Zigbee 기반의 홈네트워크 기기 보안을 위한 플랫폼 개발

고형준*, 박채민**, 류대현*, 이상진***

*한세대학교 IT학부

**(주)바른기술

***고려대학교 정보보호대학원

Platform Development for Home Network Device Security based on Zigbee

Hyungjun Ko*, Chaemin Park**, Daehyun Ryu*, Sangjin Lee***

*Division of IT, Hansei Uni.

**Baruntech, Inc.

***CIST, Korea Uni.

요 약

본 논문에서는 댁내망에서 무선 홈네트워크 기기 제어에 있어서의 트래픽 암호화 및 기기인증 등의 보안 문제 연구를 위한 플랫폼을 개발하였다. 우선 근거리 무선 통신 표준으로 자리잡고 있는 Zigbee를 적용한 도어락과 저가의 홈게이트웨이를 개발하고 다양한 암호 알고리즘을 탑재할 수 있도록 하였다. 또한 AES와 HIGHT를 탑재하여 기기인증과 트래픽에 대한 암호화가 가능하도록 하였다.

I. 서론

홈 네트워크 시스템의 핵심은 네트워크 망을 가정 내 각종 기기까지 연결시켜 원격지에서도 가정 내의 각종 기기를 제어 및 모니터링을 할 수 있도록 하여 생활의 편리를 도모하도록 하는 것이다. 그러므로 기존 네트워크 환경에서 항상 문제가 되고 있는 해킹, 바이러스, 개인정보 침해, 불건전 정보 등의 보안 문제에 홈 네트워크 시스템도 노출되게 된다. 특히, 홈 네트워크 시스템은 네트워크 망을 통해 가정 내의 정보가전을 제어가능하기 때문에 보안에 더욱 유의해야 한다.

특히 유비쿼터스 홈네트워크 환경에서는 다양한 홈기기들을 통해서 정보의 유출이 가능하며, 개인 프라이버시 문제가 발생하게 된다. 이러한 정보유출 및 개인 프라이버시 이슈를 해결하기 위해서는 보안기술이 필수적이나, 유비쿼터스 환경에서는 다양한 통신 방식이 적용되므로 유선 통신 위주의 기존의 보안기술을 그대로 적용하기 어렵다.

유비쿼터스 환경에서 홈 네트워크는 단계적으로 유·무선 통신망, 방송망, 인터넷망과 최종적으로 USN(Ubiquitous Sensor Network)이 All-IP 망으로 통합되는 형태로 구축될 것이다(그림 1). 이러한 환경에서는 개인의 사적인 정보들과 공적인 정보들이 혼재되어 광대역 네트워크에 존재하게 될 것이며, 이러한 정보들을 이용한 역기능 또한 매우 위험한 수준이 될 것이다. 이처럼 유비쿼터스 홈 네트워크에서 부각되고 있는 위협요소들을 살펴보면 다음과 같다.

o 홈네트워크는 인터넷에서 발생되고 있는 다양한 사이버공격에 그대로 노출되어 있다. 따라서 해킹, 악성코드, 웜 및 바이러스, DoS 공격, 도·감청 등에 취약하다.

o 유비쿼터스 홈네트워크 환경에서는 기존의 개별 통신망들이 상호 통합되고 융합되므로 개별망의 피해 및 기기 결함이 연결된 모든 네트워크로 확산될 소지가 매우 높다.

o 기존의 발생 위협과는 전혀 다른 새로운 취약점이 발생될 수 있으며, 망 혼재에 따른 취약점이 증가하게 될 가능성이 높다.

o 초경량, 저전력의 RFID/USN 자체의 특성에 따른 공격과 프라이버시 침해가 확대될 가능성이 매우 높다.

o 홈네트워크에는 Ethernet, HomePNA, PLC,

IEEE 801.x, Blutooth, Zigbee, UWB(Ultra Wide Band) 등의 다양한 유무선 네트워킹 기술이 적용된다. 그러나 매체 특성에 따른 보안취약성을 해결할 수 있는 대응기술을 갖고 있지 못한 실정이다. 특히, 무선구간의 경우 구성요소 및 데이터 보호 등에 취약성을 갖고있어 구성요소간 인증기능과 데이터의 암호화 기능이 필요하다.

o 댁내망에서 정보가전기기와의 연동을 통한 제어 시 불법적인 디바이스 접속을 통해 주요자원에 대한 공격이나 주요 데이터의 유출 가능성이 존재한다.

o 미들웨어의 경우에도, 각 미들웨어들이 요구하는 보안요구조건을 모두 만족시키지 못하고 있다. 또한 통합 미들웨어 환경에서도 유연하게 보안기능을 제공할 수 있는 보안인프라도 개발될 필요가 있다.

