무선 센서 네트워크에서 침입 탐지 시스템

이우식, 김현종, 김남기
경기대학교 컴퓨터과학과 네트워크 연구실
e-mail:humlws@kyonggi.ac.kr

Intrusion Detection System for Wireless Sensor Networks

Woo-Sik Lee, Hyun-Jong Kim, Nam-Gi Kim
Dept of Computer Science, Kyonggi University

요 약

유비쿼터스(Ubiquitous) 시대의 도래와 함께 무선 센서 네트워크기반 연구가 다방면에서 활발히 진행되고 있다. 또한 센서 네트워크를 이용한 산업이 활발하다. 본 논문에서는 유비쿼터스 시대에 걸맞게 센서 네트워크 기술을 이용한 침입 탐지 시스템을 제안하고, 이를 구현하였다. 이에 MICAz모트를 이용하여 설계하였으며 조도, 가속도센서와 RF신호를 이용하였다.

1. 서론

최근 IT산업이 활발히 진행되면서 사람과 사물, 그리고 컴퓨터가 융합되는 형태로 급속히 발전되고, 네트워크로 연결되어 인간의 삶을 도와주는 유비쿼터스 환경이 도래 되고 있다. 이런 환경 속에서 온도와 습도, 조도, 소리, 자기장, 가속도 등의 기능을 가진 센서들로부터 유용한 정보를 얻어 다양한 서비스를 제공 할 수 있으며 가속도 센서를 이용하여 사물의 움직임을 파악 할 수 있다. 예를 들어, 가속도 센서를 장착한 문의 움직임을 파악 할 때, 문을 열고 닫을 때 발생하는 가속도의 변화를 감지 할 수 있다. 가속도 센서는 움직임, 진동, 충격 등의 동적 힘을 감지하며 관성력, 전기변형, 자이로의 응용 원리를 이용한 것이다.

센서 네트워크 기술은 여러 센서들이 무선 통신을 이용해 정보를 주고받으며, 인터넷과 같은 네트워크 환경에 연결된 노드에 정보를 전달하는 시스템이다. 물리적 세계와 사이버 세계와 연결할 수 있는 특징 때문에, 이 기술을 사용해 재난 방지, 환경 감지, 물류 관리, 모바일 헬스케어 등에 적용을 시도하고 있다.[3]

본 논문에서는 Crossbow사에서 판매하는 MICAz 모트와 센서보드 MTS310을 가지고 RF(Radio Frequency) 신호와 조도, 가속도 센서를 이용한 침입 탐지 시스템을 설계 및 구현 하였다.[1] 구현된 시스템으로 어두운 실내에 문과 창문에 각각 모트를 설치한 후 가속도 센서를 사용해 침입 탐지를 하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 무인경비 시스템 동향과 센서 네트워크 활용에 관하여 살펴보고, 3장에서는 제안하는 침입 탐지 시스템에 설계 및 구현을 설명한다. 4장에서는 구현한 시스템으로 실험 후 결과를 살펴보며, 5장에서는 본 논문의 결론을 맺고 향후 계획을 기술하고자 한다.

2. 관련연구

고도의 산업화와 경제 성장으로 삶의 질이 높아지면서 외부로부터 침입을 감지하기 위한 움직임이 활발히 진행되고 있다. 자연스럽게 보안 시스템에 대한 수요도 급격하게 증가하고 있다. 현재 국내에서는 다국적 기업인 에스원(SECOM), 캡스(ADT)와 국내 브랜드인 KT텔레캅, KSC 등이 무인기계경비 시장을 주도하고 있다.[4]

센서 네트워크는 주변 정보를 센서를 통해서 정보를 획득하는 형태로 이를 활용한 서비스가 많다. 군부대에서 적의 동태 추적, 이질적인 네트워크를 통한 정보 획득, 위치 추적 시스템 등 많은 곳에서 활용 되고 있다. 또한 센서들은 점점 소형화 되고 있으며, 배터리 수명 또한 늘어나고 있는 추세이고, 무게 또한 가벼워지고 있다. 현재 센서 네트워크 관련된 연구가 많이 진행 중이다.[5]

