DOI: 10.3745/KIPSTC.2008.15-C.6.481

무선 네트워크 로밍 환경에서 이기종 네트워크간 연동을 위한 AAA 메커니즘

문 종 식[†] · 이 임 영[††]

요 약

인터넷과 네트워크의 발전에 따라 유선 네트워크와 무선 네트워크가 결합되어 유/무선 통합시대가 전개되고 있다. 유/무선 통합 서비스 중에서 이기종 네트워크 환경에서의 보안 기술에 대한 연구는 아직 미흡한 실정이며, 이기종 네트워크의 융합은 서로 다른 네트워크의 융합으로 인해 기존의 보안 기술 및 통신 기술을 그대로 적용하기가 매우 어려워 보안 측면에서도 많은 취약점을 내포하고 있다. 또한 사용자들이 제공받는 서비스의 형태는 대부분 이동 사용자를 위한 서비스가 될 것이며, 이러한 서비스에서는 로밍 시 빠른 인증 및 안전성을 제공하여야 한다. 따라서 본 연구는 이기종 네트워크 환경에서 로밍 및 AAA 메커니즘에 관한 연구를 진행하여 안전성과 효율성을 제공할 수 있도록 하였다.

키워드 : 인증, 인가, 과금, 로밍, 이기종 네트워크

AAA Mechanism for the Integration between Heterogeneous Network in Wireless Network Roaming Environment

Jong-Sik Moon[†] · Im-Yeong Lee[††]

ABSTRACT

With the advancement of the Internet and networks, the combination of wired/wireless technologies is spreading rapidly since it enables the creation of new services and provides new features to both users and service providers. In such wired/wireless integrated services, network integration is very important because such systems are integrated by a linkage between heterogeneous networks and they involve an integration of transmission technologies across networks. In this situation, existing security and communication technologies are unsuitable since the network are integrated with heterogeneous networks. The network may also have several security vulnerability. Also, form of service that users offer will be service for roaming user. In these service, we must provide fast authentication and security at roaming. Therefore in this paper we proposed roaming and AAA mechanism in heterogeneous network environment. Our system provides secure communication and efficiency.

Keywords : Authentication, Authorization, Accounting, Roaming, Heterogeneous Network

1. 서 론

유선 네트워크의 빠른 전송속도 및 다양한 서비스와 무선 네트워크의 편리성 및 이동성이 결합되어 사용자와 서비스 제공자 모두에게 새로운 변화를 가져올 신기술로 유/무선 통합 시대가 전개되고 있다. 유/무선 통합 서비스 중에서 네트워크의 통합은 이기종 네트워크간 연동에 의한 네트워크 융합과 네트워크상에서 전송기술간 융합으로써 매우 중요한 부분을 차지하고 있다[8]. 모바일 디바이스 및 네트워크의 발전에 따라 사용자들은 언제 어디서나 안전하고 편리하게 서비스를 제공받기 원하며, 유/무선 통합 네트워크 환경에서 사용자들이 제공받는 서비스의 형태는 대부분 이동 사용자를 위한 서비스가 될 것이다. 이러한 서비스에서는 로밍 시 빠른 인증 및 안전성을 제공해야 하지만 기존의 보안기술 및 전송 기술은 새롭게 변화되는 환경에 적용하기에 많은 보안 취약점이 발생한다. 또한 이기종 네트워크를 이동하며 서비스를 제공받기 때문에 서비스에 대한 과금을 처리하기가 어려워지며, 홈 인증 서버의 오버헤드가 발생할 수 있다. 이러한 여러 취약점이 존재함에 따라 본 연구에서는 이기종 네트워크 환경에서 로밍 및 AAA(Authentication, Authorization, Accounting) 메커니즘에 관한 연구를 진행하였다. 모바일 디

※ 본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업으로 수행된 연구결과임
† 준 회 원 : 순천향대학교 컴퓨터학과 박사과정
†† 종신회원 : 순천향대학교 컴퓨터학부 교수
논문접수 : 2008년 1월 23일
수 정 일 : 1차 2008년 8월 29일
심사완료 : 2008년 9월 1일

바이스를 이용하여 서비스를 제공받는 사용자 인증을 위해 OTP(One-Time Password)와 ID(IDentification) 기반 공개키 방식을 이용하였으며, 티켓을 이용하여 빠른 로밍 및 홈 인증 서버의 오버헤드를 감소시켰다. 과금 서비스는 초기에 모바일 디바이스가 이용할 금액에 대해 결제를 하고 홈 인증 서버가 결제에 따른 금액 정보를 포함하여 티켓을 구성한다. 그 후 모바일 디바이스가 서비스 이용 시 현재 위치한 네트워크 인증 서버에게 티켓을 제시하면 신뢰 관계를 가진 인증 서버는 티켓의 금액 정보에서 이용 금액을 차감하고 티켓을 재구성하여 갱신한다. 이로 인해 모바일 디바이스는 과금 처리에 관한 정보 요청을 매번 홈 인증 서버에게 전송하지 않아도 되며, 신뢰 관계 서버에서 처리할 수 있다. 이와 같은 방식을 사용하면 이기종 네트워크 환경에서 계층적 신뢰 관계 서버를 이용하여 과금 정보 갱신과 빠른 로밍을 제공할 수 있다. 또한 모바일 디바이스가 이기종 네트워크로 이동하더라도 홈 네트워크로 접근하지 않고 계층적 신뢰 관계를 가지는 이기종 네트워크 인증 서버에서 인증을 받아 서비스를 지속 받을 수 있다. 따라서 계층적 신뢰 관계 서버를 이용한 인증기술을 제안하여 안전성과 효율성을 제공할 수 있도록 하였다. 본 논문의 구성은 다음과 같다. 2장에서는 개요 및 보안 요구 사항에 대하여 기술하고 3장에서는 기존 방식에 대하여 분석한다. 4장에서는 안전하고 효율적인 로밍 및 AAA 메커니즘을 제안하고, 5장에서는 2장의 보안 요구 사항으로 제안 방식을 분석하여 마지막으로 6장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. 연구 배경

본 장에서는 AAA 및 겹선형 쌍함수의 개요에 대하여 알아보고, 보안 요구 사항에 대하여 분석하고자 한다.

2.1 AAA의 개요

IP 기반의 인터넷이 보편화 되면서 무선 이동 환경에서 네트워크에 접근하려는 요구가 증가되고 있으며, 무선 환경에서도 QoS(Quality of Service) 제공 또는 선불카드 등 사용자의 서비스 환경이 다양해지고 있다. 이러한 사용자의 요구를 충족하기 위하여 유/무선 또는 유비쿼터스 통신 사업자는 적법한 사용자에 대하여 안전한 고도의 서비스를 제공하여야 할 것이다. 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(Remote Authentication Dial In User Service) 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 IETF(Internet Engineering Task Force)의 AAA 워킹그룹에서는 로밍 환경에 적합한 AAA 서비스를 제공하기 위하여 Diameter 프로토콜에 대한 다양한 표준화 작업을 진행하였으며, 이동 환경을 고려한 표준화를 진행하고 있다. 국내의 경우에도, 최근 휴대인터넷 사업자 선정을 앞두고, 후보 사업자들은 이동 환경에서 이동 네트워크 서비스를 제공하는 Mobile IPv4, Mobile IPv6 서비스를 서두르고 있다. 이러한 이동환경을 위하여 도메인간 AAA 서비스가 반드시 적용되어야 하며, 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 프로토콜에 관한 표준이 완성되었으며, 이동 인터넷 환경이 보편화됨에 따라 Diameter 프로토콜의 사용이 급속도로 확대될 것으로 예상되어 이에 대한 시장도 급성장할 것으로 기대된다[4][6][7].

2.2 겹선형 쌍함수

겹선형 쌍함수(Bilinear Pairing)는 타원곡선 상의 이산대수 문제를 유한체상의 이산대수 문제로 축소시켜 그 어려움을 줄여 타원곡선 암호시스템을 공격하는 도구로 원래 제안되었다. 최근에는 공격 도구가 아닌 정보보호를 위한 암호학적 도구로 사용되고 있으며, 겹선형 쌍함수는 다른 말로 겹선형 사상(Bilinear Map)이라 한다. 겹선형 사상에서는 다음과 같은 표기법을 사용하며, 이 사상의 정의는 다음과 같다.

