Wireless Short Range Communication Technologies for Home Automation

Master’s Thesis in Computer Network Engineering

Oyekunle Abiola Taiwo
Wireless Short Range Communication Technologies for Home Automation

Master Thesis in Computer Network Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

June, 2008
Description of cover page picture/figure: Home Automation Service Diagram by SK Telecom, South Korea
Preface

Oyekunle Abiola Taiwo

University: Halmstad University
Program of Study: Computer Network Engineering
Title of Thesis: Wireless Short Range Communication Technologies for Home Automation
Supervisor: Per Arne Wiberg
Opponent: Björn Nilsson
Examiner: Tony Larsson

Halmstad University, June 2008
Abstract

A modern home contains varieties of electronic equipment and systems like: TV, Hi-fi equipment, central heating systems, fire alarm systems, security alarm systems, lighting systems etc. Enabling these devices to communicate is the first step towards the long-predicted smart home, but this requires communication standards to follow. It can be anticipated that the technology must be wireless in order for such network to be feasible. Large set of standards are present for as well wired as wireless communication in between such devices, but today no standard communication interface available.

The goal of this project is to survey available standards for short-range wireless communication, and to evaluate and compare their capabilities to become a general standard for home automation. The evaluation must take such aspects as security, range, network architecture and the heterogeneous set of devices into consideration. Furthermore, this thesis proposes how to interconnect the home network to the external network for remote supervision and control.
## Contents

**PREFACE** .............................................................................................................................................. 1

**ABSTRACT** ........................................................................................................................................ 3

**CONTENTS** ....................................................................................................................................... 5

1 **INTRODUCTION** ............................................................................................................................. 9

1.1 **APPLICATION AREA AND MOTIVATION** ............................................................................... 9

1.2 **PROBLEM DEFINITION** ............................................................................................................. 9

1.3 **THESIS GOALS AND AIMS** .................................................................................................. 9

2 **BACKGROUND** ............................................................................................................................... 11

2.1 **CHALLENGES WITH WIRELESS MEDIUM FOR HOME AUTOMATION**.............................. 11

2.2 **WIRELESS LINK REQUIREMENTS FOR HOME AUTOMATION** ........................................... 12

3 **APPLICATION AREA OF HOME AUTOMATION** ........................................................................ 16

3.1.1 **FOCUS SUBSYSTEM** .......................................................................................................... 16

3.1.2 **INTEGRATED WHOLE SYSTEM** ......................................................................................... 16

3.1.3 **DISTRIBUTED SYSTEM** ...................................................................................................... 17

3.2 **SECURITY SERVICES** ............................................................................................................. 17

3.3 **ENERGY/UTILITIES** ............................................................................................................... 18

3.4 **COMFORT/HEALTH/SAFETY** ............................................................................................... 18

3.5 **MULTIMEDIA/ENTERTAINMENT** ............................................................................................ 18

3.6 **PROPOSE HOME SECURITY SYSTEM** .................................................................................. 19

3.7 **IDEAL HOME SECURITY SYSTEM** ....................................................................................... 19

3.8 **MAIN SPECIFICATIONS OF SECURITY SYSTEM** ................................................................. 21

4 **WIRELESS TECHNOLOGY** ............................................................................................................... 24

4.1 **ZIGBEE AND HOME SECURITY SYSTEM** ............................................................................. 24

4.1.1 **ZIGBEE SPECIFICATIONS** ................................................................................................. 25

4.1.2 **COMPARISONS OF ZIGBEE WITH OTHER STANDARDS** ................................................ 26

4.2 **BLUETOOTH** ............................................................................................................................ 26

4.3 **NEAR FIELD COMMUNICATION** ............................................................................................. 29

4.4 **ULTRA WIDE BAND** ............................................................................................................... 30

4.5 **RFID** ......................................................................................................................................... 31

4.6 **WLAN** ...................................................................................................................................... 32

4.6.1 **COMPARISONS OF WLAN AND BLUETOOTH** .................................................................. 33

4.7 **EXTERNAL NETWORK** ............................................................................................................. 34
List of Figures

1.1 Diagram of Home Network Scenario by South Korea Telecommunication Company.

2.2 Diagram Showing the Four Classifications of the Security System

4.5 Diagram Showing RFID Tag

4.8 Diagram of a Propose Home Security System Architecture over the Internet

5.1 Zigbee Radio Modules with an Internal Antenna and External Connectors

5.1.21 Mesh Network Topologies Diagram

6.0 Diagram of Zigbee S-o-C Design

6.1.2 Diagram Showing Step-by-Step Usage of Mobile Control Program

List of Tables

3.2 Table Showing Comparison of the Four Classifications of the Security System

3.8.1 Table Comparing the Different Scenario for Home Security System

4.1.1 Table Showing Zigbee Specifications

4.1.2 Comparison of Zigbee with other Wireless Technologies

4.6.1 Comparison of WLAN and Bluetooth
1 Introduction

Modern homes contain varieties of appliances, electronics devices and electrical system. Examples include kitchen appliances like refrigerators, microwave ovens, coffee maker machines, multimedia systems or devices such as televisions, audio systems or CD-players others like lightning systems, heating systems, motorized window blinds and communication devices like telephone - fixed line, internet also alarm security systems etc.

These appliances now have microprocessors embedded in them ranging from computers to coffee-makers and improve capabilities [28, 42]. Enabling these devices to communicate with one another and human is the first step towards the much-anticipated smart home or home automation. Smart Homes simply means real-time local or remote control of home appliances not the introduction of robots. Most important is the communication technology to be deployed in making this a reality. With recent development in microprocessors, ability to communicate is now being embedded in most microprocessor chips or devices couple with the benefit of easy deployment, low cost and power consumptions and their tiny nature [42].

1.1 Application Area and Motivation

The possibility for home automation is real with a huge market but limitation factors like communication technology standard and cost are major hindrances. Analysts have suggested that the huge potential in the home automation industry can be unlocked with focus on Utility/Energy Automation and Security System Automation [6]. Utility Automation is a value-based benefit for controlling the cost of utilities and energy consumption on home devices like stereo, television etc. Security or Safety Automation provides the necessary security and safety to homeowners.

The home security system must be affordable and efficient thus, the need to arrive at a standard communication technology of choice to be deployed universally.

1.2 Problem Studied

The followings areas are addressed in this study:

Communication technology standard media to be deployed for home automation which can either be wired or non-wired:

- Identifying the challenges with choice of media and the requirements for the links
- Introduction and applications of home automation
- A propose home security system; features and requirements specifications
- Identifying available standard wireless technology of choice and evaluations in areas of reliability, range, adaptation and co-existence of links, as wells as cost
- External network and home security system
- Matching of proposed home security system specifications with features of Zigbee
Zigbee as home automation standard and features

How to interconnect the home network to external network

1.3 Thesis Goals and Expected Results

The aim of the thesis work is to survey available standards for short range wireless communication for home security system automation. And, also propose how to interconnect the home network to the external network for remote supervision and control:

1. Discussion on the various applications of home automations technologies.
   - Security
   - Energy/Utilities
   - Comfort/Safety/Health
   - Multimedia/Entertainment

2. Emphasis on home security system application, the various requirements and specifications.

3. Since the network technology of choice is wireless links, survey of available communication standard available and matching these standards with requirements specifications.

4. Propose how to integrate the home security system to the external network for remote supervision and control.
2. Background-Communication Standard

Communication media can either be wired or non-wired that is wireless. Ease of deployment is a major advantage of wireless over wired, the communication media discussed in this project work is wireless. Wireless is most ideal for home automation to realize or make feasible our goals for a smart home. Also there are two options of wireless media, optical medium or radio medium for transmission of signal for communications. Our reasons for deploying wireless medium for home automation are explained below:

- **Flexibilities** Wireless link provides room for flexible set-up, the choice of location of appliances or devices when considering wireless medium is irrelevant, also the two wireless links have some comparative advantage too, optical and radio are the two wireless media with the latter providing flexibility, so there is no need for line-of-sight for sender and receiver to talk unlike optical medium in which an angle range is specified as not more than 30 degree and within a certain range like one meter, for example in a TV remote controlled device. Planning and design, ease of set-up or infrastructure deployment with no special needs for wiring plans unlike the case for cable or wired infrastructure. Emphasis is place on the communication standard technology rather design or set-up.

- **Robustness** Wireless link can survive disasters like earthquakes, fire or social engineering attacks in the forms of destroying the interconnecting cables or wire or simply unplugging cables. So long the wireless devices are intact, communication among appliances is still feasible.

- **Cheaper** the cost, size and power requirements of wireless functions are falling drastically. The radio is 110-years-old couple with microprocessors just under 50-years-old [42]. These two technologies now put on chips. It saves time and cost of wiring or laying cables. Microprocessors with radio functions are now in form of small computer chips with prices falling over the years making it ideal technology for home automation.

- **Scalable** Wireless chips provide room for open network, with more scalability when compared to their wired counterparts. Deploying these technologies for home automation will bring along all the development and benefits associated with computing world in terms of innovation, short-cycle development, low cost, ease of expansion and open infrastructure needed for the future deployment of smart home.

2.1 Challenges with Wireless Medium for Home Automation

- **Proprietary** Wireless communication standard especially for local area network are mostly developed by companies to provide solutions to certain demands, and this technology remains a proprietary solutions. In order to interconnect appliance in home network scenario, the technology must be open, that is, interoperability must be ensured. In that sense companies must make their specification open for easy deployment and interoperability.

