

논문 2006-43TC-7-6

# 이종 무선 이동망간 통합 인증 및 키관리 기법

## (Integrated Authentication and Key Management Method among Heterogeneous Wireless Mobile Networks)

박형수\*, 이형우\*\*, 이동훈\*

(Hyung-Soo Park, Hyung-Woo Lee, and Dong Hoon Lee)

### 요약

서비스 사업자와 통신 제조업체에 의해 선도되는 새로운 통신 패러다임은 무선 이동 통신망을 All-IP(Internet Protocol) 망으로 빠르게 전환하도록 하고 있다. 이러한 패러다임에서 이종망간 IP의 개방 접근성으로 인해, 가입자에 대한 인증과 세션 키를 제공하는 것이 중요한 연구 과제들 중의 하나가 되었다. 본 논문에서는 이종 무선 이동망들의 인증 처리 절차를 소개하고, 모든 이동 망간 연동을 안전하게 지원하면서, 기존 망에 대한 인증 호환성(Backward Compatibility)을 제공하는 통합 이동 인증 서버(IMAS; Integrated Mobile Authentication Server)를 제안한다. 특별히, IMAS의 디자인에 있어서 무선 인증 상호 연동 기법, 키 관리 기법 및 극복되어야 할 쟁점 사항들을 제시한다. 세션 키를 생성하는 인증 알고리즘의 성능 결과를 분석하고 평가한다. 또한, IMAS의 실험 환경을 구축하여 성능(TPS; Transaction Per Second) 결과를 분석하며 평가한다. IMAS는 기존망의 기능과 효율에 대한 보상없이 이종 무선 이동망 간 연동이 가능하도록 하였고, 분산된 DB(Data Base) 통합으로 인해 망간 데이터 중복성과 불일치성을 줄였다.

### Abstract

The new communication paradigm is rapidly shifted from wireless mobile networks to an All-IP(Internet Protocol) network, led by service industry leaders and communication manufacturers. In this paradigm, providing authentication and session keys of a subscriber becomes one of the critical tasks because of IP open accessibility among heterogeneous networks. In this paper, we introduce authentication process procedure of heterogeneous wireless mobile networks and develop so-called IMAS(Integrated Mobile Authentication Server) which can securely inter-work among all mobile networks and support the legacy networks with backward compatibility. Especially, in designing IMAS, mobile authentication inter-working mechanism, key management technique, and other issues to be overcome are presented. We analyze and evaluate the performance of authentication algorithm which creates session key. A simulation environment of IMAS is established, and a performance(TPS; Transaction Per Second) result is analyzed and evaluated. It turned out that IMAS works among heterogeneous wireless mobile networks without compensating efficiency and functionalities of the legacy networks and decrease the entropy of data redundancy and data inconsistency among networks because of the integrity of the distributed Data Base(DB).

**Keywords:** All-IP Network, Authentication Inter-Working, Heterogeneous Wireless Mobile Networks

## I. 서론

유선의 빠른 전송속도와 무선의 이동성이 결합된 시너지를 바탕으로 신규 통신 서비스 영역을 창출하고 서비스 사용자와 제공자 모두에게 새로운 변화를 가져 올 새로운 패러다임으로 유무선 통합 시대가 전개되고 있다<sup>[1]</sup>. 이러한 상황 속에서 망간 연동 시 망의 보안과 사용자에 대한 권한 검증 및 인증이 중요한 과제로 떠오르고 있다. 적법

\* 정회원, 고려대학교 정보보호대학원  
(Graduate School of Information Security, Korea University)

\*\* 정회원, 한신대학교 컴퓨터 정보 소프트웨어학부  
(Div. of Computer Information and Software, Hanshin University)

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음.  
실험 환경 및 실험은 (주)엔텔리아에서 제공되었음.  
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

한 사용자에게 대한 인증 처리 절차는 개인 정보의 기밀성과 무결성을 보장하며 음성 암호를 통해 개인 사생활 침해를 방지해 준다. 또한, 단말의 불법 복제를 방지하여 흠없는(Seamless) 서비스를 제공할 수 있도록 해 준다.

이동 망간 인증 처리 연동 기법은 2G 이동 통신망에서부터 All-IP망까지 다양한 연구가 진행되어져 왔다. [2]는 단말의 프라이버시와 인증, 이동성 관리, 시스템간 핸드오프에 관한 쟁점 사항들을 제시하였다. 제조업체와 서비스 사업자들이 협력하여 쟁점 사항들을 해결함으로써 흠없는 PCS(Personal Communication Service)를 제공 가능하다고 주장하였다. 특별히, 인증에 있어서 PACS(Personal Access Communications System)이 선택사항으로 지원될 수 있음을 제안하였다. [3]에서는 "Quintet" 인증 벡터가 "Triplet"으로 변환되는 방식을 통해 기존 GSM(Global System for Mobile Telecommunication)망과의 인증 호환성을 제공하였다. 이는 가입자가 3GPP(3rd Generation Partnership Project)망에서 2G GSM망으로 로밍하여 GSM 인증이 필요할 경우 "Quintet-to-Triplet" 변환 방식을 사용하는 것이다. [4]에서는 Milenage<sup>[16]</sup> 알고리즘과 CAVE (Cellular Authentication and Voice Encryption) 알고리즘을 모두 지원하여 ANSI(American National Standards Institute)/3GPP2 망간 인증 연동이 가능하도록 하였다. 3G망과 WLAN(Wireless Local Area Network) 간 인증 연동에 관한 연구들로서, 이동통신망의 CDMA2000 (Code Division Multiple Access 2000)과 WLAN의 통합된 802.1X 기반 인증을 제안하였고<sup>[5]</sup>, 3GPP와 WLAN 간 인증 연동<sup>[6]</sup>이 연구되었다. IP 기반 무선망에서 WLAN 시스템간 인증 연동에 관한 연구도 진행되었다<sup>[17]</sup>.

