AAAv6에서의 EAP-TLS 인증모델 성능평가

정 윤 수[†]·김 형 도[†]·이 해 동[††]·김 현 곤[††]·이 상 호[†††]

요 약

Mobile IP에서 이동노드와 서버간의 안전한 통신을 제공하고 급증하는 사용자 인증 서비스 요구를 만족시키기 위해 AAAv6기반 다이어미터(Diameter) 기술이 사용자 인증에 사용 되고 있다. 따라서 이 논문에서는 사용자 인증기능 수행을 위한 서버들의 최적 성능 지표를 구하고자 도메인간의 이동성을 가지는 AAAv6 인증 모델중의 하나인 EAP-TLS기반의 서버 성능 평가 모델을 설계한다. 그리고 DSA/RSA암호 알고리즘을 이용하여 사용자 인증 기능을 수행하는 각 서버의 최적 성능지표를 도출하여 AAAv6의 운영을 최적화 시킬 수 있는 환경을 제시한다.

A Performance Evaluation of EAP-TLS Authentication Model in the AAAv6

Yun Su Jeong[†]·Hyung Do Kim[†]·Hae Dong Lee[††]
Hyun Gon Kim[††]·Sang Ho Lee[†††]

ABSTRACT

AAAv6-based Diameter method is using in the user authentication to satisfy the users' increasing user authentication demand and to supply a safe communication between mobile node and server in the Mobile IP. therefore, In this paper, We design a model of server capacity based on EAP-TLS that in one of AAAv6 models with mobility among domains to get the optimized capacity index of the server for user authentication accomplishment. We elicitat the authentication capacity index for each server of which is accomplishing in user authentication using DSA/RSA algorithm and purpose the optimized condition for the AAAv6 capacity by the index.

키워드 : 인증(Authentication), 인가(Authorization), 과금(Account), EAP-TLS, AAAv6,

1. 서 론

인터넷 사용자의 급속한 증가와 무선 통신 기술의 빠른 성장으로 개인 또는 기업의 사용자는 이동 통신 기술을 이용한 정보의 처리에 따른 Roaming, VoIP, Internet FAX, QoS등과 같은 복잡한 inter-domain 응용 서비스가 등장하게 되었다. 이들 서비스들은 기본 서비스들에 비해 보다 신뢰적이고 안전한 관리를 요구하게 되었고, 이들의 요구사항을 받아들여 각 분야에 적합한 AAA를 지원하기 위한 연구가 시작되었다[3, 13].

AAA(Authentication, Authorization, Account) 프로토콜로는 레디어스(RADIUS : Remote Authentication Dial-In User Services), 다이어미터(DIAMETER), TACACS+, SNMP (Simple Network Management Protocol) 등이 있으며 이중에서 현재 가장 널리 사용되고 있는 AAA 서버는 레디어스 프로토콜을 기반으로 하고 있다. 레디어스는 인증과 과금을 위한 프로토콜로 이미 많은 분야에서 사용되고 있으며 서버 기반의 인증이 필요한 소수 가입자들을 지원하는 소규모 망 장치를 위한 프로토콜로서, 다양한 기술 기반 위에서 동시에 수백~수천의 사용자를 지원해야만 하는 통신 사업자들에게는 적합하지 않다. 이러한 레디어스의 한계와 문제점을 해결하기 위해 다이어미터라는 새로운 프로토콜이 AAA 워킹그룹에서 개발 중에 있다[4-8].

현재 PPP(Point-to-Point)나 터미널 서비스 액세스와 같은 서비스를 위한 AAA 프로토콜기술은 업체간에 연동 가능한 망 개수가 겨우 4개에 불과한 데다 로밍 서비스나 인터넷 전송 과정에서 보안성이 크게 떨어져 다양한 유·무선 통신망의 융합, 급증하는 로밍 서비스의 수요 충족에 부족한 것으로 평가되고 있다[1, 2]. 이러한 문제점들을 해결하기 위해 AAA 환경을 구성하고 있는 다양한 서버들은 CMS (Cryptographic Message Syntax) 확장을 통해 보안을 강화하고 NASREQ-EAP 응용 기술을 사용하여 신뢰적이고 효율적인 사용자 인증을 요구하고 있다.

† 준 회 원 : 충북대학교 대학원 전자계산학과
†† 정 회 원 : 한국전자통신연구원 정보보호연구단연구원
††† 종신회원 : 충북대학교 전기전자컴퓨터공학부 & 컴퓨터정보통신연구소 교수
논문접수 : 2004년 1월 20일, 심사완료 : 2004년 5월 3일

AAAv6 환경 구축을 위한 서버로는 AAA attendent, AAAv (AAA local authority), AAAb(AAA broker), AAAh(AAA home authority), HA(Home Agent)등 5개의 엔터티를 정의하고 있다. AAA attendent는 이동 노드가 외부 링크에서 가장 먼저 접속하게되는 외부 엔티티로서 이동 노드가 전송하는 패킷에 대한 통과, 폐기, 보류 등의 정책을 수행할 수 있으며, AAA 서버를 통한 인증 성공시 패킷을 통과 시킬수 있다. AAAv는 외부 링크의 AAA 인증 서버로서 이동 노드로부터 인증 요청을 수신하면 먼저 AAA attendent를 인증하고 메시지의 NAI나 홈 주소를 통해 이동 노드의 홈 도메인에 존재하는 AAA 인증 서버로 전송한다. AAAh는 홈 도메인의 AAA 인증 서버로서, 이동 노드의 인증에 필요한 인증 정보들로 구성된 프로파일을 관리하고 있다. AAAv6의 효율적 운영을 위해서는 각 서버의 성능 보장을 통한 유기적 연계가 필수적 요소이다.

따라서, 이 논문에서는 AAAv6 환경의 서버들이 도메인 간의 이동성을 가지는 사용자들에 대해서 안정적으로 서비스할 수 있도록 사용자 인증에 필요한 암호 알고리즘을 DSA(Digital Signature Algorithm)와 RSA(Rivest-Shamir-Adleman)로 구분하여 사용자 인증기능 수행을 위한 각 서버의 최적 성능지표를 구하고자 한다.

이 논문의 구성은 다음과 같다. 2장에서는 다이어미터 프로토콜과 Mobile IPv6와 다이어미터에서의 인증과정에 대해 기술한다. 3장에서는 EAP 확장모델인 EAP-TLS에 대해서 설명하고, 4장에서는 성능평가를 위한 모델설계를 한다. 5장에서는 성능 평가 및 분석을 기술하고, 마지막으로 6장에서는 결론에 대해 기술한다.