- **Quality of Service** Efficiency and optimization of resources can be low when compared to the wired medium in terms of bandwidth usages, reliabilities and real-time demands. Interference is a major challenge with wireless link because of the open nature. For examples, signals sharing the same bandwidth or unintended attacks from other signals like microwave ovens and other signal-emitting electronics devices are easily introduced. Microwave ovens operate at the same free unlicensed frequency range as most wireless local area networks, and personal area networks causing interferences. This problem could be solved by having a good distance between
devices, and is difficult to recommend the specific distance due to different products specifications and designs. In deploying the various wireless schemes within an area, special attention must be paid to the modulation schemes to be deployed by the technology and advanced error correction schemes.

- **Restriction** National bodies, Government and non-government agencies or regulators regulate the operational range of frequencies to minimize interferences this present some challenges with home networks. Most wireless local area networks operate at certain license-free frequency bands, which are not the same world wide.

- **Safety** Our body absorbs small quantities of electromagnetic waves or signals. Nevertheless, it is not very clear the effect of this has on the health of human beings.

### 2.2 Wireless Link Requirements for Home Automation

The various wireless links or standards are classified according to the range in terms of personal area networks, local area network and metropolitan area networks. They have different reasons to exist variations in terms of carrier frequencies, power requirements and data rate with some standards playing dominant roles not because of the technological merits but for ease of deployment of technology.

- **Interoperability** the medium to be deployed for home networks must be open and easy to understand. The technology or specification must be easily available.

- **Global Operation** In terms of the frequency range to be deployed for home network the frequency allocation must be available for use globally.

- **Low Power** Ideally the power consumption must be low and efficient to make it appeal to the customers deploying the technology.

- **License Free** The medium frequencies range must be available worldwide and free for use with minimal interferences.

- **Robustness** the wireless medium must be robust with good error detection and correction schemes, errors due to interferences from the environment. Regarding ease of use, the medium must be customer friendly and easy to deploy and operate.

- **Secure** Consideration must be given to the major weakness of using wireless medium: the technology must have extra security features to monitor attacks. These include features like the unique identifier features of Bluetooth to determine member and secure the network, unique SSID features in wireless local area network another good features to determine a network.

- **Ad hoc** Network infrastructures are easily set-up. This makes it an ideal network infrastructure for home deployments.

Wireless links are either public land mobile network link, PLMN family operated by cellular telecommunication service providers, examples are GSM,CDMA etc or wireless network providers of the IEEE 802 families of standards like Zigbee, Bluetooth, WLAN, UWB, etc. As previously discussed radio links are more suitable for the home network environment or smart home when compare to optical links, it can be argued that optical links also have some features that provide solution to the problems with the use of radio links. Advancements in optical technology specifically infra red ray might provide the needed features for home automation.

**Major Advantages with Optical Links are:**

- The technology is simple to understand and deploy when compared to radio links
- Chips needed for light transmission are cheaper than that of radio chips.
- The links transmit directionally, line-of-sight. The coverage range can be controlled, making it more secure against intruder - an intruder can easily be detected, making the medium safer.
- Unlike the radio links with many technologies sharing a frequency band in a home environment, the optical links is an ideal solution with less of this factor, but signals from other light sources, such as fluorescent, direct sunlight might present some problems.

**Limitations**

IrDA is a point-to-point narrow angle transmission with the problem of Line-of-sight and coverage areas/distance of zero to one meter; at a speed of 9600bps to 16mbps. This limits the application of IrDA wireless technologies. Also, direct sunlight or fluorescent light may create some problems. Standardizations may present challenges, too, when more than one device exists in a room, the problem of mutual interferences may occur.

Diagram by SK Telecom South Korea
3. Application of Home Automation

Home automation provides numerous services to the householder; applications of home automation include Security, Energy or Utilities, Multimedia/Entertainment and Comfort/Health/Safety. Experts believe to unlock the market for home automation security application and utilities provide the key to the huge market [6]. Also the drastic change in the population demographic with more elderly people and the need for social and medical care imposes great pressure on social services and healthcare. The ability to diagnose remotely, to monitor health, to provide a panic facility and to oversee and control appliances from an armchair or remotely, will help to improve safety, comfort and the provisions of health services.

The core technology of home automation is communicating and controlling devices or sensors. Home automation involves technological developments can be categorized into three according to research work by Peter Bergstrom, Kevin Driscoll and John Kimball of Honeywell Laboratories [6]

3.1.1 Focused Subsystem

This entails using local information to automate the performance and control the behaviour of home appliances. A programmable thermostat changes home temperature based on a time schedule. A typical household has more than two remote controllers for home appliances, more than two wired systems, all these different wired systems varied in nature, and they are for different purposes.

Historically, the focus subsystem is the first design of automated homes. The technology is simple to understand and is appliance based; this has being around for some time in most homes in Europe, Japan and United State. Basically they are appliances based and other examples like coffee-making machine with a timer, the electric kettle or gas with timer, multimedia devices like CD player, TV and other home entertainment electronics devices providing such services. These services are provided by manufacturers of home appliances in providing value added services bringing more satisfaction and comfort to consumers. The market for this technology is great and widely accepted by consumers in developing and developed countries of the world.

3.1.2 Integrated Whole-Home Behaviour

Security, comfort, health monitoring, entertainment and information services can be integrated to a whole system and settings can be controlled, based on variable occupant activities rather than fixed time schedule, also there is ease of use when multiple appliances and control devices are networked together. Updating takes a fair amount of effort and involves trips sometimes by service technicians. The integration sometimes requires the effort of technicians for installation and possible repairs. This technological development gives more control and comfort to homeowners. The adoption of this technological development is slow for homes in Europe and America with Japan doing somewhat better, but it is very slow in developing countries. The reason for this is not well understood.

Analysts stated it could be the problem of cost involved in installation and repairs and the problem of a common standard for integration or communication. Since most home automation services in this respect are proprietary solutions the problem of communication standard prevails. For example since it is not feasible to have all your home appliances from a company, the problem is how to integrate these various appliances together to provide the needed services.
3.1.3 Distributed Home Automation

Widespread adoption of the internet, advancement in telecommunication services present a new class of applications using controllable embedded devices – microprocessors with network capabilities, microcontrollers, sensors actuators and network bridges within the home. Upgrading this application is easy and can be tailored to needs of consumers. In the 1990s the computer and communication technology evolution led to industrial and office automation. The same trend is now happening for home applications.

Embedded devices and networking make possible remote control and supervision of home appliances. The question now is whether consumers would accept this? This is answered by asking would not be interested in monitoring conditions of their homes remotely from their mobile devices, phones or PDA, no matter his location.

The challenge with this technological development is greater; it requires a common communication standard for easy deployment, security, flexibilities, scalabilities and defense against such threat as power outage attack, damage to connecting cables and jamming of the wireless links as well as eavesdropping. This is very promising industry for the future and the service is already available in the US and Europe, with South Korea making a giant strides in deploying these services.

3.2 Services

Security Services:

Ideal home security services must be affordable, small, lightweight, and multipurpose with 24-hour, real time monitoring. Home security systems can be categorized based on the techniques deployed to generate alarm as well as to control it [28]. A Passive system, which is manually controlled, but can be monitored remotely, and is the most common system. The homeowners set the alarm when about to leave, if anyone tries to break in, the alarm is activated. The Second system is phone- based System; monitoring and controlling can be done over the public telephone network PSTN. The third is web- based System in which monitoring and controlling are done over the web that is internet and last is a hardware- based system monitoring and controlling are done with configuration changes to the hardware as the case might be [28].

Our goal of idea system is to provide a solution which is easy to deploy, flexible and allows for local and remote security controls and monitoring of homes alerting by SMS to mobile phones in case of danger and dispatch of personnel or security staff, remote controls via internet of digital door locks etc. This is one of the major applications of home automation and consist of various technologies and heterogeneous devices from wire systems to modern-days wireless systems .In this project, we going to consider the various wireless communication standards for security applications and how to interconnect the systems to the internet/GSM for remote control.

Earlier we discussed four classifications of security systems based on the control; the table below and diagram shows briefly a comparison of their features for easy evaluations [28].

<table>
<thead>
<tr>
<th>Performance</th>
<th>Security</th>
<th>Controller</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware based</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>
3.3 Energy/Utility Services

This is value-based added services to provide control of bills or cost for energy or other utilities within the home, remote control of lightning devices, gas heating and cooling system, washing machine and microwave ovens. The rising cost for energy and the need to keep green our environment call for efficient usage of available resources in order to meet these challenges. The deployment of home automation services will provide the necessary means. This application integrates advancement in information technology/digital technology with modern sensors and actuators couple with microcontrollers to provide the needed services.

The home appliances will not only communicate but will cooperate to provide a form of predetermined/programmed behaviour in response to the environment. Imagine a scenario where you are able to remotely turn on your heating system in order to heat up prior to your arrival, or switches. These services will be appliance added services, in the future with energy companies also providing this kind of service to their customers as added value for their loyalty.

3.4 Comfort/Health/ Safety

The application of home automation to provide helps the handicapped, the elderly and able-bodied people as well, putting conveniences into our homes. It comprises the ability to control appliances locally from armchair by speech or pressing of a button, ventilations; air purification systems in keeping your homes at optimum comfort level. In the future, will integrate the introduction of robots, provide services like cleaning, laundry, and care for the handicapped in homes. The remote control and monitoring of situations at home will provide safety and reduce pressure on social and medical services.

With the world population ageing, especially in developed countries of the world, it is expected that the number of people over the age of 65, with disabilities or in need of special care, will double in the next two decades. This is spurring a great interest in the area of how to apply modern technology to achieve the needed solutions. The other services provided by home automation in supporting care services are; teleshopping, home banking, medical monitoring and diagnosis and home information services.

3.5 Multimedia/Entertainment

This application comprises home entertainment services and home communication with information services. Application of home automation to add joy to our homes through entertainment and information, transferring pictures from our computer systems or remotely to digital picture frames within the home, chatting with friends via video telephony etc.

