트랜시버용 결함방지 알고리즘을 이용한 홈네트워크 시스템 제어

안동헌, 양훈기
광운대학교 전파공학과

Home Network System control using defect avoidance transceiver algorithm

Dong-hun An, hoon-gee Yang
Department of Wireless Communications Engineering, Kwangwoon Univ.

Abstract - 본 논문은 결함방지 알고리즘이 적용된 트랜시버 모듈을 사용해서 홈네트워크 내에서 발생한 결함, 침입 등에 대응 할 수 있는 방법을 설명한다. 시스템 구성도와 결함방지 알고리즘에 대해서 설명하고 알고리즘을 수행하는데 있어서 필요한 데이터베이스의 구조와 역할을 제시하였다. 마지막으로 알고리즘을 적용한 테스트용 홈기기가 올바르게 동작하는 것으로 시스템 제어 결과를 확인 하였다.

1. 서 론

홈네트워크 시스템은 PC와 인터넷의 발달과 통신기술 및 지능형 설비의 고속발전에 따라서 등장하였고, 가정의 가전제품을 유선 혹은 무선 네트워크의 통신 프로토콜을 이용해서 유기적으로 연결하고 게이트웨이를 통해서 외부 통신망으로 원격제어를 지원하는 시스템이다.[1] 시스템은 하드웨어와 통신 프로토콜, 네트워크 접속방식, 콘텐츠 서비스 제공, 네트워크 운영 등으로 구성되고 가정안의 모든 가전기기들은 내부 네트워크로 연결되어서 셋톱박스와 홈게이트웨이를 통해 외부 네트워크로 연결되어 있다.

가정에서 구성된 네트워크가 인터넷과 연결됨으로써 시스템의 접속과 제어가 가정에서 뿐만 아니라 가정밖에 어디서나 가능하게 되었다. 그러나 외부와 연결됨으로써 외부 네트워크에서 발생되는 보안의 문제가 홈네트워크 시스템에서도 발생될 수가 있다. 외부 네트워크 시스템에서 제공하는 기능 중에서 보안이나 시스템 안정화 기능등이 홈네트워크에도 적용 되어야 하고 시스템 특성에 맞게 연구되어야 할 필요성이 있다. [2]

본 논문에서는 홈네트워크 시스템에서 사용되어지는 보안기술에 대해서 설명하고 트랜시버를 이용해서 홈서버에 연결되는 홈기기의 동작의 보안을 유지하는 방법과 알고리즘에 대해서 설명한 다음에 테스트보드로 알고리즘을 검증하고 결론을 맺고자 한다.

2. 본 론

2.1홈네트워크 보안 기술

대부분의 홈네트워크 시스템에서의 보안은 PC용 보안 알고리즘을 간략화 시켜서 홈서버에서 사용하고 시스템 결함이나 외부침입탐지에 대한 대응 방법등이나 내부에 발생하는 문제들은 보안의 우선순위에서 밀려 있다.

홈네트워크 시스템은 크게 접근망과 댁내망으로 나누어지는데 홈서버를 기준으로 구분한다. 시스템에서 입출력되는 모든 데이터는 접근망에서 노출된다. 그리고 보안이나 침입탐지 및 오류 데이터 수정에 대한 대응 방법은 외부 네트워크에서 제공되는 방법을 사용한다. 댁내망은 외부 네트워크에서의 데이터가 홈서버를 통과하면서 부터이고 가정에서 내부 네트워크이다. 내부에서 발생되는 데이터의 오류나 무선통신 방법에 의한 데이터 왜곡, 외부에서 침입에 대한 대응방법을 댁내망에서 처리하여야한다.[3]

외부에서 침입 가능한 공격은 해킹, 악성코드, 웜 및 바이러스, DoS(Denial of Service)공격, 통신망 도·감청 등이 있고 현실적으로 맞지 않는 왜곡된 데이터등이 있다.[4] 침입에 대한 대응방법은 홈서버에서 기존 보안 알고리즘을 간략화해서 소프트웨어적으로 구현한다. 침입에 대한 대표적인 유형은 <표 1>과 같다.