2. 다이어미터 프로토콜과 AAAv6

이 절에서는 연구의 기반이 되는 다이어미터 프로토콜과 Mobile IPv6와 다이어미터 기반 AAA 인프라가 정합된 AAAv6의 인프라구조(Infrastructure)의 구성 및 정합 시나리오에 대해서 설명한다.

2.1 다이어미터 프로토콜

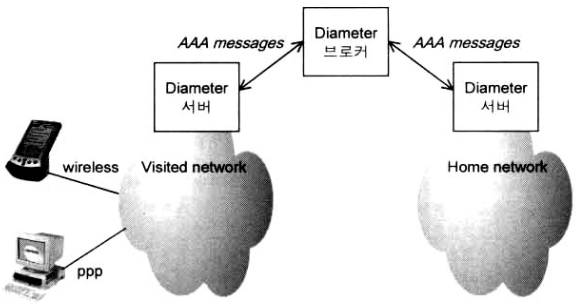
레디어스 프로토콜은 원래 단순한 서버 기반의 인증을 원하는 소수의 엔드유저를 위하여 설계되어, 일단의 소규모 PPP 도메인에서 서버 접속에 대한 AAA 서비스를 제공하는데에 사용되어 왔다. 사용자와 서비스 도메인이 늘어남에 따라 이동이 빈번한 도메인 사이의 이동이 발생하는 환경에서 보안성을 위한 메커니즘의 복잡성과 조밀성이 증가하게 되었다. 따라서 서로 다른 도메인의 이동을 효과적으로 지원하기 위한 단-대-단(peer-to-peer) 프로토콜 구조, 브로커 개념의 적용에서 다른 새로운 프로토콜 다이어미터의 중요성이 증가하였다.

〈표 1〉 AAA 서비스 요소와 표준기법

네트워크 형태	AAA 서비스 사용자	표준화 기법
고정 네트워크	고정 사용자	레디어스
	로밍(Roaming) 사용자	레디어스와 다이어미터
이동 네트워크	이동(Mobile) IP 사용자	다이어미터
	Strong Security 사용자	
	Enhanced Accounting 사용자	

다이어미터는 PPP(Point-to-Point Protocol), 로밍(Roaming), 이동(Mobile) IP와 같은 기존 기술과, 새롭게 요구되는 기술에 대한 AAA 서비스를 제공하기 위한 가볍고 확장성이 있는 peer 기반의 AAA프로토콜이다[6, 9]. 다이어미터는 AVP(Attribute/Value Pair)와 프록시를 지원한다는 점에서 레디어스와 비슷하나 AVP의 사용 범위에 있어서는 큰 차이를 보인다. 레디어스 주소 공간은 256쌍으로 제한되어 있지만 다이어미터는 32bit의 AVP 주소 공간으로 수백만 쌍 이상을 지원할 수 있다. 이와 같은 강력한 AVP 주소 공간 특성은 이동 사용자나 전용 사용자들을 서비스하기에도 충분하다[15]. 다이어미터 프로토콜은 서버가 NAS (Network Application Support)에게 NAS가 처리할 수 있을 만큼의 메시지를 전송하는 것을 허용하는 신뢰성 있는 윈도우 통신 기반의 전송을 지원한다. 레디어스 서버는 사용자가 요구하지 않으면 메시지를 보낼 수 없는 반면 다이어미터는 가능하며, 이는 서버가 NAS에게 특별한 과금 기능이나 연결 종료 같은 오퍼레이션 수행을 알릴 때에 유용하게 사용된다. 또한 다이어미터는 재전송과 장애 복구 기능을 개선하여 초보적이고 느린 레디어스에 비해 향상된 망 회복력을 제공한다. 마지막으로, 다이어미터는 레디어스가 제공하지 않는 종단간 보안 기법을 제공한다[14].

다이어미터는 로밍과 Mobile IP 망을 지원하기 위해 처음 설계되었다. (그림 1)은 다이어미터 브로커가 방문망에 접속하여 홈망의 자원을 이용하고자 하는 로밍 및 Mobile IP 사용자에 대해 AAA 서비스를 어떻게 제공하는지를 보여준다. 이 경우 방문망 ISP에 있는 다이어미터 서버는 AAA 기능을 수행하기 위해 브로커에 대한 peer로 동작한다.



(그림 1) 로밍을 지원하는 다이어미터 구조

다이어미터 서버와 브로커사이의 통신은 브로커가 CA (Certificate Authority)의 역할을 하므로 안전한 연결상태에서 동작한다. 서버에 대해 인증서를 분배하는 것은 모든 서버가 공유 비밀키를 가지는 것보다도 확장성이 있으면서도 효과적인 방법이다.

다이어미터 기본 프로토콜은 그 자체 그대로 사용되기보다 대게 특별한 application을 위해 확장되는 형태로 사용되고, 다음과 같은 IETF WG들에 의해 확대되어 개발되고 있다[12, 21].

① ROAMOPS(Roaming Operations) : ISP들 사이에서 사용자의 로밍을 지원하도록 메커니즘, 절차, 프로토콜을 개발 중에 있다.

② NASREQ(Network Access Server Requirements) : 간단한 다이얼 업 사용에서부터 VPN 지원, 스마트 인증 방법, 로밍에까지 지원하기 위한 NAS의 디자인이 이루어진다.

③ MobileIP(IP Routing for Wireless/Mobile Hosts) : IPv4나 IPv6를 사용하는 IP 노드들이 IP 서브넷과 매체 종류들 사이에 로밍을 지원하도록 라우팅 기술 개발 중에 있다.

④ AAA(Authentication, Authorication, Account) : 과금, 전송, 보안, 프록시를 지원하는 다이어미터 관련 프로토콜들을 개발하고 있다.

2.2 Mobile IPv6와 다이어미터에서의 인증과정

Mobile IP는 사용자가 이동중에도 서비스 단절없이 동일한 IP 주소를 유지하면서 인터넷에 대한 접속점을 변경할 수 있게 한다. Mobile IP가 이질적인 관리 도메인상에서 이동성을 제공할 수 있도록 확장하기 위해서는 Mobile IP 프로토콜이 AAA 인프라와 정합되어야 한다. Mobile IPv6와 다이어미터간의 인증과정을 살펴보면 다음과 같다[18, 19].