Multimedia applications enabling users to play high-quality multimedia. Data transmitted from outside, such as movies, mp3, HDTV on the audio/video devices, the home users can also retrieve contents inside their home, from outside or playfield. The informative aspects support data exchange, remote information processing, home shopping, e-government, Internet and email and album and file sharing. This will serves as a new business model for
operators of wireless communication, service providers, fixed-line communication service providers, and broadcast service providers in the future.

3.6 A Propose Home Security System

A conventional home security system provides security against burglars. It can detect an intruder, and raise an alarm and contact the police either directly or indirectly with a cost. In some cases, false alarms are raised: this amount to valuable time and money being wasted in terms of police hours, and the need to employ more policemen. In order to avoid the waste of time and money, security companies assume responsibilities of responding to the alarm system, that is leaving the cost of false alarms with the alarm or security system owners. On the other hand, on dispatching of security guards by the security companies to the venues the intruder might have escape. This is a major weakness of the system. The device can only communicate in one direction from the home/office to the security companies, information about the venue is acquired but control of the condition cannot be done remotely. This can be described as passive security system and most common.

Traditionally electronic surveillance consists of cameras, motion detectors etc. , with lots of wires or cable connections which are expensive to install, and when connecting wires or cables the system become inflexible and cost of relocation or reconfiguring become huge. All these shortcomings are overcome by wireless home security system.

3.7 Our ideal security solution or services must have the following features/specifications explained below:

- Multipurpose- Our proposed scheme will be multipurpose, constructed to protect from emergent accidents such as gas leakage and fires. Moreover, the security system must be 24-hour, real-time monitoring of events and conditions with supervision capabilities.
- The integration of other functionalities, from the traditional intruder detection function to home control functions. Our proposed system must incorporate these two functionalities to make it more effective.
- The system must be able to control home appliances as well as monitoring to prevent disaster, making the security system smarter.
- Also, apart from smarter systems we must be able to have 24-hour, real time monitoring of events. The householder should, irrespective of its location of the property, be able to monitor and supervise conditions at his or her home. To ensure this, we make use of recent advancements in information technology, the use of mobile devices like palmtops, mobile phones and PDA to control and monitor events at home locally, or remotely over the internet and over GSM, making it more user-friendly.
- The system can be described as phone and web-based system, ensuring the control and monitoring of events locally and remotely, it must be bi-directional communication that will deploy two-way communication technology techniques.
- Affordable with low cost of installation and maintenance- The proposed security system must be affordable, with a low cost of installation and maintenance, that in turn means the technology to be adopted for the system must have these features. Different security companies have various designs; with the various systems exhibiting these features instead of the traditional system of deploying or running fixed wire cable for the entire buildings. Wireless schemes are being deployed to reduce the cost of installation along with wired schemes. Even in cases where the wired alarm system is cheaper to deploy
compared to the wireless scheme the cost associated with the installation can be overwhelming, and more importantly, is the cost of maintenance. The wired link will incur higher costs than the wireless scheme and the technology for the wireless link is becoming cheaper and available. Increased in processing power and computational capabilities of sensory nodes allow for more complex applications and network protocols.

- Efficient to Manage and Deploy- The proposed security system must be easy to manage and deploy. New modern systems are deployed by simple installation of CCD camera, detection units or sensor units with a control unit which coordinates or supervises the local home network, which is sometimes referred to home controller gateway, or local home network, and a modem for external connection or remote connection.

- The security guard work of monitoring the conditions of environment is simplified with handheld devices able to access the security system configurations. The guard can see from the device the state of the security, and can make changes to the system by simply altering the configurations from its handheld devices; it saves time and space, and it does not need to be at a control terminal before changes are made.

- User Interface- The user interface must be simple to understand and operate by the customers with ease of changing the setting or configurations to suit the customers’ needs. This comprises the software and hardware sections. The software section can be manipulated to change settings of the hardware to suit the needs of the customers. It must be able to work with standard mobile phones keeping in mind the smallness of mobile devices and limited power source and low number of keys .The internet information services for mobile devices uses XML because it is platform independent and easy to deploy.

- Image Monitoring and Scalabilities- The system must provide image-monitoring activities over the Internet and mobile phones with high extensibilities or scalabilities.

- It will render internet protocol connection service, cellular phone that has email functionalities and web browsing functionalities can be used also to see images of an intruder and conditions of the homes .This can assist in investigations and identifying the identities of the intruder. Also provide real-time image of the intruder to the security guard or police alike for quick respond and arrest. The traditional security system deploys by running cable, but it has constraint with scalabilities. To add a new device or functionalities means a total redesign of the entire system, at a cost, and this looks cumbersome to engineer. In some cases, where you are dealing with a large area or security system for a big homes, corporation or organization alike the cost of expanding might be at the same cost of installing a new security system economically.

- Low Power Consumption, Reliable and Secure System.-The alarm or home security system power consumption must be low and it should be robust enough to function reliably. As for the wired link part, this must provides some security against attack on the connecting wire or cables from being vandalized and from eavesdropping. Also, for the wireless link, there is the problem of jamming, making communication impossible among devices and eavesdropping also protection against interferences of all kinds affecting the smooth two-way communication system. The power consumption must be economical since, in some cases, the devices are battery-powered. The reliability of the system is also important for a good system. Imagine a scenario where the power source is being destroyed or cut-off, it must provide services in this scenario, alerting householders.
3.8 The Main Specifications:

- It must be a wireless sensor network, with features like low cost, low power consumption, small in size, easy deployment, a programmable, ad-hoc system, and reliable.

- It will be an open system, standard with capabilities to send and receive data over the internet/cellular network {that is, a two-way communication or bi-directional}.

- There will be a sensor, with capabilities to communicate with a central home server in the home or within the buildings to acquire the condition and control and, with supervision, by the central home server /coordinator of sensors units

- The central home server consists of the internal server, the main control program and a database making up for the home server

- The home gateway and modem should allow access to the external network; conversion of analog signals to digital and vice versa and to allow the usage of GSM, should in case the Internet is not available. This serves as modem to the home local network.

- The detection or sensor unit consists of a module serving as transceiver node and another module as microcontroller module for control of appliances.

- The user can browse condition using the web, and use of GSM where the Internet is not available. Mobile phones, or devices with web capabilities, are used for remote control of appliances.

- The user would be informed promptly if there is an intruder. Not only the user will be able to have remote access to his homes and facilities, he will be able to remotely control appliances enjoy home function technology.

- In the nearest future, the user will be able to view images of the intruder over the web, and possibly a video of events at that time of intrusion. This also makes the system more efficient and smarter. The uses of digital door lock over the initial conventional door lock provide the platform for some functions such as local and remote monitoring and controlling of home security system/devices.

- The digital door lock becomes cheaper and smarter, providing more convenience to customers, more affordability, and with the necessary sensor technology platform for some other applications. The integration of technologies like sensor, digital door lock, wireless communication technologies as well as wired communication, web server, home controller and network hub, will provide an intelligent door lock system.

- Engineers and scientists alike must arise at a standard communication technology for home automation for easy deployment.

3.8.1 Scenario for Home Security System

<table>
<thead>
<tr>
<th>Scenario Characteristics</th>
<th>Via Home Server</th>
<th>via Service Provider</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect to the server which communicates via appropriate interfaces with controllable devices and returns information two-way</td>
<td>Connect to a Service provider which connects directly with appliances/facility control buses</td>
<td>Combination of two scenarios</td>
<td></td>
</tr>
<tr>
<td>Advantages</td>
<td>Home server provide other functionality like multimedia</td>
<td>Offered as professional service</td>
<td>Many options to integrate devices</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>System remains under control of the user issues like privacy and security</td>
<td>Bundling of efforts and devices lower power consumption and more efficient</td>
<td>System provider can offer advice on installation and maintenance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disadvantages</th>
<th>Home server is an additional device, with more power consumption and maintenance</th>
<th>Devices require external interface, like PBX, that can be configured remotely over ISDN or integrated network port</th>
<th>Complexity of overall system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>More user know-how necessary</td>
<td>High complexity of the devices in terms cost maintenance.</td>
<td></td>
</tr>
</tbody>
</table>

The next discussion surveys available standards for short range and long range communication technologies for home automation with emphasis on the security system applications. We evaluate and compare their capabilities in areas like security, range, network architectures and heterogeneous devices. The list of technologies available for short range wireless communication, remote control and monitoring are Wi-Fi, Bluetooth, Zigbee, Uwb, Dect, RFID, NFC, WiMax, 3GP. Others like Rubee, Wibree and Z-wave.
1. Wireless Technology

Recently, the popularity of wireless technologies can be seen everywhere in the form of cellular networks, wireless local area network and wireless personal area network. Devices are increasingly being equipped with microprocessors with wireless capabilities and with cost, complexity, power consumption and size of network-enabled devices are becoming cheaper and available. Many new applications are available: more portable devices, equipped with network-enabled devices ranging from small portable computing devices to coffee-making machine.

The various wireless technologies can be integrated in a transparent manner. This opens the door for many diverse applications of wireless technologies. Home automation is one of the many diverse applications of wireless technologies. The wireless technologies can be classified into three, according to the design objectives or coverage areas, wireless personal area network for small area network like body area etc, wireless local area network designed to cover more area or expanded range and, lastly, wireless cellular area network for metropolitan area networks.

We start our discussion with wireless personal area network technologies for home security system applications. The major technologies to be considered are the IEEE 802 family of standards. The PHY and MAC layers are defined by IEEE for the various wireless technologies for short range transmission while alliances of companies have developed specifications covering the network, security and application layer profile for commercial reasons.