<표 1> 홈네트워크 침입 유형[5]

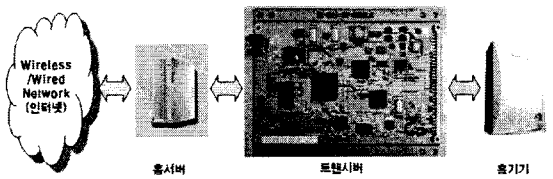
공격 유형	공격 내용	대상
도청	패스워드, 중요데이타, 특정 서비스의 기능등에 대한 정보 수집	접근망 패킷 댁내망 패킷
데이타 변형	홈네트워크 프로토콜의 취약점을 이용하여 정당한 사용자나 시스템으로 위장	홈게이트웨이 댁내망
서비스거부공격	네트워크 사용량 초과, 메일 폭탄	홈게이트웨이 무선AP
개인정보	특성 서비스의 사용량 수집	사용시간

홈서버에서 보안에 대응하기 위한 방법은 기기를 사용할 때 마다 인증을 통하는 방법이 가장 기본적으로 사용되어진다. 인증 방법은 디바이스 인증, 사용자 인증, 접근권한 제어기능, 미들웨어 보안기능등이 있다.[4] 디바이스 인증은 디바이스 자체에 고유한 인증서를 부여하여 사용할 때 마다 인증절차를 통해서 인증된 디바이스만을 사용하도록 한다. 사용자인증은 디바이스 사용자의 신원확인 작업을 하는 방법으로 일반적으로 패스워드, 공인(사설) 인증서, 생체인식(지문, 홍채등), RFID 태그기반 기술등의 다양한 사용자 인증 방법을 사용한다. 접근권한 제어기능은 홈네트워크에서 디바이스에 대한 사용자 접근제어를 사용자 마다 다르게 설정하는 방법으로 디바이스 마다 보안 등급을 다르게 해서 사용하는 방법이다. 미들웨어 보안 기능은 홈네트워크에서 사용되는 미들웨어에 대해서 다른 디바이스와는 별도로 보안이나 제어가 필요하기 때문에 미들웨어 차원에서 침입 대응 방법이나 보안 기능 고려하는 방법이다. 미들웨어 보안 기술에서 대표적으로 사용하는 방법이 UPnP(Universal Plag and Play) 보안기술이다. UPnP은 마이크로소프트가 제안하였으며 매체와는 상관없이 IP, TCP, UDP, HTTP, XML과 같은 프로토콜을 사용해서 홈네트워크 기기 간에 제어와 명령을 가능하게 P2P(peer to peer)방식으로 연결시켜 주는 구조이고 장치보안(device security), 보안 콘솔 (security console), 신뢰 장치(secure device)를 중요한 3요소로 고려한다. [6,7]

홈네트워크 침입 탐지와 보안에 대응하는 방법에는 외부 네트워크에서 사용하는 소프트웨어적인 요소가 기반기술로 되어 있지만 댁내망에서는 보안에 대처하기는 데에는 한계가 존재해서 트랜시버를 사용해 보안에서 미비한 부분을 보충한다.

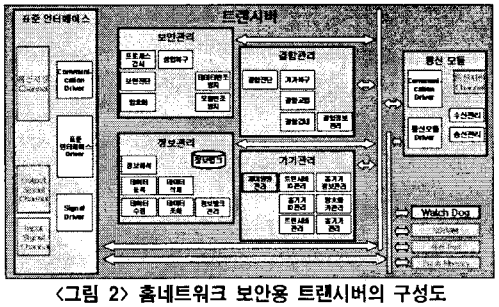
2.2 홈네트워크 시스템 구성도

홈네트워크 시스템은 크게 홈게이트웨이가 내장된 홈서버를 중심으로 가전기기들이 연결되는 형태로 구성되어 있다. 여기서 트랜시버는 홈네트워크의 보안과 네이트워크 시스템의 안정성을 유지하는 역할로서 홈서버를 보조하는 매개체로 연결되어 진다. 홈네트워크는 외부망인 유선 인터넷망이나 무선망인 핸드폰망으로 연결되어 질 수 있다. 그리고 외부망에 홈서버가 연결되고 홈서버에 홈기기가 연결되고 트랜시버는 홈서버와 홈기기 중간에 연결된다. <그림 1>은 홈네트워크에서 홈서버, 트랜시버, 홈기기가 연결되는 홈네트워크 시스템 구성도이다.