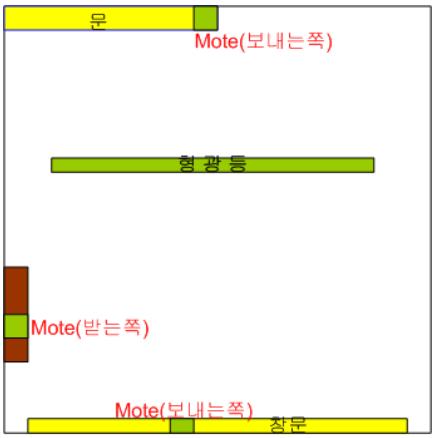
3. 침입 탐지 시스템 설계 및 구현

센서 네트워크에 사용되는 운영체제는 컴포넌트 기반의TinyOs로 핵심코드는 4000바이트 이하이고 데이터 메모리는 256바이트인 임베디드 시스템을 위해 특별히 디자인된 초소형 운영체제이다. 이를 위한 센서 모트가 많이 개발된 상태이다[2]. 본 논문에서는 버클리 대학에서 개발한 MICAz 모트를 하였고, 센서 보드로 MTS310을 사용하였다. 시스템 구성은 세 개의 MICAz모트로 구성되어 있다. 두 개의 MICAz모트는 송신자 역할을 하며 RF신호를 발생시키고 나머지 한 개 모트는 수신자 역할을 한다. 수신자 MICAz모트는 송신자 쪽에서 보낸 RF정보를 호스

트 PC로 전송해 주는 역할을 한다. 이 장에서는 침입 탐지 시스템 설계에 필요한 MICAz모트를 설치한 후 구현하고자 한다.

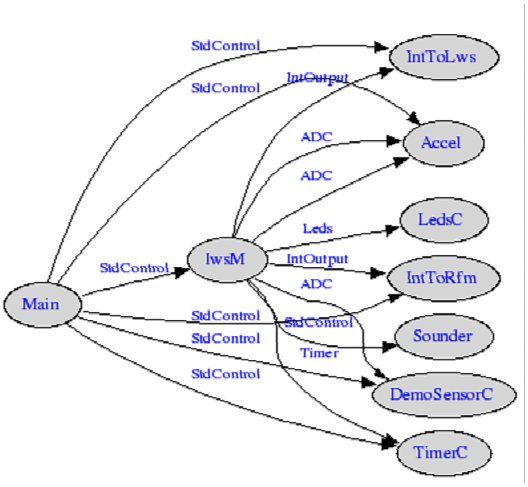
3.1 침입 탐지 시스템 설계

본 논문의 침입 탐지 시스템은 MICAz모트 세 개로 구성된다. 각 모트는 MTS310센서보드를 장착하고 있다. 센서보드는 조도 및 가속도 센서를 이용해 침입자를 탐지하게 된다.



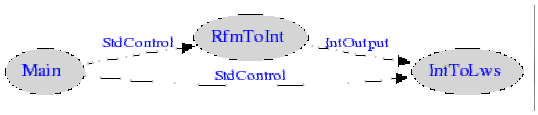
(그림 1) 기본 설계도

실내에 배치한 기본적인 설계는 그림 1과 같이 문과 창문 쪽에 송신자 역할을 하는 모트를 배치하였으며, 수신자 역할을 하는 모트는 호스트 컴퓨터가 있는 자리에 배치하였다. 이런 구성은 상황에 따라 유동적으로 배치가 가능하다.



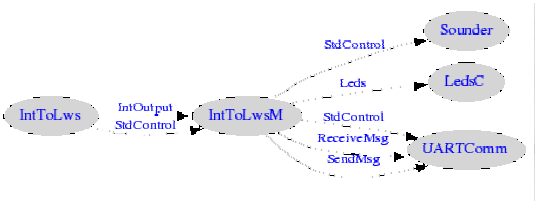
(그림 2) 송신측 Component

그림 2는 송신 측의 컴포넌트 설계를 보여주고 있다. 기본적으로 제공하는 컴포넌트를 바탕으로 설계하였다. LedsC 컴포넌트는 모트에 LED로 표시를 해주는 컴포넌트로 현재 상태를 LED로 확인할 수 있게 해주고, DemoSensorC는 조도를 측정하는 컴포넌트로 10bit의 값을 받아와 상위 3bit만을 가지고 현재 조도를 측정한다. 조도 측정으로 현재 방의 상태를 확인할 수 있다. Accel 컴포넌트는 가속도를 감지하는 컴포넌트로 침입 탐지 시스템의 핵심적인 컴포넌트라고 할 수 있다.



