유비쿼터스 무선환경을 위한 개인 상호인증 시스템☆

Personal Mutual Authentication System for Ubiquitous Wireless Environments

김 병 기* 홍 상 선** 전 영 길***
Byung-Gi Kim Sang-Sun Hong Young-Keel Jouhn

요 약

컴퓨터 네트워크에서 고려해야 할 두 가지 중요한 보안 문제는 안전한 자료 전송과 사용자 인증에 관한 것이다. 특히 무선 LAN에서는 이 문제가 더욱 심각하기 때문에, 무선 LAN을 기반으로 하는 개인 네트워크 환경과 유비쿼터스 네트워크에서 보안 문제가 중요한 이슈로 떠오르고 있다.

본 논문에서는 이런 환경에서 이용 가능한 인증 시스템인 UPMA(Ubiquitous Personal Mutual Authentication) 모델을 제안한다. UPMA 모델은 각 시스템에 대해 개인의 확인이 가능한 인증구조를 지원한다. 세션 키 설정 과정을 통하여 통신 내용을 기밀화하고, 통신자 각각의 장비와 사용자를 확인함으로써 상호 동등한 인증을 수행한다.

제안하는 방법은 네트워크를 통한 인증서버와의 접속 없이 접속자간 인증 또는 시스템 간의 인증으로 접속단말 간 상호 인증을 실현하여 유비쿼터스 네트워크에서의 보안 문제를 해결한다. UPMA 모델은 인터넷 또는 공공의 네트워크를 통하여 글로벌 로밍 서비스를 가능하게 하는 글로벌 인증 시스템이며, 이것은 또한 회사 내부의 네트워크와 홈 네트워크에 안전하고 쉽게 접속할 수 있도록 개발된 적절한 보안 인증 시스템이다.

Abstract

Two general security measures in computing networks are secure data transmission and user authentication. These problems are still critical in the wireless LAN environments. Thus security becomes most significant issue in personal network environments and ubiquitous networks based on wireless LANs.

We purpose a new authentication system for these kind of environments, and coined it UPMA(Ubiquitous Personal Mutual Authentication) model. UPMA supports authenticating configurations which provides personal verification for each system. It guarantees secure communications through the session key setup, and provides mutual authentication by verifying each user and his/her station.

UPMA solves security problems in ubiquitous networks without accessing authentication server. Instead it performs mutual authentication between terminals or between systems. It is a global authentication system which enables global roaming service through the Internet or other public networks. It can be used to guarantee safe and convenient access to a company Intranet or to a home network.

Keyword : Adhoc communication, Ubiquitous, Peer-to-Peer Security, Personal Mutual Authentication.

1. 서 론

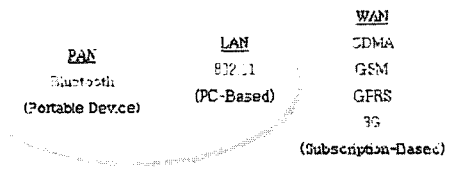
인터넷과 이동통신의 사용 증가는 고객으로 부터 새로운 요구사항을 증가시키고 있다. 이에 대한 대응 솔루션 분야로 무선 LAN 시장이 빠르게 부상 중이다. 시장의 급격한 변화로 인하여 표준화 요구가 증대되고 있으며 연관한 보안 표준도 다양한 방법이 강구되고 있다. 무선 LAN은 이동성 면에서 유선망 보다 뛰어나고, 통신 속도 또한 이동통신에 비해 빠르기 때문에, 무선 홈 네트워크의 블루투스(Bluetooth), RF 등의 기술보다 넓은

* 정 회 원 : 숭실대학교 정보과학대학 컴퓨터학부 교수
bgkim@comp.ssu.ac.kr(제 1저자)
** 정 회 원 : ㈜메이자이 대표이사
sshong@m-magi.com(공동저자)
*** 정 회 원 : 경영정보연구소 소장
sshong@m-magi.com(공동저자)
☆ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음.

영역을 지원하고 전송속도가 빠른 강점으로 확산 가능성이 높은 사업영역으로 평가되고 있다. 또한 무선 LAN은 향후 확대될 이동 네트워크의 모든 요소를 포함하고 있으며 다양한 환경요소를 제공하고 있다. 무선 LAN의 표준화는 미국중심의 IEEE802.11과 유럽 중심의 하이퍼랜(Hiperlan), 일본중심의 MMAC-PC(Multimedia Mobile Access Communication Systems-Promotion Council)로 표준화가 진행 중이며, 미국중심의 IEEE802.11 규격이 가장 대표적인 표준으로 인정되고 있다.

무선 LAN은 전파를 매개체로 브로드 캐스팅되며, 적용되는 공간적 범위가 넓기 때문에 도청, 위장, 스푸핑, 기기의 도난 등의 문제가 있음으로 기존의 유선 네트워크보다 보안이 취약하다. 이러한 보안상의 취약성을 효율적으로 해결했을 때 원활한 무선 LAN을 자유롭게 사용하며, 인터넷 다음에 도래하는 유비쿼터스 컴퓨팅 시대의 기반 솔루션으로 자리잡을 것으로 기대한다.

본 논문에서는 앞에서 언급한 무선 LAN의 보안상 취약점을 제거하는 방안과 무선 LAN 이후 유비쿼터스 컴퓨팅 시대에서도 통합적으로 필요한 효율적인 보안 솔루션의 기반(Infrastructure)을 위하여 사설 망 네트워크에서의 무선 LAN 보안 방법과 공중 무선 LAN에서의 보안방법을 고찰할 것이다. 그림 1은 무선 네트워크의 개념을 나타낸다[1]. PAN (Personal Area Network), LAN(Local Area Network), WAN(Wide Area Network)으로 구분되며, 각 네트워크 별로 상호 연동을 가지고 함께 발전될 가능성이 높음으로 네트워크의 형태가 다를 경우에도 함께 지원 가능한 모델이다.



(그림 1) 무선 네트워크 개념도

또한 각 영역별 표준은 다른 영역의 표준과 함께 포괄적인 표준화가 고려될 것으로 기대된다. 그러나 무선 LAN의 표준은 유·무선 네트워크의 표준을 고려할 것이므로 자연스럽게 통합될 것으로 본다. 이에 따라 편리하고, 다양한 용도로 활용되기 위하여 필요한 인증(단일사용자 인증 등)의 문제, 암호화의 문제 등의 보안 취약점을 해결함으로써 자유로운 무선통신 시대를 선도할 것이다. 따라서, 본 논문에서는 현재 진행 중인 표준화를 고찰하여 궁극적으로 이루어야 할 더욱 효과적인 인증 방법을 제시하여 실용적이고 효과적인 무선 LAN 보안 방법을 연구하고자 한다.

