Small Portable Object Technology Based Physical Network Security System

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering

By:
Gurpal Singh Chhabra
(80731007)

Under the supervision of
Dr. Maninder Singh
Associate Professor
Computer Science and Engineering Department

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

July 2009

Dedicated To Almighty
With the grace of guru

CERTIFICATE

I hereby, certify that the work which is being presented in the thesis entitled, **"Small Portable Object Technology Based Physical Network Security System"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my research work carried out under the supervision of ***Dr. Maninder Singh*** and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(Gurpal Singh Chhabra)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Maninder Singh)
Computer Science and Engineering Department
Thapar University
Patiala

Countersigned by

14/07/09

(RAJESH BHATIA)
Assistant Professor & Head
Computer Science & Engineering. Department
Thapar University
Patiala

15/7/2009

(R.K.SHARMA)
Dean (Academic Affairs)
Thapar University,
Patiala.

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to my guide **Dr. Maninder Singh,** Associate Professor, Computer Science and Engineering Department for immense help, guidance, stimulating suggestions, and encouragement all the time with this thesis work. This work would have not been possible without his encouragement. He always provided a motivating and enthusiastic atmosphere to work with; it was a great pleasure to do this thesis under his supervision.

I am equally grateful to **Dr. Rajesh Bhatia,** Assistant Professor and Head, Computer Science and Engineering Department for his appreciation and satisfactorily healing me off my inexperienced inquisitions about the new subject.

I am grateful to **Dr. R.K. Sharma**, Dean of Academic Affair for his constant encouragement that was of great importance in the completion of the thesis.

I would also like to thank all the staff members and PhD Scholar Ms. Shashi Bhanwar who was always there at the need of the hours and provided with all the help and facilities, which I required for the completion of my thesis. I am deeply indebted to my parents and friends for their inspiration and ever encouraging moral support, which enabled me to pursue my studies.

I am also very thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection which made my stay at Thapar University memorable.

Gurpal Singh Chhabra

(80731007)

ABSTRACT

Network security should be shaped in such a way that saturates the enterprise, in addition to the man power, methodologies and technology. Network security is one of the biggest concerns for a network manager in the fastest growing age of information technology. Now, this concern is further enriched by the upcoming age of participation, wherein everyone and everything is participating to make world, better place to live in. Participation is not restricted to just any specific area, but extends to Enterprises, Consumers, Developers and even public sector.

With the growing network infrastructure to double the previous year, the hacking has became much easier because each node on the internet is connected to other to another directly or indirectly and the tools for hacking increase at slightly higher speed than the tools to protect the intrusion. Any industry that doesn't have much concrete ways to stand in front of their weaknesses is at mercy of cracker, for its integrity. And in such a speed of growth of ways to breach the security and prevent them, the physical security is often overlooked; although the physical security is at the highest level of concern. For instance, some 16,000 students' identities were exposed when a laptop belonging to Buffalo State College in New York was stolen. Actually, the laptop was stolen from SunGard, a vendor help Buffalo State transition to a new computer system. As a result, The University sent out letters to affected individuals.

For protecting their network infrastructure, the network manger of the today's world apply various latest and exiting tools and techniques such as firewalls , anti-viruses and anti-spy for protecting their networks. But in the run of this expansion, the physical security of network is one major concern that requires much more attention than what it has. Use of remote monitoring using wireless sensor for physical security is one major answer to it. This thesis work design and develops one of the way in which Sun Spot can provide Physical security to the network infrastructure.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

INTRODUCTION

Network has been defined as any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances. A computer network is a collection of computers and devices connected to each other. Computer network allows information and resources to get shared between two or more computers.

Computer network has played an exciting role in bringing the world at the mini-possible difference of a key press. The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. Severity of computer attacks can vary from mere announces that disrupt business for a few hours to attacks designed to shut down or even corrupt the entire systems.

1.1 Network Security

Network security is a state of well-being of information and infrastructure in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable.

Some of industries have come up with a model to maintain network security and how all security activities in a network must evolve around security policies. A very important concern or a point to make is that network security is a ongoing continuous process. The processes are classified as follows steps (Figure 1.1):

- Implement Network Security.
- Monitor network and responds to incidents.
- Test the Security of Network.
- Improve Network security

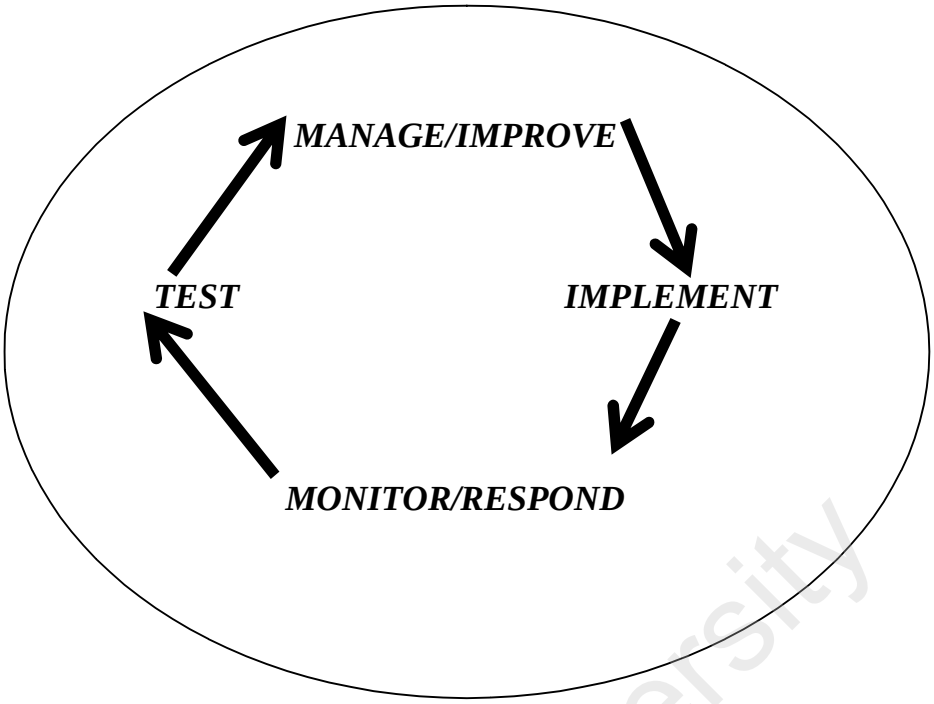

Figure.1.1 Security Wheel

1.2 Physical Security of Networks

Physical security refers to the daring task of ensuring that no unauthorized person has physical access to the systems [4]. and can also define as:

> "Physical security is the protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution" [9].

This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism. Physically securing the network environment provides the major and initial defense of the IT territory. Problem is that, system administrators leave the physical accessibility concerns while concentrating on the more enticing technical fixes. It is often thought that password protecting the *bios* would prevent anybody from being able to get access to the operating system. But anyone can bypass BIOS security and boot up system by using a screwdriver. The tools required for the physical hacker are the following:

• Phillips screwdriver (with cross-headed design),

Anybody can take out the hard-disk and connect some other system with same configuration to get data out of it.

• KNOPPIX CD,

A person can boot from a knoppix CD and delete SAM file to make is easy to login to the server as an administrator.

• KNOPPIX boot floppy disk,

Same thing can be done as with Knoppix CD.In this system with boot, making floppy, a first boot device. Move to the SAM file location and delete it.

• USB key (at least 256 MB)

Making the system boot from the USB, and load the Operating System within it to get data or make Administrator password blank [5].

1.3 Wireless Sensor Networks

Wireless sensors are the key devices used for exchange of data or gathering information related to any specific area or field. The IEEE-802.15.4 describes the various protocols for the wireless sensor networks. With the ongoing rapid growth of wireless, sensor networks, the installation cost of sensors and actuators while enabling sensor rich-environment has decreased a lot. The diagram (Figure 1.2**)** depicts how IEEE fits into the ISO's – open systems interconnection (OSI) reference model [6].

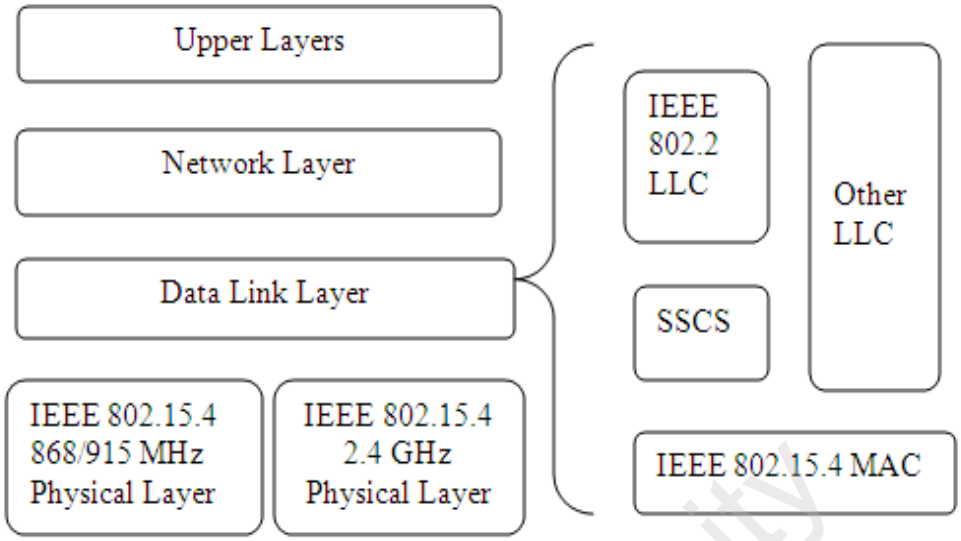

Figure 1.2 IEEE 802.15.4 in ISO-OSI 802.15.4.

The feature of broadcasting, of the wireless communication, makes the environment a little more insecure due to increasing possibilities of eavesdropping, denial of service, MITM (man-in-the-middle) and many more attacks. The upper layer ensures the confidentiality, integrity and a bit of authenticity. And also 802.15.4 does implements high security level by the use of AES algorithms with key up to the 128 bits.

A sensor is a device that produces a managed response to a change in a physical condition, such as temperature conductivity, or to a change in chemical concentration. The sensors are particularly useful for making actual measurements such as in industrial process control. Sensors are an important part to any measurement and automation application. The sensor is capable of converting any physical phenomenon into a quantity measurable by a data acquisition process, available within the device containing it.

