情報保護學會論文誌
第17卷 第4號, 2007. 8

AAA시스템의 인가 티켓을 이용한 네트워크 서비스에 관한 연구*

강 서 일,† 이 임 영‡
[1]순천향대학교 컴퓨터학부

A Study on Network Service Using Authorization Ticket in AAA system

Seo-Il Kang,† Im-Yeong Lee‡
Division of Computer, Soonchunhyang University

요 약

유비쿼터스 환경은 사용자가 서비스를 장소나 시간에 구애 없이 제공 받아야 한다. 이러한 환경을 제공하기 위해서 현재 무선 통신 기술과 모바일 단말기가 발전하고 있다. 서비스를 제공하는 업체는 사용자에 대한 인증, 인가 그리고 과금이 중요한 과제이다. 이러한 서비스를 AAA(Authentication, Authorization, Accounting)라고 하며, 지속적인 연구가 진행되어져 왔다. 기존의 연구들은 모바일 단말기의 인증과 효율성에 대해 진행되었는데 외부 인증 서버를 통해 모바일 단말기가 등록된 홈 인증 서버에 매번 접속하는 방식과 중계서버가 중간에서 인증을 제공하는 방식이 있다. 이에 본 연구에서는 티켓을 이용하는 방식에 대하여 알아보고 외부 인증 서버가 모바일 단말기에 티켓을 제공하여 이동시 마다 서비스에 대하여 인증과 인가를 제공한다. 또한 티켓을 이용함으로써 이동에 대한 검증과정을 효율적으로 제공할 수 있다.

ABSTRACT

A ubiquitous network environment is a system where the user can avail of the network's services anytime, anywhere. To establish such an environment, studies continue being conducted on wireless communication technology and mobile terminals. The company that provides such services should have an established system for authentication, authorization and charging for users. This service is referred to as Authentication, Authorization, Accounting(AAA), and its aspects have been consistently studied. On the other hand, existing studies have been promoted with regard to the authentication and efficiency of the mobile terminal. One of the method is that the mobile terminal contacts to the home authentication server through the external authentication server every time it is required and; another one is to use a medium server to provide authentication in the middle between them. Thus, this study aims to determine the best method to use ticketing, where tickets are provided through a mobile terminal, complete with authentication and authorization features. Also, as it uses ticket, it can efficiently provide mobile verification processing.

Keywords : 인가 티켓, 인증 서버, AAA, 무선 통신 보안

접수일: 2007년 1월 2일; 채택일: 2007년 6월 22일
* "이 논문 또는 저서는 2006년 정보(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임"(KRF-2006-311-D00851)
† 주저자, kop98@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

Ⅰ. 서 론

IT의 발달은 사용자들에게 다양한 서비스를 제공하고 있으며, 유선의 인터넷 서비스가 무선 통신 서비스로

이동하고 있다. 앞으로 다가올 유비쿼터스 환경에서는 언제, 어디서나 서비스를 사용자에게 제공할 수 있어야 한다. 이러한 서비스 제공을 위해 사용자의 인증 및 서비스의 권한을 제공하는 인가, 그리고 사용한 서비스에 대한 과금이 필요하게 된다. AAA는 인증, 인가와 과금을 제공하는 것으로서 사용자가 어디서 서비스를 요구하더라도 제공 받을 수 있게 한다. 그러나 사용자가 홈 네트워크를 벗어나 외부 네트워크를 이용하는 경우 외부 인증 서버는 사용자를 인증하지 못하기 때문에 서비스를 제공하지 못한다. 그러므로 모바일 단말기는 외부 인증 서버를 통해 홈 인증 서버에 접근하고, 홈 인증 서버는 인증 정보를 통해 외부 인증 서버가 모바일 단말기에 서비스를 제공할 수 있게 한다. 이와 같이 외부 인증 서버를 통하는 경우 전송되는 데이터의 안전성을 제공하기 위하여 보안 기술이 필요하다. 그러므로 본 논문에서는 인증과 동시에 서비스의 인가를 제공하여 빠른 인증 및 서비스를 제공한다. 외부 인증 서버가 홈 인증 서버로부터 인증한 데이터를 전송받아, 사용자가 이동을 하더라도 외부 인증 서버를 통하여 인증 데이터를 지속적으로 제공하여 인증 및 티켓을 갱신할 수 있도록 한다. 2장에서는 기존의 인증 및 인가 방안에서 요구사항에 대하여 알아보고 3장에서는 기존 연구에 대하여 논의한다. 그리고 4장에서는 제안 방식에 대하여 설명하고 5장에서는 2장의 요구사항으로 제안 방식을 분석한다. 마지막 6장에서 향후 연구 방향 및 결론을 도출한다.

