# Home Security Using Zigbee Technology

R.Saravanan
Associate Professor,
CSE Department, Saveetha Engineering College,
Thandalam, Chennai- 600 095, Tamil Nadu, India.

A.Vijayaraj
Associate Professor,
IT Department, Saveetha Engineering College, Thandalam,
Chennai- 600 095Tamil Nadu, India.

**Abstract-: Security is the most important in day-to-day life for almost all the sectors of the world. A special security is most essential for houses and it is made possible by integrating various sensors with Zigbee network. We would like to provide simple and effective security solution for whatever the threatening is. The threatening may be a human intrusion, metal detection, fire hazardous problems, door tampering problems, gas leakage problem. A real time and true model home sensors and transducers will be used in this project along with a camera unit for continuous security monitoring. Powerful intruder detection systemic Emitter and detectors will be used in this project to monitor the walls or where the intrusion monitoring is essential. If anybody intrudes in that particular area can be detected along with photography of the intruded person. This sensor can really work up to 10m distances. FireSensors: True model fire sensors will be employed in this project, which can capture the fire and provides logic signals to the electronic circuits. Metaldetector: An inductive proximity sensor will be used in this project to detect bomb and metal hazards. This sensor is so powerful, that it can sense metals inside a plastic box. Even metal foils greater than 2 microns can be sensed by this device and can produce electrical output for the same. Gas leakage sensor also used in this project to identify the gas leakage inside the houses.**

**Keywords: Sensors, Zigbee network, Intrusion, Metal detection, Transducers, Emitter and detectors, Metal hazards.**

## I. INTRODUCTION

This paper presents architecture for secure service discovery for use in home networks. We give an overview and rationale of a cluster-based home network architecture that bridges different, often vendor specific, and network technologies. In this paper , we propose the Zigbee home network devices are represented as device proxy service bundles. Such proxy service bundles are dynamically downloaded, installed and registered to the service registry by the dynamic device integration manager on the corresponding devices' joining the Zigbee network. Wireless Monitoring for home security is among the cutting-edge researches in the field of International Intelligent Building. To implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBee technology. The introduction of a variety of sensors and the enhancement of system's reliability guaranteed that the intelligent remote monitoring system can be responsible for home security. The hardware and software design and system performance are expounded in details. A number of surveillance devices in wireless network are connected. The experimental result shows that the system can attain remote surveillance of intelligent home safety with high availability and reliability. Zigbee standard for WSNs (Wireless Sensor Networks),has become one of the most promising protocols for wireless home networking and automation due to its low power consumption, low cost, and support for various ad hoc network configurations .

## II. SCOPE OF THE PAPER

Zigbee provides a light-weight software stack supporting multi-hop networking, device management, and security over the IEEE 802.15.4 WPAN Wireless Personal Area Network standard. Consequently, one of the most essential functionalities for home gateway systems is to support flexible interoperability between home network applications and various Zigbee enabled consumer devices such as wireless sensors, appliances, and mobile consumer devices. In the home networking and automation area, some tentative and proprietary researches on integrating sensor networks and ubiquitous devices have been performed. The design and implementation of a home remote control network using Zigbee devices and a home gateway is based on an embedded server. Home wireless network technology based on ZigBee and its network topology, and clarified the hardware and software design of home gateways and device nodes. An intelligent home care system based on context-awareness that consists of a sensor platform. Sensor platform collects raw data from the home environment and sends them to the context-aware framework to provide context for home care services.

