International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

# Zigbee: A High Speed Wireless Data Transfer Technology

**Ankita Khasanvis; Sonal Bansod & Prof. Dharmesh Dhablia**

## 1. Introduction:-

ZigBee is the most popular industry wireless mesh networking standard for connecting sensors, instrumentation and control systems. ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the "Internet of things." Theoretically, your ZigBee-enabled coffee maker can communicate with your ZigBee-enabled toaster. ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. ZigBee and IEEE 802.15.4 are low data rate wireless networking standards that can eliminate the costly and damage prone wiring in industrial control applications. Flow or process control equipment can be place anywhere and still communicate with the rest of the system. It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve.

The ZigBee RF4CE standard enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application profiles that can be used to create interoperable multi-vendor consumer electronic solutions. The benefits of this technology go far beyond, ZigBee applications include:

- Home and office automation
- Industrial automation
- Medical monitoring
- Low-power sensors
- HVAC control Plus many other control and monitoring uses


Figure 1: ZigBee Application

ZigBee targets the application domain of low power, low duty cycle and low data rate requirement devices. Figure below shows the example of a ZigBee network.

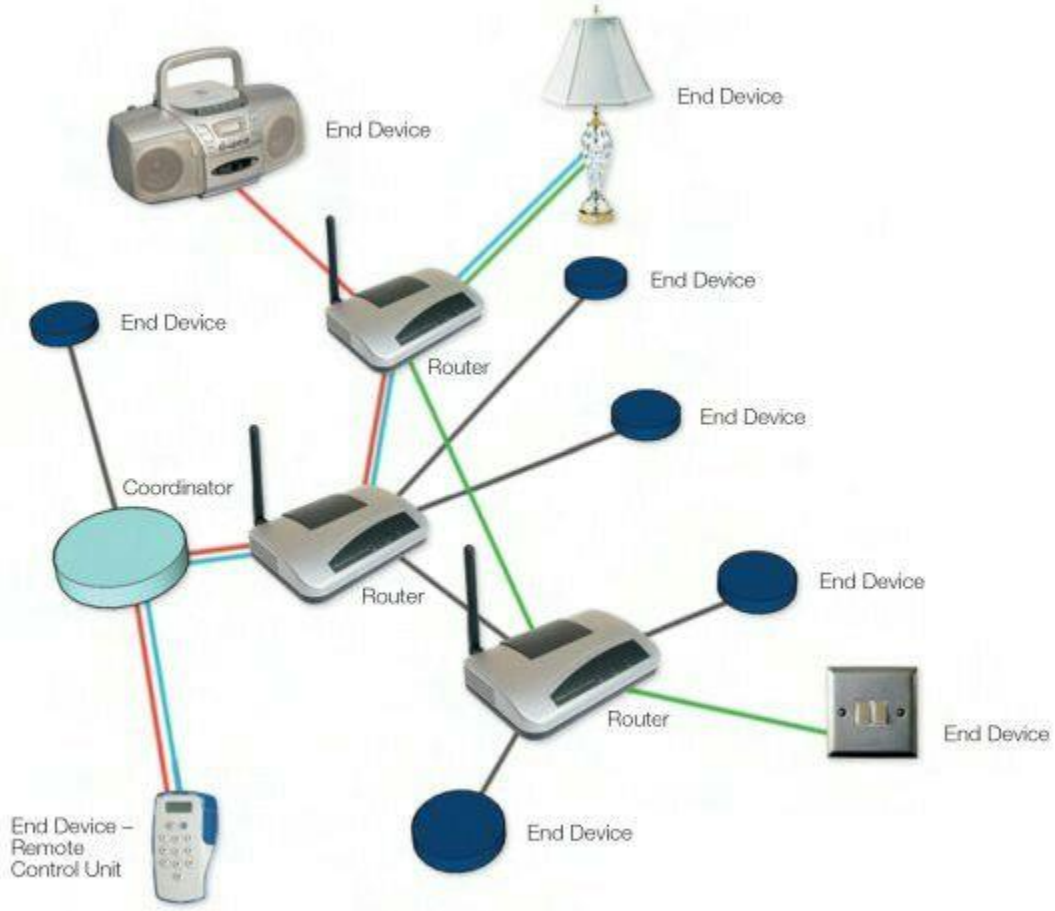


Figure 2: ZigBee Network

ZigBee is poised to become the global control/sensor network standard. It has been designed to provide the following features:

– Low power consumption, simply implemented – Users expect batteries to last many months to years – Bluetooth has many different modes and states depending upon your latency and power requirements such as sniff, park, hold, active, etc.; ZigBee/IEEE 802.15.4 has active (transmit/receive) or sleep – Even mains powered equipment needs to be conscious of energy. ZigBee devices will be more ecological than its predecessors saving megawatts at it full deployment.

