AAA시스템에서의 이동에 따른 PIN 기반의 인증 및 ID 등록에 관한 연구

강 서 일[†] · 이 임 영[††]

요 약

AAA(Authentication, Authorization, Accounting)는 인증, 인가 그리고 과금을 제공하는 것으로써 서비스를 이용하는 모바일 단말기는 AAA가 필요하다. 모바일 단말기 인증 과정은 외부 네트워크의 인증 서버를 통해 홈 네트워크의 인증 서버에 접근하여 인증 결과를 외부 인증 서버가 통보 받는다. 이후 홈 인증 서버는 안전한 서비스를 제공하기 위하여 외부 에이전트, 사용자 그리고 홈 인증 서버간의 안전한 통신을 위한 사용될 키가 분배된다. 본 논문은 모바일 단말기가 외부 네트워크의 이동시 외부 인증 서버간의 안전한 통신을 위한 키 분배에 대하여 논의하고 제안한다. 제안한 방식은 외부 인증 서버간의 이동시에 홈 인증 서버로부터 인증을 재발급 받지 않으므로 홈 인증 서버의 과부화를 줄일 수 있고, PIN 기반을 이용하여 키를 분배한다.

키워드 : AAA, 인증, 패스워드, ID등록, PIN

A Study on PIN-based Authentication and ID Registration by Transfer in AAA System

Seo-Il Kang[†] · Im-Yeong Lee[††]

ABSTRACT

AAA(Authentication, Authorization, Accounting) is the service that offers authentication, authorization, and accounting method, and every terminal that accesses the network requires this AAA service. The authentication process of a mobile terminal is as follows: a mobile phone accesses an authentication server in a home network via the authentication service in an external network, which receives the authentication result. And, for the home authentication server to offer secure service, a unique key is distributed for the secure communication between the external agent and the user, the external agent and the home authentication server, and the user and the home authentication server. This paper discusses and proposes the key distribution for secure communication among external authentication servers when a mobile terminal travels to an external network. As the proposed method does not require the home authentication server to reissue another authentication when a user travels to other external networks, it reduces the overload in the home authentication server. It can also distribute a PIN-driven key.

Key Words : AAA, Authentication, Password, ID Registration, PIN(Personal Identity Number)

1. 서 론

IT의 발달로 인해 많은 서비스가 현재 네트워크를 통해서 제공되고 있다. 다양한 서비스를 제공받기 위해서 이용자들은 자신의 정보를 서비스 서버에 등록하고 사용 금액을 지불하며 서비스를 이용한다. 이와 같은 과정에서 서비스 서버는 정당한 사용자라는 것을 확인할 수 있는 인증 과정, 인증을 통해서 자원이나 서비스를 이용할 수 있는 권한, 즉 인가를 제공한다[7, 9-11]. AAA는 인증, 인가 및 과금의 앞글자를 모은 것으로 Authentication, Authorization, Accounting이 된다. AAA에서 인증은 기존의 기술을 이용하는 것으로 아이디 패스워드부터 시작하여 원 타임 패스워드, 생체 정보 등 을 활용할 수 있다. 인가의 경우 5개의 모델을 기본적으로 정의하고 있으며, 로밍이 포함되어 있다. 로밍은 모바일 단말기에 적용되는 기술로써 어느 장소로 이동하더라도 서비스를 제공 받을 수 있게 된다. 기본적인 모델에서는 각각의 인증 및 서비스를 제공 받기 위해 홈 인증 서버에 접근하여 인증과정을 통해 인증된 결과 메시지를 받아야 한다. 이와 같은 과정은 홈 네트워크의 인증 서버에 오버헤드가 크며, 모바일 단말기의 이동으로 인해 효율성을 제공하

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성 지원 사업의 연구 결과로 수행되었음.
† 준 회 원 : 순천향대학교 전산학과 박사과정
†† 종신회원 : 순천향대학교 컴퓨터학부 교수(교신저자)
논문접수 : 2005년 11월 21일, 심사완료 : 2006년 5월 2일

지 못한다. 그러므로 본 논문에서는 모바일 단말기의 이동에 따른 인증 서비스를 외부 인증 서버에서 제공하여 효율적인 인증을 받을 수 있도록 하는 동시에 외부 인증 서버와 안전한 통신을 할 수 있도록 키를 생성한다. 기존의 키 분배 및 생성에서는 IKE(Internet Key Exchange)방식을 이용하여 홈 네트워크의 인증 서버가 모든 암호화 키를 생성하여 분배하므로 외부 인증 서버와 모바일 단말기 통신에는 안전한 키 분배가 없다[12]. 제안 방식은 외부 인증 서버와 모바일 단말기가 안전한 통신 채널을 설립하여 키를 공유하게 한다. 2장에서는 보안 요구 사항에 대하여 제시하고 3장에서는 기존의 연구에 대하여 알아보며, 4장에서는 제안 방식에 대하여 서술한다. 5장에서는 보안 요구 사항에 따라 제안 방식을 분석하고 마지막으로 6장에서는 결론 및 향후 연구 방향에 대하여 서술한다.

2. 보안 요구 사항

AAA에서 가장 중요한 것은 인증 서비스이며, 인증의 경우 정당한 사용자를 확인할 수 있는 과정으로 인가와 과금을 적용할 수 있는 기초가 된다. 인가는 인증을 통해서 부여 받은 권한을 주는 것으로 자원 접근에 대한 권한이나 서비스의 이용 등을 말하는 것이다. 인증을 제공하기 위해서 AAA에서는 다양한 인증 프로토콜을 적용한다. 이때 AAA의 표준 문서에서는 패스워드부터 시작하여 OTP(One Time Password)까지 다양한 기술을 적용할 수 있다고 기술되어 있다. 또한 홈 인증 서버에 등록되어 있는 아이디와 패스워드를 매칭하기 위해 안전하게 메시지를 전송하는 방안도 보안 사항에 포함이 되어야 한다. 왜냐하면 사용자가 이용하는 모바일 단말기는 다른 외부 네트워크를 통해서 인증을 받을 경우, 외부의 공개되어 있는 네트워크망에서 안전하게 데이터가 전송되어야 하기 때문이다. 그러므로 사용자와 인증 서버가 공유한 대칭키를 가지고 암호화 방식이나 AP와의 통신 보안 기술로 WEP 혹은 802.11i의 기술을 적용한다[15]. 이후의 통신이나 서비스를 위한 키 분배는 홈 인증 서버가 중심이 되어 외부의 네트워크에서 사용할 수 있는 암호화 키를 생성하여 제공하며, 모바일 단말기 사용자는 인증 서버로부터 전송받는 키 생성 인자를 통해서 외부 네트워크에서 이용할 수 있는 키를 생성할 수 있게 된다. 이와 같은 과정은 다음과 같은 보안 사항을 요구한다.

