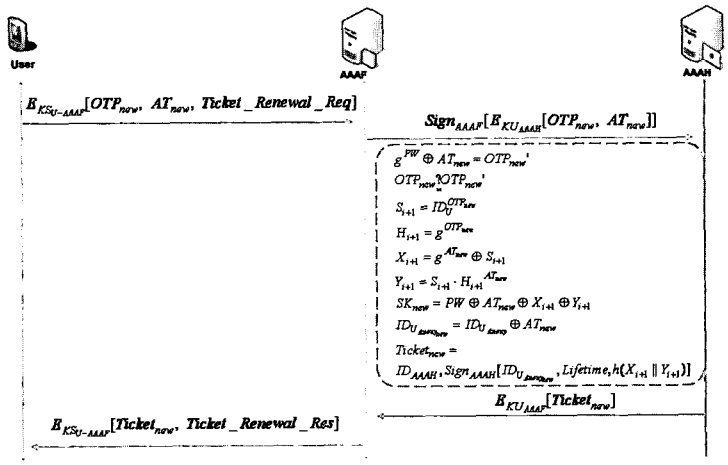
$Sign_{AAAF}[E_{KU_{AAAH}}[OTP_{new}, AT_{new}]]$ (10)

- Step 3. 홈 인증 서버는 지역 인증 서버에게 전송 받은 값을 복호화 하고 데이터베이스에 저장된 사용자의 패스워드와 전송된 AT_{new}를 XOR 연산하여 OTP_{new}'를 생성한다. 생성한 값과 전송된 OTP_{new}를 비교 하여 값이 일치하면 사용자 인증을 완료하고 새로운 S_{i+1}, H_{i+1}, X_{i+1}, Y_{i+1} 값과 익명 ID를 생성하고 티켓을 생성한다. 그 후 지역 인증 서버에게 갱신한 티켓을 지역 인증 서버의 공개키로 암호화 하여 전송한다.

$OTP_{new}' = g^{PW} \oplus AT_{new}$ (11)

$OTP_{new} \stackrel{?}{=} OTP_{new}'$

$S_{i+1} = ID_U^{OTP_{new}}$, $H_{i+1} = g^{OTP_{new}}$



〔그림 5〕 외부 네트워크에서의 티켓 갱신 단계

$$X_{i+1} = g^{AT_{new}} \oplus S_{i+1},\ Y_{i+1} = S_{i+1} \cdot H_{i+1}^{AT_{new}}$$

$$SK_{new} = PW \oplus AT_{new} \oplus X_{i+1} \oplus Y_{i+1}$$

$$ID_{U_{Anony_{new}}} = ID_{U_{Anony}} \oplus AT_{new}$$

$$Ticket_{new} = ID_{AAAH}$$
$$, Sign_{AAAH}[ID_{U_{Anony_{new}}}, Lifetime, h(X_{i+1} \| Y_{i+1})]$$

$$E_{KU_{AAAF}}[Ticket]$$

- Step 4. 지역 인증 서버는 홈 인증 서버에게 전송받은 값을 복호화 하여 갱신된 티켓을 획득한다. 그 후 갱신된 티켓과 티켓 갱신 응답 메시지를 대칭키로 암호화 하여 사용자에게 전송한다.

$$E_{KS_{U-AAAF}}[Ticket_{new}, Ticket\_Renewal\_Res] \quad (12)$$

V. 제안 방식 분석

제안 방식의 프로토콜을 2.1에서 언급한 안전성과 제 3자의 공격에 대한 요구사항에 맞추어 분석하고, 통신에 따른 효율성을 분석하면 다음과 같다.

- 기밀성(Confidentiality) : 통신에 사용되는 데이터는 정당한 객체만이 확인할 수 있어야 한다. 데이터의 출처와 목적지, 횟수, 길이, 또는 통신 선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다. 사용자와 홈 인증 서버사이에 공유한 대칭키(KS_{U-AAAH}), 사용자와 지역 인증 서버사이에 공유한 대칭키(KS_{U-AAAF}), 사용자와 서비스 제공자 사이에 사용되는 세션키(SK)로써 기밀성을 제공한다.
- 무결성(Integrity) : 통신 채널에서 전송되는 데이터는 중간에 위조, 삭제 및 변조 되지 않았음을 확인할 수 있어야 한다. 제안 방식에서는 해쉬 값($h(X_i \| Y_i)$)과 ID기반 OTP를 검증함으로써 제공된다.
- 인증(Authentication) : 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다. 제안 방식에서는 OTP와 ID기반 티켓을 이용하여 인증을 제공한다. 인증 서버는 패스워드와 AT(Authentication Time)을 XOR 연산하여 사용자를 검증할 수 있다.
- 접근제어(Access Control) : 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.
- 익명성(Anonymity) : 사용자가 이용한 서비스에 대해서 제 3자가 알 수 없어야 한다. 본 제안 방식에서는 사용자의 ID에 AT를 XOR 연산하여 익명 ID를 생성하고 티켓에 포함한다. 이로써 사용자가 어떠한 서비스를 제공받았는지 알 수 없으며, 사용자의 익명성이 보장된다.
- 도청 공격(Eavesdropping Attack) : 통신 채널에서 전송되는 데이터를 제 3의 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가

데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다. 제안 방식에서는 메시지를 암호화 하여 도청 공격으로부터 안전하다.