All-IP 이동망에서 이동 가입자의 인증은 IETF(Internet Engineering Task Force)의 표준인 EAP(Extensible Authentication Protocol)-AKA(Authentication and Key Agreement) 방식<sup>[15]</sup>을 사용한다. 이 방식은 단말과 인증 서버가 동일한 인증키를 안전하게 공유한 후, 인증 절차를 수행한다. 즉, 대칭키 기반의 인증을 수행한다. EAP-AKA 인증 방식은 기존 AKA 인증에 EAP<sup>[14]</sup> 개념을 도입함으로써 사용자의 단일 인증을 통한 편의성, 호환성 및 보안이 한층 강화된 인증 절차를 수행할 수 있다. Base Station(BS)는 사용자의 식별자(Identity)를 EAP-Request/AKA-Identity 메시지를 통해 요구하고 단말기 내의 USIM(Universal Subscriber Identity Module)은 자신의 identity를 EAP-Response/AKA-Identity 메시지에 포함하여 전달한다. 인증 서버

는 해당 메시지를 수신하면 해당 가입자의 권한을 검증한 후, 인증 벡터(Quintet)를 생성하여 EAP-Request/AKA-Challenge 메시지를 통해 중간 노드인 RNC(Radio Network Controller)/SGSN(Serving General Packet Radio Service Support Node), ACR(Access Control Router)에게 전달하고 중간 노드는 인증벡터 중에서 RAND(Random Number)와 AUTN(Authentication Token)을 USIM에게 전달된다. USIM은 AUTN에 포함된 MAC(Message Authentication Code) 값을 검증하고 RES(Result)를 생성하여 중간 노드 또는 인증 서버에게 전송한다. 또한, USIM은 데이터의 기밀성과 무결성을 위한 CK(Ciphering Key)와 IK(Integrated Key)를 생성한다. 중간 노드 또는 인증 서버에서는 저장하고 있는 XRES(Expected Result)와 USIM으로부터 수신한 RES를 비교하여 사용자 인증을 수행한다.

기존 연구에서는 다양한 이동망간 인증 연동을 특정 망간에만 처리하도록 제안했다. 인증 연동이 지원되는 망에서는 무결성과 기밀성이 보장되지만, 인증 연동이 되지 않는 망으로 로밍하여 서비스(데이터 통신, 음성 통화 등)를 받을 경우, 개인 정보 및 사생활이 노출될 수 있다. 본 논문에서는 이러한 취약점을 보완하기 위해 모든 이동망에서 인증 연동을 제공할 수 있는 보다 강력한 IMAS를 구축하여 누구나 어디에서든지 어느 시간에서든지 기밀성과 무결성이 보장된 서비스를 받을 수 있도록 한다.

본 논문의 구성은 다음과 같다. II장에서는 2G와 3G 망에서의 인증 처리 절차를 소개하며, III장에서는 All-IP 망에서 제시되는 인증 처리 절차 및 망간 인증 연동 방안을 소개하고 이를 기반으로 인증 키 관리 방안과 세션 키 생성에 대한 성능을 실험한 결과를 제시하여 이를 분석한다. 또한, 실험 환경을 구축하여 IMAS에 대한 성능(TPS)을 측정하고 이 측정 결과를 분석한다. 구현 과정에서 요구되는 핵심 기술, 쟁점 사항, 그리고 장단점을 제시한다. 결론에서는 논문에서 제시한 인증 서버에 대해 요약하며 향후 연구되어야 할 분야에 대해서 제시한다.

## II. 무선 이동망에서의 인증

### 1. All-IP 기반의 무선 이동망

전세계적으로 통신시장에서 새로운 패러다임으로, IP 기반으로 하는 네트워킹이 주요 연구 과제로 부각되고 있다. 이러한 네트워킹을 기반으로 제안된 시스템이 바로 3GPP의 IMS (Internet Protocol Multimedia Sub-

system)<sup>[9]</sup>와 3GPP2의 MMD(Multi Media Domain)<sup>[10]</sup>다. 이동성과 IP 망과의 통합 기술은 미래에 새로운 서비스 창출에 결정적인 역할을 담당하게 될 것이다.

그림 1-a는 3GPP망과 IMS를 나타낸 것으로, 유럽 방식의 비동기 시스템은 ETSI(European Telecommunications Standards Institute)/3GPP에서 표준화를 추진하고 있다. 북미 방식의 동기시스템은 TIA (Telecommunications Industry Association)/EIA (Electronics Industries Alliance)/3GPP2의 표준화 기구에 의해 표준화가 진행된다. 기존 3G 이동 통신망에서 이동 단말은 RAN(Radio Access Network) /SGSN을 통해 HSS (Home Subscriber Server) 또는 HLR(Home Location Register)에 위치 등록된다. 이와 동시에, IMS에서는 PDP(Packet Data Protocol) 연결을 활성화하는 동안에 GGSN(Gateway GPRS Support Node)/P-CSCF/I-CSCF/S-CSCF(Proxy/Interrogating /Serving-Call Session Control Function)를 통해 위치 등록된다. 이동 단말이 동영상 호를 발신하거나 착신하게 되면, RAN/MRF(Media Resource Function) /MGW(Media Gateway)를 통해 실제 동영상 데이터 트래픽이 설정된다. 이를 제어하기 위한 신호 메시지는 CSCF/MRFC (Media Resource Function Controller/MGCF(Media Gateway Control Function) 등을 통해 전달된다. HSS는 위치 등록 및 호 처리 과정 중에 가입자의 권한 검증 및 인증 절차를 수행하고, AS (Application Server)는 CSCF와 신호 메시지를 송수신하며 지능망 서비스와 같은 서비스를 제어한다. PSTN(Public Switched Telephone Network), ADSL (Asymmetric Digital Subscriber Line), PLMN(Public Land Mobile Network)과의 연동은 MGW(Media Gateway)/BG(Border Gateway)/SGW (Signaling Gateway)을 통해 처리된다. MMD는 IMS를 기본 모델로 하여 동기망에 적합하도록 수정/제안된 All-IP 망이다. 이는 기본 서비스 처리 절차는 동일하며 무선 처리 방식과 패킷 구조가 상이하다. 그림에서 할 수 있듯이, 망 구조가 거의 동일하며 단지 패킷 데이터 망의 구조만 다르다. 이 그림 1-b는 3GPP2망과 MMD를 표현한 것이다. IEEE 802.16에서 표준화된 OFDMA(Orthogonal Frequency Division Multiple Access) 무선 방식을 사용하여 단말간 데이터 및 VoIP 통신을 가능하도록 하는 망(그림 1-c)으로서, WiBRO (WiMAX<sup>[11]</sup>)가 있다. 그림 1-c에서 RAS (Radio Access Station)는 이동 통신망의 무선 접근망

