# 홈 게이트웨이 보안 관리 방식에 관한 연구

김 현 철* · 안 성 진** · 정 진 욱* · 김 성 혜*** · 유 윤 식*** · 전 용 일***

**요 약**

가정 내의 각종 기기를 유선 또는 무선으로 연결하는 홈 네트워크(Home Network) 기술과 액세스 네트워크 기술, 그리고 각종 서비스 제공 기술 또한 괄목할만한 성장을 거듭하고 있다. 이러한 홈 네트워킹 기술을 이용하여 가정에 서비스를 제공하기 위해서는 홈 네트워크 환경, 액세스 네트워크 환경, 그리고 다양한 서비스 및 콘텐츠 제공 기술 등이 유기적으로 이루어져야한다. 이러한 기술들 중에서 강력한 인증 및 보안 기능이 요구되는 홈 네트워크에서 체계적이고 효과적인 홈 네트워크의 관리 방법의 정립은 홈 네트워킹 서비스의 안전성과 신뢰성을 제공하기 위한 가장 시급하고도 중요한 요소이다. 본 논문에서는 SNMPv3을 이용한 홈 게이트웨이 보안 관리 체계와 방식을 제안하였다. 또한 다양한 홈 네트워킹 보안 시나리오를 지원하기 위한 홈 네트워크 관리 시스템의 구조와 기능에 대해서도 제안한다.

# An Investigation on Security Management Architecture of Home Gateway

Hyun Cheol Kim* · Seong Jin An** · Jin Wook Jung*
Seung Hae Kim*** · Yoon Sik Ryu*** · Young Il Jun***

**ABSTRACT**

Home network technologies which interconnect various wire and wireless home appliances, access network technologies and service offer technologies are continuing growth. To provide secure services in the home, home network environment, access network environment, and various service and contents offer technologies are consist organically. Thesis of administration method of systematic and effective groove network is most urgent and important urea to offer safety and authoritativeness of home networking service in home network that strong certification and security function are required among these technologies. In this paper, we propose home gateway security management architecture and the way to use SNMPv3. Also, we propose structure and function of home network management system to support various home networking security scenarios.

* 성균관대학교 컴퓨터공학과
** 성균관대학교 컴퓨터교육과
*** 한국전자통신연구원 네트워크연구소

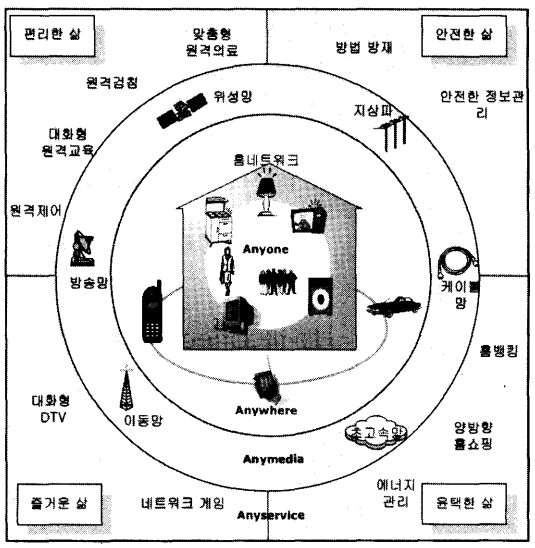
## 1. 서 론

지난 수년간 정부의 정보화 촉진정책의 성공에 힘입어 우리나라는 세계 최고수준의 초고속 IT 환경을 구축하였고, 1999년 4월 초고속 정보통신 건물 인증제도 도입 이후 대도시의 아파트 단지를 중심으로 한 초고속 인터넷 열풍은 가입자망 인프라를 단기간에 고도화시켰다. 이러한 추세에 발맞추어 (그림 1)에서 나타내고 있는 바와 같이 가정 내의 각종 기기를 유선 또는 무선으로 연결하는 홈 네트워크(Home Network) 기술과 액세스 네트워크 기술, 그리고 각종 서비스 제공 기술 또한 괄목할만한 성장을 거듭하고 있다[1, 2].