Low cost (device, installation, maintenance)

Low cost to the users means low device cost, low installation cost and low maintenance. ZigBee devices allow batteries to last up to years using primary cells (low cost) without any chargers (low cost and easy installation). ZigBee's simplicity allows for inherent configuration and redundancy of network devices provides low maintenance.

High density of nodes per network

ZigBee's use of the IEEE 802.15.4 PHY and MAC allows networks to handle any number of devices. This attribute is critical for massive sensor arrays and control networks.

Simple protocol, global implementation

ZigBee's protocol code stack is estimated to be about 1/4th of Bluetooth's or 802.11's. Simplicity is essential to cost, interoperability, and maintenance. The IEEE 802.15.4 PHY adopted by ZigBee has been designed for the 868 MHz band in Europe, the 915 MHz band in N America, Australia, etc; and the 2.4 GHz band is now recognized to be a global band accepted in almost all countries.

## 2. ZIGBEE PROTOCOL ARCHITECTURE

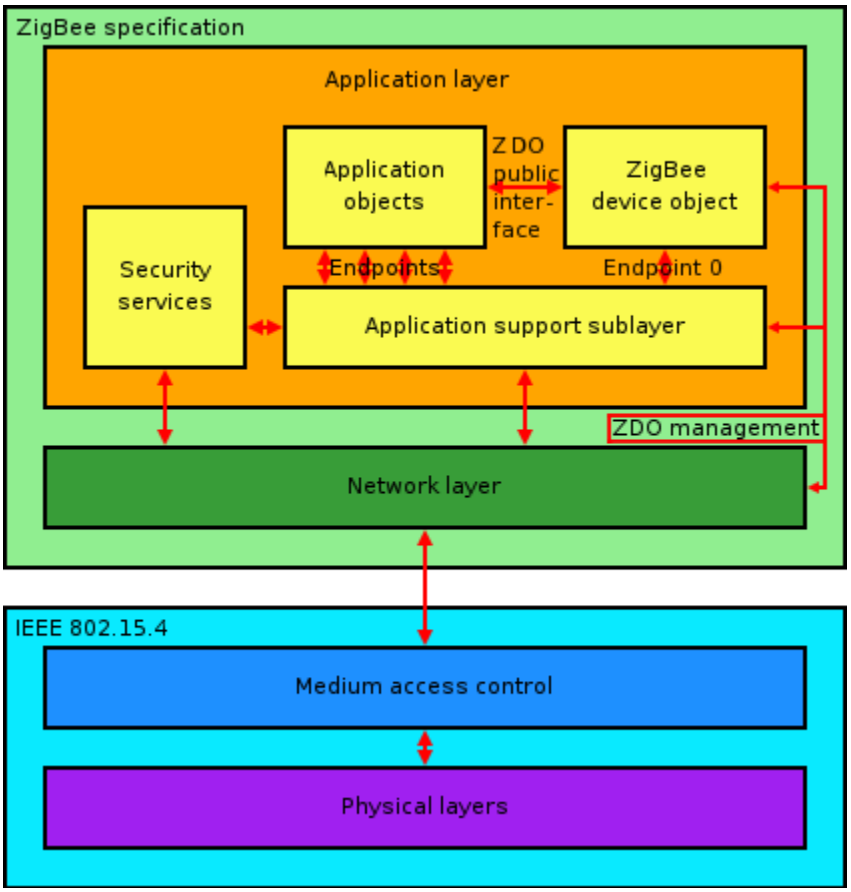


Figure 2: Zigbee protocol Architecture

### 2.1 Physical Layer

The physical layer of the IEEE802.15.4 standard is the closest layer to the hardware, which control and communicate with the radio transceiver directly. It handles all tasks involving the access to the ZigBee hardware ,including initialization of the hardware, channel selection, link quality estimation, energy detection measurement and clear channel assessment to assist the channel selection. Supports three frequency bands, 2.45GHz band which using16 channels, 915MHz band which using 10

channels and 868MHz band using 1 channel. All three using Direct Spread Spectrum Sequencing (DSSS) access mode.

