

홈 게이트웨이 기반 보안 시스템 개발

조수형 이상학*

전자부품연구원 RFID·USN 융합 연구센터

An Development of Security System based on The Home Gateway

Soohyung Cho Sanghak Lee*

RFID·USN Convergence Research Center, Korea Electronics Technology Institute

요 약

보안 시스템에 사용되는 많은 감시 카메라들이 RS-485 통신 방식을 통해 제어된다. 이러한 상황에서 RS-485 연결을 센서 네트워크 기술을 이용한 무선 연결로 대체할 수 있다면 선으로 연결할 필요가 없어 설치가 쉬워지고 카메라의 배치 또한 자유로워 질 것이다. 본 논문은 RS-485 연결을 대체할 수 있는 무선 센서 네트워크 기반의 감시 카메라 제어 시스템에 대한 개발로 홈 게이트웨이와 무선 센서 노드, 스마트폰 감시 카메라 제어 어플리케이션의 개발 및 구현에 대해 설명한다. 홈 게이트웨이는 유·무선 인터넷 뿐만 아니라 무선 센서 네트워크를 지원하도록 설계되었으며 MicaZ 기반의 센서 노드는 RS-485 인터페이스로 카메라와 연결된다. 넓은 지역에 분산된 보안 카메라들을 제어하기 위해 멀티-홈 또한 지원하도록 구현되었다. 보안 시스템의 감시 카메라들은 스마트폰 기반의 어플리케이션에 의해 제어 된다. 실제 환경에 배치하여 실험한 결과, 스마트폰에서의 카메라 제어에 대해 실제 카메라가 매우 빠르게 반응하는 것을 확인할 수 있었다.

1. 서 론

컴퓨터 뿐만 아니라 셋톱박스나 스마트폰과 같이 가정에서 사용 가능한 유·무선 네트워크 기기들의 증가로 가정에서의 홈 게이트웨이 사용이 보편화되고 있으며 유비쿼터스 환경이 실현되면서 인터넷 뿐만 아니라 이기종 네트워크의 접속을 지원하는 게이트웨이의 기능이 중요시되고 있다. 홈 게이트웨이는 다양한 가전 기기들을 제어하기 위해 유·무선 인터넷을 비롯하여 전력선 통신이나 무선 센서 네트워크를 지원하는 등 기능이 점차 확장되고 있다.

현재까지 가정에서의 보안 시스템은 별도의 폐쇄망으로 구성된 유선 망을 기반으로 개발되어 왔다. 대부분의 보안 시스템들은 하나의 컨트롤러에 여러 대의 감시 카메라들을 연결하여 구성되며 이들은 RS-485 통신 방식을 통해 제어된다. RS-485 통신은 ID를

지정하여 특정한 카메라를 제어할 수 있으며 약 1.2Km 까지 멀리 신호를 보낼 수 있고, 설치 시 +/-신호 두선만 연결하면 되므로 다른 통신 방식에 비해 비교적 간단하다. 그러나 유선 망에 기반한 보안 시스템은 무선에 비해 카메라의 설치가 용이하지 않으며 별도의 망으로 구성되므로 설치 비용이 높은 단점이 있다.

주로 주변 상황 정보를 모니터링하기 위해 많이 사용되는 무선 센서 네트워크 기술은 여러 분야에서 다양하게 응용되고 있다. 각각의 센서 노드들은 메쉬 네트워크 형태로 연결 되어 넓은 지역에 분산 될 수 있으며 배치가 자유롭다. 이러한 장점을 보안 시스템에 적용하면 무선으로 감시 카메라의 제어가 가능해 진다.

본 논문은 무선 센서 네트워크를 지원하는 홈 게이트웨이 기반의 보안 카메라 제어 시스템에 관한 개발로 2장에서 무선 센서 노드들을 활용한 감시 카메라들과 홈 게이트웨이와의 연결 방법, 홈 게이트웨이와 무선 센서 노드, 스마트폰 감시 카메라 제어 어플리케이션의 개발 및 구현에 대해 설명하며 3장에서 홈 게이트웨이 기반 보안 시스템의 장점과

본 연구는 지식경제부의 홈네트워크 게이트웨이 대기전력 절감 기술개발사업의 지원에 의한 것임.

문제점 및 향후 연구방향에 대해 기술한다.