- 정당한 개체만이 메시지를 확인 할 수 있어야 한다.
- 전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며, 만약 위조, 삭제 및 변조가 된다면 그 사실을 알 수 있어야 한다.
- 정당한 사용자는 정당한 서버에 대해 자신이 정당한 사용자라는 것을 즉시 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.
- 사용자는 외부 네트워크에서의 사용되는 암호 키가 동일하다는 것을 검증할 수 있어야 한다.

위의 보안 요구 사항은 제 3자가 정당한 사용자로 위장하는 것과 메시지의 트래픽 분석을 통해 정보를 획득하는 것을 막을 수 있어야 한다는 것이다. 또한 안전한 통신을 위해 키를 분배하며, 인증을 받은 사용자에 대해서는 서비스를 이용할 수 있는 권한을 부여하여야 한다. 키를 분배한 경우 통신의 객체들은 동일한 키를 이용하고 있다는 것을 검증할 수 있는 과정이 필요하다. 그러므로 본 제안 방식에 있어 위의 보안사항을 중심으로 하여 논의 한다.

3. 기존 연구

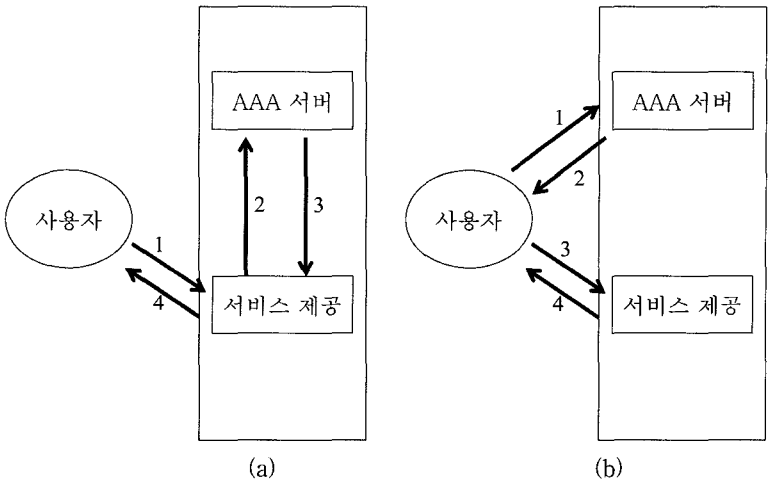
AAA에 대한 기존 연구를 알아보고 인증에 제공되는 보안 기술과 외부 네트워크를 활용하는 로밍 방식 그리고 기존의 모바일 단말기에 AAA를 이용하여 인증을 효율적으로 제공하는 방안에 대하여 언급한다[4, 5, 10].

3.1 인증 기술

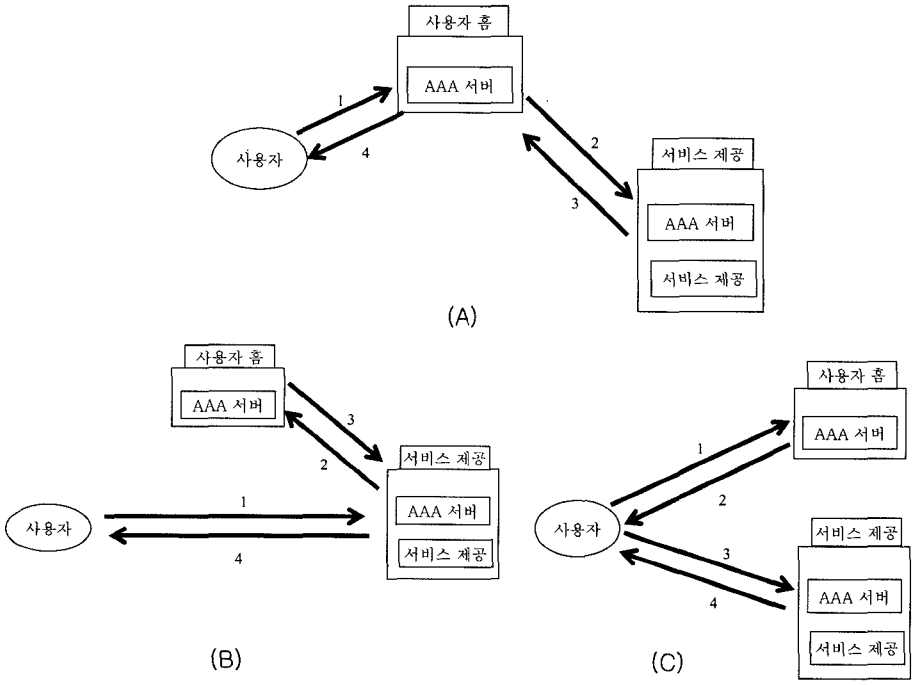
인증 기술로 가장 많이 활용되는 기술은 아이디와 패스워드 방식이다. 패스워드의 경우 기존에 제 3자의 예측이나 짧은 길이 그리고 사전 공격에 취약할 수 있다. 하지만 서비스를 제공하는 업체에서 많이 활용하는 방안이며, 현재의 서비스를 제공하는 사이트들은 위와 같은 공격에 대응하기 위하여 8자 이상의 길이와 숫자, 영문자 조합을 요구하거나 유추하기 쉬운 휴대폰 번호, 생일 등은 등록하지 못하도록 한다. 또한 패스워드를 평문으로 데이터베이스에 저장하는 것이 아니고 해쉬 함수를 적용하여 저장함으로 내부의 관리자까지도 알 수 없도록 하고 있다. 다른 기술로는 원 타임 패드 및 생체기술을 활용할 수 있다. 생체 인식 기술의 경우 현재는 아직 활용이 널리 사용되고 있지 않지만, 사용자의 유일한 정보가 될 수 있는 방안으로 제시되고 있으며, 이와 같은 경우 사용자가 직접 지니고 있으므로 확실한 인증 방안이 될 수 있다. 하지만 생체의 정보를 데이터베이스에 저장하는 과정과 생체 인식용 단말기기가 널리 보급되지 못한 점이 단점으로 작용하고 있다. 원 타임패드는 원 타임 패드 생성기와 서버의 동기화 문제를 해결하는 방안이 급선무이다.

