DOI: 10.3745/KIPSTC.2008.15-C.5.343

모바일 디바이스의 로밍을 위한 사용자 인증에 관한 연구

강 서 일[†] · 박 춘 식[††] · 이 임 영[†††]

요 약

유비쿼터스 환경에서 사용자는 다양한 디바이스를 이용하여 서비스 및 이동성을 제공 받는다. 사용자가 이용하는 네트워크는 홈 네트워크(사용자가 인증 서버를 통해 속해 있는 네트워크)와 외부 네트워크(사용자가 이동 혹은 외부 인증 서버가 존재하는 네트워크)로 나눌 수 있으며, 사용자는 모바일 디바이스 및 외부 네트워크의 디바이스를 이용할 수 있다. 본 논문은 사용자가 모바일 디바이스를 가지고 외부 네트워크에서 서비스에 접근 하였을 때 안전하게 개인 정보(암호화 키 등)를 로밍하여 서비스를 제공하는 방안과 외부 네트워크의 디바이스를 이용하여 홈 네트워크에 접근하는 방안을 제시한다. 본 제안 방식을 활용 한다면 외부 네트워크에서도 안전하게 서비스를 제공 받을 수 있게 로밍을 제공할 수 있다.

키워드 : 로밍, 인증, 모바일 디바이스, 보안 프로토콜

A Study on User Authentication for Roaming in Mobile Device

Seo-il kang[†] · Choon-sik Park[††] · Im-yeong Lee[†††]

ABSTRACT

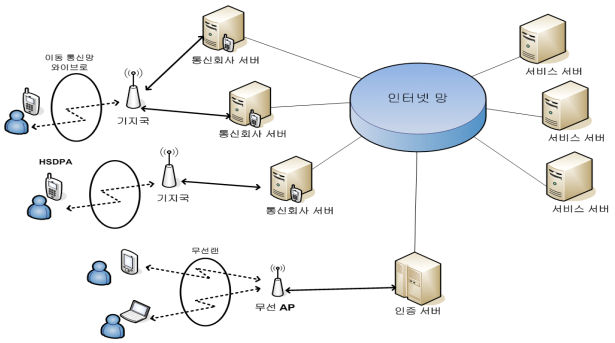
In ubiquitous environment, a user has been provided with service and mobility using various devices. The users' network can be divided into a home network (a user belongs to the network through an authentication server) and an external network (when a user moves or external authentication server is). Users can use a mobile device or a device at an external network. In this paper, when a user has access to a service in an external network with a mobile device, there is a skim that a service is securely provided by roaming private information (encryption key etc…) and a skim which gives access to a home network using a device in an external network. If you use these skims, roaming is provided in order that you can use a secure service in an external network.

Keywords : Roaming, Authentication, Mobile Device, Security protocol

1. 서 론

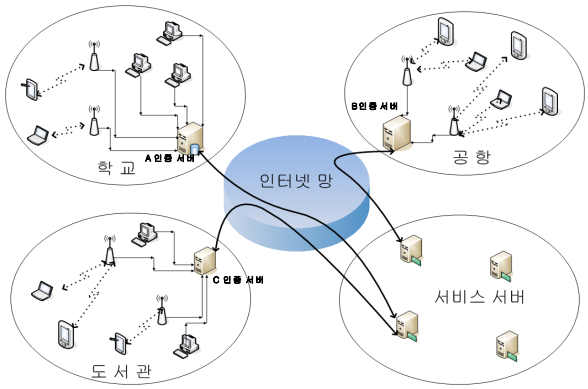
IT기술의 발달로 사용자는 다양한 모바일 디바이스(모바일 폰, PDA, 노트북 등)를 이용 하며 길거리나 기차, 도서관 등 여러 장소에서 무선 통신 서비스를 제공 받을 수 있다. (그림 1 참조)

모바일 디바이스는 와이브로, HSDPA(High Speed Downlink Packet Access), 무선 랜 등의 무선 통신 기술을 이용한다[1,2,6]. 사용자의 인증 및 보안 기술은 무선 통신에 따라 차별성을 갖는데 모바일 폰의 경우 통신 회사의 인증 센터 및 3G 통신에서는 USIM(Universal Subscriber Identity Module)카드를 이용한다. 무선 랜의 경우 인증 서버인 RADIUS(Remote Authentication Dial In User Service)[13], SSID(Service Set IDentifier)와 WEP(Wired Equivalent Privacy) 등을 활용하게 된다. 무선 랜은 홈 네트워크, 도서관, 공항, 학교 등 건물이나 지역 내의 구축이 용이하며, 유선망에서 AP(Access Point)를 통해 무선 망 구축이 쉽기



(그림 1) 무선 통신 서비스의 흐름도

† 준 회 원 : 순천향대학교 전산학과 박사과정
†† 정 회 원 : 한국전자통신연구원 부설연구소 책임연구원
††† 종신회원 : 순천향대학교 컴퓨터학부 교수(교신저자)
논문접수 : 2008년 3월 18일
수 정 일 : 2008년 6월 27일
심사완료 : 2008년 8월 14일



