제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

# 홈 네트워크 관제 센터를 이용한 홈 네트워크 관리 및 보안

안계순*, 손진호**, 윤민우*, 정태명***
*성균관대학교 정보통신공학부 인터넷관리기술 연구실
**LG 전자기술원 정보기술연구소
***성균관대학교 정보통신공학부
e-mail : *{ksahn, mwyoon}@imtl.skku.ac.kr
**jhsohn@lge.com
***tmchung@ece.skku.ac.kr

# Home Network Management Using the Home Network Surveillance Center

Gaesoon Ahn*, Jin-Ho Son**, Min-Woo Youn*, Tai M. Chung***
*IMT Lab, School of Information & Communication Engineering, SungKyunKwan University
**LG Electronics Institute of Technology Digital Network System(DNS) Group
*** School of Information & Communication Engineering, SungKyunKwan University

요 약

홈 네트워킹 기술을 이용하면 가정내의 각각의 기기를 연결하고, 인터넷에 동시에 접속할 수 있다. 뿐만 아니라 홈 네트워킹 기술로 연결된 가정 기기들은 상호운용이 가능하며 인터넷을 통해 외부에서도 가정내의 기기를 제어할 수 있다. 그러나 이러한 외부로부터의 제어 가능성으로 인하여 홈 네트워크에 대한 접근 및 제어에 대한 인증의 필요성이 대두되었을 뿐만 아니라 전자상거래의 증가 및 VPN 을 이용한 자택근무의 증가로 인하여 홈 네트워크의 보안도 중요한 관리요소에 포함되었다.

본 논문에서는 홈 네트워크 보안 및 관리를 위한 홈 네트워크 관제 센터의 구조 및 설계에 대하여 기술한다. 기존의 홈 게이트웨이에 집중되었던 홈 네트워크 관리기능과 방화벽이나 사용자 인증 등의 보안 기능을 홈 네트워크 관제 센터로 이동함으로써 보안관리의 편리성 제공 및 홈 게이트웨이의 부하를 줄일 수 있을 뿐만 아니라 좀 더 완벽한 홈 네트워크 보안을 제공할 수 있다.

## 1. 서론

CEA(Consumer Electronics Association)의 HNIT(Home Networking and IT)분과에서는 홈 네트워크에 대해서 "가전 기기 및 전자 시스템들이 원격접근 및 원격제어가 가능하도록 서로 연결하는 것" 이라고 정의하고 있다[1]. 즉 홈 네트워크를 통하여 각 제품들은 서로 연결되어 상호간에 서비스들을 공유할 수 있어야 하며, 사용자는 원격에서 분산되어 있는 제품들을 제어하거나 각각의 제품들이 제공하는 서비스를 이용할 수 있어야 한다. 예를 들면 사용자는 귀가하기 이전에 인터넷으로 보일러를 가동시켜 따뜻한 집으로 귀가할 수 있으며, 저녁식사에 사용하기 위한 음식물을 귀가 시간에 맞추어서 해동 시켜놓을 수 있다.

그러나 홈 네트워크 사용자는 공학적인 개념이 없는 일반인이라는 특성 때문에 일반인들을 위하여 쉬운 설치, 유지, 사용이 전제되어야 한다[2]. 뿐만 아니라 네트워크에 연결된 가전제품의 수 및 종류가 늘어나고, 홈 네트워크를 통하여 제공되는 서비스가 다양

화됨에 따라 자동화된 홈 네트워크 관리의 필요성이 제기되고 있다.

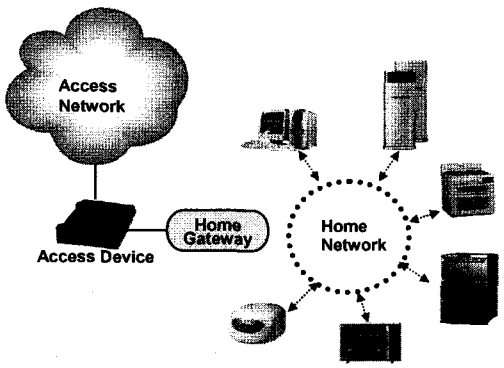
기존의 홈 네트워크 관리는 홈 게이트웨이를 중심으로 설계되었다. 그러나 홈 네트워크에 연결된 가정용 기기의 수와 종류가 늘어감에 따라 관리의 복잡성이 증대되었고, 외부에서의 홈 네트워크 접근 및 제어가 늘어남에 따라 인증 및 보안을 위한 요구사항 또한 증가하였다[3]. 이러한 이유로 홈 게이트웨이를 기반으로 한 홈 네트워크 관리 및 보안은 확장의 제한, 보안관리의 어려움 등의 문제점들이 유발되었다.