PHY Packet Fields

• Preamble (32 bits) – synchronization • Start of Packet Delimiter (8 bits) • PHY Header (8 bits) – PSDU length • PSDU (0 to 1016 bits) – Data field •

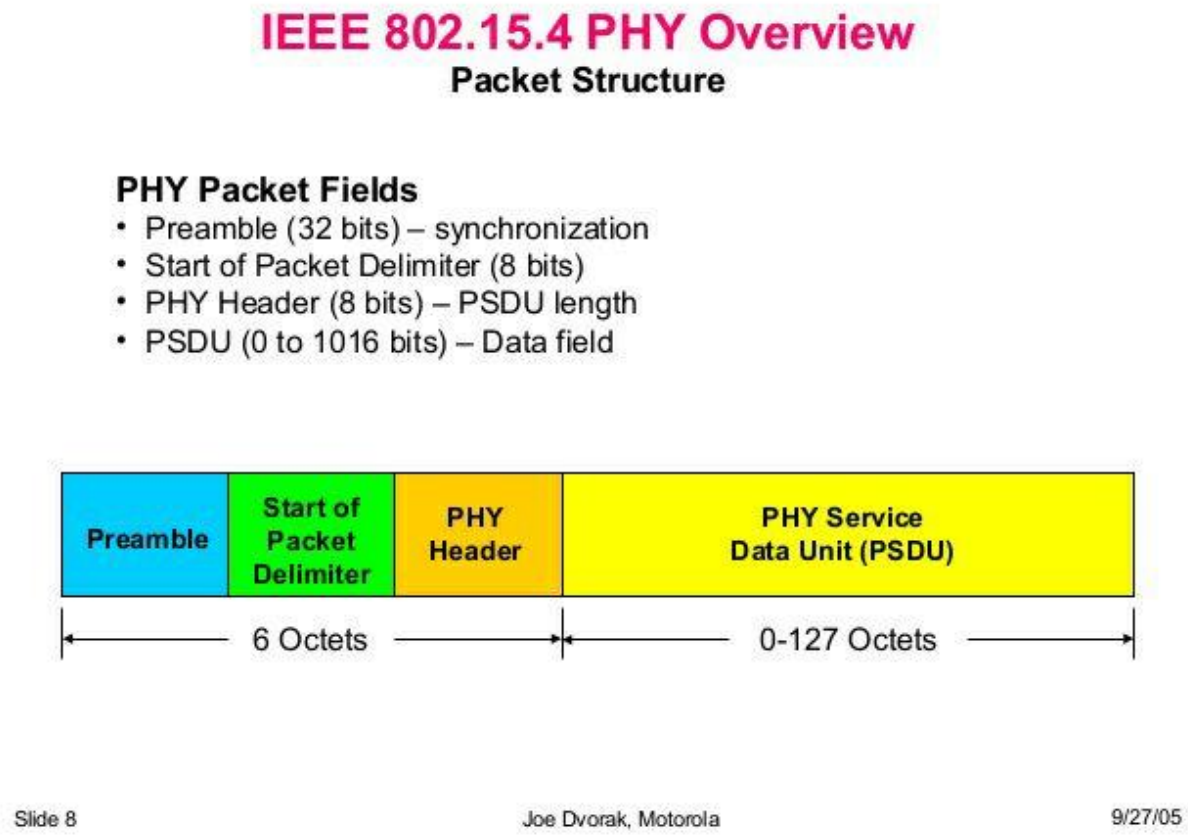


Figure 3: Packet structure

**2.2 MAC Layer**

This layer provides interface between physical layer and network layer. This provides two services; MAC data services and MAC management service interfacing to the MAC sub Layer Management Entity (MLME) Service Access Point called (MLME-SAP). The MAC data service enables the transmission and reception of MAC protocol Data Units (MPDUs) across the PHY data service. MAC layer is responsible for generating beacons and synchronizing devices to the beacon signal in a beacon enabled services. It is also performing association and dissociation function. It defines four frame structures, are Beacon frame, Data frame, Acknowledge frame, MAC command frame. Basically there are two types of topology; star and peer to peer. Peer to peer topology can take different shapes depends on its restrictions. Peer to peer is known as mesh, if there is no restriction. Another form is

tree topology. Interoperability is one of the advantages of ZigBee protocol stack. ZigBee has wide range of applications, so different manufacturer provides ZigBee devices. ZigBee devices can interact with each other regardless of manufacturer (even I if the message is encrypted).