(그림 2) 무선 랜 망을 이용한 서비스 제공 흐름도

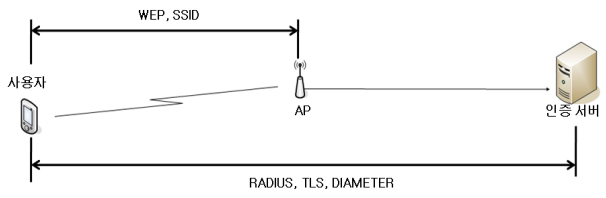
때문에 활용도가 매우 높다. (그림 2)에서 A, B, C의 인증 서버는 네트워크를 이용하는 사용자 인증 서버이고, 서비스 서버는 사용자가 이용하는 서비스 업체의 서버이다. 대부분 공공 기관의 무선 랜 서비스는 사용자를 인증하지 않고 네트워크를 무료로 이용할 수 있으나, 학교, 회사, 혹은 호텔의 경우 네트워크 사용자 인증을 통해 서비스가 제공된다. 하지만 무선 랜을 이용하는 경우 외부에서 인증받기 어렵다는 점과 디바이스 변경에 따른 암호 기술의 적용의 어려움이 존재한다. 그러므로 메인 인증 서버가 필요하며 이 역할을 홈 네트워크의 홈 인증 서버가 하게 된다. 본 논문의 2장에는 기반 연구에 대하여 알아보고, 제 3장에서는 사용자의 이동에 따른 인증과 활용 방안 및 그룹키에 대한 제안 방식을 설명한다. 제 4장에서는 제안 방식을 분석하고, 마지막인 제 5장에서 결론 및 향후 연구에 대하여 논의한다.

2. 기반 연구

무선 랜에서 보안 적용 구간은 두 구간으로 나눌 수 있다[5, 6]. 첫 번째 구간은 사용자의 모바일 디바이스와 AP간이고, 두 번째 구간은 사용자와 인증 서버간의 통신 구간이다. (그림 3)을 보면 사용자가 이용하는 모바일 디바이스와 AP간의 통신 구간은 SSID와 WEP를 이용하고 사용자와 인증 서버간은 RADIUS, TLS와 DIAMETER 등을 이용한다.

2.1 무선 랜 보안 기술

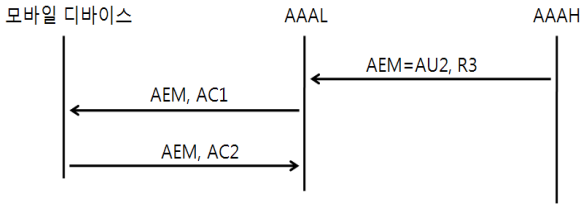
무선 랜의 WEP와 SSID는 사용자가 이용하는 모바일 디바이스와 AP사이의 보안을 제공한다. SSID의 경우 네트워크 아이디만 알면 접근 가능하다. WEP의 경우는 비밀키를 공유하고 있어 SSID보다 보안성을 제공하나, 짧은 길이의 비밀키와 초기 벡터값의 노출 그리고 트래픽 분석 공격에 취약하며, 제 3자의 중간자 공격도 가능하다. 사용자와 인증 서버간의 보안 방식으로 RADIUS를 적용하는 방안도 있다[13]. 그러나 사용자의 모바일 디바이스와 RADIUS간 사전에 안전한 통신로가 필요하며 이를 제공하기 위해 TLS(Transport Layer Security)를 이용한다. 이러한 방식은 메시지 교환이 증가하고 인증서를 검증하기 위한 방법이 추가되게 된다.