- q : 매우 큰 소수
- G_1 : 위수가 q인 타원곡선 위의 덧셈군
- G_2 : 위수가 q인 유한체 위의 곱셈군
- $P, Q, R \in {}_R G_1$
- $a, b, c \in {}_R Z_q^*$
- $\hat{e}: G_1 \times G_1 \rightarrow G_2$ 겹선형 사상

다음과 같은 특성을 만족하는 $\hat{e}: G_1 \times G_1 \rightarrow G_2$를 사용가능 Admissible Bilinear Map이라 한다.

- 겹선형(Bilinear) : 임의의 P, Q, R에 대하여 다음이 성립해야 한다.
  - $\hat{e}(P, Q+R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$
  - $\hat{e}(P+Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$
- 비퇴화성(Non-Degenerate) : G_1의 모든 쌍 P, Q에 대하여, $\hat{e}(P, Q)$는 G_2의 항등원이 아니어야 한다.
- 계산가능성(Computable) : 임의의 P, Q에 대하여 $\hat{e}(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재해야 한다.

겹선형 사상의 특성에 의해 다음이 성립한다.

$$\hat{e}(aP, bQ) = \hat{e}(P, bQ)^a = \hat{e}(aP, Q)^b = \hat{e}(P, Q)^{ab}$$
$$= \hat{e}(abP, Q) = \hat{e}(P, abQ)$$

이 사상 때문에 타원곡선 상에서 D-H 결정 문제는 다음

과 같이 정의된다.

$$\hat{e}(aP, bQ) = \hat{e}(cP, P) \Rightarrow ab = c$$

따라서 겹선형 사상을 암호학적 도구로 사용하는 많은 암호프로토콜에서는 다음 문제의 어려움에 기반하고 있다. BDHP(Bilinear Diffie-Hellman Problem)는 G_1의 원소 P, aP, bP, cP가 주어졌을 때, $\hat{e}(P, P)^{abc}$를 계산하는 문제를 말한다. 이 문제는 타원곡선 이산대수 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP로부터 a를 계산할 수 있으면 $\hat{e}(bP, cP)^a$를 통해 $\hat{e}(P, P)^{abc}$를 계산할 수 있다. 뿐만 아니라 이 문제는 타원곡선 D-H 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP, bP로부터 abP를 계산할 수 있으면 $\hat{e}(abP, cP)$를 통해 $\hat{e}(P, P)^{abc}$를 계산할 수 있다.

2.3 보안 요구 사항

이기종 네트워크 환경에서는 유선 네트워크뿐만 아니라 무선 네트워크의 취약성까지도 존재할 수 있으며, 전송되는 메시지 및 통신은 다음과 같은 보안 요구 사항을 만족해야 한다.

2.3.1 일반적인 보안 요구 사항

기본적으로 다음과 같은 일반적인 보안 요구사항을 고려해야 한다.

- 기밀성 : 통신에 사용되는 데이터는 정당한 개체만이 확인할 수 있어야 한다. 데이터의 출처와 목적지, 횟수, 길이, 또는 통신 선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다. 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 제공된다.
- 무결성 : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다. 만약 삭제 및 위/변조가 되었다면 그 사실을 확인할 수 있어야 한다. 전송된 데이터의 무단 변경을 감지하기 위해 전자 서명 등을 이용한다.
- 인증 : 인증 서비스는 통신이 기밀성을 갖도록 보증하는 것이 중요하다. 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 전자문서의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근 제어 : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분하여 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다. 시스템에서는 운영체제의 접근 통제 기능을 사용하며 네트워크에서는 침입차단 시스템을 사용해서 접근 통제 수준을 높일 수 있다. 또한 서비스를 이용함에 있어서 정당하지 않은 사용자는 서비스를 제공받을 수 없다.
- 부인 봉쇄 : 합법적인 개체들 사이에서 송/수신된 정보는 이 정보를 송/수신한 개체가 이 사실을 부인할지라도 당사자 및 제 3자에 의해 확인될 수 있어야 한다. 거래 당사자 간에 정보 제공 부인을 방지하는 것이다. 특히 네트워크를 이용한 전자상거래나 법률 행위에서는 매우 중요하다. 부인 방지는 무결성 보장과 마찬가지로 전자서명에 의해 해결할 수 있다.

2.3.2 제 3자의 공격에 따른 보안 요구 사항

무선 네트워크 및 이기종 네트워크의 특성에 따른 보안 요구 사항 외에도 제 3자가 다음과 같은 공격을 할 수 있다.

- 도청 공격 : 통신 채널에서 전송되는 데이터가 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다.
- 재전송 공격 : 공격자가 프로토콜상에서 유효 메시지를 선택해 복사한 후 재전송함으로써 정당한 사용자로 가장하는 공격이다. 통신 중에 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받는 것을 막을 수 있어야 한다. 시간이나 순서에 따른 유효성을 검출할 수 있도록 순서 번호나 타임스탬프, 또는 도전/응답 등으로 방어할 수 있다.
- 위장 공격 : 안전하지 않은 통신로 상에서는 악의적인 제 3자가 정당한 사용자처럼 위장하여 인증을 받거나 서비스를 제공받을 수 있다. 이에 제 3자가 정당한 사용자처럼 접근하는 것에 대한 안전성을 제공해야한다.
- 패스워드 추측 공격 : 안전하지 않은 통신로 상에서 악의적인 제 3자가 전송되는 메시지를 분석하여 패스워드를 추측할 수 있다. 따라서 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것에 대한 안전성을 제공해야한다.
- 서비스 거부 공격 : 악의적인 제 3자가 전송되는 데이터를 위조 및 변조하여 정당한 객체가 인증 받지 못하도록 하거나 정당한 사용자에게 지속적인 서비스를 제공하지 못하도록 하는 것에 대한 안전성을 제공해야한다.

2.3.3 이기종 네트워크에서의 보안 요구 사항

기존의 보안기술을 이기종 네트워크에 적용하였을 때 취약점이 존재할 수 있기 때문에 이기종 네트워크에서의 특성에 따른 보안 요구 사항을 만족해야 한다. 또한 도메인간 로밍이 빈번하게 일어나는데, 로밍 시 끊김없는 서비스를 제공하기 위해서는 다음과 같은 요구사항을 만족해야 한다.

- 상호 인증 : 상호 인증은 통신하는 개체간에 양방향으로 각각의 개체를 인증하는 것이다. 이기종 네트워크에서는 다양한 개체간 통신이기 때문에 상호간의 인증이 필요하다.
- 단대단 보안 : 단대단 보안의 경우 암/복호화 과정은 두 종단 시스템에서 수행되며, 출처 호스트나 터미널이 데이터를 암호화한다. 데이터는 암호화된 형식으로 네트워크를 통하여 목적지 터미널이나 호스트로 변경 없이 전송된다. 이기종 네트워크에서의 단말간 통신은 단대단 보안이 제공되어야 한다.
- 빠른 로밍 인증 : 이기종 네트워크에서는 도메인간의

로밍이 빈번하게 일어나는데, 이때 인증에 소요되는 시간이 길면 끊김없는 로밍 서비스를 제공할 수 없게 된다. 따라서 로밍 시 끊김없는 서비스를 제공하기 위해서는 빠른 인증 방식에 대한 고려가 필요하다.