Ⅱ. 인증 및 인가의 보안 요구 사항

AAA에서 가장 중요시하고 있는 것은 인증 서비스이다. 인증의 경우 정당한 사용자를 확인할 수 있는 과정으로 서비스 제공의 인가와 과금에 기반 할 수 있는 정보이다. 인가는 인증을 통해서 부여 받은 권한으로 시스템의 접근에 대한 권한이나 서비스의 이용 등을 말한다. 인증을 제공하기 위해서 AAA에서는 다양한 인증 프로토콜을 적용한다. 홈 인증 서버에 등록되어 있는 아이디와 패스워드를 매칭하는 것으로 어떻게 안전하게 아이디와 패스워드를 홈 인증 서버에 전송할 것인지가 관건이다. 그러므로 사용자가 이용하는 모바일 단말기가 외부 네트워크를 통해서 안전하게 데이터를 전송할 수 있는 방안이 필요하다. 이와 같은 방안으로는 모바일 단말기와 홈 인증 서버가 공유한 대칭키를 소유하여 암호화 방식을 이용한다. 이후의 통신이나 서비스를 위한 키 분배는 홈 인증 서버가 중심이 되어 외부 인증 서버에서 사용할 수 있는 키를 생성하여 제공하며, 모바일 단말기는 홈 인증 서버로부터 전송받은 키 생성 인자를 통해서 외부 인증 서버에서 이용할 수 있는 키를 생성할 수 있게 된다. 이와 같은 과정에서는 다음과 같은 보안 요구사항을 제시할 수 있다.

- 정당한 개체만이 메시지를 확인 할 수 있어야 한다.
- 전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며, 만약 위조, 삭제 및 변조된다면 그 사실을 알 수 있어야 한다.
- 정당한 사용자는 정당한 서버에 대해 자신이 사용자라는 것을 확인 시킬 수 있어야 한다.
- 정당한 사용자가 전송하는 메시지를 제 3자가 도용할 수 있어서는 안 된다.
- 제 3자가 정당한 사용자나 인증 서버로 위장하여서는 안 된다.
- 사용자와 외부 인증 서버에서 이용되는 암호 키는 동일하다는 것을 검증할 수 있어야 한다.

인가 메시지는 다음과 같은 보안 사항이 필요하다.

- 인가 메시지는 변조 및 위조가 가능해서는 안 된다.
- 정당한 객체는 인가 메시지를 검증할 수 있어야 한다.
- 재전송공격에 취약해서는 안 된다.

본 논문에서는 위에 열거된 사항에 만족하는 인증과 인가 방식을 제안하며, 빠른 이동성을 제공할 수 있는 방안으로 티켓 방식에 대해 논의 하겠다.

Ⅲ. 기존 연구

AAA시스템에서의 인증 및 인가를 제공하는 방안으로는 중개하는 시스템과 티켓 시스템으로 각각의 사용자가 인증 및 인가를 받아 사용하는 것이다. 브로커 시스템의 경우 이동을 제공하는 것이 아니라 인증에 대한 대리적인 역할을 수행한다. 그러므로 사용자는 브로커를 이용하는 경우 브로커 시스템에 접속해야 한다는 제약이 있으며, 직접적인 홈 서버로부터 인증 받기가 어렵다. 티켓 시스템의 경우 중간의 경우가 없고 홈 인증 서버로부터 직접적인 티켓을 발급 받아 이용하게 된다. 그러므로 인증 티켓을 이용하는 방안은 직접적인 과금을 할 수 있는 방안이며 브로커의 역할이 필요 없게 된다. 그러므로 AAA 시스템에서 인증 및 인가를 제공하는

티켓 방식에 대해 논의 한다. 기존의 인증 방식에서 티켓의 역할은 사용자가 인증을 받고나서 서비스의 권한을 제공하는 것으로 서비스 서버가 검증하는 방식을 적용한다. 이때 발급된 티켓은 유효 시간 안에 서비스를 제공할 수 있다. 다음의 연구에서는 모바일 단말기에 티켓을 이용하여 서비스를 제공하는 방식이다.