## III. NEED FOR THE PAPER

While looking forward to the establishment of security for the houses it is necessary to overcome the above mentioned threats. In this project , three different sensors are used such as fire sensors, gas leakage sensors, human intrusion sensors, metal detection sensor. These sensors are uniquely used to recognize each corresponding incidents that happens every house. Zigbee networks are mainly used in the home security in order to provide complete security over long range . The following operations are to be performed in our project, when the sensors read a Particular problem i.e. for our consideration let us assume a home in fire ,the fire sensor reads it and sends the signal to the Zigbee ,the Zigbee transmits the signal to the control room, since the Zigbee is the transceiver the same is used to receive the signal at the control room .the obtained signal using Zigbee is then processed and appropriate action is performed that is for this case considered the water is sprayed as soon as the fire is detected.Thus the system considered is said to be more secure by the considerations of the human intrusion detection, Thus PIR(Passive Infrared Radial sensor) sensors are used in order to obtain the intrusion of the unknown humans in the home during vacation or during when no one is at home ,the PIR sensor detects the human using performance infrared sensor for use in alarm burglar systems, visitor presence monitoring, light switches and robots. These compact, easy to use sensors can be easily implemented in your design and full design information is available in the datasheet link below. It has dual compensation, operating stability.

## IV. LITERATURE REVIEW

### SECURE SERVICE DISCOVERY IN HOME NETWORKS

Objective is to develop an open, secure, interoperable, and seamless global home platform. approach is to define a suitable middleware platform that allows the seamless interworking of a wide variety of appliances found in a home environment. Industry sees a wide range of business opportunities when the platform supports legacy services and existing standards next to new compliant services. Examples include UPnP, Bluetooth, SLP , mini, and Salutation.Security is a key component in design. If required, the entire process from the first discovery of a service in the network, through the use of that theservice, to the closing down of a service can be secured. Security is therefore an integral part of the architecture.This paper presents work done in The European Application Home Alliance project. Objective is to develop an open, secure, interoperable, and seamless global home platform. Approach is to define a suitable middleware platform that allows the seamless interworking of a wide variety of appliances found in a home environment. Industry sees a wide range of business opportunities when the platform supports legacy services and existing standards next to new compliant services. Examples include UPnP, Bluetooth, SLP ,Jini, and Salutation. Security is a key component in design. If required, the entire process from the first discovery of a service in the network, through the use of that service, to the closing down of a service can be secured. Security is therefore an integral part of the architecture.System components. In this section we present the principal components of the platform. We start with the articulation of its main requirements. Seamless interworking of services and technologies requires: The architecture to support heterogeneous technologies. Standardization may help to reduce the diversity of technology but it is insufficient. Moreover legacy technology must be supported.The architecture to support “cluster cultures”. Applications and services that reside in one cluster share the interests of a specific value chain. Necessarily, stakeholders of the same application area share the same culture; they use an accepted terminology, and must cope with the same set of industrial requirements, standards, and regulations.The architecture to provide a zero-configuration environment (touch and play). The end users of the platform expect out-of-the-box operation. A. Communication At the bottom,as an example, four devices are connected to two different types of network . Devices A and B offer a service according to the UPnP protocol, while Devices C and D offer a service following the CECED protocol. In addition, the services of A and C belong to the Lighting cluster whereas the services of B and D belong to the White Goods cluster . Clusters represent business alliances with a predefined application programming interface (API). The offered services of each cluster reside on devices that are connected to different network technologies, moreover each service uses a different protocol. We therefore must bridge the technologies (proxy) as well as the respective protocols (cluster).

The middleware offers a rich set of technology drivers to connect to a wide range of devices. In order to access the offered services, the middleware provides a set of proxies that bind a specific protocol to a specific technology. Proxies, in turn, support a plug-in mechanism to specialise protocol transformations, i.e., the clusters of Figure 1. The default plugin of a proxy is useful for inter protocol communication, e.g.,between two UPnP services or between two services.Consider as an example figure 1 once more. Device Aconnects to an IP driver. Since the service of Device A followsthe UPnP protocol it will be handled by the UPnP/IP proxy,moreover the communication can be specialised to follow theprotocol of the Lighting cluster. The service of Device A is now available as a Lighting/UPnP service, which can be used by other Lighting services as well as UPnP services. Suppose we have a Device X (not shown) that connects to the EHS cluster and its service follows the UPnP protocol then it would require UPnP/EHS proxy with a default cluster plug in to connect the service of Device X with the service of Device.AB.