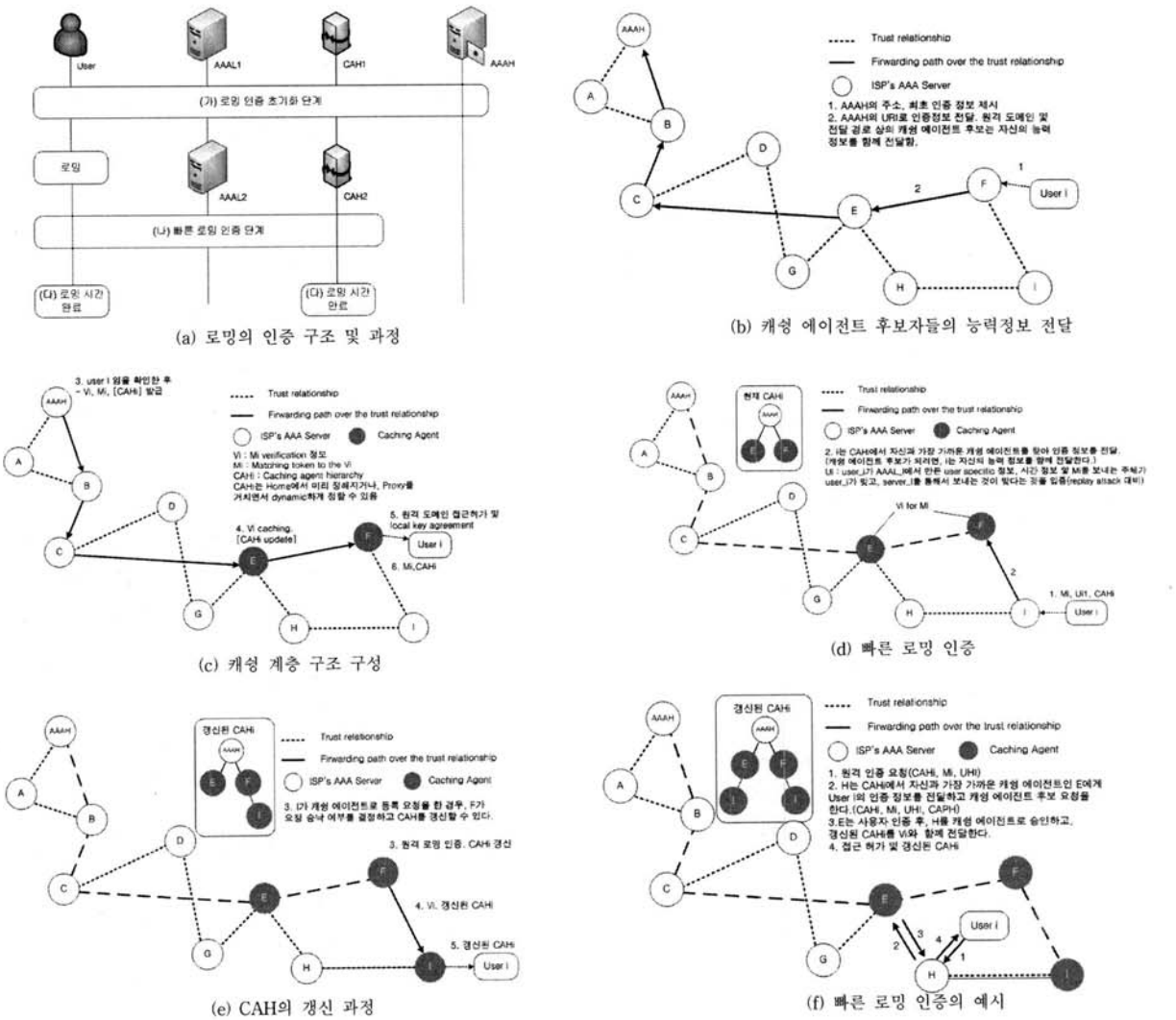
- 홈 인증 서버의 오버헤드 : 원격지에서 홈 인증 서버로 전송되는 인증 요청이 빈번하게 일어나면 홈 인증 서버의 오버헤드가 발생할 수 있다. 따라서 홈 인증 서버로 요청되는 인증 횟수 및 접근을 감소키시거나 분산시켜 오버헤드를 줄이는 방안에 대한 고려가 필요하다.
- 과금 정보의 갱신 : 기존의 방식은 사용자가 이용한 서비스에 따른 과금을 중앙의 관리 서버에서 서비스 이용 시 마다 처리하는 방식을 적용하였으나, 이러한 방식은 중앙 관리 서버의 오버헤드 증가 및 효율성을 저하시킬 수 있다. 따라서 누적된 과금 정보를 이용하여 처리하는 방식이 필요하다.
- 계층적 신뢰 관계 : 계층적 신뢰 관계는 홈 네트워크를 중심으로 외부 네트워크간의 신뢰 관계를 구성하는 트리 형식의 구조적 성질을 가진다. 기존의 모바일 디바이스의 이동 환경에서는 디바이스가 이동하여 인증을 요청하거나 티켓을 갱신하고자 하였을 경우 홈 인증 서버로 접근하여 요청하였다. 이와 같은 방식은 홈 인증 서버의 오버헤드에 직접적인 영향을 미치며, 네트워크의 부하를 가져온다. 따라서 계층적 신뢰 관계를 이용하는 방식을 고려해야 한다.

3. 기존 연구

기존 연구로 로밍, 과금, ID 기반 방식의 개요에 대하여 알아보고 각 방식별 특징 및 장/단점을 분석하고자 한다.

3.1 로밍 확장성을 높인 인증 방식

국제 로밍 및 이기종 망간 핸드오버가 활성화된 환경



(그림 1) 로밍 확장성을 높인 인증 방식 전체 흐름도

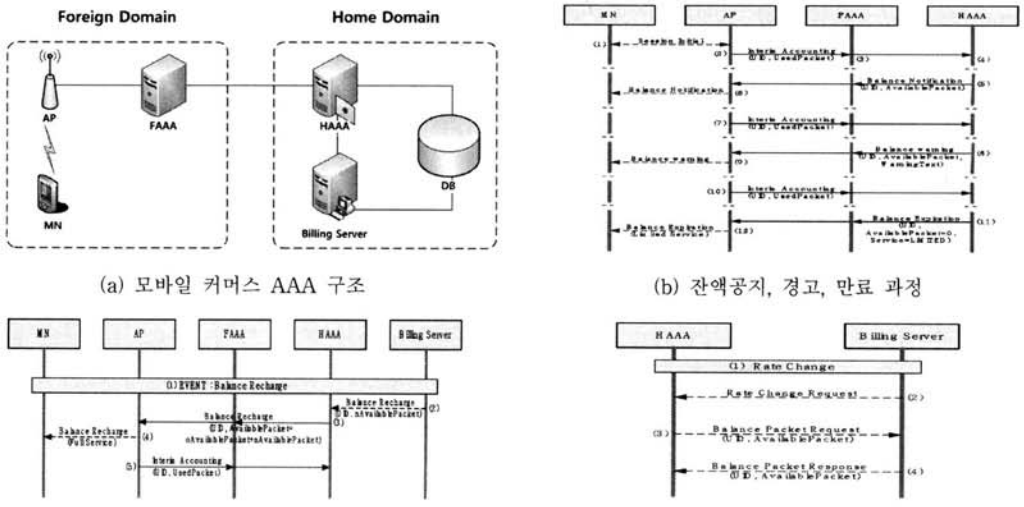
에서 사용자에게 끊김없는 통신 서비스를 지원하기 위해서는 보다 빠르고 확장성이 뛰어난 인증 기법이 필요하다. 본 방식은 빠른 로밍을 지원하기 위한 확장성 높은 인증 프레임워크에 관한 것으로, 직/간접적으로 구성된 도메인간의 일반적인 신뢰 관계를 바탕으로 계층적 캐쉉을 구성한다. 계층적 인증 캐쉉을 이용할 경우 확장성을 보장함은 물론 인증 지연 및 인증으로 인한 망의 오버헤드를 줄일 수 있으며, 일반적인 신뢰 관계를 갖는 도메인간의 부드러운 로밍을 지원할 수 있는 확장 가능한 인증 체계를 제공한다[9]. 그러나 초기 로밍을 위한 인증단계 및 캐쉉 에이전트 후보 등록으로 인한 지연이 발생한다는 단점이 존재한다(그림 1 참조).