3.1. 무선 통신에서 티켓 기반의 AAA시스템

무선 통신에서는 모바일 단말기가 이동하더라도 서비스를 제공하기 위해서 홈 에이전트에 이동한 네트워크의 IP를 등록하여 서비스를 지속적으로 제공한다[6]. 홈 에이전트는 모바일 단말기의 IP를 홈 인증 서버에 제공하여 인증을 받고, 이동에 따른 IP를 업데이트 하는 방안을 제시하였다. 또한 외부의 이동 중인 모바일 단말기는 홈 인증 서버에 매번 접근하기에 어렵기 때문에 중계 인증 서버를 이용하여 모바일 단말기 인증에 있어 효율성을 제공한다. 무선 통신에서의 티켓 방식은 모바일 단말기의 식별자, 서비스 주소, 티켓의 유효 시간, 비밀 공유키를 포함하여 티켓을 구성하고 중계 서버에 제공함으로서 기존의 홈 인증 서버 방식 보다 효율성을 제공할 수 있다. 또한 티켓은 외부 인증 서버에 제공됨으로 중계 서버까지의 오버헤드를 줄 일수 있다. 그러나 키 협상이나 보안 설정 방안은 기존의 방식을 그대로 활용하기 때문에 티켓을 제공하더라도 인가만 제공할 뿐 인증을 제공할 수는 없다. 그러므로 모바일 단말기가 인증을 받기 위해서는 중계 서버 및 홈 인증 서버의 인증 단계가 필요하게 된다.

3.2. 티켓을 이용한 AAA 시스템

티켓을 이용한 AAA시스템은 사용자가 홈 인증 서버에 모바일 단말기의 정보를 등록하고, 홈 인증서버가 발급하는 티켓을 가지고 AP에 접근하여 사용한다. 티켓의 구성은 공개키 함수와 해쉬 함수를 이용하는 것으로써 모바일 단말기의 인증을 제공하고 외부 네트워크의 AP로부터 티켓을 받아 검증하여 서비스를 제공받는다[4]. 이와 같은 단계는 인증, 인가, 키 등록 단계로 이루어져 있으며, 인증이후 인가에서 티켓을 발급하도록 제안되어 있다. 시스템 계수는 다음과 같다.

- Dev : 모바일 디바이스
- AS : 서비스 시스템
- BM : 무선 통신 관리시스템
- PA : 무선 통신 관리 포인터
- UID : 디바이스의 아이디
- Certificate : 인증서
- h : 해쉬 함수
- E() : 암호화
- r : 랜덤 수
- T :타임 스템프

1) 인증 단계

모바일 단말기는 자신의 아이디와 인증서를 서버의 공개키로 암호화 하여 다음과 같은 메시지를 제공한다.

$$Dev -> AS : UID, P_u, Certificate,$$
$$E_{as}(UID, sreq, h(\eta), nonce, Sign_u)$$

2) 인가 및 티켓 발행

홈 인증 서버는 무선 통신 관리자한테 모바일 단말기의 아이디와 난수의 해쉬 값을 제공하고, 무선 통신 관리자는 티켓을 생성하여 각각의 AP로 전송한다. AP는 티켓의 메시지 내용을 브로드 캐스트하여 접근한 모바일 단말기가 확인한다.

$$AS -> BM : UID, sreq, h(\eta)$$
$$BM -> PA_i : TK_r$$
$$PA_i\ broadcasts : TK_r$$

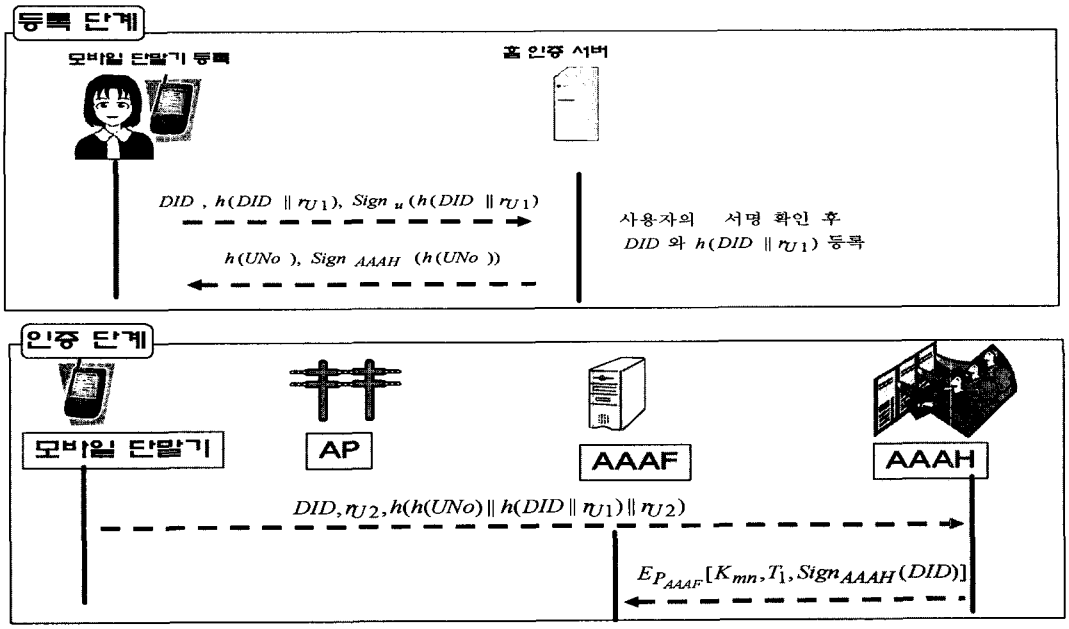
$$TK_r = D_{bm}(UID, ID_{channels}, h(\eta), T_1)$$