<그림 1> 홈네트워크 시스템 구성도

트랜시버는 홈네트워크에서의 보안과 홈네트워크 시스템의 안정성을 유지하는 역할을 목적으로 사용되어진다. 경우에 따라서 트랜시버는 보안과 시스템 안정성 외에 홈기기를 사용하기에는 홈네트워크 구성이 어려운 환경에서 홈게이트웨이를 대처 할 수도 있다. 트랜시버는 적응형 침입탐지 알고리즘과 기기의 안정성을 보호하는 기능 등이 구현되어지고 트랜시버의 FPGA Chip에는 적응형 침입탐지 시스템의 알고리즘과 홈네트워크에서 데이터의 오류와 감시를 위해서 통신모듈과 표준 인터페이스로 구성되어 진다. 트랜시버는 알고리즘은 데이터를 유지 관리하기 위해서 데이터베이스를 사용한다. <그림 2>는 홈네트워크 보안용 트랜시버의 구성도이다.



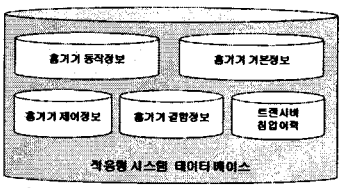
<그림 2> 홈네트워크 보안용 트랜시버의 구성도

"본 연구결과물은「2005 산업자원부 성장동력산업」의「유비쿼터스 홈 네트워크 범용 침입대응 시스템 개발사업」의 지원으로 수행 되었음"

2.3 적응형 데이터베이스와 결함 방지 알고리즘

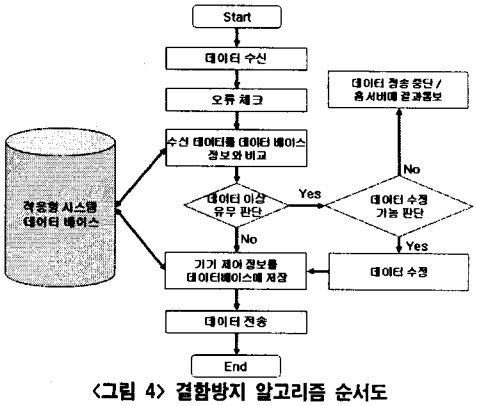
홈네트워크용 트랜스버의 주된 기능은 홈서버에서 홈기기로 향하는 데이터의 결함이나 비정상적인 데이터를 관리하는 기능이다. 홈서버에서 홈기기로 전달되거나 홈기기에서 홈서버로 전달되는 데이터는 트랜시버에 저장되어 있는 데이터와 비교하는 과정을 거치면서 비정상적인 데이터가 발생되면 차단하거나 데이터 수정이 가능하면 수정하는 과정을 거치게 된다. 정상적인 데이터는 트랜시버의 정보뱅크와 데이터를 비교 후에 전송하게 된다. 트랜시버용 결함 방지 알고리즘은 트랜시버를 통해서 지나가는 데이터를 정보뱅크에 저장된 데이터와 비교하는 역할을 수행하게 되고 데이터의 비교는 정보뱅크 안에 존재하는 적응형 시스템 데이터베이스에 저장된 정보와 비교를 한다.