Secure Service Discovery The concept of service discovery is present in many systems.Examplesare Jini, UPnP, SLP, FRODO and Salutation. In contrast to most other systems,service discovery and security are embedded in the architecture. The security features rely on the trustworthiness of the proofs of registration and the confidentiality of cryptographic key material. The security component handles all security-critical operations. It also stores the identity of the device in which it is installed. In order to facilitate the zero-configuration of devices, we implement a touch and play paradigm. The touch is a physical registration process, which exchanges credentials among a gateway and a registering service; for instance by means of RFID tagging. We use a hierarchy of services as exemplified. Once registered a service is granted access to all services down the hierarchy. Our service discovery process uses distributed directories, where each directory maps one-on-one to a pool of registered services. Discovering a service boils down to a query on the local registry followed with a tree traversal if the requested service cannot be resolved locally. In our initial design each directory only stores locally registered services, however if required for reasons of efficiency a directory could store more information. This does not change the design. Our security mechanism relies on a security engine for storage of device credentials and a cryptographic kernel. We use a shared key protocol for the authentication and integrity proof of transferred messages. We chose the stationto-station protocol , which is an authenticated variant of the well knownDiffie-Hellman key agreement protocol.This protocol has proven security properties, is simple, and allows piggybacking with a service discovery protocol. As an example of the integration of the security component and the service discovery mechanism consider the following scenario. A Service K actively searches for Service M, which is willing to acknowledge the request provided Service K can be authenticated (is properly registered). Once accepted theydecide to exchange messages in a secure way. The scenario is outlined in the diagram of Figure 3. The steps are as follows: Service K sends a Search request that includes a so-called Ping message. The Ping entails the key agreement request of Service K and an authenticity proof, which allows Service M to verify that Service K posed the request. Once authenticated, Service M replies with an Accept message that includes a Pong message. The Pong entails the key agreement response of Service M and an authentication proof. After the (authenticated) receipt of the Pong message Service K and M share a secret session key, which can be calculated from the exchanged key agreement information?

The session key is used to encrypt data messages in the further communication among Service K and M. The architecture, while still under development, reached a state that makes prototyping expedient. We are developing a prototype based on commodity technology that includes seamless interworking, security, and service discovery. The technology of choice includes an OSGi platform and networking. It supports clusters for white goods and lighting, it supports protocols like and Konnex, and it supports technologies such as ZigBee, Ethernet and EHS. In this paper we have presented an architecture for home networks that supports secure seamless interworking for heterogeneous networks and clusters. One of the main features is the integration of a flexible transport system, security, and secure service discovery. The quality of the architecture will be assessed through prototyping.

## V. EXISTING SYSTEM

### SECURE SERVICE DISCOVERY IN HOME NETWORKS

This paper presents architecture for secure service discovery for use in home networks . We give an overview and rationale of a cluster -based home network the architecture that bridges different, often vendor specific, and network technologies. We show how it integrates security, communication, and service discovery to achieve a secure and trusted way of deploying services in a domestic environment. TEAHA's objective is to develop an open, secure, interoperable, and seamless global home platform. TEAHA's approach is to define a suitable middleware platform that allows the seamless interworking of a wide variety of appliances found in a home environment. Industry sees a wide range of business opportunities when the platform supports legacy services and existing standards next to new TEAHA compliant services. Examples include UPnP, Bluetooth, SLP , mini, and Salutation.Security is a key component in TEAHA's design. If required, the entire process from the first discovery of a service in the network, through the use of that theservice, to the closing down of a service can be secured. Security is therefore an integral part of the architecture.

1.The architecture is to support heterogeneous technologies Standardization may help to reduce the diversity of technology but it is insufficient.