3) 키 등록 및 모바일 단말기의 접근

사용자의 모바일 단말기는 브로드 캐스트된 메시지의 내용을 전송받아 서비스 이용을 위해 모바일 단말기의 난수를 확인한다. 이때 난수가 틀리면 서비스를 제공받지 못하게 된다. 모바일 단말기와 AP는 안전한 통신을 위해 키를 갱신하며, 두 번째 티켓을 생성하게 된다. 연산은 다음과 같이 이루어진다.

$$PA_i\ broadcasts : P_{PA}, certificate$$
$$Dev -> PA_i : E_{PA_i}(UID, \eta, TK_r, nonce)$$
$$PA_i\ broadcasts : UID, ID_{channels}, TK_m, Sign_{PA_i}$$
$$TK_m = (k', T')$$

이 방식에서는 인증 티켓을 브로드 캐스트하는 메시지를 모든 모바일 단말기가 받을 수 있다는 것이다. 모바일 단말기가 받은 메시지는 난수에 대해서만 안전성



〔그림 1〕 등록 및 인증 단계 흐름도

을 의존하고 있다. 또한 모든 AP가 모바일 단말기들의 티켓을 가지고 있어야 하는 오버헤드가 존재하고 있다.

Ⅳ. 제안 방식

본 연구에 있어서는 모바일 단말기의 이동에 따른 서비스 제공을 위해 티켓 방식을 이용하여 홈 인증 서버의 사전 등록을 통해 안전성을 제공한다. 또한 외부 네트워크 망에서 서로 다른 AP간의 이동을 고려하여 외부 인증 서버가 발행하는 티켓으로 AP간의 이동에 효율성을 제공한다. 제안 방식을 각각의 단계로 나누면, 등록, 인증, 인가, 티켓 갱신 단계로 총 4단계 이다.

4.1. 시스템 계수

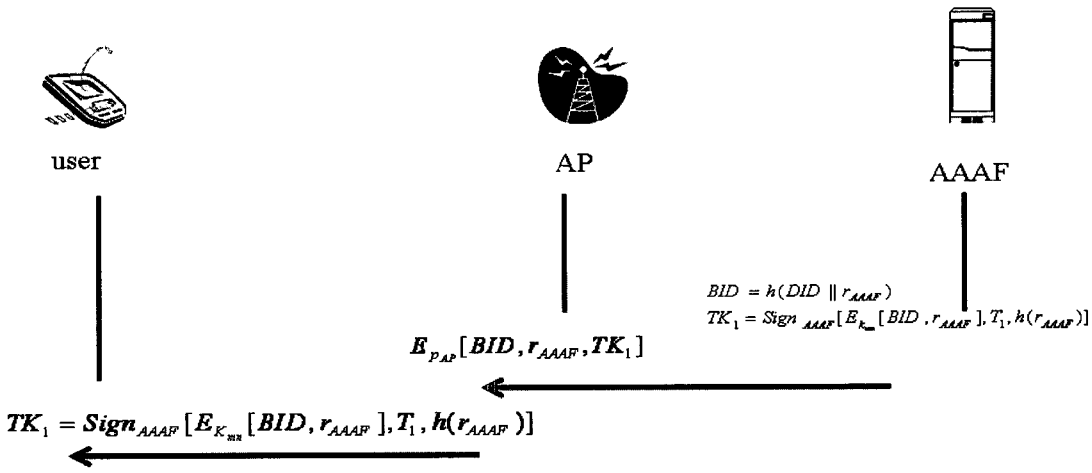
다음은 본 제안 방식에서 사용되는 시스템 계수이다.

