무선 환경의 홈네트워크 보안 메카니즘의 설계

김정태, 류대현*, 허창우, 류광열
목원대학교, 한세대학교*

Design of an Home Network Security Mechanism for Wireless Environment

Jung-Tae Kim, Dae-Hyun Ryu*, Chang-Wu, Hur, Kwang-Ryol Ryu
Mokwon University, Hansei University*
E-mail : jtkim3050@mokwon.ac.kr

요 약

홈 네트워킹 기술은 기존의 유선방식의 홈 네트워킹 기술과 무선 방식 홈 네트워킹 기술로 나눌 수 있다. 현재 다양한 홈 네트워킹 기술이 존재하는 데 각 기술마다 장단점을 가지고 있어 각 기술 영역에 따라 독립적으로 발전되고 있다. 현재 각각의 고유한 기술방식에 따라 배타적으로 시장을 점유하고 있다. 따라서 본 논문에서는 향후 유비쿼터스 환경하에서의 무선 데이터통신의 사용 시 고려해야 하는 보안 메카니즘에 대해서 알아보았다.

Ⅰ. 서 론

기존의 통신 네트워크하에서의 유선망과 무선망에서는 서로 다른 네트워킹을 사용하는 디바이스들 간에는 통신이 불가능하였다. 즉, 유비쿼터스 환경에서는 서로 다른 네트워크에 접속된 디지털 기기 간에도 상호 통신이 보장되어야하는데 현재 홈 네트워크를 위하여 다양한 미들웨어 기술이 개발되고 있지만 이러한 문제는 완전히 해결되지 못하고 있다. 가정 내에서 존재하는 다양한 디바이스들이 각각 서로 다른 홈 네트워킹 기술에 의하여 연결되어 있을 경우에 각 디바이스 간의 정보를 교환해 줄 수 있는 방법이 없으면 데이터 전송이 불가능하다. 이것을 가능하게 하는 것이 미들웨어 기술이다. 미들웨어 기술을 이용하면 분산형 연산 환경과 서비스를 지원할 수 있으며, 데이터 네트워크와 제어 네트워크를 쉽게 통합할 수 있고, 다양한 네트워킹 기술을 이용하는 디바이스간의 통합이 용이하며 상위 계측의 응용을 구현하기에 용이하다. 일반적으로 미들웨어의 대표적인 기술은 HAVIi(Home Audio Video interoperability), SUN 사의 Jini, 그리고 마이크로소프트사가 지원하는 UPnp(Universal Plug and Play) 등이 있다. 기존의 연구개발 동향의 경우 보안성을 유지시키기 위하여 미들웨어 환경에서의 프로토콜에 대한 보안 대책을 수립하였다. 이와는 대조적으로 추후에는 종단 간에서의 이종간의 단말장치의 다양성으로 인해 각 각의 시스템에 적합한 암호알고리즘, 암호 등급의 부여 등에 대한 고려가 필수불가결하다. 따라서, 시스템의 효율적인 성능 분석을 위해서는 필수적으로 고려되어야 한다. 그런데 전세계적으로 이에 대한 원천적인 기술 혹은 아이디어의 정립이 되지 않아 본 논문에서는 이에 대한 요구사항을 정의하고자 한다.

일반적으로 홈 네트워크 시스템 구현의 일부분으로서 현재 업체에서 구현하고자 하는 홈 네트워크 시스템에서의 미들웨어에서의 각종 응용 분야를 실현하기 위한 미들웨어 에서의 구성을 알아본다. 암호 알고리즘을 펌웨어로 구현하여 정보가전이나, 무선기기, PC 등 모든 종류의 기기들을 연결하는 네트워크 구조로 발전되어 가고 있다. 이경우 가정이나 작은 사무실과 같이 관리자가 없는 네트워크에서 사용자의 작업없이 쉽게 표준화된 방법으로 기기간의 연결이나 인터넷으로의 연결을 제공 가능하게 한다. 기존 PC에서 디바이스를 제어하던 Plug and Play 개념을 확장하여 사용자에게 어떤 작업도 요구하지 않고 기기를 네트워크에 접속시킨다. 따라서 기기는 언제든지 네트워크에 접속시킬 수 있고 IP 주소나 기능 등을 네트워크에 연결된 다른 기기들에게 알려줄 수 있다. 또한 네트워크에서 빠져나올 때도 다른 기기에 영향을 주지 않고 연결을 해지할 수 있다.