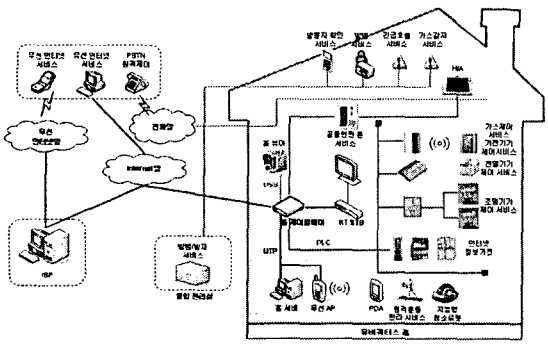

그림 1. 홈 네트워크 구성도

본 논문에서는 댁내망에서 무선 홈네트워크 기기 제어에 있어서의 트래픽 암호화 및 기기인증 등의 보안 문제 연구를 위한 플랫폼을 개발하였다. 우선 근거리 무선 통신 표준으로 자리잡고 있는 Zigbee를 적용한 도어락과 저가의 홈게이트웨이를 개발하고 다양한 암호 알고리즘을 탑재할 수 있도록 하였다. 또한 AES와 유비쿼터스 컴퓨팅 환경에서 암호 서비스를 적용할 수 있도록 초고속, 초경량으로 개발된 블록 암호 알고리즘인 HIGHT를 탑재하여 기기인증과 트래픽에 대한 암호화가 가능하도록 하였다.

II. 홈네트워크 보안 기술동향

현재까지 홈네트워크 구성요소 중 가장 많은 연구가 진행된 것은 홈게이트웨이 부분으로, 다양한 상용제품이 개발되어 시판되고 있다. 홈게이트웨이는 댁외의 공중망과 댁내의 홈네트워크를 연결하는 입구로서 외부의 불법 침입에 대해 일차적인 대응 방안을 제공 한다는 개념에서 최우선적으로 보안기능이 탑재되고 있다. 홈 게이트웨이 플랫폼에 VPN(Virtual Private Network), Firewall 기술을 적용하여 외부망과 홈 게이트웨이 사이의 정보보호에 대한 연구가 진행 중이다.

안전한 홈서비스 제공을 위해서 사용자 인증, 정보가전기기 인증, 접근권한 제어, 정보의 무결성과 기밀성을 지원하는 HAvi, UPnP, Jini, OSGi 미들웨어 정보보호 기술이 연구되고 있다.<표 1>

홈게이트웨이와 정보가전기기간의 제어를 위해 필요한 미들웨어들에서도 기본적인 보안기능이 제공되고 있으며, 관련 보안기능에 대한 표준화도 이루어지고 있다.

<표 1> 미들웨어 정보보호

구 분	기술 현황
미들웨어	서비스 전달, 보안기능, 멀티미디어 서비스 기능 등 사용자의 엔터테인먼트 서비스 및 편의성 향상에 대한 요구사항을 만족시키기 위한 연구가 진행 중
UPnP	Device Security Service, Security Console을 통하여 인증 및 접근 제어 기능을 제공
OSGi	사용자가 제시한 인증정보를 바탕으로 인증서버를 통하여 사용자 인증을 제공하고 Role Repository를 통하여 접근 권한에 대한 제어 기능을 지원

III. 홈네트워크 보안 요구사항

홈네트워크에서는 이종의 유무선 네트워크와 다양한 프로토콜 등이 혼재하고 있다. 따라서 기존의 보안취약성 이외에 추가적으로 고려해야할 보안취약성이 존재한다. 홈네트워크의 다양한 정보가전기기들은 인터넷과의 연결로 사이버공격의 대상이 될 수 있다. 뿐 만아니라. 네트워크 내의 정보기기의 다양성과 기기간 자원의 공유 등으 로인해 보안요구사항은 더욱 복잡해지고 다양하다.