1.5 Sun™ Small Programmable Object Technology (Sun SPOT)

The Sun SPOT project extends wireless transducer technologies to enable the emerging network of things. It is a combination of a hardware and software research platforms to overcome the challenges that currently inhibit development of tiny sensing devices. These changes have dramatically brought a revolution in nature and type of wireless sensor network applications. The Sun SPOT hardware platform is a small, battery operated,

Figure.1.3 Sun SPOT

wireless device with the Squawk Java Virtual Machine (VM without an underlying OS. This VM acts as both operating system and software application platform. Every part of it is made from device drivers and development tools, with easy assistance to help users to quickly create embedded wireless applications [8].

CHAPTER-2

LITERATURE SURVEY

2.1 Need for Network Security

Network security is vital to keeping hackers from viewing sensitive information. Network Security is a continuous process, which keeps the network resources away from any kind of unauthorized access. For example someone may think that using firewall and antivirus efficiently is what network security means. But, it's not actually.

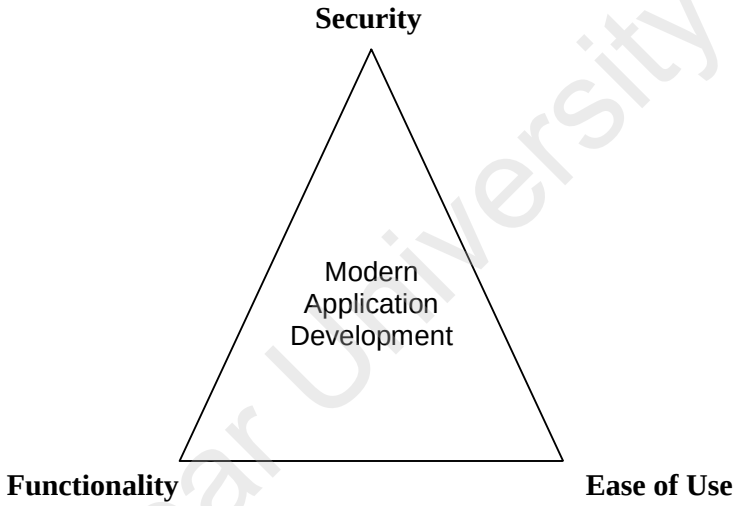

Figure 2.1 Security Triangle

The Figure-2.1 depicts that the balance between the security, functionality and ease of use need to be maintained during the software development. The most effective antivirus or firewall cannot prevent hacker from taking control over your system. The ongoing process of network security keeps note of hacker trying to check in or forcing system to compromise. With the wide range to jobs been done on internet, ranging from buying a pen to purchasing of companies through online transfer of money, the importance of network security is simply unavoidable. [3]. Security has become the most concerning part of network because of the:

- Increasing complexity of network environment and network based applications.
- Evolution of technology focused on the ease of use

- Increasing severity of attacks.
- Direct impact of security breach on the corporate assets base and good will
- Financial encouragement for hacker for new inventions
- Decreasing skill level needed to exploits [1].

Networks have exponentially grown in both size and importance in a very short time. To make the security management more challenging, the types of potential threats to network security are continuously evolving. As e-business and Internet applications continue to grow, finding the balance between isolated and open system is really critical. Also the rise of mobile commerce and wireless networks demands that security solutions become seamlessly integrated, more transparent, and flexible.

It is remarkably very easy to get an access to information in an insecure network environment, and it is really hard to find the intruders. There are a lot of tools available in the market that can be used to gain access. For example, an anonymous user can login into any system that as lower privilege user and then escalate the permission to the administrator rights.

2.2 Types of Threats

Figure - 2.2 shows some of the major threats that a computer network or the network environment faces during the information flow. Today, the list of possible attacks to the network is expanding continuously, as shown in diagram are as follow:

Scanning the network - Finding the as much as possible information about the target. Some of them are as follows:

- PING Scan.
- TCP-Connect Scan.
- TCP-Sync Scan.
- FIN, Xmas, ACK, NUL Scan.
- UDP Scan.

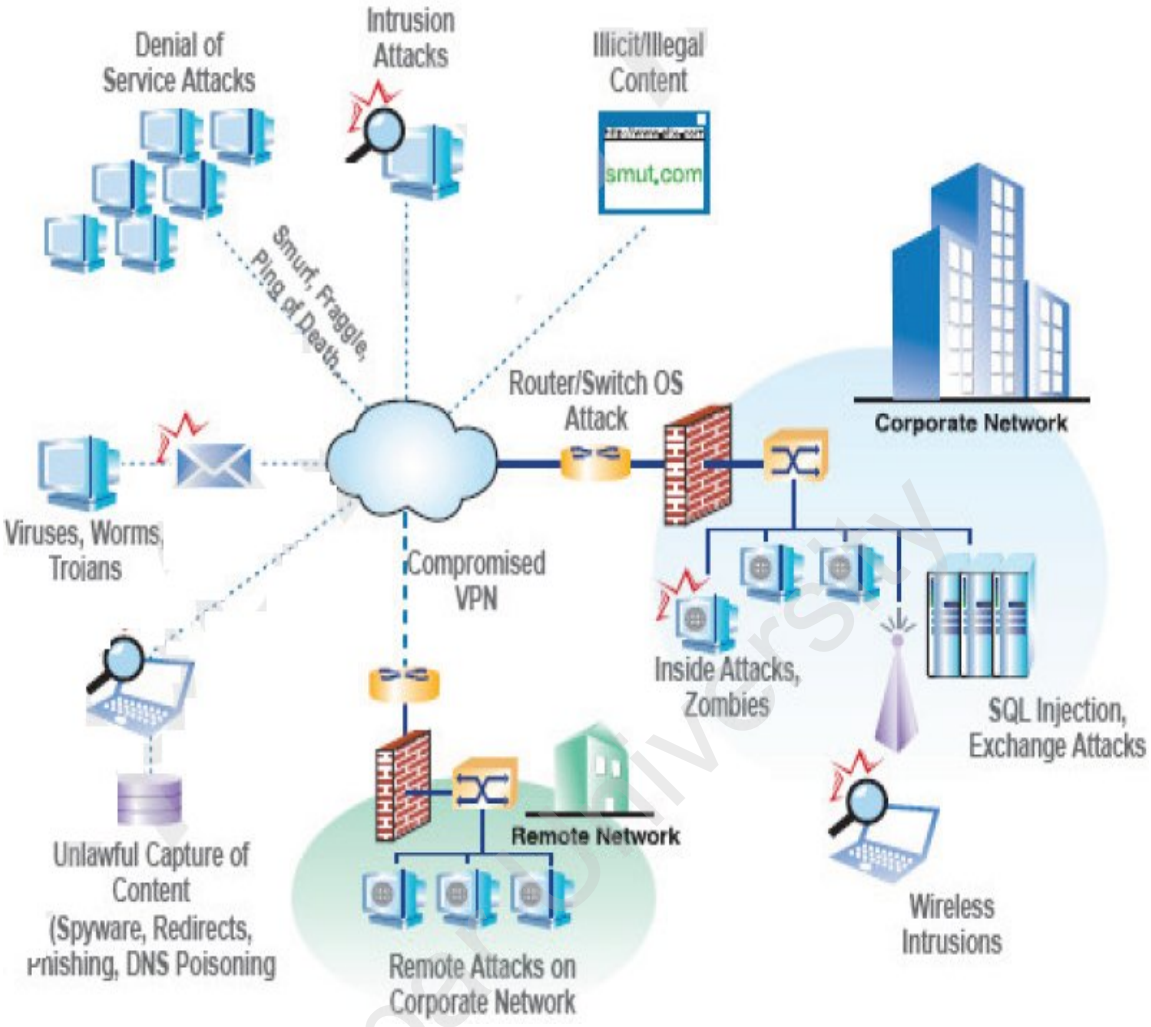

Figure. 2.2 Major Threats In the Computer Networks [7].

Buffer Overflow-Programming code overflows the buffer and enter command buffer. So anything written after is executed as command and can cause the system to return back with very secret and vital information.

Open Door and Abused Trust-For ease of access and remote authentication, system accept assertion made by trusted systems.

Social Engineering - Playing with the words to extract password from him.

Application Attack – Convincing the application to do something which is not expected like – overwriting files, etc

Trojan Software – An unauthorized program contained in a legitimate program.

Spyware – Most confusing of all threat because it is really a tough task to identify whether it is annoying program or really a threat [3].

As security scenario is continuously changing with time, some of the most common types of attacks have diminished in frequency, while new ones have emerged. Conceiving of the network security solutions begins with an appreciation of the complete scope of computer crime. Following are the most commonly reported acts of computer crime that have network security implications:

- Insider abuse of network access,
- Virus,
- Mobile device theft,
- Phishing where an organization is fraudulently represented as the sender,
- Instant messaging misuse,
- Denial of service,
- Unauthorized access to information,
- Bots within the organization,
- Theft of customer or employee data,
- Abuse of wireless network,
- System penetration,
- Financial fraud,
- Password sniffing,
- Key logging,
- Website defacement,
- Misuse of a public web application,
- Theft of proprietary information,
- Exploiting the DNS server of an organization,
- Telecom fraud,
- Sabotage [11].

2.3 Physical security (Its Need)

Information Professionals generally focuses on electronic or digital security measures. But,

"What if an attacker simply gets a physical access to the computer?"

Physical security is a critical component of your security plan, because a failure in physical security can quickly eliminate all the work done on the software side to secure the systems. Basically, the spread ongoing fight and cloud of viruses, antivirus, crackers, ethical hackers, and others, has completely decrease the concern for the physically securing the network environment and resources. If any person has physical access to the server, no matter what and how much security of antivirus and firewall server has, it is fully in control of cracker to cash the opportunity. For example, the cracker, with access to operating system, can reboot system & change setting to freely accessible mode [4]. As per old adage, no security measure is worth anything if an attacker gets a physical access to the machine [12]. Figure 2.2 depicts that the physical security of a network relies on the confidentiality, availability and integrity of information (or resource).