3.2 모바일 커머스 AAA 메커니즘

무선랜은 빠르게 차세대 모바일 통신에서 중요한 구성요소가 되고 있다. 이러한 가능성에도 불구하고 사용자의 프라이버시와 접근 제어, 인증과 같은 문제점은 과금의 문제점과 함께 부각되고 있다. 특히, 과금 분야에서 IP 기반의 패킷 과금에 관한 연구는 서비스 제공자에게 과금을 위한 고정된 합산 시스템 도입의 어려움을 가져오고 있다. 따라서 본 방식은 모바일 커머스와 검증 결과를 위해 국제 표준과 상호 운용성을 가지는 패킷 과금을 제안하였다[3]. 그러나 과금 확인 및 Recharge를 위한 단계를 따로 거쳐야 하며, 홈 인증 서버와 Billing 서버로 집중되는 오버헤드가 증가되는 단점을 가지고 있다(그림 2 참조).

3.3 ID 기반 인증 키 교환 방식

ID 기반 인증 키 교환 방식은 이기종 무선 접속의 안전성을 위해 신원기반 인증과 AKE(Authentication Key Exchange)프로토콜을 제안하였으며, CK(Canetti and Krawczyk)-Model을 사용하여 이상적이고 안전한 키 교환 프로토콜을 처음 제안 하였다[5]. ID 기반 인증 키 교환 방식에서는 1984년 Shamir[1]에 의해 처음 제안된 신원 기반 공개키 암호 시스템을 이용하여 효율적인 AKE 프로토콜을 디자인하였다. 인증서가 필요 없는 신원 기반 공개키 시스템은 공개키 암호의 장점을 그대로 가지면서 전통적인 인증서 기반 공개키 암호 시스템의 복잡성을 감소시켰다. 따라서 ID 기



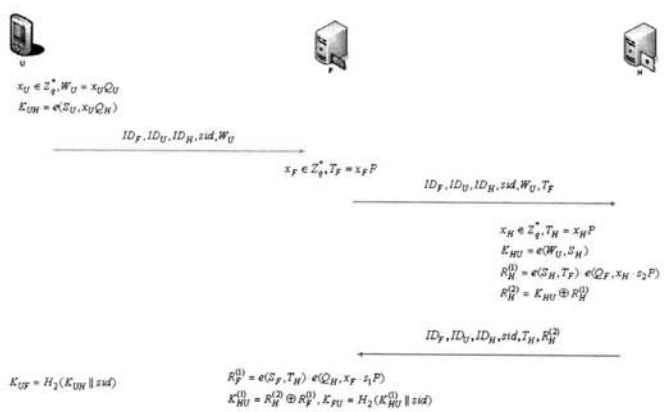
(a) 모바일 커머스 AAA 구조

(b) 잔액공지, 경고, 만료 과정

(c) 잔액 충전 과정

(d) 요금 변경 이벤트

(그림 2) 모바일 커머스 AAA 메커니즘 전체 흐름도



(그림 3) 이기종 무선 접근을 위한 ID 기반 키 교환 프로토콜

반 인증 키 교환 프로토콜은 사용자 측면에서 계산의 로드를 주로 고려하여 다른 방식들 보다 계산량에서 효율성을 높였다. 또한 안전성을 증명할 수 있는 CK-Model을 적용함으로써 안전성을 증명하였으며, 메시지에 인증자를 적용하는 대신에 사용자와 네트워크 사이에 명시적인 상호 인증을 제공한다(그림 3 참조).

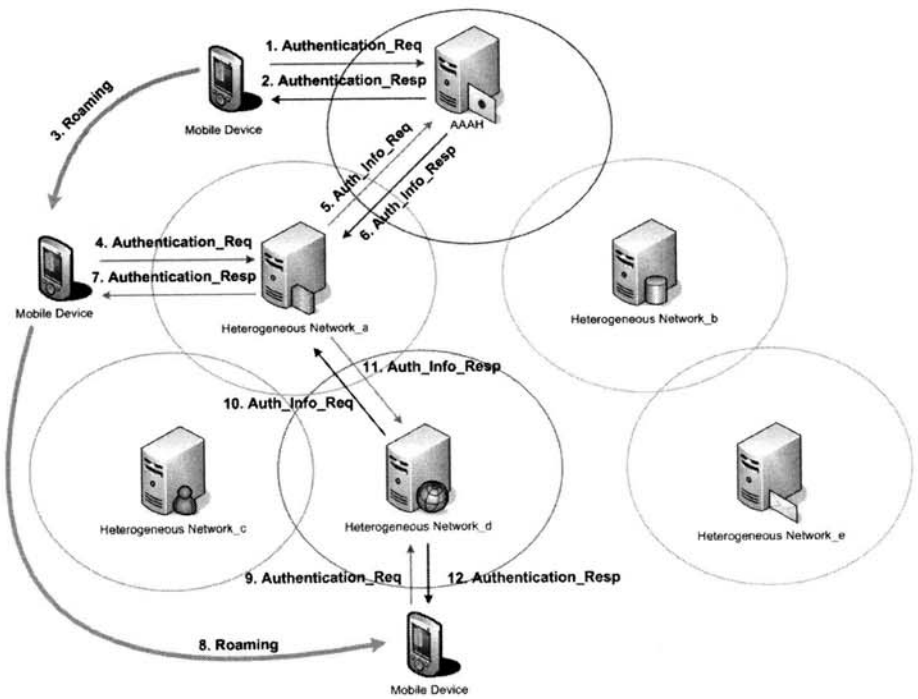
4. 제안 방식

제안 방식은 (그림 4)와 같이 이기종 네트워크 환경에서 모바일 디바이스가 홈 인증 서버에게 자신이 결제할 금액과 결제를 위한 정보를 전송하여(1. *Authentication_Req*) 인증을 요청하고 티켓을 발급 받는다(2. *Authentication_Resp*). 이후 모바일 디바이스는 이기종 네트워크로 이동하더라도 (3. *Roaming*) 홈 인증 서버로부터 발급받은 티켓을 이기종 네트워크 인증 서버에게 제시하면(4. *Authentication_Req*) 이기종 네트워크 인증 서버는 인증 요청 메시지에 신뢰 관계 인가 요청 메시지를 추가하여 홈 인증 서버로 전송한다 (5. *Auth_info_Req*). 홈 인증 서버는 티켓을 검증하고 이기종 네트워크에서 모바일 디바이스를 인증할 수 있도록 ID 기반 개인키 생성 값을 이기종 네트워크 인증 서버에게 전송한다 (6. *Auth_info_Resp*). 모바일 디바이스는 이기종 네트워크 인증 서버에게 인증을 받고 서비스를 제공받을 수 있다 (7. *Authentication_Resp*). 이기종 네트워크에서 모바일 디바이스의 서비스 이용에 따라 티켓에 포함되어 있는 선불 금액 정보에서 이용한 금액만큼 차감을 하고 티켓을 재구성 하여 과금을 처리할 수 있다. 이후의 로밍 및 인증은 전과 동일한 단계를 거쳐 수행한다(8. *Roaming* ~ 12. *Authentication_Resp*). 이로 인해 모바일 디바이스는 과금에 관한 정보 및 인증 요청을 매번 홈 인증 서버에게 전송하지 않아도 되며, 신뢰 관계 서버에서 처리할 수 있다. 또한 다른 이기종 네트워크로 이동하면, 이전 단계의 서버와 신뢰 관계를 구성하고 모바일 디바이스를 효율적으로 인증할 수 있다. 이와 같은 방식을 사용하면 이기종 네트워크 환경에서 계층적 신뢰 관계 서버를 이용하여 인증 및 과금 정보 갱신과 빠른 로밍을 제공한다.

