Intrusion Detection In Wireless Sensor Networks

2006

Hong Nhung Nguyen
University of Central Florida

INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

by

HONG NHUNG THI NGUYEN
B.S. University of Central Florida, 2005

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science
in the School of Electrical Engineering and Computer Science
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Spring Term
2006

ABSTRACT

There are several applications that use sensor motes and researchers continue to explore additional applications. For this particular application of detecting the movement of humans through the sensor field, a set of Berkley mica2 motes on TinyOS operating system is used. Different sensors such as pressure, light, and so on can be used to identify the presence of an intruder in the field. In our case, the light sensor is chosen for the detection. When an intruder crosses the monitored environment, the system detects the changes of the light values, and any significant change meaning that a change greater than a pre-defined threshold. This indicates the presence of an intruder. An integrated web cam is used to take snapshot of the intruder and transmit the picture through the network to a remote station. The basic motivation of this thesis is that a sensor web system can be used to monitor and detect any intruder in a specific area from a remote location.

To my

Parents and sister

with love

ACKNOWLEDGMENTS

There are no appropriate words or ways that I can find to show how much I appreciate the ideas, support and help from my friends and family. They believe in me and have no doubt in my abilities to reach my goal. They are always there for me, encourage and provide me strength with continuing and loving support throughout my school years. They are the main reasons of what I have now.

I would like to send a special thank to my advisor, Dr. Damla Turgut of the School of Electrical Engineering and Computer Science at the University of Central Florida, for her guidance, expertise and encouragement for this whole thesis. I also would like to say many thanks to my committee members, Dr. Ladislau Bölöni and Dr. Samuel M. Richie, for their comments and addition guidance. I would like to express my deep-felt gratitude to Ravi Palaniappan of the Institute of Simulation and Trainning at the Central Florida Research Park for his kindness, suggestions and enduring patience .Moreover, I would like to thank to Jin Shiyuan for his assistance and advise in this thesis. They all have guided me patiently along the way for which I am grateful.

In addition, I especially want to thank the Accelerated BSEE to MSEE program (to all people who work on this program) and to the University of Central Florida professors and staff for all their hardwork to give me such a wonderful opportunity to continue on my education road. They are all invaluable to the completion of this thesis. Last, but not least, I would like to thank all my friends at University of Central Florida for spending time with me on offering their suggestions and comments on my thesis. Their full support is the key to the success of this thesis.

Thank you everybody, again.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background

This chapter introduces the concept and the challenges of this intruder detection system. Many people have heard about smart dust and wireless sensor networks. Sensor motes are the main components of this new computing concept. Many applications are currently using these sensor motes. The various applications span in the areas are home, healthcare, automotive industry, defense, environmental, and so on. For instance, civil engineers use them to mix into concrete and to internally monitor the health of buildings and bridges.

Over the years, many people have seen the use of alarm systems and video cameras in combination to detect and prevent intruders. A complete security requires large numbers of cameras with alert operators who are actively looking for intruders or suspicious activity. For a large installation, video surveillance would require many cameras that by themselves will not be an effective way with few numbers of operators [2]. Therefore, this thesis is concentrated on looking for a technology that is easy to deploy and non-intrusively locates targets and intruders. A system should alert the operator to look at a specific area only where intrusion detected by the sensor motes. This system can also detect the target location with this information.

There are several sensor motes to collect data, such as light level and pressure, etc. A threshold is needed to be set for each of these sensors. Each sensor node communicates with each other and transmit the data to the central control station which is the stargate computer. More details of this stargate computer will be discussed later on.

Sensor motes operating at 900 MHz frequency in ad-hoc mode will be used to detect the movement of intruders in a sensor field. The real-time sensors data are used to check for the presence of an intruder. First, these motes are programmed to send out sensor data at a preset frequency. Then, sensor data is collected and monitored from the motes using a stargate computer in a wireless mode. Finally, a webcam is added to take a picture of the intruder and transmits the picture through the internet to a remote station using a web application such as Apache web-server. In order to carry out the measurements, a baseline data and background noise calibrations are needed to calibrate and collect background information. For example, when someone crosses close to the motes located on the ground, there would be a change in pressure or light sensitivity, which in turn might indicate an intruder. Figure 1.1 illustrates the system overview. The connection between sensors and MIB510 or between clients and stargate computer are all wireless. The MIB510 is linked to a local computer by a RS-232 serial port cable. The same connection is used between this local computer and stargate computer. A webcam is connected to stargate computer by a regular cable through a USB port provided on stargate.

1.2 Milestones

The experimentation requires extensive field testing and coding. In order to accomplish the task at hand, the list of milestones carried out are as follows:

- Use motes in ad-hoc network mode to collect sensor data from environment for the application
- Collect and monitor sensor data from the motes using a stargate computer in wireless mode
- Configure the stargate computer to receive sensor data and operate the camera. This

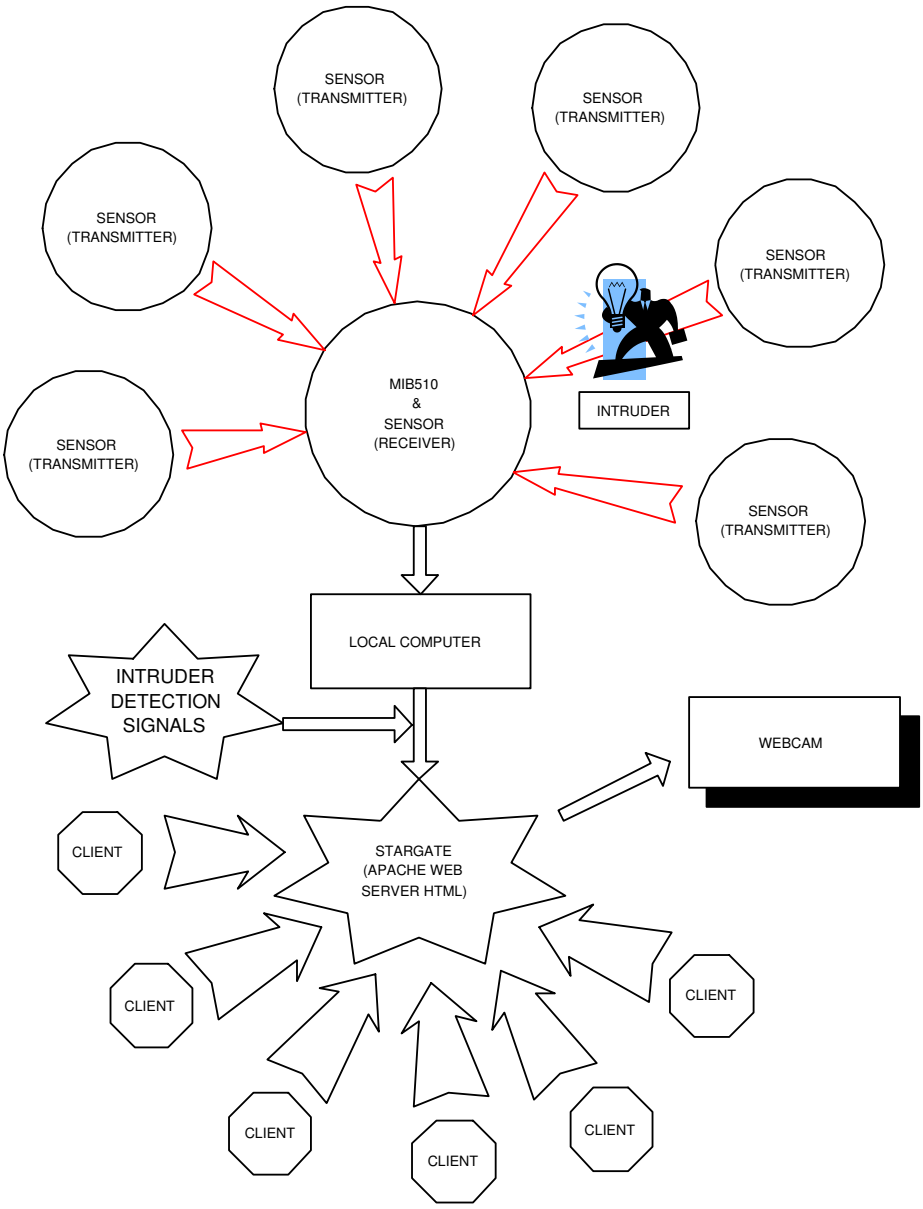

Figure 1.1: System Overview

involves a number of critical tasks:

  - Install Linux operating system in stargate to setup the network access, partition the drives, and build the Linux kernel.
  - Build the Apache web-server on the stargate. This web-server is the gateway to the internet and enable us to remotely connect to the stargate to retrieve data and images from it
  - Set up webcam Linux driver such that the stargate can take pictures of the intruder based on the available sensor data
  - Write a bash script program (webcam.sh) to check the pre-defined threshold level and run by stargate
  - Write a bash script program (webcam-transfer.sh) to store and update intruder images in local computer.