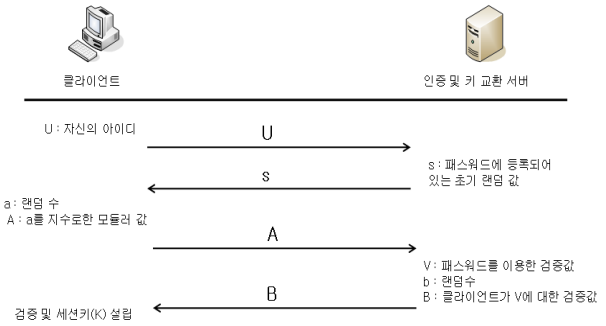
(그림 3) 무선 랜에서의 보안 기술 적용

2.2 Mobile 환경에서의 AAA 지역 등록 인증 방식

모바일 환경에서의 AAA 지역 등록 인증 방식은 모바일 IP환경의 AAA 구조에서 모바일 디바이스의 이동으로 인한 핸드오프와 모바일 디바이스 인증 처리과정을 간소화하는 방안으로 제시되었다[5]. 모바일 디바이스는 외부 이동시 홈 망의 AAA 서버로부터 재 인증 및 세션키 설립에 대한 취약성을 해결하고자 하였다. 해결방안으로 AAA 구조에서 인증 절차를 처리 해줄 수 있는 AEM(Authentication Extension Message)를 제시하였다. AEM의 구성은 홈 인증 서버로부터 사용자를 인증할 수 있는 검증값(AU1)과 알고리즘(R1)으로 되어 있다. 이와 같은 AEM을 제공함으로 인해 중간의 외부 에이전트를 설정할 필요가 없다. 그러므로 모바일 디바이스가 홈 인증 서버(AAAH)에 등록시 AEM 인증 확장 메시지를 전송받고, 이후에 해쉬 값과 알고리즘을 이용하여 사용자 인증을 외부 인증 서버에서 제공하며, 빠른 핸드오프를 지원한다. 모바일 디바이스가 외부의 인증 서버에 자신의 인증을 알려주는 것으로 홈 인증 서버에는 접근이 필요하지 않다. 하지만 이렇게 되는 경우 AEM를 가지고 있는 모바일 디바이스가 인증을 요구 하지 않아도 모든 지역의 외부 인증 서버는 AEM에 응답할 수 있는 메시지를 가지고 있어야 한다. 인증 절차는 간단히 이루어지지만 각각의 사용자 모바일 디바이스의 AEM을 유지하기 위해 외부 인증 서버는 적어도 홈 인증 서버와 1회 이상의 통신을 해야 하는 오버헤드를 가지고 있다. (그림 4)를 보면 홈 인증 서버는 외부 인증 서버에 AEM 메시지로 인증(AU2)과 알고리즘(R3)를 제공한다. 외부 인증 서버는 모바일 디바이스에 인증 챌린저(AC1)와 AEM을 제공한다. 모바일 디바이스는 AC1에 응답하는 AC2를 생성하여 외부 인증 서버에 제공하고 외부 인증 서버는 AC2의 값이 올바른지 검증하게 된다.



(그림 4) AEM을 이용한 모바일 디바이스 인증 흐름도



(그림 5) SRP 프로토콜

2.3 SRP 방식

SRP(Secure Remote Password)방식은 인증과 키 교환을 제공하는 것으로 기존의 패스워드의 취약점인 능동적 공격(사전 공격 및 재전송 공격 등)과 유추 공격을 막을 수 있는 방안으로 제시되었다[11]. 사용자의 패스워드(p)를 서버와 클라이언트가 공유한 상태에서 모듈러 연산 및 해쉬 함수(SHA)를 이용하여 검증 값(S)을 생성한다. 또한 검증 값(S)로 세션키($K=h(S)$)를 생성하여 활용한다. 인증 및 키 교환 방법은 다음과 같다(그림 5참조).

step 1 : 클라이언트가 자신의 아이디(U : User Name)를 서버에 전송한다.

step 2 : 서버는 사용자의 패스워드(p) 파일에 등록된 초기 랜덤 값(s)를 클라이언트에 전송한다.

step 3 : 클라이언트는 랜덤 수(a)를 선택하여 모듈러 연산($A=g^a \bmod n$)을 하여 서버에 A의 값을 전송한다.(n은 소수)

step 4 : 서버는 패스워드(p)를 이용한 $x(SHA(s\|SHA(U\|p)))$를 생성하여 검증 값($V=g^x \bmod n$)와 랜덤 수(b)를 이용하여 클라이언트에서 검증할 수 있는 값($B=(V+g^b) \bmod n$)을 생성하여 클라이언트에 B를 전송한다.

step 5 : 클라이언트는 서버로부터 전송받은 B를 이용하여 클라이언트 검증 값 S를 다음과 같이 생성 한다.

$$S=(B-g^x)^{(a+ux)}\bmod n=((V+g^b)-g^x)^{(a+ux)}\bmod n$$
$$=(g^x+g^b-g^x)^{(a+ux)}\bmod n$$
$$=g^{b(a+ux)}\bmod n$$

step 6 : 서버는 클라이언트의 A값을 이용하여 다음과 같이 클라이언트와 동일한 서버 검증 값 S를 생성한다.

$$S=(A*g^{xu})^b\bmod n=(g^a*g^{xu})^b\bmod n=g^{(a+ux)b}\bmod n$$

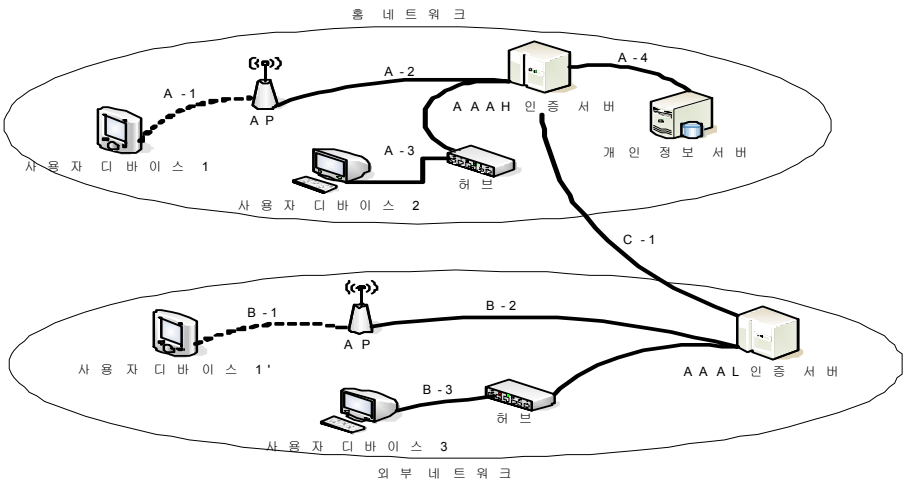
step 7 : 서버와 클라이언트는 상호 검증 값 S를 이용하여 서버와 클라이언트의 공통 세션키 K를 다음과 같이 생성한다.

$$K=SHA(S)$$

SRP방식은 인증 및 세션키 설립 방식으로 개인 정보 서버의 인증 방식에 적용할 수 있는 방안이 된다. 그러나 여러 디바이스가 사용되는 상황에서는 디바이스의 연산 능력이 제약 사항으로 취약점이 될 수 있으며, 개인 정보의 디바이스 이동을 통한 인증 방식으로는 적합하지 않은 부분이 존재한다.