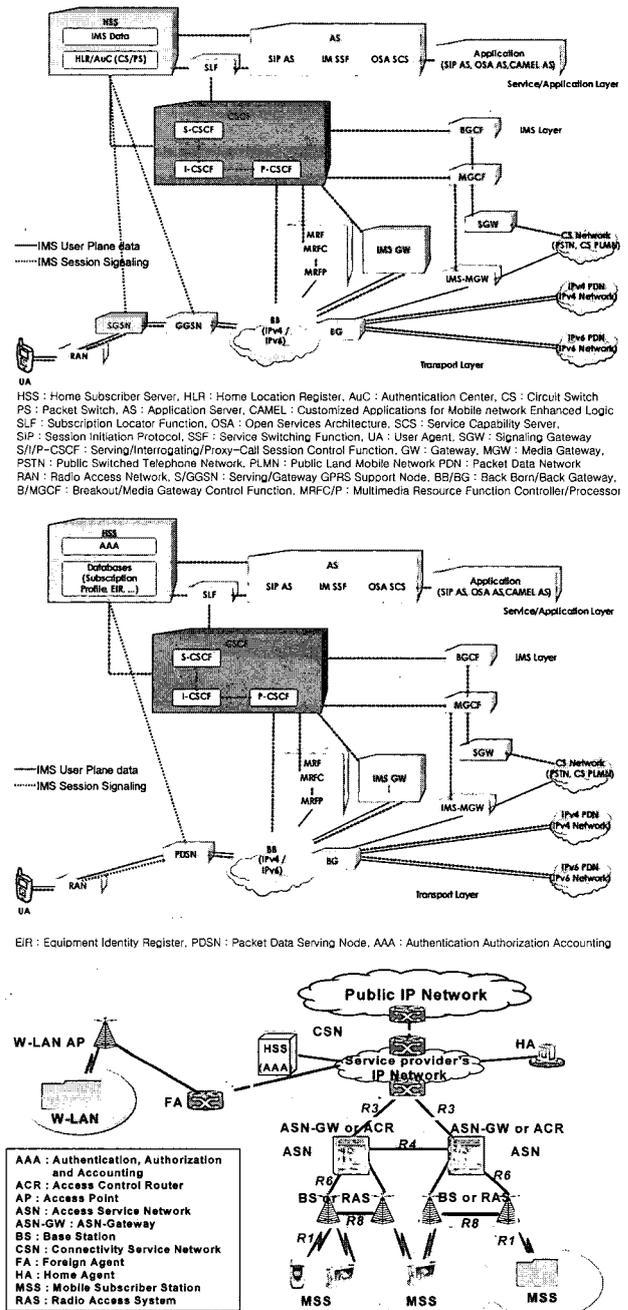


그림 1. 무선 이동망(위로부터): (a) 3GPP의 IMS, (b) 3GPP2의 MMD, (c) WiBRO(WiMAX) or WLAN  
 Fig. 1. Wireless Mobile Networks (from upper): (a) IMS in 3GPP, (b) MMD in 3GPP2, (c) WiBRO(WiMAX) or WLAN.

으로서, 3GPP 이동통신망의 Node-B에 해당되며, ACR은 데이터를 전송/제어하는 핵심 노드로서, 이동통신의 핵심망의 요소인 RNC, CSCF(Call Session Control Function), 그리고 GGSN에 해당된다. MSS (Mobile Subscriber Station)는 무선 접근망인 BS (Base Station) 또는 RAS를 통해 패킷 데이터를 ASN-GW(Access Service Network Gateway) 또는

ACR(Access Control Router)에게 전달하고, ASN-GW는 외부망과 연동하거나 다른 ASN-GW를 통해 트래픽 경로를 설정하여 착신지에 데이터를 전달한다.

2. 이동망에서의 인증

가. GSM

인증키는 각 SIM(Subscriber Identity Module)마다 저장되어 있는 고유한 비밀 Key이다. 단말기 인증 시, network에서는 Random Number를 단말기로 전송하고 단말기는 이를 SIM으로 전송한다. SIM에서는 인증키와 Random Number를 입력으로 A3 알고리즘을 수행하여 결과값(SRES)을 생성한다. 생성한 SRES를 network으로 전송하면 VLR(Visited Location Register)에서 검증을 한다. 인증서버에서 생성하여 VLR로 전송하는 파라미터를 Triplet이라 하며, 이는 Random Number, SRES, KC를 말한다. 현재, GSM에서 사용하는 A3/A8 알고리즘은 표준화되어 있는 알고리즘을 사용한다<sup>[3]</sup>. 그러나 표준화 되어 있는 A3/A8 알고리즘은 비도 등의 문제가 제기되어 자신들의 알고리즘을 따로 선택하여 사용하는 사업자들도 존재한다.

나. ANSI

ANSI 인증 절차는 Global challenge를 사용하는 것을 특징으로 한다. 단말기는 기지국에서 항상 Broadcasting 하는 RAND(Random Number)를 주기적으로 수신하여 등록, 발호, 착호 시에 생성하는 인증벡터(AUTHR)를 계산하는데 사용한다. AUTHR은 세션키인 SSD(Shared Secret Data), MIN(Mobile Identification Number), Electronic Serial Number(ESN), RAND을 입력 파라미터로 사용하는 CAVE 알고리즘에 의해 생성된다. 이는 단말과 인증서버(SSD share mode인 경우는 VLR)에서 생성되어지며 인증 성공 여부를 결정하는 결과값이다.<sup>[18]</sup>

다. 3GPP

UMTS(Universal Mobile Telecommunications System)의 인증은 GSM의 Unique Challenge처럼 시스템에서 단말만 인증 하는 것이 아니라, 단말에서 시스템도 인증하는 상호인증(Mutual Authentication)을 사용한다. Quintet는 인증서버에서 생성하여 VLR로 전송되는 것으로 RAND, XRES, CK, IK, AUTN을 말한다. f1~ f5는 해당 파라미터를 생성하는데 사용되는 알고리즘이다. 현재 UMTS에서 필요한 알고리즘은 f0~f10, f1\*, f5\* 총

13개가 필요하며 인증서버에서는 f0~f5, f1\* 7개의 알고리즘이 필요하다<sup>[3, 7, 16]</sup>.

라. 3GPP2

해당 인증 기능은 기본적으로 3GPP와 동일하며, AKA/ESA를 지원하지 못할 경우 ANSI 인증 기법으로 처리하게 된다<sup>[4]</sup>.