- JAVA programming

  It is necessary to use this programming language since the existing application provided by Crossbow Inc. is in Java.

  - Acquiring the relevant sensor data from the sensor motes is needed. This task is very important to reduce bandwidth required in the system.
  - Adaptive threshold for locating targets. Due to a constant change in the noise and ambient conditions, the target might be missed because of a high threshold or raise a false alarm. In order to maximize the detection, a threshold mechanism is programmed in the motes that measures the noise level in a place and decides a threshold. This task is performed based on the sensor data collected in the testing stage.

- Hardware and testing tasks involved

  An extensive field testing is conducted over a period of time to collect sensor data,

test not only the transmission range of the sensors but also the working of the system under different environmental conditions such as rain and wind. A threshold is set based on the ambient conditions at a particular measurement time.

- Deliverables and demonstration of technology

  A number of sensor motes, local computer, stargate computer and webcam, etc. will be set up in a UCF laboratory to demonstrate the intrusion detection system. When the light data is collected by sensors, they have to decide if the intruder is detected based on the threshold. The stargate records a picture and one should be able to view the image from any computer connected to the UCF network and the stargate server. This demonstrates the remote access and monitoring capability of our system.

1.3 Contribution of This Thesis

The sensor web project is a very useful system for detecting and monitoring intruders in inhospitable places like deserts. The system has a unique feature of remote monitoring that helps the user to control the system from a distant location. This work is done as part of a large sensor web project for the Office of Naval Research to develop long term monitoring systems for border security along the southern borders of Arizona. Our contribution for this project was to develop this proof-of-concept sensor web system that can be deployed under different environments. The next stage of this project would test the system on the field to study the effects of long term deployment such as wear and tear, battery life and communication bottlenecks.

The rest of organization of this thesis is as follows. Chapter 2 gives an overview of the literature. In Chapter 3, a list of hardware and software components used is discussed. Chapter 4 gives the detailed discussion of the implementation and the results. Finally, Chapter 5 presents our conclusions and possible future extensions.

CHAPTER 2

RELATED WORK

In order to develop an effective sensor based intrusion detection system, a review of some of the previous work done in this field is needed. There are many different applications in wireless sensor networks. However, no one has yet applied this sensor network to detect intruder. After doing a little research on detecting/tracking a moving object, there are a better understanding of the intricacies of developing a sensor network for this application, analyze the advantages and shortcomings of the other methods, and clearly differentiate an approach from other related work in the same field.
Some of the questions that needs to be addressed are:

- What types of sensors were used and what was the final application?
- What was the sensing mechanism?
- What was the data collection mechanism?
- How large were the sensor networks?

Lubrin et al [20] developed a mote based wireless sensor network with remote monitoring capabilities using a PDA to display patient vital information such as heart rate and body temperature. The PDA (mobile monitor) sent this data through the internet to a central database server that used Microsoft IIS to interface with the PDA. With this approach, there is a possibility of data interception when transferring vital and confidential patient data over the internet. Using secure shell software can be one solution to avoid this problem.

Sikka et al [25] in their work described a couple of sensor network hardware that was developed for specifically monitoring animals and tracking them. The work compared two

emerging hardware technologies: “Motes” and “Flecks”. While the motes were developed based on the Amtel 128 processor the Fleck was based on the Nordic NRF903 radio chip. The authors developed the Fleck chip specifically for animal monitoring and equipped it with GPS and inertial measurement units for cattle monitoring. The advantages over the motes include greater range and receiver sensitivity.

Hamrita et al [12] attempted to demonstrate an event driven smart sensor and RFID reader integrated system. They deployed wireless smart sensors in a controlled environment. They used “enventListener” program, one piece of software package in nesC, to write the sensor readings of environmental parameters to the database enabling real time remote monitoring of the system. The paper also discussed setting up a database on a server and access the network by querying through a web form to make monitoring of the system possible. However, they were unable to find sufficient documentation on the RFID reader to integrate it with the MICA2DOT mote, thus they cannot capture the actual RFID read event.

Patnode and his colleagues [23] created WISNET, a TinyOS based wireless sensors network. It is used to monitor the environmental conditions, such as light, temperature and humidity of labs and offices in ECE Department of Bradley University. WISENET used the new state-of-the-art Chipcon CC1010 microcontroller with integrated RF transceiver. To measure the temperature and humidity, SHT11 sensors were used. The light sensor was from Texas Advanced Optoelectonic Solution (TAOS) with SMBus interface. These sensors, after collecting the data, switched into a low-power idle mode to conserve energy. Both sensors were used on an original Mica mote sensor board designed by the TinyOS development team, and communicated directly with the gateway mote. This gateway mote listened and forwarded the received data to a server. A web-based data access system was created to provide a user friendly interface to the acquired information. They used WISENET’s web program to query MySQL database.

Hsieh [13] discussed highway and traffic applications by using sensor networks. In this application, GaAs Metal Semiconductor Field-Effect Transistor (MESFET) technology was used since it was conductive to high-performance and low-cost sensors for mass production. However, TinyOS micaboard motes were the primary sensor technology of interest. Many TinyOS motes can easily be formed into a viable and reliable sensor network with the transmission of packets of data of interest. Moreover, the analog-data interface and magnetometer located on the mica sensorboard can be used to detect magnetic matericals such as cars. The main reason of using this technology was the signal strength readings to infer the distance between the motes. This information is helpful not only for this particular traffic application, but also for others, such as security to track moving object.

Closed-Circuit Television (CCTV) [10] was an intelligent intruders detection and tracking system. This project used a Video Motion Detection (VMD) system to differentiate between an intruder and environmental conditions such as rain, animals or lighting effects. Basically, this CCTV system was used to monitor live images. This technique included a motion detection algorithm and an intruder identification test. When a moving object had been identified, the Intelligent Scene Monitoring (ISM) system was used to track the intruders. This technique combines several of rules to eliminate false alarms, track only an individual associated with series of suspicious events, and then trigger the alarm.

Blumenthal, et al [1], described a software architecture for mobile sensor networks. This paper mainly discussed a framework to simplify the development of software for sensor network applications.

In [22], the authors discussed the problem of tracking objects with sparsely located binary sensors. They argued that tracking with sensor network localization was complicated and presented many problems such as the inaccuracy of sensors. Also, sensor network had a low detection probability of tracking and high false detection probabilities due to a lim-

ited power supply and operates in the low signal to noise ratio (SNR) regime. Thus, they developed a distributed tracking algorithm based on the formulation and over the finite state space of sensor without sensor model and sensor network localization. In summary, this project was suitable for indoor tracking problems where the level of tracking an object movement and sensor network self-localization were high. For outdoor tracking application, it was only helpful when the degree of the passage connectivity graph of a sensor network was small.

In [16], Kulawik described the motes's hardware design. Understanding the details of mote would help to develop applications for this device better. The content of this paper was as helpful as a user guide for mica 2 mote users since it provided many practical hints. The software section gave us a better understanding of how this sensor can be implemented in TinyOS and how nesC came along. The hardware details discussed in this paper had persuaded us to use mica 2 as our sensors for this thesis.

In [26], the Police Communications Research Center in Japan had developed an intruder detection system by an image processing technique. The system was based on judgment rectangle, no-judgment area, area factor, and area factor threshold. The system processed images taken with a surveillance TV camera and gave an alarm if an intruder was detected with a speed less than 0.3 second per one cycle. This processing period included a comparison between video images from a TV camera with a basic one to find out the motion of objects; an extraction of unnecessary parts of pictures based on brightness differentials, and discriminated intruder from other moving objects by their sizes and locations. More over, this system can control direction and zooming of another TV camera to zoom in on the intruder automatically based on data calculation.

Another system applicable to surveillance had been developed is the Perimeter Intruder Detection System (PIDS) [24]. This system was used to control areas of responsibility

where risks were accessed, such as swimming pools, school precincts, museums, embassies, warehouses, etc. It was a detection-transmission system with many micro-controllers that had infra-red and ultrasound emitters and digital output transducers, which gave no harm to human's eyes. These miro-controllers were used to perform continuous surveillance of a perimeter line of arbitrary length and shape. The PIDS is distributed and triggers pattern recognition at local execution; sent the alarm byte transmission toward a Master controller, uses four-wired bus for power, external interruptions, and serial transmission of data bytes. When the pattern recognition recognizes predetermined trespassing pattern detection, a coded byte is transmitted with priority along the string to the master, then activates the alarm and orders to continue patrolling afterward. In case of a false alarm arisen, it uses some degree of assessment to discard this issue.