2. 본 문

2.1. 홈 게이트웨이 기반 보안 시스템 구성

현재의 보안 시스템에서 감시 카메라들과 컨트롤러와의 연결은 RS-485 통신 케이블로 연결되며 컨트롤러는 카메라 ID(RS-485 ID)를 통해 특정 카메라를 제어한다. 컨트롤 메시지는 모든 카메라에게 전달되지만 카메라는 컨트롤 메시지의 카메라 ID가 자신의 카메라 ID와 일치했을 경우에 반응하며 그렇지 않으면 컨트롤 메시지를 무시한다.

RS-485 연결을 무선 센서 네트워크 연결로 대체하려면 센서 노드에서 RS-485 연결을 지원해야 한다. 컨트롤러에 부착된 센서 노드는 RS-485 인터페이스를 통해 입력 받은 데이터를 카메라에 부착된 다른 센서 노드들에게 무선으로 송신하고 카메라에 부착된 센서 노드는 무선으로 수신된 데이터를 RS-485 인터페이스를 통해 카메라로 출력하면 간단하게 무선 센서 네트워크 기반의 감시 카메라 제어 시스템을 구성할 수 있다. 홈 게이트웨이 기반의 보안 시스템은 컨트롤러가 대신 스마트폰을 이용하여 카메라를 제어하도록 설계되었다. 스마트폰은 홈 게이트웨이와 무선 인터넷으로 연결되어 카메라 제어 어플리케이션을 통해 RS-485 제어 메시지를 전송하고 홈 게이트웨이의 카메라 제어 서버 프로그램은 이를 무선 센서 네트워크 망을 통해 카메라들에게 전달한다. 그림 1은 이와 같은 구성을 나타낸다.

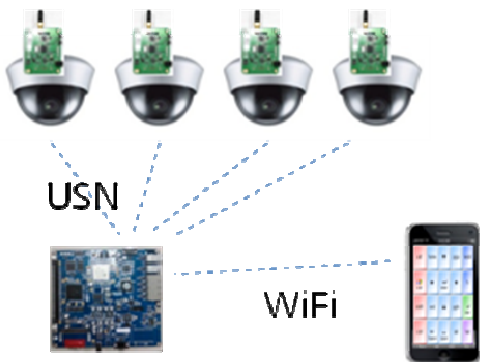


그림 1. 홈 게이트웨이 기반 보안 시스템 구성

그림 1과 같은 구조는 홈 게이트웨이가 카메라들과 서로 통신 가능한 범위에 있어야 한다는 제한점이 있다. 카메라들을 넓은 지역에 배치하거나 다른 층에 배치하여 제어하려면 좀 더 개선된 형태의 통신 구조를 필요로 한다. 그림 2와 같은 구조를 일반적으로 스타형 토폴로지라 하며 이러한 네트워크 구조에서 셀(혹은 섹터)은 하나의 마스터 노드와 이와 연결된 다수의 슬레이브 노드들로 구성된다. 하나의 셀보다 넓은

지역을 커버하기 위해서는 셀과 셀 사이의 연결이 필요한데 쉬운 방법으로 각 셀의 마스터 노드들을 연결하여 데이터를 전달하는 방법이 있다. 마스터 노드를 통해 멀티-홉 라우팅이 이루어짐으로서 홈 게이트웨이에서 먼 거리에 배치된 카메라의 제어가 가능하다. 그림 2는 이와 같은 구성을 나타낸다.