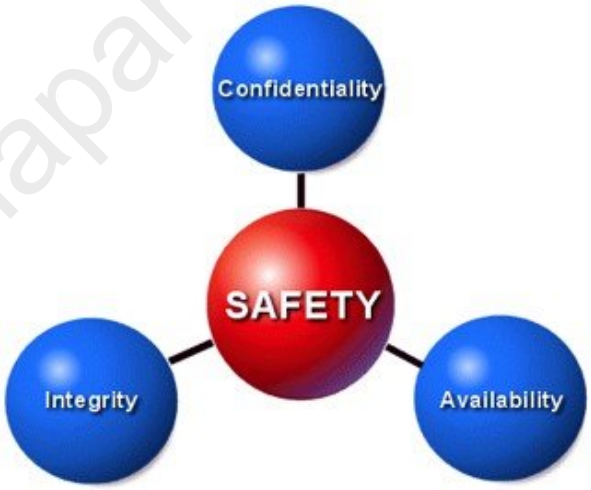

Figure 2.3 Physical Security Model

Confidentiality: It is the concealment of information or resources

Integrity: It refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.

Availability: It refers to the ability to use the information or resources [1].

A cold boot attack, cold ghosting attack or iceman attack is actually a side channel attack (attack based on information gained from the physical of a cryptosystem), where attacker actually has physical access to the system and retrieves encryption keys, from a running operating system after giving system a cold restart. This attack is based on the residual representation of data property of RAM. For example, on systems like BitLocker and FileVault, encryption key lives in RAM and attacker just has to cool the RAM modules with the air duster held upside down, yank the DIMM (dual in-line memory module), and insert it into another machine, where it can then be read to access the key [12].

Physically securing a server is often not seriously considered, but all of the firewalls and software controls in the world won't stop someone from messing with the system if someone can sit down at the keyboard and open the Finder. If necessary, keep the server in a locked closet or server room. The computer doesn't need to have a user logged (with some remote ftp tool) to run, and this way, even if someone does gain physical access to the computer, they won't be able to get into the Finder without a system username and password [14].

Overlooking of physical security and concentrate more on software intrusions issues such as viruses, Trojans, rootkit and spyware is a common practice. Although, these are the issues that need to be tackled, but the most important is the physical security of the system. Physical security can be breached without or with little technical knowledge. In most organizations physical security is entirely separate from information security and is not really a consideration for protecting information. There can be many ways for ensuring physical security of the system such as:

1. **Through Obstacles:**

   Includes, hardening of the environment, to prevent the system from the accidental and natural disasters. For example by putting multiple locks, fire proof or airtight, concrete walls, fencing, etc.

2. **By Planting Intelligence System:**

   If someone is able to break the first then administrator should be acknowledged by means of heat sensors, intrusions detections system, alarms (smoke & fire) and using cameras. It helps in providing a non integral part of information security that is physical security.

3. **By Keeping Backups:**

   If still attacker is able to breach security, then for that, there should be a well defined pre-plan. That is, by keeping the backups by various means, as quickly as possible. Mainly it is required in case of natural causes [2].

The first two ways, actually depends on the parameters and the requirements, but third part is essential for any type of system to maintain the integrity of the system. Any of the first two or both of them can be applied , but third one is necessary part of well managed network.

2.4 Classes of Physical Threats

Network security, or even computer security, is all about, attackers exploiting software vulnerabilities. A less glamorous, but level of importance is as much as any other, class of threat is the physical security of devices (servers, firewall, etc). An attacker can deny the use of network resources if those resources can be physically compromised. The four Types of physical threats are:

- **Hardware threats** - Physical damage to servers, routers, switches, cabling plant, and workstations

- **Environmental threats** - Temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).

- **Electrical threats** - Voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss

- **Maintenance threats** - Poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling [11].

2.5 Mitigation Options

For meeting the physical threats that network resources, generally suffer from can again be better understood by taking the mitigation step corresponding to the threats as follows:

Hardware Threat Mitigation	a) Lock up the resources to secure and prevent unauthorized access through ceiling, raised floor, window, ductwork, or point of entry other than the secured access point. b) Use electronic access control, and log all entry attempts. c) Use security cameras for continuous monitoring
Environmental Threat Mitigation	a) Temperature control,

	b) Humidity control, c) Positive air flow, d) Remote environmental alarming, and e) Recording and monitoring.
Electrical Threat Mitigation	a) Installing UPS systems and generator sets, b) Following a preventative maintenance plan, c) Installing redundant power supplies, and d) Performing remote alarming and monitoring.
Maintenance Threat Mitigation	a) Use neat cable runs, b) Label critical cables and components, c) Use electrostatic discharge procedures, d) Stock critical spares, and e) Control access to console ports. [11].

Table 2.1: Ways to meet different types of Physical threats

2.3 Wireless Sensor Network Terminology

2.3.1 Wireless Sensor Networks

A wireless sensor network (WSN) is a integral part of the wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or

pollutants, at different locations. These conditions can be classified under the four options as shown below in the Figure 2.4 [20].

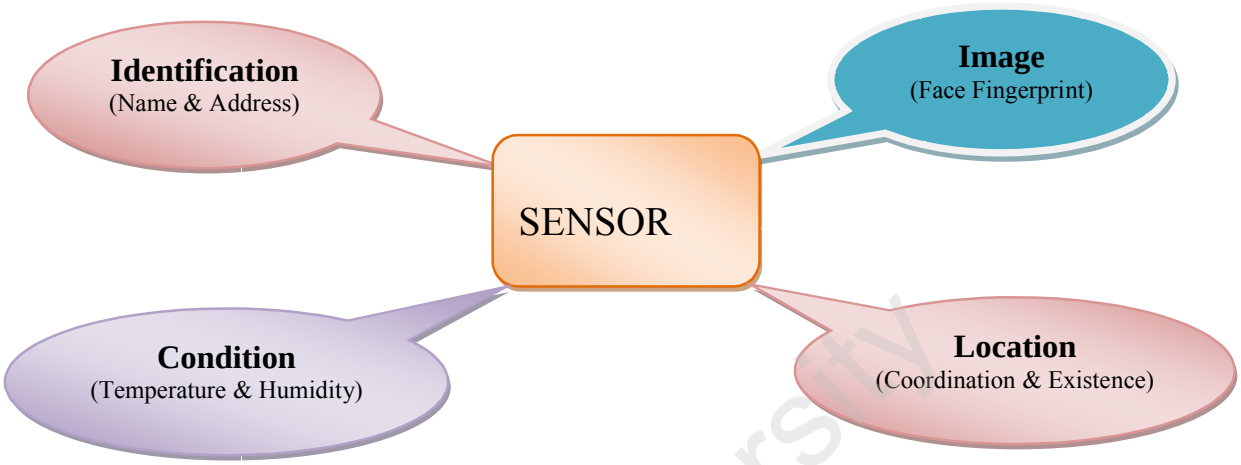

Figure 2.4 Capabilities of Wireless Sensor Network

Table-2.2 depicts the comparison between various wireless technologies in the market, including the WSN that uses the 802.15.4 IEEE standard for communicating up to 300m. It also shows comparison between the various advantages of various technologies like the data cost [19].

Sensor nodes are like small computers, having basic interfaces and components. It usually contains a processing unit with limited computational power and limited memory, sensors (including specific conditioning circuitry), a communication device (usually radio transceivers or alternatively optical), and a power source usually just like a battery that works on less. WSN has the power they can harvest or store is restricted or limited and can operate with worst environmental conditions.

Sensor nodes have fully fledged ability to cope with the node failures that may occur and the mobility of these nodes is also possible. It also is flexible to adapt any kind network technology and communication is also possible in the heterogeneous type of nodes. And the market says that a long awaited large scale development with theses sensor node has already started.

	Bluetooth	ZigBee (802.15.4)	802.11a/ b/g	802.11n	802.16a	2G/2.5G/3 G
Typical Range	< 10m	70-300m	100m	100m	50km	Cellular Network
Cost of Data	Free	Free	Free	Free	Free	Free
Freq. Range	2.4GHz	868/915MHz 2.4GHz	2.4GHz - 5.8GHz - a	2.4GHz	2-11GHz	869-894MHz
Network	P2P	Mesh	IP & P2P	IP & P2P	IP	IP
IT Network Connectivity	No	No	Yes	Yes	Yes	Yes
Application	Cable replacement	Sync and Transmission	of video/ audio data	LAN, Internet	LAN, Internet	Metro area broadband Internet connectivity

Table 2.2: Comparison between various Wireless Technologies

TinyOS is the one of the standard operating system for sensor nodes, that provides an event driven operating environment and uses a component model for designing sensor network applications [21].

2.3.2 Applications of WSN

Main area of applications of the WSN terminology can be commonly divided into natural cause, human daily activities and the various human construction works. Table 2.2 shows some of the area where the WSN is being effectively used

Natural Cause	Monitoring water/ soil/ air quality Tracking wild animal

	Being aware of disaster
Human Activity	Tracking people Studying pollution Medical care support
Human Construction	Controlling office environment Managing business inventory Informing traffic circumstances

Table 2.3: Various current Application Areas of WSN

2.4 Types of Wireless Sensor Devices

Idea of "Smart Dust" came in to existence by the Kris Pister around the year 1998-2001, with the emergence of Berkley Motes, followed by intel launching its own version of it. Here are some types of Tiny sensor devices.

1. **Berkley Motes, Tiny OS :**

Berkley introduced its first small sensor device with Tiny OS that consist of Mica2, Mica2Dot , 8- bit microcontroller, 7.37/4.0Mhz clock , 128 KB flash, KB SRAM, 512 KB external flash, 2 AA batteries /3V lithium cell battery.

2. **Intel Mote :**

Then Intel Corporation launched its own tiny devices with the Zeevo module. Intel mote consist of the:

a) Zeevo module (ARM 7 c or e, SRAM and f la s h memory, Bluetooth, wireless), Tiny O S.
b) Mote2 ,
c) 32- b it X-scale PXA 271 CPU,
d) Large RAM and f la s h memory ,
e) r uns Linux and the Jav a VM

3. Sun SPOT

Sun Microsystems brought Java technology to wireless sensor and actuator devices with :

a) Ease of development and security of Java.

b) Take advantage of the Java programming language dynamic capabilities for developer productivity

c) Use standard Java IDEs and debugger tools.

Because of the flexible programming and availability of IDE and working environment , Sun SPOT is the most preferred workplace for sensor programmers [23]. The Sun Labs research project to investigate small wireless sensor technology with, Powerful 32-bit processor (180MHz ARM9), 6 analogue inputs, USB interfaces, 2.4 GHz 802.15.4 radio with antenna, Sensors:

- 3-axis 2G/6G Accelerometer
- Light Sensor
- Temperature Sensor
- 8-TriColor LEDs for display
- 5 GPIO pins for external I/O control – 4 high current I/O pins [25].