- 재전송 공격(Replay Attack) : 통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받는 것을 막을 수 있어야 한다. *OTP*, 비밀 값 생성에 포함되는 AT와 티켓의 유효시간으로 재전송 공격으로부터 안전하다.
- 패스워드 추측 공격(Password Guessing Attack) : 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야한다. 패스워드 인증 기법은 사용자 인증에서 가장 널리 사용되고 있는 기법이다. 제안 방식에서 패스워드를 추측하기 위해서 공격자는 g^{PW}를 통해서 패스워드를 추측할 수 있다. 그러나 이산대수 문제의 어려움에 근거하여 패스워드를 추측하기 어렵게 하여 패스워드 추측 공격으로부터 안전하다.
- 위장 공격(Impersonation Attack) : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다. 제안 방식은 *OTP*를 사용하여 인증을 받기 때문에 사용자로 위장을 할 수 없으며, 각 메시지의 암호화 및 인증 서버의 서명으로 인해 위장 공격으로부터 안전하다.
- 효율성(Efficiency) : 본 방식은 티켓을 사용함으로써 인증 지연 및 절차를 감소시킬 수 있으며, 외부 네트워크에서 티켓 갱신을 통하여 홈 인증 서버의 오버헤드를 줄여 효율성을 제공한다. 티켓의 발행에서 생기는 연산량이나 소요시간은 증가하나 매번 홈 인증 서버로 인증을 요청하는 시간에 비해 미비하기 때문에 크게 문제될 것이 없다. 그러나 인증 서버가 악의적인 목적을 가진다면 사용자와 서비스 제공자 사이의 통신을 알 수 있으며, 지역 인증 서버의 증가 시 공유 대칭키의 개수가 증가한다는 단점이 있다. 이로 인해 인증 서버는 신뢰된 개체라고 가정한다.
- 통신에 따른 효율성 : 통신에 따른 효율성 분석은 표 1과 같다. 제안 방식의 총 통신 횟수가 기존 연구에 비해 많은 것은 기존 연구는 등록 및 인증 단계를 계산한 것이지만 제안 방식은 인증 단계 및 서비스 이용, 외부 네트워크 인증, 티켓 갱신 단계까지 계산한 것이기 때문이다. 초기 인증 횟수는 기존 방식에 비해 1회 감소하였으며, 암호화 연산 중 공개키 연산은 인증 서버의 연산이기 때문에 사용자의 연산량에는 영향을 미치지 않는다. 지수승 연산은 사용자 측면에서의 연산량을 나타낸 것이며, 보유키의 개수는 지역 인증 서버의 개수가 증가함에 따라 같이 증가한다.

Ⅵ. 결론 및 향후 연구 방향

인터넷 및 네트워크의 발달과 유비쿼터스 환경의 도래에 따라 최근 모바일 디바이스를 이용하여 다양한 서비스를 제공받는 방안이 많이 모색되고 있으나, 무선 네트워크의 특성으로 인해 프라이버시 노출 등의 보안 취약점이 잇따라 발생하고 있다.

따라서 본 제안 방식은 유비쿼터스 환경에서 모바일 디바이스를 사용하는 사용자 인증을 위해 *OTP*와 ID 기반 티켓을 사용하며, 홈 네트워크에서 외부 네트워크로 이동하더라도 티켓을 이용하여 서비스를 끊김없이 지속 받을 수 있다. 또한 외부 네트워크에서 티켓이 손상 되었거나, 티켓의 유효시간이 만료되더라도 홈 인증

〔표 1〕 통신에 따른 효율성 분석표 〔S : 대칭키 암호화 연산, P : 공개키 암호화 연산, n : 지역 인증 서버의 수〕

	ID기반 패스워드 방식 [2]	ID기반의 사용자 인증 방식 [8]	ID기반의 키 교환 방식 [10]	제안 방식
총 통신 횟수	3 회	3 회	4 회	11 회
초기 인증 통신 횟수	3 회	3 회	3 회	2 회
암호화 연산	S : 3 회	S : 3 회	S : 2 회	S : 7 회 P : 2 회
해쉬 연산	1 회	1 회	1 회	1 회
지수승 연산	4 회	2 회	5 회	4 회
보유키 개수	1 개	1 개	2 개	n+2 개