2. Moreover legacy technology must be supported.
3. The quality of the architecture will not be assessed through prototyping.

## VI. PROPOSED SYSTEM ARCHITECTURE

**TRANSMITTER SECTION:**

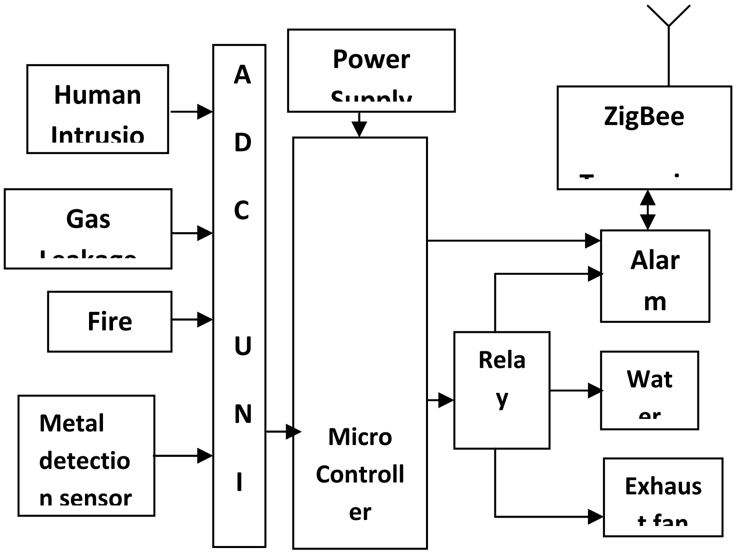


FIG : TRANSMITTER SECTION

**RECEIVER SECTION:**

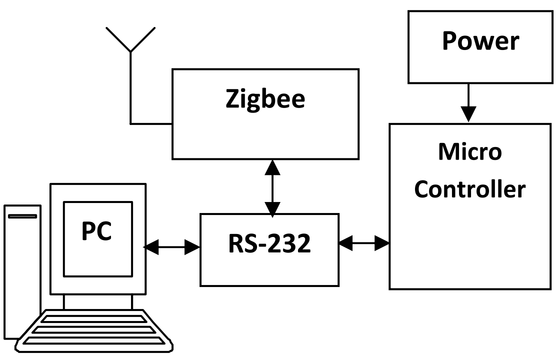


FIG : RECEIVER SECTION

## VII. SYSTEM DESIGN

### a) MODULE DESCRIPTION

To illustrate the implementation of the home security using various sensors in appropriate manner and hence implementing them in suitable manner.Home security. . Wireless Monitoring for home security is among the cutting-edge researches in the field of International Intelligent Building. To implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBeetechnology.Modules are used in paper.i)Fire sensor module ii )Intrusion detection module iii)Metal detection module iv)Gas leakage detection module

### b) FIRE SENSOR MODULE

The fire sensor that is used in this module is basically of lithium form which transfers by detecting in an appropriate manner. Once the detection is made water is made to spray in that particular part of the building. In general fire or spark in motor operation is quite normal because of heating of coils under overload condition. In such abnormal conditions, the fire must be detected and preventive action must be taken. Since human vigilance is not possible in these circumstances, we must go for auto flame detection system to overcome the above problem and to inform the control room about the status of the flame.