적응형 시스템 데이터베이스에는 홈기기 동작정보 데이터베이스, 홈기기 제어정보 데이터베이스, 홈기기 결함정보 데이터베이스, 트랜시버 침입이력 데이터베이스, 홈기기 기본정보 데이터베이스 등으로 구성되어 진다. 홈기기 동작정보 데이터베이스는 홈기기의 기능에 대한 동작 정보 데이터가 저장되고 기기를 동작하기 위한 명령어나 홈기기가 동작한 후에 홈서버로 전달하는 데이터 정보의 유형이 저장된다. 정상적인 상황에서 홈기기가 생성하는 데이터의 정보를 가지고 있다. 홈기기 제어정보 데이터베이스는 홈서버가 홈기기를 언제 제어 했는지에 대한 이력정보를 저장하는 데이터로 구성한다. 제어정보는 홈기기의 사용 빈도나 사용패턴을 분석할 때 사용되어지고 이 기능은 트랜시버의 성능에 따라서 시스템이 사용자에 적응하는 시스템으로 사용할 때 참고 정보로 사용한다. 홈기기 결함정보 데이터베이스는 트랜시버를 통과하는 명령어가 현재 상황에 맞지 않는 오류명령어, 명령어에 상관없는 기기 자체결함, 명령어는 맞지만 알고리즘에서 발생되는 결함에 대한 이력정보등이 저장된다. 결함정보 데이터베이스에 저장된 정보는 홈기기, 홈서버, 트랜시버에서 발생한 에러나 기능 장애등을 수정할 때 사용되어지고 빈도수가 높은 결함 정보는 시스템 구조를 수정하는데 사용한다. 트랜시버 침입이력 데이터베이스는 외부에서 트랜시버를 통과하는 데이터가 홈서버나 홈기기의 오작동이나 부하를 목적으로 하는 데이터나 날씨, 시간, 계절에 맞지 않는 데이터 사용자가 실행할 수 없는 데이터에 대한 정보가 저장된다. 홈기기 정보 데이터베이스는 트랜시버에 연결되어 있는 홈기기의 제작년도 , 일련번호, 모델번호, 제작사, 기기의 사양 등을 저장한다. 기기정보 데이터베이스는 홈기기 동작 정보 데이터베이스를 구성할 때나 입력할 때 동시에 입력하고 두 개의 데이터베이스는 연결된다. <그림 3>은 적응형 데이터베이스의 구조도이다.



<그림 3> 적응형시스템 데이터베이스 구조도

결함 방지 알고리즘은 트랜시버로 들어오고 나가는 데이터를 적응형 시스템 데이터베이스와 비교해서 홈네트워크의 불안정한 요소를 제거하고 관리하는 역할을 한다. 알고리즘은 데이터가 홈기기나 홈서버에서 트랜시버로 들어오면 데이터의 검증 과정이 끝날 때 까지 일정시간 동안에 버퍼에 저장해 놓는다. 저장된 데이터는 홈기기 동작정보 데이터베이스에 저장된 동작정보에 맞는지 비교를 하고 데이터에 이상이 없으면 홈기기나 홈서버 쪽으로 데이터를 내보낸다. 검증 과정에서 데이터에 이상이 발생하면 동작정보 데이터베이스와 데이터와 데이터의 이상 정도를 판별해서 알고리즘 자체적으로 수정가능하면 수정한 후에 데이터를 내보내고 수정 가능한 범위가 아닐 경우에 홈기기 결함정보 데이터베이스와 비교를 해서 기존에 빈번하게 발생된 데이터이면 결함정보 데이터베이스와 홈기기 동작정보 데이터베이스를 바탕으로 데이터의 수정작업을 수행한다. 데이터의 수정 작업이 실패하면 데이터의 결함이나 침입으로 판단하고 데이터의 형태에 따라서 결함정보 데이터베이스나 트랜시버 침입이력 데이터베이스에 저장한다.

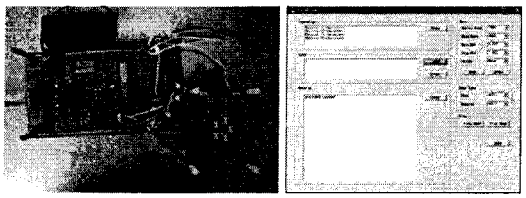


<그림 4> 결함방지 알고리즘 순서도

트랜시버를 통해서 홈기기를 제어하거나 홈기기에서 발생되는 데이터는 홈기기 제어정보 데이터베이스 해당되는 이력을 기록한다. 결함방지 알고리즘은 트랜시버로 수신되는 데이터의 검증이 끝났으면 버퍼를 비우고 다음 데이터를 수신하고 위해서 초기화 상태로 돌아간다. 결함 방지 알고리즘은 발생되는 데이터의 저장을 위해서 데이터베이스를 사용하기 때문에 시스템 업그레이드를 통해서 홈서버나 홈기기와 무관하게 독립적으로 홈네트워크에서 동작하는 홈기기에 대해서 사용자 특성에 맞는 적응형 시스템으로 구성 할 수가 있다. <그림 4>는 결함 방지 알고리즘이 동작 순서도 이다.