〔표 2〕 제안 방식 분석표 〔○ : 제공, 안전함 △ : 보통 X : 제공 못함, 안전하지 않음〕

	ID기반 패스워드 방식 [2]	ID기반의 사용자 인증 방식 [8]	ID기반의 키 교환 방식 [10]	제안 방식
기밀성	X	○	○	○
	비밀 값을 알 수 있음	비밀키	비밀키/세션키	대칭키/공개키 /세션키
무결성	○	○	○	○
	묵시적 무결성 제공	묵시적 무결성 제공	묵시적 무결성 제공	해쉬함수
인증	△	○	○	○
	실제적인 인증을 제공하나 인증에 사용되는 비밀값을 알 수 있음	패스워드 인증	패스워드 인증	OTP/티켓
접근제어	X	○	○	○
	비밀 값의 노출로 인해 제공 안함	인증을 받지 않은 사용자는 서비스를 제공 받을 수 없음		
익명성	X	X	X	△
	익명성에 대한 고려사항 없음			익명 ID ($ID_{U_{Anony}}$)
도청공격	X	○	○	○
	소극적인 도청에 안전하지 못함	제 3자가 메시지를 획득하더라도 비밀값을 유추 할 수 없음		
재전송 공격	○	○	○	○
	타임스탬프/난수	시스템클럭	세션 난수	OTP/AT/Lifetime
패스워드 추측 공격	△	△	○	○
	패스워드 추측 가능	패스워드 추측 가능	이산 대수 문제의 어려움에 근거	이산 대수 문제의 어려움에 근거
위장 공격	△	○	○	○
	비밀 값 노출로 위장 가능	이산 대수 문제의 어려움에 근거	이산 대수 문제의 어려움에 근거	인증 서버의 서명
효율성	X	△	△	△
	안전성 제공 못함	시스템클럭의 동기화/ 스마트카드에 의존	연산량 증가/ 사용자의 편리성 저하	대칭키 공유 개수 문제

서버로 접근하지 않고 티켓을 갱신하여 홈 인증 서버의 오버헤드를 줄일 수 있으며, 익명 ID를 통해 서비스를 이용할 때 사용자가 어떠한 서비스를 제공받았는지에 대한 익명성을 보장하는 방안에 대한 연구를 진행하였다.

이와 같이 ID기반 티켓 방식을 이용함으로써 네트워크에서 이동하는데 있어 통신 횟수를 줄이고 안전성과 효율성을 높일 수 있다. 그러나 지역 인증 서버의 개수가 증가함에 따라 보유키의 개수가 증가하기 때문에 유비쿼터스 환경을 위한 경량화된 공개키 ID기반 티켓 방식에 대한 연구가 필요하며, 향후 구현 시 통신량에 대한 분석 및 실험을 통한 성능평가가 등 구현 시 필요한 자세한 사항의 정의가 필요할 것으로 사료된다.

참고문헌

[1] A. Shamir, "Identity-based cryptosyste-ms and signature schemes," *CRYPTO 84*, pp. 47-53, 1984.

[2] H. S. Kim, S. W. Lee and K. Y. Yoo, "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM Operating Systems Review*, Vol. 37, No. 4, pp. 32-41, 2003.

[3] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-based remote user authentication scheme using smart cards," *Electronics Letters*, Volume 38, Issue 12, pp. 554-555, 2002.

[4] Michael Scott, "Cryptanalysis of an ID-based Password Authentication Scheme using Smart Cards and Fingerprints," *ACM Operating Systems Review*, Vol. 38, pp. 73-75, 2004.

[5] 김현곤, 이병길, 최두호, 유상근, 김말희, 이해동, 유희종, "AAA 정보보호 기술 표준화 동향," *전자통신동향분석*, 제20권, 제1호, 2005.

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

[7] 이상억, "ID기반의 단말간 무선랜 인증," 경북대학교 대학원, 2004.

[8] 이원진, 김은주, 전일수, "스마트카드를 이용한 ID기반의 사용자 인증 프로토콜," 한국컴퓨터종합학술대회, Vol. 32, No. 1, pp. 166-168, 2005.

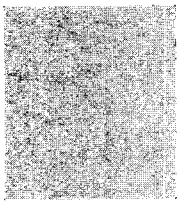
[9] 배은희, "IPv6 이동 네트워크에서의 티켓 기반 AAA 서비스 모델에 관한 연구," 이화여자대학교 과학기술대학원, 2002.

[10] 배헌중, 김현성, 유기영, "스마트 카드를 이용한 ID기반의 키 교환 프로토콜," 한국정보과학회학술대회, Vol. 30, No. 1, pp.491-493, 2003.

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

〈著者紹介〉

문 종 식 (Jong-Sik Moon) 정회원
2006년 2월: 순천향대학교 정보기술공학부 졸업
2006년 3월~현재: 순천향대학교 컴퓨터학과 석사과정
<관심분야> AAA, 이기종 네트워크



백 창 현(Paek Chang Hyun)
1989년 8월: 한밭대학교 전자공학과 졸업
1994년 2월: 충남대학교 정보통신공학과 석사 수료
1982년 3월: 한국전자통신연구원 입원
2000년~현재: 한국전자통신연구원 부설 연구소 선임 연구원
<관심분야>

이 임 영 (Im-Yeong Lee) 종신회원
1981년 2월: 홍익대학교 전자공학과 졸업
1986년 2월: 오사카대학 통신공학전공 석사
1989년 2월: 오사카대학 통신공학전공 박사
1985년~1994년: 한국전자통신연구원 선임연구원
1994년~현재: 순천향대학교 컴퓨터학부 교수
<관심분야> 암호이론, 정보이론, 컴퓨터 보안