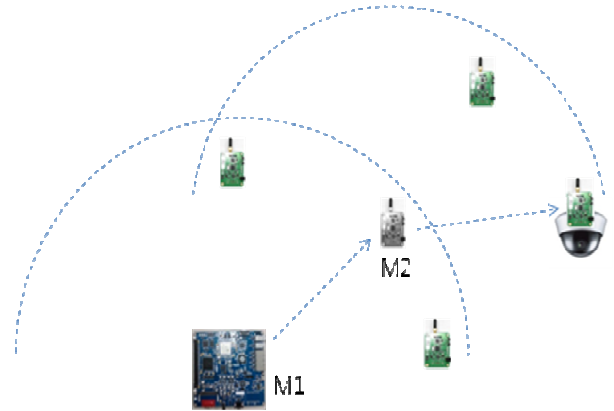


그림 2. 멀티-홉 지원 보안 시스템

2.2. 홈 게이트웨이 개발

보안 시스템에 적용된 홈 게이트웨이는 유·무선 인터넷 뿐만 아니라 무선 센서 네트워크를 지원하도록 설계되었다. 시스템은 두 개의 프로세서(메인 프로세서, AVR 프로세서)와 FPGA가 사용되었다. 메인 프로세서는 홈 게이트웨이 역할을 수행하고 FPGA는 저전력 상태에서 홈 네트워크 내부의 패킷을 감시하며, AVR 프로세서는 대기 모드 상태에서 네트워크 신호 감지 및 시스템 전원을 제어한다. 무선 센서 네트워크에 접속하기 위해 CC2420 라디오 트랜시버가 연결되어 있다. 그림 3은 홈 게이트웨이의 하드웨어 구조를 나타낸다.

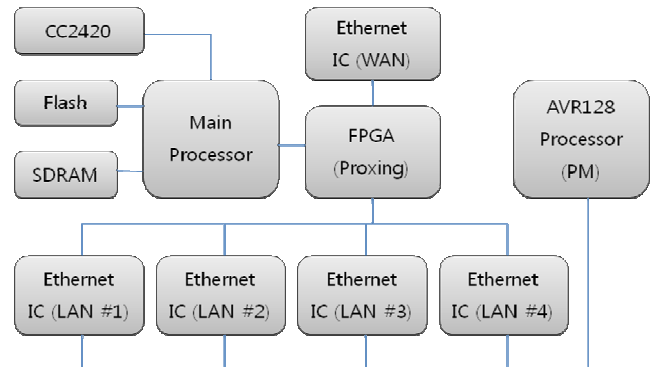


그림 3. 홈 게이트웨이 하드웨어 구조

홈 게이트웨이의 운영 체제로 임베디드 리눅스와 마이크로 블레이즈, 펌웨어 코드가 두 개의 프로세서 및 FPGA의 운영을 위해 사용된다. 임베디드 리눅스는 메인 프로세서에서 게이트웨이 기능을 수행한다. 마이크로 블레이즈가 FPGA 상에서 동작하며 수신되는 패킷을 감시한다. AVR 펌웨어는 AVR 프로세서에서

네트워크 신호 감시 및 전원 관리 역할을 담당한다. 전체 시스템의 부트 속도는 약 6.4초. 무선 센터 네트워크 망을 통해 RS-485 제어 메시지를 송신하기 위해 CC2420 라디오 트랜시버 제어를 담당하는 리눅스 기반의 CC2420 디바이스 드라이버가 추가로 개발되었다.

홈 게이트웨이에서 보안 시스템 역할을 수행하는 카메라 제어 서버 프로그램은 스마트폰의 무선 인터넷 연결을 허용하며 스마트폰의 카메라 제어 어플리케이션으로부터 전송되는 RS-485 제어 메시지를 수신하여 무선 센서 네트워크 망을 통해 카메라들에게 전달한다.

2.3. 센서 노드 개발

감시 카메라 제어 시스템을 위한 무선 센서 노드 하드웨어 플랫폼은 센서 네트워크 시스템에 많이 사용되는 MicaZ 플랫폼을 기반으로 설계되었다. 여기에 RS-485 인터페이스가 추가되어 카메라와 연결된다. 프로그래밍을 위해 ISP 인터페이스를 제공하여 AVRISPMKII 프로그래머와의 연결 될 수 있도록 지원한다. 하드웨어 구성은 그림 4와 같이 ATmega 128L 프로세서와 2.4GHz RF 트랜시버인 CC2420 그리고 RS-485 트랜시버로 이루어진다.

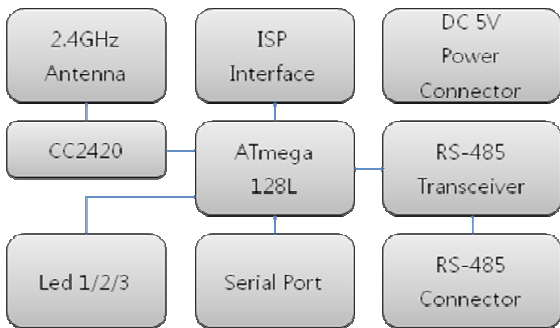


그림 4. 센서 노드 하드웨어 구조

무선 센서 노드에서 동작하는 소프트웨어는 TinyOS 기반의 어플리케이션으로서 마스터 노드에서 동작하는 어플리케이션과 슬레이브 노드에서 동작하는 어플리케이션으로 크게 구분된다. 마스터 노드는 셀 간의 데이터 통신을 위해 무선으로 수신된 데이터를 다시 무선으로 전달할 수 있지만 슬레이브 노드는 전달하지 않는다.