In [3], the authors presented a method used to protect of intruders in a small room. The experiment used one speaker and four microphones. The main idea was to use the variation of features of the room acoustic transfer function. This transfer function was computed by cross-correlation method (the impulse responsed between the speaker output and the microphone inputs). When there was a large variation between reference features and those of barrier existence, an alarm would sound.

There are many types of sensors used for intruder detection purposes. In [5], Cogdell provided the Fiber Optic Sensor System (FOSS) program. This program explored the use of fiber optic sensors and the optical multiplexing techniques for intruder detection application. The reasons to choose fiber optic sensor were the ability to detect in a wide range and changes in temperature, electrical magnetic, and acoustic energy fields, and linear or rotational accelerations. This FOSS program had explored the sensors' phase-modulated and intensity-modulated functions. The phase modulated offered high sensitivity and geometric versatility while the intensity modulated provided a low cost system. The cross-correlation technique was used here to sense the acoustic, seismic, thermal and motion of an intruder.

In order to protect the water industry, Chowdhury and Tarr [4] had introduced a security hatch intruder detection system by using seismic sensor and an open/close contact switch. This switch was used to detect the opening of a hatch. The seismic sensor incorporated microphones that used the piezoelectric effect to measure an attack signature. Basically, the microphone transmited sound waves via a diaphragm to the piezoelectric material. A software algorithm was used to analyze the electromotive force occured in this piezoelectric material. Then, an alarm was generated and sent to a control center using public-switched-telephone-network, a private wire, or even a mobile phone via the short messaging service when a threshold value was reached.

Freer et al [9] described a method and system to perform moving object surveillance and analysis using CCTV along with digital image processing techniques. Basically, the object detection algorithm isolated, detected and classified moving objects within the camera field of view in term of shape (shape factor) and size (pixel area); positional information was then extracted pertaining to each object. The shape factor was used to distinguish the elongated form of a human figure, and the pixel area was used to measure the number of pixels of intensity value in a given cluster to obtain the relative size of the object. A risk factor value also set up to compare with a set threshold level in a given period of time before the system send an alert to a human operator.

Gupta and Das [11] had developed a simple algorithm to track and predict the movement of an appropriate target and alerted sensors nodes along the projected path of the target. The algorithm localized the communication in the vicinity of the location of the target and its trajectory. The sensors had a capability of estimating the distance of the target to be tracked and the node location from the data. When the sensor reading reached above a particular threshold, the network would alert nodes that lied close to it to take appropriate actions. The experiment used 17 Berkeley MICA motes with an on-board GPS receiver

and used a light source (bulb of a flashlight) as the moving target. This test presented a few problems. The photo sensor used in MICA motes was sensitive to the angle at which light rays were incident on the sensor. The authors had to use freshly recharged batteries for all experiments in order to ensure that the light source always emited light with the same power, etc.

As many other tracking moving objects applications, Kung and Vlah [17] described a Scalable Tracking Using Networked Sensors (STUN) and Drain-and-Balance (DAB) methods to perform the task. By using hierarchy, STUN can handle a large numbers of sensors and moving objects. DAB was used to compute from expected characteristics of the objects' movement patterns over a region. Based on the simulation the authors performed, it seemed that DAB method was useful in large-scale sensor tracking systems and environments.

CHAPTER 3

HARDWARE AND SOFTWARE COMPONENTS

This thesis required many different components. Most of which are from Crossbow Inc. [7]. In this section, a greater detail on the components used will be explained. The hardware components include stargate computer, MICA2 motes, MIB510 serial interface board, MTS 310 sensor board, and a webcam. The software components are Xlisten, cygwin, Java JDK, and apache web-server. Figure 3.1 shows all of the components.

3.1 Stargate

Stargate is a powerful single board computer with enhanced communications and sensor signal processing capabilities. It supports applications around TinyOS based wireless sensor networks and smart dust technology. Figure 3.2 is a typical stargate is used.

Stargate has 400MHz RISC Processor, 64MB RAM, 32MB flash with a very small and convenience size of 3.5 x 2.5 inches [8]. It also has one type II compact flash dot (a 802.11*b* wireless compact flash card). A 256MB SanDisk compact flash card is used in order to have sufficient storage space for our database. This size of card should provide a couple years worth of space to store sensor data. Moreover, 32 MB of Intel Strata Flash, one Personal Computer Memory Card International Association (PCMCIA), a reset button, a real time clock, a lithium ion battery option, an I2C connector via an installable header, and a SA1111 StrongARM companion chip for multiple I/O access are added. The most important feature of this stargate is the MICA2 and MICAz mote capability (which directly supports our application), general purpose i/o (GPIO/SSP) and other signals via 51-pin expansion connector. The stargate is used to download programs onto motes via

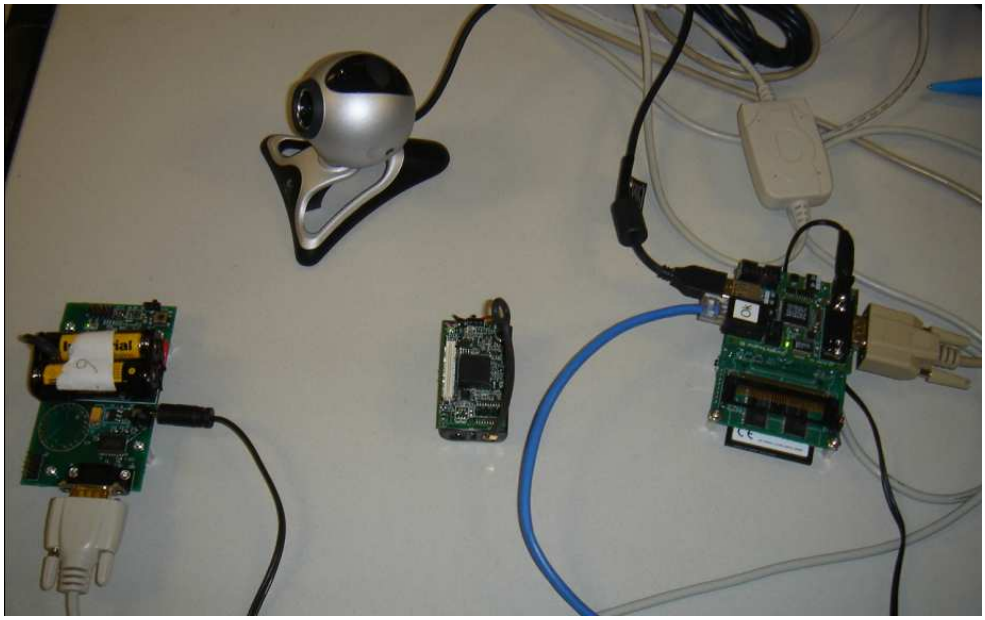

Figure 3.1: Components overview

the on-board connector. The last but not least feature of the stargate is a 51-pin daughter card interface for wired Ethernet via a 10 base-T Ethernet port (this option is not used in this thesis), a host USB webcam, a JTAG port, an external A/C power supply adapter, a RS-232 serial port via DB-9 connector.

In addition, the stargate development platform has a pre-installed software on the board and additional software on the CDROM to enable application program development. From the CDROM contents, there are many software can be used, such as an embedded Linux operating system (OS) kernel, a Linux board support package, and file system, an additional drivers in source code with instructions on how to build and install them, a bootloader for initial loading of the kernel and file system images, a flash programmer utility for programming the flash ROM, a GNU cross platform development tools and a system configuration support file archives.