4.1 시스템 계수

제안 방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 각각의 개체 (*MD* : 모바일 디바이스, *AAAH* : 홈 네트워크 인증 서버, *HN_i* : 이기종 네트워크 인증 서버)
- i : 이기종 네트워크의 도메인 네임 ($i=a, b,...,z$)
- ID_* : $*$의 아이디
- PW : *MD*의 패스워드
- $h()$: 충돌성이 없는 안전한 일 방향 해쉬 함수
- PIN : *MD*의 일련번호
- AT_* : $*$의 인증 시간 값
- OTP_* : $*$의 일회용 패스워드(One-Time Password)
- g : 곱셈군 Z_n^*의 생성자
- e : $G_1 \times G_1 \rightarrow G_2$ 겹선형 사상
- α_*, β_* : $*$의 인증을 위한 인증 값
- MAC : *MD*와 *AAAH* 사이의 사전 공유키로 생성한 MAC
- KGV : ID 기반 개인키 생성을 위한 MAC 값



(그림 4) 네트워크간 티켓을 이용한 AAA 메커니즘의 전체 흐름도

- $E_*[\,]$: *의 대칭키/공개키로 암호화
- $Sign_*$: *의 개인키로 서명
- KU_*/KR_* : *의 ID 기반 공개키/개인키
- $KUCert_*/KRCert_*$: *의 인증서 기반 공개키/개인키
- KS : MD와 $AAAH$가 사전에 공유한 대칭키
- HTS_Req : 로밍 인증을 위한 계층적 신뢰 관계 서버 인가 요청 메시지
- $Account\_info$: 결제를 위한 정보
- $Balance\_info$: 사용할 수 있는 선불 금액 정보
- $Balance\_info_{renewal}$: 갱신된 선불 금액 정보
- $Lifetime$: 티켓의 유효 시간

4.2 제안 프로토콜

제안 프로토콜은 인증 및 금액 정보를 포함하는 티켓 발행 단계 및 이기종 네트워크에서 과금 정보 갱신 단계와 계층적 신뢰 관계 이용한 과금 정보 갱신 단계로 이루어지며, 모바일 디바이스의 일련번호(PIN) 및 패스워드와 대칭키(KS)는 사전에 등록 단계에서 분배되었다고 가정한다. 과금은 사용자가 사전에 사용할 금액을 선불로 결제하고 금액에 따른 티켓을 발급 받는 방식을 이용한다. 이에 따라 사용자가 이용한 서비스만큼 과금하여 선불 금액 정보를 갱신하고 티켓을 재구성함으로써 선불 금액이 소진될 때까지 이기종 네트워크간에 이동하면서 서비스를 제공받을 수 있다.

4.2.1 인증 및 금액 정보 티켓 발행 단계

본 단계에서는 모바일 디바이스가 홈 인증 서버에게 인증 및 사용할 금액과 결제를 위한 정보를 전송하여 티켓을 발급받는다(그림 5 참조).

Step 1. 모바일 디바이스(MD)는 자신의 디바이스 일련번호를 해쉬한 값($h(PIN)$)과 패스워드 그리고 인증 시간 값(AT_{MD})을 이용하여 MD의 일회용 패스워드 $OTP_{MD}(=h(PIN)\oplus PW\oplus AT_{MD})$를 생성한다.

Step 2. MD는 홈 인증 서버($AAAH$)와 사전에 공유한 대칭키(KS)로 MAC 값 $KGV(=MAC_{KS}[OTP_{MD}])$를 생성한다.

Step 3. MD는 KGV를 이용하여 ID 기반 공개키 $KU_{MD}(=g^{ID_{MD}})$/개인키 $KR_{MD}(=g^{ID_{MD}}\cdot KGV)$ 쌍을 생성하고, MD의 일회용 패스워드, MD의 인증 시간 값, 결제를 위한 정보($Account\_info$)를 대칭키로 암호화하여 자신의 아이디와 함께 $AAAH$에게 전송한다.
$ID_{MD},\ E_{KS}[OTP_{MD},\ AT_{MD},\ Account\_info]$

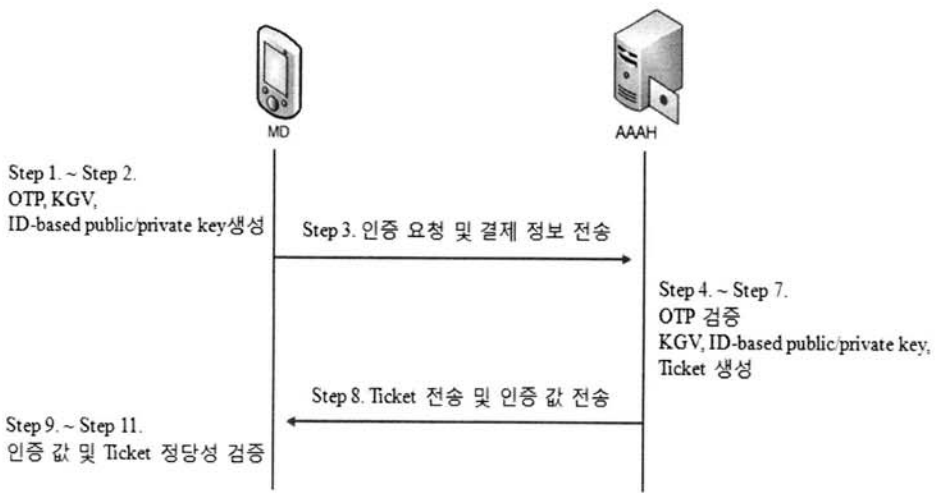
Step 4. $AAAH$는 데이터베이스에 저장되어있던 MD의 일련번호를 해쉬한 값, 패스워드, MD의 인증 시간 값을 이용하여 $OTP_{MD}'(=h(PIN)\oplus PW\oplus AT_{MD})$를 생성하고, 전송된 MD의 일회용 패스워드(OTP_{MD})와 일치한지 비교한다.

Step 5. 비교한 값이 일치하면 MD와 사전에 공유한 대칭키로 MAC를 계산하여 $KGV(=MAC_{KS}[OTP_{MD}])$를 생성한다.

Step 6. $AAAH$는 KGV를 이용하여 ID 기반 공개키 $KU_{AAAH}(=g^{ID_{AAAH}})$/개인키 $KR_{AAAH}(=g^{ID_{AAAH}}\cdot KGV)$ 쌍을 생성하고, 인증을 위한 값 $\alpha(=AT_{AAAH}\cdot g^{ID_{AAAH}})$, $\beta(=e(KR_{AAAH}, AT_{AAAH}\cdot KU_{MD}))$를 생성한다.

Step 7. $AAAH$는 MD가 이기종 네트워크로 이동하였을 때, 빠른 로밍 및 인증을 제공받기 위해 티켓을 생성한다. 티켓은 MD의 아이디, 인증을 위한 해쉬 값($h(\alpha\|\beta)$), MD가 결제한 금액 정보($Balance\_info$), 티켓의 유효시간($Lifetime$)을 공개키로 서명한 값과 $AAAH$의 아이디로 구성되어 있다.
$Ticket = ID_{AAAH}, Sign_{AAAH}[ID_{MD}, h(\alpha\|\beta),$
$Balance\_info, Lifetime]$

Step 8. $AAAH$는 생성한 티켓과 인증을 위한 값 α, β를 MD의 ID 기반 공개키로 암호화하여 MD에게 전



(그림 5) 인증 및 금액 정보 티켓 발행 단계 흐름도

송한다. $E_{KU_{MD}}[Ticket, \alpha, \beta]$

Step 9. *MD*는 α와 자신의 개인키를 이용하여 $\beta'(=e(KR_{MD}, \alpha))$를 생성한다.

$e(KR_{MD}, \alpha)=e(g^{ID_{MD}} \cdot KGV, AT_{AAAH} \cdot g^{ID_{AAAH}})=$

$e(g^{ID_{AAAH}} \cdot KGV, AT_{AAAH} \cdot g^{ID_{MD}})$

Step 10. *MD*는 생성한 β'와 전송된 β의 값이 일치하는지 비교한다.

Step 11. 비교한 값이 일치하면 $h(\alpha\|\beta)'$을 생성하고 티켓에 저장되어 있는 인증을 위한 해쉬 값($h(\alpha\|\beta)$)과 비교하여 티켓의 정당성을 검증한다.

4.2.2 과금 정보 갱신 단계

과금 정보 갱신 단계는 모바일 디바이스가 이기종 네트워크로 이동하여 이기종 네트워크 인증 서버에게 티켓을 제시하고 인증을 받은 다음 서비스 이용에 따라 과금을 한 후, 티켓의 금액 정보에서 차감하고 티켓을 갱신한다(그림 6 참조).