3. 제안 방식

본 제안방식은 사용자가 네트워크를 이동하더라도 이전



(그림 6) 제안 방식 전체 흐름도

의 개인정보를 이용하여, 안전한 서비스를 제공할 수 있는 방안을 제시한다. (그림 6)은 제안 방식의 전체 흐름도로 사용자가 이용하는 디바이스 1, 2, 3와 홈 인증 서버(AAAH), 개인 정보 서버 그리고 외부 인증 서버(AAAL)로 구성된다. 사용자의 외부 네트워크 이동으로 인하여 처음 사용하게 되는 디바이스((그림 6)의 사용자 디바이스 3)와 모바일 디바이스((그림 6)의 디바이스 1과 1`(동일한 디바이스))로 분류할 수 있다. 사용자 디바이스 중심으로 설명하면, 사용자 디바이스 1과 1`는 모바일 디바이스로 홈 네트워크 및 외부 네트워크로 이동 가능하다. 이 경우 디바이스 1은 A-1, A-2와 A-4를 통해 홈 인증 서버 및 개인 정보 서버에 접근 가능하고 외부의 디바이스 1`는 B-1, B-2와 C-1을 통해 홈 인증 서버에 접근 가능하다. 디바이스 2는 홈 네트워크의 고정 디바이스가 되며, 디바이스 3는 외부 네트워크의 고정 디바이스가 된다. 이때 사용자가 외부에서 고정된 디바이스 3를 이용하는 경우 B-3와 C-1을 통해 홈 인증 서버에 접근하게 된다. 제안 방식은 다음과 같이 디바이스 등록, 인증 그리고 그룹 서비스로 총 3개 프로토콜로 이루어진다.

1) 디바이스 등록 프로토콜

사용자의 디바이스를 홈 인증 서버 및 개인 정보 서버에 등록하는 것으로써 오프라인과 온라인 과정으로 이루어진다.

2) 인증 프로토콜

사용자는 네트워크에서 홈 인증 서버의 인증을 받아 서비스를 제공받게 된다. 외부 네트워크의 경우 외부 인증 서버에 대한 인증 과정으로 외부 네트워크 정책을 따라 제공 받게 된다. 그러므로 외부 인증 서버와 홈 인증 서버의 인증 기술이 필요하다.

3) 그룹 서비스 프로토콜

인증 받은 사용자는 권한을 획득하여 서비스를 제공받게 된다. 그러므로 그룹 단위의 정책을 적용하여 사용자가 속해 있는 서비스만 제공 받을 수 있는 방안이 필요하다.

3.1 시스템 기호

본 제안 방식에서는 다음과 같은 시스템 기호를 이용하여 프로토콜을 설계한다.

- ID : 사용자 아이디
- PW : 사용자 패스워드
- $AAAH, AAAL$: AAA시스템의 인증 서버(H : 홈 네트워크, L : 외부 네트워크)
- No_D_n : 디바이스 일련 번호
- P_* : *의 공개키(* : AAAH, AAAL)
- H : 안전한 일방향 해쉬함수 (예 : SHA-1)
- $E_*[]$: []의 데이터를 *키로 암호화
- R_* : *가 생성한 랜덤 수
- || : 데이터의 연접
- No_R_s : 난수 표의 임의 번호
- Gn : 그룹 관리 번호

3.2 디바이스 등록 프로토콜

사용자 디바이스를 홈 인증 서버에 등록하는 단계로써 오프라인과 온라인을 통해서 등록한다(그림 7참조).

(1) 오프라인 과정

사용자는 오프라인으로 사용자 아이디(ID)와 패스워드(PW)를 제출하고 난수표를 발급받는다.(난수표는 R_1부터 R_n까지의 수로 n($n \geq 20$)개의 난수가 적혀 있다.)

(2) 온라인 과정

step 1. 사용자 디바이스를 온라인으로 등록하기 위해서 AP에 접근한다. AP는 모바일 디바이스에 아이피(IP)를 할당하고 인증을 받기 이전까지는 인터넷 망의 접근을 차단한다.