3.2 AAA시스템의 인가 방식

AAA의 인가 방식은 다음의 (그림 1, 2)에서 전체의 흐름을 보여주고 있다[9, 10]. (그림 1)은 홈 네트워크 안에서 홈 인증 서버를 통해 서비스를 제공 받는 것으로 (그림 1)의 A는 사용자가 서비스를 요청하고 서비스 제공 업자는 AAA 인증 서버에 인증을 요청하여 사용자의 인증을 받고나서, 서비스를 제공한다. (그림 1)의 B는 다른 방법으로 AAA의 인증 서버에서 인증을 받고 서비스를 이용할 수 있는 인가 메시지를 서비스 업체에 제공하여 서비스를 받는다. (그림 2)는 홈 인증 서버를 이용한 로밍 서비스로 홈 인증 서버와



(그림 1) 홈네트워크 인증 서버를 통한 서비스 제공



(그림 2) 홈 인증 서버를 이용한 로밍 서비스

외부 인증 서버 두 개로 구성되어져 있다. (그림 2)의 A는 홈 인증 서버를 통해 외부 인증 서버에 접근하여 서비스를 제공받는 방식이고 (그림 2)의 B는 사용자가 외부 인증 서버에 접근하였다가 홈 인증 서버로 이동하여 인증 결과 메시지에 따라 서비스를 제공한다. (그림 2)의 C는 홈 인증 서버로부터 인증 메시지를 받고 그 인증 메시지를 가지고 외부 서비스에 접근하는 방식이다.

3.3 무선 랜에서 안전한 인증 모델 방식

무선 랜에서의 보안을 제공하는 방식으로 WEP(Wired Equivalent Privacy), SSID (Service Set IDentifier)가 있다 [1, 16]. 그러나 모바일 단말기와 AP(Access Point)사이에서 제 3자가 중간자 공격을 할 수 있으며, 공유키 취약성 및 WEP의 XOR연산 데이터를 트래픽분석하여 공격가능하다. 이와 같은 취약점을 극복하기 위해 AAA의 기술을 적용한 RADIUS(Remote Authentication Dial In User Service)를 이용하는 방식을 제시하고 있으나 사용자에 따른 키 증가와 기존의 신뢰되어 있는 망을 활용하여야 한다. 공개된 네트워크망을 이용하기 위해서는 RADIUS에서 TLS(Transport Layer Security)를 적용해야 한다[7, 13, 14]. 그러므로 메시지교환이 증가하고 MAC(Media Access Control)어드레스를 이용한 공격과 인증서를 이용하는 경우 인증 서버와의 통신도 포함해야하는 단점을 가지고 있다. 그래서 단말기에서 사용자를 인증할 수 있는 방안으로 USIM(Universal Subscriber Identity Module)을 이용하고 홈 인증 서버와 모바일 단말기 사이에 중계서버를 두어 모바일 단말기가 인증을 제공받을

수 있게 제안되어 져 있다. 또한 DIAMETER방식을 이용하여 단대단 보안 및 TCP연결을 지원하고 있다[11]. 그러므로 RADIUS보다는 안전한 통신을 제공할 수 있는 방안이 되며, 로밍서비스를 제공할 수 있는 방법이 된다. 그러나 USIM의 경우 모바일 단말기에서 사용자를 인증할 수 있는 방안이며, 인증 서버와 중계서버간의 통신은 초기에 한번만 통신하므로 모바일 단말기와 홈 인증 서버간의 동기화가 문제 될 수 있다.

3.4 Mobile 환경에서의 AAA지역 등록 인증 방식

이 방식은 모바일 IP환경의 AAA구조에서 모바일 단말기의 이동으로 인한 핸드오프와 모바일 단말기 인증 처리과정을 간소화하는 방안을 제시하였다[6]. 모바일 단말기는 지역 이동시 홈 망의 AAA서버로부터 재 인증을 받아야 하며 인증에 필요한 새로운 세션키를 생성하거나 전송받아야하는 취약성을 해결하고자 하였다. 이를 위한 해결방안은 AAA구조에서 인증 절차를 처리 해줄 수 있는 AEM(Authentication Extension Message)를 제시하였다. 이 메시지의 구성은 초기 인증 서버로부터 인증할 수 있는 검증값과 알고리즘을 포함하고 있다. 이와 같은 메시지를 제공함으로 인해 중간의 외부 에이전트를 설정할 필요성이 없는 장점이 있다. 이 방식에서는 홈 인증 서버 등록시에 AEM인증 확장 메시지를 모바일 단말기에 전송하고 난 이후에 모바일 단말기는 해쉬 값과 알고리즘을 이용하여 인증을 제공하며, 빠른 핸드오프를 지원한다. 이 방식은 모바일 단말기가 외부의 인증 서버에 자신의 인증을 알려주는 것으로 홈 인증 서버에는 접근을 하지 않는다. 하지만 이렇게 되는 경우 AEM 메시지를 가지고 있는 모바일 단말기가 초기 인증을 요구하지 않아도 모든 지역의 외부 인증 서버는 AEM에 응답할 수 있는 메시지를 가지고 있어야 한다. 외부 인증서버에서 인증 절차는 간단히 이루어지지만 각각의 AEM메시지를 유지하는 것은 많은 오버헤드를 필요로 하고 어느 외부 인증 서버에 접근할지 모르는 상태에서는 모든 외부 인증 서버와 홈 인증 서버가 적어도 한번 이상의 통신을 해야 한다.