2.4 결함방지 알고리를 이용한 홈기기 제어 테스트

결함방지 알고리즘이 적용된 트랜시버를 홈기기에 연결하기 위해서는 기본적으로 홈기기가 전자적으로 동작을 하여야 한다. 따라서 홈기기를 트랜시버에 연결하기 전에 전자적인 홈기기의 테스트 보드가 필요로 하게 되고 가정에서 필수적으로 사용되는 방안의 전등을 테스트 기기로 정하였다. 전등을 구성하는 구성요품 중에 스위치 부분만이 실제로 트랜시버와 연결되기 때문에 스위치 부분만을 테스트 보드로 옮겨서 제작하고 형광등 부분은 하이퍼플렉스 LED로 대처 하여서 테스트 보드를 구성하였다. <그림 5>는 테스트 보드와 결함방지 알고리즘을 포함한 제어용 PC 프로그램 이다.



<그림 5> 홈기기제어 테스트용 프로그램과 실험용 보드

전등을 제작하기 위해서 테스트 보드를 스위치 부분과 전구 구분으로 나누어 제작하였고 결함방지 알고리즘은 트랜시버에 적용하기 전에 PC상에서 제이용 프로그램과 같이 구성하였다. 테스트에서 사용된 시스템에서는 PC상에 홈서버와 트랜시버의 기능을 같이 있다고 가정하고 테스트를 진행하였다. 테스트보드의 동작은 프로그램과 보드 둘 다에서 별도로 동작이 가능하고 서로 연동되어서도 동작되었고 결함방지 알고리즘은 결함이 발생 될 때 동작 데이터가 발생하여도 테스트 보드의 동작이 안 되게 실행되었다. 실행 결과는 별도의 데이터베이스에 저장된다.

3. 결 론

홈네트워크 시스템은 디지털 컨버전스를 추구하면서 현재 가장 발전하는 분야 중에 하나이고, 홈네트워크의 제어를 외부에서 가능하게 되면서부터 외부에서의 침입이나 내부 보안 문제가 대두가 되고 대응 방안이 필요로 하게 되었다. 대부분의 홈네트워크 시스템에서는 보안 문제를 단순히 홈서버에서 간략 화된 시스템으로 적용시켜 왔으나 홈기기나 홈네트워크에서 발생되는 보안의 문제점을 대응하지 못하는 단점이 있고, 결함방지 알고리즘을 적용한 트랜시버를 이용하면 단점을 보완할 수가 있다.

트랜시버는 홈서버와 홈기기 사이에서 동작하고 홈네트워크에서 발생되는 데이터를 항상 데이터를 분석해서 불필요한 명령어나 오류데이터를 검출하고 수정하는 작업을 수행해서 홈기기의 동작의 안정성을 확보한다. 따라서 홈네트워크 시스템의 불안정한 요소를 제거하고 홈기기를 안전하게 동작 시킬 수 있게 된다. 또한 홈기기 사용 이력 관리를 이용해서 사용자에 맞는 적응형 시스템으로 변경할 수 있는 기본정보를 축적 할 수 있다. 알고리즘의 테스트를 위해서 전등을 구현한 테스트 보드를 사용해서 홈기기의 안정성을 확인하였다.

앞으로 트랜시버에 알고리즘을 적용해서 원활한 동작 테스트가 필요하고 다른 트랜시버와 호환성 연구와 사용자에 맞는 적응형 시스템으로 변경하는 연구가 필요하다.

[참 고 문 헌]

[1] 한국전자통신연구원, "홈네티워크 기술 및 시장동향", 2005.4.

[2] 전용희, "홈네트워크 보안 관련 기술", 한국통신학회지 (정보통신) 제21권 3호, 2004. 3.

[3] 유동영, "홈네트워크 서비스에서 정보보호 필요성 및 고려사항", 한국통신학회지 (정보통신) 제22권 8호, 2005. 8.

[4] 한종욱, 이덕규, 정교일, "홈네트워크 보안기술 동향", 한국통신학회지 (정보통신) 제23권 제9호, 2006. 9.

[5] 유동영, 김영태, 노병규, "유비쿼터스 홈네트워크 환경에서의 침해 위협 및 대응 방안", 한국정보과학회 2004년도 가을 학술발표논문집 제31권 제2호(I), 2004. 10.

[6] 조충래, 박광로, "UPnP 기술 표준화 현황", 주간기술동향 통권 1075호, 2002. 12.

[7] UPnP Security Ceremonies Version 1.0, October, 2003, http://www.upnp.org