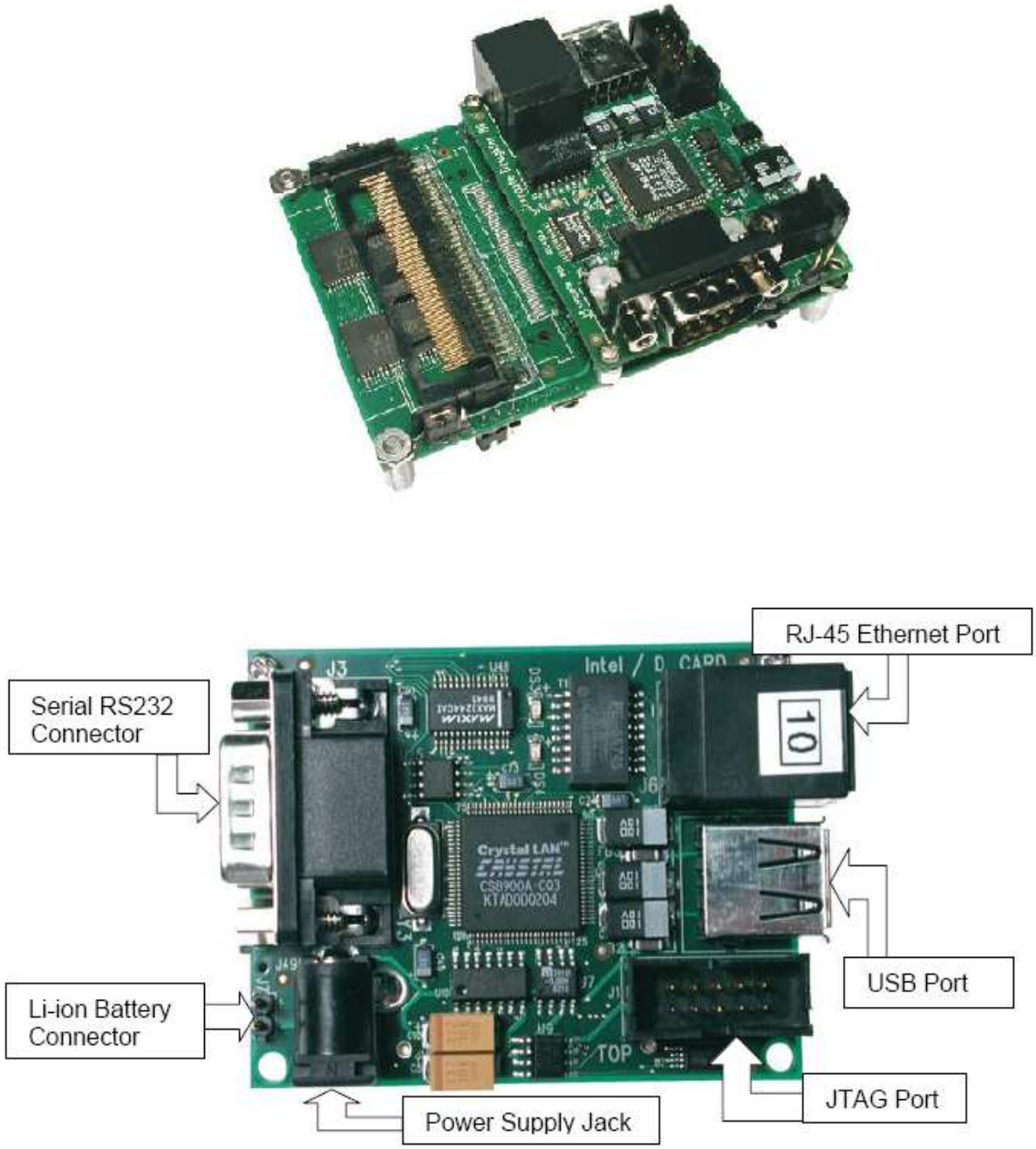

Figure 3.2: Stargate Development Platform (Processor board (top) and daughter card(bottom))

One of the interesting uses for the stargate is an application server. It is a remotely deployed stargate configured with software for local management of a sensor network. There are two server software that can be installed: Apache web-server for web based applications and a Java runtime. A version of the Apache web-server is located on the stargate support CDROM. In this particular application, Apache web-server is used to display picture of the intruders. Xlisten is a basic softwares installed for this purpose. Xlisten takes an input stream of wireless sensor data from the base station mote. More detail about this program will be discussed in later sections. The stargate processor board also has many different applications. Here are the lists of what are used:

- A single-board computer running embedded Linux OS
- Sensor network gateway
- Distributed computing platform
- Embedded sensor signal processing

3.2 MICA2 Motes

There are many different kinds of sensor motes being used in the past researches by other people on the wireless sensor network field. It supports the applications such as wireless sensor networks, security, surveillance, force protection, and environmental monitoring, etc. In prior work by the researchers, it mentioned that MICA2 range of motes have both on board sensing capabilities, and the ability to interconnect to a wide variety of devices through general I/O. As a result there is a huge potential to combine other physical information (such as light levels) into the system to provide enhanced information [14]. In this project, MICA2 is used as the system's sensor motes for detecting the intruders. Figure 3.3 is a typical MICA2 used.

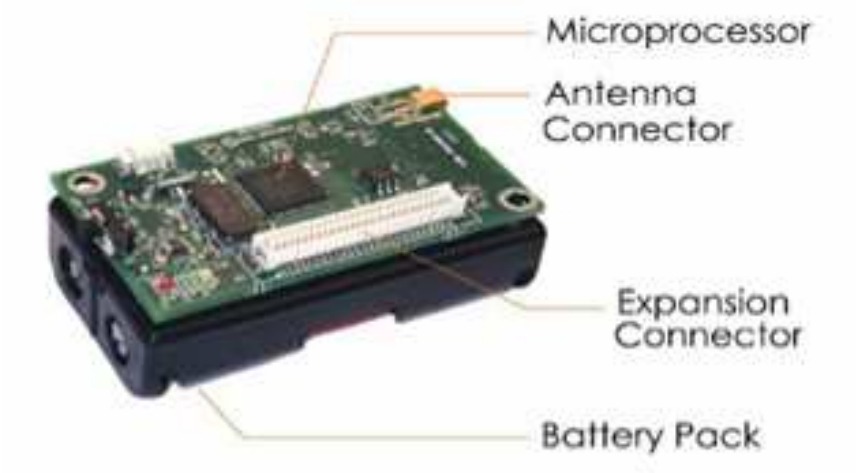

Figure 3.3: Crossbow MICA2 Measurement System

Crossbow MICA2 measurement system:
The MICA2 mote is a third generation mote modules. It is designed mostly for embedded sensor networks. Its frequency is 916 MHz, and can be chosen in any single frequency range from 903 MHz to 927 MHz [16]. For outdoor application, the range can reach to 70 feet. If the MICA2 is on the ground, however, its range is 40 feet. Similarly, for in door application, its range changes between 50 and 70 feet. When there are lots of multipath (which can block the process of transmitting data), its range is 30 feet. The sensor is a thumb-size computer which combines microprocessors and memory with radio transceivers, onboard power supplies and a variety of sensors. Inside the microprocessor, it has a microchip which contains a 7.3728 MHz clock, 128 kB of Flash for program memory, 4 kB of SRAM for data and variables, 2 UARTs (Universal Asynchronous Receive and Transmit), Serial Port Interface (SPI) bus, Inter IC (I2C) bus.

Moreover, MICA2 also provides an external serial flash memory of 512 kB, 51-pin expansion connector, eight 10-bit analog I/O, 21 general purpose digital I/O, user interface (3 programmable LEDs, and a JTAG port). It can collect and analyze sensor readings inde-

pendently and it also can link up with the motes around the other motes to form a network. For the power supplies, this sensor uses two AA batteries with 1850 mAh capacity. Many questions have arisen around this mote battery life since it is a one of the most critical parameters for a wireless sensor network. It also affects the performance of a mote's RF transmission. Assuming that motes broadcast data every three minutes, it can run for up to one year on regular AA batteries. To extend the battery life of motes, there are two options: either provide larger batteries or modify the transmission rate. OCTAVEX, wireless sensor network software, allows users to selectively adjust transmission rates; thus, it can extend the battery life as much as few additional years. In other words, the motes send data when it is reached to a threshold value. It can also measure temperatures and humidity. Upon all the features in this mote, the most important reasons of using MICA2 are as follows:

- It uses to enable low-power wireless sensor networks.
- It has the expansion connector for light, temperature and pressure, relative humidity (RH), barometric, acceleration/seismic, acoustic, magnetic and other Crossbow Sensor Boards.

3.3 MIB 510 Serial Interface Board

The MIB510 is a type of serial interface board. This serial interface board allows for the aggregation of sensor network data on a computer and any other standard computer platforms. It acts as a base station for wireless sensor network with the MICA2 motes. Whenever the MICA2 node is connected to the MIB510, that mote will act as a base station [3]. This serial interface board also provides an RS-232 serial interface for both programming and data communications. Another feature that this board provide us are the light emitting diodes (LEDs). When there is sufficient power on the board, it will display a green light and when the programming is in progress, it will then display a red

Figure 3.4: An image of MIB510

light. Figure 3.4 is a typical MIB510 that is used.