2. 무선 LAN 통합 보안

무선 LAN의 보안 표준화는 이루어져 있지 않으며 진행과정에 있다. 현재 논의되고 개발되고 있는 방안에서 가지고 있는 문제점 요소 중 무선 LAN에서 해결되어야 할 기밀성과 인증의 문제를 함께 해결하는 방안을 Peer-To-Peer(Ad hoc, WPAN) 네트워크인 양 단말간의 UPMA 방안을 제시하여 해결 가능성을 제시 할 것이다. 여기서 유비쿼터스 라는 용어를 채택한 이유는 향후에 일반화 될 개인 네트워크는 유비쿼터스 시대에서 네트워크의 근간 백본으로 되었을 때 개인 휴대장비 또는 무선 단말장치는 매우 유용하고, 보안이 강력해야 하며, 편리하고 간단하게 활용할 수 있어야 한다. 기밀성 문제와 인증문제를 해결하여무선 LAN 보안에 이 두 가지 요소를 함께 만족하여 보안성을 갖도록 하는 효율적인무선 LAN 보안 모델이 필요하다. 또한 개인화 된 미래의 네트워크는 이동통신 망을 이용하든지 또는, 인터넷 망을 이용하든지 하부 인프라와 무관하게 사용자의 입장에서는 하나의 단일 망을 이용하는 것처럼 사용되도록 모델이 이루어져야 한다.

무선 LAN의 보안은 궁극적으로 유선 네트워크에서 필요한 보안과 이동통신에서 활용되는 보안 및 서비스를 모두 포함할 때에 가장 적절하고 완

벽한 보안을 이룰 수 있다. 즉 무선 LAN의 효율적 보안방법은 통합보안에 있는 것이다. 특히 무선 인터넷 로밍 서비스 제공을 위한 로밍 서비스 보안 기술을 기술적인 측면은 이동통신 기술에서 발전되어 있으나 IP 네트워크에서는 다루어지지 않았으며 무선 LAN의 발전으로 통합적인 서비스를 위한 보안 방법이 강구되어야 한다. 이동통신 망을 통한 무선 인터넷 사용의 최대 강점은 사용자에게 로밍 또는 핸드오프 기술을 통해 언제 어디서나 누구와도 통신을 가능하게 한다는 점이다. 개인화 된 네트워크 환경은 집에서 근무하는 재택근무 등을 가능하게 될 것이며, 이에 따라 무선 인터넷은 이동통신 망을 이용하든지 또는, 인터넷 망을 이용하든지 하부 인프라와 무관하게 사용자의 입장에서는 하나의 단일 망을 이용하는 것처럼 느껴지도록 발전되어야 한다. 즉, 다수의 사업자가 운영하는 무선 LAN 공중망간 로밍 서비스 그리고 무선 LAN 공중망과 이동통신 망의 조합인 이종 망간 로밍 서비스, 더 나아가 이러한 로밍 서비스들의 국제적인 확장이 이루어져야 한다. 또한 다양한 접속환경을 통하여 사내의 네트워크와 서버에 안정하게 접속할 수 있어야 한다. 이를 위해서는 다양한 액세스 망들에 대해 단일화된 라우팅 프로토콜이 적용되어야 한다.

무선 LAN 공중망간 로밍 서비스를 지원하는 관련 업체로서, "GRICcommunication", "HereYouAre communication", "I-Pass" 등이 있다. 이종 망간 로밍 서비스를 지원하기 위한 관련 업체의 연구 동향으로서, 일본 J-Phone의 3G W-CDMA 망과 무선 LAN 망간 연동 기술 개발, 판란드 WNS사의 400개 기지국을 이용한 GPRS와 무선 LAN 통합 서비스 준비, 미국 AT&T Wireless 및 Cingulare Wireless사에서 적용성 검토, 퀄컴의 듀얼모드 칩셋(cdma2000 1xEV-DO/무선 LAN) 개발 예정 등을 들 수 있다. 국내에서도 최근 한국통신 사업자연합회 내 무선 LAN 사업자 협의체가 구성되어 무선 LAN 공중망 서비스 사업자간 주파수 혼신 방지와 공용 서버 구축에 대한 논의가 시작되고 있다[3,8].

그러나 이동 IP 서비스는 공개된 다수의 망간에 걸쳐 이루어지므로, 많은 보안 취약점을 가질 수 있다. 특히, 무선 인터넷 사용자의 로밍으로 인해 사업자간 망간 연동이 빈번하게 이루어지기 때문에 망간에 걸친 가입자 인증, 권한 검증, 과금, 사업자 망간에 걸쳐있는 망 노드들 간 인증을 제공하는 안전한 로밍 서비스 기술 즉, AAA 기술이 기본적으로 요구된다. 이러한 로밍 서비스는 통신 서비스 사업자 망간에 걸쳐있으므로 제도적인 측면, 정책적인 측면, 기술적인 측면에서 다양한 요구 사항들이 반영되어야 하며, 보안 기술로서 AAA 기술을 적용한다고 가정하고 관련 기술과 효율적인 보안방법이 제시되어야 한다. 이를 이룩하기 위해 UPMA을 제시하고 통일된 인증방안을 제시하고자 한다. 통일된 인증방안이 마련되었을 때 현재 고민하는 문제들이 자연스럽게 해결을 이룰 수 있을 것이다.

3. UPMA 모델

UPMA(UbiquitousPersonalMutualAuthentication)는 공인인증의 방식과 달리 개인의 인증 시스템이다. 즉 사용자 자신 스스로 인증 가능하다. 그러나 완벽한 인증 시스템이라기 보다는 상대방을 확인(또는 인증)하는데 목적이 있지 않고 자신의 정보를 보호하는 데에 목적이 있다. 또한 자신을 보호하는 부분에 상대방을 확인해야 하는 필요성이 발생하는 것을 충족하는 데에 있다. 그러므로 UPMA는 사설 인증의 유효성과 동일하게 먼저 묵인의 신뢰가 필요하다. 이러한 통신의 요구 자와 필요 자들 간에 몇 가지 전제적인 사항이 필요하다.