The Sun SPOT is a small wireless computing device or a (platform) that runs Java directly, with no operating system. The system is available with an onboard set of sensors, and I/O pins for easy connections to external devices, as shown in annexure I. The Sun SPOT is a Java platform powered by the Java ''Squawk" virtual machine (VM) [13]. Here, Squawk VM means VM acts as both operating system and software application platform, as further shown in annexure II. The Sun SPOT system uses Java™ technology to up-level programming [17].

By simplifying the development of wireless transducer applications, the Sun SPOT system from Sun Labs helps transform the potential of wireless sensors into real-world products. The Sun SPOT project explores wireless transducer technologies that enable the emerging network of things. It is a hardware and software research platform to overcome the challenges that currently inhibit development of tiny sensing devices [18]. The current focus of SunSPOT is on:

Operating Environment

Writing and deploying Sun SPOT applications by providing user friendly, by basing the Sun SPOT platform on Java technology-top to bottom, hardware and software. With such working environment, it is easier to write code for small wireless transducers, sensors, and other consumer electronics devices.

Development Tools: NetBeans and SPOTWorld

There are standard Java development tools such as Netbeans or Eclipse to programs and debug applications, that have made SunSPOT application development much easier. Sun SPOT Manager, Netbeans, Apache-Ant, etc are all compatible to SUN SPOTWorld

SPOT Manager

Sun SPOT Manager is a tool by Sun Labs that uses Java WebStart Application for installing and managing your Sun SPOT Software Development Kit (SDK). The Sun SPOT Manager tool is a Java WebStart Application for installing and managing your Sun SPOT Software Development Kit (SDK).

Security

With the use of ECC technology in Sun SPOT device, it is now possible to add strong security without compromising with the memory and processing capabilities of mini devices.

Scalability

New technology or application created on the Sun SPOT platform will be capable of leveraging the massive scalability, so deployments can be carried out on virtually any scale with ease. For example, with vertically integrated systems from one to thousands of

processors, horizontally scalable grids incorporating thousands of nodes, and Storage scalability to petabytes of capacity [22].

SPOT is in millions of set-top boxes, printers, Web cams, games, car navigation systems, lottery terminals, medical devices, parking payment stations, etc. To name some application

- Swarm intelligence
- Rapid Prototyping and Experimenting with Ideas
- Rocket Launch Monitor. [23].

Sun SPOT development has already tested on Windows XP, Macintosh OS X 10.4, running on both PowerPC- and Intel-based hosts, Linux (Fedora Core 5, SuSE 10.1 and Ubuntu 6.06), and Solaris x86. [24].

2.5 SunSPOT Radio Stack

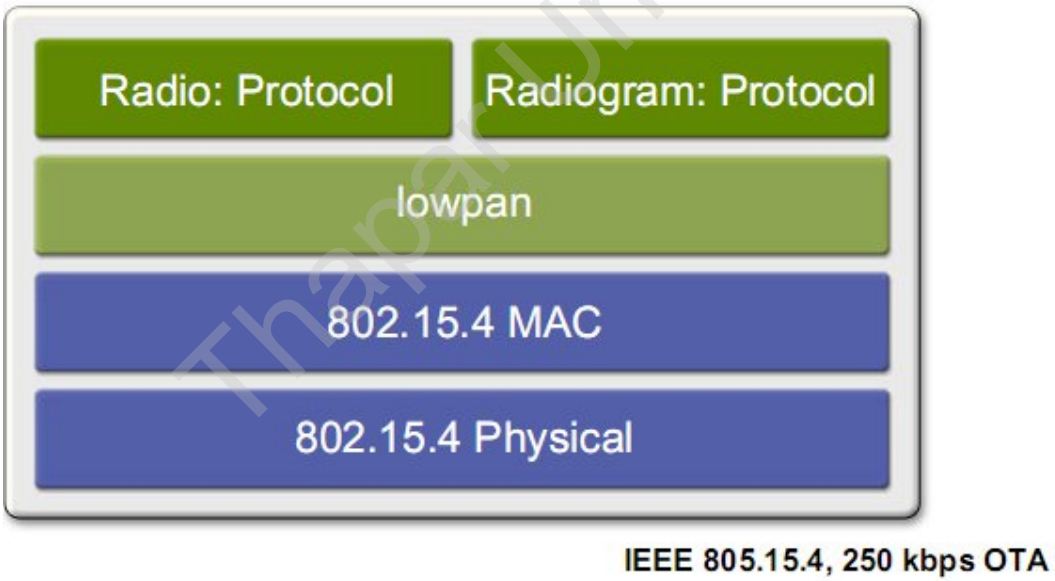

Figure 2.5 Sun SPOT Radio Stack

CHAPTER-3

GAP ANALYSIS

3.1 Gap Analysis

Network security is a continuous ongoing process to safeguard the infrastructure against exploits by knowing the enemy (the malicious hacker(s) who seek to use the very infrastructure for miscellaneous activities). There are two different types of approaches that can be used, namely proactive post active. As, seen in the literature survey, proactive approaches include activities such as placing obstacles like firewalls and antivirus and post active like rollback using backup. But, if an attacker simply steals the server, they have unlimited time, resources and many well defined ways, with which to work on breaching the security and compromising the data on it. In other word these approaches (pro &post active) ignores one of the non-integral part of security, without which network security can never be achieved i.e. - Physical Security of network environment.

For providing physical security to the network environment, there are two steps. First is to place simple (door locks) or high level (finger or face recognition) obstacles. Secondly, by using a continuous (real-time) monitoring system, so as to keep a track of or log of unsuccessful or successful physical access of any kind. Monitoring physical access by any unauthorized person, such as black hat, that to without the knowledge of intruder, is really a challenging task.

There are many wireless sensor devices in the market such as Berkley motes, Intel Mote, and Sun SPOT. But applications are hard to develop with devices other than Sun SPOT because of usages of low level languages such as C languages whereas Netbeans in case of Sun SPOT is the most efficient platform available for it. And another important drawback of these devices is that software developers need to interact with hardware, to develop applications which they don't actually know how to and not accessible to majority of software developers. Work has not yet been initiated or successfully been done to use the Sun SPOT's sensor capabilities to provide physical security to the network environment.

So, thesis focuses on looking for possibilities to have a monitoring system for making the networks environment a much secure place for network peripherals to reside on. This would ensure the physical security of the network environment via sensor technology and sending alert SMS to the concerned administrator. And is currently focused on giving an alert to the administrator about anybody enter the restricted area or the area of concern, by using the sensor technology.

3.2 Problem Statement

As described in literature review, even if latest security patches and security tools are installed then also without physical security all this is worthless. Therefore, using wireless sensor technology for physical security is very important for the most efficient and up required security corresponding to increasing physical security threats today because of its negligence. It ensures that an administrator get an alert about any unauthorized attempt enter network environment. It is more efficient and reliable means of physical security than assigning a security guard the duty to keep check on physical devices. Humans can neglect their duties, they can be bribed by the attacker, and providing 24x7 services is not possible and many more. Wireless sensors are better choice. It is only one-time investment and a longtime headache free option. Wireless sensors come up with a wide range of radius of 100 m. they are very small in size and be easily hidden from attacker's eyes. The main advantage of using such a technology is that the security officer can be informed about the attempt of attack, being anywhere in the world via his mobile or via any other online information system, so that appropriate step can be taken at the as per the current date requirement.

CHAPTER-4

DESIGN AND IMPLEMENTATION

4.1 Designing a System

The working of system follows from the opening (or rather motion) of the door to the snap being forwarded to mobile of administrator mobile phone. First of all, when the door moves, and signal is generated in remote SPOT devices, which is further forwarded to the Base station SPOT device. This SPOT is connected to a system (Laptop), which takes up the snap of the person trying to enter the room and forward the snap to the mobile of the administrator, informing him about the physical intrusion in the server room. Figure 3.1 depicts the rough sketch of how the system is suppose to perform its distributed set of task according to the solution of the stated problem.

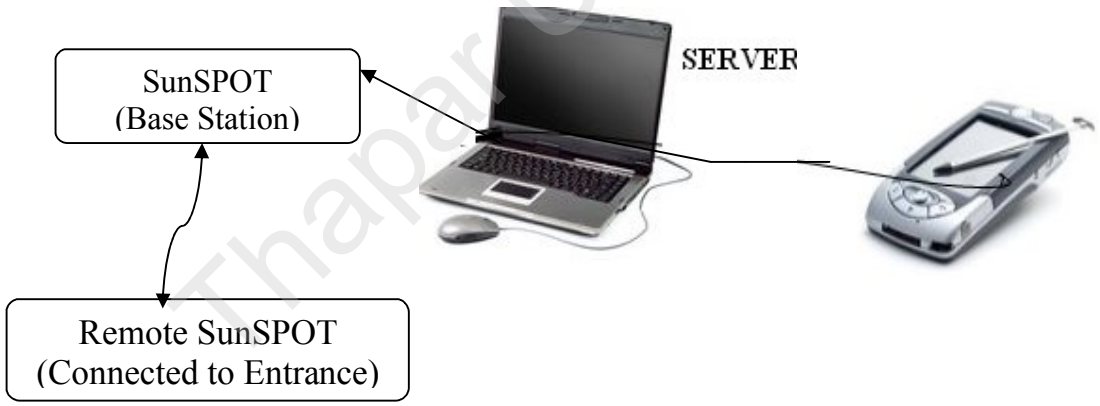

Figure 4.1 Block Diagram of Security System

The Sun SPOT, it actually has five interfaces to interact with other applications, namely:

1) Light Sensor
2) Temperature Sensor
3) **Accelerometer (Used in the thesis work)**

4) Switches (2 buttons)
5) LED Array.

Again applying the old phenomenon of the divide-and-rule, the system is divided into four major modules, based on the variation in the functionality of the subsystem namely:

Client Side :	Remote Sun-SPOT.
Server Side :	Base station (Sun-SPOT), Web cam module, SMS Forwarding.