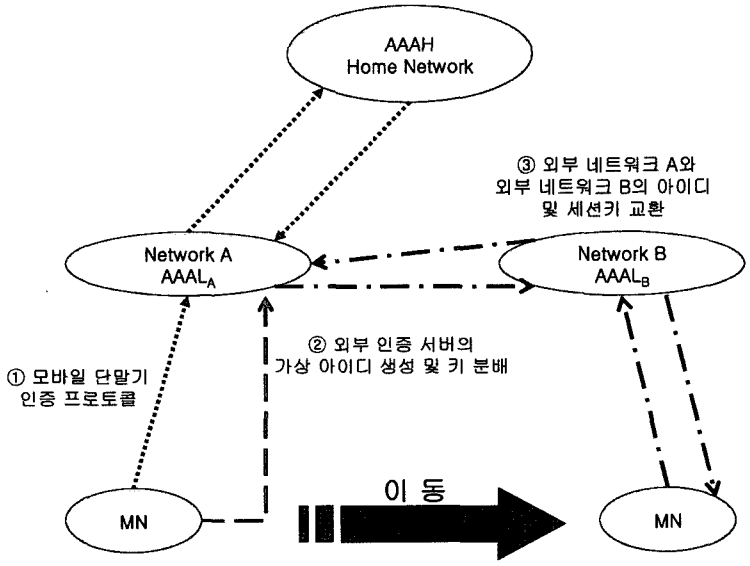
4. 제안 방식

제안 방식은 모바일 단말기를 사용하는 사용자가 외부 네트워크를 통해서 홈 인증 서버에 접근하여 인증을 받은 후에 인증 메시지를 외부 네트워크의 인증 서버에 저장한다. 이후 모바일 단말기가 또 다른 외부 네트워크의 인증 서버에 접근했을 때 가까이에 존재하고 있는 외부 인증 서버가 인증한 정보를 제공하여 홈 네트워크의 오버헤드를 줄인다. 또한 외부 인증 서버를 통해서 인증 정보를 제공하므로 모바일 단말기는 안전한 통신을 위하여 외부 인증 서버와 안전한 키 공유를 제시한다. 제안 방식의 (그림 3)을 참고적으로 보면 모바일 단말기가 외부 네트워크 A에 접근하여 홈 네트워크의 인증 서버로부터 인증을 받고 나서 모바일 단말기와 외부 인증 서버는 가상 아이디 생성 및 키 분배를 한다. 이후 또 다른 외부 네트워크 B로 접근하면 인증 메시지를 외부 네트워크 A의 외부 인증 서버로 인증을 받아온다. 그러므로 홈 네트워크의 홈 인증 서버를 찾아 가서 인증을 받아올 필요성이 없으므로 홈 네트워크에 등록되어 있는 모바일 단말기의 인증의 오버헤드를 줄일 수 있다.

4.1 시스템 계수

본 제안 방식에서는 다음과 같은 시스템 계수를 이용한다.

- MN : 모바일 단말기
- $AAAL_A$, $AAAL_B$: 외부 인증 서버 A, B
- AAAH : 홈 인증 서버
- KS : 모바일 노드와 홈 인증 서버과 비밀리에 공유한 대칭키



(그림 3) 제안 방식의 전체 흐름도

- R* : 의사 난수 발생기에서 생성한 랜덤 수(* : 모바일 단말기(MN), 홈 인증 서버(AAAH), 외부 네트워크(AAAL))
- ID_{MNi} : 외부 인증 서버에서 이용하는 가상 아이디(i(1, ..., n)는 가상 아이디의 번호)
- P_* : *의 공개키로 인증 서버의 공개키
- S_* : *의 개인키로 인증 서버의 개인키
- h( ) : 안전한 일방향 함수
- PIN : 개인 식별 코드로 사용자가 등록한 패스워드
- S_i : i(1, ..., n)에 해당하는 값으로 홈 인증 서버와 모바일 단말기에 사전 분배
- Sig* : *에 해당하는 객체의 서명
- E*[] : *의 키로 메시지를 암호화
- g : 대칭키와 공개키의 연산에 이용되는 밑수
- n : 모듈러 연산에서의 법의 수
- x_* : *에 해당되는 키의 지수

4.2 제안 프로토콜

제안 프로토콜은 총 3부분으로 구성되어 있다. 첫 번째 모바일 단말기 인증으로 홈 인증 서버가 모바일 단말기를 인증한 메시지를 외부 인증 서버에 제공한다. 두 번째는 외부 인증 서버와 모바일 단말기 사이에서 가상 아이디와 키 분배를 제공한다. 마지막으로는 모바일 단말기가 외부 네트워크 A에서 B로 이동함에 따라 외부 인증 서버($AAAL_A$, $AAAL_B$)끼리 인증을 제공하는 방안이다.

4.2.1 모바일 단말기 인증

홈 인증 서버와 모바일 단말기는 사전에 ID_{MN}, PIN, S_i를 저장하였으며, 대칭키(KS)를 공유하고 있다. 모바일 단말기의 사용자는 외부 네트워크를 통해서 홈 인증 서버에 접근을 한다.

[Step 1] 모바일 단말기 사용자는 외부 인증 서버에 자신의 아이디(ID_{MN})와 홈 인증 서버와 공유하고 있는 대칭키로 암호화한 인증 메시지를 외부 인증 서버에 전송한다.

$$ID_{MN}, E_{KS}[h(ID_{MN}\|S_i),i]$$

여기서 인증 메시지는 재 전송공격에 취약해서는 안 된다. 재 전송공격은 도청한 메시지를 다시 전송하여 이득을 얻는 행위로써 위 인증 메시지는 재 전송공격에 강하다. 그 이유는 사용자가 임의 S_i를 선택하여 PIN과 연접하고 해쉬를 하여 전송한다. 매번 사용자가 선택하는 S_i가 변하고 이미 사용된 S_i는 홈 인증 서버에서 알고 있기 때문에 재사용은 불가능하다.