또한, Ethernet, HomePNA, IEEE1394, PLC, IEEE 802.1x, Blutooth, Zigbee, UWB 등 다양한 홈네트워킹 기술이 활용될 것으로 예상되고 있으나 대부분은 보안취약성에 대한 대응기술이 아직 개발되지 못하고 있다. 따라서 홈네트워크를 구성하는 다양한 통신매체나 프로토콜 등과 관계없이 요구되는 보안기능을 만족할 수 있는 보안프레임워크가 정립될 필요가 있다.

홈네트워크 보안 요구사항 중 디바이스 인증, 사용자 인증, 홈 기기간 인증, 접근제어에 대해 간단히 살펴보았다.

o 디바이스 인증 : 불법 디바이스의 사용을 방지하기 위해서는 홈 네트워크의 구성요소인 디바이스 자체에 대한 인증과정이 필요하다. 현재까지 디바이스 인증은 미들웨어 레벨에서 제공되고 있다.

o 사용자 인증 : 홈네트워크에서는 디바이스 인증 외에 디바이스를 사용하는 사람의 신원확인을 위한 사용자 인증 기능도 반드시 필요하다. 홈네트워크에는 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 사용자 인증기술의 활용이 가능하겠지만, 유비쿼터스 컴퓨팅 환경으로의 진화를 고려할 때 정보단말

기기의 낮은 성능을 고려한 사용자 인증기술의 활용 및 적용성이 검토되어야 한다.

o 홈 기기간 인증 : 원활한 홈서비스 제공을 위해서는 기본적으로 홈네트워크 구성요소 간의 자원 공유를 위한 신뢰가 확보되어야 한다. 이를 위해서는 구성요소 간의 기기간 상호인증이 필요하다. 현재 기기 간의 인증기능은 어느 정도 미들웨어 레벨에서 제공하는 보안기능에 의존할 수 있다. 하지만, 모든 미들웨어가 보안기능을 제공하고 있지 않으므로 이에 대한 해결방안이 수립되어야 하며, 기기 간 인증 기능은 다양한 홈서비스를 위한 기본적인 보안기능이라고 할 수 있으므로 홈서비스 제공을 위해서는 다른 보안기능과의 원활한 연동성이 확보되어야 한다. 즉, 사용자 인증 기능, 접근제어 기능 등을 위해서는 기본적으로 기기 간 인증기능이 우선되어야 하므로 다른 보안기능과의 연동성이 고려되어야 한다.

o 접근제어 : 홈서비스에 따라 홈네트워크 자원에 대한 접근 권한 제어 기능이 요구된다. 홈 구성원별로 제공받을 수 있는 홈서비스의 종류가 다르고 홈네트워크 구성요소에 대한 제어 범위도 다르므로 이에 대한 접근 제어 기능이 필요하다.

IV. 시스템 구성

4.1 시스템 구성

본 논문에서는 홈 네트워크 기기 중 디지털 도어락 장치를 대상으로 홈게이트웨이와 디지털 도어락 간의 기기인증 및 트래픽 암호화를 구현하였다.

(그림 2)에 시스템의 전체 적인 구성도를 나타내었다. 외부망의 원격지 PC 는 홈 게이트웨이를 통하여 홈네트워크 기기를 제어한다. 이때 게이트웨이와 홈기기 간에는 Zigbee 를 이용하여 통신하도록 하였으며 이 구간의 기기인증 및 트래픽 암호화를 위하여 암호알고리즘인 AES와 HIGHT를 포팅하였다.