Table 4.1 Distribution of the System

4.1.1 Client Side: (Remote Sun SPOT)

On the Client side of the system, there is only have only single interface i.e. Remote Sun SPOT, that is as per the planning is suppose to detect any change in the velocity of the object attached (i.e. acceleration) produced due to the motion of the door, by any person trying to enter the restricted area. As shown in the Figure 4.2, system explores the accelerometer of the remote Sun SPOT device, which is one of the five I/O feature or integral part of the device. First of all, an instance of the EDemo Board class of the Sun SPOT SDK's API list provided by the Sun Labs, is created. It is then required to open a tunnel, through the radio of the Sun SPOT, such as opening a broadcast connection for the other devices to capture any information posted on tunnel. Then, a datagram connection is created. It actually works to provide wrapper kind of support to support the flow of data amongst different hops of the SPOT environment. In the system this datagram capacity has been restricted to some bytes, but the system requirement is actually very less than that. Continuously reading and sending the data after the default time (nanosecond), is not actually required in this case. So the sleep class to make is variable according to our requirement, was used. Last, but not the least, this data on the datagram was placed and send it through the radio broadcast connection that was created in the initial stages of the design.

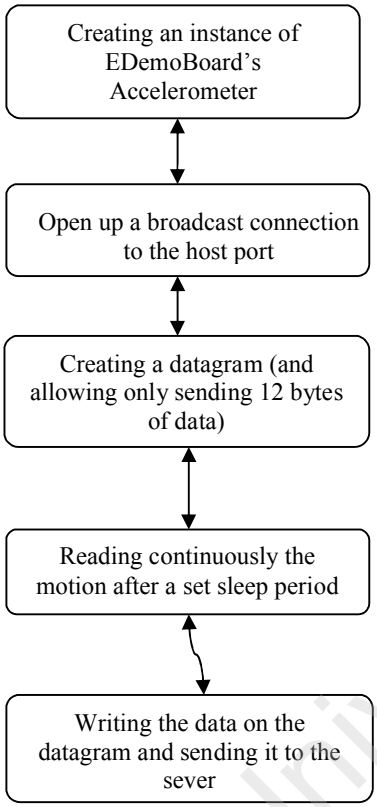

Figure 4.2 Flowchart of the Remote Sun-SPOT

4.1.2Server Side:

The server side design is suppose to capture data send on broadcast connection and then initiates a webcam, which further log the image of the person entering the room and sends a alert message to the administrator by using SMS (Short Message service). This whole job is further divided into three various subpart to make its design and implementation easier to process and understand.

4.1.2.1 Base Station (Sun-SPOT)

In the base station, using the same SDK's API, a server-side broadcast connection is created or rather opened, and is kept or put into the listening mode continuously, to capture any data or information been send unicast or broadcast for it. After reading the sample reading send by the remote client, it finds senders Id and the values corresponding to it and

finally gives a signal to webcam to take a snapshot of the person entered, as shown in the Figure 4.3

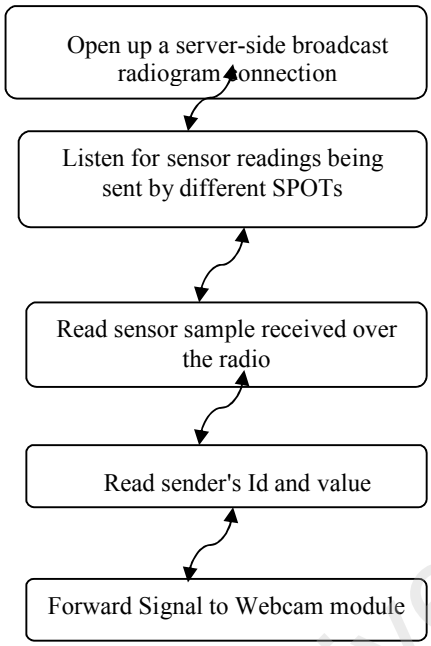

Figure 4.3 Flowchart of the Base Station

4.1.2.2 Webcam Module

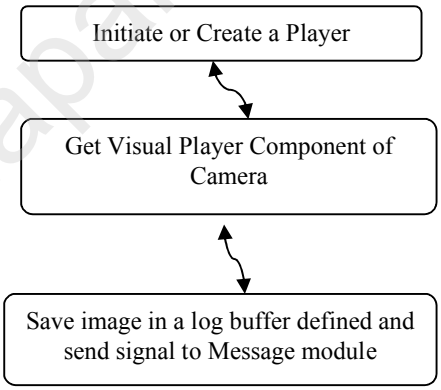

Figure 4.4 Flowchart of the Webcam

Webcam module's job is to just click create a platform ready for take a snapshot and log the photograph of the person trying to enter. What happen is that a player is created to capture the picture of the person next to the door. And when a signal fron the base station is

forwarded to webcam it takes and snapshot logs it and give a signal to the Message module to send alert to administrator.

4.1.2.3 Messaging Module

This is the module which sends the alert to the administrator about the entrance of an individual in the premises if the area which is actually restricted for normal users. Actually, after the photograph is taken, signal is given to the picture SMS module to send the alert to the administrator. For this, APIs for this module from some registered service provider such as clickatell or ValueFirst, is the mandatory requirement. This service provider gives the username and password to pass on internet in addition to the APIs for the process. In this very module, the computer system or device running the application is made web server, using IIS.

4.2 Block Diagram of Sun-SPOT Application Environment

The purpose of the Sun SPOT Base station software is to allow applications running on the Host to interact with applications running on Targets. The physical arrangement is:

Figure 4.5 Physical Structure of SPOT Environment [16].

The Host may support any platform i.e. Windows PC, Mac. The Host application is a J2SE program. The Target application is a Squawk Java program. The Base station runs on different modes.

1. Dedicated mode The Base Station runs within the same Java VM as the host application and can only be used by that application. In this model, the host's address is that of the base station.

2. Shared mode: In shared mode, two Java virtual machines are launched on the host computer: one manages the base station and another runs the host application. In this environment, the host application has its own system-generated address, distinct from that of the base station. Communication between the host application and the target application, takes place over two radio hops, compared to one hop in the dedicated mode [27].

4.3 Steps to Develop and Execute Sun SPOT Application

Building and deploying Sun SPOT applications provides information about how to build, deploy and execute Sun SPOT applications. The Steps may be included in the process are as follows:

1. Create a directory to hold the application and write Java code.

For instance, The default directory *Demos/Code Samples/SunspotApplication Template* contains a very simple Sun SPOT application that can be used as a template to write your own. All the four sub modules using the templates was developed and copy those java files and save as directory at a location in root (E:) directory (Sun SPOT) .

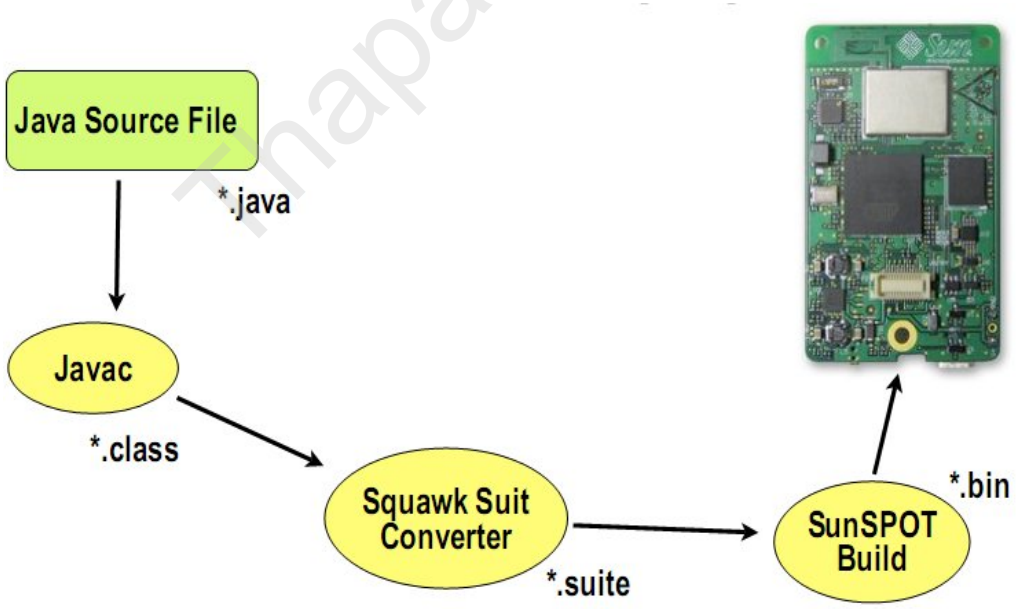

Figure 4.6 Process of deploying Sun SPOT Application [26].

3. Compile the template example and create a jar that contains it by using the " *ant jar-app* " command. For this go to command prompt and type the sommand or use Netbeans and press compile button. The output would be somewhat like the Figure 4.11. The created jar is called *imlet.jar* and is created in the suite folder.

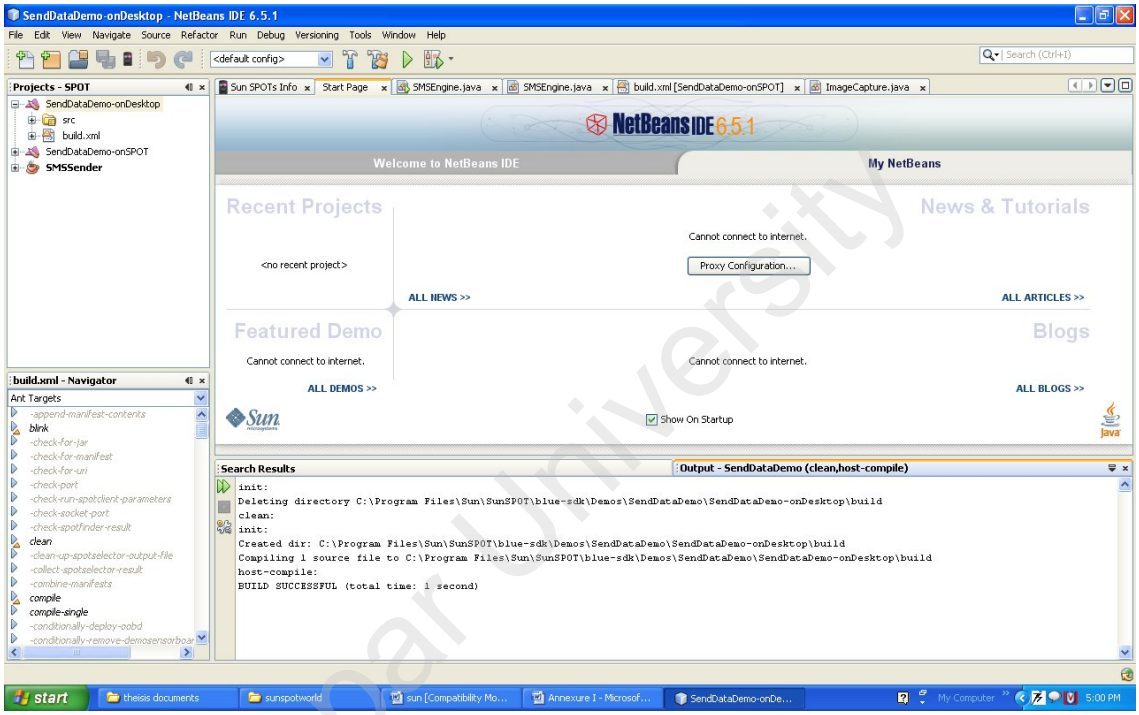

Figure 4.7 Compile and Build of Sun SPOT Remote Client application

4. Connect the Sun SPOT to your desktop machine which is suppose to remote client using a mini-USB cable.

5. Check communication with your Sun SPOT using the "*ant info*" command, which displays information about the device.

6. To deploy the example application, use the "*ant jar-deploy*" *or* "*ant run deploy*" command.

If this step fails, this most likely reason for it could be that, system does not know the location of the JVM. If the issue still continues, we can configure ant variables by using *"ant environment"*.