[Step 2] 외부 네트워크의 인증 서버는 접근한 모바일 단말기에 대한 등록 정보를 가지고 있지 않으므로 모바일 단말기를 인증하지 못한다. 그러므로 홈 네트워크의 홈 인증 서버에 메시지를 전송한다. 이때 외부 인증 서버가 정당한 서버라는 것을 증명하기 위해 서명을 이용한다. 다음과 같이 홈 인증 서버의 공개키로 모바일 단말기에서 받은 메시지와 외부 인증 서버가 선택한 랜덤수(R_{AAAL_A}) 암호화하고, 외부 인증 서버의 개인키로 자신의 아이디(ID_{AAAL_A})와 랜덤수 해쉬값을 서명하여 제공한다.

$$E_{P_{AAAH}}[ID_{MN}, K_S[h(ID_{MN}\|S_i),i], R_{AAAL_A}]$$
$$Sig_{S_{AAAL_A}}[ID_{AAAL_A}, h(R_{AAAL_A})]$$

홈 인증 서버가 정당한 외부 인증 서버라는 것을 검증하는 것은 암호화 메시지를 복호화하여 획득한 랜덤수(R_{AAAL_A})가 외부 인증 서버의 서명으로 제공받은 해쉬값과 동일한지를 검증하는 것이다.

[Step 3] 홈 인증 서버는 외부 네트워크의 인증 서버로부터 전송받은 메시지의 서명을 확인하고 개인키로 복호화하여 모바일 아이디를 확인하여 공유하고 있는 대칭키로 암호화된 메시지를 복호화하여 S_i의 값을 찾아 PIN과 연접하여 해쉬값을 검증한다. 또한 외부 인증 서버의 랜덤값을 검증한다.

$$h(ID_{MN}\|S_i) \stackrel{?}{=} h(ID_{MN}\|S_i)'$$
$$h(R_{AAAL_A}) \stackrel{?}{=} h(R_{AAAL_A})'$$

위 과정이 완료되면, 다음 과정인 모바일 단말기와 외부 인증 서버 사이에서 사용할 가상 아이디 생성 및 키 분배 과정을 시작한다.

4.2.2 외부 인증 서버의 가상 아이디 생성 및 키 분배

홈 인증 서버에서 인증이 이루어진 이후 외부 인증 서버에서 사용될 가상 아이디(ID_{MN2})와 키를 분배하는 과정으로 모바일 단말기 인증 프로토콜에서 전송되는 외부 인증 서버의 랜덤수(R_{AAAL_A})를 이용하게 된다.

[Step 1] 홈 인증 서버는 본 아이디(ID_{MN})와 외부 인증 서버의 랜덤수(R_{AAAL_A})를 XOR연산하여 가상 아이디(ID_{MN2})를 생성한다. 그리고 외부 인증 서버와 모바일 단말기가 안전한 통신을 할 수 있게 키를 생성하는 인자(α)를 각각 제공한다.

$$ID_{MN_2} = ID_{MN} \oplus R_{AAAL_A}$$
사용자에게 전송하는 메시지 : $E_{KS}[\alpha, ID_{MN_2}]$
외부 인증서버에 전송하는 메시지 :
$$E_{P_{AAAL_A}}[Sig_{S_{AAAH}}(ID_{AAAH}, h(R_{AAAL_A})), g^{\alpha}(\mathrm{mod}n)]$$

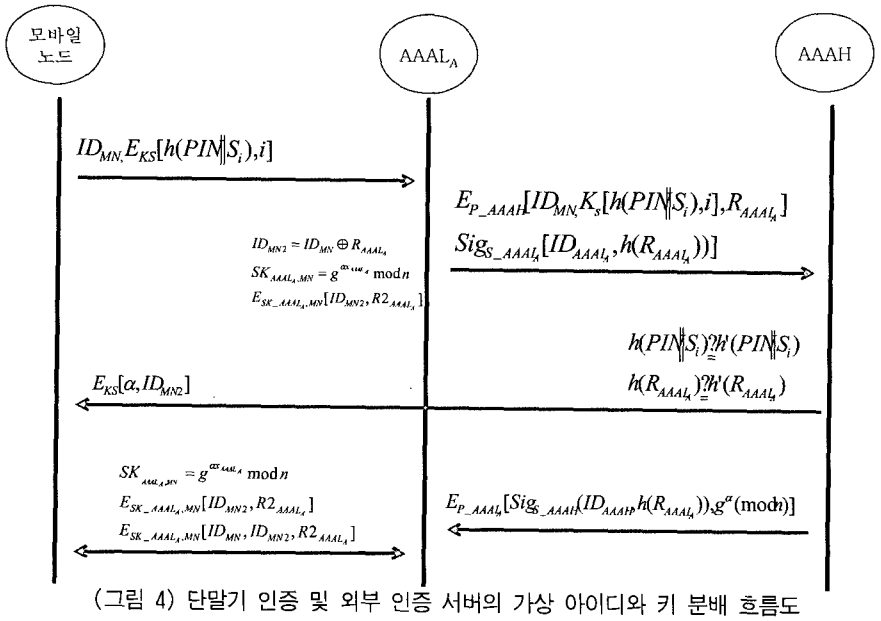
모바일 단말기 사용자에게 전송되는 메시지는 정당한 모

바일 단말기 사용자만이 풀 수 있게 공유한 대칭키(KS)로 암호화 되어 있으며, 외부 인증 서버에 전송하는 것은 외부 인증 서버의 공개키로 암호화 되어 있다. 이때 외부 인증 서버가 제공한 랜덤수의 해쉬값($h(R_{AAAL_A})$)과 홈 인증 서버의 아이디(ID_{AAAH})를 서명하여 제공하므로 정당한 홈 인증 서버라는 것을 증명한다.