4.1 Zigbee and Home Security System

Overview

It is a personal area standard network with low-cost, low-data rate, low-power consumption, and small volume: it is scalable, reliable, easily deployed, operating on a license- free, globally available frequency band and two-way communication standard. It is specifically designed for wireless sensor networks for machine-to-machine communication.

A key enabling standard for wireless sensor networks is Zigbee with recent release of the standard, the technology evolved from its early sensors with proprietary routing algorithm and radio frequencies technology to standard based networking and radio frequency technology leading to deployment in vast areas like home automation, building automation, utility metering and a host of others domestic, industrial and health applications.

Technology

The standardization of Zigbee defines both the physical and Mac layer, and is referred to as IEEE802.15.4. The physical layer supports three radio bands, 2.4GHz ISM band worldwide with 16 channels, 915MHz ISM band for America with 10 channels and 868MHz and 433MHz for Europe with single channel with also varied data rate according to the frequency band specifications, for 2.4GHz the data rate is 250 kbps, 915 MHz the data rate is 40 Kbps and 868MHz with data rate of 20 Kbps.

The coverage area is 1 to 100 meters and can easily be expanded due to multihop technology and, theoretically, can support 65,536 nodes. This makes it the ideal technologies for home automation and security applications at home. The transmission is based on DSSS direct sequence spread spectrum scheme using the binary phase shift keying modulation scheme. For security, Zigbee uses 128-bit, advanced encryption standard cryptography. The MAC
layer medium access control layer controls the access to the radio channels using carrier sense multiple access scheme with collision avoidance, which can be slotted or un-slotted carrier sense multiple access.

4.1.1. Zigbee Specifications 802.15.4

<table>
<thead>
<tr>
<th></th>
<th>868MHz</th>
<th>902-928 MHz</th>
<th>2.450GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Rate</td>
<td>20kbps</td>
<td>40kbps</td>
<td>250kbps</td>
</tr>
<tr>
<td>Channels</td>
<td>1</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>Receiver Sensitivity</td>
<td>-92dBm</td>
<td>-92dBm</td>
<td>-85dBm</td>
</tr>
<tr>
<td>Link Budget</td>
<td>89dB</td>
<td>89dB</td>
<td>82dB</td>
</tr>
<tr>
<td>Adjacent Channel Rejection</td>
<td>30dB</td>
<td>30dB</td>
<td>30dB</td>
</tr>
</tbody>
</table>

Zigbee defines two types of device, full function device FFD, and reduced function device, RFD, the reduced function device is used for simple applications such as light switches, little amount of data and minimal resources needed while the full function device used for complex network serving as PAN personal area network coordinator or coordinator and also regular device.

The network topologies are star, peer to peer and cluster tree network, the star network all devices can only communicates via a coordinator either as PAN coordinator or just coordinator serving as central office. The coordinator initiates, perform routing operations, and terminates the connections, and can be found in home automation scenario. Peer-to-Peer Network is used for large scale, more complex, networks and, finally, the cluster tree networks with routers that make routing decisions using hierarchical routing algorithms.

The data transmission mechanism between Zigbee devices are either from a coordinator to a device or from a device to a coordinator between two peer devices, it also depends on whether the transmission supports beacon or not. In a non-beacon transmission environment we simply use the un-slotted CSM/CA. For a beacon environment, the device listens first to the network beacon and acts at the right time, using slotted CSMA/CA, or by synchronizing with other nodes so that power can be saved.

### Zigbee Network in Home Security Automation Environment

**Reliability**

The Zigbee mesh network environment is implemented with routing functions with most suitable routes followed, in a scenario where some problems occur with a particular route, let say node- A route, a new route via node B will be discovered automatically keeping the system alive. This feature makes application of Zigbee to home security or home automation secured and reliable.

**Latency**

Real time performances for wireless communications need to consider the latency. For Zigbee network, the latency depends on the number of hops. For a single hop network, the latency is very low dozens of milliseconds but in a multihop network the latency is proportional to the number of hops though the latency times are not specified by IEEE or Zigbee.
Distance/Range

1MW 0dBm output radio power is available from a built -in amplifier of a commercial chip of the coverage area can be increased easily, using multihop techniques to extend without significant changes to the radio power. The time for set up of a multihop network is not specified by IEEE.

Adaptation/Co-existence

The frequency band of Zigbee is widely shared by other wireless technologies, WLAN and WPAN technologies. The question of whether this affects the performance of Zigbee arises with the coexistence of other WLAN and WPAN applications and the system suffers from interferences. Zigbee uses dynamic frequency selection/adaptive scheme and transmission power control to solve the problem of co-existence with other technologies sharing the same frequency band.

4.1.2 Comparison of Zigbee Standard with other well know Wireless Technologies Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Zigbee 802.15.4</th>
<th>Bluetooth 802.15.1</th>
<th>Wi-Fi 802.11b,g,a</th>
<th>GPRS/GSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Monitor and control sensor</td>
<td>Cable Replacement</td>
<td>Web, Video, Email, Voice</td>
<td>WAN Voice and Data</td>
</tr>
<tr>
<td>Battery</td>
<td>100-1000 30mA</td>
<td>1-7 40mA</td>
<td>0.1-5 400 mA</td>
<td>1-7</td>
</tr>
<tr>
<td>Nodes Per Network</td>
<td>Over 65,000nodes</td>
<td>7</td>
<td>30</td>
<td>1000plus</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>20-250kbps</td>
<td>3Mbps B.T 2.1 EDR</td>
<td>56Mbps</td>
<td>16Mbps</td>
</tr>
<tr>
<td>Key Attributes</td>
<td>Reliable Low Power Low Cost Effective</td>
<td>Low Cost Effective</td>
<td>Speed Reliable</td>
<td>Reach More Quality</td>
</tr>
</tbody>
</table>

4.2 Bluetooth-Overview

Bluetooth is for personal area networks like Zigbee but with more data rate and for voice and data applications. Therefore it consumes more power when compared to Zigbee also an idea choice for home automation-security solutions.

Bluetooth technology was named after Harald Blatand, a tenth- century king Danish Viking king, who unified Denmark and Norway. The name was adopted because Bluetooth technology unifies the telecommunications and computing industries. Bluetooth provides low cost, low power, short –range radio technology, flexibility, Robustness, in data and voice applications. Bluetooth was developed by Ericsson Mobile Communications to provide cable-free connection between mobile phones and accessories. Recently, the application of the technology has extended beyond computer and mobile, and towards industrial, home and
health applications. In 1998, four years after Bluetooth special interest group was formed consisting of leading companies like Intel, IBM, Nokia, Toshiba and others. The radio frequency specifications are for point-to-point communications as well as point-to-multipoint connections, with a range of 10 to 100 meters, depending on the device class of power output for class 1 the radio power output is 100mW, and with coverage of 100meters. Class 2 2.5mW and class3 with power output of 1mW and 0.dBm and covers a maximum of 30feet, i.e. about 10meters.

The ad hoc network connections is one of the major strengths of Bluetooth for home automation coupled with data and voice applications, though the problem with ad hoc networks, like the absence of a centralized server, creates challenges with channel access and routing schemes, which are all addressed at the MAC layer of the protocol architecture.

Technology

Bluetooth physical layer operates at license-free, globally available, bands of 2.4GHZ to 2.483GHz band. In the USA and Europe, due to non-availabilities of the 2.4 band, the 2.483 band is used. The frequency band is shared by many other wireless applications. To avoid interferences, Bluetooth employs a fast hopping spread spectrum scheme coupled with additional error correction scheme, short data packets and adaptive power control. Specifications of the radio frequency were relaxed to facilitate low cost and low power design and the modulation employs Gaussian frequency shift keying modulation scheme GFSK. The Frequency hopping sequences also provide resistance to multipath effects and provide a forum for multiple accesses among co-located devices in different piconet. It is worth nothing that negative effect of humidity, gravitational forces, vibrations and dirt are not noticeable.

The latest Bluetooth specification called the enhanced data rate mode increases the data rate from traditional 1mb/s to the modern 3mb/s because of the increasing need for multimedia applications. The frequency hopping scheme divides the frequency band into a number of hop channels, let us say 79 hop channels In most cases a carrier spacing of 1MHz with up to 80 different frequencies channels is available, and 23 hop channels where the frequency band is not readily available. In Europe and America, during a connection, the transceivers hop from one channel to another is pseudorandom fashion with a group of devices sharing a common channel. The channels determine the hopping sequence; the master is the major determinant and also determines the channel access. The same hopping sequence is shared among all devices in the same Pico net with hope rate of 1600hops per second, so that each physical channel is occupied for a duration of 0.625ms referred to as the time slot, time division duplex protocol TDD employ for the scheme, the master allocates the time using polling protocols. A master is any device that first initiates a connection and it can be any device in the connections.

Bluetooth provides symmetric circuit switching and asymmetric packet switching or synchronous connection oriented and asynchronous connections. The latter provide a point-to-multipoint connection between master and slaves. It employs a broadcast scheme and best effort service protocol, while earlier synchronous connection oriented allocates a fixed bandwidth involving a master and a slave.

B-WPAN is a Bluetooth wireless personal area network consisting of Pico nets called scatter nets, while a Pico net consists of a master and seven slaves. A device in one Pico net may exist as part of another network, either as a device or a master. The protocol involves inquiry, paging and scanning before connection and then transmitting and receiving after connections.
Every Bluetooth has its own unique address consisting of a 48bit address preset by the manufacturers when it participates in a network; it a network. It is given a new logical address which is temporary. The physical layer consists of a radio and baseband layer. The baseband Layer is for connection establishing connections, within a Pico net, addressing, packet format timing and power control

**Bluetooth OSI reference model**

Application Layer = Application  
Presentation Layer = RFCOMM/SDP  
Session Layer = L2CAP  
Transport Layer = HCI  
Network Layer = Link Manager  
Data Layer = Link Controller  
Physical Layer = Baseband and Radius

We already discussed the physical layer, the data -link layer is for transmission, framing, and error control over a link for carrying out link level operations in response to higher level commands. The link manager protocols are responsible for link setup between devices and ongoing link establishment and management. The logical link control and adaptation protocols, for adapting upper layer protocols to the baseband connectionless and connection oriented. While the service discovery protocols use for device information, services and characteristics, and the RFCOMM serving as cable replacement portal included in the specification, it is a virtual serial port designed to make cable replacement technologies transparent. And lastly the application layer if for transfer of files, documents, directories, streaming media format.