① MN은 인증을 위하여 MIP-Reg-Request를 AAA attendent에게 전송하고, AAA attendent는 MIP-Reg-Request를 수신하여 ARR(AA-Registration-Request)를 AAAv에게 전송한다.

② ARR을 받은 AAAv는 해당 MIPv6 Feature Vector AVP를 생성하여 AAAB를 통해 AAAh에게 전송한다.

③ AAAh는 ARR을 수신하여 정당한 AAAv가 보낸것인지 확인한 후 MIP-Reg-Request에 따라 HA에게 HOR (Home-Agent-MIPv6-Request Command) 메시지를 보낸다.

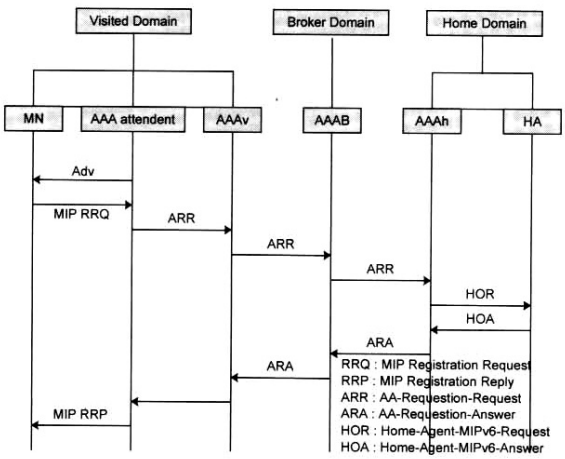
④ HA는 HOR 메시지를 수신하여 정당 여부를 판별하고 MIP-reg-Request에 따라 MIP-binding-Update를 한다. 이때 Authenticator를 확인하여 MN을 인증하게 된다.

⑤ 인증 후 HA는 HOA(Home-Agent-MIPv6-Answer) 메시지를 AAAh에게 전송한다.

⑥ AAAh는 HOA 메시지에 따라 MIP-Bingding-Acknowledgement 메시지를 생성하여 ARA(AA-Registration-Answer)메시지를 생성하여 AAAB를 통해 AAAv에게 전송한다.

⑦ AAAv는 ARA 메시지를 받아 추가적인 EAP 메커니즘이 없을 경우 AAA attendent에게로 ARA 메시지를 포워딩(Forwarding)한다.

⑧ AAA attendent는 ARA 메시지가 MN의 인증을 허가하는 것이면 MIP-Registration-Answer 메시지를 생성하여 MN에게 전송한다.



(그림 2) AAAv6 인증 과정

(그림 2)의 인증과정에 나타난 구성요소들을 기술하면 아래와 같다.

① AAA attendent : Mobile IPv6와 다이어미터를 지원하는 방문 망(Visited Domain)에 위치한 AAA 클라이언트

② AAAv(AAA local authority) : Mobile IPv6를 지원하는 다이어미터 서버로서, 방문 망에 위치한 로컬 인증서버

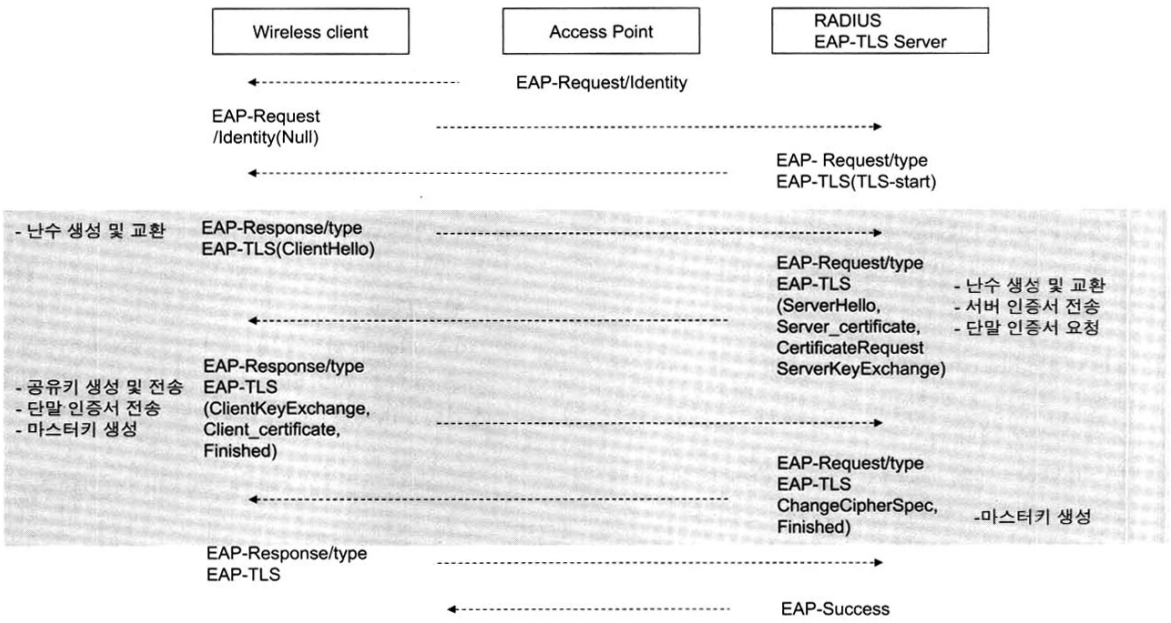
③ AAAb(AAA broker) : 브로커 망(Broker Domain)에 위치한 인증서버

④ AAAh(AAA home authority) : Mobile IPv6를 지원하는 다이어미터 서버로서, 홈 망(Home Domain)에 위치한 홈 인증 서버

⑤ HA : Mobile IPv6와 다이어미터를 지원하는 홈 망(Home Domain)에 위치한 AAA 클라이언트

3. EAP-TLS

RFC2284에 정의된 EAP(Extensible Authentication Protocol)는 다중 인증 메커니즘을 지원하기 위한 인증 프레임



(그림 3) EAP-TLS 상호 인증 및 키 분배

워크이다. EAP는 스위치 회로뿐만 아니라 링크와 유·무선에서도 사용되고 있다.

다이어미터 EAP는 NASREQ에 많이 의존하며 초기 드래프트(draft)에서 다이어미터 NASREQ 애플리케이션의 일부분이었다. 선택된 다이어미터 EAP 애플리케이션은 인증 메커니즘 사용에 기반하며, 새로운 Command-codes와 AVPs로 정의되고 레디어스 EAP 지원과 함께 작업할 수 있다[20].