홈 게이트웨이를 중심으로 구성되는 홈 네트워크에서 각종 정보 단말기나 가전들은 유선, 무선 인터페이스를 거쳐 홈 게이트웨이와 접속되며 홈 게이트웨이는 다양한 액세스 네트워크에 접속된다. 이러한 가정 내 기기들을 제어하는 홈 네트워크 제어기술은 가전업체들이 내세우는 HAVi (Home Audio/Video Interoperability), Sun사의 Jini, MS사의 UPnP(Universal Plug and Play), 삼성전자의 HWW(Home Wide Web)과 HPnP, OSGi(Open Service Gateway Initiative) 등이 있다. 홈 네트워크 전송기술은 크게 유선과 무선으로 나뉘는데, 유선방식에는 고속으로 데이터를 전송할 수 있는 별도의 통신선로를 이용하는 이더넷과 IEEE 1394, 전력선을 이용하는 PLC(Power Line Communication) 등이 있고, 무선방식에는 2.4GHz 대역의 HomeRF, IEEE 802.11a/b/g, 블루투스, 5GHz 대역의 하이퍼 LAN2, IrDA 등이 있다[1, 2, 3].

이러한 홈 네트워킹 기술을 이용하여 가정에 서비스를 제공하기 위해서는 홈 네트워크 환경, 액세스 네트워크 환경, 그리고 다양한 서비스 및 콘텐츠의 제공 기술 등이 유기적으로 이루어져야한다. 이러한 기술들 중에서 강력한 인증 및 보안 기능이 요구되는 홈 네트워크에서 체계적이고 효과적인 관리 방식의 정립은 홈 네트워킹 서비스의 안전성과 신뢰성을 제공하기 위한 가장 시급하고도 중요한 요소이다[6].

본 논문에서는 SNMPv3(Simple Network Management Protocol version 3)을 이용한 홈 게이트웨이 보안 관리 체계와 방식의 제안을 목적으로 한다. 또한 다양한 홈 네트워킹 보안 시나리오를 지원하기 위한 홈 네트워크 관리 시스템의 구조와 기능에 대해서도 제안한다. 마지막으로 웹 기반 홈 네트워크 상태 관리, 트래픽 관리, 실시간 상태정보 보고 체계 등을 기술한다.




(그림 1) 홈 네트워크 개념

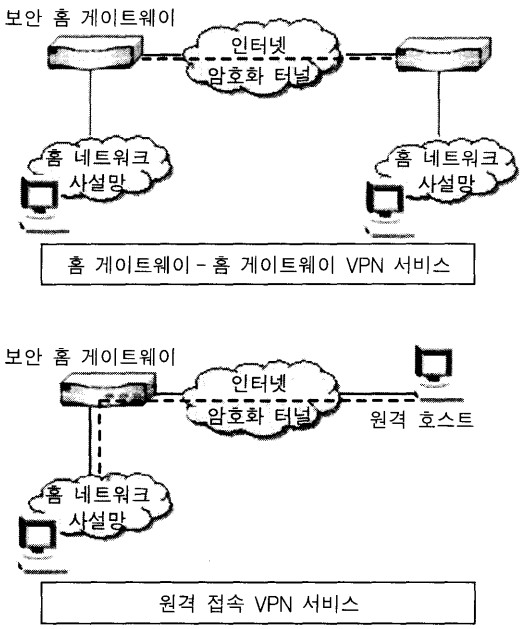
## 2. 홈 게이트웨이 보안

가정 내의 단말이나 가전 기기들은 홈 게이트웨이를 통하여 원격지에서도 손쉽게 제어하고 관리 할 수 있다. 그러나 침입자가 원격지에서 홈 네트워크를 자유롭게 접근할 수 있기 때문에 홈 게이트웨이는 강력한 인증 보안 및 상태 관리 기능을 제공해야 한다.

홈 게이트웨이 시스템은 보안 기능을 위해 홈

네트워크와 외부 네트워크 사이의 패킷 흐름을 지속적으로 모니터링 하여 패킷의 통제 및 제어를 수행하는 방화벽(Firewall) 기능, IPSec 프로토콜에 기반을 둔 터널링 기법을 이용하여 사설 네트워크간의 보안 통신을 가능하게 하는 가상 사설 네트워크(VPN : Virtual Private Network) 기능 등을 주로 사용한다.