Ⅱ. 홈 네트워크에서의 보안 모델

정보화 사회가 진행됨에 따라 기업의 기술, 영업 비밀 또는 개인의 민감한 데이터 파일을 정확하고 (무결성) 안전하게(기밀성) 관리하는 기술의 중요성이 부각되지만 정보의 도용, 남용, 해커, 불법 접

근 등 정보화 사회의 역기능은 계속 증가하고 있다. 이에 과거 국방 등에 한정되어 사용하던 암호기술을 기업 정보나 주요 공공 정보, 전자상거래 정보, 그리고 개인의 프라이버시 보호를 위해 사용되어지고 있으며, 국가적 차원에서 권장되고 있다. 홈 네트워크는 현재 가장 주목받고 있는 차세대 IT 기술로써 댁내의 정보가전기기에 대한 제어, 관리, 통합 및 연동을 바탕으로 인터넷과 결합하여 생활의 편리함을 극대화하기 위한 기술의 집합체이다. 홈 네트워크는 그 기술적인 계층에 따라 물리적인 데이터 전송을 위한 하부 네트워크 기술과 상위 응용과의 연동을 위한 미들웨어 기술 그리고 각각의 가전기기에 적용되는 정보가전 기술로 나누어진다. 현재는 광대역 통신, 무선인터넷, 센서 기술 등과 결합하여 유비쿼터스 컴퓨팅으로 확장되어 가고 있다. IEEE1394 기술은 오디오 비디오 기기의 디지털화가 이루어지고 멀티미디어 환경이 부상함에 따라 이들간의 공통된 새로운 인터페이스 방식의 필요에 의해 발생한 직렬 버스 방식을 이용한 디지털 인터페이스 방식으로, 고속의 실시간 데이터 전송을 가능하게 해 주는 차세대 핵심 기술이다. 기가비트급의 높은 데이터 전송율을 자랑하는 IEEE1394 기술은 멀티미디어 PC와 오디오/비디오 등 높은 대역폭을 요구하는 가전기기를 하나로 묶어줄 수 있는유일한 기술이며, 그 위에 TCP/IP 프로토콜을 얹어서 인터넷과도 직접 연결되므로, 옥내 통신망 구축을 위하여 제안되고 있는 HomeRF나 Bluetooth, 그리고 IEEE 802.11 계열의 기술들과 비교하면 그 효용성과 기능성, 그리고 필요성과 속도 면에서 다른 위치를 점유하고 있다. 따라서 IEEE1394 기술은 1394b와 같은 유선 홈 네트워킹 기술을 사용하거나 IEEE802.1la 혹은 11g와 같은 무선 랜 기술을 이용한 Home Network의 Backbone 기술을 이용하면 IEEE1394 기술이 갖고 있는 미래의 시장 규모는 가히 폭발적이라 할 수 있다. 홈 네트워킹은 일반적으로 PC를 비롯한 가정내 정보가전기기들이 하나의 네트워크로 통합되어 통신이 가능하도록 함을 일컫는다. 홈네트워킹은 네트워킹기술, 기반소프트웨어 그리고 정보 가전기기의 발전에 따라 급속히 확산되고 있다. 간단히 '가정내 정보화'라고 표현할 수 있는 홈네트워킹은 멀티PC를 갖고 있는 가정이 증가하면서 그 중요성이 대두되기 시작했다. 지난 90년대의 디지털혁명은 산업현장에 엄청난 영향을 주어 정보화가 모든 업무추진의 기본 방향이 되었으며 그 중심에 PC와 전세계를 엮어주는 인터넷이 있었다. 그러나 21세기에는 그 주역이 산업현장이 아닌 가정내부로 들어가고 있다. 그 이유는 여러 가지가 있겠지만 우리의 삶을 보다 풍요롭고 편리하게 하는 홈 네트웍크의 문화가 중요시되는 시대가 되었기 때문이다. 2005년 세계 3대 인터넷 정보가전 대국 실현을 목표로 정보통신부에서는 홈네트워킹분야를 포함하여 인터넷 정보가전 기술개발 사업을 2000년 11월 확정하여 2002년까지 총 1,470억원을 투입하기로 하였다. 또한 2000년 3월에 정보가전관련 산.학.관 관련기관으로 구성된 '인터넷 정보가전 산업협의회'를 통해 제반 기술개발을 주도하고 있으며 핵심제품의 경쟁력 강화를 위한 기반기술 확보에 주력하고 있다. 협의의 홈네트워킹은 유/무선을 통합하는 네트워크기술에 한정되지만 광의의 개념은 이를 기반으로 정보가전기기와의 통합, 그리고 이러한 하드웨어를 제어하고 관리할 수 있는 기반 소프트웨어를 총칭하여 홈네트워킹이라고 할 수 있다. 홈네트워킹은 네트워킹 기술의 발전과 이를 바탕으로 운영되는 정보가전기기 그리고 이러한 통합환경을 원활히 작동시켜주는 응용소프트웨어의 발전이 함께 이루어져야 하기 때문에 무엇보다 관련기술의 완성도와 표준화의 작업이 중요하다. <표1>은 다양하게 발전되고 있는 홈네트워킹 분야별 관련기술 내용을 정리한 것이다.

현재 인터넷에서 사용되고 있는 IPv4는 이동 호스트의 현재 위치에 대한 정보를 표현할 수 없고 호스트가 최초에 접속하고 있는 홈 네트워크에서의 위치 정보를 표현 할 수 있다. 이러한 인터넷 단말들의 이동성 및 홈네트워크를 구현하기 위한 기반 기술 등이 표준화로 개발 중에 있다. 현재 하부 네트워크 계층과 정보가전기기의 제어 및 관리를 위한 응용 계층 사이의 인터페이스에 해당하는 UPnP, Jini, OSGi, HAVi와 같은 다양한 홈 네트워크 미들웨어는 어느 것도 기술적인 우위를 점유하지 못한 상태로 상호 공존하고 있다. 이러한 다양한 홈 네트워크 미들웨어들은 자신만의 고유한 방식으로 댁내에 존재하는 정보가전기기를 제어, 관리, 통합하고 있으며 각각의 정보

<표 1> 홈네트워킹 분야별 관련 기술

분 야	기 술	내 용	국내적용
홈네트워킹	HomePNA	전력선 네트워킹 기술	상용화
	PLC	전력선 네트워킹 기술	개발중
	IEEE 1394	디지털기기간 전송 표준	일부상용화
	이더넷 랜	기업내 표준 네트워킹 방식	상용화
	홈RF	가정내 로컬 무선 네트워킹	상용화미정
	802.11b	무선 네트워킹의 표준(WIFI)	상용화
	블루투스	정보기전연결용 무선 네트워킹	개발중
	홈게이트웨이	인터넷과 유무선통합 홈네트워킹	개발중
정보가전기기	홈서버	가정내 통합 관리서버	개발중
	디지털TV	디지털HDTV, PDP 등	상용화
	정보가전제품	인터넷냉장고, 전자렌지, DVD	일부상용화
	게임기	PS2, XBOX, 삼성게임기 등	상용화
	휴대용 정보단말	PDA, 이동전화, 노트북PC 등	상용화
기반소프트웨어	RTOS	정보가전용/홈서버용 실시간OS	개발중
	정보가전 미들웨어	Jini, UPnP, HAVi, HWW 등	개발중
	시스템유틸리티	가전보안, 인터페이스, DB 등	개발중

를 교환하기 위한 방법이 존재하지 않는다. 그러므로 현재 홈 네트워크 미들웨어 기술의 가장 핵심인 OSGi를 기반으로 다양한 미들웨어를 연동하기 위한 UPnP 프로토콜의 설계 및 구현에 초점을 맞추

고 있다. 가정내 네트워크의 신규 설치 없이 UPnP (기기간 Networking 및 Control용 OS)를 통한 Home MM 구현 안 제시하고 있으며, oMS와 Alliance 기기업체는 Home MM 환경 대응을 위해 UPnP 내장형 제품으로 출시되고 있는 경향이며, 다음은 그 주된 회사의 연구개발 동향이다.

• 홈 네트워크의 세계시장 영역
- 프로토콜과 표준 : EHS, HAVi, Jini, Konnex, UpnP, VHN/R7.4
- 전용 유선 네트워크 : IEEE 802.3, FireWire, USB
- 전화회선 베이스의 네트워크 : HomePNA
- 전력라인 네트워크 : HomePlug, CEA R7.3
- 무선 네트워크 : IEEE 802.11x, HomeRF, Bluetooth, HyperLAN
- 네트워크 기기 메이커 : D-Link, Linksys, Netgear, SMC Networks

• Mobile Application

UPnP를 이용한 네트워크 프로그램 모듈을 모바일 환경에 적합하면, 생산, 재고, 배송 관리 등을 위한 제조분야, 상품, 회원, 배송, 판매 관리 등을 위한 유통분야, 은행, 증권, 신용카드, 보험 업무 등을 위한 금융분야, 통계리서치, 수도검침, 전기검침 등을 위한 통계, 검침 분야, A/S 분야, 모바일 엔터테인먼트 사업 등 폭넓은 분야에 활용 될 수 있다.

III. 보안 기술의 요소

가. 무선 환경에서의 보안 요구 조건

1) Eavesdropping : 무선 네트워크망에서 가장 기본적인 위협요소이다. 따라서, 이에 대한 기밀성을 보장하기 위한 알고리즘의 선택이 중요하다.
2) Tampering : 제 3자로부터 중요한 정보를 얻기 위해서 트래픽에 가장하여 들어가 정보를 변경하는 위협적인 방법이다. 따라서, 이러한 위협 요소에 대처하기 위한 무결성(Integrity)에 대한 대책을 세워야 한다.
3) Replayin attack : 공격자가 도청한 내용을 제 3자에게 분배하는 공격 방업으로 이에 대한 메시지의 완전성을 보장하기 위해서 timestamp 등의 방법을 사용해야 한다.

나. 무선 네트워크망의 특징

- Use of wireless medium
- Heterogeneous of device capabilities and requirement
- Heterogeneity of applications
- Mobility
- Low cost and Ease-of-use

IV. 무선 네트워크망에서의 보안 메카니즘

일반적으로, 무선 통신망의 경우 보안 위협 및 요구사항에 따라서, 실현하고자 하는 무선 환경에 맞추어 보안 메카니즘을 설정하게 된다.

첫째로, 시스템간의 제어를 위해 접근 가능한 인증 서버와의 연동성에 대해서 고려해야 한다. 둘째로, 두 사용자 간에서의 보안 등급(SA : Security Association)이 성립되고, 두 사용자간의 상호 인증 문제가 인증 서버를 통해 수행되어야 하며 세션 키를 공유해야 한다. 이렇게 함으로써 실제적인 통신이 성립하게 된다. 따라서 다음에서는 이러한 보안 메케니즘의 절차에 대해서 살펴본다.

1. Trust & Authentication
2. Authentication & Key Management
3. Secure Routing(Availability)
4. Communication Protection
   - Confidentiality, Integrity and Freshness
5. Other mechanism
   - Firewall, antivirus, IDS

Link Layer Security(LLS)는 LLC(Logical Link Control) 와 MAC(Medium access control) 사이에 존재한다. LLS는 일반적인 통신 경로 구조를 제공하고, 통신 속도와 정보보호의 요구조건 상호간의 trade-off 관계를 유지하며 암호화, 해쉬 알고리즘을 허용한다. LLS의 기본적인 형식이 (그림1)에 나타나 있다. 일반적으로 패킷의 암호화가 수행되었다면, 수신자는 비밀키를 사용하여야 하고 DES, AES 등의 대칭키 암호화 방식을 사용하여 데이타를 복호화한다. 또한 데이터의 무결성을 보장하기 위해서 수신된 MAC 값을 계산하게 되고, 이때 HMAC-MD5 알고리즘을 일반적으로 사용한다.

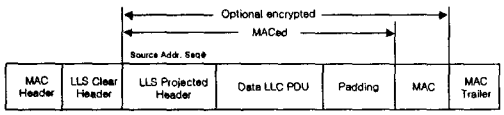

그림 1. LLS 보호 패킷의 형태

일반적으로 원거리의 서버와 시스템을 연결하기 위한 상향 및 하향 링크의 경우, 일반적으로 종단간 보안 프로토콜을 사용하게 되는데, RSA, DH등의 비대칭 알고리즘을 사용하게 된다. 그런데, 무선통신 환경하에서는 낮은 알고리즘의 연산 속도와 리소스 등을 고려해야 한다. 따라서, SDS는 IPSec과 TLS와 같은 종단간 암호 프로토콜에서 주로 사용되어지며, 낮은 속도 계산을 하는 무선 장치간에서의 효율적인 성능을 제공한다. SDS를 위한 절차를 살펴보면 다음과 같다. 먼저 클라이언트

는 SDS 서버와 통신하여 LLS SA를 설정하고, 원거리 서버와 연결하기 위하여 IPSec/IKE 혹은 TLS 프로토콜을 사용하여 연결을 수행한다.

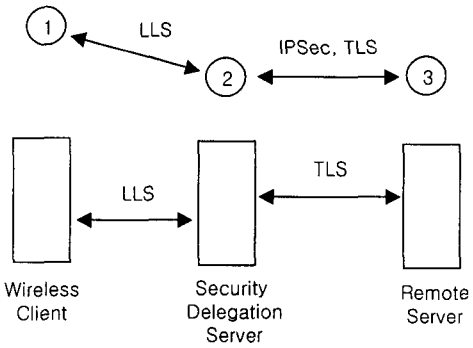

그림 2. SDS 서버를 가진 보안 통신 경로

V. 결 론

본 논문에서는 유비쿼터스 환경하에서의 홈네트워크 환경에서 야기될 수 있는 보안성의 문제점에 대해서 알아보고, 고려해야 할 내용에 대해서 설명하였다. 고려 대상이 되는 핵심 기술들은 기존의 유선망과 무선망에서 사용되고 있는 기술로서 유무선 통합 환경에서는 보안 알고리즘의 설정 및 키의 통합 분배 등에 대한 연구가 반드시 필요하리라 생각된다.

참고문헌

[1] C. M. Ellison, "Home network security," Intel Technology Journal, Vok.6, No.4, Nov. 2002

[2] P. Krishnamurthy, J Kabara and T. Anusas-amornkul, "Security in Wireless Residential Networks", IEEE Transactions on Consumer Electronics, Vol.48, N.1, pp.157-166, Feb. 2002

[3] http://ccmc.knu.ac.kr/files/research/home.html

[4] 배창호, 외 2인, "IEEE 1394를 이용한 홈 네트워킹에 관한 연구", 전자통신분석 제17권 제2호 2004 4권, pp.1-pp.6

[5] Hongmei Deng 외 2인, "Routing Security in Wireless AD Hoc Networks", IEEE Communication Magagine, Oct. 2002, pp.70-75