3.4 MTS 310 Sensor Board

Currently, there are many ongoing research projects in the field of wireless networks. The MTS 310 is a flexible sensor board with a variety of sensing modalities. These modalities include 2-axis accelerometer (ADXL202), 2-axis magnetometer, light, temperature, acoustic, and sounder. The MTS 310 is used with the MICA and MICA2 motes.

The advantages of the wireless sensors are that they are suitable to monitor an environment. Although these smart sensors have limited power and processing capabilities, an assembly of hundreds of them can spontaneously organize into a perceptive network that is spread throughout the physical world, able to perform tasks no ordinary computer system could. However, a mote is not a miniaturized PC; every aspect of the system, from the way

it runs programs to the way it communicates data, must be optimized to conserve power, space and cost. A rule of thumb in designing motes and their networking protocols for long-lived applications is that each device should sleep 99 percent of the time and perform its task in the remaining one percent. This type of sensor has low impact and visibility; it also can provide us with storing the data collected by the sensor in a smaller data logger. Once data is collected by the data loggers, the wireless network will also make it easier for researchers to recover the information. Also, researchers will be able to download the data onto a laptop from the safety of the base of the surveillance. Therefore, the wireless sensor network will change the way people do ecological research.

Because of the fast growing in this technology, the price of motes fall and their capabilities rise along with the rest of semiconductor technology; those wireless sensors are used for boosting productivity, opening fresh avenues for scientific research, and enabling creative ways to prevent and respond to emergencies, environmental and military applications. This type of sensor nodes run an operating system known as TinyOS. These sensors link up with their neighbors from the moment they are turned on. When one of the sensors needs some information that the other sensor has, they will send the information back and forth between each wireless node [2]. Depends on the foliage and environmental conditions, the radio range is different. The lower radio frequencies will have longer ranges in an outdoor deployment. It expects to have 433 MHz at a range of 200 to 500 feet, and 916 MHz at a range of 100 to 300 feet. Sensors, in general, and MTS 310 in specifically, are suitable for a wide range of application. One thing to keep in mind is that sensor units should be placed at least 1 to 3 feet above the ground to maximize the communication range. Placing units at ground, grass or other foliage are factors of decreasing the distance.

MTS 310 and MTS 420 are very similar to each other except that MTS 420 has a GPS module. In this thesis, we used MTS 310 due to unavailability of the MTS 420. MTS 420 is developed by UC Berkeley and Intel Research Lab and it is the latest generation of

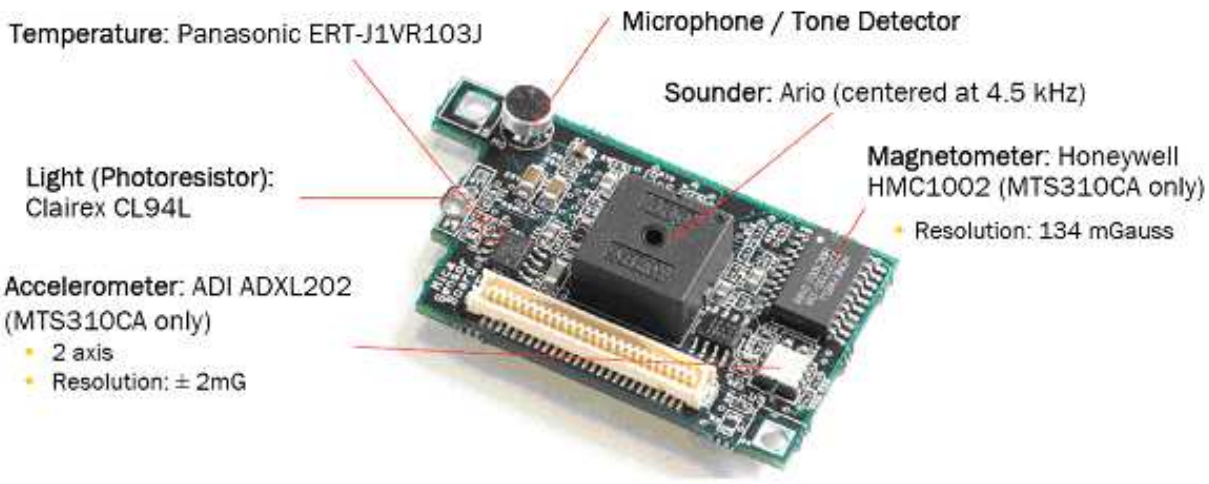

Figure 3.5: MTS310

IC-based surface mounts sensors. It can be used to measure the temperature, humidity, barometric pressure, and ambient light sensors. This board also provides extended battery life and low maintenance. Figure 3.5 illustrates this idea.

For this application, it is used to position the sensor location. It is compatible with the MICA2 processor used as well. Moreover, pressure and light level are used to determine whether there is an intruder or not.

3.5 Webcam

To enhance the way people communicate and animate life, the usage of webcams is considered to take picture of any intruder and send it to the web-server in real-time. However, not any webcam can work with stargate. There are only two units that are suitable with stargate because of their special drivers. The reason is that stargate uses Linux, which support for Philips USB webcams and OVcam drivers.

Figure 3.6: Logitech QuickCam Pro 4000

One of these two special webcams is the Logitech QuickCam Pro 4000. It provides a simple-to-install, easy-to-use software which makes it a breeze to create, edit and enhance. This webcam includes many advance features, such as high-performance VGA CCD sensor, 640x480 video resolutions, the combination of digital zoom, live indicator light, stop-motion, and time-lapse animation and a built-in microphone. Another good features from this webcam are creating amazing videos comparable to a professional with studio-quality video editing software, taking up to thirty frames per second (with recommended system), and shooting up to 1280 x 960 pixels, 1.3-megapixel still photos with ease. Moreover, instant video calls, set up a video monitoring system, or send fabulous photos and video with our emails or to mobile phones with Logitech Mobile Video through a snap function can be made as well. It has an ability of automatic zoom in and follow the movements since the product provides motion detection software. Most importantly this Logitech product uses pwc driver Phillips chipset. This webcam can be used for Microsoft Window XP, Mac OS 9.04 and 9.1, Microsoft Windows 98/ME/2000 and is compatible with USB 2.0 and 1.1. Figure 3.6 is a picture of this type of camera [19].

Figure 3.7: Creative WebCam Pro.

The second type of webcam mentioned earlier is the Creative WebCam Pro. It uses the ov511 chipset drivers [6], which reserves for stargate driver. Similarly with Logitech Pro 4000, Creative Webcam Pro provides an excellent video quality at VGA resolution, a crystal clear, full-motion video which gives us the definitive edge for all our video needs. It also has a smart face detecting feature to track our face quickly and accurately. This is the first web camera with certified high speed USB 2.0 connection for speedy and sharp video. In another words, it lets us capture fast, smooth and high-resolution videos in more detail than other traditional webcams. It also works great with USB 1.1 equipped PCs and internet dial-up connections, but unable to deliver the same performance as the USB 2.0 does. One differentiating factor of this webcam than the others, including Logitech, is a feature of a separate clip-on lapel microphone, which is uniquely designed for better audio with less noise than webcams with built-in microphones. A picture of this camera is displayed in Figure 3.7.

Now, types of webcam are cleared to choose. Another question has risen: which programs use to capture images on the stargate? It is the “vidcat” program, which is in /home/video directory. One problem with using this vidcat is the library locations. There are different

types of libraries. It is necessary to have that these libraries are in the same folder as the video files. In order to make this work, the drivers need to be installed first. The next step is to untar the archive and download the user-space program that takes pictures, vidcat, to the /bin directory [8]. After the file is downloaded in the bin directory, it is need to be executable and then use command to make the camera to take pictures. In order to let stargate to take pictures automatically, sign in the stargate without the need of entering a password is very important. The solution is the secure shell software, SSH. It is a configured to prompt users for a password when they try to establish a connection to an SSH server. By using SSH keys and its related commands, it is possible to configure SSH and allow connections without user intervention [18].

3.6 Xlisten

This program is supplied by Crossbow Inc. As its name indicates, its main function is to listen for incoming sensor data messages, such as temperature, humidity in a serial port. On stargate, it acts as the intermediary between the sensor readings from the wireless network of sensors and the Postgres database installed on stargate. Xlisten is able to recognize and interpret packets in a standardized format, including node ID, parent, sensor-board ID, and voltage. Data transmitted by the motes is a raw analog or digital reading.

As mentioned earlier, final conversion to engineering units is done by Xlisten. The full C source code for conversion is available and provides a good reference for how to convert sensor readings for the entire line of Crossbow wireless products [7].