방화벽 기능을 위해 홈 게이트웨이를 통해 전달되는 패킷을 제어하는 기능을 패킷 필터링(Packet Filtering)이라 한다. 패킷 필터링은 해당 패킷의 통과 여부를 결정하는 일련의 과정으로 홈 네트워크의 특정 클라이언트가 외부의 특정 주소로 접근하지 못하게 하거나 외부의 특정 클라이언트로부터 홈 네트워크로의 접근을 막는 등 임의의 목적에 따라 패킷을 제어하는 기능을 의미한다. 홈 게이트웨이에서는 상기한 보안 기능의 수행을 위해 보안 정책을 설정할 수 있고 외부에서 입력되는 패킷의 처리 방식을 규정할 수 있다.

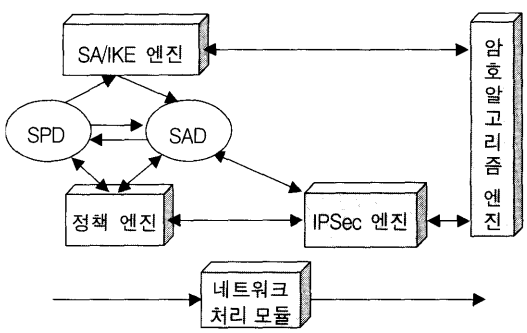



(그림 2) 홈 게이트웨이 VPN 서비스 구성

VPN은 사설 네트워크 연동의 어려움과 원거리 네트워크 구축시 과다한 비용이 소모되는 단점, 그리고 공중 네트워크의 취약한 보안성을 극복하기 위해 인터넷을 사용하여 사설 네트워크를 구축하는 기술이다. 홈 게이트웨이 시스템은 홈 네트워크와 공중 네트워크를 연결해 주는 네트워크 장치이므로 (그림 2)에서와 같이 VPN을 이용하여 가정뿐만 아니라 SOHO(Small Office Home Office) 용으로 사용 범위를 확장할 수 있다. 따라서 홈 네트워크 규모 이상의 강력한 인증과 보안 관리 기능을 필요로 한다.

VPN을 사용하고자 할 때 가장 중요한 사항은 보안 환경을 제공하는 것이며, 이를 가능하게 해주는 기술이 터널링(Tunneling) 기술과 암호화 기술이다. 터널링 기술로는 네트워크 계층에서 터널링을 제공하는 IPSec이 가장 효과적이다.

IPSec 프로토콜은 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 헤더를 이용한 IP 캡슐화와 암호화에 필요한 키 관련 부분으로 구성되며, 보안 서비스인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 부인 방지 등의 기능을 제공한다.




(그림 3) IPSec 기반 VPN

IPSec 기반 VPN 기능을 제공하기 위해서는 위에서 설명한 기술들이 (그림 3)과 같은 형태로 구현된다. IP 주소를 바탕으로 보안정책을 수행하는 정책엔진(Policy Engine), SA(Security As-

sociation)와 키 관리를 담당하는 IKE 엔진(Internet Key Exchange Engine), AH/ESP 캡슐화를 담당하는 IPSec 엔진 및 IPSec 및 IKE 엔진에 필요한 각종 암호연산 라이브러리로 구성되는 암호알고리즘 엔진, 정책엔진은 보안정책 데이터베이스(SPD)에 정책에 따라 IPSec 엔진을 호출하고 보안연결 데이터베이스(SAD)의 정보에 따라 IP 패킷에 대한 처리를 수행한다.