TLS(Transport Layer Security)는 인터넷에서 통신상의 보안을 제공하는 프로토콜로써 클라이언트 서버간의 어플리케이션에서 도청이나 간섭, 메시지 위조와 같은 비 권한 제어를 방지할 수 있다. EAP-TLS는 TLS 핸드쉐이크를 EAP 프로토콜로 확장한 방법으로써 상호 인증과 키 분배에 대한 메커니즘을 포함한다. (그림 3)은 EAP-TLS의 핸드쉐이크 과정을 보여주고 있다[10, 11].

무선 단말이 새로운 AP(Access Point)영역에 도달을 감지하게 되면 EAP-TLS(TLS-start)메시지를 통하여 핸드쉐이크가 시작된다. 무선 단말은 난수를 생성하여 ClientHello 메시지에 포함시켜 서버로 전송한다. 인증 서버도 난수를 생성하여 ServerHello를 통해 보낸 후, 서버의 인증서를 전송하고, 필요시 단말의 인증서를 요청하는 메시지를 보낸다. 무선 단말은 두 개의 난수와 자신이 생성한 공유키를 이용하여 마스터키를 생성한다. 단말은 서버의 인증서에 포함된 공용키를 이용하여 공유키를 암호화하여 서버에게 전송한다. 서버는 자신이 가지고 있는 비밀키를 이용하여 공유키를 추출하고 두 개의 난수와 함께 마스터키를 생성한다. 무선 단말은 서버의 인증서를 통해 네트워크를 인증하고, 단말의 인증서 요청을 통하여 단말을 인증할 수 있게 되어 상호 인증이 가능하다.

4. 다이어미터 기반의 EAP-TLS 인증 모델

각 서버의 효율적인 서비스를 위해 HA에서 등록 메시지를 처리하는 전/후 과정을 등록 요구처리/등록 응답처리라고 정의하고, 암호처리 프로세스와 등록 프로세스 수치값들을 구하기 위한 실험 가정을 각 서버 환경에 맞게 설정한다. 설정된 수치값들은 암호 연산 시간과 등록 연산 시간을 합한 평균 처리시간를 기반으로 AAAv6 시스템 환경에서의 사용자 인증 수행에 최적인 각 서버별 요구성능 지표를 구한다.

4.1 가 정

다이어미터 기반 EAP-TLS 환경에서의 각종 서버들의 최적 요구성능을 얻기 위한 실험 모델의 가정은 아래와 같다.

① 각 서버의 안정적 운영을 위하여 서버의 이용율은 70% 수준으로 설정한다.

② 하나의 local 도메인에는 20개의 AAA attendent가 있고, 각 AAA attendent의 처리능력은 동일하다.

③ 다이어미터 EAP-MD5 인증 메시지는 한개의 AAA 브로커(Broker)을 경유한다.

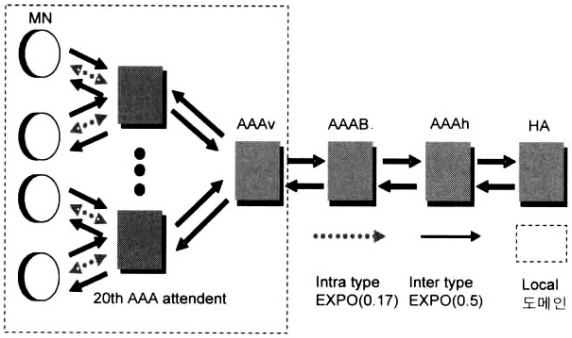
④ Registration Message Request 처리는 Mobile IP 등록 요청 전달 이전 단계라 정의하고, Registration Mes-

sage Response 처리는 Mobile IP 등록 이후 단계로 정의한다.

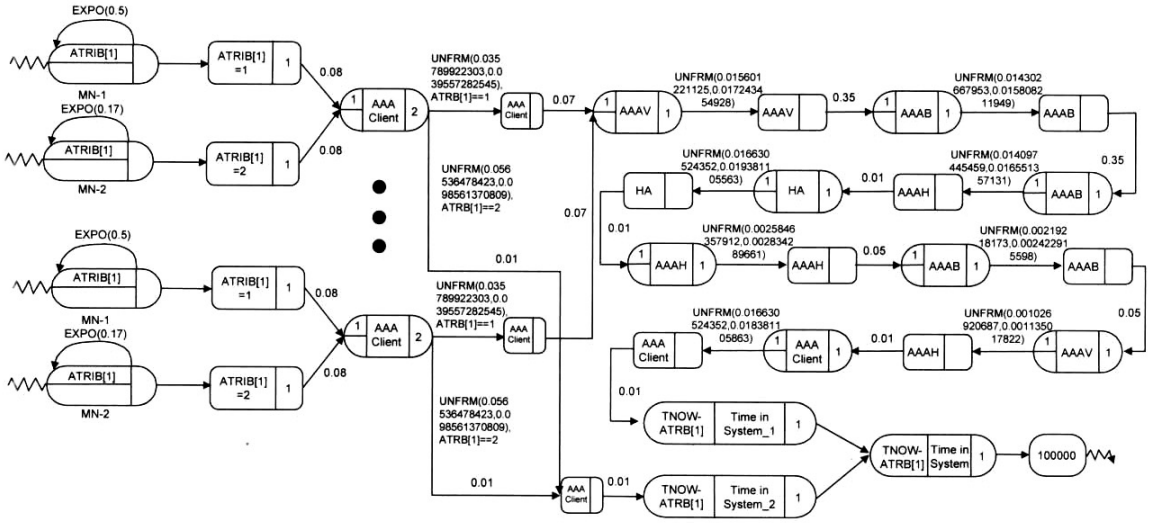
4.2 모델 설계

시뮬레이션을 위한 다이어미터기반의 EAP-TLS 인증모델은 (그림 4)와 같으며, EAP-TLS의 환경을 구성하고 있는 MN들의 입력 패턴은 크게 Intra 도메인과 Inter 도메인으로 구분하고, 각 도메인별 입력에 대한 평균 도착시간 간격은 0.17와 0.5의 지수분포로 정의한다.