- * : 통신의 개체(User : 사용자, AAAH : 홈 인증 서버, AAAF : 외부 인증 서버)
- DID : 사용자 모바일 단말기 아이디
- BID : 외부 네트워크에서 사용되는 가상 아이디
- h() : 충돌성이 없는 안전한 일방향 해쉬 함수
- r* : *가 선택한 랜덤 수
- T* : 타임 스탬프로서 키를 발급한 시간
- UNo : 홈 인증 서버가 등록한 모바일 단말기에 부여하는 일련 번호
- Sign* : *의 전자 서명 값
- P* : *의 공개키
- oAP : old AP (모바일 단말기가 외부 네트워크에서 초기 접속한 AP)
- nAP : new AP (외부 네트워크에서 이동에 따라 새로 접속하게 되는 AP)

4.2. 등록 단계

등록단계는 사용자가 모바일 단말기를 홈 인증 서버에 등록하는 것으로써 안전한 통신로를 통해 키 분배가 이루어진다. 다음과 같은 과정을 통해 사용자의 모바일 단말기를 홈 인증 서버에 등록한다.

Step1 : 모바일 단말기는 홈 인증 서버에 모바일 단말기 아이디(DID)와 랜덤수(rU1)를 해쉬(h(DID|| rU1))하고 서명 값(SignU(h(DID||rU1)을 전송한다.



〔그림 2〕 인가 단계 흐름도

Step2 : 홈 인증 서버는 전자 서명을 확인한 후 DID와 h(DID||rU1)를 등록한다. 이후 모바일 단말기에 일련번호(UNo)를 부여하고 해쉬한 값(h(UNo))과 홈 인증 서버의 서명 값(SignAAAH(h(UNo))을 전송한다.

4.3. 인증 단계

사용자는 등록된 모바일 단말기를 가지고 외부 네트워크에서 서비스를 요청할 수 있다. 그러므로 정당한 사용자 인지를 확인하기 위해 홈 인증 서버에 인증을 요청한다. 홈 인증 서버는 외부 인증 서버에서 사용할 수 있는 키를 설립하여 제공한다. 이로 인해 외부 인증 서버와 모바일 단말기는 안전한 통신을 할 수 있게 된다. 이때 통신 메시지는 제 3자에 의해 위장, 재전송, 변조할 수 없어야 한다.

Step1 : 모바일 단말기는 홈 인증 서버에 다음과 같이 모바일 단말기 아이디(DID)와 임의 난수(rU2) 그리고 해쉬값(h(h(UNo)||h(DID||rU1)||rU2)을 전송한다.

Step 2 : 홈인증 서버는 전송 받은 데이터를 검증한고 검증이 올바르면 키 설립을 한다.

검증 단계 : $h(h(UNo)\|h(DID\|r_{U1})\|r_{U2}) \doteq h'(h(UNo)\|h(DID\|r_{U1})\|r_{U2})$

키 설립 : $K_{mn} = h(h(DID\|r_{U1})\|T_1')$

Step3 : 홈 인증 서버는 외부 인증 서버의 공개키를 이용하여 생성된 키와 모바일 단말기 인증 메시지를 전송 외부 인증 서버에 전송한다.

$E_{P_{AAAF}}[K_{mn}, T_1, Sign_{AAAH}(DID)]$

4.4. 인가 단계

인가는 외부 인증 서버가 모바일 단말기에 서비스를 제공하는 것으로써 인가 메시지를 받은 모바일 단말기는 외부 네트워크 내에서 어디로 이동하더라도 서비스를 지속적으로 받을 수 있다. 또한 세션키를 제공하여 모바일 단말기의 통신에서 안전한 통신로를 제공한다.

Step1 : 외부 인증 서버는 접근한 모바일 단말기의 가상 아이디와 티켓을 생성한다.

가상 아이디 : $BID = h(DID\|r_{AAAF})$

티켓 : $TK_1 = Sign_{AAAF}[E_{K_{mn}}[BID, r_{AAAF}], T_1, h(r_{AAAF})]$

Step2 : 외부 인증 서버는 AP의 공개키를 이용하여 생성한 내용을 암호화하여 AP에 전송한다.