**2.3 Network Layer**

Network layer interfaces between application layer and MAC Layer. This Layer is responsible for network formation and routing. Routing is the process of selection of path to relay the messages to the destination node. This forms the network involving joining and leaving of nodes, maintaining routing tables (coordinator/router), actual routing and address allocation. ZigBee coordinator or router will perform the route discovery. This layer Provides network wide security and allows low power devices to maximize their battery life. From the basic topologies, there are three network topologies are considered in IEEE802.15.4 are star, tree Network and mesh.

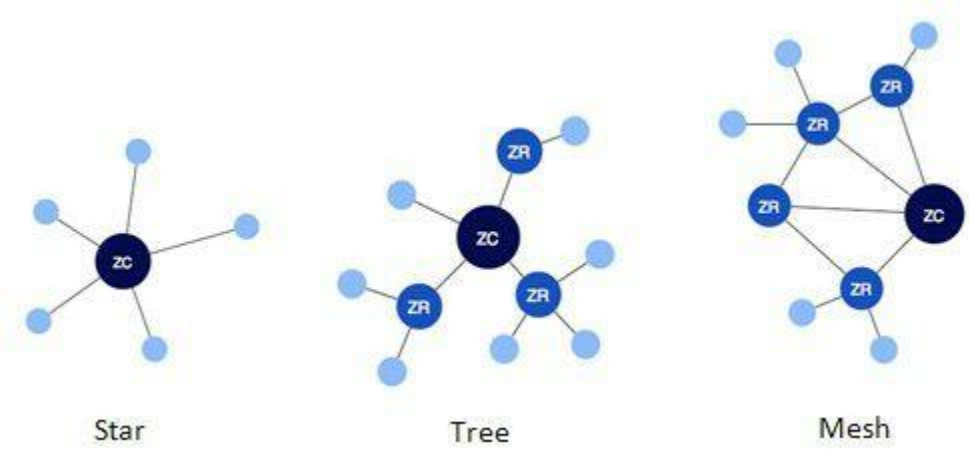


Figure 4: ZigBee topology

**2.4 Application Layer**

The application Layer is the highest protocol layer and it hosts the application objects. ZigBee specification separates the APL layer into three different sub-layers: the Application Support Sub layer, the ZigBee Device Objects, and Application Framework having manufacturer defined Application Objects.

**The application objects (APO) :** Control and manages the protocol layers in ZigBee device. It is a piece of software which controls the hardware. Each application objects assigned unique end point number that other APO's can use an extension to the network device address to interact with it [6]. There can be up to 240 application objects in a single ZigBee device. A ZigBee application must conform to an existing application profile which is accepted ZigBee Alliance. An application profile defines message formats and protocols for interactions between application objects. The application profile framework allows different vendors to independently build and sell ZigBee devices that can interoperate with each other in a given application profile.

**ZigBee Device Object:** The key definition of ZigBee is the ZigBee device object, which addresses three main operations; service discovery, security and binding. The role of discovery is to find nodes and ask about MAC address of coordinator/router by using unicast messages. The discovery is also facilitating the procedure for locating some services through their profile identifiers. So profile plays an important role. The security services in this ZigBee device object have the role to authenticate and derive the necessary keys for data encryption. The network manager is implemented in the coordinator and its role is to select an existing PAN to interconnect. It also supports the creation of new PANs. The role of binding manager is to binding nodes to recourses and applications also binding devices to channels .

**Application support sub layer:** The Application Support (APS) sub layer provides an interface between the NWK and the APL layers through a general set of services provided by APS data and management entities. The APS sub layer processes outgoing/incoming frames in order to securely transmit/receive the frames and establish/manage the cryptographic keys. The upper layers issue primitives to APS sub layer to use its services. APS Layer Security includes the following services: Establish Key, Transport Key, Update Device, Remove Device, Request Key, Switch Key, Entity Authentication, and Permissions Configuration Table.