7. Run the application. To run the application, use the *"ant run"* command.

8. Now connected the base station to the laptop or desktop and similarly compile or build and run the the server application [26].

4.4 Implementation of System

4.4.1 Environment Used

System developed here is actually worked out, keeping in mind the platform independence that is, one of the many reasons for using Sun SPOT devices, java platform, Netbeans, and Apache-Ant. Windows Xp was used because it is easy and user-friendly to work on some new emerging technology, because it has less issues working with the other application and another important reason is that Sun Micro System has provided well documented tutorial to interact with the Sun SPOT using Windows Xp. Language is actually not a major concern because the Sun SPOT's applications are all written in java and SPOT project itself developed itself in **java** at Sun Labs. Netbeans also is written in java to support the java applications. It especially provided in-build integration configuration with the ANT, SDK, SPOT-SDK, and SPOT Manger.

4.4.2 Implementation

AODV runs as the routing protocol on the Sun SPOTs. Different parts in the package com.sun.spot.peripheral.radio.mhrp.aodv are easily available. Javadoc for a good overview or can be checked with AODVManager.getInstance (). AODV works as follows:

1. Send a unicast message every second and output the previous AODV sequence number.
2. Send a broadcast message every second and output the previous AODV sequence number.
3. Register a route event listener and look at what happens you unicast a packet to a known and a non-existing Sun SPOT.

There is another example available at SunSpotworls.com that can be seen to explore more on it"Packet Sniffer".

Certain Sun SPOT SDK's APIs that is included to help in in both client side and base station

```
import com.sun.spot.sensorboard.EDemoBoard
import com.sun.spot.sensorboard.io.IScalarInput;
import com.sun.spot.io.j2me.radiogram.*;
import com.sun.spot.sensorboard.peripheral.*;
import com.sun.spot.util.Utils;
import javax.microedition.io.*;
import javax.microedition.midlet.MIDlet;
import javax.microedition.midlet.MIDletStateChangeException;
```

***Client Side* (Remote Sun-SPOT)**

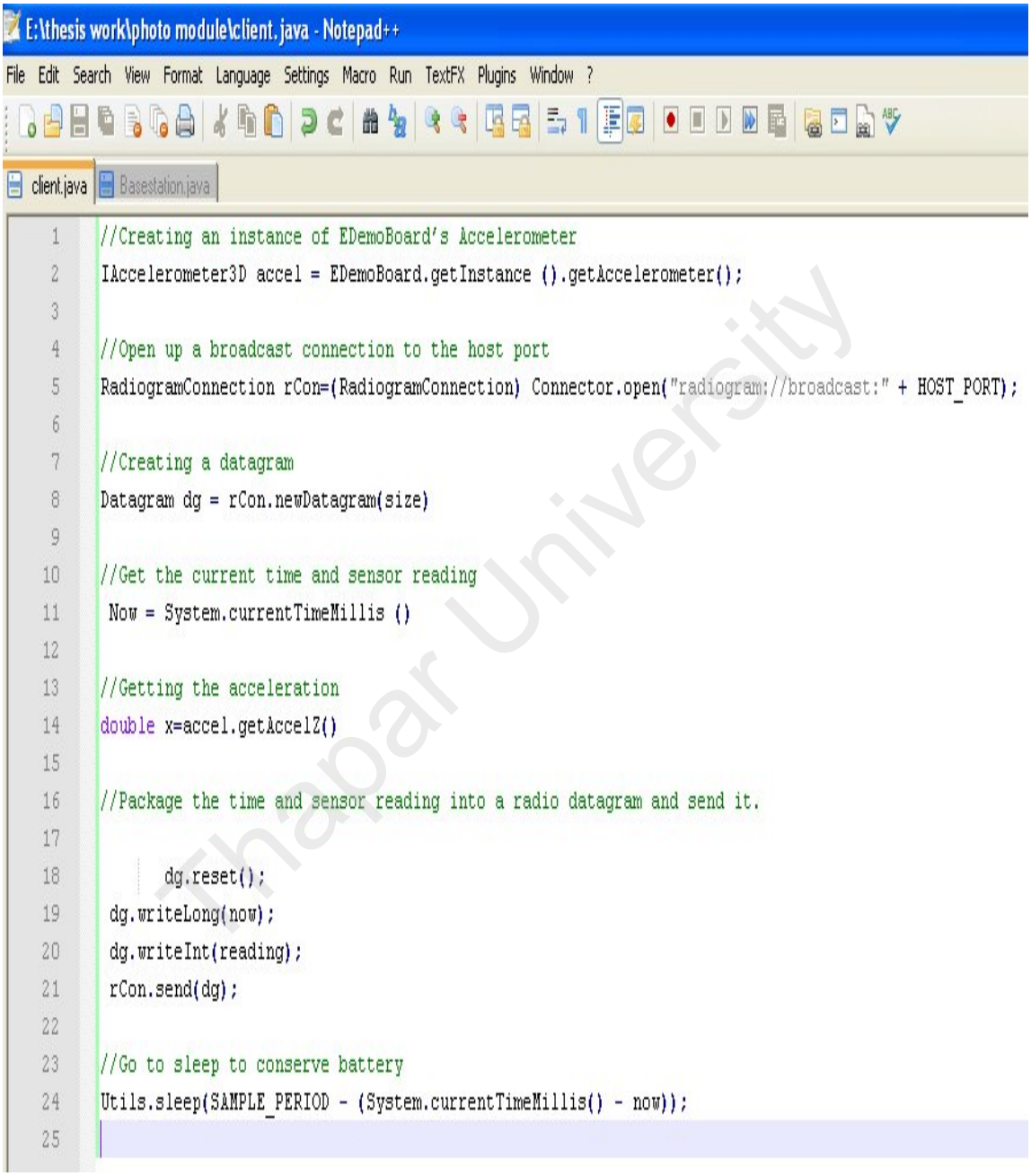

FIGURE4.8:Snapshot Remote Sun SPOT Application

Base Station **(Sun-SPOT)**

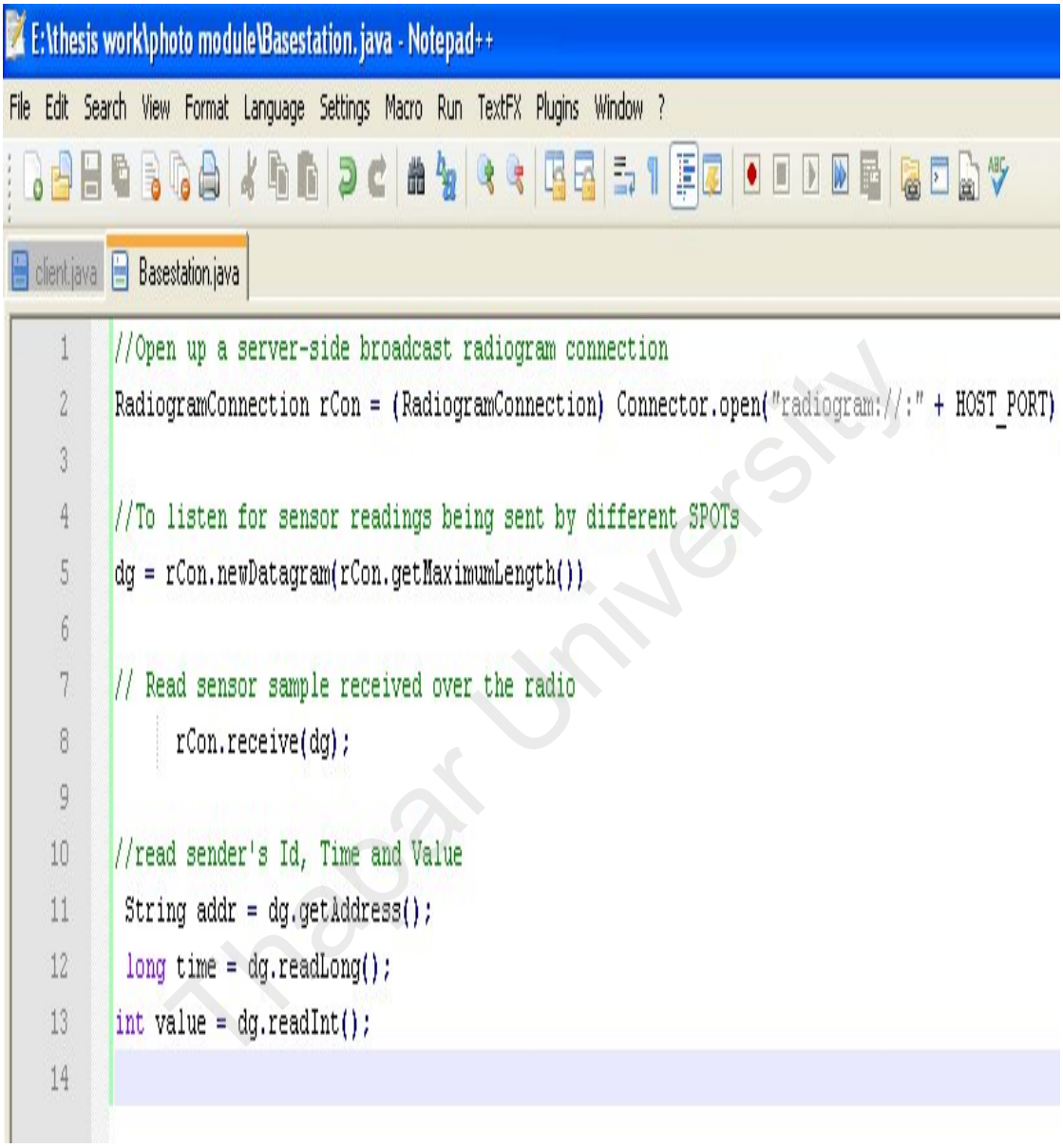

FIGURE4.9:Snapshot:BaseStation Application

Webcam Module

*E:\thesis work\photo module\ImageCapture.java - Notepad++

File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?