(그림 3) 수신측 Component

그림 3은 수신 측 컴포넌트 설계를 보여주고 있다. 수신 측 컴포넌트는 송신 측 컴포넌트에 비해 간단히 설계되어 있다. 이유는 단순 송신 측에서 보낸 RF신호를 처리해 호스트 PC로 데이터를 보내는 역할만을 하기 때문이다.



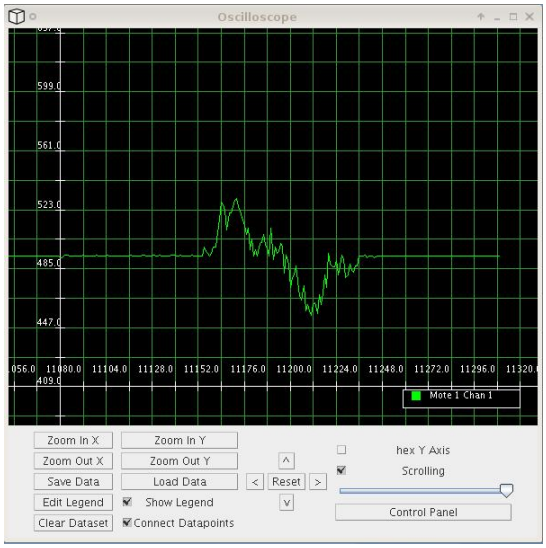
(그림 4) UART 통신 Component

그림 4는 호스트 PC에 연결되어 있는 모트에서 Serial port를 통해 Data를 전송하는 컴포넌트의 구조를 보여주고 있다. Data를 받은 호스트 PC는 데이터를 활용해 현재 침입자가 들어온 시간을 측정할 수 있고, 파일로 저장 할 수도 있으며, 그 밖의 활용범위가 다양하다.

3.2 가속도 센서의 측정 및 응용

침입 탐지 시스템의 핵심적인 역할을 하는 가속도 센서에 대해 살펴본다. 가속도는 속도가 변하는 정도를 나타내는 물리량으로, 어떤 물체가 속력이나 운동방향이 변하면서 속도가 시간에 따라 변할 때 가속도 운동을 한다. 간단한 식으로 살펴보면 $\Delta t = t_2 - t_1$와 같이 시간 간격 동안 속도의 변화 $\Delta v = r_2 - r_1$로 나타낼 수 있다. 이와 같은 식을 이용한 평균 가속도는 $a_{av} = \frac{\Delta v}{\Delta t}$ 로 나타낸다. MTS310 센서보드는 ± 2g의 가속도를 측정하는 2축 가속도 센서인 ADXL202를 가지고 있다.[6] 이 특징을 이용하여 문의 움직임에 따른 가속도의 변화를 측정 하였다.

그림 5는 실제 MICAz모트를 한 축으로 일정한 속도로 움직인 후 가속도 변화를 측정한 결과이다. 가속도가 불규칙적으로 증감하는 것을 볼 수 있다. 따라서 Δt따라 Δv가 일정하게 변하는 등가속도 운동이 아닌 불규칙적인 가속도의 움직임을 이용해 문의 움직임을 탐지 하였다. 또한 지면의 진동이나 외부 충격을 고려해 countC란 카운터 변수를 넣어 중심축에서 ± 3까지 경계를 두고, 경계 안 값은 항상 원점을 향하게 하였다.

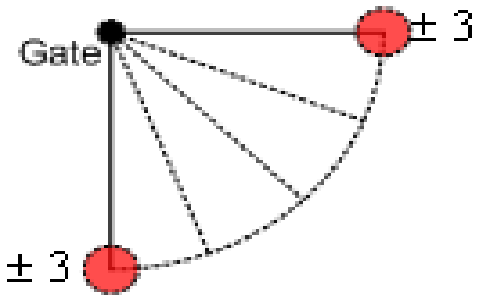


(그림 5) 가속도 변화 측정

```
//Accel gap
  if((int)value > (initA+1) || (int)value < (initA-1))
  {
    countC += ((int)value - initA) ;
    call Leds.yellowOff() ;
  }
  else
  {
    call Leds.yellowOn();
    if(countC >=3 ) countC -= 1 ;
    else if(countC <= (-3)) countC +=1 ;
  }
```