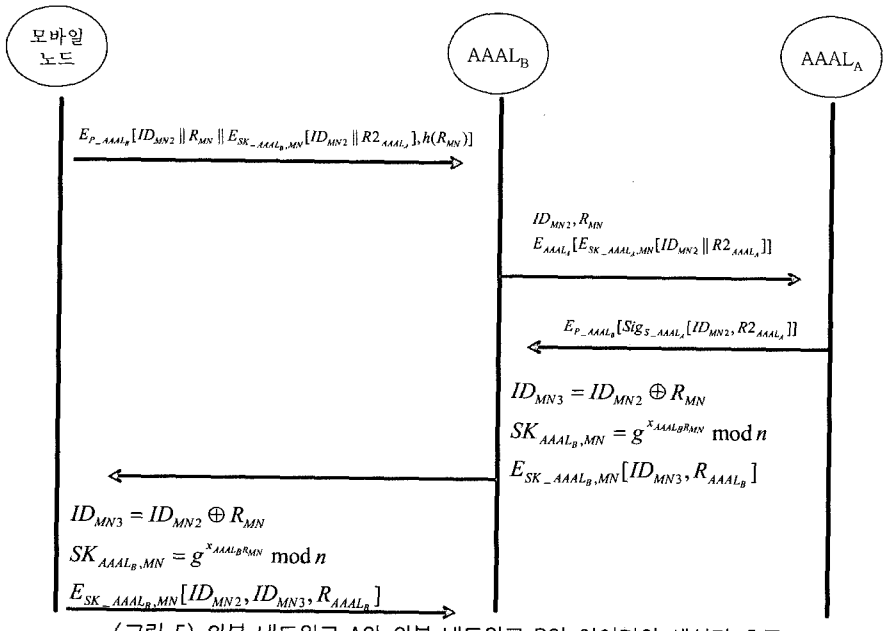
[Step 2] 외부 인증 서버는 초기 전송된 메시지에서 모바일 단말기의 아이디(ID_{MN})를 알 수 있고, 랜덤수는 자신이 선택하였으므로 가상 아이디(ID_{MN2})를 다음과 같이 생성할 수 있다. 그리고 단말기와 안전하게 통신할 수 있는 세션키를 생성한다. 이후 동일한 세션키를 가지고 있다는 검증 메시지로 가상 아이디(ID_{MN2})와 랜덤수($R2_{AAAL_A}$)를 선택하여 세션키로 암호화 하여 전송한다.

$$ID_{MN2} = ID_{MN} \oplus R_{AAAL_A}$$
$$SK_{AAAL_A,MN} = g^{\alpha x_{AAAL_A}} \bmod n$$
$$E_{SK_{AAAL_A},MN}[ID_{MN2},\ R2_{AAAL_A}]$$

[Step 3] 모바일 단말기 사용자는 홈 네트워크 서버로부터 전송 받은 메시지를 복호화 하여 가상 아이디(ID_{MN2})와 세션키를 생성할 수 있는 인자(α)를 획득하여 다음과 같이 생성한다. 그리고 외부 인증 서버로부터 전송되어온 암호화된



(그림 4) 단말기 인증 및 외부 인증 서버의 가상 아이디와 키 분배 흐름도



(그림 5) 외부 네트워크 A와 외부 네트워크 B의 아이디와 세션키 흐름도

메시지를 복호화하여 동일한 가상 아이디인지를 확인하고 세션키를 이용하여 가상 아이디(ID_{MN2}), 이전 아이디(ID_{MN}), 그리고 외부 인증 서버가 선택한 랜덤수($R2_{AAAL_A}$)를 암호화하여 외부 인증 서버에 전송한다.

$$SK_{AAAL_A,MN} = g^{\alpha x_{AAAL_A}} \bmod n$$
$$E_{SK_{AAAL_A},MN}[ID_{MN}, ID_{MN2}, R2_{AAAL_A}]$$

외부 인증 서버가 모바일 단말기 사용자와 동일한 세션키를 가지고 있다는 것을 검증하는 방법은 전송되어져 온 암호화 메시지를 복호화하여 이전 아이디와 가상 아이디 그리고 자신이 선택한 랜덤수($R2_{AAAL_A}$)가 정확한지 검증하면 된다.

4.2.3 외부 네트워크 A와 외부 네트워크 B의 가상 아이디와 세션키 교환

모바일 단말기 사용자가 이동을 통해 외부 네트워크 A에서 B로 이동하면 다음과 같이 외부 네트워크 A와 B가 통신을 하여 가상 아이디(ID_{MN3})와 세션키($SK_{AAAL_B,MN}$)를 생성한다.

[Step 1] 모바일 단말기 사용자는 외부 네트워크 B의 인증 서버 공개키로 이전 외부 네트워크와 통신에 이용한 가상 아이디(ID_{MN2}), 모바일 단말기에서 선택한 랜덤수(R_{MN}) 그리고 이전 세션키로 암호화 한 메시지($E_{SK_{AAAL_A},MN}[ID_{MN2} \| R2_{AAAL_A}]$)를 암호화하여 전송한다.

$$E_{P_{AAAL_B}}[ID_{MN2} \| R_{MN} \| E_{SK_{AAAL_A},MN}[ID_{MN2} \| R2_{AAAL_A}], h(R_{MN})]$$

[Step 2] 네트워크 B의 인증 서버는 복호화하여 모바일 단말기 가상아이디(ID_{MN2})와 랜덤수(R_{MN})를 획득하고 암호화된 메시지는 외부 A의 인증 서버 공개키로 암호화 하여 전송한다.

$$E_{P_{AAAL_A}}[E_{SK_{AAAL_A},MN}[ID_{MN2} \| R2_{AAAL_A}]]$$

[Step 3] 네트워크 A의 인증 서버는 네트워크의 B에서 전송된 데이터를 가지고 모바일 단말기 사용자를 인증하고 네크워크 B의 인증 서버 공개키로 A의 인증 서버가 서명한 메시지를 암호화하여 네트워크 B의 인증 서버에 전송한다.

$$E_{P_{AAAL_B}}[Sig_{S_{AAAL_A}}[ID_{MN2}, R2_{AAAL_A}]]$$

[Step 4] 네트워크 B의 인증 서버는 A의 인증 서버로부터 전송받은 메시지를 복호화하여 서명된 가상 아이디가 맞는지 확인하고 B에서 사용될 가상 아이디(ID_{MN3})와 세션키를 다음과 같이 생성한다. 이후 세션키의 검증을 위해 사용될 가상 아이디(ID_{MN3})와 외부 인증 서버 B가 선택한 랜덤수(R_{AAAL_B})를 세션키로 암호화하여 모바일 단말기에 전송한다.