Step 1. 모바일 디바이스(*MD*)는 홈 네트워크에서 이기종 네트워크로 이동하면 티켓을 홈 인증 서버(*AAAH*)와 공유한 대칭키(*KS*)로 암호화하여 이기종 네트워크 인증 서버(*HN_a*)로 전송한다.

$E_{KS}[Ticket]$

Step 2. *HN_a*는 *MD*로부터 전송 받은 값에 신뢰 관계 인가 요청 메시지 *HTS_Req*를 포함하고 자신의 인증서 기반 개인키 $KRCert_{HN_a}$로 서명하여 *AAAH*에게 전송한다. $Sign_{HN\_a}[HTS\_Req, E_{KS}[Ticket]]$

Step 3. *AAAH*는 전송받은 값의 서명을 확인하고, *MD*로부터 전송된 값($E_{KS}[Ticket]$)을 복호화하여 티켓을 검증한다. 정당한 *MD*로부터 전송된 티켓인지 확인하면, ID 기반 공개키/개인키 쌍을 생성하는데 필요한 *KGV*를 *HN_a*의 인증서 기반 공개키 $KUCert_{HN_a}$로 암호화하고 자신의 인증서 기반 개인키 $KRCert_{AAAH}$로 서명하여 *HN_a*에게 전송한다. $Sign_{AAAH}[E_{KUCert_{HN\_a}}[KGV]]$

Step 4. *HN_a*는 *AAAH*로부터 전송받은 *KGV*로 자신의 ID 기반 공개키 $KU_{HN\_a}(=g^{ID_{HN\_a}})$/개인키 $KR_{HN\_a}(=g^{ID_{HN\_a}} \cdot KGV)$ 쌍을 생성하고, 인증을 위한 값 $\alpha_{HN\_a}(=AT_{HN\_a} \cdot g^{ID_{HN\_a}})$, $\beta_{HN_a}(=e(KR_{HN_a}, AT_{HN_a} \cdot KU_{MD}))$를 생성한다.

Step 5. *HN_a*는 생성한 인증 값 α_{HN_a}, β_{HN_a}를 *MD*의 ID 기반 공개키로 암호화하여 *MD*에게 전송한다.

$E_{KU_{MD}}[\alpha_{HN\_a}, \beta_{HN\_a}]$

Step 6. *MD*는 전송받은 α_{HN_a}와 자신의 개인키를 이용하여 $\beta'(=e(KR_{MD}, \alpha_{HN_a}))$를 생성한다.

$e(KR_{MD}, \alpha_{HN\_a})=e(g^{ID_{MD}} \cdot KGV, AT_{HN\_a} \cdot g^{ID_{HN\_a}})=$

$e(g^{ID_{HN\_a}} \cdot KGV, AT_{HN\_a} \cdot g^{ID_{MD}})$

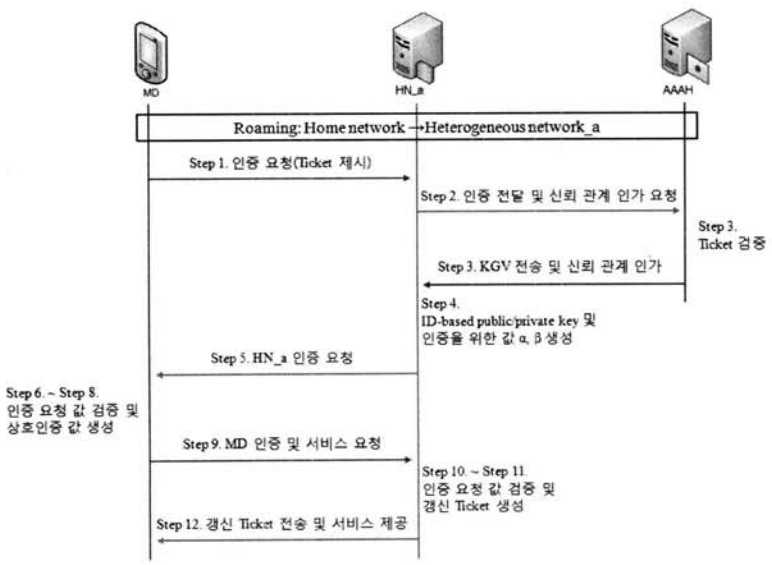
Step 7. *MD*는 생성한 β_{HN_a}'와 전송된 β_{HN_a}의 값이 일치하는지 비교한다.

Step 8. 비교한 값이 일치하면 *MD*는 상호 인증을 위해 $\alpha_{MD}(=AT_{MD} \cdot g^{ID_{MD}})$, $\beta_{MD}(=e(KR_{MD}, AT_{MD} \cdot KU_{HN_a}))$를 생성한다.

Step 9. *MD*는 인증 값 α_{MD}, β_{MD}, 서비스 요청 메시지 *Service_Req*를 *HN_a*의 ID 기반 공개키로 암호화하고 전송한다.

$E_{KU_{HN\_a}}[\alpha_{MD}, \beta_{MD}, Service\_Req]$

Step 10. *HN_a*는 step 6~step 7과 동일한 과정으로 값을 검증한다.



(그림 6) 과금 정보 갱신 단계 흐름도

Step 11. *HN_a*는 값이 일치하면 접근을 허용한다. 이후 *MD*가 이용한 서비스에 따라 과금을 한 후, 티켓의 금액 정보에서 이용한 금액만큼 차감한 후 티켓을 갱신한다.

$Ticket_{renewal} = ID_{HN\_a}, Sign_{HN\_a}[ID_{MD}, h(\alpha_{MD} \| \beta_{MD}), Balance\_info_{renewal}, Lifetime]$

Step 12. *MD*가 서비스를 이용하고 세션을 로그아웃 할 때, *HN_a*는 *MD*에게 갱신된 티켓을 *MD*의 ID 기반 공개키로 암호화하여 전송한다.

$E_{KU_{MD}}[Ticket_{renewal}]$

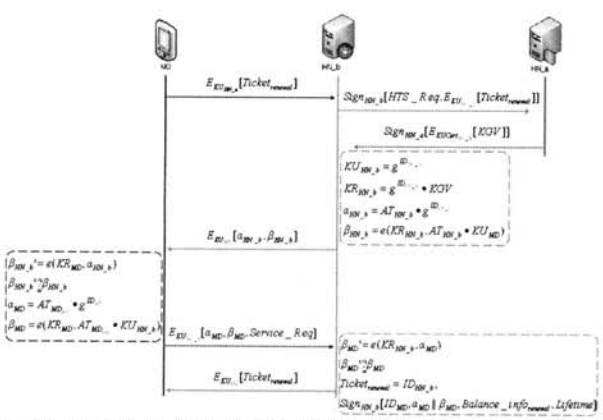
4.2.3 계층적 신뢰 관계를 이용한 과금 정보 갱신 단계

모바일 디바이스가 기존의 이기종 네트워크(a 네트워크)에서 다른 이기종 네트워크(b 네트워크)로 이동하였을 때, 이전의 이기종 네트워크 인증 서버(*HN_a*)가 발행한 티켓을 이동한 이기종 네트워크 인증 서버(*HN_b*)에게 제시하여 과금 정보 갱신 단계와 동일한 과정을 거친다. 기존의 방식과는 다르게 인증 요청 및 티켓 갱신이 홈 인증 서버에서 이루어지지 않으며, 이전 단계의 이기종 네트워크 인증 서버에서 처리한다. 이와 같이 신뢰 관계를 구성하고 있는 인증 서버로 접근하여 인증 및 인가와 과금을 처리하기 때문에 홈 인증 서버의 오버헤드를 줄일 수 있다(7 참조).

Step 1. 모바일 디바이스(*MD*)는 기존 이기종 네트워크(a)에서 다른 이기종 네트워크로(b) 이동하면 티켓을 기존 이기종 네트워크 인증 서버(*HN_a*)의 공개키로 암호화하여 새로운 이기종 네트워크 인증 서버(*HN_b*)로 전송한다.