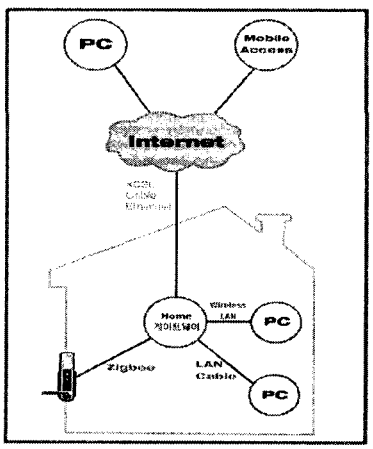

그림 2. 시스템 구성도

HIGHT는 스마트 카드, RFID 등과 같이 유비쿼터스 컴퓨팅 환경에서 암호 서비스를 적용할 수 있도록 정보통신 선도기반기술개발사업의 일환으로 초고속, 초경량으로 개발된 블록 암호 알고리즘이다. HIGHT 알고리즘은 하드웨어 구현시 3,823개의 게이트를 필요로 하며, 약 125 Mhz의 동작 주파수를 갖는다. 암호 및 동작에 필요한 클록의 수는 34 클록이며, 암호 및 복호 성능은 약 235 Mbps이다.

4.2 하드웨어 구성

하드웨어는 크게 Zigbee 모듈과 홈게이트웨이 두 개로 나누어 진다. (그림 3)은 Zigbee 모듈의 하드웨어 구성도이다. MCU는 Atmel의 132K 메모리와 512K 플래시 메모리를 내장한 ATmega128L을 사용하고, RF 칩은 Chipcon의 2.4GHz 주파수를 사용하는 CC2420을 사용하였다.

	Device Node	Mobile Node	Sink Node
MCU	ATmega 128L		
RF	CC2420 (2.4 GHz)		
Sensor		도어락 IF	
Software	TinyOS 1.1.14 Ver.		

그림 3. Zigbee 모듈 하드웨어 구성

(그림 4)는 홈 게이트웨이의 하드웨어 구성도이다. MCU인 ADM5120, 내부망을 구성하는 4개의 LAN 포트와 802.11g 무선랜카드, 외부망과 연결되는 WAN 포트, Zigbee 모듈과 연결되는 시리얼 포트로 구성된다.

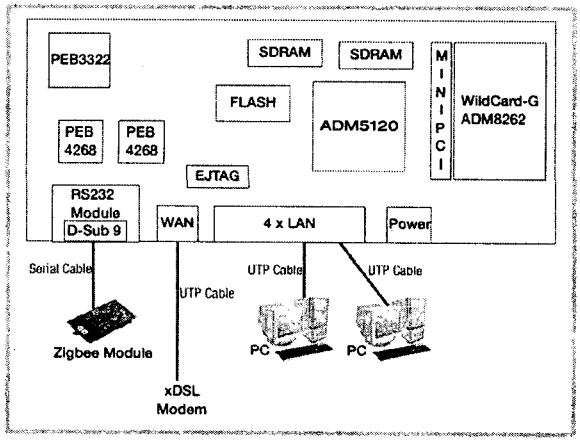

그림 4. 홈 게이트웨이 하드웨어 구성도

4.3 소프트웨어 구성

Zigbee 모듈은 UC Berkeley에서 개발한 TinyOS

에 AES 와 HIGHT 컴포넌트를 추가하여 구현하였다. (그림 4)는 TinyOS 의 컴포넌트 계층도 이다.

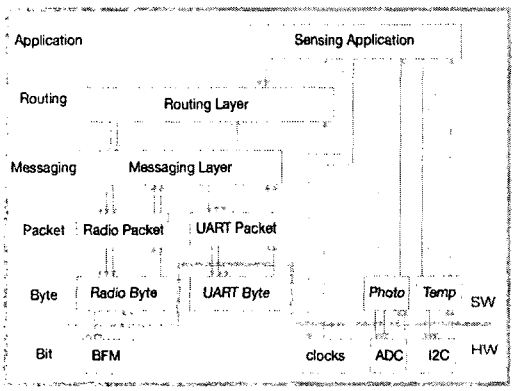

그림 4. TinyOS 의 컴포넌트 계층도

홈 게이트웨이는 리눅스 커널을 포팅하여 구현하였고, Zigbee 모듈과 통신하기 위한 응용프로그램을 추가하였다. (그림 5)는 홈게이트웨이의 소프트웨어 구성도 이다.