$$ID_{MN3} = ID_{MN2} \oplus R_{MN}$$
$$SK_{AAAL_B,MN} = g^{x_{AAAL_B} R_{MN}} \bmod n$$
$$E_{SK_{AAAL_B},MN}[ID_{MN3}, R_{AAAL_B}]$$

[Step 5] 모바일 단말기 사용자는 자신이 생성한 세션키로 복호화하여 가상 아이디(ID_{MN3})를 확인하고 이전 아이디(ID_{MN2})와 B의 인증 서버가 전송한 랜덤수(R_{AAAL_B})를 암호화하여 전송한다.

$$E_{SK_{AAAL_B},MN}[ID_{MN2}, ID_{MN3}, R_{AAAL_B}]$$

5. 제안 방식 분석

제안 방식의 프로토콜을 2장에서 언급한 보안 요구 사항에 따라 인증과 키 분배를 분석을 안전성, 효율성 및 오버헤드로 나누어 제시한다.

5.1 안전성

1) 정당한 객체만이 메시지를 확인할 수 있어야 한다. 우선 홈 인증 서버와 모바일 단말기는 공유하고 있는 대칭키를 이용하여 메시지를 암호화하여 전송하고, 외부 네트워크의 경우에는 공개키를 이용하여 기밀성을 제공하고 있다. 아이디와 서명의 값을 이용하여 메시지는 정당하게 생성되었다는 것을 확인 할 수 있으며, 수식에서 $E_{KS}[h(IIN \| S_i), i]$를 검증하면 정당한 모바일 단말기만이 사전의 분배된 S_i를 가지고 있으므로 확인 가능하다. 외부 인증 서버의 경우에는 다음과 같이 서명의 값($Sig_{S_{AAAL_A}}[ID_{AAAL_A} \| h(R_{AAAL_A})]$)으로 외부네트워크의 아이디와 선택한 랜덤값을 제공하므로, 정당한 객체임을 알 수 있다.

2) 전송되는 메시지는 중간에 위조, 삭제 그리고 변조할 수 없어야 하며 만약 위조, 삭제 및 변조가 된다면 그 사실을 알 수 있어야 한다. 제안 방식에서 위조, 삭제 및 변조를 알 수 있는 방법으로 각각의 메시지마다 두 가지의 내용을 포함하고 있으며, 서명과 해쉬값으로 제공한다. 서명에는 암호화되는 메시지에 내용이 해쉬로 포함되어 있다. 이는 두 가지의 관점에서 안전성을 제공할 수 있다. 해쉬된 내용으로 메시지의 무결성을 검증할 수 있고, 서명값은 자체는 전송한 객체의 메시지 인증을 제공할 수 있는 방법이 된다. 또한 서명과 암호화 메시지 두 개를 동시에 위조, 변조하는 것은 매우 어렵다.

3) 정당한 사용자는 정당한 인증 서버에서 자신이 정당한 사용자라는 것을 확인시킬 수 있어야 한다. 정당한 인증 서

〈표 1〉 효율성 비교표

	3.3 방식	3.4 방식	제안 방식
단말기 초기 인증 통신 횟수	4회 (외부 인증 서버 경유)	4회 (외부 인증 서버 경유)	4회 (외부 인증 서버 경유)
외부 네트워크 인증	제공 안함	4회 (외부 인증 서버 경유)	4회 (외부 인증 서버 경유)
외부 네트워크와 외부 네트워크 이동시 인증	제공 안함	제공 안함	5회
메시지의 암호화 연산 대칭키 및 공개키	대칭키 : 7회	대칭키 : 2회 공개키 : 1회	대칭키 : 1회 공개키 : 1회
외부 인증 메시지 암호화 연산	제공 안함	공개키 : 2회	대칭키 : 1회 공개키 : 3회

〈표 2〉 오버헤드 비교표

	3.3 방식	3.4 방식	제안 방식
홈 인증 서버 오버헤드	n * 4회 * N	n * 4회 * M	n * 4회 * 1회
단말기 오버헤드	홈 인증 1회 연산 2회	홈 인증 1회 연산 2회	홈 인증 1회 연산 4회
외부 인증 서버 오버 헤드	없음	n * M *2회	n * 5회

(n : 단말기 개수, N : 인증 요청 횟수, M : 외부 인증 서버 개수)

〈표 3〉 제안 방식 분석표

	3.3 방식	3.4 방식	제안 방식
안전성	우수 (인증과 IKE)	보통 (인증만을 제공)	우수 (인증과 세션키)
효율성	우수 (단 홈 네트워크만 지원 외부 네트워크의 접근은 지원하지 않음)	떨어짐 (모든 외부 인증 네트워크는 인증할 수 있는 메시지(AEM)를 가지고 있어야 함)	보통 (단말기가 접근하는 외부 인증 네트워크만 인증할 수 있는 데이터를 갖는다.)
단말기 오버헤드	적음 (기본 인증 메시지 1회 생성)	적음 (기본 인증 메시지 1회 생성)	높음 (N개의 접근시마다 N개의 연산 필요)
외부 네트워크 인증 오버헤드	외부 인증 서비스 제공 안함	적음 (단점으로 n개의 인증 서버가 모든 단말기의 인증 메시지를 가지고 있음)	적음 (접근하는 인증 서버만 메시지를 생성)
홈 인증 서버 오버 헤드	높음 (n개의 단말기 요구에 n개의 인증 메시지 생성)	높음 (초기 외부 인증 서버의 인증 메시지 생성)	적음 (외부 인증 서버의 1회 인증 메시지)

버는 자신이 등록한 모바일 단말기마다 아이디, PIN 그리고 S_i값을 가지고 있으며 공유한 대칭키(KS)를 가지고 있다. 아이디가 존재하는 정당한 사용자라면 S_i와 PIN을 연접한 해쉬값 검증과정에서 알 수 있다. 그리고 정당한 외부 인증 서버를 확인하는 것으로는 공유된 키가 없으므로 공개키 방식에서 서명과 랜덤 값을 검증하는 과정으로 대처되어 있다. 홈 인증 서버에서 전송되는 데이터에 외부 인증 서버가 선택한 랜덤 값을 포함하여 전송하므로 정당한 홈 인증 서버에서 전송되었다는 것을 알 수 있다.