$E_{KU_{HN\_a}}[Ticket_{new}]$

Step 2.~*Step 12.* 이후의 프로토콜은 과금 정보 갱신 단계의 프로토콜의 step 2~step 12와 동일한 과정으로 진행된다.



(그림 7) 계층적 신뢰 관계를 이용한 과금 정보 갱신 단계 프로토콜

5. 제안 방식의 분석

제안 방식을 2장의 일반적인 보안 요구 사항, 공격에 따른 보안 요구 사항, 이기종 네트워크에서의 보안 요구 사항에 맞추어 분석한다. 분석표는 <표 1>과 같다.

- 기밀성 : 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다. 제안 방식은 사전에 공유한 대칭키와 ID 기반 공개키/개인키 쌍($KU_{MD} = g^{ID_{MD}}$, $KR_{MD} = g^{ID_{MD}} \cdot KGV$)을 가지고 암호화를 통해 기밀성이 제공된다.
- 무결성 : 전송된 데이터를 바로 검증 가능함으로써 무결성이 제공되며, 메시지의 해쉬 값($h(\alpha \| \beta)$)과 MAC 값($KGV = MAC_{KS}[OTP_{MD}]$)으로 제공된다.
- 인증 : 제안 방식은 모바일 디바이스와 홈 인증 서버, 모바일 디바이스와 이기종 네트워크 서버간에는 일회용 패스워드(*OTP*), α, β, 티켓을 검증함으로써 제공된다.
- 접근제어 : 불법적인 사용자는 서비스에 접근할 수 없어야 하기 때문에, 정당하게 인증을 받지 않은 사용자는 키 관리 서버로부터 이기종 네트워크 키를 분배 받을 수 없어 키 설립이 불가능하다.
- 부인 봉쇄 : 부인 봉쇄는 전자서명에 의해 해결할 수 있으며, 제안 방식은 ID 기반 공개키/개인키 쌍으로 부인 봉쇄를 제공한다. 또한, 홈 인증 서버와 이기종 네트워크 서버간에는 서명($Sign_{HN\_a}[HTS\_Req, E_{KS}[Ticket]]$)으로써 제공된다.
- 도청 공격 : 통신 채널에서 전송되는 데이터가 제 3의 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀값을 유추할 수 없도록 해야 한다. 제안 방식은 암호화 통신을 하기 때문에 도청 공격으로부터 안전하다.
- 재전송 공격 : 제안 방식은 인증 및 금액 정보 티켓 발행 단계 및 과금 정보 갱신 단계에서 *OTP*, 인증 시간 값(*AT*)와 티켓의 유효시간(*Lifetime*)으로 재전송 공격에 안전하다.
- 위장 공격 : 제 3자가 정당한 사용자처럼 접근하는 것을 막아야 한다. 제안 방식은 각 단계마다 상호 인증을 제공하기 때문에 위장 공격이 불가능하다.
- 패스워드 추측 공격 : 사용자를 인증하는 실제적인 값은 패스워드가 아니라 *OTP*이기 때문에 *OTP*에서 패스워드의 추측은 불가능하다. 이는 모바일 디바이스의 일련번호와 패스워드 그리고 *AT*를 XOR 연산을 하고, 홈 인증 서버와 공유한 대칭키로 암호화하기 때문에 메시지를 분석 하여도 패스워드 추측 공격에 안전하다.
- 서비스 거부 공격 : 불법적인 제 3자는 통신 데이터를 획득할 수는 있지만 암호화와 무결성 제공을 위한 해쉬 값 때문에 데이터를 위조 및 변조할 수 없으며, 정당한 객체들 간에 비밀 값을 공유함으로써 정당한 객

〈표 1〉 제안 방식 분석표

	기존방식 1[9]	기존방식 2[3]	기존방식 3[5]	**제안방식**
기밀성	○	○	○	○
	대칭키	대칭키	공개키/세션키	**대칭키/ID 기반 공개키**
무결성	○	○	○	○
	해쉬 함수	해쉬함수	해쉬함수	**해쉬 함수/MAC**
인증	○	○	○	○
	캐싱 에이전트	Challenge-Response	ID 기반 공개키	**OTP/Ticket**
접근제어	○	○	○	○
	인증을 받지 않은 사용자는 서비스를 제공받을 수 없음			
부인봉쇄	X	△	○	○
				인증 서버의 전자 서명
도청공격	○	○	△	○
	암호화		메시지 노출	**암호화**
재전송 공격	△	○	○	○
	시간 만료 시 CAH 갱신(Option)	Nonce/Sequence	Nonce	**OTP/AT/Lifetime**
위장 공격	△	△	○	○
	CAH*			**인증 서버의 서명**
패스워드 추측 공격	○	X	○	○
	패스워드 추측 불가	중요정보 난수노출	패스워드 추측 불가	**패스워드 추측 불가**
상호 인증	X	○	△	○
		CHAP**(Option)	사용자와 홈 서버간의 상호인증만 제공	**디바이스와 키 관리 서버간 상호인증**
단대단보안	△	△	○	○
	계층 구조간 암호화	종단간 메시지 암호화		**종단간 메시지 암호화**
빠른 로밍 인증	△	X	X	○
	계층적 인증 캐싱 이용	인증 서버로 인증 요청		**신뢰 관계 서버 이용**
홈 인증 서버의 오버헤드 감소	X	X	X	○
	CAH의 요청으로 증가	인증 요청으로 증가		**이기종 네트워크에서 인증**
효율성	△	△	△	○
	캐싱 에이전트 후보 등록으로 인한 지연	인증 서버의 오버헤드, 로밍에 대한 문제	완전한 전방향 안전성 제공 못함	**빠른 로밍 인증, 오버헤드 감소, 과금 정보 갱신**

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

* : CAH(Caching Agent Hierarchy)

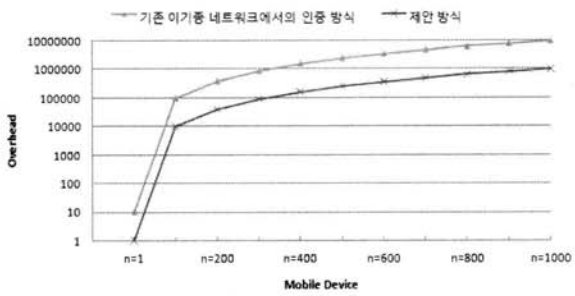
** : CHAP(Challenge Handshake Authentication Protocol)[2]

체로의 위장이 불가능하며 서비스 거부 공격에 성공할 수 없다.

- 상호 인증 : 제안 방식의 초기 인증 및 티켓 발행단계에서 홈 네트워크 인증 서버는 모바일 디바이스의 *OTP*를 이용하여 인증을 확인하며, 모바일 디바이스는 홈 네트워크 인증 서버의 티켓을 검증하여 상호 인증을 할 수 있다. 이기종 네트워크에서의 모든 인증 단계도 티켓과 α, β으로 상호 인증을 제공한다.
- 단대단 보안 : 이기종 네트워크에의 단말간 통신은 단대단 보안이 제공되어야 한다. 제안 방식에서는 종단간 뿐만 아니라 단대단 보안까지 제공함으로써 안전성을 강화 시켰다.
- 빠른 로밍 인증 : 이기종 네트워크 환경에서는 로밍이 빈번하게 일어나기 때문에 인증 시 지연이 발생하면 서비스를 이용하는데 문제점이 생길 수 있다. 제안 방식은 빠른 로밍 인증을 위해 계층적 신뢰 관계 서버를 이용하여 인증 지연을 줄였으며, 티켓을 이용하여 과금을 처리하기 때문에 메시지의 교환 횟수도 감소시켰다.
- 홈 인증 서버의 오버헤드: 이기종 네트워크 로밍환경에서 외부 네트워크로 이동한 모바일 디바이스가 홈 네트워크 인증 서버로 빈번하게 인증을 요청하면 홈 인증 서버의 오버헤드가 일어날 수 있다. 따라서 제안 방식은 매번 로밍 시 홈 인증 서버로 인증을 요청하

지 않고 계층적 신뢰 관계를 가지는 서버에게 인증을 제공받기 때문에 홈 네트워크 인증 서버의 오버헤드 및 지연을 줄일 수 있다.