3.7 Cygwin

Cygwin is developed by Cygnus Solutions. Since it has many free software tools, Cygwin provides Microsoft Windows to have a Linux-like environment. In other words, many

UNIX applications can be compiled and run on a windows platform. Mainly, it is used to port software that runs on POSIX systems to run on Windows with little more than a recompilation. Cygwin has a GNU ("GNU is Not Unix") development toolchain to allow basic software development tasks, and some application programs equivalent to common programs on the Unix system. It consists of two parts: a cygwin1.dll and a collection of tools, which provides Linux capabilities.

3.8 Java JDK

JDK is needed to compile and run mote-test and other software applications. The communications API package, javax.comm, provides applications access to RS-232 hardware or serial ports.

3.9 Apache Web-Server

By using a web browser such as Internet Explorer or Netscape, the Apache web-server allows for remote web based client connections. It provides a full source code HTTP web-server with unrestrictive license for Unix-like systems, Microsoft windows, and other platforms. It is used to serve static and dynamic content on the World Wide Web. Apache has many different features, such as compiled modules which extend the core functionality. These can range from server-side programming language support to authentication schemes. With all the characteristics it provides, Apache becomes the most popular web-server. Apache is used for many other tasks where content needs to be made available in a secure and reliable way. For example, in this thesis, files can be shared of a personal computer over the Internet. In this project, Apache web-server is installed in stargate. Files are in the Apache's document root which can then be shared. This software is convenient since a designer can preview and test code as it is being developed. Basically, this server is used to upload and update new images of any intruders collected from stargate. The stargate runs

an HTML file to check the intruder detection signal sent from the local computer. When there is a signal detected an intruder from the stargate, the html file will immediately trigger the remote machine to execute the bash shell (webcam.sh) to take picture. This web-server will be refreshed every one seconds to ensure that new pictures are updated.

CHAPTER 4

IMPLEMENTATION AND RESULTS

When an intruder crosses the monitored field, some of the sensor motes will detect a change in the intensity of the light since the intruder might obstruct the ambient light conditions in the environment which the sensors are programmed for. When this happens, depending on how much light was interrupted by the intruder, the system will conclude that the light intensity crossed the threshold for triggering the alarm to indicate the presence of an intruder.

4.1 Measurement of Light Value

A real-time sensor data can be accessed either from PostgreSQL database or from raw data streams. It is inefficient to read data from the database because each time a packet is read, the JDBC record-set needed to be updated; new data are continuously flooding into the database table. However, it is straightforward to read sensor data directly from raw data packets. The following is an example of a raw data packet. Comparing to Crossbow's manual for the raw data's message format, it is assumed that the first three bytes in the packets are used to indicate a new set of data is started.

FF FF 007D 1D 84010500 A801 F2011602 EF 013800780229032703000000000000000000

Each data packet contains several fields of data. The overall message format is as follows:

Destination address: 7D 1D

Message handler ID: 84

Group ID: 01

Source address: 0500

Temperature: F201

`Light:` 1602

`Microphone:` `EF` 01

`accelX:`3800

`accelY:` 7802

`magX:` 2903

`magY:` 2703

where accelX and accelY represent values of accelerometer; magX and magY are values of magnetometer which measures the strength of magnet field. Date is in little-endian format: 1602 where 16 is the least significant and 02 is the most significant, so 1602 equals to 0x0216 = 534 (decimal). The MTS 310 mica sensor board has five sensors: Accelerometer, Magnetometer, Microphone, Light, and Temperature. In our application, only the light data is interested since the change of light data can be used in detecting an intruder. In existing software packages, the file named "Listen.java" is used to receive real-time sensor data packets. This file is modified such that it is able to read and categorize light data based on different senders (sensors). Figure 4.1 is a flowchart of our design.

There are three sensors (two senders, one receiver) used in this thesis. From our experiment set up in Insitute of Simulation and Training, the threshold is set as 5.5. However, it needs to be changed and tuned according to different testing environments. Initially, our program waits for 5 seconds for signal stabilization since the initial signals are unstable. On being activated, the local computer will collect sensor data from the motes placed at random locations on the field through the serial MIB510 connector. After receiving each packet, the 14th and 15th bytes (corresponding to light data) of each packet are picked out and converted into decimal data. Then, the variations of light data is checked from remote sensors. Instead of having the sensor system to read a complicated threshold level, the operation is simplified by having the local computer write a binary code to a data-file file. If the light_changes (standard deviation) exceeds a pre-defined threshold, the Listen.java code will start to write a value of "1" to the data-file file, meaning that there is an intruder.