ULP ultra low power Bluetooth, with features similar to Zigbee technology, is an existing platform and widely accepted technology with over 2 billion chips shipped worldwide, according to Mike Foley Executive Director of Bluetooth organization. The technology is being deployed in most gadgets, ranging from mobile phones to wrist watch, and is definitely an ideal choice for home automation.

**Bluetooth Network in Home Security Automation Environment**

Bluetooth security

Is an acknowledged standard worldwide with low cost, ad hoc nature with a good security system an encryption key of 8-128 bit in the code with a unique number for identifications which eliminates problems of unidentified microwave radio or other technologies operating in the same band within the home.

Range

Depending on the power output class, the distance covered varies from 0 to 100meters and can be enhanced with more radio power, as the case might be, also the ability to co -exist with other Pico nets in the same area also enhances the coverage areas. Notes if more than one Pico net device exists within each others range, they will interfere, but only when the same frequency hop channels occur in the two Pico nets. With 79 available hop sequences to be used the chance of occurrences is relatively small.
Adaptation/Co-existence

The hopping sequence scheme, coupled with short data packets, advanced error correction protocols, provides resistances to the noisy environments of shared network infrastructure within a home. Also, with a reduce radio power output just like the case with Zigbee, the chances of interferences will be reduced.

Reliability and Latency

The Bluetooth link controller detects new devices within range and easily forms a link with them, and with the error correction schemes, to correct errors and retransmission of data. To account for lost data packets, the issues of latency as parameters, also other important parameters, classified into two – communication latency time taken to deliver a data through a network and connection latency time taken to discover and connect a device. Though Bluetooth data rate of 1mbs, 625 microseconds slices hurt throughput, it provides advantage of resistant to interferences, since any given packets can quickly be retransmitted at a given frequencies.

4.3 Near Field Communication

Near Field Communication is a short-range bi-directional wireless communication standard. It allows contact less communication between devices in close proximity. Ultra low power Bluetooth called Wibree, RFID and NFC, shows similarities in their flexibility, ease of deployments, and standard for wireless communication, instead of the radiation interception pattern for communication in use for far field and near field communication. The near field communication adopts coupling magnetic field in the near field wireless communication. A shorter transmission range and lower data rate distinguish NFC from other similar technology standard and its application in mobile phone usages as contactless payment card for commerce, its application found in ticket sales facilities and in office and home automation as security smart card for access control into computer and facilities.

Near Field Communication, jointly developed by Philips and Sony in 2002 for contact less communication, and was in December 2003 was adopted as a standard by IEEE and ISO international standard organizations as a standard for wireless communication in short range. In 2004 a consortium for promoting the technology was founded consisting of mobile phones makers and consumer electronics manufacturers like Philips, Sony, Nokia and credit and debit card companies, and the likes. The contact less solutions provided by NFC is raising universal hopes for diverse applications. Due to slow availabilities of devices with NFC enabled devices, a separate accessory called NFC interface was developed; this also provides a solution better than the traditional NFC enabled devices, and with more added functionalities and as interface.

Technology

The technology operates at very low frequencies band of 13.56MHz spectrum; it allows point to point communication between devices with a maximum range of 20cm, serving as the major limitations for the adoption of the technology. Communication is based on inductive coupling and with a very slow data rate within the range of 106,212 and 424 kbps, which is considerably low when compared to RFID, IrDA and Wibree – ultra – low power Bluetooth. When a device gets close enough to contact the near field, the magnetic inductive coupling transmission energy and data from one device is transferred to another device. There are two types of device in near field communication, internal powered devices, which are called the active devices, and a device with no internal power source, such as a smart card (Which is
referred to as passive), Inductive coupling causes the passive device to absorb energy from an active device on getting close and, once powered up, exchange of data will now occur.

The components are easy to implement on a chip, which means an easy time for the vendor in adoption of the technology, the magnetic inductive coupling can be easily done on a silicon chip, while other components, like the RF-level detector, can be tuned in easily to recognize the 13.56MHz signals and also identify the presence of near field communication radio field. Near field communication requires close proximity, with intercepting made difficult, and so eliminating the need for purchaser to give his credit card to a merchant reducing fraud considerably

**Near Field communication in Home Security Automation Environment**

Reliability

It provides a reliable two-way communication among devices. Once devices are in close contact, the radio frequency can contact any near field enabled devices. The device battery life is longer, or it is sometimes a battery-less wireless sensor application.

Ad hoc and ease of use/co-existence

It is easy to use, with less complex technology, when compared to Bluetooth and Zigbee technology, and can co-exist with other technology within a given area with no significant interferences, the weak signals by very low power source and a shorter area of transmission and lower bit rate, makes is less susceptible to interferences from other short range standards.

Latency

In real time performance applications the latency of the technology proves to be outstanding. The set up latency, as a measure throughput, is typically in some hundreds of milliseconds.

Distance/Range

The distance, or coverage, is at a maximum of 20cm. This is the major limitations for the technology for the use in home automation scenario. The technology does not suit devices that require online connectivity, and connectivity to other devices, or to a fixed access point, it has shorter range and lower bit rate.

### 4.4 Ultra Wide Band

Ultra Wide Band provides high-speed, short range wireless communication with very low power consumption, making it an ideal solution for multimedia applications. For example, video streaming requires a high bandwidth with high power to be transmitted. The other available short range wireless standards, like Bluetooth and Wi-Fi, seem not to be working, with features of low power consumption and high data rate in the range between 100mbps to 480mbps. The technology provides the perfect solutions, though faced with the major weakness of small coverage area of 10meters. The lack of unified standard has been a major hindrance to the adoption of this technology in that there are two approaches and with the two approaches simply not compatible.

Technology

UWB is a radio wave technology that can be embedded in chips, and the modulated signals spread signals across multiple frequencies the ultra wide spectrum in the U.S., according to the IEEE 802.15.3a, is between 3.1 to 10GHz. Since the transmission is across multiple frequencies, it causes interferences with other signals like WLAN etc this makes the standard
difficult to operate for commercial applications for a long time. Nowadays engineers and scientist alike have come out with a solution to curtail the band mast by specifying the specific band spectrum, the short impulsive waveform, rather than the normal continuous waveforms, creates the magic: it gives UWB technology, at the physical layer enhanced capability to penetrate walls, high precision range, support for high data rates and high capacity by spreading bandwidth over very large frequencies overcoming some of the problem with narrowband like limited bandwidth, multipath fading and high susceptibility to interferences. Also the maximum range is small, 10 meters, that is a personal area network in the group of Bluetooth and NFC, but provides a higher data rate at very low power consumption. Contrary to that, an advanced Bluetooth technology which also provides high data rate, similar to UWB, has being developed. Low power consumption with little processing power, with the low processing power presenting some challenges with security of the technology.

**UWB in Home Security Automation Environment**

**Reliability**

The standard is not widely deployed because of the issues of standardizations, but proves to be reliable because of the lower transmission range, maximum of 10 meters, with high signals power to penetrate walls, immunity to interference and immunity to multipath fading, providing a reliable transmission between devices but weak security solutions. The technology power consumption is quite low and it has high data rates.

**Ad hoc/co-existence**

This is a major drawback to the technology: it interferes with signals from other standards and also employs adaptive frequency hopping schemes, like in Bluetooth to avoid channel collision. The problem of jamming can be solved by specifying a frequency band mast for modulation and transmission. It uses the 3.1-10.6 GHZ, unapproved and jammed 802.15.3a standard of which the two spreading techniques, DS-UWB and MB-OFDM, are available.

**Range**

The range is extremely small, a maximum of 10 meters, with possibility of an increase in the future to provide more services away from computers and phone accessories.

### 4.5 Radio Frequency Identifier RFID

Radio Frequency Identifier RFID uses can be dated back to Second World War 2. It serves as a replacement for the bar codes system by using a tag that contains transponders that emit messages and can be read from a distance to identify an object. It does not need line-of-sights and can work perfectly in harsh environments. Information can be stored and read from a tag and it works in harsh environments. Information can be stored and read from a tag. It consists of integrated circuits equipped with a radio antenna, which can be deployed in home automation to improve quality of life. Imagine a scenario where book shelves, refrigerator, house key, microwave and washing machine are all RFID reader-enabled appliances/devices. In line with that, they can list out items for example; the refrigerator can list out items or purchase items that are of RFID tags on an embedded display screen with information like expiry date, manufacturing date etc.

**Technology**
Different vendors operate using different MAC protocol, medium access control in their RFID protocols. Mostly custom-made, they are not interoperable. To solve this, vendors are now developing middleware that will help link new RFID into existing back-end infrastructures helping with the current lack of standard. RFID operates as passive, active or semi-active based on the power source. Passive RFID are powered by the radio field of the reader device, the power of the incoming signals from the reader to read out desired data from memory, and send it back to the reader after processing, with a distance no more than 3 meters, example is skin implantations. It less expensive compared to active RFID, and smaller. While active RFID are primarily powered by power source in the tag like onboard battery, processing and transmission of data. The major problem seems to be the power or battery life of the tag, though it has stronger signals and covers more distance range between 20-100 meters. Finally, semi-active is the hybrid combination of the two previous technology use power source in the tag to power but not for sending any radio energy. RFID can be also classified, based on the frequency used as low frequencies under 100MHz and in the range of 1-meter also not sensitive to moisture, ultra high frequencies at over 800MHz operates at far field, with a range of up to 2-meters and sensitive to moisture. The technology has no support for multicasting and broadcasting at the MAC layer of the RFID system.