마. WiBRO(WiMAX)

WiBRO(WiMAX)에서의 인증은 EAP-AKA 또는 PKI(Public Key Infrastructure) 인증 방식을 사용한다. 3 Party Authentication Model을 기본으로 하며, 3 Party는 인증 요청을 하는 MSS(Suppliant), MSS와 실제 인증 절차를 수행하는 BS(Authenticator), 인증 키 관리 및 인증 벡터를 생성하는 AAA(Authentication Server)로 구성된다<sup>[8]</sup>.

3. 이동망에서의 인증 처리 비교

GSM 인증은 Unique Challenge를 이용한다. GSM에서는 망이 단말을 인증하는 Unique Challenge만을 사용하지만, 3GPP에서는 인증 기능을 강화하여 망과 이동단말이 상호 인증하는 Mutual Authentication을 지원한다. ANSI-41은 Global Challenge를 기본으로 한다. 기지국에서 항상 Broadcast하는 Random Number를 단말기가 수신하여 저장하고, 인증이 필요한 경우 이를 사용한다. 이의 장점은 GSM보다 Random Number를 전송하는 부하를 줄일 수 있다. 그러나 전체적인 인증 절차를 살펴보면 ANSI-41의 부가적인 인증 절차로 인하여 이러한 장점이 상쇄된다. 3GPP2의 인증절차는 3GPP 인증 절차에 따라 동일한 방법으로 표준화 되었다. 3GPP/3GPP2의 인증 절차가 동일해짐에 따라 상호 연동에 장애가 되어온 인증 문제가 해결되었다. 또한, WiBRO(WiMAX) 인증 절차에 있어서도 EAP-AKA 인증 방식으로 처리

표 1. 이동망에서의 인증 기법 비교

Table 1. Comparison of Authentication Method in Mobile Networks.

Auth.	GSM	ANSI	3GPP	3GPP2	IMS	MMD	WiBRO (WiMAX)
Method	Unique Challenge	Global Challenge	EAP-AKA	EAP-AKA	IMS-AKA	MMD-AKA	EAP-AKA or PKI
Protocol	MAP	MAP	MAP	MAP	Diameter	Diameter	Diameter
Algorithm	A3/A8	CAVE	MILE NAGE	ECA	MILE NAGE	ECA	ECA

\* IMS-AKS, MMD-AKA : UMTA-AKA over IP

\* ECA : Enhanced Cryptography Algorithm

되기 때문에 망간 인증 상호 연동 처리에 있어서도 상호 호환이 가능할 수 있다. 표 1은 각각의 이동망에서 사용되고 있는 인증 기법, 알고리즘, 그리고 프로토콜을 정리한 것이다.

### Ⅲ . 무선 이동 통신망간 통합 인증

#### 1. 망 참조 모델

본 논문에서 제안한 IMAS를 위한 망 참조 모델은 그림 2와 같다. IMAS는 모든 이동망과 연동되어 인증 기능이 제공된다. 각 망으로부터 이동 단말의 위치 등록 및 호 처리 요구를 받으면, 가입자 인증 절차를 수행하게 된다. CSN(Connectivity Service Network)은 IMAS를 통해 각 망에 적절한 인증 처리를 수행하는 제 3의 사업자 망이다. 3GPP/3GPP2/ANSI/GSM 망은 이동 통신망으로서, SS7(Signaling System No. 7) 프로토콜을 사용하기 때문에 반드시 CSN의 IP망과 연동을 가능하도록 처리해주는 SGW가 필요하다.

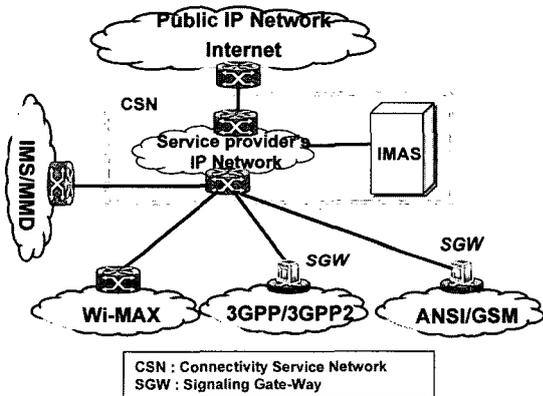


그림 2. 통합 인증을 위한 망 참조 모델  
Fig. 2. Network Reference Model for Integrated Authentication.

#### 2. 전제 조건 및 요구 사항

##### 가. 전제 조건

IMAS는 여러 이동망과 연동되어야 하므로 이 연동을 위해서 전제 조건들이 충족되어야 한다.

망간 서비스 제공자가 서로 다를 경우, 로밍 규약이 체결되어져 있어야 한다. 각망은 IMAS와 직접적으로 연결하여 안정된 환경 하에서 메시지를 송수신할 수 있어야 한다. 로밍망과 홈망간 인증 시, 단말과 인증 서버에서

제공되는 메시지는 투명하게 전달되어야 한다. 각 망에 로밍되어 있는 단말에는 해당 망에서 필요로 하는 인증 처리 절차를 수행할 수 있어야 한다. (e.g. 단말이 2G GSM 망으로 로밍되어 있을 경우, A3/A8 인증 모듈이 제공되어야 한다.)

#### 나. 요구 사항 및 구현 메커니즘

위에서 제시한 전제 조건들과 더불어 통합 인증 서버를 구현하기 위해서는 필수 요구 사항들과 이에 대한 구현 메커니즘들이 필요하다. 그림 3은 IMAS 구조도를 표현한 것이다. 그림 3에서 IMAS는 각 망으로부터 요구된 인증 메시지를 송수하는 프로토콜 스택부와 인증 요구 메시지를 처리하는 응용 처리부, 그리고 해당 메시지를 처리하기 위해 필요한 가입자 정보를 저장/관리하는 DB부로 구성된다. 특히, 응용 처리부는 해당 인증 요구 메시지를 분석하여 적절한 인증 알고리즘을 수행하여 인증 벡터를 생성한다. 프로토콜 스택부는 IP/SCTP (Stream Control Transmission Protocol)/M3UA (Message Transfer Part 3 User Application)/SCCP(SS7 Signaling Connection Control Part)와 Diameter Base Protocol로 구성되고, 응용 처리부는 TCAP(Transaction Capability Application Part)/ASE (Application Service Elements)/Cx Command Applications)으로 구성된다. 응용 처리부의 인증 모듈에서는 망에서 필요한 모든 인증 알고리즘과 처리 절차를 제공한다.