본 논문에서는 이러한 기존 홈 네트워크 관리 및 보안의 어려움을 해결하기 위하여 홈 네트워크 관제 센터를 이용한 홈 네트워크 관리 및 보안구조를 제안한다. 홈 네트워크 관제 센터는 관리 및 보안으로 인한 홈 게이트웨이의 부하를 줄이고, 자동화된 홈 네트워크 관리를 지원하며, 홈 게이트웨이에서 제공하는 것보다 다양한 보안기능을 제공하기 위하여 설계되었다.

본 논문은 총 5 장으로 구성된다. 2 장에서는 홈 네트워크의 일반적인 구조 및 홈 네트워크에서 제공되어야 하는 보안 서비스에 대하여 살펴볼 것이며, 3 장에서는 기존에 제안된 홈 네트워크 관리 구조 및 문제점에 대해서 언급할 것이다. 4 장에서는 홈 네트워크 관제 센터에 대하여 기술 함으로써 기존의 홈 네트워크 관리구조가 가지는 문제점 및 필요한 보안 서비스들을 어떻게 해결할 수 있는지를 제시할 것이다. 마지막으로 5 장에서는 결론 및 향후계획에 대하여 기술할 것이다.

## 2. 홈 네트워크 구조

일반적인 홈 네트워크 구조는 [그림 1]과 같이 외부 인터넷으로 연결시켜 주는 가입자망(access network)과 홈 네트워크로 연결된 가정용 기기들, 그리고 이들을 연결시켜주는 홈 게이트웨이로 구성된다[4].




**[그림 1] 홈 네트워크 구조**

[그림 1]과 같이 홈 네트워크를 구성하기 위해서는 먼저 홈 게이트웨이 및 각각의 가전기기들을 연결하는 기술이 필요하며, 이러한 기술 중 유선기반 기술로는 이더넷(ethernet)과 전화선을 이용하는 HomePNA (Home Phoneline Networking Alliance), 전력선을 이용하는 PLC(Power Line Communications), IEEE 1394 기술이 있고, 무선기반 기술로는 블루투스(bluetooth)와 IEEE 802.15 표준의 WPAN(Wireless Personal Area Network), UWB(Ultra Wide Band)와 IEEE 1394 를 무선으로 전송하기위한 Wireless 1394 기술이 있다[5].

홈 네트워크를 구축하기 위해서는 가전기기들의 연결로 그치는 것이 아니라 새로운 기기의 추가 시 홈 네트워크에 연결된 모든 기기들이 이를 인식 및 기능을 파악한 후 이에 따라 원하는 제어를 할 수 있어야 한다. 이를 위해서는 홈 네트워킹 제어 및 스트리밍 미들웨어 기술이 필요하다. 이러한 미들웨어 기술로는 썬마이크로시스템즈의 Jini 와 마이크로소프트웨어의 UPnP(Universal Plug and Play), 소니 및 필립스와 같은 가전회사들이 참여한 HAVi(Home Audio Video interoperability), 서비스 게이트웨이 표준인 OSGi(Open Service Gateway initiative)가 있다[6]. 이러한 홈 네트워크의 구조로 인하여 각각의 가전 기기들의 펌웨어와 미들웨어와의 정확한 연동을 위하여 펌웨어 및 미들웨어의 업그레이드가 가장 중요한 관리작업이며 이러한 작업은 일반 가정의 비 전문가들에게는 어려운 작업이다.

### 2.1 홈 네트워크의 보안 요구사항

인터넷에 연결되어 있는 네트워크는 인터넷으로부터의 불법적인 침입이나 바이러스 유입등의 위협요소를 가진다. 홈 네트워크도 미들웨어의 업데이트나 외부로부터의 사용자 접근이 가능하기 위해서는 항상 인터넷에 연결되어 있어야 하므로 네트워크 환경에서의 위협사항이 공통적으로 존재한다[3]. 따라서 식별(identification), 인증(authentication) 접근제어(access control), 기밀성(confidentiality), 무결성(integrity), 가용성(availability)과 같은 일반 엔터프라이즈 환경에서의 보안 서비스가 홈 네트워크 환경에서도 필요하다. 그러나 홈 네트워크 환경은 일반 가정의 비 전문적인 사용자들에게는 보안 소프트웨어 설치 및 재구성 어려움, 개별 보안 소프트웨어간의 상호 연관성/연동 어려움, 보안 시스템 비용 부담이라는 기존의 네트워크 환경과의 차이점을 갖게 된다. 이러한 차이점으로 인하여 기존 엔터프라이즈 환경과는 다른 보안 요구사항을 가진다.