RFID technology is used for personnel identification in form of identification cards to control building access. ID card, or smart card, contains RFID tags or transponders embedded in the chips. At a distance from the entrance the signals are emitted, processed and, after validation, the entrance door can be monitored and controlled.

RFID in Home Security Automation Environment

Reliability

Though faced with the problem of interoperability of devices due to the different vendors protocol employ, RFID offers a reliable solution and is less susceptible to jamming. The technology is simple to implement, and the major obstacles to the adoption for home automation are that is a two-way communication protocols, and also less coverage area when compared to network technology like the Zigbee. This is couple with more power consumption when compared to Zigbee, making RFID less attractive for home automation or appliances to appliance communications.

Co-existence

RFID suffers less interference from other wireless technologies in the same area; the frequency band is low and with low emissions.

4.6 WLAN
WLAN provides connectivity to devices over longer range compared to technology in the wireless personal area network family of standards, but at a cost of more power consumption and larger sizes. For quick connection defining the MAC procedures, used for accessing the physical layer, can be either radio frequency or infra red, though no commercial infra red physical layer medium available in the market for now. IEE 802.11 knows, as Wi-Fi a trademark for defining devices with interoperability relative to WLAN standard.

Technology

The frequency is unlicensed band, operating at 2.4-2.4835GHZ bands in the USA and Europe. In Japan it is 2.471-2.497GHZ, when a Wi-Fi device is powered on, a station/device scan for available channels to discover active networks where beacons are being transmitted, a network is selected afterwards, and it can be an ad hoc or infrastructure network. Authentication is carried out at the access point and then associates or connects; WPA security is implemented for further authentication leading to improved security. The technology was based on cellular architecture and we can describe each cell has a BSS basic service set. This is a set of mobile devices with fixed Wi-Fi stations, referred to as access point, and IBSS independent basic services set can be described as ad hoc networks with multihop characteristics and no access point. Thirdly, a set of BSS is referred to as ESS extended service set connected via a distribution system.

4.6.1 Comparison of Bluetooth and Wi-Fi technologies. [29]

<table>
<thead>
<tr>
<th></th>
<th>Wi-Fi</th>
<th>Bluetooth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>2.4GHZ and 5GHZ</td>
<td>2.4GHZ</td>
</tr>
<tr>
<td>Co-Existence Mechanism</td>
<td>Dynamic Frequency Selection</td>
<td>Adaptive Frequency Hopping</td>
</tr>
<tr>
<td></td>
<td>Adaptive Power Control</td>
<td></td>
</tr>
<tr>
<td>Multiplexing</td>
<td>DSS, CCK, OFDM</td>
<td>FHSS</td>
</tr>
<tr>
<td>Future Multiplexing</td>
<td>MIMO</td>
<td>UWB</td>
</tr>
<tr>
<td>Noise Adaptation</td>
<td>Physical Layer</td>
<td>Link layer</td>
</tr>
<tr>
<td>Typical output power</td>
<td>30-100Mw(15-20dBm)</td>
<td>Same as Wi-Fi</td>
</tr>
<tr>
<td>Max-one way data rate</td>
<td>31.4mb/s</td>
<td>3mb/s EDR</td>
</tr>
<tr>
<td>Basic Cell</td>
<td>BSS</td>
<td>Pico net</td>
</tr>
<tr>
<td>Extended Cell</td>
<td>ESS</td>
<td>Scatter net Not in Real life solutions</td>
</tr>
<tr>
<td>Max. No of Devices in a Cell</td>
<td>Unlimited in ad hoc network IBSS, up to 2007 devices in infrastructure devices</td>
<td>8 active devices, 255 in a park mode</td>
</tr>
<tr>
<td>Max.Signal Rate</td>
<td>54mb/s</td>
<td>3mb/s</td>
</tr>
<tr>
<td>Channel Access Method</td>
<td>Distributed-CSMA/CA</td>
<td>Centralized-polling</td>
</tr>
<tr>
<td>Channel Efficiency</td>
<td>Decreasing with Traffic</td>
<td>Constant</td>
</tr>
<tr>
<td>Spatial Capacity</td>
<td>ABOUT 15kb/s.m2</td>
<td>From 0.1 to 400kb/s.m2</td>
</tr>
<tr>
<td>Data Protection</td>
<td>32 bit CRC</td>
<td>16 Bit CRC ACL links only</td>
</tr>
<tr>
<td>Network Set-up</td>
<td>Ad-hoc Scan, authentication Infrastructure scan, authentication, association</td>
<td>Inquiry, page</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Authentication</td>
<td>Shared secret, challenge response</td>
<td>Shared secret and pairing</td>
</tr>
<tr>
<td>Encryption</td>
<td>RC4 stream cipher, RES</td>
<td>E0 Stream cipher</td>
</tr>
<tr>
<td>QoS Mechanism</td>
<td>Coordination Functions</td>
<td>Link types</td>
</tr>
<tr>
<td>Current absorbed</td>
<td>100-350Ma</td>
<td>1-35Ma</td>
</tr>
<tr>
<td>Power Save modes</td>
<td>Doze</td>
<td>Sniff, hold, park standby</td>
</tr>
</tbody>
</table>

### Wi-Fi in Home Security Automation Environment

#### Reliability

Wi-Fi is highly reliable, and the major drawback is the cost, in terms of power and device cost, when compared to other technologies. It has higher data rate, that is, its capacity is more, but this is not needed in machine-to-machine communication or home security automation deployment, with requirements for less power consumption, low range and low data rate.

#### Co-existence

Of the technology with others competing technologies operating at the same, sharing unlicensed band, raises issues like interferences. There will be, at time frequency collisions and WLAN adopts adaptive frequency hopping schemes and co-existence signalling.

### 4.7 External Networks

In order for remote monitoring and control of home security systems, we deployed an external network. The home security system network architecture consists of an external network, gateway, modem and local area network. Earlier, we discussed short-range technology for the local network solution. For external network solution, we will briefly consider DECT, WiMax and 3G for mobile wireless technologies. Our choice technology must be efficient, have widespread coverage, a high security infrastructure, maximum reliability and security against eavesdroppers. Satisfying most of these goals are Network of family, operated by the cellular telecommunication service provider, with a high cost and complexity of the system. Importantly, the network must be a data network, GSM/GPRS, 2.5G, 3G and WiMax.

Digital European Cordless Telecommunications DECT was standardized by ETSI serving essentially as access technology for residential buildings and offices; it provides wireless access both for indoor and outdoor densely packed environments. Area above 300- meters to 3000-meters requires LOS while those of less than 300-meters, are with less need for LOS, are not suitable for countrywide coverage. Bandwidth is between 1880-1900MHZ, with transmission techniques as TDMA/TDD. The voice coding is up to 32kbit/s, with dynamic channel selection. Security is similar to GSM authentication and encryption. Main application is to provide digital home cordless services with longer coverage area.

WiMax offers long range wireless technology countrywide and inter-countrywide applications, developed by the computing industry. It has a lower cost when compared to other similar technologies like DSL-Digital Subscriber Line, with high bandwidth and it is...
easily deployed, bridging the gap between digital divisions. It operates at both license and unlicensed bands, initially operating at 10-66GHZ band. These frequencies have more available bandwidth and less risk of interferences in order to alleviate the problem of LOS associated with this and to deploy the technology for more coverage area, the developers adopted a frequency band of lower frequencies between 2-11GHZ. This seems more commercially viable with dynamic frequency Selection scheme chooses between ranges of frequencies for high performances and prevent interferences by this adaptive selection scheme. The 802.16 is developed for point to multipoint topologies. That is, a single WiMax base station can serve a region also allows for mesh networking. The topology relaxes need for LOS requirements and uses OFDM and OFDMA radio technology, the MAC layer supports QoS with support for different transport technologies such as IPv4, IPv6 and ATM. WiMax is independent of the transport technology and allows for both WLAN and MAN network connection on the same chips. Nokia will start to sell cell phones using WiMax technology.

**WiMax in Home Security Automation Environment**

Reliabilities

Though at lower cost when compare to technologies for long-range transmission, with WiMax there is no need for laying down expensive cables or expensive infrastructure deployments, yet it is less attractive because of unresolved standardization issues. Application of WiMax seems to be a promising technology for the future, competing favourably in the likes of 3G for high data rates, and long range communication for mobile access at a far cheaper cost for deployments. The technology is reliable, with availability of range of frequency and its adaptive features of channel selection for best performances in both local and metropolitan area network. Also, IP-platform ensures reliable solution, preventing needs for LOS in deploying the technology; at lower frequencies, it is more susceptible to interference but it travels longer.

Co-Existence

At lower frequencies bands, it suffers from interference from other wireless technology. Sharing the same bandwidth of the unlicensed spectrum the adaptive scheme is used to reduce the losses due to interferences

Range

This is the main advantage of deploying the technology over all other wireless technology; it is dynamic, serving both LAN and MAN connections, at relatively cheaper cost.