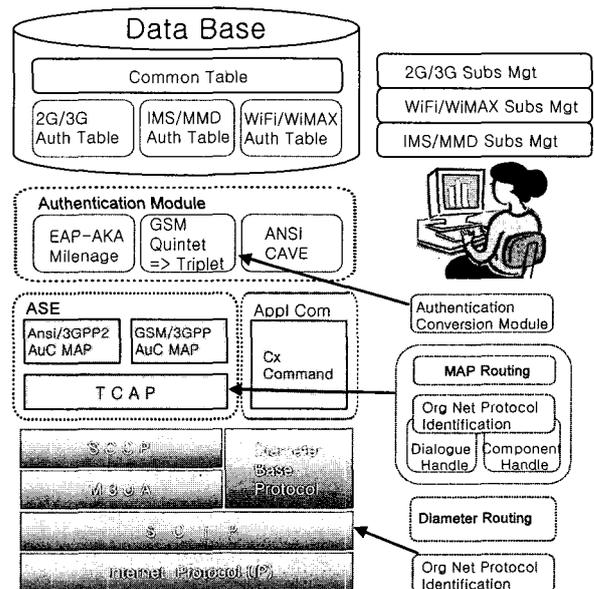


그림 3. 통합 인증 서버 구조도  
Fig. 3. IMAS Structure Diagram.

(1) DB부의 가입자 관리

가입자 구성 정보는 크게 네 부류로 구성된다. 로밍 시 망의 정보를 확인하는 공통 테이블, ANSI/3GPP2 인증 정보 테이블, GSM/3GPP 인증 정보 테이블, 그리고 WiBRO(WiMAX) 인증 정보 테이블로 구성된다. 각 테이블에는 연동 서비스에 요구되어지는 정보를 포함하고 있다. 각 테이블에서 사용되는 가입자 식별 번호는 Primary Key로서 사용되어지고 이를 기반으로 가입자를 관리한다.

(2) 응용 처리부의 프로토콜 식별/분배

대국으로부터 수신된 TCAP 메시지는 DHA(Dialogue Handle)와 CHA(Component Handle) 기능블록에서 처리된 후, 프로토콜 식별부(Origination Network Protocol Identification)로 전달된다. MAP(Mobile Application Part) 프로토콜 식별 기능은 수신된 TCAP 메시지에 대화부(Dialogue Portion) 포함 여부에 따라 수신된 TCAP 메시지가 ANSI/3GPP2 망으로부터 수신된 것인지 GSM/3GPP 망으로부터 수신된 것인지를 판단할 수 있다. TCAP이 수신된 메시지를 식별하게 되면 상위 계층(MAP)으로 메시지를 전달하거나 SCCP에게 전달하게 된다. MAP은 동일한 기능을 수행하는 여러 개(이중화 또는 다중화)의 프로세스로 구성된다. 따라서 TCAP과 MAP은 1:M 매핑 관계를 갖는다. TCAP은 MAP과 메시지를 송수신할 때 Modulo 연산 방식을 사용하여 처리한다. Diameter Base Protocol<sup>[13]</sup>도 상위 계층(Cx Command Application)에게 메시지를 분배할 때, TCAP에서 처리하는 동일한 방식으로 처리한다. 해당 요구 사항은 "MAP/Diameter Routing" 모듈과 TCAP의 "Org Net Protocol Identification" 모듈에서 구현된다.

(3) 응용 처리부의 기존망과의 인증 호환성

로밍한 망이 2G 망일 경우 2G 인증 절차가 수행되어야 한다. 가입자가 ANSI 망으로 로밍하였을 경우 인증 서버는 CAVE 알고리즘을 이용한 인증 절차를 수행하고 GSM 망으로 로밍하였을 경우 Milenage 알고리즘에 의해 Quintet 인증 벡터를 생성하고 이 벡터를 Triplet으로 변경하여 처리한다<sup>[3]</sup>. 이에 대한 처리는 "Authentication Conversion Module"과 "Authentication Algorithm Module"이 담당하게 된다.

(4) 프로토콜 스택부의 SCTP에 의한 ASP 식별

SCTP<sup>[12]</sup> 상위 계층의 Application에서 상대 노드와 연결하고자 할 때, 반드시 자신의 IP 주소, 상대 노드의 주소, 포트 번호가 요구된다. 이 세 파라미터는 유일한 Association ID를 생성하게 된다. 이후 해당 연결을 통해 메시지가 송수신되어질 때 Association ID는 반드시 포함되어진다. SCTP는 메시지를 수신하였을 경우, 해당 메시지에 포함된 Association ID를 검사하여 어떤 ASP(Application Service Part)에게 전달할지를 알 수 있다. SCTP의 Application에서 메시지를 송신할 경우 application 자신의 Association ID를 제공하고 SCTP는 해당 Association ID에 해당하는 착신지 IP 주소와 포트를 통해 메시지를 상대 노드에게 전송한다. 따라서, SCTP에서는 다중의 ASP에게 적절한 메시지를 전달하기 위해(일명, Multi-Path Function) 세 파라미터(발신 IP 주소, 착신 IP 주소, 포트 번호)와 Association ID간 매핑 테이블이 관리되어야 한다. 이 매핑 테이블은 연결 상태에 따라 동적으로 생성되고 삭제된다. IP 기반의 인증 메시지를 받게 되면 SCTP는 발신 이동망을 구별하여 해당 메시지를 처리할 수 있는 Application으로 메시지를 처리하고 Application에서는 그 메시지에 일치되는 인증 알고리즘을 수행시켜 인증 처리 절차를 수행한다. 해당 요구 사항은 SCTP의 "Org Net Protocol Identification"에서 처리하게 된다.

다. 인증 처리 절차

IMAS는 여러 이동망과 연동하여 인증 메시지를 처리할 수 있다. IMAS는 인증 메시지 송수신 시 상대망의 노드를 구분하여 적절한 인증 절차를 수행한다. 그림 4는

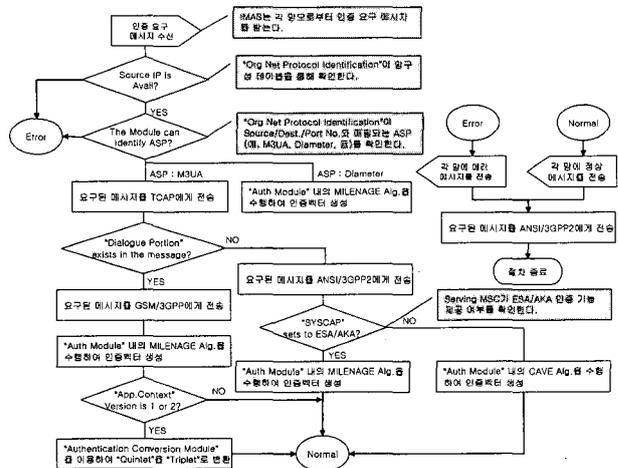


그림 4. 인증 요구 메시지 처리 흐름도  
Fig. 4. Flow Chart of Authentication Request Message.