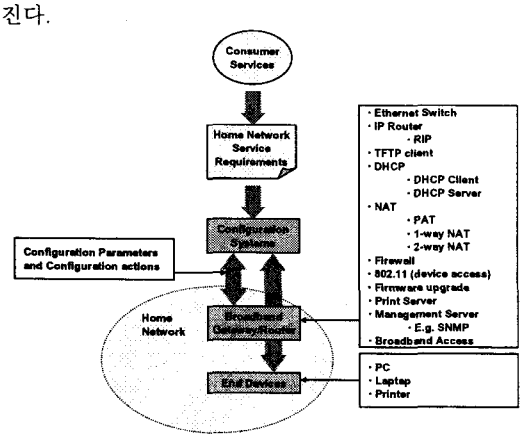
따라서 홈 네트워크를 위하는 보안 시스템은 사용자가 쉽게 조작할 수 있어야 하며, 설치되어 있는 각각의 보안 시스템간에 쉬운 연동이 가능해야 하고, 홈 네트워크의 특징에 맞게 경량화 되어야 한다.

## 3. 기존의 홈 네트워크 관리 구조

현재 제안된 홈 네트워크 관리 기술들은 대부분 홈 게이트웨이를 중심으로 제안되고 있다.

[그림 2]는 홈 게이트웨이 중심의 홈 네트워크 관리 기능 구조를 나타낸다[7]. 그림에 나타난 바와 같이 현재 홈 게이트웨이에서는 각 가전기기들에게 IP 를 할당하기위한 DHCP 서버, 홈 네트워크의 보안을

위한 방화벽 및 NAT, 홈 네트워크에 연결된 가전기기들의 펌웨어 업그레이드(firmware upgrade), 홈 네트워크를 관리하기 위한 SNMP 서버와 같은 기능이 이루어진다.




[그림 2] 홈 네트워크 관리의 기능 구조

홈 게이트웨이에서는 이러한 관리에 관련된 작업들 뿐만 아니라 사용자가 외부로부터 접근할 수 있는 웹 인터페이스(web interface)도 제공해야 하며, 외부로부터의 불법적인 접근을 막기 위해서 사용자 인증 작업도 이루어 져야 한다[3].

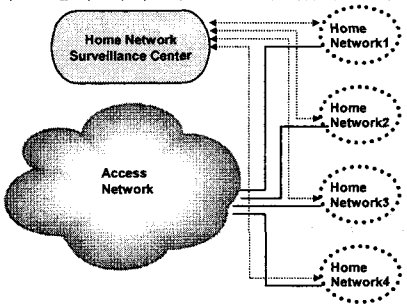
홈 게이트웨이는 일반 가전기기에 구현되거나 PC 기반으로 구현된다. 일반 가전기기에 구현될 경우에는 앞서 설명한 것과 같이 다양한 관리작업들을 수행하기 위하여 높은 사양의 시스템이 요구되며, 홈 네트워크에 포함된 가전기기들의 수가 늘어나거나 관리요소가 추가될 경우 홈 게이트웨이의 업그레이드는 불가능하기 때문에 새로운 홈 게이트웨이를 설치해야 하는 문제점이 발생한다. 이러한 경우 두 개의 홈 게이트웨이 간의 작업 스케줄링등의 작업이 추가로 필요하다. PC 기반의 홈 게이트웨이의 경우에도 새로운 관리항목이 추가될 경우나 홈 네트워크내의 가전기기들의 펌웨어가 업그레이드되어야 할 경우 홈 게이트웨이에서 작업이 이루어 지기 때문에 사용자가 이러한 작업을 직접해야 하는 문제점이 발생한다.

## 4. 홈 네트워크 관제 센터

앞 장에서 제시된 문제점들은 홈 네트워크 관제 센터의 도입으로 해결될 수 있다. 홈 네트워크 관제 센터는 [그림 3]에서와 같이 관제 센터의 관리 범위에 속해있는 홈 네트워크를 관리한다.

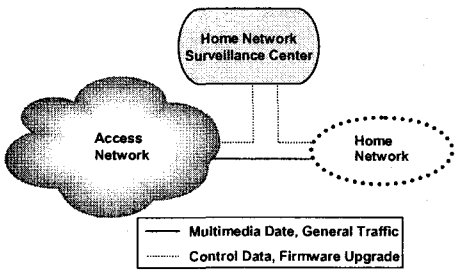
홈 네트워크 관제 센터에서는 기존의 홈 게이트웨이에서 수행되는 홈 네트워크 관리작업 중 일부 및 보안에 관련된 작업 및 웹을 이용한 사용자 인터페이스를 제공한다. 즉 홈 게이트웨이는 홈 네트워크에 연결된 가전기기들에 대한 간단한 정보만을 가지고 있고, 이를 이용하여 복잡하거나 많은 연산을 필요로하는 작업들은 홈 네트워크 관제 센터에서 이루어지게 된다.

홈 게이트웨이는 해당 홈 네트워크내에 존재하는 가전기기들의 종류 및 수량, 가전기기들이 사용하는 펌웨어의 버전, 홈 네트워크에서 사용하는 미들웨어의 정보등 홈 네트워크 관리에 필요한 항목들을 MIB(Management Information Base) 형태로 보관하게 된다. 관제 센터는 각각의 홈 게이트웨이가 보관하고 있는 MIB 을 이용하여 각각의 홈 네트워크의 상태를 파악할 수 있다. 각 홈 게이트웨이에 있는 MIB 을 이용하여 홈 네트워크 관제 센터는 관리 대상 가전기기들의 종류를 파악하여 일괄적으로 펌웨어 업그레이드와 같은 작업을 할 수 있다. 따라서 사용자는 자동화된 홈 네트워크 관리 서비스를 받을 수 있게 된다.




[그림 3] 관제 센터를 이용한 관리 구조

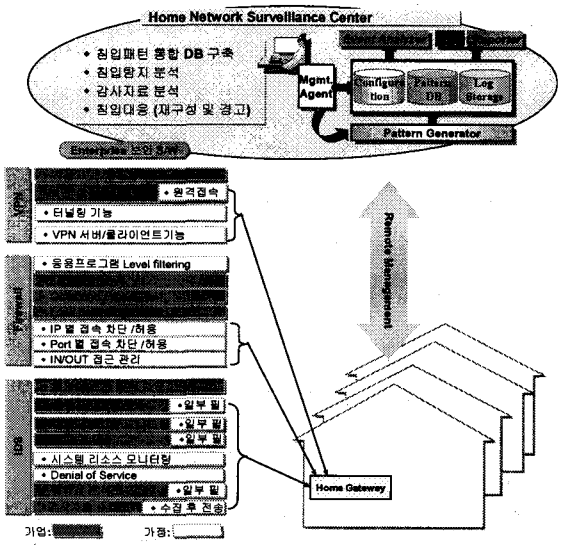
홈 네트워크 관리 센터를 이용하였을 경우 인터넷에서 홈 네트워크로 유입되는 트래픽을 구분하여 관리할 수 있다. 즉 [그림 4]에 나타난 바와 같이 소프트웨어 업그레이드나 가전기기들의 제어를 위한 접근과 같은 제어 트래픽은 홈 네트워크 관제 센터를 통하여 유입되기 때문에 홈 게이트웨이에서 지원되는 것에 비하여 더욱 강화된 사용자 인증 및 제어 데이터에 대한 무결성 검사를 서비스할 수 있다. 뿐만 아니라 홈 게이트웨이는 홈 네트워크 관리 센터로부터 유입되는 데이터에 대해서는 특별한 검사를 할 필요가 없기 때문에 홈 게이트웨이의 부하 역시 줄일 수 있다.




[그림 4] 관제 센터를 통한 데이터의 흐름

따라서 이러한 홈 네트워크 관제 센터를 이용하여 홈 네트워크를 관리할 경우, 2.1 절에서 언급한 홈 네트워크에 특화된 보안 서비스들을 쉽게 제공할 수 있다. 즉 제어를 위한 외부에서의 접근이나 펌웨어 업그레이드와 같이 가전기기들에게 직접 영향을 미치는

데이터들은 홈 네트워크 관제 센터를 거치기 때문에 방화벽이나 Anti-Virus 와 같은 기능을 홈 네트워크 관제 센터에서 제공하면 효율적으로 보안 서비스를 제공할 수 있다. 개별 홈 게이트웨이에서는 단순히 관제 센터와의 VPN 연결만 유지하면 되기 때문에 각각의 홈 게이트웨이에 대한 부하를 줄여 경량화 된 홈 네트워크 보안 시스템을 갖출 수 있다. [그림 5]는 기존의 엔터프라이즈 환경에서의 보안 서비스들이 홈 네트워크 관제센터에 적용된 경우를 나타내고 있다.