### 4.8 3G

Also, in the same specification for long range communication for remote monitoring and control, we are going to consider 3G wireless cellular technologies for broadband wireless access just like WiMax. The evolution in GSM network, from original, circuit-switched network for voice application, to packet-based networks for data services with the overlaying of the network to support IP-based packet services, 3G technology will ensure ubiquity of service and a scenario whereby we are able to access the network with any devices, efficient battery life of mobile devices and portable size of devices. This will, in turn, lead to many other applications, for example home monitoring and control over the GSM network. The technology acceptability will depend on the cost of deployment and billing. 3G GSM operates at theoretically 384kbit/s to 2mbit/s for a single channel user of the network.
The networks gives more spectral efficiency, lessen power consumption and enables the introduction of SIM subscriber identity module. It allows for international roaming, which is a situation whereby a subscriber can use the phone, even when not at his location, register or moves from countries of subscription to other. In home security system householder can monitor/control situation at home country and even when abroad or foreign countries. Ubiquities of service, longer battery life, small portable devices—mobile phones—these, are some of the advantages associated with GSM network.

4.8.1 3G in Home Security Automation Environment

Reliability

Though the cost of deployment is high, it is highly reliable for remote monitoring of a home security system. Widely adopted worldwide with roaming features, mobile devices with efficient power consumption capabilities and use of data over the network can deliver a rich range of IP-based services plus highly secure infrastructures.

4.8.2 A propose Home Security system.

The system above integrates short-range transmission technology-wireless sensor network and long-range transmission technology for local and remote monitoring /controlling of home security systems. The sensory nodes are multipurpose for better and more efficient home monitoring and safety. Sensors are used to detect motion, break-in sensors functioning as window or door sensors and other abnormal occurrences, such as gas or smoke detectors, with the capabilities for these sensors to communicate with one another wirelessly and can be connected to a gateway/hub for remote monitoring of home security, this brings solutions to problems associated with traditional security systems like ease of set-up by placing sensors around with no need for wire installations, drilling of holes, hiring of workmen and other disruptions and the system is more robust can survive disaster in that if one of the connecting nodes shut down an alternative route will be discovered automatically, also present some challenges of how to make sure every node is reached in the network. Efficient with a great
reduction in cost and the killer application is the add-on service allowing for remote monitoring and controlling of home security system.
5.0 Features of Zigbee and Requirements Specifications for Home Security System

A home security system is all about monitoring of the environments and control. Zigbee provides low power wireless sense and control network distinct advantage over others short range wireless technologies. The first wireless wave is for voice communication, providing effective person-to-person communication. The second wave is wireless data-internet for computer-to-computer communications comprises of wireless technologies like Wi-Fi and Bluetooth. The third wave is for machine-to-machine communication, with no need for middle-men deployment or computer. This founds its application into modern home security systems, with need for energy management [12] Zigbee provides the best solutions.

It is not enough to get rid of connecting cables or wire by providing a wireless system; a truly wireless system must also get rid of power wires. Running power cable greatly complicates deployment issues and installation cost [11]. Wireless power solution exists in form of batteries. Battery operated devices are not free of maintenance with also cost and problems of replacement of battery and charging in most cases. Zigbee sensors provide the best features meeting, the requirements specifications with battery life expectancy up to 2-years or more [11].

Sensors applications have totally different requirements, when compared to existing wireless voice and data network requirements; importantly the availability of power is the most apparent differences, sensors will work for years on a non-rechargeable, coin-sized battery or by energy harvesting from the environments. The harvesting is through solar panel or vibration harvester in some cases. Other specific requirements for wireless sensor networks are network configuration for reliable link, range and number of nodes etc [12].

---

**Zigbee radio module with an internal antenna and external connectors [11]**

**Zigbee-Home Automation Standard [11, 12]**

1. Mature, stable and open multi-vendor standard
2. Self-configuring, self-healing mesh network
3. Strong security with built-in encryption
4. Standard messaging through home automation profile
5. Proven robustness, co-existence with other wireless technologies

5.1.1 Features of Zigbee
The technology is cheap to deploy, low-cost when compared to other short-range wireless technologies (2 to 3 dollars per chip with no need for workmen and installation cost).

It has a low data rate, and is an ideal solution for machine-to-machine communication for effective monitor and control-automated solutions.

It has low power consumption. In applications like the sensory nodes for local and remote monitoring, the battery power could last for longer period. Sleep-mode current is less than 1uA. Ultra low power Bluetooth devices have similar power feature.

The bandwidth is for sufficient transmission. Though it is relatively low when compared to other personal and local area networks, but it is sufficient for local and remote control and monitoring of appliances.

Network topology is ideal for flexible installations of sensory nodes for an effective security system; the network topologies available are star, three and mesh, with engineers flexibility to choose best-suited topology for designs.

Scalability, support for large no of nodes/sensory nodes.

Ad hoc networking no infrastructure needed in setting up the security system.

Good security, with support for in built AES-128 encryption and authentication schemes. Security mechanisms are implemented on three layers MAC, NWK and APL.

Viruses have not been found in the protocols, for now there is no fear of virus.

It establishes connection quickly; there is a short-time delay, with fast respond speed of 15ms converting from sleep mode to work state, Bluetooth needs 3 to 10s for connection.

The range is small, 10-100meter; with ranges varied for line-of-sight and for non line-of-sight and also for indoor and outdoor. Also the range can easily be expanded by advancing RF transmitting power for more coverage. Also network multiple routing paths schemes lead to increased coverage.

There is a widespread adoption of the technology for monitoring, sensing and automated control of appliances.

**JAMMING** With the very low transmitting power of sensory nodes, there is a reduction in the probability of the network signals to being detected by an attacker or jammer. It will take the jammer to locate or discover a signal first, if, eventually, the network signal was detected, it is relatively easier for an attack to be carried out by just using a very high-powerful signal, or by jamming source, a great disruption can occur as a result. Also an intelligent jammer can use bypass, wireless sensor protocol are weak or with small computational capabilities and can easily be attacked by jammer. The protocol layer addresses the problem of jamming and interferences by employing FHSS and DSSS schemes though it is not totally free from an attack.

5.1.2 Features of Home Security System are:

- Low cost installation and deployments of the home security system.
- The system has a very low-power consumption and could last for longer duration.
- Secure and reliable solution for home security system
- 24-hour monitoring, and control for home security system.
- Local and remote monitoring/control of the home security system can easily be integrated with other long-range technology for remote monitoring and control.

Home security system architecture can either be star or mesh network topology; the latter is preferred over the star network topology despite the simplicity of the former. An important consideration for the wireless network stack design is the ability of the wireless sensor nodes to cope with constant changing quality of the wireless links. For example, sensor nodes
employed in home automation-security must cope with the effects of people/obstruction; an obstruction or people moving around could result in a formidable effect. It reduces the quality of the links and takes into account that a sensory node or network node might be isolated or disappear at any moment as a result. Our ideal security system, employing Zigbee technology, must be able to cope with this, as well as interferences by other wireless technologies sharing the same bandwidth like Bluetooth and WLAN. Zigbee has little effect on these two technologies but Bluetooth class 1 and 2, increased transmitting power, have an effect on Zigbee. Likewise, WLAN reduces the throughput/performance of the system; it employs spread spectrum techniques DSSS and OFDM to cope with the problems of shared spectrum.

5.2 Features of Mesh Network:

- Every sensory node connects directly to all its neighbouring nodes
- Every sensory node is capable of routing to and from all of its neighbour nodes
- Network is self-forming, which means the node is automatically added to the network without the need for manual configurations.
- Network is self-healing, which means it automatically adjusts routes to and from sensory nodes if the network changes, for example, if a node disappear, attack, the network is highly reliable.
- Network is self-healing, which means it automatically adjusts routes to and from sensory nodes if the network changes, for example, if a node disappear, attack, the network is highly reliable.
- It is very robust compared to star network.
- Maintaining end-to-end solution for wireless sensor nodes is very challenging, since the network topology might change frequently due to nodes or sensors failure. Mesh topology provides the best solution, a reliable network topology putting into considerations mobility factor.

5.2.1 Why Mesh Topology?

- It is self-configuring and self healing; automatically discovers other Zigbee enabled devices when the destination device is not in line-of-sight/connectivity.
- Messages can be routed through other Zigbee enabled devices to the destination device with the bottleneck problem eliminated and the latency problems solved.
- The reach of the network can be much greater than the range of individual radio modules themselves.
- Adapted to challenging/changing conditions of the home and its environment.
- Scalability can easily be expanded; ideal for home automation.
A pure Zigbee network device consists of network coordinator devices NCs, full function devices, FFD-Zigbee routers and reduced function devices, and RFC-Zigbee end devices. In a particular zigbee network, only the FFD are meshed and can talk to one another/relay and respond to messages in the network. Also, a FFD do require much power unlike a RFD which do not require as much power as FFD sensor devices with less workload.

In our proposed home security system, the sensory nodes-motion detectors, with abilities to talk, send and receive messages will function as RFD devices—reduced function device, implemented with Zigbee end device module, and can route messages to a central hub. The central hub will be the network coordinator device in the home security system network. The NFC or coordinator device will also be integrated with gateway for external network connection. The reduced function devices have less power requirements (battery-powered).

There can only be one network coordinator in the system/gateway/modem/central hub and the initial configurations and continued control of the wireless home security system is done by the network coordinator devices.

NFC—Network coordinator
   1. Overall knowledge of the network.
   2. Most sophisticated of the three types of device
   3. Most memory and computing power.

FFD—Full function
   1. It can function as network coordinator
   2. Additional memory and computing power
   3. Ideal for network-edged routers.

RFD—Reduced function device
   1. Limited functionalities
   2. Less memory and computing power
   3. Power by battery or sometime battery less
6.0 Zigbee a Standard for Home Automation

In the future integrating other home devices/appliances, the Zigbee routers, though generally line-powered devices as they need to be active continually in order to forward messages in the network, will find their functions in meshing of networks together to extend size of the network. Also it will be possible to build a mesh network that combines the essence of both a Zigbee network, and a low power router network, with possibilities for a battery-less end-devices, where the mesh routers/nodes will require battery power instead of former line-powered source and the battery less end devices will be powered by solar energy, harvested from the environment.