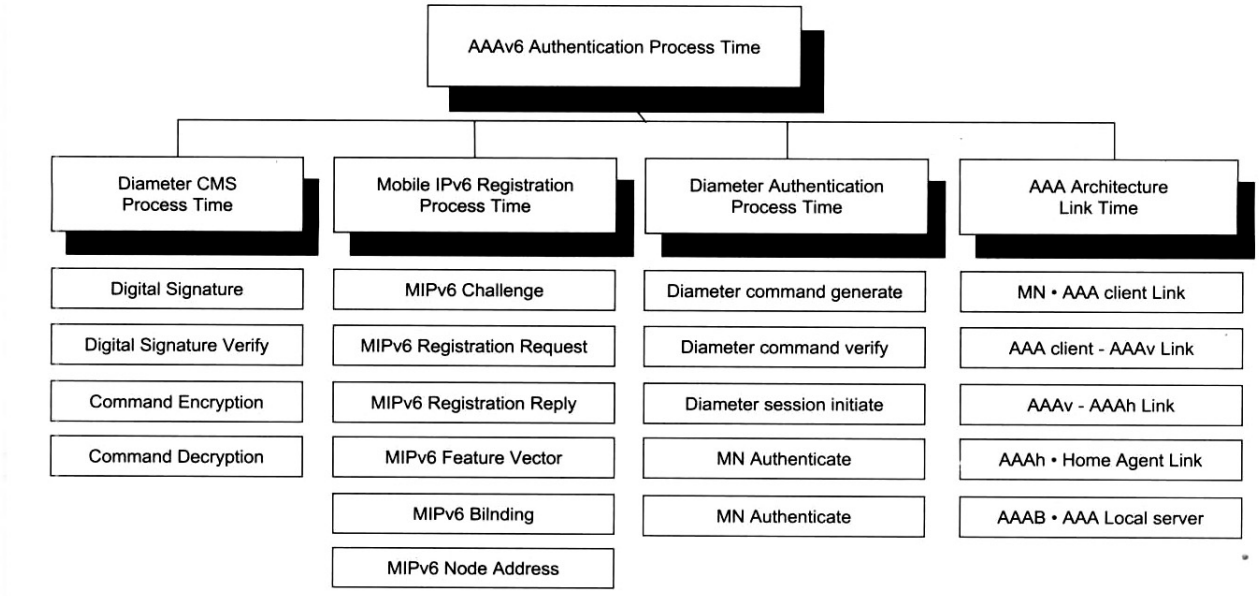
(그림 4)의 모델을 Awesim 모델로 표현하면 (그림 5)와 같다.



(그림 4) 다이어미터 EAP-TLS 사용자 인증 실험 모델



(그림 5) Awesim 모델

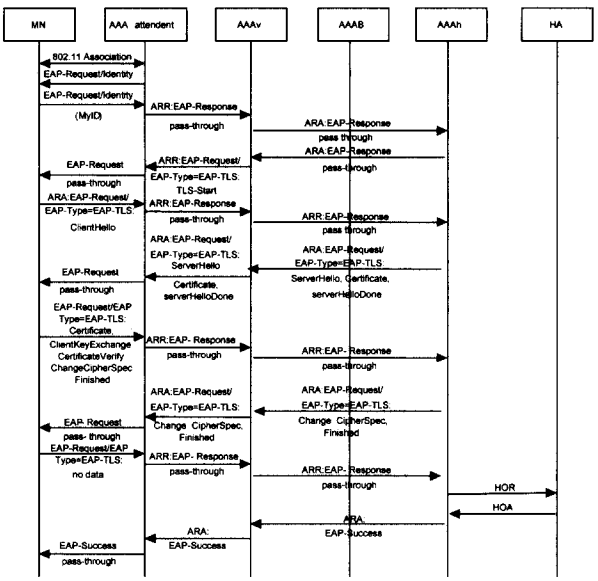


(그림 6) AAAv6 인증과정에서 발생되는 Processing 시간

4.3 성능 평가를 위한 파라미터의 설정

성능평가 실험을 위해 필요한 AAA 서버들의 수치값은 다이어미터 CMS(Cryptographic Message Syntax) process time, Mobile IPv6 Registration process time, 다이어미터 Authentication process time, AAA Architectural Link Delay time등이 있고, 이들 프로세스 수치값들의 합은 각 서버의 평균 처리 시간으로 구한다. (그림 6)은 Mobile IPv6를 지원하는 AAAv6 인증과정에서 소요되는 각종 처리시간을 나타낸다[13, 16, 17].

(그림 7)의 EAP-TLS 인증 메커니즘은 TLS 핸드쉐이크를 EAP 프로토콜로 확장한 방법을 적용한 결과로써 상호 인증과 키 분배에 대한 메커니즘을 포함하고 있다.



(그림 7) EAP-TLS 인증 흐름도

4.3.1 MN으로부터의 인증요청 유형

AAAv6 인증 모델중의 하나인 EAP-TLS의 환경을 구성하고 있는 서버들의 서비스 입력 유형은 크게 Intra 도메인과 Inter 도메인으로 분류할 수 있다. Intra 도메인의 경우 local 도메인내에서 평균 도착시간 간격을 0.17의 지수분포로 서비스하는 유형을 말하고, Inter 도메인의 경우는 local 도메인간의 평균 도착시간 간격을 0.5의 지수분포로 서비스하는 유형을 말한다[17]. 그리고 각 서버가 사용자 인증을 처리하는데 소용되는 시간의 오차 범위는 서비스 환경에 영향을 줄 수 있는 여러 가지 요소들을 감안하여 ±5%의 이항 분포로 설정한다.

4.3.2 다이어미터 암/복호 처리시간

Hop-by-Hop Security를 위하여 이 논문에서 사용되고 있는 다이어미터 CMS 프로세스 시간은 DSA와 RSA를 이용한 Digital Signature와 3DES를 통한 암호화 처리시간를 사용하고 있으며, 암호 알고리즘에 사용되는 속도는 속도 Benchmarks를 참조하여 유추하였다[16].

다이어미터 EAP-TLS의 메시지 길이는 RFC 2246 문서를 참조하여 TLS알고리즘 협상시, TLS_RAS_WITH_DES_SHA가 선택되었을 경우로 가정하여 <표 3>과 같이 설정하였다.

〈표 3〉 TLS 메시지 크기

메 세 지	크 기
ClientHello message size	60bytes
ServerHello message size	66bytes
Certificate	493bytes
ClientKeyExchange message size	64bytes
Finished message size	12bytes
CerficateVerify message size	64bytes

다이어미터 CMS 프로세스을 위해 사용하는 각 암호화 알고리즘들의 Signature와 Verification 수치는 암호화 알고리즘을 평가한 연구를 참조하여 다이어미터 EAP command의 길이와 처리시간을 구하였다[1, 7, 16]. <표 4>는 CMS 프로세스 처리과정에 의해 DSA와 RSA의 평균 처리시간을 계산한 최종 결과값이다.