UPMA 구성을 위해 단말시스템의 하드웨어 식별자와 사용자의 식별자를 설정한다. 하드웨어 식별자는 기기 자신의 유일한 하드웨어 식별 값을 선택하고 기기를 사용자와 연관성이 없는 기기자체의 식별 값을 선택하는데 가장 일반적인 선택은 MAC 어드레스나 CPU 일련번호(Stepping Number), BIOS 등의 정보를 예로 들 수 있다. 사용자의 식

별자는 하드웨어 식별자 보다 변동가능성이 높으며 그에 따라 임시적으로 변경이 가능하다. 그러나 사용자가 기기의 사용을 자신 이외에 사용치 않도록 설정하는 경우에는 하드웨어 식별자와의 결합을 하여 타사용자의 사용을 제한 할 수 있다. 그러나 일반적인 경우에는 사용자가 접속 시마다 다른 형태의 사용자인증 확인이 가능하도록 하는 것이 필요하다. 예를 들어 암호 또는 생체인식, 스마트카드(Smart Card) 등을 사용할 수 있다. 또한 보안 및 인증의 강화를 위해서는 사용자 유일의 식별 값을 사용하는 것이 바람직하다. UPMA는 하드웨어 식별 방법과 사용자 인증의 두 가지를 함께 확인하여 적용한다. 적용 방법으로 접속에 따른 세션 키를 생성 후 하드웨어 식별자와 사용자 식별을 통하여 최종 인증하는 방식을 적용한다. 또한 UPMA에서 접속시점에 세션 키를 형성 후에 대칭 키 암호시스템을 사용하여 기밀성, 무결성 보안과 인증의 문제를 동시에 해결한다. 디지털 서명 인증서 포멧은 별도의 인증서 포맷을 구성하더라도 국제표준 DSS나 국내표준인 KCDSA에 맞도록 해야 할 것이다. UPMA에서는 부인방지 디지털 서명방식 (undeniable signature)의 효과를 볼 수 있다. 먼저 무선 LAN 환경이 아닌 단말간의 동작과정을 설명하고 이에 따른 적용방안을 무선 LAN에 접목하는 방법으로 진행한다. 편의상 사용자 시스템을 "A"라하고 접속 대상 시스템을 "B"라고 하자. A와 B 각각은 하드웨어식별 값과 사용자 식별 값을 가지고 있다. 이 식별 값들은 하드웨어관련은 하드웨어 유일한 값(타 시스템과 구별되는 값), 사용자 관련은 사용자 확인에 유일한 값을 선택한다.

또한 접속에 따른 중요 정보(식별자 값, 각 생성된 키 값, 타인의 인증 관련 정보 등)의 안전한 보호를 위해 각각의 단말기 저장 매체에(HDD 등)에 안전폴더(Safe Folder)를 설정하는데, 하드웨어 식별자와 사용자 식별자의 확인이 될 때에만 사용 가능하게 하여 안전하게 사용하도록 한다.

A와 B는 각각은 하드웨어식별 값과 사용자 식별 값으로 개인 키와 공개키를 만든다.

A : 하드웨어식별값 : **AHP(개인키)와 공개키(AHS)** 사용자식별값 : **AUP(개인키)와 공개키(AUS)** B : 하드웨어식별값 : **BHP(개인키)와 공개키(BHS)** 사용자식별값 : **BUP(개인키)와 공개키(BUS)**

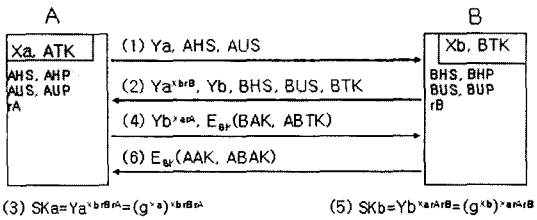
*** 키 설정 설명

AHP(A의 Hardware Personal 키), AHS(A의 Hardware Share 키), AUP(A의 User Personal 키), AUS(A의 User share 키), BHP(B의 Hardware Personal 키), BHS(B의 Hardware Share 키), BUP(B의 User Personal 키), BUS(B의 User Share 키), BAK(B의 Authentication Key), BTK(B의 Transport 키), ABAK(A, B 간의 Authentication Key), AAK(A의 Authentication Key)

3.1 세션 키 생성과정

A와 B가 각각의 개인키와 공개키를 만들고, 접속 시 난수를 발생하여 세션키를 생성한다. 세션키는 일상적으로 두 접속간의 기밀성 유지를 위하여 생성하며, 부분적으로 간략한 인증과정을 겸하기도 한다. 본 고에서는 이에 대하여 기존의 증빙 된 방법을 사용한다 단, 키의 생성방법은 조금 다르다. A의 난수 rA와 상대 시스템(B)의 난수 rB를 검증된 의사난수 발생기(시간값, Intel RNG 등)에 의하여 키를 생성한다.

UPMA접속으로 통신시에 PKI인증과 같이 인증기관(또는 제3자)의 증빙을 필요한 경우에는 공개등록 파일을 제3자의 신뢰성이 있는 기관에 등록하여 등록 여부 확인(기존의 PKI 공인 인증 시스템과 동일)하여 접속이 가능하다. 이 경우에 비밀서명 생성 정보 검증용 비밀 보관키(식 (8)값)와 공개 검증 정보(검증키 서명 값의 Hash 값)를 활용하여 검증용 비밀 보관키 정보는 비밀리에 보관하고 공개 검증이 필요할 경우에 검증 키(식 (3), (4), (5), (6), (7))와 동일한 해쉬(hash) 함수를 가지고 있는 검증 기관의 공개 목록에 등록하고



(그림 2) 직접(Direct) 키 분배 방식

양측의 확인 협조로 확인이 가능하다. 편의상 사용자 시스템을 A라 하고 접속 대상 시스템을 B라고 하자. A, B 각각은 유한체 GF(P)상의 원소 중 임의의 원소를 각각 비밀정보 Xa, Xb를 선택하고, 공개정보 $Ya=g^{Xa} \bmod P$, $Yb=g^{Xb} \bmod P$라고 한다. 여기에서 세션키는 다음과 같이 생성할 수 있다[24,25].

$$SK=Yb^{Xa} \bmod P=g^{XbXa} \bmod P \quad (1)$$

$$SK'=(Ya^{XbrB})^{rA} \bmod P=g^{XaXbrBrA} \bmod P=(Yb^{XarA})^{rB} \bmod P$$
$$=g^{XbXarArB} \bmod P \quad (2)$$

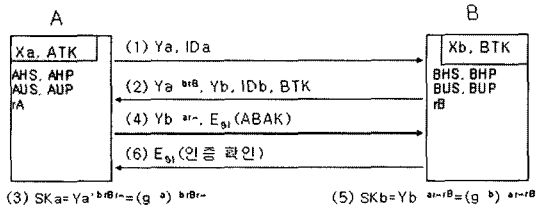
즉, 상대방의 공개정보에 자신의 비밀정보를 멱승하면 (1)식과 같이 세션키를 만들 수 있으나 두 접속간에 매번 동일한 세션키(값)를 얻게 되므로 A는 (Yb^{Xa})에 임의의 난수 rA를 멱승하여 B로 보내면 B는 $(Yb^{Xa})^{rA}$다시 임의의 난수 rB를 멱승하여 세션키 SK'를 (2)식과 같이 얻는다. 이후 SK'를 SK라 하자.