마스터 노드에 구현된 소프트웨어는 매우 간단한 멀티-홉 라우팅을 지원한다. 마스터 노드는 수신된 메시지가 중복된 메시지인지 체크하고 새로운 메시지이면 주변 노드에게 브로드캐스팅 한다. TinyOS의 Collection/Dissemination 과 같은 멀티-홉 라우팅 방식을 이용하지 않고 이와 같이 간단한 형태의 라우팅 방식을 구현한 이유는 TinyOS의 멀티-홉

라우팅은 신뢰성이 높은 반면에 라우팅이 바뀔 경우 라우팅 경로를 재설정 하는데 시간이 많이 걸려 감시 카메라 제어 시스템에 적합하지 못함을 실험을 통해 확인하였기 때문이다[1].

2.4. 스마트폰 기반 감시 카메라 제어 어플리케이션 개발

보안 시스템의 감시 카메라들은 스마트폰 기반의 어플리케이션에 의해 제어 된다. 사용자가 어플리케이션을 통해 제어하고자 하는 카메라를 선택하여 제어할 때 어플리케이션은 RS-485 제어 메시지를 생성하여 홈 게이트웨이의 카메라 제어 서버로 전송한다. 사용자는 카메라의 방향과 렌즈의 줌-인/아웃 등 표 1과 같이 Pelco-D 프로토콜에 따른 8가지 제어가 가능하다[2].

표 1. 카메라 제어 명령

Command 1	Focus Far
Command 2	Zoom Wide
Command 3	Zoom Tele
Command 4	Tilt Down
Command 5	Tilt Up
Command 6	Pan Left
Command 7	Pan Right
Command 8	Fixed to 0

3. 결 론

홈 게이트웨이 기반 보안 시스템을 구현하기 위하여 홈 게이트웨이와 무선 센서 노드의 하드웨어 및 소프트웨어를 개발하였으며 개발된 무선 센서 노드들을 실제 주차장에 배치하고 실험한 결과 스마트폰에서의 카메라 제어에 대해 실제 카메라가 매우 빠르게 반응하는 것을 확인할 수 있었다.

인접하여 배치된 무선 센서 네트워크 디바이스와 게이트웨이를 동시에 운용할 경우 WiFi(802.11b/g)와 IEEE 802.15.4 라디오 사이에 심각한 간섭이 발생할 수 있다[3]. 이 문제는 IEEE 802.15.4 라디오와 WiFi의 RF 채널 사이에 겹쳐진 부분이 있기 때문에 발생한다. 그러므로 WiFi 기반의 컴퓨터 네트워크와 무선 센서 네트워크를 같이 운용했을 경우 RF 간섭과 혼잡을 피할 수 있도록 IEEE 802.15.4 라디오의 채널 선택과 할당에 주의해야 한다.

본 논문에서의 홈 게이트웨이 기반 보안 시스템은 무선 인터넷 망과 센서 네트워크 망을 혼용하는 하이브리드 망에서의 보안 카메라 제어 시스템으로 카메라의 영상부에 대한 처리는 포함하지 않는다. 카메라 영상은 유선을 통해 연결되며 이를 무선으로

처리하기 위해서는 좀 더 세부적인 분석 및 설계가 필요하다. 이러한 문제점이 보완된다면 홈 게이트웨이 기반 보안 시스템은 실제 가정 뿐만 아니라 다양한 분야에서 매우 유용하게 활용될 수 있을 것이다.

참 고 문 헌

- [1] "TinyOS 2.0.2 Documentation",
<http://www.tinyos.net/tinyos-2.x/doc/>
- [2] "Pelco "D" Protocol Manual", PELCO, July 7, 2003,
p. 6.
- [3] "Avoiding RF Interference Between WiFi and Zigbee", Crossbow, <http://www.xbow.com>