〈표 4〉 다이어미터 암/복호 처리시간

(단위 : μs)

서버 / 처리시간	AAA-attendent	AAAv	AAAB	AAAh	HA
DSA 평균처리시간	2287.0267125	4567.83215	4567.8321375	4567.8321378	4567.832138
RSA 평균처리시간	2491.735459	4968.912205	4968.9122	4968.9122	4968.9122

4.3.3 MIPv6 등록/인증 수행 시간

등록메시지에 대한 각 노드별 평균 처리시간을 토대로 각 노드별 프로세싱 시간을 가정하여 MN이 등록을 요청하면, AAAh와 AAAv는 HA와 AAA attendent의 메시지를 Relay 하는 역할의 비중이 가장 크므로, AAAh와 AAAv는 AAAB와 동일한 수행시간을 갖는다고 가정한다.

다이어미터 인프라구조를 구성하는 각 서버들의 인증 메시지 Registration 관련 처리속도는 AAA관련 보고서의 결과를 참조하여 P-2.1GHz에서의 연산 속도 가정치를 구하면 <표 5>와 같다[13].

〈표 5〉 P-2.1GH에서의 연산 속도 가정치

(단위 : μs)

서버 / 처리시간		AAA attendent		AAAv	AAAB	AAAh	HA
		Inter	Intra				
평균 처리 시간	등록 요구처리	49700	697	49700	697	249900	49700
	등록 응답처리		697	697	697	49030	

4.3.4 EAP-TLS 수행 시간

EAP-TLS의 수행시간은 AAA key와 128bit의 challenge 그리고 home address를 keyed hashing하는 과정으로 이루어져 있다. 사용되는 56bit의 키를 secret key로 가정하면 hashing하는 총 길이는 216bit가 된다.

① HMAC-TLS 연산 : 215.761 MByte/Second
→ 1809.9344 bit/μs
② SH1-TLS 연산 : 72.604 MByte/Second
→ 580.832 bit/μs

216bit를 hashing하는 SHA1과 TLS hash operation 시간은 각각 0.1μs과 0.125μs가 되고, EAP-TLS의 수행 노드는 AAA attendent와 AAAh 모두 2곳에서 이루어진다.

4.3.5 EAP-TLS 링크 통신시간

실험평가를 위한 AAA 인프라구조의 링크는 A.Hess의 EAP-TLS AAA 인프라구조 성능평가 실험 연구를 통해 얻은 링크 시간 수치를 이용한다[17].

통신 실험을 위하여 Link process을 (그림 7)의 메커니즘처럼 변경하면, AAA command message들은 인증을 위하여 Mobile IP Registration 이전 단계 중 MN-AAA attendent는 8번, AAAh-HA는 1번, 나머지는 모두 7번에 걸쳐 링크를 지나가게 된다. <표 6>은 처리절차에 따른 링크 처리시간을 나타내고 있다.

〈표 6〉 링크 통신시간

(단위 : μs)

Delay 시간 \ 서 버		MN-AAA attendent	AAA attendent-AAAv	AAAV-AAAB	AAAB-AAAh	AAAh-HA
Delay	등록 요구처리	80,000	70,000	350,000	350,000	10,000
	등록 응답처리	10,000	10,000	50,000	50,000	10,000

5. 성능 평가 및 분석

5.1 실험 환경

EAP-TLS기반의 AAAv6 모델을 실험하기 위해 사용되는 시뮬레이터는 Awesim3.0으로 하고, 실험에 사용되는 MN의 사용자 인증요청 메시지는 Inter/Intra 도메인에서 총 10만건이 AAA Attendent에 인증을 요청하는 것으로 한다. 또한 실험환경에서 인증 요청메세지가 모두 처리되는데 소요되는 시간은 총 6시간이며 실험 환경은 <표 7>과 같다.

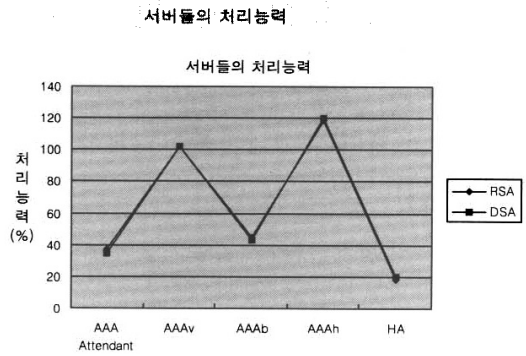
〈표 7〉 실험 환경

구 분	내 용
시뮬레이션 툴	AWESIM 3.0
메모리	256 MB
컴퓨터사양	Pentium4 2.4GHz Processor
OS	Windows XP SP1

5.2 실험 및 결과

4.3절에서 설정한 수치를 기반으로 AAAv6 모델에서의 암호처리는 AAA attendent에서 처리하고, 실험을 통하여 서버의 요구처리능력, 서버에서의 인증요청 메세지 대기시간, 인증 처리시간 등의 지표를 구하고자 한다.

서버의 성능 요구지표를 구하기 전에 EAP-TLS을 적용한 AAAv6기반 서버들의 처리능력을 DSA와 RSA로 나누어 살펴보면 (그림 8)과 같다. (그림 8)에서 보는것과 같이 AAAv6기반 서버들이 처리할 수 있는 최대 처리능력을 100%라고 할때 AAAh는 능력이상의 과부하 일을 하고 있는 반면 AAA Attendent, AAAb, HA는 처리 능력이하의 일을 하고 있다. 이런 결과는 각 서버간의 처리능력이 비효율적으로 동작되는 것을 알 수 있다.