4) 메시지를 제 3자가 사용할 수 없어야 한다. 초기 인증에 이용되는 메시지에 OTP의 개념인 S_i를 이용하기 때문에 재전송을 할 수 없다. 그리고 다른 값을 재전송하는 경우 이전에 사용한 랜덤 값을 다시 이용하게 되며, 이미 사용한 랜덤 값은 인증 서버에 저장되어 동일한 랜덤 값이 오면 다시 한 번 메시지를 생성해서 전송하기를 요구한다. 그러면 동일한 랜덤 값으로 만들어진 메시지를 재전송할 수 없게 된다.

5) 제 3자는 사용자, 홈 인증 서버 혹은 외부 인증 서버로 위장해서는 안 된다. 우선 제 3자가 사용자로 위장하기 위해서는 PIN과 S_i 그리고 비밀리에 공유한 대칭키(KS)를 알아야 한다. 그리고 홈 인증 서버나 외부 인증 서버로 위장하기 위해서는 인증 서버의 개인키를 알아야 한다. 그러므로 본 제안 방식에서는 제 3자가 위장하기는 매우 어렵다.

6) 세션키를 검증을 할 수 있어야 한다. 외부 인증 서버와 모바일 단말기 사이에 안전한 통신을 할 수 있게 홈 인증 서버가 세션키 생성 인자를 분배해준다. 이후 외부 인증 서버와 모바일 단말기는 생성한 세션키가 동일한지 검증을 하여야 한다. 검증 과정으로는 가상 아이디를 암호화여 전송하면 다른 쪽에서는 가상 아이디와 확인 메시지를 암호화하여 전송한다. 이때 동일한 키를 생성하지 못하였다면 가상 아이디와 확인 메시지를 검증 할 수 없게 된다.

5.2 효율성 및 오버 헤드

3.3 방식은 홈 인증서버가 모든 단말기의 인증을 제공하고, 3.4와 제안 방식은 외부 인증서버가 인증을 제공 해줄 수 있다. 그러므로 이를 효율성과 오버 헤드로 비교한다. <표 1>의 경우 초기 통신 횟수는 같으나 외부 네트워크를 통한 인증에서 차별성이 나타난다. <표 2>는 오버 헤드로써 홈 인증 서버 및 외부 인증 서버의 오버 헤드는 제안 방식이 가장 낮으나, 단말기의 오버 헤드는 높은 단점을 가지고 있다. <표 3>는 최종적으로 각각을 분석한 내용을 포함하고 있다.

6. 결 론

본 논문은 외부 인증 서버를 이용하여 홈 인증 서버의 역할을 대리적으로 수행하는 방안에 대하여 제시하였다. 기존의 많은 연구에서도 대리적인 수행에 대하여 언급하였으나 대리적인 수행을 할 수 있는 중계 서버를 이용하는 경우 중계 서버에 접근하기 위한 오버헤드가 발생하게 된다. 이에 중계 서버 방식이 아닌 외부 인증 서버 자체가 홈 인증 서버의 역할을 대행함으로 기존의 인프라를 그대로 사용할 수 있으며, 인증 메시지 또한 아이디와 패스워드에 기반하여 생성됨으로 기존의 통신 모델을 활용 할 수 있다. 그리고 외부 인증서버와 단말기의 안전한 통신을 위하여 세션키 설립과정과 제 3자의 위장을 막기 위해서 세션키의 검증 과정을 포함 시켰으며, 5장을 통해서 효율성과 오버 헤드를 분석하였다.

향후 연구를 위해서는 우선 모바일 단말기의 연산 능력을 중요시하여야 한다. 모바일 단말기는 현재 발전을 거듭하고 있으며, 컴퓨팅 능력은 지속적으로 발달 하고 있다. 그러므로 본 논문에서 효율성이 떨어지는 모바일 단말기의 연산은 극복할 수 있는 방안이 된다. 암호화 키는 인증 서버 및 모바일 단말기에서 사용되는데 이와 같은 경우 다양한 단말기에 대한 키 관리가 필요하게 된다. 특히 모바일 단말기의 이동으로 인해 키를 관리하는데 어려움이 따를 수 있다. 그러므로 암호화 키를 관리하는 방안 또한 효율적으로 제시되어야 할 부분이 될 것이다. 그러므로 모바일 단말기에 대한 인증과 안전한 통신을 위한 키 관리는 지속적으로 연구되어야 할 분야이다.

참 고 문 헌

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

[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*, 2005.

[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.

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

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

[8] F. Johansson and T.Johansson, "Mobile IPv4 Extension for Carrying Network Access Identifiers," RFC 3846.

[9] J, Vollbrecht, P. calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruihjn, C.de Laat, M. Holdrege and D.Spence, "AAA Authorization Application Examples," RFC 2905.

[10] 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.

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

[12] P. Hoffman, "Algorithuns for Internet Key Exchange version 1," RFC 2409.

[13] T. Dierks and c. Allen "The TLS Protocol Version 1.0," RFC 2246.

[14] IEEE Standard 802.1X-2001. IEEE Standard for Local and metroplitan area networks-Port-Based Network Access Control. June. 2001.

[15] IEEE Standard P802.11i/D10.0 Medium Access Control Security Enhancements, Amendment 6 to IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11 Wireless Medium Access Control and Physical Layer Specifications. April. 2004.

[16] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, insecurity of the WEP algorithm

강 서 일

e-mail : kop98@sch.ac.kr
2003년 순천향대학교 정보기술공학부(학사)
2004년~2005년 순천향대학교 전산학과 (석사)
2005년~현재 순천향대학교 전산학과 박사과정
관심분야 : 전자 투표, 전자 화폐, 전자 상거래

이 임 영

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