여기에서 하드웨어 공개키와 사용자 공개키를 조합하여 ID를 정의한다.

$$IDa = AHS \cdot AUS$$
$$IDb = BHS \cdot BUS$$

또한 임의의 사용자 i IDi = iHS · iUS

정의 된 ID는 일상적으로 적용하는 ID 즉, 이메일주소, 이름, 글로발 ID 등과 대칭하여 일상적인 ID로 사용자를 구별할 수 있도록 할 수 있다. 다음의 접속과정으로 해당키를 교환하여 세션키를 생성하고 인증을 한다.



(그림 3) 재 접속의 경우

<접속과정>

1) A -> B

Ya, IDa(또는 AHS, AUS)

2) B -> A

$Ya^{Xb \cdot rB}$, Yb, IDb(또는 BHS, BUS), BTK

3) A -> B

Yb^{XarA}, E_{SK}(BAK, ABTK)

4) B -> A

E_{SK}(AAK, ABAK) 전송, 인증 확인

최초의 인증과정 이후 재 접속의 경우 ID값의 확인으로 인증이 가능하다. 이후의 접속에 따른 인증 수행과정이 간편하게 처리된다.

3.2 UPMA 상호 부인 방지 인증 설정

상기 제시된 세션 키 교환 방법에 의하여 보호된 통신이 연결과 함께 사용자 인증의 과정이 수행되며 상호 부인 방지되는 인증 구성을 이룬다. 상기 세션 키 생성 과정에서 A와 B는 AHS, AUS, BHS, BUS의 키(또는 ID)를 교환하였고 알고 있다. 세션 키 생성 이후 AES 대칭 키 암호 방식(E_{SK})으로 인증 데이터가 교환되며, 다음의 인증 구성을 가진다.

다음은 각 키의 설정 방법을 설명한다.

하드웨어 확인키 : ABTK= ATK · BTK

ATK, BTK는 자신의 개인 키(AHP, BHP)의 연관 대체(치환) 키와 System 정보를 연접하여 자신의 공개키로 암호화한 값이며, 암호화하기 전의 값을 hash하여 검증키로 사용한다.

검증키 A1=hash{(AHP(대체 키) || A의 System 정보)} (3)

검증키 B1=hash{(BHP(대체 키) || B의 System 정보)} (4)

A:하드웨어확인키:ATK=AHP*(160+352)=E_{AHS}(AHP(대체 키)||A의 System 정보)
B:하드웨어확인키:BTK=BHP*(160+352)=E_{BHS}(BHP(대체 키)||B의 System 정보)
ATK, BTK는 자신의 시스템의 인벤토리 (Inventory, System 정보)를 포함, System 정보는 자신만이 확인 가능

인증 키(ABAK) : ABAK=(AAK · BAK)|| Time
인증 키 (ABAK) : 사용자 식별 공개키(AUS, BUS)와 하드웨어 확인키, 그리고 상대방의 사용자 개인키로 구성된 키 값이다.

A 인증 키 : AAK=(AUS · BUP*)||ATK
B 인증 키 : BAK=(BUS · AUP*)||BTK

BUP*, AUP*는 상대의 개인 키(AUP, BUP)의 연관 대체(치환) 키와 사용자 신상 정보 및 서명 값을 연접하여 자신의 공개키로 암호화한 값이며, 암호화하기 전의 값을 hash하여 검증키로 사용한다.

BUP* = E_{BUS}(BUP(대체 키) || B의 사용자 신상 정보 및 서명)

검증키 A2=hash{(BUP(대체 키) || B의 사용자 신상 정보 및 서명)} (5)

AUP* = E_{AUS}(AUP(대체 키) || A의 사용자 신상 정보 및 서명)

검증키 B2=hash{(AUP(대체 키) || A의 사용자 신상 정보 및 서명)} (6)

검증키 AB=hash{ABAK} (7)

이로써 ABAK는 AB간 통신의 인증키이다. 이를 통하여 **상호 부인 방지** 가능하다. 하드웨어 확인키(ABTK)와 인증키(ABAK)은 접속자의 인증 증빙 자료가 되며, A와 B는 필요에 따라 이에 대한 인증 데이터베이스(DataBase)를 구성할 수 있다. UPMA 인증 시스템에서 두 시스템간의 세션 키는 매 접속 시마다 다르지만 인증 데이터는 시간 값을 제외하고는 항상 동일하다. 이로 인하여 동일한 사용자의 재 접속 시에 인증 과정을 간편하게 처리할 수 있으며, 또한 명확한 사용자 인증이 가능하다. 즉 세션 키 교환 과정에서 공개키를 확인하여 최종 인증키를 확인되면 사용자 인증 확인이 가능하다. 이로써 1회 이상의 접속 과정 이후에 세션 키 교환 과정만을 통하여 개별 상호 인증이 가능하여 편리한 사용자 인증 시스템을 구현하게 된다.

<인증 데이터 베이스에 구성 목록 예; 사용자를 i,j로 설정 j측에서의 저장정보>

1. iHS : i의 하드웨어 공개키, iUS : i의 사용자 공개키; 또는 iDi
2. ijTK : ij 하드웨어 확인키
3. ijAK : i와 j간의 인증키
4. 검증용 비밀 보관키 :
   iTK, iAK, jTK, jAK (8)
5. 기타 인증시간(TIME)값, 검증키(A1, B1, A2, B2, AB) 등 필요 보관키.

이로써 공개키 값 또는 공개키 값으로 설정된 ID값으로 사용자 인증이 가능하며 접속을 이룬 상대 시스템에서도 동일한 형태의 해당 목록을 보관하며, 이 보관은 안전폴더(Safe Folder)에 보관한다. 결과적으로 UPMA가 공인인증시스템과 같은 인증기능을 수행하기에 필요한 것은 검증키를 이용하여 제3의 공인인증기관에 의하여 검증

되었을 때 인증시스템이 되며, 그렇지 않았을 때는 상호 부인 방지되는 인증 가능한 구성과 인증에 필요한 값들을 가졌다고 할 수 있다.

<제3자 인증에 필요한 사항>

제3의 인증기관에 검증키의 보관여부를 확인하기 위하여 제3의 인증기관과 UPMA접속을 한 후에 인증기관에서 제공하는 등록 검증키로 등록여부를 확인한다.