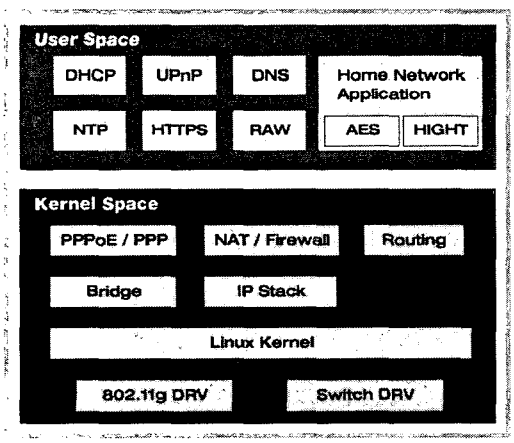

그림 5. 홈 게이트웨이 소프트웨어 구성도

4.4 데이터 포맷

(그림 6)은 홈 게이트웨이와 홈 기기 간의 Zigbee 무선 통신 데이터 포맷이다. TinyOS의 Active Message 포맷의 데이터 필드에 암호화 된 데이터와 암호 알고리즘에 사용되는 변수와 메시지 인증 코드를 포함한다. 복호화된 HIGHT_Data 구조체는 기기의 주소와 명령타입과 Data로 구성된다.

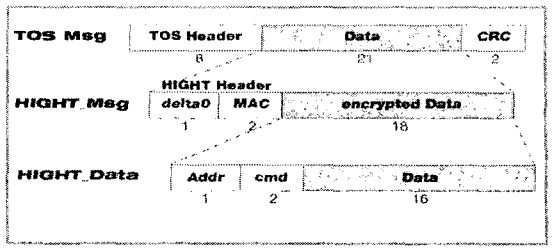

그림 6. 데이터 포맷

V. 결론

본 논문에서는 댁내망에서 무선 홈네트워크 기기 제어에 있어서의 트래픽 암호화 및 기기인증 등의 보안 문제 연구를 위한 플랫폼을 개발하였다. 우선 근거리 무선 통신 표준으로 자리잡고 있는 Zigbee를 적용한 도어락과 저가의 홈게이트웨이를 개발하고 다양한 암호 알고리즘을 탑재할 수 있도록 하였다. 또한 AES와 유비쿼터스 컴퓨팅 환경에서 암호 서비스를 적용할 수 있도록 초고속, 초경량으로 개발된 블록 암호 알고리즘인 HIGHT를 탑재하여 기기인증과 트래픽에 대한 암호화가 가능하도록 하였다.

홈네트워크에는 다양한 위협요소가 존재한다. 이와 같은 위협요소와 유비쿼터스 홈 네트워크에 대한 불법적인 공격 또는 홈네트워크 기기의 결함은 개인의 프라이버시 침해뿐 아니라 생명 및 재산에 직접적인 피해를 줄 수 있다. 따라서 홈 네트워크에 대한 침입 및 결함 취약성에 대한 대응책 마련이 매우 시급하다.

뿐만 아니라 홈 네트워크의 고가용성을 확보하기 위하여 홈 기기의 방어기능 및 안정성 확보를 위한 기술개발도 필수 불가결하다. 또한 홈 네트워크 보안 및 재해 복구를 위하여 피해 복구 시스템 및 각종 진단 및 모니터링을 위한 기술들도 개발할 필요가 있다.

[참고문헌]

[1] 나기준, 채기준, 정교일, 센서 네트워크 보안 연구 동향, 정보통신동향분석, 제 20권 제 1호, 2005년 2월

[2] 한종욱, 김도우, 주홍일, 이윤경, 남택용, 장종수, 안전한 홈 네트워크 구축을 위한 보안 요구사항, 정보처리학회지, 제11권 제3호, 2004년 5월

[3] 김옥경, 홈 네트워크 환경에서 안전한 정보 전송을 위한 홈 게이트웨이 보안 구조 설계 및 구현, 이화여자대학교 과학기술대학원, 2003

[4] 임진우, 이옥연, Home Network 환경에서의 보안 기술, 한국멀티미디어학회 춘계학술발표대회논문집, 2004

[5] 신순자, 서운석, 이용진, 김유정, 신상철, 유비쿼터스 환경의 홈 네트워크 보안 및 인증서비스 모델,