Implementing Zigbee is low cost, despite the protocol complexity. Low cost implementation of hardware and software, running on a small microcontroller. Ideally, to use single chip SoC, that integrates IEEE 802.15.4 radio, MAC, embedded microcontrollers core, AES, RAM, flash memory, peripherals for SPI, VART, GPIO, ADC and timers. To ensure interoperability of devices, it must be certified by the Zigbee alliance. Interoperability with other Zigbee devices at protocol level is the requirements to earn the right to use Zigbee alliance logo. It gives room for multi-vendor environment, with functions like multi-hop, which can be implemented, allowing for flexible large domain deployment. Example of Zigbee SoC -system on chip includes processors, flash memory, MAC, 2.4GHz radio and other peripherals by Ember Corporation.
6.1 How to Interconnect Home Security System to External Network

A Zigbee home security system network can be connected to the external network for remote monitoring and control of the home security system. The communication technologies available for the external network-long range transmission are wireless LAN technology, dial-up modems, private radio network, and Satellite communication, WiMax, Internet and GSM. Reliable and available remote monitoring and control of the system can be done via GSM/GPRS and the internet, informing users in real time at a low-cost.

GSM cellular networks provide the best convenient solutions with features like international roaming, spectral efficiency due to the adoption of packet switching techniques over the circuit switching techniques, and introduction of SIM, meaning that each GPRS/GSM mobile terminal or phone can potentially have their own IP address and will be addressable as such over the data network since the SIM card IP addresses are fixed and always available. GSM can send data over the traditional voice network as SMS, the data rate is slow and there is no guarantee on delivery time. Also, SMSs are limited to 160 characters, and there is a limited data rate when compared to enhance features of 2.5G, 3G, GSM/GPRS but it is sufficient for remote monitoring and control, with the use of SMS-Short Message Service for the operations. With the advancement in the cellular network, providing more bandwidth for multimedia services and increased data rate, providing guarantee delivery time. GSM network applications for real time monitoring and control is now more efficient, other home appliances can now be integrated into the home network with sufficient bandwidth for remote operations/supervisions.

Widespread coverage with roaming features, high secure infrastructure which provides reliable transmission and availabilities and accept abilities of the GSM technology with low-cost makes, it best option for remote monitoring over the public network. The Internet provides broadband connection coupled with IP mobile devices like PDA and IP mobile phones; these offer another good option for remote monitoring of home security systems over the data networks, ensuring that clients either stationary or mobile clients, can access the home security system network anytime. In order to accomplish this, a web server is designed to take request from remote client as an interactive interface, where commands can be made by the client.

6.1.1 Remote Monitoring and Control

Via Home Server Using GSM and Internet [5]

The services of remote monitoring and control of home security systems can be offered via home server; the home security system network is connected to the home server, which is mostly in form a PC. The system, via home server, provides additional functionality like multimedia, and can integrate other devices; also the system is under the control of householder with issues of privacy and security addressed. The home server processes the incoming commands from the web server or GSM modem/GPRS modem, digitizes the commands and sends them to relevant units. The units’ transceiver picks up the signals couple with the microcontrollers, apply the commands to the device attached to. The device also can send back commands through the transceiver into the home server, two-way, real time communication between the device and the home server.
GSM provides connection to the home server when Internet is not available. Communication is established by SMS short message service. The communication is carried out by the GSM modem/GPRS modem, using AT commands. The prescription description units (PDU) perform the task of allowing for GSM module with various text modes. In the mobile part, an interactive software J2ME platform, supported by Java is used. A motion is detected by the motion sensor, information would be sent by the motion sensor to the home server which in turn will send information via GSM modem to the registered GSM mobile number.

![Step by step usage of Mobile control program](image)

**Fig. Step by step usage of Mobile control program**

SMS message is created, with a content (lock the door) command. Commands are encrypted and send to GSM modem, which in turns, is connected to the server main control program, the Server decrypts commands, reads and interprets the message appropriate commands send to the door lock system via the transceiver node. Feedback SMS sends to the mobile number.

Internet: an interactive websites is created to take request from the remote clients to the home security system, and the home security system can, in turn send their status to the remote devices for monitoring. The client can send a request to the home server to control the home security system network and the home security system network can also send their status to be displayed on the remote client’s mobile phone via the server.

6.1.2 via Service Provider Using GSM and Internet

The home security system network connects with remote users through a service providers, instead of a home sever. The server is at the authority and management of the service provider; connection to the home security network is through a remote server which, in turn, connects with the home network control facility. It is cheaper to manage with fewer skills and less technical know-how is needed. Also, for the service provider; income for professional service rendered to customers. It is more efficient, though more complicated, than the home server scenario.

The server technology is more complex, with complex devices and maintenance costs. It requires an external interface, like PBX, that can be configured remotely over ISDN or an
integrated network port. It is more efficient, and allows for billing with capacities to integrate other functions or home automation services.

6.1.3 via Gateway

Internet Gateway

An internet gateway is unlike the home automation server discussed above, which integrates both IP network-packet based network and circuit-based cellular network with the use of GSM modem to the home security system network. The residential gateway provides integration of the home security system network to the IP network/internet alone, connecting various home networks to the access networks/public network. The gateway includes a router, bridge, protocol transfer technology etc.

The gateway absorbs the different keeping network protocols; this becomes necessary putting in mind that other network topologies will co-exist in the home environment. In order to use http protocol for remote access, we propose the home gateway should be based on web server technology, just like in the home automation server technology, where request(commands are submitted.

GSM/GPRS Gateway

GSM-3G/GPRS provides a convenient way to access the data network, providing data packet services to GSM clients and establishing a wireless connection for real-time activities solutions. The data rate is between 20-170 kb/s and with short access time. In some cases, the gateway also serves as coordinator for the home security sensor device and consists of wireless transceivers, GSM/GPRS module, microprocessors, LCD, and light emitting diodes.

The integration of both Internet gateway and GSM/GPRS gateway as home gateway for remote monitoring and control provides the best solution serving both functions.
7. Conclusions

Home automation communication standard must be, of course wireless, with two options available, namely radio and optical. The radio link emerges as the technology standard of choice for home automation; it must satisfy other pressing needs like: interoperability, low power, low cost, ease of deployment and operations of the links, security and range etc. Home automation technological development comprises three stages: focus, integrated and distributed technological developments and also the applications of home automation can be grouped into security, energy, health/comfort and entertainments.

A Survey of available wireless technologies - short range wireless technologies in becoming a general standard for home automation was carried out by me, with a focus on the security system/alarm application of home automation. Wireless technologies available for deployments in home environments are: Zigbee, WLAN, Bluetooth, NFC, RFID and UWB. After careful evaluations of the above mentioned standard, Zigbee, WLAN and Bluetooth could be described as open multi-vendor, stable and mature wireless technologies standard for home automation. It also satisfies conditions for the range of coverage for homes. Evaluation of Zigbee, Bluetooth and WLAN, in terms of cost, the operational cost and deployment cost, Zigbee and Bluetooth have comparative advantage compared to WLAN.

On the other hand, when considering the cost: operational and deployment cost also, in term of already existing platform and availabilities, Bluetooth and WLAN have comparative Advantage compare to Zigbee. Cheaper to deploy and operate. Conditions like data rate, security schemes, co-existence with other wireless technologies Sharing the same bandwidth, was met by the three standards - Zigbee, Bluetooth and WLAN. All are proven to be robust, good security schemes with support for in built for AES Advance encryption standard with authentication schemes. All establish connection quickly, are scalable and support a number of sensory nodes for home security application.

Scientist and engineers alike will design or build on the technologies that best suit their needs, with cost of deployments and operations serving as determinant factors. However, I concluded that Zigbee technology is an ideal choice for home automation putting in considerations the home Security system would be built from the very scratch, with no existing infrastructure to deploy on.

Zigbee technology provides low-power wireless sense and control of appliances. It get rids of connecting cables and power cables, the sensory nodes could be operated with a battery and with a longer battery life. And in the nearest future the zigbee nodes will be able to harvest energy from the environment. Other important features like maturity of the standard, widespread adoption of the technology for monitoring, sensing and automated control of appliances

Worldwide, features of the network topology like the mesh network technology put the technology at the forefront for automation and home automation alike.
8 References


[10] Satyajit Chakrabarti Liyun wu, Son Vuong, Victor C.M Leung Department of Computer Science/Electrical Engineering, University of British Columbia Vancouver, Canada “A Remotely Controlled Bluetooth Enabled Environment”, IEEE, 2004


[20] Satyajit Chakrabarti, Liyun Wu, Son Vuong, Victor C.M Leung, Department of Computer Science, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver Canada, “A Remotely Controlled Bluetooth Enabled Environment”
[28] Vishnu Chunduru Software Engineer 3HT Technologies, Reston, Virginia and Nary Subramanian Department of Computer Science, University of Texas at Tyler, Texas, “Perimeter-Based High Performance Home Security System”.
[29] K. Shuaib, M. Boulmalf, F. Sallabi and A. Lakas College of Information Technology UAE, University, “Co-Existence of WLAN and Zigbee, a Performance Study”.
Comparative Study of Wireless Protocol: Bluetooth, UWB, Zigbee, and Wi-Fi”, *33rd Annual Conference of the IEEE, Nov.5-8*, Taipei, Taiwan

[31] Steven J. Vaughan-Nicholas, “Mobile WiMax: The Next Battleground” IEEE Computer Society


[34] Zigbee Organisation Tutorials [www.zigbee.org](http://www.zigbee.org)

[35] Ember Corporations Technology [www.ember.com](http://www.ember.com)


[38] Neeli Prasad and Anand Prasad, “WLAN Systems and Wireless IP for Next Generations Communications”.

9 Appendix