제3의 인증기관에서 사용자검증을 위해 양자간의 UPMA 접속하여 검증과정을 거쳐 서로의 신상을 파악한다. 여기서 제3 인증기관을 3이라 하자.

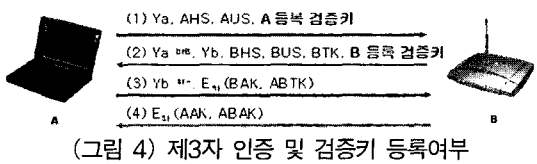
A 등록 검증키 = hash{(AUS • 3UP*)||A3TK}
B 등록 검증키 = hash{(BUS • 3UP*)||B3TK}

제3의 인증기관은 등록 검증키를 UPMA 접속에 따른 값이 아닌 별도의 포맷으로 정의하고 사용하여도 무방하다. 다만 복제될 수 없는 확인 값으로 되어야 한다. 이로써 다른 접속에서 개인정보를 유출하지 않고 검증키 보관여부만을 제3의 인증기관과의 등록 여부를 등록 검증키로 확인하여, 이후에 제3의 인증기관을 신뢰할 수 있다고 가정할 때 기존의 공인인증시스템과 동일하다. 이를 통하여 안전한 접속을 위해 신분확인 등을 이루어진 사용자와 만 접속을 허용하도록 설정이 가능하다.

<검증(UPMA 인증방법)>

1. A가 검증을 요청할 때
   1) 인증기관은 검증키 B1, B2, AB, ABAK를 A로부터 받음.
   2) 인증기관은 B에게 개인키로 암호화되지 않은 BUP*, BTK와 ABAK를 요청.
   3) 2)의값, 암호화되지 않은 BUP*, BTK와 ABAK를 해쉬하여 검증키와 비교.
   4) 검증결과를 A, B측에 통보.

2. B가 검증을 요청할 때
   1) 인증기관은 검증키 A1, A2, AB, ABAK를 B로 부터 받음.
   2) 인증기관은 A에게 개인키로 암호화되지 않은 AUP*,ATK와 ABAK를 요청.
   3) 2)의값, 암호화되지 않은 AUP*, ATK와 ABAK를 해쉬하여 검증키와 비교.
   4) 검증결과를 A, B측에 통보.

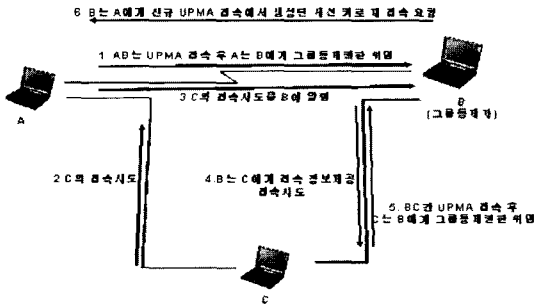


(그림 4) 제3자 인증 및 검증키 등록여부

3.3 개인 및 임시그룹간 접속 통신

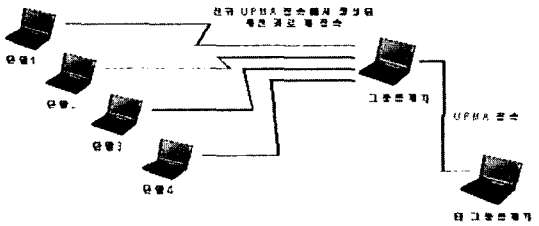
일 대 다의 접속 환경 구축 시에 동일한 형태의 UPMA 인증 과정을 거쳐 각각의 단말간 연결이 된 후 접속그룹통제자(이하 그룹통제자라 한다)를 설정하여 이후 접속의 통제 권한을 부여하도록 설정할 수 있다. 일 대 다의 접속을 하고자 할 경우 먼저 UPMA의 접속 과정으로 일 대 일의 통신을 이루고, 그룹통제자가 설정된 후 다른 제 3자의 접속이 요청되거나 요청하면 그룹통제자가 아닌 사용자는 그룹통제자에게 이 사항을 전달하면 그룹통제자는 새로운 접속 자의 공유키로 자신의 정보를 전달하여 접속을 이룬다. 이로써 새로운 세션 키를 사용하게 되며, 기존의 관리하는 접속자에게도 새로운 세션 키를 전달하여 접속 그룹 내에서 동일한 세션 키를 사용하여 접속 그룹을 형성한다.

그림은 A, B간에 UPMA 접속이 이루어지고 난 후 A는 B를 그룹통제자로 설정할 때 또 다른 C가 A로 접속을 시도해오면 A는 C의 접속시도를 알리고 C의 공개키를 A에게 전달한다. A는 C의 공개키에 접속정보를 보내어 C와 UPMA 접속을 하고 최종 세션키를 A에게 전달하여 접속그룹을



(그림 5) 다중 임시 접속과정

형성한다. 여기서 사용자 확인은 최초 그룹통제자와 교환된 정보만 확인이 가능하다. 물론 중간에 교체되거나 위임되는 그룹통제자는 그 당시의 사용자 확인이 가능하다. 이와 같은 방식으로 그룹통제자는 또 다른 그룹통제자와 동일한 과정으로 그룹통신을 구성한다.



(그림 6) 다중 임시 접속그룹간 접속

그림은 그룹통제자 설정 후 타 그룹 통제자와 접속 과정이다. 이러한 방법을 통하여 그룹간 통신이 가능하며, 신뢰성은 그룹 통제자에 달려 있다. 다중 임시 접속은 다음의 상태를 가정하면,

① 모든 접속을 리슨(listen) 하는 상태(실제 접속 요청 시 사용자 선택)
② 사용자가 선별한 특정 접속만 허용하는 상태(허가된 접속 이외는 모두 차단)
③ 사용자가 선별한 특정 접속을 기본적으로 거부하고 나머지 접속을 리슨(listen) 하는 상태
④ 유일한 1개의 접속 상태만 유지하는 상태(폐쇄된 그룹 통신의 경우)

또한 접속의 성격에 따라 여러 가지 옵션 모드를 적용할 수 있다.