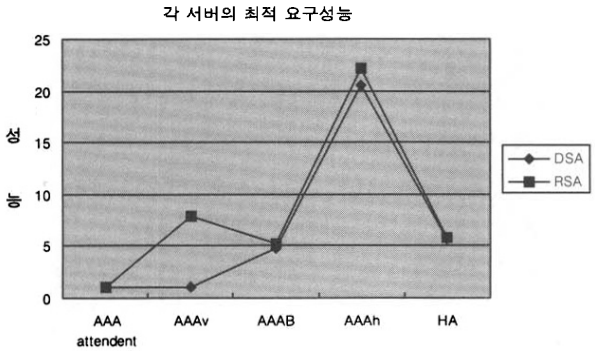


(그림 8) AAAv6기반 서버들의 요구처리능력

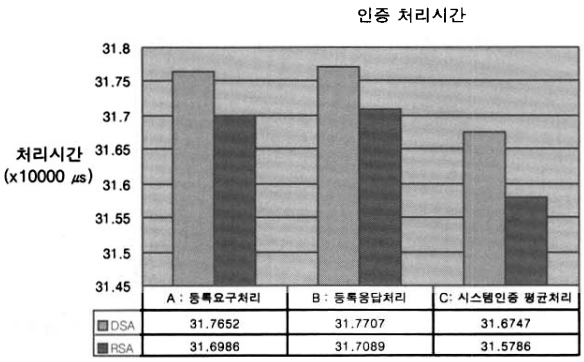
(그림 9)는 사용자들에게 신뢰적이고 효율적인 사용자 인증을 제공하기 위한 각 서버의 최적 요구성능지표를 시간적 측면에서 DSA와 RSA로 구분하여 나타내고 있다. DSA의 경우 4.3절에서 설정한 수치를 기반으로 AAA Attendent 서버의 성능을 펜티엄 4 2GHz의 성능을 가지는 서버라고 할때 AAAv는 AAA Attendent와 동일한 성능을 가지는 서버가 필요하고, AAAb, AAAh, HA 서버들은 AAA Attendent보다 각각 3.75배, 19.6배, 4.6배 빠른 서버가 필요하다. RSA의 경우 AAA Attendent 서버의 성능이 DSA와 동일한 펜티엄 Ⅳ 2GHz의 서버라고 할때 AAAv, AAAb, AAAh, HA 서버들의 성능은 AAA Attendent보다 각각 6.96배, 4.18배, 21.23배, 4.8529배 빠른 서버가 필요하다.

또한 EAP-TLS기반의 사용자 인증을 원활하게 처리하기 위하여 각 서버의 이용율을 70%로 유지하도록 가정한다. 이 가정하에 AAAv6기반 서버들의 인증처리 시간을 살펴보면 (그림 10)과 같으며, 인증처리 시간을 DSA와 RSA로

나누어 비교분석한 결과 RSA가 DSA보다 0.31% 빠르게 처리되는 것을 알 수 있다.

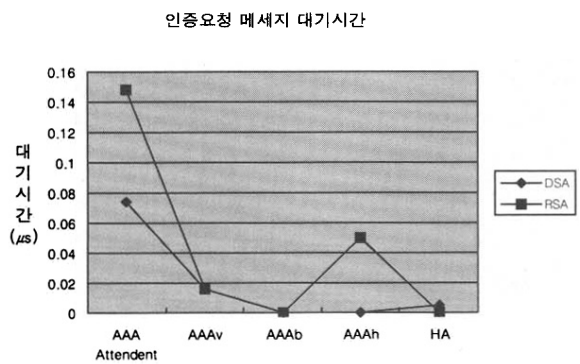


(그림 9) 각 서버의 최적 요구성능 결과



(그림 10) 서버의 인증처리시간

AAAv6기반 각 서버들의 인증요청 메시지의 대기 시간은 (그림 11)과 같으며 EAP-TLS의 환경을 구성하고 있는 AAA attendent수를 20개로하여 실험하였기 때문에 Local Domain의 AAA attendent에서 보내오는 인증 메시지가 AAAv로 집중되어 AAAv에서 병목 현상이 일어남을 알 수 있다. 또한 AAAH에서는 DSA 알고리즘을 사용하였을 때보다 RSA 알고리즘을 사용하였을때의 대기 시간이 높다. 이것은 AAAb의 메시지 처리시간이 DSA보다 RSA가 높기 때문이다.



(그림 11) 서버에서의 인증 요청 메시지 대기시간

5.3 평 가

각 서버의 CPU 요구처리률이 70%로 동작되도록 실험한 결과 암호화 방식에 있어 DSA와 RSA경우 각 서버에서의 CPU 요구처리 능력은 DSA의 경우 AAAh가 다른 서버에 비해 요구 처리율이 약 8.5배 높은 반면 RSA의 경우에는 AAAv와 AAAh의 이용율이 DSA보다 약 3.4배 높다. 전체적인 서버 요구 처리율에서 보면 AAA Attendent을 펜티엄 4 2GHz의 성능을 가지는 서버라고 볼때 AAAv, AAAb, AAAh, HA 서버들은 AAA Attendent보다 평균적으로 4.2배, 3.9배, 20.4배, 4.7배 빠른 서버가 필요하고 시간적 요구처리측면에서는 DSA가 RSA보다 CPU 요구처리률이 2.4% 좋게 나타났다.

또한 인증 메시지에 대한 각 서버에서의 인증 요청 메세지 대기시간은 AAAv에서 대기시간이 높은 것을 알 수 있다. 이것은 Local Domain에 있는 20개의 AAA attendent에서 인증 메시지가 AAAv로 집중되기 때문에 병목 현상이 일어난다. 그리고 RSA의 AAAv와 AAAh가 DSA보다 많은 수행이 일어나기 때문에 시간적 측면에서 보면 RSA보다 DSA가 약 1.9% 빠른 것으로 나타나고 있다. 마지막으로 인증 요구 메시지에 대한 평균처리시간을 시간적 측면에서 살펴보면 DSA보다 RSA가 약 0.7% 느리지만 각 서버의 서비스를 안정적으로 유지하였을때는 RSA가 DSA보다 0.32% 빠르게 처리된다.

6. 결 론

인터넷 사용자의 급속한 증가와 무선 통신 기술의 빠른 성장으로 개인 또는 기업의 사용자는 이동 통신 기술을 이용한 정보의 처리에 따른 Roaming, VoIP, Internet FAX, QoS등과 같은 복잡한 inter-domain 응용 서비스가 등장하게 되었다. 이들 서비스들은 기본 서비스들에 비해 보다 신뢰할 수 있고 안전한 관리를 요구하게 되었고, 이동전화와 Wireless LAN을 통한 무선 인터넷의 확산에 따라 이동중의 인터넷 서비스뿐만 아니라, 서비스의 안전성과 신뢰성, 보안성등을 위한 여러 가지 문제점들을 해결해야 한다.

이의 해결을 위해, IETF AAA 워킹 그룹에서는 기존 AAA 프로토콜인 레디어스를 보완 및 확장하여 새로운 프로토콜인 다이어미터의 표준화를 진행중이고, 기존 전화망에서의 PPP접속 서비스 뿐만아니라 이동 패킷 서비스를 지원하는 Mobile IP 접속 서비스를 지원하도록 설계되고 있다.