**FIRE SENSOR MODULE DATA FLOW DIAGRAM**

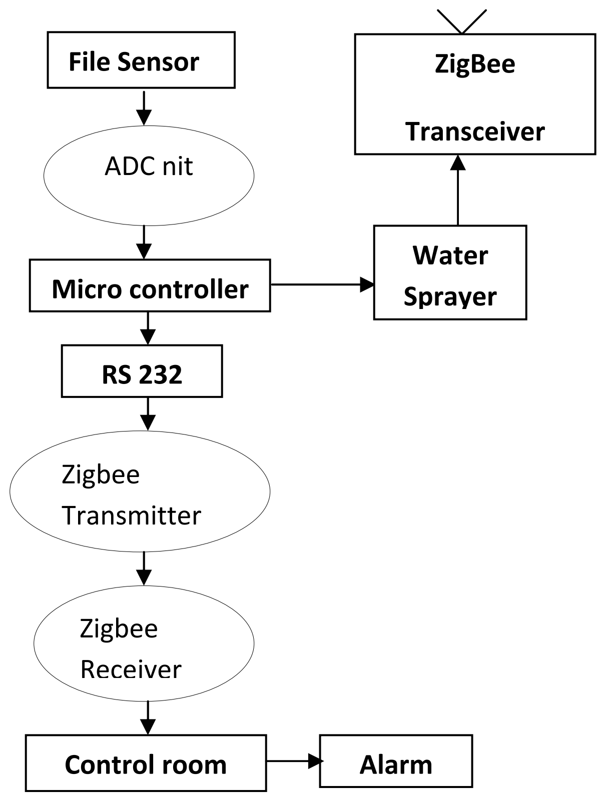


FIG : FIRE SENSOR MODULE DATA FLOW DIAGRAM

### c) INTRUDER DETECTION MODULE

The intrusion detection sensor that is used in this module is basically of simple form which transfers by detecting in an appropriate manner. Once the detection is made then the alarm is made to ring in that building.We've connected 1k resistors to +5v and to the emitter I=5v/1k = 5m amps. If we decrease the resistance, the current will increase thereby rays production also increases, more rays density allows for longer length operation. The rays emitted are sent to the IR detector, which is placed straight to the IR emitter. whenever rays are incident it conducts. A 100k resistor is used to pull up the detector, when it does'nt get IR. When rays are incident, anode detector is low. when no rays , anode is high.NPN transistor is coupled with the detector conducts only when the Base gets logic HIGH. Whenever it detects , interruption transistor will be cut-off, status of the collector is logic HIGH, output of the Schmitt trigger is LOW. During interruption, IR detection is cut-off and anode is pulled high. Transistor conducts and status of the collector is LOW. Final output of the Schmitt is logic HIGH