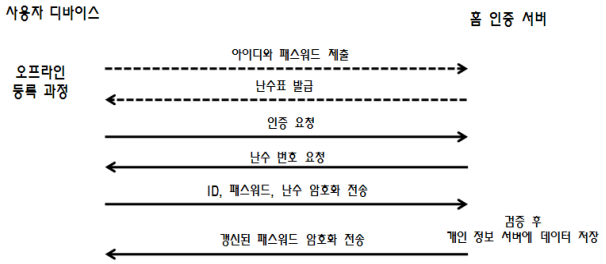
step 2. 사용자는 인증 요청을 홈 인증 서버에 전송하고, 홈 인증 서버는 난수 번호 No_R_s(s는 난수표의 난수에 해당하는 번호로 임의 번호를 서버가 선택 전송)를 요구한다.

step 3. 사용자는 홈 인증 서버가 요구한 번호(No_R_s)에 해당하는 난수를 난수표에서 찾아 패스워드와 연접하여 해쉬 값($H(PW\|R_S)$)을 구하고, 이를 사용자의 아이디 및 디바이스의 일련번호(No_D_n)와 함께 홈 인증 서버의 공개키(P_{AAAH})로 암호화($E_{P_{AAAH}}[ID\|No\_D_n\|H(PW\|R_s)]$) 하여 전송한다.

step 4. 홈 인증 서버는 아이디를 획득하여 패스워드와 난수표의 해쉬 값이 동일한지 검증한다. 동일하면 디바이스의 일련번호(No_D_n)를 사용자의 디바이스 목록에 추가하여 저장한다. 개인 정보 서버 데이터의 저장되는 필드는 다음과 같다.

사용자 아이디	초기 패스워드	갱신된 패스워드	디바이스 목록
ID	PW	$H(PW\|R_s)$	No_D_n

step 5. 홈 인증 서버는 갱신된 패스워드($H(PW\|R_s)$)를 암호화 키($K = H(PW\|R_s)$)로 디바이스의 일련번호(No_D_n)와 임의 랜덤 수(R_{AAAH})를 다음과 같이 암호화($E_K[No\_D_n\|R_{AAAH}]$)하여 사용자에게 전송한다.



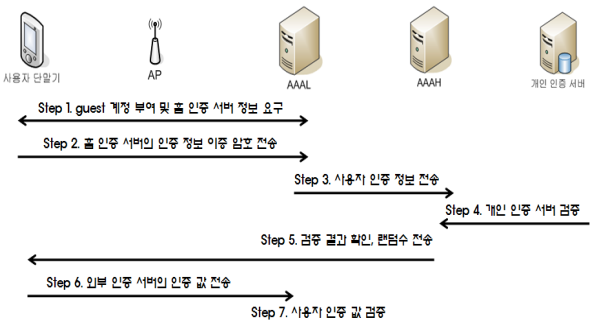
(그림 7) 등록 프로토콜 흐름도

step 6. 사용자는 복호화하여 디바이스의 일련번호(No_D_n)가 틀리면 위장 홈 인증 서버에 접근한 것으로 간주하고 다시 Step 2부터 시작하게 된다. 만약 복호화한 디바이스의 일련번호(No_D_n)가 일치하면 서버의 랜덤 수(R_{AAAH})를 암호화($E_K[R_{AAAH}]$)하여 응답 값으로 홈 인증 서버에 전송한다.

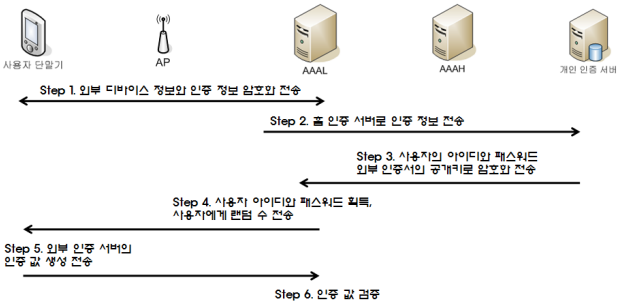
step 7. 홈 인증 서버는 사용자가 전송한 랜덤 수(R_{AAAH})가 틀린 경우 제 3자가 위장하여, 접근한 것으로 간주하고 갱신된 패스워를 삭제하고 Step 2부터 다시 시작한다. 홈 인증 서버가 사용자 인증에 성공하면 AP에 결과를 알려주고, 사용자는 인터넷 망을 사용할 수 있다.

3.3 인증 프로토콜

사용자의 인증 프로토콜은 두 가지 방식으로 나누어진다. (그림 6)에서 사용자 디바이스 1과 1`처럼 사용자가 개인 정보 서버에 등록한 디바이스를 가지고 이동하여 이용하는 경우와 사용자 디바이스 3처럼 개인 정보 서버에 등록되어 있지 않는 디바이스를 이용하는 경우이다. 두 방식 모두 외부 인증 서버를 통해서 홈 인증 서버에 접근하게 된다. (그림 8)은 등록된 사용자 디바이스 1`을 이용하는 경우의 흐름도이고 (그림 9)는 외부의 디바이스 3를 이용하는 흐름도이다.



(그림 8) 등록된 디바이스를 이용한 인증 프로토콜



(그림 9) 외부 디바이스를 이용한 인증 프로토콜

(1) 등록된 디바이스 이용 방식(사용자 디비이스 1과 1` 경우)

개인 정보 서버에 등록되어 있는 디바이스를 이용하는 경우 디바이스의 일련번호(No_D_n)가 개인 정보 서버에 공유되어 있으므로 아래의 단계와 같다(그림 8참조).

step 1. 외부 인증 서버는 접근하는 사용자 디바이스에 guest 계정을 부여하고 홈 인증 서버의 정보를 요구한다.