이 논문에서는 AAAv6 환경의 서버들이 도메인간의 이동성을 가지는 사용자들에 대해서 안정적으로 서비스할 수 있도록 다이어미터 AAAv6을 확장한 EAP-TLS의 사용자 인증에 필요한 암호 알고리즘을 DSA와 RSA으로 나누어 AAAv6 서버들이 원활하게 서비스를 할 수 있도록 ±1% 미만의 오차범위를 갖는 최적 성능 지표를 구하였다.

실험을 통해 나온 서버 성능지표중에서 DSA와 RSA의 전체 평균처리시간을 시간적측면에서 살펴보면 등록요구 처리전에는 DSA가 RSA보다 약 0.7% 빠르지만 서버의 CPU 처리능력을 70%로 유지하였을때는 RSA가 DSA보다 약 0.32% 빠른 것을 알 수 있다. 3DES 암호알고리즘에 DSA와 RSA를 적용하여 AAA 모델을 확장한 EAP-TLS의 서버 인증 성능 수치값을 실험을 통해 얻음으로써 EAP-TLS 서버들이 Mobile IPv6에서 상호간의 안전한 통신을 제공할 수 있는 개발에 유용하게 이용할 수 있을 것이다.

향후 연구에서는 EAP-TLS이외의 EAP-TTLS, EAP-AKA, LEAP등의 효율성 향상 및 실험등의 연구를 통해 실 세계에 적용 가능한 시스템 개발이 필요할 것이다.

참 고 문 헌

[1] L. J. Blunk, J. R. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)," RFC 2284, March, 1998.

[2] C. Rigney, A. Rubens, W. Simpson, S. Willens, "Remote Authentication Dial in User Service (RADIUS)," RFC2865, June, 2000.

[3] D. Mitton, M. St. Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, B. Wolff, "Authentication, Authorization, and Accounting : Protocol Evaluation," RFC 3127, June, 2001.

[4] P. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A. Rubens, "Diameter Base Protocol," draft-ietf-aaa-Diameter-11.txt, IETF work in progress, June, 2002.

[5] P. Calhoun, W. Bulley, A. Rubens, J. Haag, "Diameter NASREQ Application," IETF work in progress.

[6] P. Calhoun, C. Perkins, "Diameter Mobile IPv4 Application," IETF work in progress, 2002.

[7] P. Calhoun, W. Bulley, S. Farrel, "Diameter CMS Security Application," draft-ietf-aaa-Diameter-cms-sec-05.txt, IETF work in progress, April, 2002.

[8] Pat R. Calhoun, Tony Johansson, Charies E. Perkins, draft-ietf-aaa-diameter-mobile ip-14.txt, "Diameter Mobile IP Application," April, 2003.

[9] P. R. Calhoun, "Diameter Base Protocol," IETF Internet-Draft, draft-ietf-aaa-diameter-08.txt, work in progress, Nov., 2001.

[10] D. Nessett, "Serial Authentication Using EAP-TLS and EAP-MD5," IEEE, 802.11-01/400r22, July, 2001.

[11] T. Dierks, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan., 1999.

[12] Diameter, http://www.linkionary.com/d/diameter.html.

[13] 김현곤, "안전한 이동인터넷을 위한 AAA 서버 기술 개발 및 IMT-2000 시스템 적용을 위한 정보보호 알고리즘 연구", 한국전자통신연구원, 정보통신부, 2002.

[14] Christopher Metz, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," Cisco Systems, http://www.computer.org/internet/v3n6/w6on-wire.htm.

[15] Diameter extends remote authentication, http://www.nwfusion.com/news/tech/0131tech.html#diagram.

[16] Wei Dei, Crypto++ 5.1 Benchmarks http://www.eskimo.com/~weidai/benchmarks.html.

[17] A, Hess, G. Schafer, "Performance Evaluation of AAA," In Proc of 2ND Polish-German Teletraffic Symposium Poland, September, 2002.

[18] Eva Gustafsson, Annika Jonsson, Charles E. Perkins, "Mobile IPv4 Reg. Reg," <draft-ietf-Mobileip-reg-tunnel-06.txt>, March, 2002.

[19] D. B Johnson, "Mobility Support in IPv6" Internet Draft," <draft-ietf-mobileip-ipv6-I6.txt>, http://www.letf.org/march/2002, 2002.

[20] P. Eronen. Ed, T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application," draft-ietf-aaa-eap-02.txt, June, 2003.

[21] C. E. Perkins and David B. Johnson, "mobility support in IPv6," in ACM Mobicom '96, November, 1996.

정 윤 수

e-mail : bukmunro@netsec.cbnu.ac.kr

1998년 청주대학교(이학사)

2000년 충북대학교 대학원 전자계산학과 (이학석사)

2003년~현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사과정

관심분야 : 암호이론, 암호알고리즘, 정보보호, Network Security, 이동통신보안, 전자상거래보안

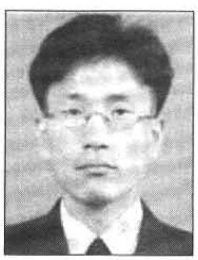
김 형 도

e-mail : archiroad@netsec.cbnu.ac.kr

2001년 충북대학교 건축공학과 공학사

2003년~현재 충북대 전기전자공학부 전자계산학과 석사과정

관심분야 : 인증, AAA, 이동통신보안, ID-Based Cryptography



이 해 동

e-mail : haenamu@etri.re.kr

1999년 경북대학교 컴퓨터과학과 이학사

2001년 경북대학교 컴퓨터과학과 이학석사

2001년~현재 한국전자통신연구원 정보보호연구단연구원

관심분야 : 이동 IP 기반 이동통신 네트워크 보안, 무선 분산 보안, 실시간 시스템

김 현 곤

e-mail : hyungon@etri.re.kr

1992년 금오공과대학교 전자공학과 학사

1994년 금오공과대학교 전자공학과 석사

2003년 충남대학교 전자공학과 박사

1994년~현재 한국전자통신연구원 정보보호연구단 AAA정보보호연구팀장

관심분야 : IP 기반 이동통신 네트워크 보안, 무선 분산 보안

이 상 호

e-mail : shlee@chungbuk.ac.kr

1976년 숭실대학교 전자계산학과 졸업

1981년 숭실대학교 전자계산학과(MS)

1989년 숭실대학교 전자계산학과(PHD)

1976년~1979년 한국전력 전자계산소

1981년~현재 충북대학교 전기전자컴퓨터공학부 & 컴퓨터 정보통신연구소 교수

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture