이종 시스템간의 홈네트워크 보안을 위한 프레임구조의 설계

김정태
목원대학교

Design of an End-to-End Home Network Security Frame for Heterogeneous System

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

인터넷을 이용한 정보가 모든 정보 전달의 기본이 되고 있다. 따라서 이러한 정보 전달의 보호를 위한 정보보호 산업이 급성장하게 되었다. 따라서, 본 논문에서는 향후, 2007년 경에 IPV6를 기반으로 하는 유비쿼터스 환경 하에서의 각 가정의 홈 네트워크를 구성할 때 필요한 보안적인 측면의 방법에 대해서 제시하고자 한다. 이러한 다양화된 디지털 매체가 디지털 가전, 정보통신 시스템과 접속하여 새로운 메카니즘의 보안 설계 대상이 필요하게 됨에 따라서, 새로운 정보보호의 접근이 필수적이다. 본 논문에서 제시하고자 하는 내용은 암호학적으로 안전한 홈네트워크의 구성과 이를 실현하기 위해서 요구되어지는 다양한 고려사항 등을 분석하여 차세대의 멀티 컴퓨팅 환경 하에서의 정보보호 시스템 구축에 대한 알고리즘 및 개발에 도움이 되고자 한다.

Ⅰ. 서 론

홈 네트워킹 기술은 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 있으며, 현재 각각의 영역에 따라 독립적으로 발전되고 있다. 현재 각각의 고유한 기술방식에 따라 배타적으로 시장을 점유하고 있다. 따라서 서로 다른 네트워킹 기술을 사용하는 디바이스들 간의 통신이 불가능하다는 것이다. 따라서 서로 다른 네트워킹을 사용하는 디바이스들 간의 통신이 불가능하다는 것이다. 즉, 유비쿼터스 환경에서는 서로 다른 네트워크에 접속된 디지털 기기 간에도 상호 통신이 보장되어야 하는데 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, 데이터통신 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), SUN사의 Jini, 그리고 마이크로소프트사가 지원하는 UPnp(Universal Plug and Play) 등이 있다. 기존의 경우 보안성을 유지시키기 위하여 미들웨어 환경에서의 프로토콜에 대한 보안대책을 수립하였다. 이와는 대조적으로 추후에는 종단 간에서의 이종간의 단말장치의 다양성으로 인해 각 각의 시스템에 적합한 암호알고리즘, 보안 등급 등의 고려가 시스템의 효율적인 성능 분석을 위해서는 필수적으로 고려되어야 한다. 그런데 전세계적으로 이에 대한 원천적인 기술 혹은 아이디어의 정립이 되지 않아 본 논문에서는 이에 대한 개념을 기술하고자 한다.

Ⅱ. 관련 연구의 기술동향 분석

홈네트워킹을 위한 많은 연구들이 이미 많은 국가에서 진행되고 있다. HAVi는 IEEE1394를 기반으로 하여 A/V 서비스를 제공하기 위해 제안된

미들웨어이다. 하지만 디바이스의 위치에 따른 그룹 제어나 다른 프로토콜들 사이의 상호 운영을 지원하는 것은 고려하지 않고 있다. UPnp의 경우 마이크로소프트에 의해 제안된 홈과 오피스 네트워크를 위한 미들웨어이다. 하지만 IP기반의 네트워크만을 지원하고 있으며 디바이스 자체의 높은 컴퓨팅 파워를 요구한다. Jini의 경우 홈과 사무실 네트워크를 위해 제안된 미들웨어로서 디바이스를 네트워크를 위해 제안된 미들웨어로서 디바이스를 네트워크 상에서 찾는 look-up, discovery 서비스를 가지고 있다. 다음은 기본적인 홈 네트워킹을 구성하기 위한 기술을 나타내고 있으며, 각 회사들이 추구하는 기술 및 내용을 기술하였다.

1. Home PNA
2. 전력선 네트워크
3. 블루투스(Bluetooth)
4. HomeRF
5. 802.11B/Wi-Fi
6. IEEE1394 / HAVi(Home Audio Video Interoperability)

현재 인터넷에서 사용되고 있는 IPv4는 이동 호스트의 현재 위치에 대한 정보를 표현할 수 없고 호스트가 최초에 접속하고 있는 홈 네트워크에서의 위치 정보를 표현할 수 있다.

III. 홈 네트워크 미들웨어 연동기술

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 정보를 교환하기 위한 방법이 존재하지 않는다. 다음의 그림1은 홈네트워크의 미들웨어의 구성도이다.

IV. 선행 연구의 문제점

기존에 개발되고 있는 홈 네트워크 시스템 구현의 경우, 현재 업체에서 구현하고자 하는 홈 네트워크 시스템에서의 미들웨어에서의 각종 응용 분야를 실현하기 위한 인터페이스를 UPnP 프로토콜을 소프트웨어적으로 구현하고, 암호 알고리즘을 펌웨어로 구현함을 목표로 하고 있다. 정보가전이나, 무선기기, PC 등 모든 종류의 기기들을 연결하는 네트워크 구조로 구성되어 있다. 이것은 가정이나 작은 사무실과 같이 관리자가 없는 네트워크에서 사용자의 작업없이 쉽게 표준화된 방법으로 기기간의 연결이나 인터넷으로의 연결을 제공한다. 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. 또 네트워크에서 빠져나올 때도 다른 기기에 영향을 주지 않고 연결을 해지할 수 있다. 기존 연구의 주된 방향의 주요 목표는 단말기 들을 하나의 표준화된 프로토콜을 사용함으로써 다수의 단말기들을 집중화시켜서 사용할 수 있는 미들웨어 상에서의 부가적인 보안 메카니즘의 개발 정도로 여겨지고 있다. 본 연구에서는 이러한 보안 게이트웨이와 각각의 단말사이의 정보를 위해 Security class와 Computational overhead, Network dependency를 고려한 설계를 하는 데 그 원천적인 기술을 개발함에 목표를 두고 있다.

표1. 홈네트워크 시스템 구성을 위한 원천기술

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

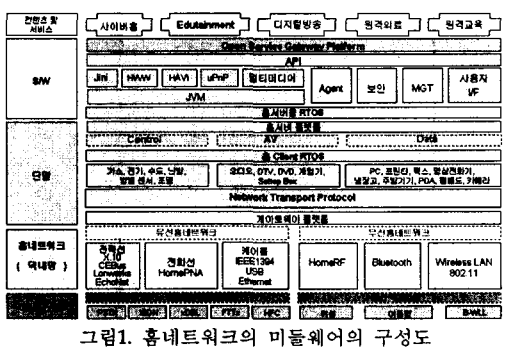

그림1. 홈네트워크의 미들웨어의 구성도

V. 보안 기술의 요소기술

일반적으로 보안이라는 개념이 암호화의 개념과 비슷하게 사용되는 데 이것은 잘못된 것이다. 일반적으로 암호화를 통한 기밀성의 문제는 적어도 보안의 해결 방법의 하나이다. 일반적으로 네트워크 보안에서는 다음과 같은 여러 요소들을 고려하여야 하며, 특히 다음과 같은 요소 기술들을 포함하여야 한다.

1. Data origin authentication
2. Command authorization
3. Message integrity protection
4. Message replay prevention
5. Data confidentiality
6. Key distribution
7. Trust versus trustworthiness

VI. 이종 시스템 간에서의 보안 문제

본 논문에서는 네트워크상의 자원과 다양한 시스템의 자원에 대한 이종단 간의 홈네트워크 의 보안 프레임을 설계하여 종단에서의 이종간의 시스템에 대한 보안 레벨에서 통신할 수 있는 방법의 실현 시 고려해야 하는 요소 기술에 대해서 기술하였다. 다음은 그 주요 목표이다.

- 홈네트워크 상에의 보안 대책 요소
- 보안성을 위한 요소 기술의 정립
  (Data origin authentication, message integrity protection, message replay prevention, data confidentiality, key distribution, trust versus trustworthiness)
- 이종간의 홈네트워크 보안을 위한 요소 기술
  (Authentication, Confidentiality 등)
- 이종간의 네트워크 연결을 위한 security level의 구성 요소 해석
- Cryptographic technique의 security level에 따른 security class의 분석

VII. 이종시스템간의 네트워크보안 요구사항

다음의 그림3은 본 논문에서 추후 연구하려고 하는 End-to-end Network Security Framework 이며 그림4는 Adative End-to-End Home Network Scurity Famework에서의 Scurity Mdel을 보여 주고 있으며 Scure Cass를 위한 요구조건은 다음과 같으며 이러한 파라메터를 이용하여 시스템의 성능 평가를 유추한다.

(1) System dependancy
  - Computational overheads
  - Message/Key size

(2) Network dependency
  - Network congestion
  - Message size
  - Network type

(3) Domain dependency
  - Message size
  - Message sensitivity
  - Participants

(4) User dependency
  - Time, cost, computing power

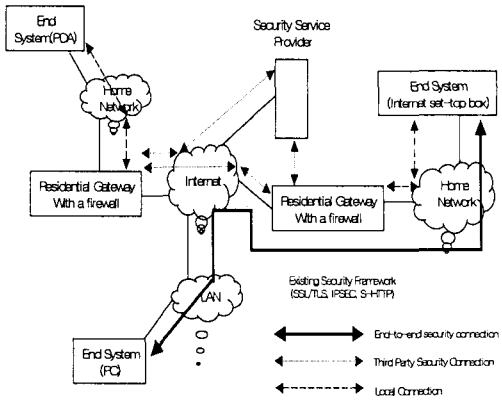

그림2. 홈네트워크 보안기술 구성도

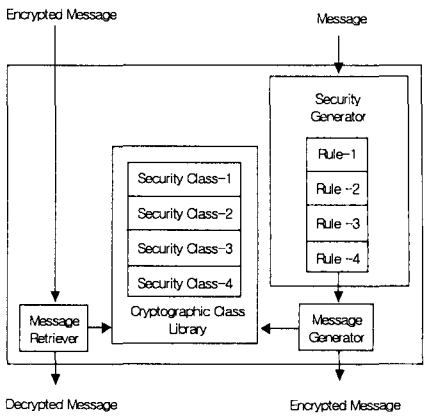

그림3. Adaptive End-toEnd Home Network Security Framework

- 홈네트워크 상에의 보안 대책 요소
- 보안성을 위한 요소 기술의 정립
  (Data origin authentication, message integrity protection, message replay prevention,

data confidentiality, key distribution, trust versus trustworthiness)
- 이종간의 홈네트워크 보안을 위한 요소 기술 (Authetication, Confidentiality 등)
- 이종간의 네트워크 연결을 위한 security level의 구성 요소 해석
- Cryptographic technique의 security level에 따른 Security class의 분석

VIII. 결 론

본 논문에서는 향후 유비쿼터스 환경하에서의 이종간 시스템간에서의 정보보호에 대한 대책으로 요소 기술에 대해서 살펴보았다. 기존에 표준안으로 사용되고 있는 블록 암호시스템과 공개키 암호시스템 간의 상호간의 연동성에 의한 문제가 발생하게 된다. 특히 이종간 시스템 간에서는 상호 시스템에서의 성능에 따른 암호화의 속도 문제와 키 관리, 분배 등에 대한 문제점을 기존의 방법으로는 해결 하기에 많은 문제점을 가지고 있다. 따라서, 본 논문에서는 특히 홈네트워크 시스템의 보안을 위한 이종간의 시스템에서 고려해야할 사항을 검토하여, 추후에 구현되는 시스템에서 이에 대한 보안대책 및 보안 알고리즘의 선정, 특히 키 분배 및 관리 시스템에 등에 대한 기초 자료가 되며 이에 대한 연구가 추후에 반드시 필요하리라 생각된다.

참고문헌

[1] Cheng-Fa, etc, "A Multi-agent architecture for intelligent home network service", IEEE Trans. on Consumer Electronics, V.48, N.3, August 2002, pp.505-514
[2] Sungwoo Tak, etc, "An end-to-end home network security framework", Elsevier, pp.412-422
[3] http://ccmc.knu.ac.kr/files/research/home.html
[4] 임승옥 외2, "유비쿼터스 통신 실현을 위한 홈 네트워크 프로토콜 구조", 정보처리학회지 제10권 제4호, 2003,7, pp,58-65
[5] 박준호 외3인, "유비쿼터스 서비스를 위한 룸 기반 홈 네트워크 관리 미들웨어" 정보처리학회지, 제10권, 제4호, 2003.7, pp.122-131
[6] B. Rose, "Home networks: a standard perspective, IEEE Communication Magizine 39, 2001., pp.75-85
[7] Jini Overview, http://www.sun.com /jini/faqs/index.html
[8] S. Teger, etc, "End-user perspectives on home networking, IEEE Communication Magazine 40, 2002, pp.114-119
[9] Prashant K., etc, "Security in Wireless Residential Networks", IEEE Trans. on Consumer Electronics, V.48, N1, February 2002, pp.157-166
[10] Peter B, etc. "Making Home Automation Communications Secure", IEE Magazine, 2001, pp.50-55