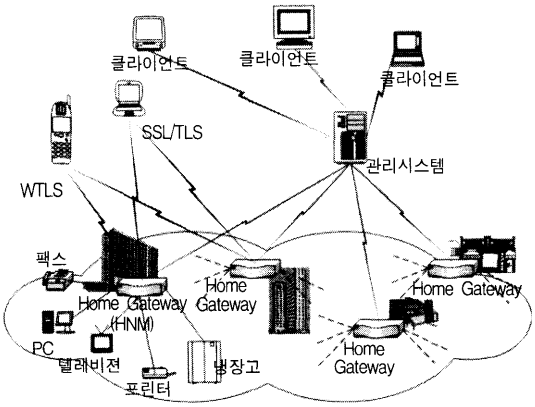
## 3. 홈 게이트웨이 관리

홈 게이트웨이 관리 형태는 (그림 4)에서와 같이 사업자 관리 측면에서의 관리 시스템(HGMS : Home Gateway Management System)과 사용자 관점에서의 관리 시스템(HNM : Home Network Manager)으로 나눌 수 있다. HGMS는 관리 도메인에 속하는 여러 대의 홈 게이트웨이 시스템을 관리하기 위한 시스템을 말하며 외부 네트워크에 위치한 관리 서버로부터 관리자가 요구하는 정보를 수집하여 분석하기 위한 시스템이다. HNM은 홈 게이트웨이 소유자 또는 HGMS가 홈 게이트웨이의 상태 및 홈 네트워크의 모든 연결 상태를 감시할 수 있도록 하는 사용자 인터페이스를 제공한다. 홈 게이트웨이 소유자는 HGMS의 도움 없이 직접 HNM을 통해 홈 네트워크를 관리할 수 있으며 이를 위해 HNM은 TLS(Transport Layer Security), WTLS(Wireless Transport Layer Security)와 같은 유·무선 보안 채널을 제공한다.

### 3.1 홈 게이트웨이 관리 구조 및 기능

홈 게이트웨이 관리 시스템 구조는 (그림 4)에서처럼 계층적 구조를 가질 수도 있고 사용자가 직접 원격으로 관리할 수도 있다. 먼저 NMS (Network Management System)는 전체 관리 도메인의 관리 정보를 총괄 관리하는 시스템이며 HGMS에서 보내주는 관리 정보를 이용하여 관리 행위를 수행한다. NMS와 HGMS는 한 시스템 내에 구현될 수 있다.

HGMS는 홈 게이트웨이에 내장된 SNMPv3 에이전트로부터 관리 정보를 수집 분석하여 지역 관리 도메인에 대한 네트워크 관리 기능을 수행하며 HNM은 홈 네트워크 상태, 홈 게이트웨이의 상태 정보, 그리고 홈 네트워크 장치들의 관리 정보를 수집하여 관리하는 기능을 제공한다. HGMS와 HNM과의 통신은 관리 정보의 안전한 전달을 위해 SNMPv3을 사용한다.



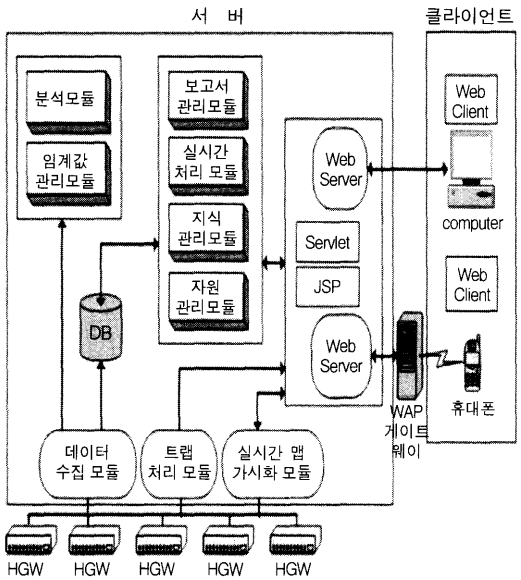

(그림 4) 홈 게이트웨이 관리 구조

### 3.2 HGMS 구조

HGMS는 홈 게이트웨이의 상태 관리뿐만 아니라 액세스 네트워크의 트래픽 관리도 수행되며, 홈 게이트웨이를 비롯한 네트워크 장치에 탑재되는 SNMPv3 에이전트로부터 관리 정보를 수집, 분석하는 기능을 제공한다. HGMS 서버는 크게 정보를 수집하고 분석하는 모듈과 관리자로부터의 분석 요청을 처리하는 모듈로 구성되고 (그림 5)는 이러한 HGMS의 구조를 나타내고 있다.

분석 정보 요청 및 처리 모듈 내부에는 보고서 관리 모듈과 실시간 처리 모듈, 지식관리 모

듈, 자원관리 모듈이 있으며 수집 및 분석 모듈은 수집 모듈, 분석 모듈, 임계값 관리 모듈로 구성된다. HGMS 클라이언트의 세부 기능 블록으로는 HGMS 계층적 실시간 노드 맵 생성 기능, HGMS 누적분석을 통한 성능 및 장애관리 기능, HGMS 무선 인터넷 인터페이스를 이용한 상태 감시 기능으로 나누어진다.




(그림 5) HGMS 구조

홈 게이트웨이 계층적 실시간 노드 맵 기능은 관리자에게 가시적이고 편리한 인터페이스를 제공한다. 이러한 계층적인 구성도를 바탕으로 대규모 그룹별 특성을 나타내는 테이블 형태의 정보도 살펴 볼 수 있고, 계층적인 구성도의 이벤트를 통하여 소규모 그룹의 홈 게이트웨이 장비 목록을 살펴볼 수 있다.

누적 분석을 통한 장애 관리 기능은 관리자에게 다양한 메뉴 인터페이스를 제공함으로써 SNMPv3 에이전트로부터 주기적으로 수집한 관리 정보를 가공하여 분석하기 위한 기능을 제공한다. 세부 기능으로는 성능 및 장애 관리 기능, 보고서 자동 생성 기능, 지식정보 관리 기능, 관리환경 설정 기능으로 구성된다.

성능 및 장애 관리 기능을 이용하여 회선 이용률 및 에러율과 같은 다양한 분석 항목을 선택하여 요일별, 일별, 월별로 분석이 가능하다. 지식 관리 기능을 이용하여 이전에 발생한 장애에 대한 데이터베이스화된 관리자 지식을 이용할 수 있으며 관리자의 등급에 따라 접근할 수 있는 관리 기능을 제한할 수 있다.

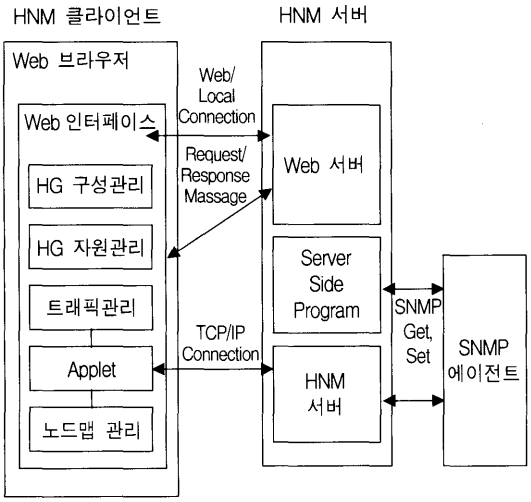
무선 인터넷 인터페이스를 통한 상태 감시 기능은 시간과 장소의 제약을 받지 않고 언제든지 필요한 정보를 휴대폰 또는 무선 인터넷 단말기를 이용하여 얻을 수 있게 하기 위하여 제공되며 홈 게이트웨이 및 중요 네트워크 중계 장치를 관리하는 기능이다.

## 3.3 HNM 구조

HNM은 홈 게이트웨이를 포함하여 홈 네트워크 장치들에 대한 기본 정보 및 상태 정보를 웹 기반으로 제공하는 시스템이다. HNM은 홈 게이트웨이에 탑재하며 홈 네트워크에 연결되어 있는 PC 및 가전기기에 대한 연결 상태를 한눈에 확인할 수 있는 노드 맵을 제공한다. 또한, 홈 네트워크 각 노드들의 구성정보 및 성능 정보를 제공한다. (그림 6)은 HNM 시스템 구조를 나타내고 있다.

홈 네트워크 및 액세스 네트워크 상태 관리 기능은 홈 게이트웨이 및 액세스 네트워크 인터페이스별 입출력 바이트 및 패킷 수, 에러율, 선로이용률의 상태 정보를 제공하며, 개별 항목들에 대해서 실시간 그래프를 통하여 실시간 데이터의 변화 추이 정보를 알 수 있다.

홈 게이트웨이 자원 이용률 조회 기능은 홈 게이트웨이의 CPU 이용률 및 메모리 사용률의 시간의 추이에 따른 변화를 출력하며, 홈 게이트웨이 상에서 동작중인 프로세스들의 실행경로, 실행상태, CPU 점유율, 메모리 사용량에 대한 정보를 조회할 수 있는 기능이다.




(그림 6) HNM 구조

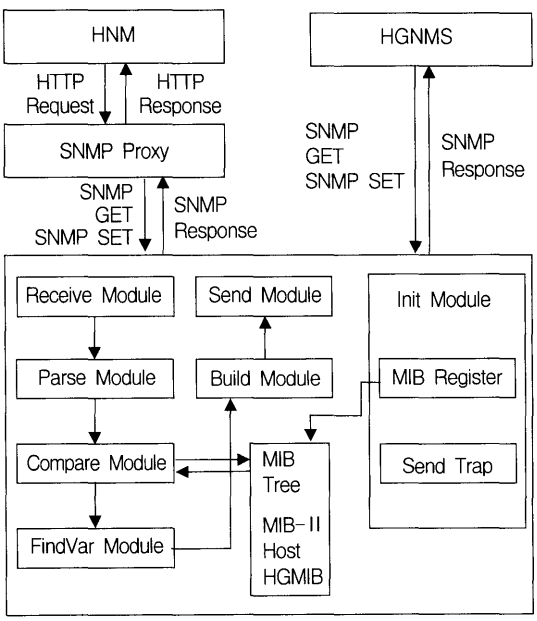
홈 네트워크 노드 맵 자동 생성 기능은 홈 네트워크에 연결되는 장치의 연결 상태를 감지하여 자동으로 홈 네트워크 장치 연결 맵을 생성한다. 홈 게이트웨이의 상태를 실시간으로 표시하며 상황판을 이용하여 실시간 선로 이용률과 에러율의 모니터링이 가능하며 새롭게 추가되거나 삭제된 노드를 자동 탐지할 수 있다.

원격 홈 게이트웨이 제어 및 시스템 구성 정보 조회 기능은 원격에서 홈 게이트웨이의 재시동 및 전원 끄기 기능을 지원하며 홈 게이트웨이에 접근 가능한 사용자를 관리하기 위한 인터페이스를 제공한다.

## 3.4 SNMP 에이전트

SNMPv3 에이전트 번들은 OSGi(Open Service Gateway initiative) 프레임워크 상에서 동작하는 소프트웨어로써 관리자는 원격에서 SNMPv3 에이전트의 라이프사이클(설치, 삭제, 추가, 변경)을 관리할 수 있다. SNMP 에이전트 번들 lbs의 역할은 홈 게이트웨이의 각 인터페이스에서 입출력되는 네트워크 트래픽 정보 및 홈 게이트웨이 관리 정보를 수집하고, 수집된 정보를 HGMS 및 HNM에 전달하는 것이다. 또한, MIB-II(Management Information Base version 2) 관리정보뿐만 아니라 HG 시스템 정보, 구성 정보, 이용률 정보, 인터페이스 정보, 서브 에이전트 트래픽 및 시스템 정보를 포함하는 사설 MIB 정보를 HGMS에게 제공한다.

SNMP 에이전트 번들의 구조는 (그림 7)과 같으며 동작은 원격의 서비스 전달 서버로부터 홈 게이트웨이의 OSGi로의 업로드로부터 시작한다. SNMP 에이전트는 MIB 모듈로부터 관리 객체 정보를 읽어 들여 MIB 트리를 구성하고 관리 시스템의 요구를 기다린다.