$E_{P_{AP}}[BID, r_{AAAF}, TK_1]$

Step 3 : AP는 개인키로 메시지를 복호화 하여 티켓(TK1)을 확보하고, 가상 아이디(BID)는 모바일 단말기의 아이디가 된다. 공유하는 대칭키는 입력값으로 rAAAF를 이용한다.

Step 4 : AP는 모바일 단말기에 티켓(TK1)을 제공한다.

$TK_1 = Sign_{AAAF}[E_{K_{mn}}[BID, r_{AAAF}], T_1, h(r_{AAAF})]$

Step 5 : 모바일 단말기는 티켓(TK1)으로 키(Kmn)를 생성하고, 키 입력값으로 rAAAF를 획득할 수 있다.

$K_{mn} = h(h(DID \| r_{U1}) \| T_1)$

4.5. 티켓 갱신 단계

티켓 갱신은 모바일 단말기가 접근 한 외부 네트워크에서 내에서 AP를 이동함으로 인해 새로운 AP에 접근하면, 기존의 티켓을 갱신하여 지속적인 서비스를 제공받을 수 있게 한다.

Step1 : 모바일 단말기는 새로운 AP에 접근하여 이전에 사용하던 세션키로 가상 아이디(BID)와 티켓 요구(R_TK2)및 메시지 요구 시간을 포함하여 전송한다.

$E_{K_{r_{AAAF}}}[BID, R_{TK_2}, T_1]$

Step2 : 새로운 AP는 외부 인증 서버에 모바일 단말기로부터 전송 받은 메시지를 제공하여, 갱신된 인가 티켓을 요구하게 된다.

Step 3 : 외부 인증 서버는 전송된 내용을 확인하고 티켓을 갱신하여 AP에 재발급을 한다.

티켓 갱신 내용 :

$TK_2 = Sign_{AAAF}[E_{K_{r_{AAAF}}}[BID, r_{AAAF2}], T_2, h(r_{AAAF2})]$

AP에 전송 내용 : $E_{P_{AP}}[BID, r_{AAAF2}, TK_2]$

Step4 : 새로운 AP는 개인키로 메시지를 복호화하여 티켓(TK2)을 획득하여 모바일 단말기에 갱신된 티켓(TK2)을 제공한다.

V. 제안 방식 분석

제안 방식의 단계를 2장에서 제시한 보안 요구 사항을 만족하는지 검증한다.

• 정당한 객체만이 확인

각각의 메시지는 공개키와 대칭키(K_{mn})로 암호화 되어 전송되며, 사용자와 서버는 사전의 등록 단계를 거쳐서 안전하게 통신을 할 수 있게 된다. 이후에 키의 갱신에서도 새로운 키를 설립하여 이전의 사용하던 메시지를 확인할 수 없는 방식을 제시하고 있다. 그러므로 각각의 키의 구성을 모르는 경우 암호화된 메시지를 확인하기는 매우 어려울 것으로 사료된다.

• 위조 및 변조

메시지를 위조 및 변조하기 위해서는 서명을 위조하여야 하며 초기 등록 과정에서의 사용자의 난수(rU1, rU2)를 알아야 한다. 또한 각각의 메시지 설립 과정의 난수를 검증할 수 있어야 하는데 난수의 해쉬 값을 제공하므로 인해 정당한 객체라도 메시지를 재 위조 및 변조를 할 수 없다. 예로 티켓의 값을 변경하려면 rAAAF를 변경해야 하고 $BID, h(r_{AAAF})$의 값도 변경하여야 한다. 또한 서명 값의 내용도 변경하여야 한다.

• 정당한 서버와 사용자 확인 방안

제안 방식에서 정당한 서버와 사용자를 확인하는 방안으로는 두 가지를 제공하고 있다. 하나는 공개키 기반의 서명이고 다른 하나는 사전 등록되어 있는 난수의 값이다. 사전의 아이디와 난수(rU1, rU2)값을 등록하여 이후의 정당한 사용자는 난수값을 알고 있기 때문에 통신에서 활용할 수 있다. 그러나 제 3자나 위장하는 경우 변경되는 난수의 값을 모르기 때문에 메시지를 생성할 수 없게 된다. 키의 갱신의 과정에서도 이전의 세션키를 활용한 암호화 메시지로 인해 이전의 사용자라는 것을 확인할 수 있다.

• 생성된 키 인증

새로 생성된 세션키의 경우 동일한 키를 생성하였는지를 확인하여야 한다. 이와 같은 과정으로 임의 메시지를 암호화하여 전송하고 복호화 메시지를 다시 확인하는 과정을 통하여 서로 동일한 세션키를 생성하였다는 것을 인증할 수 있다.