step 2. 사용자 디바이스는 외부 인증 서버에 홈 인증 서버에서 인증을 받을 수 있는 정보(아이디(ID), 디바이스 일련번호(No_D_n), 해쉬된 패스워드($H(PW)$))를 홈 인증 서버의 공개키(P_{AAAH})와 외부 인증 서버의 공개키(P_{AAAL})를 이용하여 이중 암호화 ($E_{P_{AAAL}}[ID \| E_{P_{AAAH}}[ID \| No\_D_n \| H(PW)]]$)하여 전송한다.

step 3. 외부 인증 서버는 사용자 아이디(ID)를 획득하고 홈 인증 서버에게 $E_{P_{AAAH}}[ID \| No_{D_n} \| H(PW)]$을 전송하여 사용자 검증을 요청한다.

step 4. 홈 인증 서버는 외부 인증 서버로부터 전송된 데이터를 복호화하여 개인 정보 서버에 등록된 정보를 통해서 검증한다. 검증이 완료되면 외부 인증 서버의 공개키로 검증된 사용자 아이디와 해쉬된 패스워드의 값을 암호화($E_{P_{AAAL}}[ID \| H(PW)]$)하여 외부 인증 서버에 전송한다.

step 5. 외부 인증 서버는 홈 인증 서버의 검증 결과를 확인하고 사용자의 아이디와 패스워드를 획득하고, 랜덤 수(R_{AAAL})를 생성해서 사용자 디바이스에 전송한다.

step 6. 사용자는 최종적으로 해쉬된 패스워드(H(PW))에 외부 인증 서버가 전송한 랜덤 수(R_{AAAL})를 연접하여 해쉬($H(H(PW) \| R_{AAAL})$)한다. 사용자는 외부 인증

서버의 공개키로 아이디와 H(H(PW)||R_{AAAL})를 암호화($E_{P_{AAAL}}[ID||H(H(PW)||R_{AAAL})]$)하여 제공한다.

step 7. 외부 인증 서버는 사용자를 아이디와 패스워드로 인증하게 된다.

(2) 외부 디바이스 이용 방식(사용자 디바이스 3의 경우)

사용자 디바이스 3는 외부 네트워크에 고정된 디바이스로 홈 인증 서버에 등록되어 있지 않다. 등록되지 않은 디바이스를 사용자가 이용하므로 (1)의 등록된 디바이스 인증 방식과는 다른 방식으로 인증을 제공하여야 한다(그림 9참조).

step 1. 사용자는 외부 디바이스 3를 이용하여 외부 인증 서버에 사용자 아이디(ID)와 사용 디바이스의 일련번호($No\_D_{n'}$) 그리고 초기 패스워드와 디바이스 일련번호를 연접하여 해쉬한 값($H(PW||No\_D_{n'})$)을 홈 인증 서버의 공개키로 암호화하여 $E_{P_{AAAH}}[ID||No\_D_{n'}||H(PW||No\_D_{n'})]$ 외부 인증 서버에 전송한다.

step 2. 외부 인증 서버는 홈 인증 서버에 step 1의 암호 데이터를 전송하고, 홈 인증 서버는 데이터를 복호화하여 개인 정보 서버의 디바이스 목록을 비교하여 존재하지 않으므로 초기 패스워드와 전송 받은 디바이스 일련번호를 해쉬하여 등록한다.

step 3. 홈 인증 서버는 외부 인증 서버의 공개키로 사용자 아이디와 해쉬된 패스워드를 암호화($E_{P_{AAAL}}[ID||H(PW||No\_D_{n'})]$)하여 외부 인증 서버에게 전송한다.

step 4. 외부 인증 서버는 사용자의 아이디와 해쉬된 패스워드를 획득하고 사용자에게 랜덤수(R_{AAAL})를 전송한다.

step 5. 사용자는 외부 인증 서버의 랜덤수(R_{AAAL})를 이전 생성된 패스워드에 연접하여 해쉬하고 외부 인증 서버의 공개키로 암호화($E_{P_{AAAL}}[ID||H(H(PW||No\_D_{n'})||R_{AAAL})]$)하여 전송한다.

step 6. 외부 인증 서버는 사용자의 아이디와 패스워드를 검증한다.

3.4 그룹 서비스 프로토콜

그룹 서비스는 사용자의 인증 이후에 서비스를 받을 수 있는 그룹으로 구별하여 제공하는 것으로 그룹의 구별 방법으로는 디바이스의 일련번호를 이용한다. 그룹키의 경우 사용자가 그룹의 키를 분배 받아 그룹 멤버간에 안전하게 통신하는 방법이 된다. 그룹키는 사용자의 패스워드와 디바이스 일련번호를 이용하여 생성하고 대칭키로 이용한다. 사용자의 인증을 통해 홈 인증 서버와 외부 인증 서버는 사용자의 디바이스 일련번호와 패스워드를 획득하였다. 그러므로 그룹키를 생성하는데 문제가 발생하지 않으며, 본 방식은 홈 인증 서버의 서비스를 받는 방안으로 제시한다. 각각의 사용자(i=1, 2, ..., n)에 대하여 PW는 PW_i로 디바이스의 일련 번호 No_D_n은 No_D_{ni}로 표시한다.