**INTRUDER DETECTION MODULE DATA FLOW DIAGRAM**

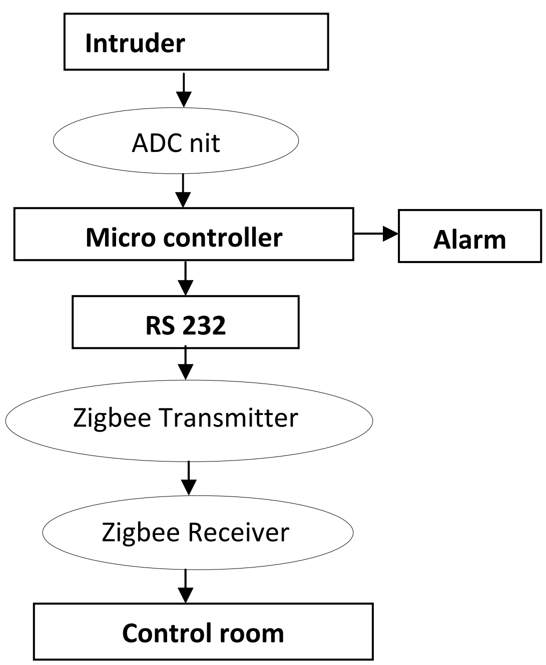


FIG : HUMAN INTRUSION MODULE DATA FLOW DIAGRAM

### d) METAL DETECTION MODULE

The metal detection sensor that is used in this module is basically of simple form which transfers by detecting in an appropriate manner .Once the detection is made then the alarm is made to ring in that building.A single chip metal detector with a range of a few inches. This is useful for detecting nails or screws in walls and floors, or for locating buried mains cable.The detector is a single 100uH choke. The IC has an integral oscillator the choke forms part of an external LC circuit, its inductance being altered by the proximity of metal objects. It is the change in oscillation that is amplified and demodulated. Led 1 will light and the buzzer will sound when the choke change sinductance.VR1 is adjusted with the choke away from any metal source so that the LED lights and buzzer sounds. The control is backed off so that the LED goes out and buzzer stops. Now when the choke comes into contact with any metal object that alters its inductance, LED 1 and the buzzer will activate. The sensors also have an integrated predamping protection function to reduce the metal free mounting area in applications. This allows traditionally flush-mounted sensors to be recessed by half a turn for increased mechanical protection. Non-flush mounted sensors may be embedded in metal up to the outer edge of the thread on barrel style sensors and on all four sides of rectangular style sensors, causing only a slight reduction in sensing distance.

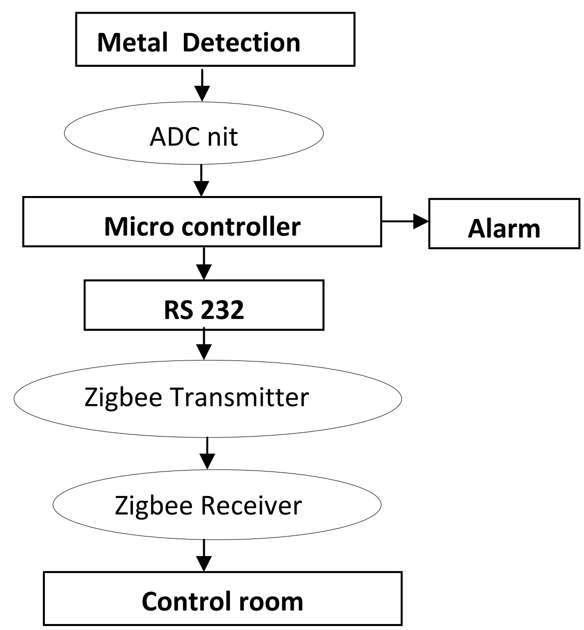


FIG : METAL DETECTION MODULE DATA FLOW DIAGRAM

### e) GAS LEAKAGEDETECTION MODULE

In this module we are using effective fire sensors that detects the gas leakage in appropriate manner ,whenever there occurs a gas leakage in a particular part of the building ,the gas leakage sensors installed in that building detects it and sends the signal to the control system using Zigbee networks. The fire sensor that is used in this module is basically of simple form which transfers by detecting in an appropriate manner. Once the detection is made the exhaust fan is made to run automatically so that it extinguishes the gas that is leaked inside the building considered. Gas detectors can be used to detect combustible, flammable and toxic gases as well as Oxygen depletion.They may also be used in firefighting.Gas detectors are usually battery operated. They transmit warnings via a series of audible and visible signals such as alarms and flashing lights, (sometimes using LED technology), when dangerous levels of gas vapour are detected. As detectors measure a gas concentration, the sensor responds to a calibration gas, which serves as the reference point or scale. As a sensor's detection exceeds a preset alarm level, the alarm or signal will be activated. As units, gas detectors are produced as portable or stationary devices.