[그림 5] 홈 네트워크 관제 센터의 구조

외부에서 접근할 수 있는 사용자의 추가 및 삭제, 바이러스 탐지항목 추가, 업그레이드를 위한 펌웨어에 대한 인증 등의 작업은 홈 네트워크 관제 센터에서 이루어 진다. 따라서 홈 네트워크의 사용자들은 홈 네트워크의 설정 변경 시 홈 네트워크 관제 센터로 요청을 함으로써 해당 작업이 이루어 질 수 있기 때문에 일반 사용자의 직접 조작으로 인한 실수를 줄일 수 있다.

## 5. 결론 및 향후과제

홈 네트워크 기술이 가전 시장을 점유하기 위해서 사용자는 홈 네트워크 기술을 이해하고, 설치할 수 있으며, 구축된 홈 네트워크를 유지하고, 홈 네트워크에 연결된 가전기기들을 사용할 수 있어야 한다[2]. 뿐만 아니라 홈 네트워크 환경에서의 취약점을 이해한 후 적합한 보안 시스템들을 구축해야 안전한 홈 네트워크 환경을 구출할 수 있다. 그러나 이러한 작업들을 공학적인 개념이 부족한 일반인들이 해야 한다는 점과 이러한 작업들이 한정된 작업공간을 가지고 있는 홈 게이트웨이에서 이루어져야 한다는 점이 문제점으로 제시되고 있다.

본 논문에서는 이러한 문제점을 해결하기 위한 홈 네트워크 관제 센터의 도입에 대하여 살펴보았다. 홈 네트워크 관제 센터를 도입함으로써 기존의 홈 게이트웨이에 편중되었던 홈 네트워크 관리 작업을 홈 네트워크 관제 센터와 양분함으로써 홈 게이트웨이의 부하를 줄일 수 있으며, 관리의 자동화도 이룰 수 있다. 또한 기존의 보안 서비스를 홈 게이트웨이에서 적용될 보안 서비스와 홈 네트워크 관제 센터에서 적용될 보안 서비스로 구분하여 좀 더 강화된 보안 서비스의 적용이 가능하게 되었다.

그러나 홈 네트워크 관제 센터가 도입되기 위해서는 관리대상인 홈 게이트웨이들에서 동일한 인터페이스가 제공되어야만 가능하다. 따라서 현실에서 홈 네트워크 관제 센터의 도입을 위해서는 이종의 홈 게이트웨이들을 관리하기 위한 방법에 대한 연구가 필요하다. 또한 홈 네트워크에 특화된 관리정보에 대한 MIB 정의 및 홈 게이트웨이가 관리하고 있는 MIB 정보를 효율적으로 업데이트하기 위한 방법에 대한 연구가 향후과제로 남아있다.

## 참고문헌

[1] R. Holtz et al., "Guide to Home Networks", http://www.ce.org/networkguide/default.asp

[2] Rose. B, "Home networks: a standards perspective", IEEE Communications Magazine , Volume: 39 Issue: 12 , Dec 2001, pp78-85

[3] Ungar. S.G, " Home network security" 2002 IEEE 4th International Workshop on Networked Appliances, pp41 - 48

[4] 한국 IPv6 포럼, 홈네트워크 및 정보가전 워킹그룹 2001 년 1 차회의 자료, http://www.ipv6.or.kr/wg/appliance

[5] 배창호, 김영성, 장호성, "IEEE 1394 를 이용한 홈 네트워킹에 관한 연구", 전자통신동향분석 제 17 권 제 2 호 2002 년 4 월

[6] Elbassioni. K, Beizhong Chen, Kamel. I, "Efficient service management in home gateway", 2002 IEEE 4th International Workshop on Networked Appliances, pp225-233

[7] Moyer. S, Tsang. S, "Home network configuration management and service assurance" 2002 IEEE 4th International Workshop on Networked Appliances, pp77-86