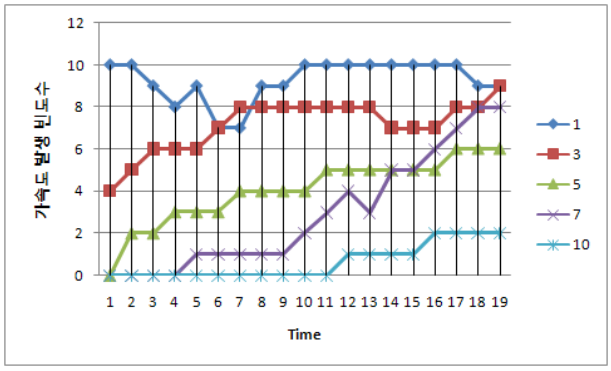
(그림 6) 가속도 경계 알고리즘

처음에는 순간 가속도 변화만을 가지고 움직임을 파악하려 하였으나, 외부 환경에 영향을 받아 정확한 움직임 파악이 불가능 하여, 그림 7과 같이 여닫이문에 Error Boundary를 설정하여 Count값을 적용 하였다.

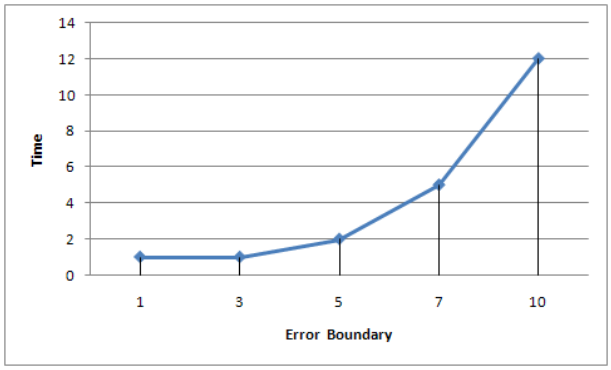


(그림 7) Error Boundary 설정

그림 8은 Error Boundary 설정값 변경에 따른 실험 결과를 나타낸다. 센서에서 보내는 데이터의 최대 개수는 10개이며, Error Boundary값이 1일 경우 다른 큰 Boundary값 보다 많은 가속도 발생 빈도수를 확인 할 수 있고, 3일 경우 빈도수가 상대적으로 적당하게 나오는 걸 확인할 수 있다. 이 결과 너무 민감하지 않고, 너무 둔하지 않은 3이란 값이 다른 값에 비해 성능이 좋다는 걸 확인 할 수 있었다. 또한 우리는 외부 환경적 요인을 고려하고 침입자 발생 시 가속도 센서가 작동되어 침입 탐지 가능한 값이 필요 하다. 그림 9는 Boundary값에 따라 최초 가속도 센서 작동하는 발생 시간을 보여주고 있다. 실험을 통해 최초 가속도 작동 시간이 1과 3사이 값일 경우 탐지 시간이 가장 짧은 것을 확인 할 수 있었다. 따라서 우리는 가속도 발생 빈도수가 Error Boundary 1처럼 많이 발생되지 않고, 5, 7, 9처럼 둔감하지 않은 ± 3의 Error Boundary값을 알고리즘에 적용해 침입 탐지 시스템을 구성 하였다.



(그림 8) Error Boundary 변화에 따른 가속도 센서 발생 빈도수



(그림 9) 침입 발생시 최초 탐지 시간

이런 시스템 설계와 가속도 실험값을 가지고 다음 장에서는 실제 실내에 모트를 문과 창문에 설치 한 후 센서를 이용해 침입 탐지 시스템 가동 후 실험 결과를 확인 하고자 한다.