인증 메시지 송수신 시 시스템 간 인증 처리 절차를 처리 흐름도로 나타낸 것이다.

그림 4에서 IMAS가 각 이동망으로부터 인증 요구 메시지를 수신하면 SCTP 계층에서는 해당 메시지가 처리 가능한지 확인하고 발신지 주소를 가진 노드와 메시지 교환이 가능한지를 확인한다. 이 조건을 모두 만족하면 해당 메시지가 발/착신지 주소 및 포트 번호에 유일하게 매핑되어 있는 ASP를 식별하여 해당 ASP에게 메시지를 전달한다. M3UA 또는 Diameter는 해당 메시지를 적당한 인증 모듈과 함께 처리한다. ASP가 Diameter일 경우 Milenage 알고리즘 또는 ECA(Enhanced Cryptography Algorithm)를 이용하여 인증벡터를 생성하고, M3UA인 경우에는 SCCP를 경유해서 TCAP 계층에게 해당 메시지를 전송한다. TCAP 헤더 데이터 구조 내에 "Dialogue Portion"이 포함되어 있으면 GSM/3GPP MAP에게 메시지를 전송하고 그렇지 않으면 ANSI/3GPP2 MAP에게 전달한다. GSM/3GPP에서는 Milenage 알고리즘을 이용하여 Quintet 인증 벡터를 생성한다. "Application Context Version"이 1 또는 2일 경우 "Quintet"를 "Triplet"으로 변경한다. ANSI/3GPP2에서는 요구된 메시지 내에 포함된 "SYSCAP(System Capability)" 파라미터에 방문망의 교환기가 ESA(Enhanced Subscriber Authentication)/AKA 기능을 지원할 수 있다는 지시자를 포함하고 있으면, ECA를 사용하고 그렇지 않으면 CAVE 알고리즘을 사용하여 인증 데이터를 생성한다.

### 3. 인증키와 세션 키 관리 기법

일반적으로 가입자 인증을 위한 마스터 키(Authentication Key)를 단말 생산 시에 주입하고, 해당 단말이 특정가입자에게 배송될 때 사업자 전용망의 Secure Channel을 통해 고객 센터로부터 인증 서버에 가입자 식별자와 함께 등록된다. 인증 키는 단순한 문자열로 DB에 저장되지 않고 사업자 고유의 암호 기법에 의해 암호화하여 DB에 저장된다. 이는 인증키가 네트워크 상에서 유출되어도 키의 기밀성을 보장하기 위함이다. 적법한 사용자가 마스터 키를 확인하고자 할 경우 해당 가입자 ID에 해당하는 암호화된 키 데이터를 복호화하여 평문의 마스터 키를 확인할 수 있다. 사용자가 DB에 질의 요청을 하는 과정에 있어서도 다단계의 접근권한 체계를 통해 가능할 수 있다. 먼저, 운용자는 시스템 운영 체제 레벨의 패스워드 기반보안 체계를 통과하고 운용자 ID와 패스워드를 입력하여 어플리케이션에서 제공하는 OMC(Operation Maintenance Center)의 Main Panel에

정상적으로 로그인한 후, 자신의 클래스에 해당하는 명령어를 수행하여 운영자가 원하는 정보를 검색 또는 변경할 수 있다. 세션 키는 마스터 인증 키와 인증 알고리즘에 의해 생성된다. 이 세션 키는 가입자의 인증 데이터 요구 시 생성되어지고, 다음 인증 데이터 요구 시점까지 DB에 저장되어 관리된다. 여기서, 세션 키는 CK와 IK를 의미하고 보다 넓은 의미에서는 인증 벡터 Quintet을 의미한다. Quintet은 단말이 위치 등록, 발호, 착호 등 이벤트가 발생될 때마다 한번 사용되고 폐기된다.

### 4. 기존 연구와의 비교

표 2는 기존 연구에서 처리 가능한 인증 방식을 IMAS와 비교하여 나타낸 것이다. [2]에서는 기존 2G 세대의 이동 통신망 간 인증 연동 기능만을 지원한다. [3, 4]에서는 각각 북미 방식과 유럽 방식의 인증 방식만을 제공한다. [5, 6, 8]에서는 3G와 All-IP망 및 WiBRO(WiMAX) 또는 WLAN간 인증 연동이 가능하도록 제안하였다. 본 논문에서 제안한 IMAS에서는 각 망에서 요구하는 모든 인증 방식을 지원하여 연동할 수 있도록 제안되었다.

본 논문에서 제안한 IMAS는 몇 가지 장점이 있다. IMAS는 분산된 DB에 대해 효율적인 통합 관리가 가능하다. 각각의 망별로 필요한 인증 서버가 분리되어 있으면, 각 서버 간 중복된 정보(망 정보, 가입자 ID 정보 등)가 발생하게 된다. 또한, 고객 센터에서 가입자 등록 시,

표 2. 기존 연구와 IMAS의 인증 연동 비교  
Table 2. Comparison of Authentication Inter-working Capabilities with related works.

Works	G S M	A N S I	3 G P P	3 G P P2	I M S	M M D	WiBRO (WiMAX) or WLAN
Vijay <sup>[2]</sup>	FS	FS					
TS33 <sup>[3]</sup>	FS		FS		FS		
X.S <sup>[4]</sup>		FS		FS		FS	
Amresh <sup>[5]</sup>				FS		FS	PS
Kalle <sup>[6]</sup>			FS		FS		PS
WiMAX <sup>[8]</sup>			PS	PS	PS	PS	FS
IMAS	FS	FS	FS	FS	FS	FS	FS

\* FS : Fully Supported PS : Partially Supported

분리된 노드 개수만큼의 provisioning 메시지가 이루어져야 하며, 노드 간의 정보 불일치 가능성(Entropy)이 높아진다.