**Security service provider:** ZigBee provides security mechanism for network layer and application support layers, each of which is responsible for securing their frames. Security services include methods for key establishment, key transport, frame protection and device management.

**3. How Zigbee Works?**

ZigBee basically uses digital radios to allow devices to communicate with one another. A typical ZigBee network consists of several types of devices. A network coordinator is a device that sets up the network, is aware of all the nodes within its network, and manages both the information about each node as well as the information that is being transmitted/received within the network. Every ZigBee network must contain a network coordinator. Other Full Function Devices (FFD's) may be found in the network, and these devices support all of the 802.15.4 functions. They can serve as network coordinators, network routers, or as devices that interact with the physical world. The final device found in these networks is the Reduced Function Device (RFD), which usually only serve as devices that interact with the physical world. As mentioned above several topologies are supported by ZigBee, including star, mesh, and cluster tree. As can be seen in above figure 3, star topology is most useful when several end devices are located close together so that they can communicate with a single router node. That node can then be a part of a larger mesh network that ultimately communicates with the network coordinator. Mesh networking allows for redundancy in node links, so that if one node goes down, devices can find an alternative path to communicate with one another.

**4. Wireless Communication**

All wireless communication systems have the following components:

- Transmitter
- Receiver
- Antennas

Path between the transmitter and the receiver

In short, the transmitter feeds a signal of encoded data modulated into RF waves into the antenna. The antenna radiates the signal through the air where it is picked up by the antenna of the receiver. The receiver demodulates the RF waves back into the encoded data stream sent by the transmitter.

**4.2 Wireless Network Types**

There are a number of different types of networks used in wireless communication. Network types are typically defined by size and location.

**4.2.1WPAN**

A wireless personal area network (WPAN) is meant to span a small area such as a private home or an individual workspace. It is used to communicate over a relatively short distance. The specification does not preclude longer ranges being achieved with the trade-off of a lower data rate. In contrast to other network types, there is little to no need for infrastructure with a WPAN.

Ad-hoc networking is one of the key concepts in WPANs. This allows devices to be part of the network temporarily; they can join and leave at will. This works well for mobile devices like PDAs, laptops and phones.

Some of the protocols employing WPAN include Bluetooth, ZigBee, Ultra- wideband (UWB) and IrDA. Each of these is optimized for particular applications or domains. ZigBee, with its sleepy, battery-powered end devices, is a perfect fit for wireless sensors. Typical ZigBee application domains include: agricultural, building and industrial automation, home control, medical monitoring, security and, lest we take ourselves too seriously, toys, toys and more toys.

**4.2.2 WLAN**

Wireless local area networks (WLANs) are meant to span a relatively small area, e.g., a house, a building, or a college campus. WLANs are becoming more prevalent as costs come down and standards improve.

A WLAN can be an extension of a wired local area network (LAN), its access point connected to a LAN technology such as Ethernet. A popular protocol for WLAN is 802.11, also known as Wi-Fi.

**4.2.3 WWAN**

A wireless wide area network (WAN) is meant to span a large area, such as a city, state or country. It makes use of telephone lines and satellite dishes as well as radio waves to transfer data.

**4.3 Wireless Network Topologies**

This section discusses the network topologies supported by the IEEE 802.15.4 and ZigBee specifications. The topology of a network describes how the nodes are connected, either physically or logically. The physical topology is a geometrical shape resulting from the physical links from node to node, as shown in the figure below. The logical topology maps the flow of data between the nodes.