client.java Basestation.java ImageCapture.java

```
1  //Getting Camera Device Information
2  CaptureDeviceInfodi = CaptureDeviceManager.getDevice(str2)
3
4  //MediaLocator for Camera
5  MediaLocator ml = di.getLocator()
6
7  //Creating Player and Start Camera Player
8  Player player = Manager.createRealizedPlayer(ml)
9  player.start()
10
11 //Getting Visual Player Component of Camera
12 Component comp = player.getVisualComponent()
13
14 //Grabbing a frame
15 FrameGrabbingControl fgc = (FrameGrabbingControl)player. getControl("javax.media. control.FrameGrabbingControl");
16 buf = fgc.grabFrame()
17
18 //Convert it to an imageBuffer
19 BufferToImage btoi = new BufferToImage ((VideoFormat) buf.getFormat ())
20
21 //Creating Image from Buffer
22 Image img = btoi.createImage(buf)
23
24 //Save image
25 saveJPG(img,"D:\\entered"+Counter+".png")
26
```


FIGURE4.10: SnapShot:Image Capturing Application

Messaging Engine

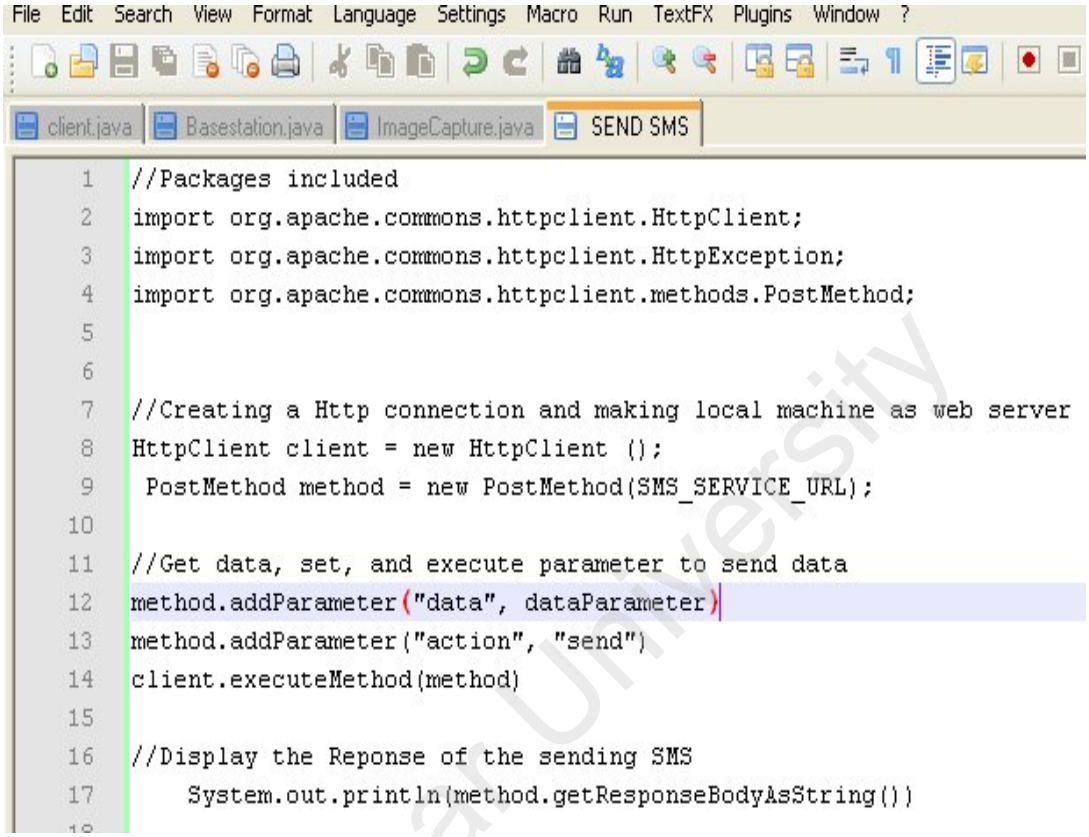

Figure 4.11: Snapshot: Message Alert Application

4.5 Summary of Design and Implementation

In design and implementation, using various Java API, we can easily develop a system of our own choice. That is, one of the main reason why we choose to use java as a programming language for implementing. Although, initially we thought of sending picture message, but later it was restricted to just sending an alert. Work is still on, till it is done by talking to some other service provider.

CONCLUSIONS AND FUTURE WORK

Conclusions

Often Security Experts says "while designing security of a system, it is safe to say that without physical security, you have no security at all". To ensure the efficient security policies, it is important, that people's work areas mesh well with access restrictions.

One of the most interesting observations we made through this project's unique course of research was that how can real time alert can be communicated to the concern, with the combination of mobile technology and the wireless sensor technology. It will help the network manager to decrease, the process of getting the unauthorized physical access of the network area to almost zero. Although it is always recommended or rather a compulsion to have system backups after a short interval of time, in order to avoid any major loss. It also creates graphical logs of any attempts or successful access by any individual and provides notification on real-time basis.

Future Work

Further in this area, system can deliver much more sophisticated system for monitoring of physical access such as movies of 10 sec get saved and forwarded to administrator as a MMS, by taking services from some networking service provider, and calling up the security head on his mobile phone, with location of security breach.

Another very exciting extension can be to have a database of the pictures on server and match the bitmap image and if doesn't match then forward it to administrator. Also, doesn't allow the unauthorized person to enter by enabling a electrical circuit in the area, as is there in militarily intelligence system.

REFERENCES

[1]. Thomas Mathew, *Ethical Hacking (EC-Council Exam 312-50): Student Courseware*, OSB Publisher, ISBN:0972936211.

[2]. ControlScan, *A Guide to The Importance of Keeping Your Company Network Secure,*www.controlscan.com/corp/AGuidetotheImportanceofKeepingyour*CompanysNetworkSecure. pdf.*

[3]. Sanmeet Kaur, Maninder Singh, *Design and Development of Policy Scripts to Detect Network Intrusions Using Bro*, Thesis report, Department of Computer Science and Engineering , Thapar University, 2008, http://172.31.19.13:8080/dspace/handle/10266/548.

[4]. Robert L. Bogue, *Don't Overlook Physical Security on Your Network,* http://articles.techrepublic.com.com/ 5100-10878_11-5034661.html.

[5]. Joel Dubin, *Taking Care About The Physical Security, Little Black Book of Computer Security*, chapter 5, 29 th Street Press, a division of Penton Media, Inc.; 2nd edition.

[6]. Jose A Gutierrez, *On The Use Of IEEE 802.15.4 To Enable Wireless Sensor Networks in Building Automation*, Embedded System and communication Group, Innovation Center, IEEE 15th International Symposium on Personal, Indoor, and Mobile Radio Communications Barcelona, Spain, 5-8 September, 2004.

[7]. esoft, *Mordern Network Security: The Migration to DeepPacket Inspection* , White Paper, 2006, http://www.esoft.com/pdf/whitepaper/DPI_white_paper.pdf.

[8]. Roger Meike, *Sun SPOT Small Java powered Wireless Transducer Devices,* http://research.sun.com/projects/dashboard.php?id=145

[9]. Whatis.com?, *Definitions - Physical security,* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150976,00.html, last updated on December 2005

[10]. *Importance of physical security*, http://netsecurity.about.com/b/2007/11/09/importance-of-physical-security.htm

[11]. cisco.com, *Cisco Certified Network Administrator Tutorials,* Cisco System Inc., http://curriculum.netacad.net/virtuoso/servlet/org.cli.delivery.rendering.servlet.CCServlet/SESSION_ID=1247314204477685,LMS_ID=CNAMS,Theme=ccna3theme,Style=ccna3,Language=en,Version=1,RootID=knet-lcms_exploration3_en_40,Engine=static/CHAPID=null/RLOID=null/RIOID=null/index.html, 2009.

[12].http://www.engadget.com/2008/02/21/cold-boot-disk-encryption-attack-is-hockingly-effective/.

[13]. Weilian Su and Wai Yen Mak, *Sensor Network Architecture For Multi-Media Traffic.,* Military Communications Conference, 2008. MILCOM 2008. IEEE, published on 16-19 Nov. 2008, current version 2009.

[14]. Maxum Development Corporation, *Server Security:How to protect your server from unauthorized use",* www.maxumdev.com/HelpfulInfo/Server%20Security.pdf.

[15]. Sun Microsystems Labs, *Sun SPOT –Owner's Manual, Blue Release 4.0, August 2008,* www.sunspotworld.com/docs/Blue/SunSPOT-OwnersManual.pdf, Sun Microsystems, Inc.,Revision No 1.8.

[16]. Roger Meike, Sun Small Programmable Object Technology (Sun SPOT) "Small Java powered Wireless Transducer Devices" http://research.sun.com/projects/dashboard.php?id=145.

[17]. Sun Microsystems Labs, *A SUN LABS RESEARCH PROJECT "Sun SPOT System" Turning Vision into Reality*, research.sun.com, Sun Microsystems Inc, 2005.

[18]. Wireless Technology comparison, http://www.dpactech.com/docs/evaluation_support/Wireless_Technology_Comparison.pdf

[19]. Mikio Takizawa, *Survey: Wireless Sensor Networking (WSN)*, www.cs.earlham.edu/~takizmi/SeniorSem/Survey_Wireless_Sensor_Networking_WSN_.pdf, Senior Capstone Seminar, 2008.

[20]. Chih-Chieh Han, Ram Kumar, Roy Shea, Eddie Kohler and Mani Srivastava, *A Dynamic Operating System for Sensor Nodes*,3rd International Conference On Mobile Systems, Applications And Services, ACM, pages 163-176 , 2005
.

[21]. Sun Microsystem Labs, *Sun SPOT Programming the Real World*, http://www.sunspotworld.com/vision.html,research.sun.com, Sun Microsystems Inc.

[22]. Cristina Cifuentes , Derek White , Eric Arseneau, *Squawk: A Java VM for Wireless Sensor and Actuator Devices,* JavaOne Conference, May 2006.