step 1. 홈 인증 서버는 동일한 서비스를 제공 받는 그룹 인원으로 구성한다. 구성된 인원들의 개인 정보 서버에서 디바이스의 일련번호와 패스워드를 획득하여 해쉬값($x_i = H(PW_i||No\_D_{ni})(i=1,...,n)$)과 홈 인증 서버의 그룹 관리 번호(Gn_AAAH)로 그룹키 $K(K = g^{x_1 x_2 x_3 \cdots x_n G_{nAAAH}} \bmod n)$를 생성한다.

step 2. 홈 인증 서버는 그룹키(K) 전송에서 전송 받을 사용자(i)의 x_i를 제거하여 $K'(K' = g^{x_1 x_2 x_3 \cdots x_{n-1} G_{nAAAH}} \bmod n)$ 전송한다.

step 3. 사용자(i)는 x_i가 제거되어 있는 키(K′)를 전송받은 후 x_i를 생성하여 동일한 그룹키$K(K = (K')^{x_i \bmod n})$를 생성할 수 있다.

step 4. 사용자는 홈 인증 서버에게 사용자 아이디와 서비스 리스트(S_{list})를 그룹키로 암호화($E_k[ID, S_{list}]$)하여 전송한다.

step 5. 홈 인증 서버는 그룹키로 복호화 하여 사용자의 아이디와 서비스 리스트를 확인하고 서비스를 제공한다.

이와 동일하게 외부 인증 서버에서도 그룹 서비스를 제공할 수 있다. 위의 단계에 사용되는 그룹키 인자로 외부 인증 서버가 검증한 패스워드와 디바이스 일련번호를 이용하면 동일한 그룹 서비스를 제공할 수 있게 된다.

4. 제안 방식 분석

제안 방식은 사용자의 인증과 그룹 서비스에 대한 취약점 분석으로, 다음과 같이 안전성을 제공할 수 있다.

- 사용자 인증 : 사용자의 인증에 있어 사용하는 패스워드는 OTP 개념과 응답 방식의 두 가지의 방안을 포

함하고 있다. OTP 개념으로 한번 사용한 패스워드는 갱신되어 재사용 되지 않으며, 응답 방식으로 홈 인증 서버의 난수 선택 번호에 대하여 올바른 응답을 하여야 한다. 그로 인해 패스워드 재전송 공격이 불가능하고, 제 3자의 위장이 어렵다. 또한 외부 인증 서버에서 처음 사용하는 디바이스를 이용하는 경우 초기 패스워드가 사용되지만 외부 인증 서버의 랜덤 수에 응답하여야 하기 때문에 재전송 및 위장을 막을 수 있다. 그리고 제 3자의 부정한 접근에 대하여는 초기 패스워드를 알아야 하는 어려운 점이 있다. 초기 패스워드를 사용하는 경우 해쉬 값을 이용하여 패스워드의 노출을 막고 있으며, 암호화된 데이터에서 값을 획득하기 위해서는 홈 인증 서버의 개인키를 알아야 하는 어려움이 존재한다.

- 그룹 서비스 : 제 3자의 불법적인 접근에 의한 서비스는 우선 그룹키를 생성할 수 없으므로 안전하며, 외부 인증 서버의 경우 디바이스의 일련번호를 알 수 있어도 패스워드의 구성에서 초기 패스워드와 랜덤수를 모두 알아야 하는 어려움이 존재한다. 또한 사용자가 로그아웃을 하였을 경우 사용자의 패스워드 갱신으로 인해 그룹키의 갱신이 이루어지므로 이후의 서비스 내용에 접근할 수 없으며, 이전의 내용에 대한 접근도 키 갱신을 통해서 접근하기 어려움 점을 가지고 있다.

<표 1>에서 제안 방식에 대한 내용을 분석하여 제공하고 있다.

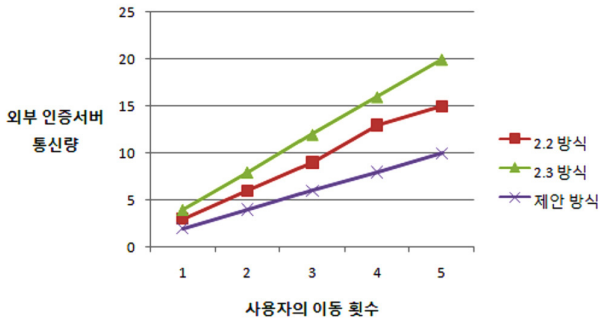
<표 2>에서 개인 정보 이동으로 외부 네트워크에서 서비스를 이용할 수 있으며, 키 교환을 제공한다. 또한 무선 통신의 보안 기술 통합으로 이기종간의 디바이스 및 컨버전스 기술을 이용하는 경우 제안 방식의 기술을 적용함으로 안전하게 서비스를 제공할 수 있게 된다. 특히 개인 정보의 이동을 제공하므로 다양한 디바이스

〈표 1〉 제안 방식 분석표

내용	암호 기술	제공 사항
제안 방식의 사용자 인증	패스워드방식 (OTP + 응답 방식)	• 재전송 및 위장에 대하여 대응
	공개키 방식	• 데이터의 안전성 제공, 외부 네트워크의 접근 서비스 제공
	대칭키 암호 방식	• 상호 인증을 통한 키 갱신을 제공
제안 방식의 그룹 서비스	대칭키 방식	• 데이터의 암/복호화에 빠름 • 키 갱신을 통한 서비스 제한 가능 • 외부 네트워크 서비스에 변경 없이 적용 가능