- 과금 정보의 갱신 : 모바일 디바이스가 이용한 서비스에 따른 과금의 정보를 누적하여 최종적으로 중앙의 관리 서버에서 처리하는 방식은 중앙 관리 서버의 오버헤드 증가 및 효율성을 저하시킬 수 있다. 제안 방식에서는 초기에 모바일 디바이스가 이용할 금액에 대해 결제를 하고 결제에 따른 금액 정보를 포함하여 티켓을 구성한다. 그 후 모바일 디바이스가 서비스 이용 시 티켓의 금액 정보에서 이용 금액을 차감하고 티켓을 재구성하여 갱신함으로써 기존처럼 중앙의 관리서버로 접근할 필요가 없다. 이는 홈 인증 서버의 오버헤드 및 효율성과 패킷에 따른 비용 감소를 가져다준다.
- 계층적 신뢰 관계 : 계층적 신뢰 관계라는 것은 인증 서버간 인증을 통해 트리 구조의 신뢰 관계를 맺는 것을 의미하며, 모바일 디바이스를 자체적으로 인증할 수 있다. 따라서 모바일 디바이스가 이동하여 인증을 요청하거나 티켓을 갱신하고자 하였을 경우, 홈 인증 서버로 접근하여 처리하게 되면 서버의 오버헤드에 직접적인 영향을 미칠 수 있지만 제안 방식은 매번 홈 인증 서버로 접근하지 않고 계층적 신뢰 관계를 기반으로 하는 서버를 이용하여 효율성을 제공한다.
- 오버헤드 분석 : 제안 방식과 기존의 이기종 네트워크에서의 인증 방식을 디바이스의 증가에 따른 홈 인증 서버의 오버헤드 연산을 통해 비교한다. 오버헤드 비교를 위해 디바이스의 수는 $n(n=1,100,200...1000)$, 홈 인증 서버로 요청되는 인증 메시지의 수는 m, 홈 인증 서버에서 발생되는 오버헤드는 OH, 모바일 디바이스가 홈 인증 서버로부터 시작하여 세션이 끝날 때 까지 이동한 횟수 $r(r=10$, 모바일 디바이스가 네트워크간 로밍 횟수는 10회로 가정한다) 정의한다. 따라서 오버헤드 분석을 위한 수식은 $OH=n*m*r$와 같다. 예를 들어 기존의 이기종 네트워크에서의 인증 방식을 수식에서 홈 인증 서버에 등록되어 있는 모바일 디바이스가 100대, 총 이동 횟수는 10회이고, 이동할 때 마다 홈 인증 서버로 인증을 요청하므로 $OH=100*100*10=100000$이 된다. 그러나 제안 방식은 동일한 가정 하에서, 초기에 이기종 네트워크로 이동하였을 때만 홈 인증 서버로 인증을 요청하므로 총 이동 횟수 10회 중 1회만 홈 인증 서버로 접근하게 되어 $OH=100*100*1=10000$이 된다. 그러므로 모바일 디바이스의 수가 증가함에 따라 기존의 이기종 네트워크에서의 인증 방식과 제안 방식을 비교하면 오버헤드가 감소하는 것을 볼 수 있다. (그림 8)은 이상의 오버헤드를 분석한 결과이다.



(그림 8) 디바이스 증가에 따른 오버헤드 분석

6. 결 론

네트워크 환경의 변화에 따라 기존 유선 네트워크의 장점과 무선 네트워크의 이동성이 결합되어 차세대 네트워크 시대가 전개되고 있다. 이러한 유/무선 네트워크의 통합은 서비스 환경뿐만 아니라 보안기술의 변화를 가져오고 있으나, 빠른 네트워크 환경 변화에 적합한 보안기술의 부재로 인하여 다가오는 유/무선 네트워크 통합 환경에서의 서비스는 다양한 공격으로부터 위협을 받고 있다. 따라서 다가오는 유/무선 통합 환경에 적합한 보안기술의 연구 및 개발이 시급한 실정이다.

본 연구는 다가오는 유/무선 이기종 네트워크 환경에서 로밍 및 AAA 메커니즘에 관한 연구를 진행하였으며, 모바일 디바이스를 이용하여 서비스를 제공받는 사용자 인증을 위해 OTP와 ID 기반 공개키 방식을 이용하였다. 또한 티켓을 이용하여 빠른 로밍 및 홈 인증 서버의 오버헤드를 감소시켰으며, 과금 서비스는 초기에 모바일 디바이스가 이용할 금액에 대해 결제를 하고 결제에 따른 금액 정보를 포함하여 티켓을 구성한다. 그 후 모바일 디바이스가 서비스 이용 시 티켓의 금액 정보에서 이용 금액을 차감하고 티켓을 재구성하여 갱신하여 모바일 디바이스는 과금에 관한 정보 요청을 매번 홈 인증 서버에게 전송하지 않아도 되며, 신뢰 관계 서버에서 처리할 수 있다. 이와 같은 방식을 사용하면 이기종 네트워크 환경에서 계층적 신뢰 관계 서버를 이용하여 과금 정보 갱신과 빠른 로밍을 제공할 수 있다. 또한 모바일 디바이스가 이기종 네트워크로 이동하더라도 홈 네트워크로 접근하지 않고 계층적 신뢰 관계를 가지는 이기종 네트워크 인증 서버에 인증을 받아 서비스를 지속 받을 수 있게 하는 계층적 신뢰 관계 서버를 이용한 인증기술을 제안하여 안전성과 효율성을 제공할 수 있도록 하였다. 향후 통신량에 대한 분석 및 성능평가를 통해 시스템 구축 시 필요한 프로토콜의 수치적 정의가 필요할 것으로 사료된다.

참 고 문 헌

[1] Adi Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO'84, pp.47-53, 1984.

[2] Brian Lloyd and William Allen Simpson, "PPP

Authentication Protocols," RFC 1334, 1992.
[3] Gwanyeon Kim, Chinu Lee, Sehyun Park, Ohyoung Song and Byungho Jung, "A Study on Mobile Commerce AAA Mechanism for Wireless LAN," HSI 2003, pp.719-724, 2002.
[4] John Vollbrecht, Pat calhoun, Stephen Farrell, Leon Gommans, George Gross, Betty de Bruihjn, Cess Laat, Matt Holdrege and David Spence, "AAA Authorization Framework," RFC 2904, 2000.
[5] Jun Jiang, Chen He and Ling-ge Jiang, "On the Design of Provably Secure Identity-Based Authentication and Key Exchange Protocol for Heterogeneous Wireless Access," ICCNMC, pp.972-981, 2005.
[6] Pat Calhoun, John Loughney, Erik Guttman, Glen Zorn, and Jari Arkko, "Diameter Base Protocol," RFC 3588, 2003.
[7] 김봉주, "차세대 인증 프로토콜 DIAMETER AAA 기술 동향," TTA 기술표준이슈, 2001.
[8] 문종식, 이임영, "유비쿼터스 컴퓨팅 환경에서 이기종 네트워크간 안전한 키 관리 기술에 관한 연구", 멀티미디어학회 논문지, 제 11권 4호, pp.504-515, 2008.
[9] 이희진, 송유경, 이명수, 김종권, "계층적 캐싱을 이용해 로밍 확장성을 높인 인증 프레임워크", 정보과학회논문지, 제 32권 5호, pp.561-573, 2005.

문 종 식

e-mail : comnik528@sch.ac.kr
2006년 순천향대학교 정보기술공학부 (학사)
2008년 순천향대학교 컴퓨터학과(공학석사)
2008년~현 재 순천향대학교 컴퓨터학과 박사과정
관심분야 : AAA, Key Management, IPTV 보안

이 임 영

e-mail : imylee@sch.ac.kr
1981년 홍익대학교 전자공학과(학사)
1986년 오사카대학 통신공학전공(공학석사)
1989년 오사카대학 통신공학전공(공학박사)
1985년~1994년 한국전자통신연구원 선임연구원
1994년~현 재 순천향대학교 컴퓨터학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안