• Known-key attack

Known-key attack은 이전의 세션키로 암호화된 메시지를 전송하는 것으로 본 제안 방식에서 r_AAAF가 노출되면 갱신단계에서 재전송으로 공격을 할 수 있다. 그러므로 메시지 내용에 T1의 메시지 요청 시간을 포함하여 유효한 시간에 메시지를 발급한 시간을 검증한다.

〔표 1〕 제안방식 분석

분류	제안 방식 기술		비고
효율성	모바일 단말기	대칭키, 난수, 해쉬 활용, 전자 서명 검증 ($K_{mn}, r_{U1}, r_{U2}, r_{AAAF}$)	모바일 단말기의 연산은 대칭키 기술과 난수, 그리고 해쉬 함수, 전자 서명 검증
	인증 서버	사용자 관리의 티켓 $TK_1 = Sign_{AAAF}[E_{K_{mn}}[BID, r_{AAAF}], T_1, h(r_{AAAF})]$	사용자의 관리에 있어 티켓의 구성으로 시간내의 정당한 사용자에게 서비스를 제공한다.
안전성	■ 사용자는 서비스의 익명성을 제공 받을 수 있음.(BID활용) ■ 동일한 외부 네트워크에서의 이동시 TK의 발급에 따른 인증 과정이 제공되지 않더라도 세션키를 활용한 정당성 부여 ($E_{K_{r_{AAAF2}}}[BID, r_{AAAF2}]$)		익명성은 서비스제공에 있어 프라이버시를 추가적으로 제공 가능하다. 별도의 인증과정이 없이 세션키를 모르면 TK2를 활용할 수 없다.

〔표 2〕 기존 방식과의 비교표

분류	기존 연구 3.1〔6〕	기존 연구 3.2〔4〕	제안 방식
인증 방식	홈 서버의 비밀 공유키 이용	사용자의 인증서를 활용	등록에 사용된 해쉬값 이용 홈 서버의 등록 인증 값 검증
이동성	티켓을 이용한 인가만 제공	인가 티켓 발행 키 갱신 및 등록	외부 인증 서버의 AP 티켓 발행, AP간의 이동에 티켓 활용
인증에 따른 효율성	홈 서버의 인증 및 브로커 서버의 인증을 제공하므로 사용자의 이동에 따른 단말기의 접근에 오버헤드가 증가함.	홈 서버의 인증 티켓 제공, 브로드캐스트 방식을 이용한 오버헤드 증가.	등록 단계에서 인증서를 이용하여 안전한 등록, AP 이동간의 티켓을 이용한 효율성 제공

〔표 3〕 모바일 단말기의 이동에 따른 인증 및 인가 제공 횟수

분류	기존 연구 3.1〔6〕		기존 연구 3.2〔4〕		제안 방식		비교
	인증	인가	인증	인가	인증	인가	
홈 인증 서버	1회	1회	10번	1회	1회	1회	홈 인증 서버의 인증 및 인가 횟수
중계 인증 서버	10번	10번	존재 안함	존재 안함	존재 안함	존재 안함	3.1의 경우 중계서버가 홈 인증 서버의 대리적 역할 수행
외부 인증 서버	제공 못함	10번	제공 못함	10번	10번	10번	제안 방식은 외부 인증 서버가 홈 인증 서버의 대리적 역할 수행
모바일 단말기 이동 횟수	10번	10번	10번	10번	10번	10번	하나의 모바일 단말기가 네트워크 내 이동을 10번하는 경우

만약 시간의 검증을 못하는 경우 메시지를 폐기하며 갱신 단계를 통과하면 이전 세션키는 r_AAAF2로 변경된다. 2회 통신문으로 Known-key attack은 어려울 것이며, 재전송도 시간에 의해 불가능할 것으로 생각된다.

기존 연구와의 차이점은 〔표 2〕에 기술되어 있다. 안전성을 제공하기 위해 공유키와 인증서를 이용한다. 본 방식에서는 인증서를 이용한 등록 과정을 인증 이전에 이루어져 안전한 키 교환을 위한 난수를 공유한다. 인증서는 등록과정에서만 사용하기 때문에 단말기는 오버헤더는 다른 방식과 비교하여 줄어든다. 또한 제안 방식에

서는 외부 인증 서버가 인증서를 이용하여 티켓을 제공하고 단말기는 이를 검증 단계로 이용한다. [표 3]을 보면 각각 방식의 서비스에서 홈 서버를 대처하는 경우와 홈 인증 서버가 직접 인증을 제공하는 이전 연구를 보면 10회의 인증 및 인가가 요구되는 것을 볼 수 있다. 그러나 제안 방식은 외부 네트워크의 서버가 대리적인 역할을 수행함으로 홈 인증 서버의 오버헤드를 줄 일 수 있다. 중계 서버의 설치가 없으므로 기존 시스템에서 적용하여 제공할 수 있게 된다.