(그림 7) SNMP 에이전트 번들 구조

관리 시스템으로부터 받은 SNMP 메시지로부터 MIB의 오브젝트 식별자를 얻은 후 이를 통하여 이미 구성된 MIB 트리를 검색한다. 검색을 통하여 관리자 시스템에서 원하는 정보가 무엇인지를 찾아내고 해당 정보 정보를 수집한다. 수집한 정보를 포함하여 SNMP 송신 메시지를 만든 후 SNMP 프록시 또는 관리 시스템으로 송신한다.

## 4. 결 론

본 논문은 유비쿼터스 컴퓨팅의 시작점이 될 홈 네트워크를 효과적으로 관리하기 위한 홈 게이트웨이 보안 관리에 관한 것이다. 다양한 형태의 홈 네트워크 서비스가 가능하고 그에 따른 다양한 형태의 홈 게이트웨이 관리 형태가 가능하지만 홈 네트워크 서비스의 특성상 강력한 인증과 암호화 기능을 갖춘 보안 관리 방식을 필요로 한다.

이를 위해 본 논문에서는 계층적인 관리 구조와 사용자가 직접 관리하는 홈 게이트웨이 관리 구조를 제시하였으며 각각의 방식에 따른 SNMPv3 네트워크 관리 프로토콜의 사용 방식을 제안하였다. 이러한 관리 구조는 유연하고 확장성 있는 홈서비스 시나리오를 보장할 뿐만 아니라 홈 게이트웨이의 서비스 지원 범위와 무관하게 사용될 수 있는 효과적인 플랫폼을 제공한다.

## 참 고 문 헌


[1] A. Nash, W., Duane, C. Joseph, D. Brink, "PKI Implementing and Managing E-Security", RSA, 2001.

[2] M. A. Hasan, "Power Analysis Attacks And Algorithmic Approaches To Their Countermeasures For Koblitz Curve Crypto-system", 1988.

[3] Dimitar Valtchev, et al., "Service Gateway Architecture for a Smart Home", IEEE Communications Magazine, Apr. 2002.

[4] Francois Bougant, et al., "The User Profile for the Virtual Home Environment", IEEE Communications Magazine, Jan. 2003.

[5] Nathan J. Muller, "SNMP's Remote Monitroing MIB", International Journal of Network Management, WILEY, Vol.6, No.1 1996.

[6] Brent A. Miller, et al., "Home networking with Universal Plug and Play, IEEE Communications Magazine, Dec. 2001.



**김 현 철**

1990년 성균관대학교 정보통신 공학부(공학사)

1992년 성균관대학교 정보통신 공학부(공학석사)

1992년~2002년 한국전자통신 연구원(ETRI) 선임연구원

2002년~현재 (주)아이트로닉스 정보통신 연구소장

**안 성 진**

1988년 성균관대학교 정보공학과 (공학사)

1990년 성균관대학교 정보공학과 (공학석사)

1998년 성균관대학교 전기전자 컴퓨터공학과(공학박사)

1999년~현재 성균관대학교 컴퓨터교육학과 조교수

**정 진 욱**

1974년 성균관대학교 전기공학과 (공학사)

1979년 성균관대학교 전자공학 (공학석사)

1991년 서울대학교 전자계산학 (공학박사)

2002년 한국정보처리학회 회장

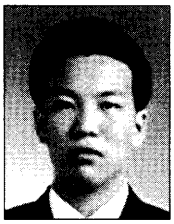
1985년~현재 성균관대학교 컴퓨터공학과 교수

**김 성 혜**

1991년 이화여자대학교 전자 계산학과(공학사)

1995년 충남대학교 전산학과 (공학석사)

1991년~현재 한국전자통신 연구원(ETRI) 선임연구원

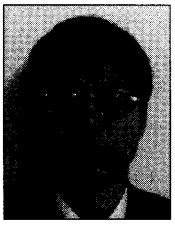


**유 윤 식**

1999년 성균관대학교 전자공학과 (공학사)

2001년 성균관대학교 전기전자 컴퓨터공학부(공학석사)

2001년~현재 한국전자통신연구원 연구원



**전 용 일**

1981년 고려대학교 전기공학과 (공학사)

1983년 한국과학기술원 전기공학과 (공학석사)

1983년~현재 한국전자통신연구원 책임연구원