〈표 2〉 제안 방식과 기존 방식의 비교

내용	2.3 방식	2.2 방식	제안 방식
키 교환	○ (패스워드기반)	X (제공 못함)	**○ (패스워드)**
사용자 인증	○ (패스워드 및 랜덤 수)	○ (AEM 방식)	**○ (패스워드 및 디바이스 일련번호)**
이동성 제공	X (제공 못함)	○ (AP간 통신)	**○ (외부 인증 서버 활용)**
개인정보 이동	X (제공 못함)	X (제공 못함)	**○ (개인 정보 서버 이용)**
외부 서비스 제공	X (제공 못함)	○ (AEM 방식)	**○ (외부 인증서버에 인증 데이터 제공)**
오버 헤드	낮음 (접근하는 디바이스만 연산 제공)	높음 (모든 디바이스의 AEM을 유지)	**낮음 (접근하는 디바이스만 연산 제공)**



(그림 10) 외부 인증서 서버의 통신량 비교

를 이용하더라도 동일한 안전성을 제공할 수 있는 장점을 제공할 수 있다. 이동성에 따른 메시지의 양을 보면 홈 인증 서버의 요청이 기존 방식에 비하여 낮은 것을 알 수 있으며, 외부 인증 서버를 통한 인증으로 빠른 보안 서비스를 제공할 수 있다.(그림 10참조)

5. 결 론

본 논문은 사용자의 이동에 따라 개인 정보 서버를 이용한 로밍으로 외부 인증 서버 및 홈 인증 서버의 인증과 그룹 서비스에 대하여 제시하였다. 인증 방식에서는 OTP개념과 응답 방식으로 패스워드를 갱신하는 방안으로 재전송 및 위장을 막을 수 있게 되었다. 또한 외부 인증 서버와 연계하여 사용자의 패스워드를 활용하고 외부 네트워크에서 사용할 수 있는 패스워드 분배에 대하여 제시하였다. 그룹 서비스의 경우 패스워드와

디바이스의 일련번호를 이용함으로써 불법적인 디바이스의 접근과 제 3자의 접근에 대해 보안을 제공하였다. 디바이스의 목록을 이용하는 방안은 향후 다양한 디바이스를 이용하는 사용자의 방안으로 제시 될 수 있다. 그러나 제안 방식의 경우 사용자의 로그인과 로그아웃으로 인한 빈번한 키 갱신의 문제점이 내포되어 있는 상태이다. 그러므로 향후 연구 방향에서는 키 갱신의 문제점을 해결할 수 있는 방안이 포함된 연구가 진행되어야 한다. 본 제안 방식은 유비쿼터스 환경에서 모바일 디바이스에 대한 사용자 인증 기술을 제시하여 보안을 강화하는 방법으로 활용 될 수 있다.

참 고 문 헌

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

[2] Salekul Islam and J.william Atwood, "A Framework to Add AAA Functionalities in IP Multicast", AICT/ICIW 2006.

[3] Jung-Min Park, Eun-Hui Bae, Hye-Jin Pyeon, Kijoon Chae, "A Ticket-Based AAA Security Mechanism in Mobile IP Network," ICCSA2003, pp.210-219.

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

[5] 이효성, 김기천, 김인수 "Mobile 환경에서의 AAA 지역 등록 인증 개선 방안", 한국정보처리학회 2004년 추계학술대회, pp.1267-1270, 2004.

[6] 진봉재, 허의남, 문영성, "IEEE802.11 무선랜 기반의 Mobile IPv6 AAA환경에서 핸드오버 최적화 방안 연구", 한국정보처리학회 2004년 추계학술대회, pp.1201-1204, 2004.

[7] RFC 2905, "AAA Authorization Application Examples"

[8] RFC 2904, "AAA Authorization Framework".

[9] RFC 3157, "Securely Available Credentials - Requirements".

[10] RFC 3760, "Securely Available Credentials(SACRED)-Credential Server Framework".

[11] RFC 2945, "The SRP Authentication and Key Exchange System".

[12] ITU-T, SG17, "SPARK:Secure Password-based authentication protocol with key exchange".

[13] RFC 2865, "Remote Authentication dial In User Service (RADIUS)".

강 서 일

e-mail : kop98@sch.ac.kr

2003년 2월 순천향대학교 정보기술공학부 (학사)

2005년 2월 순천향대학교 전산학과(석사)

2005년 3월~현 재 순천향대학교 전산학과 박사과정

관심분야 : 무선 네트워크 보안, 전자 투표, 전자 화폐

박 춘 식

e-mail : csp@ensec.re.kr

1981년 광운대학교 졸업

1983년 한양대학교 전자통신전공(석사)

1995년 일본동경공업대학 정보보호전공(박사)

1982년~1999년 한국전자통신연구원 부장

2000년~현 재 한국전자통신연구원 부설연구소 책임연구원

관심분야 : 암호이론, 정보이론, 네트워크보안

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과

1986년 오사카대학 통신공학전공(석사)

1989년 오사카대학 통신공학전공(박사)

1989년~1994년 한국전자통신연구원 선임연구원

1994년~현 재 순천향대학교 컴퓨터 학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안