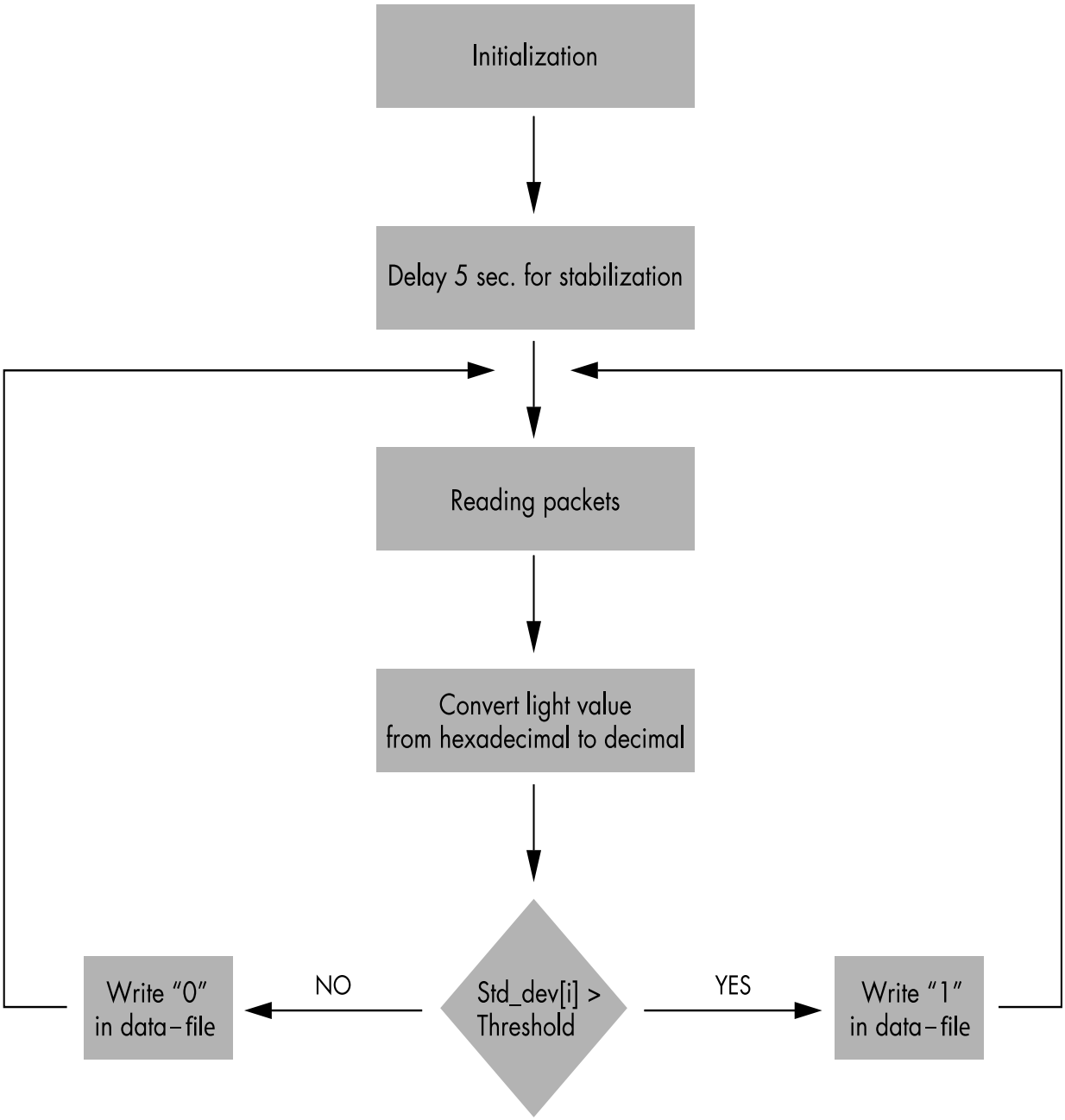

Figure 4.1: Flowchart of calculating the changes of light values

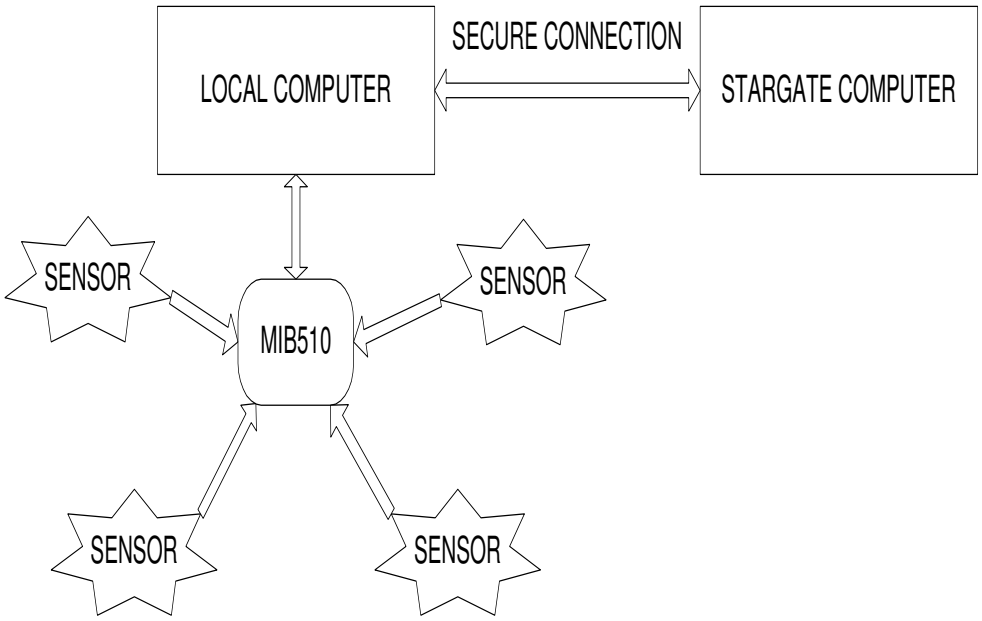

Figure 4.2: Secure connection is needed

Otherwise, a "0" is written to indicate an absence of the intruder. This "file writing" operation in the sensor java code is continuously implemented by the local computer. After the detection is achieved, the system will then delay the next set of data collection for 5 seconds for the system to time synchronize and convey the information of the presence of the intruder to the stargate to record a picture of the intruder. This data-file file is then transfered to the apache web-server, and read by another program at the apache web-server.

Whenever an intruder crosses, the change of the light value triggers the remote camera and alarms. This is achieved by sending the data file to the stargate at each instance by a network cable. This is done by establishing a "trusted" secure connection between the local computer and the stargate, as demonstrated in figure 4.2. This secure connection is necessary in order to prevent data interruption and corruption. This file transfer operation is a critical for the sensor web system as this will be used to locate the presence of an intruder. In order to achieve the file transfer operation, a Unix command "scp",

which is embedded in the Java code is used. This operation takes place after the used of "ssh-keygen" method, which are private and public keys to enable the stargate and the local computer to recognize each other as trusted hosts. Java has a method named execute which can execute the "scp" unix command.

Once the data file has securely reached the stargate, it needs to be read by the stargate continuously to indicate the presence or absence of an intruder. To do this, a bash script is run on the stargate to checks for the binary value in the data file. If it finds a "1" that indicates the presence of an intruder, the stargate will trigger the web-camera to take a picture of the intruder. This picture is then transferred to the apache web-server. The picture file is embedded in HTML file which can be accessed by all client machines. If the bash script reads a "0" from the data file, it does not take any immediate action, but tries to read from the data file again to check whether there has been a status change in the system. The webcam can be configured to take pictures at various resolutions in the code. For example, to have a high resolution image of the intruder, a picture can be taken with 640 x 480 settings. However, the system usually is set at a lower resolution to reduce system power consumption and also bandwidth required to access the pictures from the website.

Using apache web-server enables users to monitor the system from a remote location. If a user is connected to the internet, he/she would be able to access the apache web-server on the stargate to retrieve the intruder pictures from anywhere.

Even though the stargate is a small low-power computer, it has some high-end capabilities such as the ability to act as an HTTP apache web-server and run Java applications. When the stargate takes the picture of the intruder, it automatically transfers a copy of the picture to the apache server such that it can be accessed by users at remote locations. A time delay for 2 seconds is included in the stargate system such that it can synchronize

with local computer.

A webpage is designed to hold the pictures from the intruders and it refreshes every 1 second to reload the page. This ensures that there is no target or intruder will be missed. In total, the entire sensor web system will take 8 seconds (5 seconds - local computer, 2 seconds - stargate webcam, 1 second - apache server webpage) to locate the presence of an intruder which is close to "real-time" monitoring of an area.

4.2 Trigger The Camera

As mentioned above, a bash script program (webcam.sh) in stargate is used to trigger the camera to take pictures. The stargate machine is running under the scene, checking the received data-file file continuously. Whenever there is a "1" in the data-file file, it triggers the camera to take pictures and store those pictures in a specified directory. If there is a "0" in the file, it does nothing.

4.3 Display Picture

The client machines can be located in anywhere, as long as they can log on to the Internet. A client machine can access the stargate through: http://Stagate's IP Address/index.html. This is how one can access the web-server to display the pictures. This html file is programmed to refresh every 1 seconds to update pictures on the client machine.

4.4 Raw Data

Here is an example of raw data that is collected during the testing period:
`temp[0][0]=885`

```
FF FF 00 7D 1D 84010100 C701 F3017503 DF 014A 00170019031603000000000000000000
temp[0][1]=841
Light_changes[0]:31.11269837220809
intruder*************!!!
FF FF 007D 1D 84010100 C701 F3014903 EC 014A 00170019031703000000000000000000
temp[0][0]=830
FF FF 007D 1D 84010100 C701 F3013E 03 EB 014A 00170019031603000000000000000000
temp[0][1]=834
Light_changes[0]:2.8284271247461903
No intruder!
FF FF 00 7D 1D 84010100 C701 F4014203 F3014A 00170019031703000000000000000000
temp[0][0]=838
FF FF 007D 1D 84010100 C701 F4014603 F2014A 00170019031603000000000000000000
temp[0][1]=806
Light_changes[0]:22.627416997969522
intruder*************!!!
```

The Listen.java is programmed to collect every two packets of the sensor data and calculate the light_changes. Based on those calculated values, a message of intruder or no intruder is displayed for the users. The light value, such as temp[0][1]=806, is already converted into decimal data. The first number in the array, [0], indicates the sensor node. The second part of the array, [1], indicates the packet number. Since there are only two packets are picked from the raw data to calculated the light_changes at a time, [0] and [1] are the only two values used to indicate the packet number. In another words, [0] is our first data packet and [1] is the second data packet. For example, temp[0][1]=806 shows that light value is 806 from node ID 0 and this is the second packet.

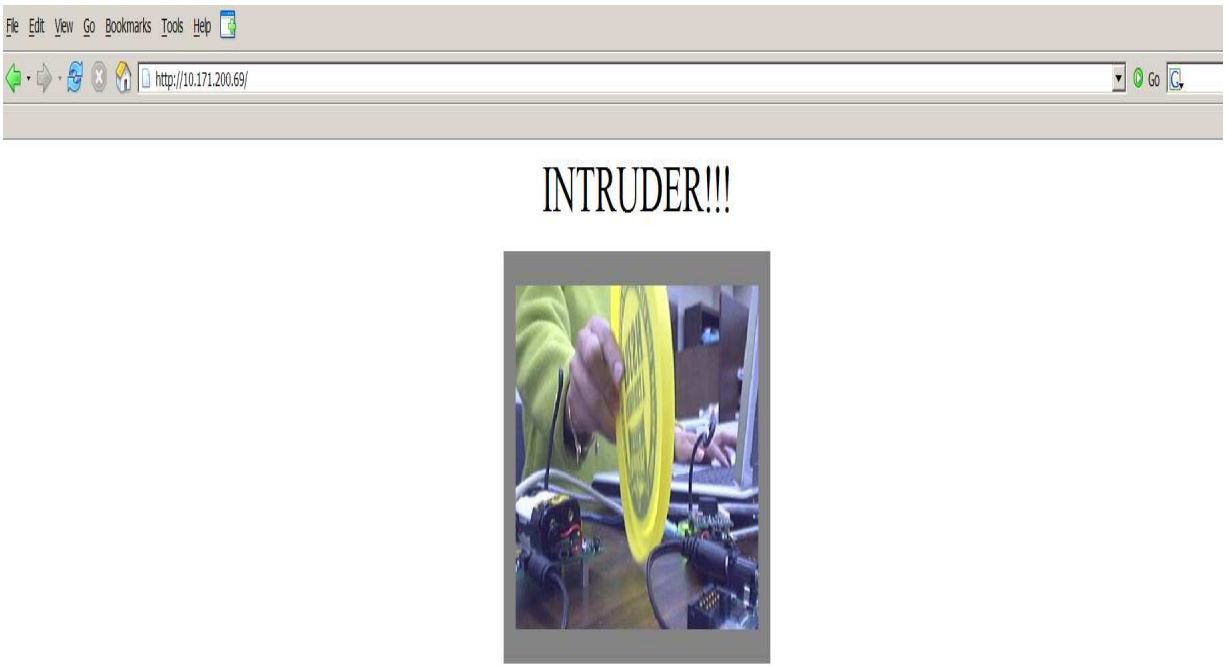

Figure 4.3: A shot of our webpage

4.5 HTTP Webpage

A simple webpage, as shown in figure 4.3 , was created. The HTTP address is the IP address of the stargate. Mainly is to show an image of an intruder. As discussed earlier, this web-server will be refreshed every one second to ensure the new pictures are updated. If there is no intruder, this browser will display no image.