Ⅵ. 향후 연구 방향 및 결론

본 제안 방식은 외부 네트워크에서 접근한 모바일 단말기를 홈 인증 서버가 인증하고 인가 티켓을 외부 인증 서버에서 생성하여 제공한다. 외부 인증 서버에서 제공 하는 티켓을 이용하여 접근한 단말기를 인가하게 되고 서비스를 제공하게 된다. 또한 외부 네트워크 내에서 이동을 하는 경우 티켓의 갱신을 제공하여 새로운 세션 키를 설립하고 홈 네트워크로 다시 접근하여 인증을 받지 않아도 되는 효율성을 제공하고 있다. 제안 방식은 모바일 단말기의 제약 사항을 벗어 날 수 있으며, 서비스를 안전하고 빠르게 제공할 수 있다. 제안 방식에서 안전성을 위한 키 분배에는 외부 인증 서버가 주도적인 역할을 수행한다. 또한 AP는 단말기에 이동에 따른 티켓을 갱신하므로 안전하게 이동 및 서비스를 제공할 수 있다. 그러나 향후 연구 방향에 있어서는 암호화에 사용된 키관리 부분이 필요하다. 특히 모바일 단말기가 증가하고 무선 네트워크가 구성됨으로 각각의 키 분배 및 폐기 방안이 필요하게 된다. 그러므로 본 제안 방식의 인증 및 인가 티켓을 이용하는 방안에 대하여 알아보고 향후의 연구에서는 무선 통신 네트워크에서의 키 관리 부분을 추가하여 진행되어야 할 것으로 사료된다.

참고문헌

[1] I.Artur Hecker, Houda Labiod, Ahmed Serhrouchnei "Authentis : Trhrough Incremental Authentication Models to Secure Interconnected Wi-Fi WLANs," ASWN2002, 2002

[2] S.patel, "Weaknesses of north american wireless authentication protocol," IEEE Wireless Communications, vol. 4, no. 3, June 1997.

[3] Qiang Tang, J.Mitchell, "On the security of some password-based key agreement schemes", Cryptology ePrint Archive, pp.1-9, 2005.

[4] Yihong Zhou, Dapeng Wu and Scott M. Nettles, "On the Architecture of Authentication, Authorization, and Accounting for Real-Time Secondary Market Services," International Journal of Wireless and mobile computing, pp.1-8, Jan, 2005

[5] Yu Chen, Terrance Boult, "Dynamic Home Agent Reassignment in Mobile IP", IEEE-WCNC02, pp.44-48, 2002.

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

[7] 이효성, 김기천, 김인수 "Mobile 환경에서의 AAA 지역 등록 인증 개선 방안", 한국정보처리학회 2004년 추계학술대회, pp1267-1270, 2004

[8] 진봉재, 허의남, 문영성, "IEEE802.11 무선랜 기반의 Mobile IPv6 AAA환경에서 핸드오버 최적화 방안 연구", 한국정보처리학회 2004년 추계학술대회, pp1201-1204, 2004

[9] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication dial In User Service(RADIUS)", RFC 2865, 2000. 06

[10] F. Johansson, "Mobile IPv4 Extension for Carrying Network Access Identifiers", RFC3846, 2004. 06

[11] J. Vollbrecht, P. Calhoun, "AAA Authorization Application Examples", RFC 2905, 2000. 08

[12] J. Vollbrecht, P. Calhoun, "AAA Authorization Framework", RFC 2904, 2000.08

〈著者紹介〉

강 서 일 (Kang Seo Il) 학생 회원
2003년 2월 : 순천향대학교 정보기술 공학부 졸업
2004년 6월~2005년 2월 : 순천향대학교 전산학과 석사
2005년 3월~현재 : 순천향대학교 전산학과 박사 과정
관심분야 : 무선 네트워크 보안, 전자 투표, 전자 화폐

이 임 영 (Lee Im Yeong) 종신회원
1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학전공 석사
1989년 3월 : 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재 : 순천향대학교 컴퓨터 학부 교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안