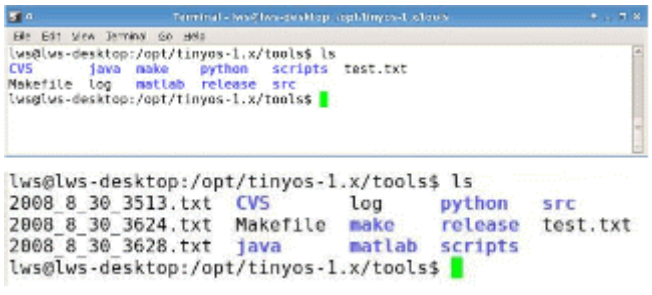
4. 실험결과 및 분석

본 논문의 실험은 그림 7과 같은 실내 공간에 MICAz 모트 세 개를 설치 한 후 실험 하였다. 상단의 그림은 모트가 설치된 학교 연구실 실내를 나타낸 그림이다. 왼쪽 하단은 송신 측 모트를 설치한 모습이고, 오른쪽 하단은

수신 측 모트가 호스트 PC와 연결된 모습을 보여준다.

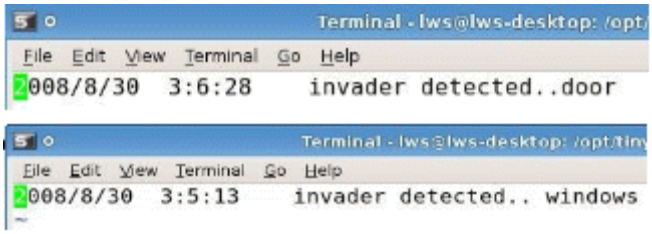
(그림 10) 실내 배치도

실내 전등이 꺼지면 침입 탐지 시스템 상태가 On이 되고, 그렇지 않다면 Off상태가 된다. On 상태에서 침입자가 감지되면 송신 측 모트는 RF 신호를 수신 측 모트에 보내고, 신호를 받은 수신 측 모트는 호스트 PC에 데이터를 보낸 후 PC는 데이터를 저장한다. 송신 측 모트는 Broadcast방식을 이용해 주변 모트에게 RF신호를 전달하게 된다. 두 개의 송신 측 모트로 부터 수신자는 RF신호를 받기 때문에 channelID로 구분을 하였고, RF신호가 겹치기 때문에 특정 데이터를 뽑아 두 개의 모트를 구분 방식을 사용 하였다.



(그림 11) 침입 탐지 파일 전후 상태

그림 9는 수신 측 모트에 연결되 있는 호스트 PC의 파일 상태를 보여주고 있다. 상단 그림은 초기 상태로 침입자 관련 파일이 전혀 없는 상태를 나타내고 있고, 하단 그림은 침입자가 생겼을 경우 상태를 나타내고 있다. 파일 이름은 침입자가 발생된 시간을 가지고 생성하였다. 이것을 통해 언제 침입자가 탐지되었는지 한눈에 알 수 있다.



(그림 12) 침입 탐지 파일 내용

그림 10의 상단은 실내 문에서 침입자가 감지되었을 경우 생성된 파일 내용이고, 하단은 창문에서 침입자가 감지되었을 때 파일 내용을 보여준다. 파일 내용만으로 침입자가 발생된 날짜, 시간, 발생장소를 알 수 있었다.

5. 결론 및 향후 계획

본 논문 에서는 MICAz모트와 MTS310센서보드를 사용해 침입 탐지 시스템을 설계 및 구현 하였으며, 조도와 2축 가속도 센서를 사용해 침입자를 탐지 하였다. 개발한 침입 탐지 시스템을 이용해 실제 문에 설치해 작동을 하였고, 침입자 발생 시 수신 측 호스트 PC에 침입자 탐지 파일을 확인 할 수 있었다. 향후 본 논문의 침입 탐지 시스템을 바탕으로 확장시켜 많은 공간에서 실습을 해보고 인터넷과 연계해 광범위 서비스를 제공하고자 한다.

Acknowledgement

본 연구는 경기도에서 지원하는 경기도지역협력연구센터 사업의 결과로 수행되었음. The research was supported by the "GRRC" Project of Gyeonggi Provincial Government, Republic of Korea.

참고문헌

[1] Crossbow (http://www.xbow.com/)
[2] TinyOS (http://www.tinyos.net/)
[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey" Computer Networks, Vol. 38, No.4, pp.393-422, March 2002
[4] 최석배, "USN을 이용한 무인기계경비 시스템 구현에 관한 연구", 2008
[5] C. Chong and S.P Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges"Proc. IEEE, Vol. 91, No.8, pp.1247-1256, 2003
[6] Analog Devices (http://www.analog.com/)