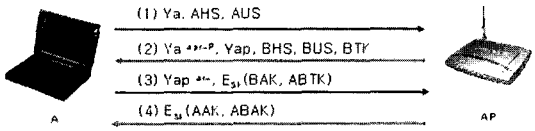
① 각 접속의 등급에 따라 시간적으로 제한된 접속을 허용 및 인증 권한 위임 시간 설정
② 지속적인 사용자 확인을 위한 주기적인 사용자 확인

여기서는 유비쿼터스 네트워크환경에서 있을 수 있는 네트워크 형태를 가정하여 임시 그룹 설정에 따른 접속방법을 UPMA를 통하여 설정하였다. 즉, 1차적인 신뢰관계에서 추가적인 이후의 신뢰관계 형성에 있어 자신의 네트워크접속의 선택은 자신과 자신의 연관된 구성요소로 이루어지기 때문에 실생활에서 직접적인 사회활동과 같이 신뢰할 수 있지만 신뢰성의 판단은 자기 자신이 하는 형태로 구성하였다. 물론 위임받은 통제자를 충분히 신뢰 할 수 있을 때 가능하며, 만일의 경우에는 위임받은 통제자를 통하여 그룹간 접속통제자가 어떤 사용자인지 확인이 가능하다. 이러한 다중접속은 예를 들어 몇 명의 소수 단체 그룹간 접속으로 학술활동, 단체 게임, 세미나, 특정 컴퓨터 접속모임 등에 활용 가능할 것이다.

4. UPMA의 무선 LAN 적용

여기에서는 UPMA 접속방법을 무선 LAN 접속 보안에 적용하여 효율적인 무선 LAN의 보안 방법을 이루는 모델을 구성하는데, 앞에서 언급한 UPMA 보안방법에서 단말과 단말간에 적용되었던 모델을 무선 LAN에 적용하는 과정이다. 여기서 단말(A)와 AP그리고 인증서버(B)간의 설정을 가정하자.

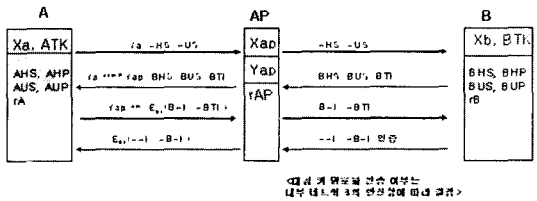
무선 LAN 환경에서는 인증자는 중간에 세션 키 생성에 대한 주체자가 된다. 또한 매개 역할로 인증 서버와 단말간의 접속 인증 과정을 전달한다. UPMA 방식으로 공중 무선 LAN 서비스를 시행할 경우에 사용자 및 사업자간 상호 인증이 가능하며, 타사 및 국가간 글로벌 개인 인증 시스템



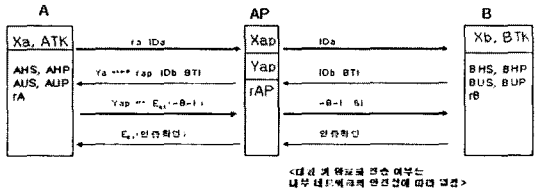
(그림 7) UPMA 방식의 데이터 교환

으로써의 역할이 가능하다. 세션키는 단말과 AP 간에서 생성되며, 인증 서버는 UPMA인증에 필요한 데이터를 가지고 있다.

편의상 사용자 시스템을 A라하고 접속 대상 시스템(또는 사업자 인증 서버)을 B라하고 중간 연결자(인증자)를 AP라 하자.



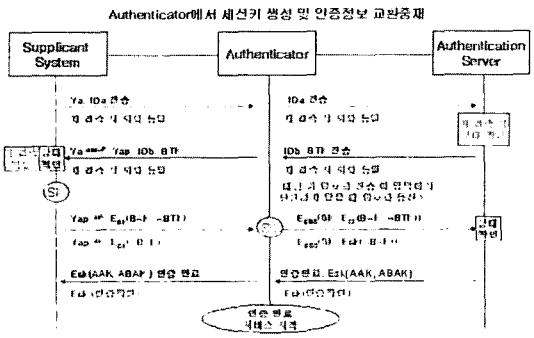
(그림 8) 무선 LAN에서의 직접(Direct) 키 분배



(그림 9) 무선 LAN에서의 재 접속의 경우

여기서 일반 접속과 무선 LAN에서의 차이점은 AP가 세션키를 생성하고 인증서버는 인증의 역할만 하여 역할을 분산하는 것이다.

그림에서 빨강색 글씨(화살표선 아래글씨)는 재접속의 경우를 나타내며, AP에서 인증 서버까지 연결되는 내부 네트워크에서도 암호화 통신이 필요할 경우에는 그림 [2-10]과 같이 인증서버의 공개키(E_{BHS})와 세션키(Esk)로 암호화 통신을 한다. 그러나 내부 네트워크가 안전할 경우에는 암호화하지 않아도 될 것이다. 무선 LAN의 경우 이외에 이동 통신 등의 무선 인터넷의 경우에는 AP 대신에 기지국이 있는데, 이 경우에 기지국과 AP의 역할을 동일하게 적용이 가능하므로 무선 이동



(그림 10) 무선 LAN에서의 UPMA 적용

통신의 인증에도 적용 가능하다. 인증자는 중간에 매개역할로 인증서버와 단말간의 접속인증과정을 전달을 하며, 세션 키를 생성한다. 인증서버에서 전달된 하드웨어 키와 사용자(사업자)키 값을 받아서 인증자에서 실제적인 접속 전달과정을 실행한다. 인증자는 향후에 네트워크 노드에서 엑세스 포인트 기능을 하는 게이트웨이 될 수도 있으며 동일한 구성으로 역할을 수행 가능하다.

<B를 공중무선 LAN 서비스 사업자라 할 때 가입자 신청 및 UPMA 인증>

1. 가입약관에 따른 기본 신상자료를 요청
   1) 성명, 주민등록번호, 지불방법에 따른 정보, ID, PW등
   2) 기타 필요한 요청자료(IP 등)

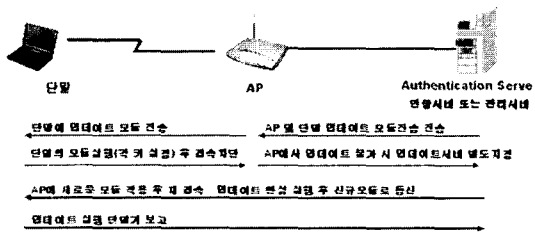
2. 사업자(B)에서 검증을 요하는 경우
   1) 인증기관은 검증키 A1, A2, AB, ABAK를 사업자(B)에게서 받음
   2) 인증기관은 A에게 개인키로 암호화되지 않은 AUP*, ATK와 ABAK를 요청
   3) A에서 전달된 암호화되지 않은 AUP*, ATK와 ABAK를 해쉬하여 검증키와 비교
   4) 검증결과를 A, B측에 통보