In conclusion, the time-line of operation of the sensor web system is:

- Activate sensor web system

  Start the sensor data collection by activating the Listen.java code in the local machine - verify the sensors are returning data through the serial connection

- Activate the stargate bash script that checks for the binary code in the data file
- Intruder enters the environment - Light threshold is crossed, sensors indicate presence of intruder. Local machine now sends a data-file file with "1" to the stargate through secure link. It then waits 5 seconds to guarantee the stargate can receive it and continuous to check for further intruders.
- Stargate bash script, webcam.sh, finds that there is a "1" in the data-file file and triggers the camera to take a picture of the intruder. It then waits 2 seconds and checks for data-file file again for the binary code.
- Apache server in the stargate stores the picture in a jpeg format and wait for a client webpage to access the server. It also refreshes the webpage every 1 second. When a user at remote location opens up a webpage with the servers web address, the apache web-server accepts the connection and sends the picture to the client machine through HTTP protocol. This client machine then displays the picture of the intruder.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

For our particular application for detecting the movement of humans through the sensor field, a device that had long term monitoring capability with extended battery life is needed. Thus, sensor mote is an option for this application. The Berkeley motes offered small size, low cost, low power, radio frequency (RF), simulation environment. The mote cons included a small memory, new programming language (nesC). Also, the project was application oriented and as such no hardware modifications to the existing platform is made. An adhoc network is planned to collect and transfer the environmental data collected from the sensors over the internet, so it could be monitored from anywhere. If the environmental parameter went above or below a particular threshold value, an alert message would be sent.

Future work can include having additional sensors on the terrain to complete more difficult tasks. For instance, more parameters can be added to the messages passed around by the sensors. Instead of only having the threshold calculation and comparison,the basic information of the landscape can be passed. The power level of the mobile agents can also be another parameter. When a sensor agent is about to run out of battery, it will let other sensors in the communicating range that it will quit sensing temperature information and change to a power save mode. The sensor changed to power save mode will only focus on receiving information from other sensors but not detecting the temperature and wind information. In addition, instead of using the RFID reader integrated system, a sensor with GPS can be used to locate the motes in real-time. A user friendly Java gui can be created with GPS coordinates to track a moving object.

REFERENCES

[1] J. Blumenthal, M. Handy, F. Golatowski, M. Haase, and D. Timmermann, "Wireless Sensor Networks - New Challenges in Software Engineering," *Emerging Technologies and Factory Automation, 2003. Proceedings of ETFA '03, IEEE Conference*, Volume 1, 16-19 Sept. 2003, pp. 551–556.

[2] W. Boyles, "Wireless Sensor Application: Homeland Scecurity," http://65.19.190.109/homeland_security_Boyles.htm.

[3] Y. Choi, K. Kim, J. Jung, S. Chun and K. Park, "Acoustic Intruder Detection System for Home Security," *Consumer Electronics, ICCE 2005 Digest of Technical papers. International Conference on*, 8-12 Jan. 2005, pp. 283–284.

[4] R. Chowdhury and S. Tarr, "Intruder Detection Systems for Water-Hatches at Reseroir Sites," *Security Technology, 2004. 38th Annual 2004 International Carnahan Conference on*, 11-14 Oct. 2004, pp. 153–155.

[5] G. Cogdell, "Fiber Optic Sensors for Intruder Detection," *Security Technology, 1988. Crime Countermeasure Proceedings, Institute of Electrical, Electronics Engineers 1988 International Carnahan Conference on*, 5-7 Oct. 1988, pp. 19–23.

[6] Creative Worldwide, http://www.creative.com/products.

[7] Crossbow Technology Inc., http://www.xbow.com.

[8] Crossbow Technology, "Manual: Stargate Developer's Guide, Processor Board (SPB400CB) and Daughter Card (SDC400CA)," *www.xbow.com*, Rev. A, Feb. 2004, Document 7430-0317011.

[9] J. Freer, B. Beggs, H. Fernandez-Canque, F. Chevrier, A. Goryashko, "Automatic Intruder Detection Incorporating Intelligent Scene Monitoring With Video Surveillance,"

Security and Detection, 1997. ECOS 97. European Conference on, 28-30 April 1997, pp. 109–113.

[10] C. Fung and N. Jerrat, "A Neural Based Intelligent Intruders Detection and Tracking System using CCTV Images," *TENCON 2000. Proceedings*, Volume: 2, 24-27 Sept. 2000, pp. 409–414.

[11] R. Gupta, S. R. Das, "Tracking Moving Targets in a Smart Sensor Network," *Vehicular Technology Conference, VTC 2003-Fall, IEEE 58th*, Volume: 5, 6-9 Oct. 2003, pp. 3035–3039.

[12] T. Hamrita, N. Kaluskar and K. Wolfe, "Advances in Smart Sensor Technology," *Industry Applications Conference, 2005. Fourtieth IAS Annual Meeting. Conference Record of the 2005*, Volume: 3, 2-6 Oct. 2005, pp. 2059–2062.

[13] T. Hsieh, "Using sensor networks for highway and traffic applications," *Potentials, IEEE*, Volume: 23 , Issue: 2, Apr-May 2004, pp. 13–16.

[14] A. Jamieson, S. Breslin, P. Nixon and D. Smeed, "MiPOS-The mote Indoor Positioning System," *The Kelvin Institute, Department of Computer and Information Sciences and University of Strathclyde*, https://www.cis.strath.ac.uk/research/publications/papers/strath_cis_ publication_178.pdf.

[15] "MIB Serial Interface Board," http://www.cmt-gmbh.de/MIB510CA.pdf.

[16] A. Kulawik, "Mica2 Sensor Nodes," http://www7.informatik.uni-erlangen.de/dressler/lectures/seminar-sensornetze-ss05/paper-adam-kulawik.pdf.

[17] H. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks," *Wireless Communications and Networking, WCNC, 2003 IEEE*, Volume: 3, 16-20 March 2003, pp. 1954–1961.

[18] "LinuxHints/SSHwithoutPasswords," http://www.hants.lug.org.uk/cgi-bin

[19] "Logitech QuickCam Pro 4000," http://www.logitech.com/index.cfm/products/details.

[20] E. Lubrin, E. Lawrence and K. Navarro, "Wireless Remote Healthcare Monitoring with Motes," *Mobile Business, 2005. ICMB 2005. International Conference on*, 11-13 July 2005, pp. 235–241.

[21] "Manuals and Docs in CROSSBOW Inc. CD."

[22] S. Oh and S. Sastry, "Tracking on Graph," http://www.eecs.berkeley.edu/sho/papers/ipsn05_graph.pdf.

[23] D. Patnode, J. Dunne, A. Malinowski, D. Schertz, "WISENET- TinyOS Based Wireless Network of Sensors," *Industrial Electronics Society, 2003. IECON '03. The 29th Annual Conference of the IEEE*, Volume: 3, 2-6 Nov. 2003, pp. 2363–2368.

[24] J. Peralta and M. Peralta, "Security PIDS with Physical Sensors, Real-Time Pattern Recognition, and Continuous Patrol," *Systems, Man and Cybernetics, Part C, IEEE Transactions on*, Vol. 32, Issue 4, Nov. 2002, pp. 340–346.

[25] P. Sikka, P. Corke and L. Overs, "Wireless sensor devices for animal tracking and control," *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, 16-18 Nov. 2004, pp. 446–454.

[26] T. Takano, K. Ushita, N. Aoyama, S. Ikeda, I. Nishimura, "Intruder Detection System by Image Processing," *Security Technology, 1994. Proceedings. Institute of Electrical and Electronics Engineers 28th Annual 1994 International Carnahan Conference on*, 12-14 Oct. 1994, pp. 31–33.