IMAS은 망의 노드 관리가 단순해지며 장애 복구 및 대처가 빠르다. 상용망을 운용하게 되면 다양한 종류의 장애 (천재지변에 의한 정전, 디스크 또는 메모리의 물리적인 H/W 장애, S/W 장애 등)들을 피할 수 없다. 이에 대한 대비는 필수적이다. 이동 통신망에서 발생한 장애는 단순히 한 노드에서 발생한 장애도 있지만, 대부분 여러 다른 노드들과 관계가 있다. 이러한 장애가 발생하였을 경우 망의 구조가 복잡하면 장애 복구가 어려워진다. 이로 인해 망의 단순화는 필수적이다. IMAS는 이러한 망의 단순성을 제공하고 각 망에서 요구하는 인증 인터페이스를 시스템 내부에서 제공함으로써 장애에 신속한 대응이 가능하다. 또한, NMS에서 여러 개의 인증서버들을 관리하는 불편함을 해소해 준다. 반면에, IMAS의 DB 통합은 시스템 장애 발생 시, 망과 서비스에 큰 영향을 미치게 된다. 따라서, IMAS 시스템 구성은 반드시 이중화(고장 감내형 또는 고가용성) 및 최소한 "N+1" 백업으로 구성되어야 한다.

#### IV. 성능 실험 및 평가

##### 1. 세션 키 생성 성능 실험 및 평가

마스터 키를 이용한 세션 키 CK, IK 생성은 Milenage 알고리즘이 사용된다. Milenage 알고리즘 f1 ~ f5을 이용하여 세션 키를 생성하는 실험을 진행하였다. 실험을 위한 환경은 SUN 시스템 450MHz 2 CPU를 사용하였고 운영 체제는 UNIX Solaris 2.5를 사용하였다. 해당 실험에서는 알고리즘의 암호화 및 복호화 절차가 정상적으로 수행되는지를 3GPP TS(Technical Specification) 35.205 ~ 208<sup>[16]</sup> 규격에서 제공한 표본 데이터를 이용하여 확인하였고 최종적으로 세션키를 10,000번 생성시켜 소요된 시간을 확인하였다. 10,000개의 인증 벡터를 생성하는데 걸리는 시간은 1.11sec이다. 이는 인증 서버에 일반 명의 가입자가 동시에 세션 키 생성을 요청해도 충분히 처리할 수 있음을 의미한다. 만약, 한 가입자가 n개의 세션 키 생성을 요구할 경우 동시에 10,000/n 명의 가입자 요구를 처리할 수 있다.

##### 2. 시스템 성능 실험 및 평가

###### 가. 실험 환경

본 논문에서 제안한 IMAS에 대한 성능 시험을 세 가

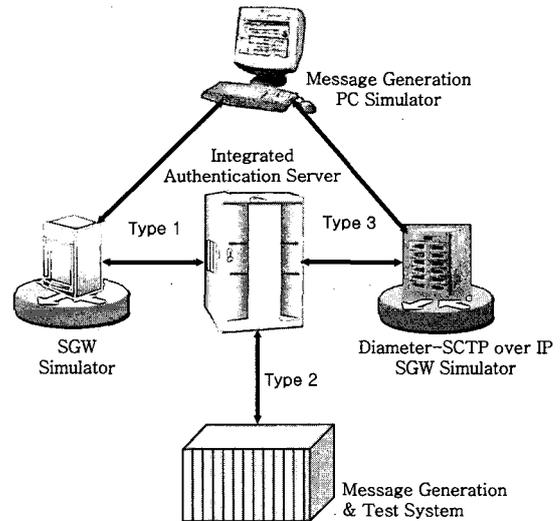


그림 5. 시험 환경  
Fig. 5. Simulation Configuration.

지 시뮬레이션 환경으로 구성하여 실시하였다. 그림 5는 성능 시험 환경을 나타낸 것이다. Type-1은 ANSI 망에서 CAVE 알고리즘을 이용한 인증 절차를 SGW 시뮬레이터를 통해 진행하였고 Type-2는 3G 망에서 EAP-AKA 인증 방식을 이용해 성능 검증용 테스트 장비(MGTS; Message Generation Test System)를 이용하여 성능을 측정하였다. 마지막으로, Type-3는 SIG-TRAN(Signaling Transport) Stack (SCTP over IP) 기반으로 Diameter 프로토콜을 이용하여 EAP-AKA 인증 처리에 대한 성능 측정하였다. Type-3 실험에서는 메시지의 크기를 변경하면서 성능 실험을 진행하였다.

###### 나. 성능 실험 및 평가

그림 6은 IMAS에 대한 세 가지 실험 결과를 도표로 나타낸 것이다.

Type-1 실험 결과에서는 1,000 Transaction Per Second(TPS) 처리 시 CPU 사용률이 40% 정도됨을 알 수 있다. Type-2에서는 1,700 TPS까지 실험을 진행하였고 이 경우 CPU 사용률이 60% 정도됨을 확인할 수 있었다. Type-2에서는 Application을 구분하여 CPU 사용률을 측정했다. 이 경우 프로토콜 스택의 CPU 사용률이 31%, TCAP & MAP이 13%, 시스템 영역이 16%가 됨을 알 수 있었다. Type-3 성능 시험에서는 사이즈별 성능 시험을 측정했는데, 사이즈가 가장 작을 때(1KB) TPS가 가장 높음을 알 수 있었다. 사이즈가 커지면 CPU 사용률에 관계없이 낮은 TPS에서도 메시지 유실이 발생함을 확인하였다. 이는 메시지 전송 시, OS에서 사용하는 Low Socket Buffer 크기의 제한 때문이다. 성능 실험 결과,

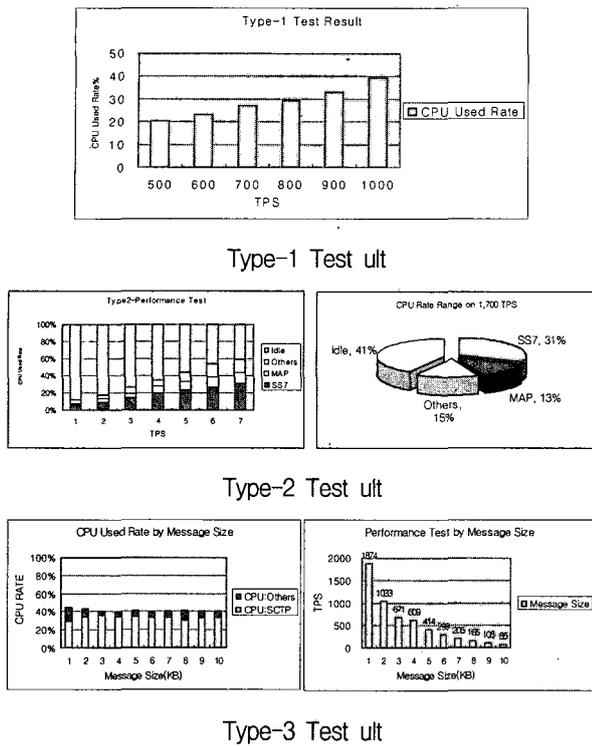


그림 6. 시스템 실험 결과  
Fig. 6. Performance Test Result.

IMAS는 기존 2G 망의 인증뿐 아니라, 3G 인증, All-IP 기반 인증을 동시에 지원할 수 있고, Wi-BRO (Wi-MAX)에서도 인증 처리 절차를 수행할 수 있음을 알 수 있었다.

### V. 결 론

본 논문에서는 기존 2G망과 3G망에 대한 인증 및 보안에 대해 고찰하였고, 이를 바탕으로 All-IP망에서 기존 망에 대한 인증 호환성(Backward Compatibility)을 제공하면서 인터넷 망과의 보안 처리 방안을 제안하였다. 본 연구에서 제안한 IMAS를 통해 비동기망 3GPP 기반의 IMS, 동기망 3GPP2 기반의 MMD, 그리고 WiBRO (WiMAX)간의 상호 인증 기법 및 쟁점 사항들을 제시하였고, 인증키를 기반으로 생성된 세션 키 관리 기법과 암호 알고리즘에 대한 성능 자료를 제시하였으며 이를 분석하고 평가하였다. 또한, 여러 망의 가입자 인증 절차를 수행하는 IMAS에 대해 장단점을 제시하였으며, 시뮬레이션 환경을 구축하여 성능(Transaction Per Second; TPS) 결과를 제시하였고, 이를 분석하여 평가하였다. 추후, 무선 이동통신의 Radio Access Network에서 직접 Public IP Network (Internet)을 접근할 때 요구되는 구

체적인 인증 처리 절차에 대한 연구가 진행될 것이다.

### 참 고 문 헌

- [1] Dong-Hoon Yang; Seongcheol Kim; Changi Nam; Ji-Sook Moon, "Fixed and mobile service convergence and reconfiguration of telecommunications value chains," Wireless Communications, IEEE, Volume 11, Issue 5, Oct. 2004.
- [2] Vijay K. Garg and Joseph E. Wilkes, "Interworking and Interoperability Issues for North American PCS," IEEE Communications Magazine, Volume 34, Issue 3, PP. 94-99, March 1996.
- [3] 3GPP TS 33.102, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture(Release 6)," V6.3.0, Dec 2004.
- [4] 3GPP2 X.S0006, "MAP Support of Authentication and Key Agreement (AKA)," v1.0, October 2005.
- [5] Amh Mahapatra, R. Uma, "Authentication in an Integrated 802.1X based WLAN AND CDMA 2000-1X network," IEEE Communications Magazine, November 2003.
- [6] Kalle Ahmavaara, Henry Haverinen, and Roman Pichna, "Interworking Architecture Between 3GPP and WLAN Systems," IEEE Communications Magazine, Volume 41, Issue 11, PP. 74-81, November 2003.
- [7] 3GPP TS 33.105, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic algorithm requirements (Release 6)," V6.0.0, June 2004.
- [8] WiMAX Forum, "WiMAX Stage 2 EAP Architecture: Three-party Authentication Model," June 2005.
- [9] Miiikka Poikselk, Georg Mayer, Hisham Khartabil and Aki Niemi, "The IMS IP Multimedia Concepts and Services in the Mobile Domain," John Wiley & Sons, Ltd, 2004.
- [10] 3GPP2 X.S0013, "All-IP Core Network Multimedia Domain," July, 2005.
- [11] WiMAX Forum, "WiMAX End-to-End Network Systems Architecture," June 2005.
- [12] R. Stewart et al. "Stream Control Transmission Protocol," RFC-2960, IETF, October 2000.
- [13] P. Calhoun et al. "Diameter Base Protocol," RFC-3588, IETF, September 2003.
- [14] B. Aboba et al. "Extensible Authentication Protocol (EAP)," RFC-3748, IETF, June 2004.
- [15] J. Arkko and H. Haverinen, "Extensible Authen-

Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC-4187, IETF, January 200

[16] 3GPP TS 35.205~208, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1\*, f2, f3, f4, f5 and f5\*; Document 1: General," V6.0.0, December 2004.

[17] W. Y. Lee, "Authentication Inter-working Methods between Wireless LAN Systems," Proceeding (464) Networks and Communication Systems, March. 2005.

[18] Snyder, Randall A., "Wireless Telecommunications Networking with ANSI-41," McGraw-Hill, 2/E, January 2000.

저 자 소 개



박 형 수(정회원)  
 1992년 고려대학교 전산학과 학사 졸업.  
 1995년 고려대학교 전산학과 석사 졸업.  
 2005년 고려대학교 정보보호 대학원 박사 수료.

1995년~2002년 LG 전자 선임 연구원  
 2003년~현재 (주)엔텔리아 개발팀장  
 <주관심분야 : 정보보호, 무선이동통신, 네트워크 보안, 데이터 베이스, 홈네트워크>



이 형 우(정회원)  
 1994년 고려대학교 전산학과 학사 졸업  
 1996년 고려대학교 전산학과 석사 졸업.  
 2004년 고려대학교 전산학과 박사 졸업.

1999년~2003년 2월 천안대학교 정보통신학부 조교수  
 2003년~현재 한신대학교 컴퓨터 정보소프트웨어 학부 부교수  
 <주관심분야 : 정보보호, 네트워크 보안, 해킹/바이러스, 스테가노그래피, 컴퓨터 포렌식>



이 동 훈(정회원)  
 1984년 고려대학교 경제학 학사 졸업.  
 1987년 University of Oklahoma Computer Science 석사 졸업.  
 1992년 University of Oklahoma Computer Science 박사 졸업.

1993년~2001년 고려대학교 전산학과 부교수  
 2001년~현재 고려대학교 정보보호대학원 교수  
 <주관심분야 : 정보보호, 암호 프로토콜, RFID, 유비쿼터스, 센서 네트워크>