3. 초기접속 시 생성된 인증키와 가입자정보를 데이터베이스로 저장관리

(표 1) 무선 LAN 인증 방법 비교

Topic	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP	UPMA
보안 솔루션	표준기반	독자방식	표준기반	표준기반	표준기반	표준에 따른 독자방식
키 생성	No	Yes	Yes	Yes	Yes	Yes
단말간 인증	No	No	No	No	No	Yes
상호 인증	No	Yes	Yes	Yes	Yes	Yes
하드웨어& 사용자 동시 인증	No (Password)	No MS-CHAP (Password)	No 인증서	No Password & others	No Password & others	Yes 하드웨어&사용자 식별
서버 인증	-		인증서	인증서	인증서	접속 시 인증서 생성
기밀성	WEP 고정키	WEP, TKIP	WEP, TKIP	WEP, TKIP	WEP, TKIP	암호통신 세션 키 생성
AP 로밍 및 글로벌 로밍	No	No	No	No	No	Yes
기타	Inadequate to WLAN	Strong PW needed	PKI needed	More flexible	Subset of TTLS	각 시스템에 인증 스킴을 가짐
공급사	-	Cisco	MS	Funk	Cisco, MS,RSA	메이자이

표 1은 무선 LAN 인증방법과 UPMA로 인증했을 때를 비교하는 표이다. 다른 방법은 무선 LAN의 보안인증을 중점으로 두고 고려한데 비하여 UPMA는 무선 LAN 이외의 무선통신 환경에서도 적용이 가능한 방법이므로 정확한 비교의 대상은 되지 않으나 이해를 돕기 위하여 비교하면 다음과 같다.



(그림 11) 무선 LAN에서의 온라인 업데이트

4.1 UPMA 적용의 온라인 업데이트 방안

편의상 무선 LAN 의 구성은 단말, 인증자, 인증서버로 이루어진다. 기존의 무선 LAN 구축 환경에서의 UPMA를 적용할 경우에 AP와 모든 사용자 단말에 새로운 인증 시스템 및 보안 프로그램의 적용이 필요한데 이에 따른 업데이트 방안을 제시한다. 무선 LAN(공중 무선 LAN 포함)에서 단말과 인증자, 인증서버간의 새로운 보안 및 인증 구성에서 추가되는 업데이트 모듈을 분배할 때 AP에서의 모듈 업데이트가 실시간으로 이루어지는 것이 필수적이다.

무선 LAN에서의 온라인 업데이트 절차를 표현한 그림이다. 이 온라인 업데이트 방안은 기존의 서비스 상태에서 직접 업데이트를 하는 방안으로 기존의 서비스를 실행 중에 추가적인 업데이트를 서비스 실행 중에 실시간 자동적으로 처리함으로써 효과적인 업데이트 방안을 제시한다. 다음의 순서에 따라 온라인 업데이트 적용이 가능하다.

① 인증서버 또는 관리서버에서 AP로, 단말과 AP의 업데이트 모듈을 전송한다.
② AP에서 단말에 적용 하고자 하는 모듈을 기존의 통신 방법에 의하여 단말로 전송한다.
③ 단말에서 새로운 모듈(각 키 설정 등)이 실행되도록 하고
④ 접속을 차단한다.
⑤ AP에서 신규로 업데이트 된 모듈을 실행

(기존 접속 모듈을 위한 필터링 과정 포함 [*])하고

⑥ 단말과 새로운 모듈로 접속한다.

⑦ 새로운 모듈로 접속하여 인증서버에 어떤 사용자가 신규 모듈 접속자 인지를 구분하여 기록한다.

UPMA의 모듈을 적용하였을 때 구분 방법은 기존의 인증 데이터베이스와 UPMA 인증 정보가 다르므로 쉽게 구분 지어 관리가 가능 할 것이다. 만일 AP에서 단말에 대한 모듈을 업데이트 할 수 있는 메모리가 부족할 경우에 AP에는 신규 모듈을 적용하고 난 후 사용자에게 특정 인터넷 Site 또는 지정 server를 통하여 사용자 스스로 업데이트하도록 하여 신규모듈을 실행한다.

그러나 [*]이외의 상황으로 업데이트 과정 중 접속하지 않는 사용자의 경우에는 기존의 접속 모듈을유지하도록 AP에서 함께 서비스하도록 한다.

5. 결 론

본 고에서 Peer to Peer UPMA 모델을 구성하여 무선 LAN에서 적용과 부가적인 모델 응용으로 기밀성과 인증을 동시에 해결 문제 인 기밀성 유지와 인증의 동시적 해결을 하였으며, 다양한 네트워크환경에서 단일 망을 이용하는 것처럼 구성이 가능하도록 하는 방안을 두 접속간의 유일한 인증키 생성과 무선 LAN에서 적용방안을 통하여 언제나 동일한 형태의 인증구조와 유일한 인증 키의 형성으로 UPMA 모델로 다양한 네트워크에서 단일 망 접속형태로 구현이 가능함을 알 수 있다. 유무선 통합 서비스로 다양한 기술과 솔루션이 발전되고 있지만 본 연구에서는 무선 LAN의 보안을 통하여 향후 도래하는 유무선 통합, 그리고 이동통신과 컴퓨터 네트워크의 결합에서 발생할 수 있는 효율적인 보안의 문제의 해결 방법을 알아보았다. 즉 무선 LAN은 이전의 컴퓨터 네트워크와 이동통신의 요소를 모두 포함하고 있음으로 무선 LAN에서 보안솔루션의 고찰로 인하여 유무선 통합과 이동통신과 컴퓨터 네트워크의 보안 문제를 해결하는 방안 이야말로 궁극적인 보안 기반구조를 형성할 것으로 생각된다. 패쇄된 기업의 네트워크는 인터넷의 연결 없이는 더 이상 중요한 업무를 다룰 수 없다. 이것은 곧 각각의 컴퓨터 및 터미널에 대한 인증과 신원확인을 통하여 개별화된 네트워크의 보안 인증의 문제를 해결하여 재택근무와 이동 근무 등이 가능해지고 향후 도래할 미래의 통합네트워크에서 가장 필요한 보안요소가 될 것이다. 본 고의 방안은 국내의 성숙된 정보통신과 IT 인프라를 가장 적절하게 이용할 수 있으며 유무선 통합 서비스라는 패러다임의 변화가 구체화되고 있다. 점진적으로 무선 LAN 공중망 서비스가 확산됨에 따라 시장이 확대되고, 이로 인해 무선 LAN 공중망간 로밍 서비스 그리고 무선 LAN 공중망과 이동통신 망간 로밍 서비스 요구가 증대될 것이다. 무선 LAN 자체의 강화된 보안 기술 개발, 망간 로밍 서비스 제공을 위한 정책 수립 및 기술 표준화 등이 이루어져야 하며 안전한 로밍 서비스보안 기술 개발 등이 이루어져야 한다. 머지 않은 미래의 무선 인터넷은 다양한 액세스 망간에 걸쳐있는 이동성이 필수적으로 요구될 것이다. 망간에 걸친 가입자 인증, 권한 검증, 과금, 망 노드들 간 상호 인증을 제공하는 AAA 기술은 중요도가 더해 질 것이다. 이러한 AAA 기술은 가장 빠르게 확산되는 무선 LAN에 적용하여 검증하고 이후 이동통신에서 추가되는 인터넷 서비스에 응용되었을 때 실제적인 빛을 보게 될 것이다. 그러나 그 기술의 구현하기 위한 노력은 급속하게 변화되는 정보통신 및 컴퓨터 네트워크의 변화에 순응하면서 필요한 부분에 대한 기술로 이어졌을 때 더욱 빛을 발할 것이며, 본 고의 모델이 국내에 성숙된 정보통신 및 IT 기반구조에서 유용한 기술로 평가되어 세계를 향해 발전될 수 있기를 바란다.