**GAS LEAKAGE DETECTION MODULE DATA FLOW DIAGRAM**

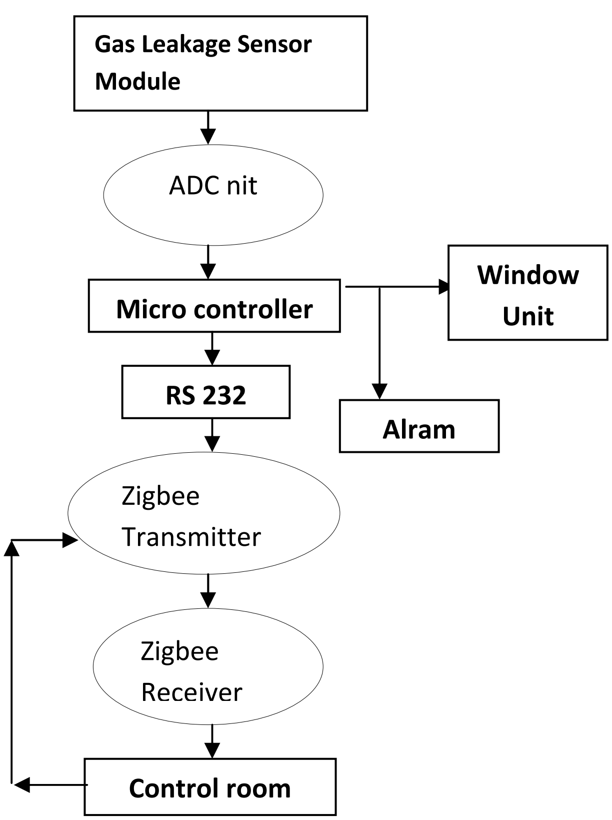


FIG : GAS LEAKAGE DETECTION MODULE DATA FLOW DIAGRAM

## VIII. CONCLUSION

Our system realize remote home automation control based on the emerging wireless communication technology, and implement hardware and and coordinator, the device nodes can be placed anywhere in the room, this solution also future in low power consumption, the energy conservation and the environmental protection. software of home gateway and device node. his design realizes the wireless connection between device node and in experiments in a home network tested to prove its feasibility and effectiveness. The proposed architecture is expected to contribute to the development of ubiquitous service systems not only for home network service domains but also for a variety of service domains including automotive, office, and hospital services. The current priority for the proposed architecture is to enhance its security. For instance, if a Zigbee device node that contains an URL to a proxy service bundle with malicious code is deployed, the home gateway and the entire home network may be in danger. Thus, it is essential to authenticate Zigbee device nodes and their proxy service bundles for the security of home network systems that are based on the proposed architecture.

## IX. FUTURE ENHANCEMENTS

As the development in the field of security we rely on providing one step further by sending the information to fire station from the place of occurrence of fire and information to police station if any intrusion occurs using GSM technology. Further enhancement is provided to our project by adding more appropriate sensors like magnetic detector and complete home monitoring systems so by which the system monitors the happenings.

## REFERENCE

1. Callaway, "ZigBee technology: wireless control that simply works," Proc. of communications Design Conference, Oct. 2003.
2.E.Kinney P. Gordy, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with IEEE 802.15.4
3.George.P.Franklin Zigbee Alliance, "Zigbee home automation public application profile version 1.0,"
4.Sun Liming, Li Jianzhong, Wireless sensor network [M], Beijing tsinghua university press, 2005

5.Zigbee Alliance, "Zigbee vision for the home: Zigbee wireless home automation," Zigbee Whitepaper, Nov. 2006.

**AUTHORS PROFILE:**

**R.Saravanan** is an Associate Professor in Department of Computer Science and Engineering at Saveetha Engineering College. He received his Master of Engineering in Computer Science and Engineering from Sathyabama University at 2005. He has 13 years of teaching experience from various Engineering Colleges during tenure he was Awarded **Best Teacher Award.** He is a Member of ISTE. He has 7 Papers in International and National Level conferences. His area of interest includes Data Mining, Computer Architecture, Object Oriented Programming, Operating Systems, Mobile computing and Database Management Systems.

**A.Vijayaraj** is an Associate Professor in Department of Information Technology at Saveetha Engineering College. He received his Master of Computer Application in Bharathidhasan University, in 1997 and his Master of Engineering in Computer Science and Engineering from Sathyabama University at 2005. He has 12 years of teaching experience from various Engineering Colleges during tenure he was Awarded **Best Teacher Award** twice.He is a Member of, CSI and ISTE. He has Published 2 papers In International journal 10 Papers in International and National Level conferences. His area of interest includes Operating Systems, Data Structures, Networks and Communication.