[23]. Doug Simon, Cristina Cifuentes, Dave Cleal, John Daniels, Derek White, *Java on the Bare Metal of Wireless Sensor Devices,* ACM, 2nd Conference on Virtual Execution Environments '06, June 14–16.

[24]. David G. Simmons, *Sun SPOTs Small Technology Programmable Object Project Sun ,* www.sensornet.gov/net_ready_workshop/Dave_Simmons_ SUN_SPOTS.pdf.

[25]. Souvik Das Gupta, *Sun Small Programmable Object Technology (Sun SPOT), www.sensornet.gov/net_ready_workshop/Dave_Simmons_SUN_SPOTS.pdf.*

[26]. Sun Microsystem Labs, *Sun SPOT Developer's Guide*, version 2.0, www.sunspotworld.com/docs/Purple/spot-developers-guide.pdf, updated on 16th April 2007.

LIST OF PUBLICATIONS

Gurpal Singh, Maninder Singh, *Real Time System For Monitoring and Graphical Logging of Physical access*, IEEE-TENCON , Singapore, 23-26 November 2009 [status: communicated].

ANNEXURE I

SUN SMALL PROGRAMMABLE OBJECT TECHNOLOGY

Sun SPOT is based on a 32 bit ARM-7 CPU and an 11 channel 2.4GHz radio, SunSPOT radically simplifies the process of developing wireless sensor and transducer applications. The platform use familiar Integrated Development Environments (IDEs), such as Net-Beans TM to write code and enables developers to build wireless transducer applications in Java TM using a sensor board for I/O, an 802.15.4 radio for wireless communication. Some of the applications of SPOT that has been well tested in Sun laboratories are as follows:

Figure I: Sun Small Portable Object Technology

- Debugging tools that allow developers to debug a wireless transducer application as it runs on the device.

- A discovery mechanism that will enable any Sun SPOT operating within the radio field and running a special "meta-isolate" application to report its status even pause and resume applications.

- **"**Migratable application" capabilities that enable applications—with their complete state information—to move from one Sun SPOT device to another while they're still running.Over-the-air (OTA) reprogramming capability for sensor devices deployed in large numbers, or in difficult to access or hostile environments.

- Mesh networking among the Sun SPOT devices in order to use an efficient algorithm for power efficiency and fault-tolerance in the network.

- Developing new architecture for auto-configuration of the sensor network and its global connectivity to the Internet [18].

ANNEXURE II

SUN SPOT SPECIFICATIONS

Hardware Specification

A Sun SPOT system is composed by stacking a Sun SPOT Main Board with other optional boards. It does consist of following parts as soon in the diagram that follows:

Figure II: Main Board, Sensor Board and Test Board

Sun SPOT Main Board	General Purpose Sensor Application Board
Test Board	Serial Battery Board
USB Battery Board	eflash
eserial	eproto.
eprotoMega.	eUSBHost [18].

Software Specification

Squawk Virtual Machine:

- ✓ Fully capable J2ME-level Java VM with OS functionality.
- ✓ Currently 80K RAM for VM.
- ✓ Can execute directly out of flash memory.

- ✓ Libraries 270K flash including most of the Java components of the VM.
- ✓ Device drivers written in Java.

Developers Tools

- ✓ Use standard IDEs. e.g. NetBeans to create Java Code.
- ✓ Simple scripted build and deploy process (Ant based).
- ✓ Simple debugger available .
- ✓ Deployment Options.
    - Wired Serial or USB connection to Battery Board.
    - Wired USB connection to Test Board .
    - Over-The-Air Deployment Of Java Code to Sun SPOT.
    - Sun SPOTs wired via Serial to a computer can act as a base-station
    - Integrates with J2SE Applications.

Standard Libraries

- ✓ CLDC 1.0 libraries.
- ✓ 802.15.4 compliant MAC layers.
- ✓ Hardware and Sensor integration/control libraries.

Squawk Java Virtual Machine

Squawk JVM

The Squawk virtual machine is type of small Java virtual machine (VM) written in Java that runs without an operating system on a wireless sensor platform. Squawk is an open source research virtual machine for the Java language that examines better ways of building

virtual machines. Most commercial virtual machines are written in low level languages such as C and assembler. It is believed that virtual machines can be simplified by writing them in in higher level languages, and further simplified by implementing the VM in the language that the VM is implementing. A Sun Labs software research project into Java on small devices:

1. Fully capable J2ME CLDC 1.1 Java OS
2. Executes directly out of on-board flash memory
3. Complete set of native Java device drivers
4. Automatic power management
5. Bring the ease of Java development to the world of sensors
6. Rapid prototyping, development and deployment of sensor

Squawk translates standard java class file into an internal pre-linked, position independent format that is compact and allows for efficient execution of byte codes that have been placed into a read-only memory. Application isolation also enables Squawk to run multiple applications at once with all immutable state being shared between the applications. Mutable state is not shared. The aggregation of the features reduces the memory footprint of the VM, making it most effective environment for deployment on small devices.

Comparison between JVM and Squawk JVM

Squawk have an integrated wireless API for the IEEE 802.15.4 protocol, which extends on the generic connection framework (GCF) and provides for radio and radiogram connection types. The radiogram permits normal point-to-point communication, as well as broadcasting to multiple listeners.

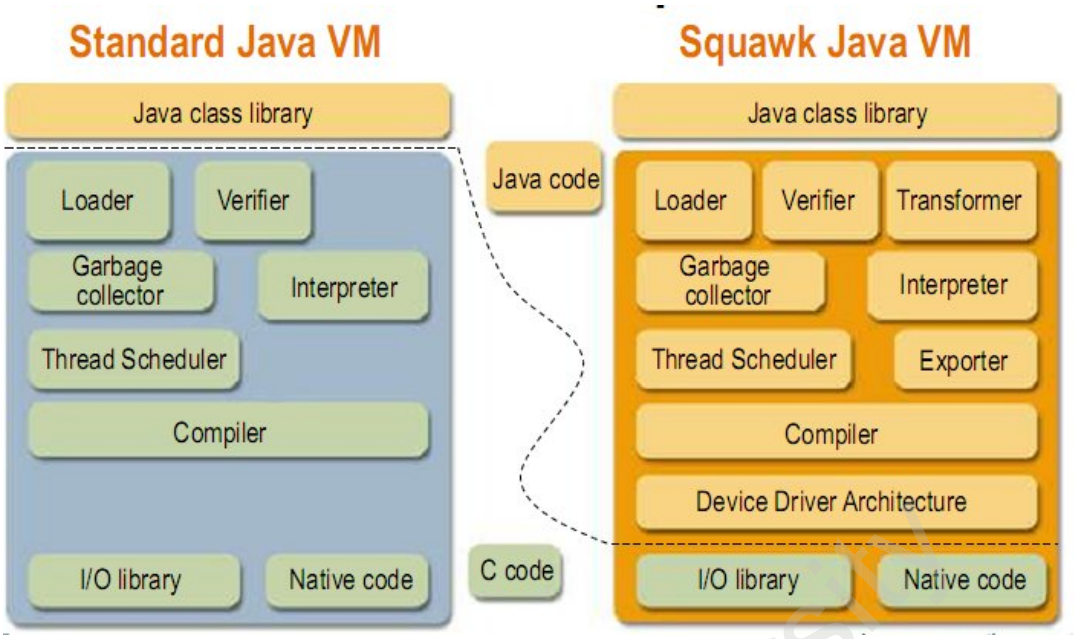

Figure III Comparision between JVM and Squawk JVM

Results from some of the experiences with Squawk JVM (SJVM) show that, even without performance tuning, SJVM performs reasonably well when compared to other interpreted JVMs, even though Squawk is mainly written in Java . Squawk's size is small despite implementing OS-level functionality to run on the bare metal, and the suite fi les it generates are about one third of the size of standard Java class file, as shown in the Figure III [24]. *Squawk Java VM acts as both operating system and software application platform.* Some of the silent features of the Squawk JVM for the wireless networks are as follows:

1. Specially designed for memory constrained devices,
2. Runs on the bare metal on ARM,
3. Isolate application model,
4. Ease of development.

Squawk's Split VM Architecture

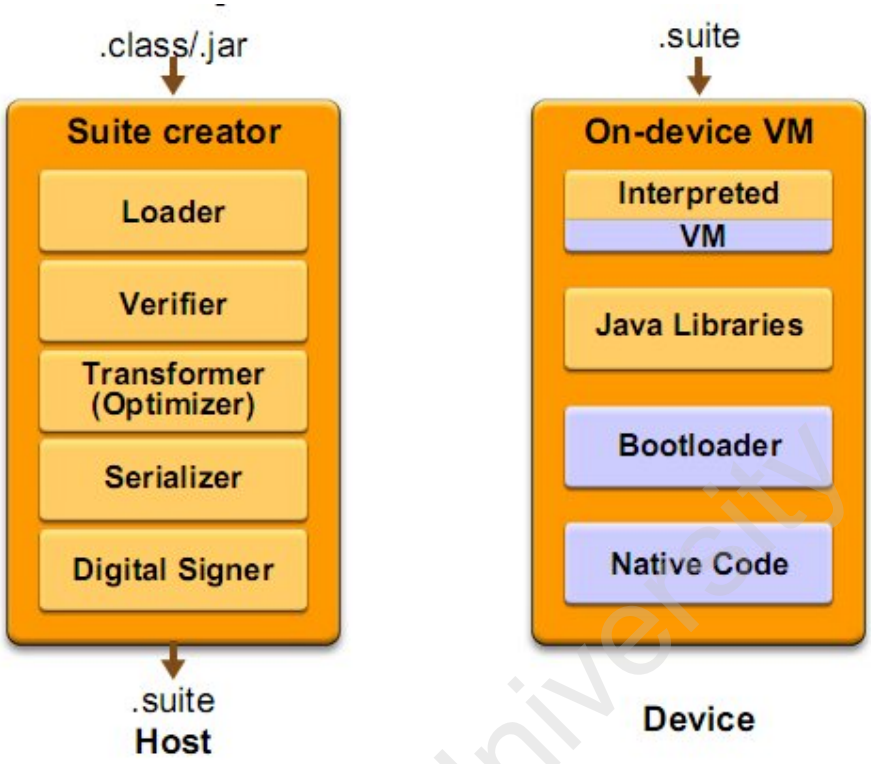

Figure IV Squawk JVM Architecture