참고문헌

[1] 편집자, KAIT "해외정보통신동향자료," 2002.

[2] 편집자, 기술시장동향 무선 LAN 기술과 시장 동향," ETRI 주간 기술동향 1006호, 2001.

[3] 홍승표, 정현수, 하원규, 2002년 전 세계 무선 LAN 기술 및 시장전망," ETRI 주간 기술동향 1047호, 2002.

[4] Mike Wolf, Gemma Paulo, Amy Cravens, Allen Nogee, "In-Stat/MDR Wireless LAN Teleconference," WIP Research Report No. IN020383WI, 2002.

[5] 김용균, 이윤철 무선 LAN 기술 및 시장 동향," ETRI 주간 기술동향 1026호, 2001.

[6] 김용균, 무선 LAN 시장현황 및 전망," ETRI 주간 기술 동향 1052호, 2002.

[7] 송영근, 김한주, 근거리 무선통신기술에 대한 분석 및 전망," ETRI 주간 기술 동향 1021호 2001.

[8] 김형곤, 유희종, 이윤주, "AAA의 Diameter CMS 보안 응용 기술," ETRI 주간 기술 동향 1030호, 2002.

[9] C. Finseth, "An Access Control Protocol, Sometimes Called TACACS," July 1993, ASCII INFORMATIONAL; RFC 1492.

[10] 서광현 "무선통신 서비스 발전방향과 정책방향," 정보통신부, 2002.

[11] Larry Blunk, "Extensible Authentication Protocol (EAP)," draft-ietf-eap-rfc2284bis-03, May 2003, RFC2284.

[12] W. Simpson, Ed. January "PPP LCP Extensions" 1994 ASCII Updates RFC1548, Updated by RFC 2484 PROPOSED STANDARD.

[13] W. Simpson, RFC1994; "PPP Challenge Handshake Authentication Protocol (CHAP)," August 1996, ASCII Obsoletes RFC1334, Updated by RFC2484 DRAFT STANDARD.

[14] B. Aboba, D. Simon, "PPP EAP TLS AuthenticationProtocol," RFC 716,October 1999 ASCII EXPERIMENTAL.

[15] "DRAFT IEEE Standard for Local and Metropolitan Area Networks-Port Based Network Access Control-Amendment 1," Technical and Editorial Corrections, IEEEStd802.1aa-D3, 2002.

[16] "IEEE Standard for Local and metropolitan area networks-Port-Based Network Access Control," IEEEStd802.1x-2001.

[17] "Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements-Part 11, Specification for Enhanced Security," IEEEStd 802.11i-D2.3., 2003.

[18] "80211 A Standard for the Present and Future," Meetinghouse WhitePaper, http://www.mtghouse.com/.

[19] Gartner Research R-17-7369, November 2002.

[20] Gartner Technical Overwiew, October 2002.

[21] 디지털타임스, "통신사업자들 무선 LAN 시장 본격 공략," 2003.

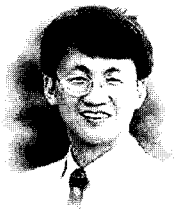
[22] 디지털타임스, "차세대 유.무선 복합 서비스 '초읽기'," 2003.

[23] 김대근, 정한욱, "공중무선LAN 서비스," KT 멀티미디어연구소, 2002.

[24] 원동호, "현대 암호학," 그린출판사, 2003.

[25] EIJI OKAMOTO, "Key Distribution System Based on Identification Information," 1989.

◐ 저 자 소 개 ◑

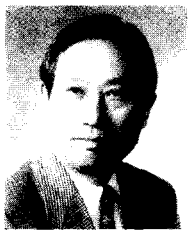


김 병 기

1977년 2월 서울대학교 공과대학 전자공학과 졸업(공학사)
1979년 2월 한국과학기술원 전산학과 졸업(이학석사)
1997년 2월 한국과학기술원 전산학과 졸업(공학박사)
1979년 3월~1982년 2월 경북대학교 공과대학 전자공학과 전임강사
1993년 3월~1994년 2월 한국과학기술원 인공지능연구센터 교환교수
1999년 9월~2001년 2월 숭실대학교 정보과학대학 학장
1982년 3월~현재 : 숭실대학교 정보과학대학 컴퓨터학부 교수
관심분야 : Mobile Wireless Communication Ubiquitous Computing
E-mail: bgkim@comp.ssu.ac.kr

홍 상 선

1988년 전남대학교 물리학과(학사)
1993년~1998년 ㈜트렌드코리아 Acting Country Manager
1998년~2000년 ㈜하우리 사업부장
2000년~2002년 ㈜잉카인터넷 대표이사
2001년~2003년 숭실대학교 정보과학대학원 정보산업학과(석사)
2003년~현재 : ㈜메이자이 대표이사
관심분야 : Adhoc 통신, 원격제어, PC 방화벽, Anti-virus
E-mail: sshong@m-magi.com



전 영 길

1966년 서울대학교(학사)
1968년 서울대학교(석사)
1994년 성균관대학교(박사)
1970년~1977년 서울대학교 경영대학원 강사
1969년~1971년 Control data System 시스템엔지니어
1972년~1981년 Fujitsu Korea 기술본부장
1982년~1984년 한화그룹 상무이사
1985년~1999년 한국컴퓨터기기 대표이사
1987년~현재 : 경영정보연구소 소장
1988년~현재 : 숭실대학교 정보과학대학원 강사
2003년~현재 : 민주평화통일협의회 의원
관심분야 : 지식경영
E-mail: sshong@m-magi.com