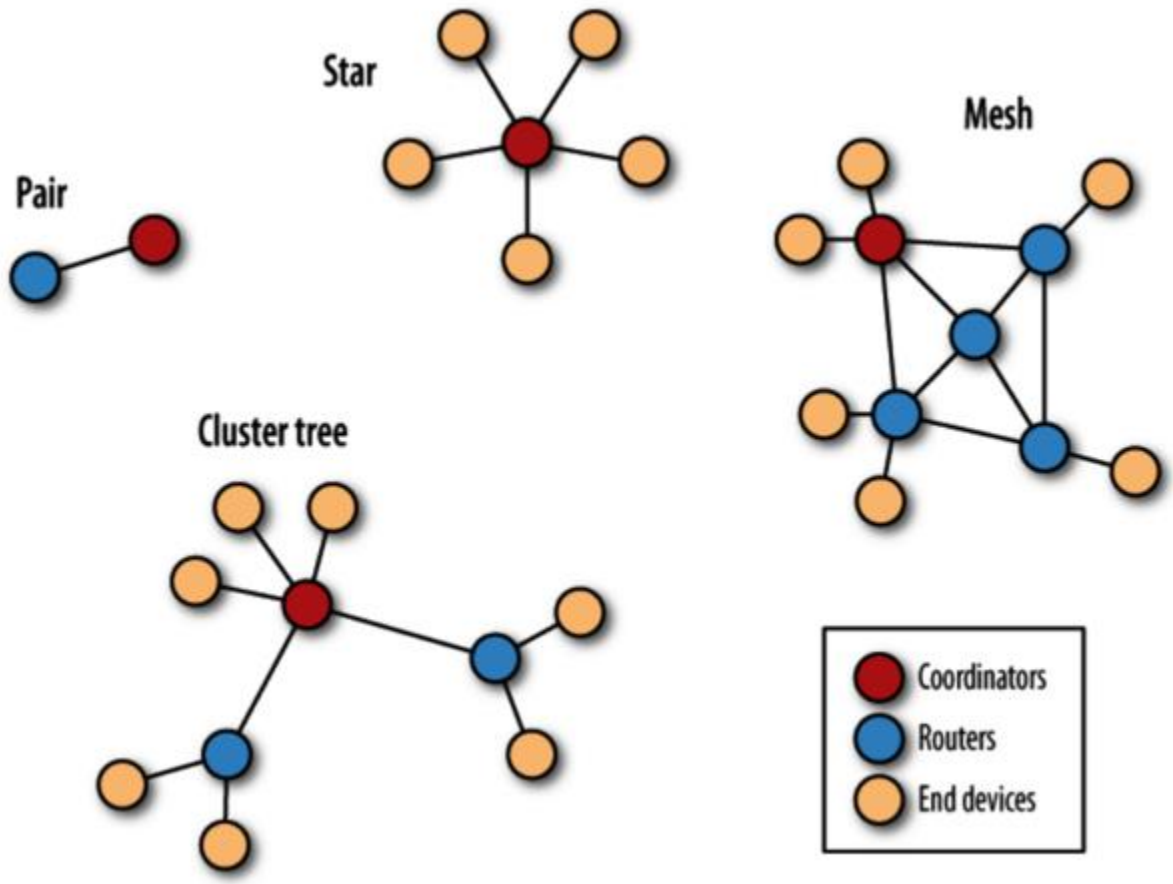


Figure 3: ZigBee Network Topology

IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree.

ZigBee-compliant devices are sometimes specified as supporting point-to- point and point-to-multipoint topologies.

**5.Security in a Wireless Network**

This section discusses the added security issues introduced by wireless networks. The salient fact that, signals are travelling through the air means that the communication is less secure than if they were travelling through wires. Someone seeking access to your network need not overcome the obstacle of tapping into physical wires. Anyone in range of the transmission can potentially listen on the channel.

Wireless or not, a network needs a security plan. The first thing to do is to decide what level of security is appropriate for the applications running on your network. For instance, a financial institution, such as a bank or credit union offering online account access would have substantially different security concerns than would a business owner offering free Internet access at a coffee shop.

**5.1 Security Risks**

After you have decided the level of security you need for your network, assess the potential security risks that exist.

- Who is in range of the wireless transmissions?
- Can unauthorized users join the network?
- What would an unauthorized user be able to do if they did join?
- Is sensitive data traveling over the wireless channel?

**6.REFRENCES**

[1] ZigBee Alliance, ZigBee Specification[z]. Version 1.0, http://www.ZigBee.org, 2005-06-27

[2] ShizhuangLin; JingyuLiu; YanjunFang; Wuhan Univ., Wuhan" ZigBee Based Wireless SensorNetworks and Its Applications in Industrial"IEEE International Conference on Automation and Logistics, 200718-21Aug.2007page(s):1979-1983Location:Jinan

[3] Zhou Yiming, Yang Xianglong, Guo Xishan, Zhou Mingang, Wang Liren ," A Design of Greenhouse Monitoring & Control System Based on ZigBee Wireless Sensor Network",IEEE journa1-4244-1312- 5/07 2007

[4] R Vishnubhotla, PS Rao, A Ladha, S Kadiyala, A Narmada, B Ronanki, S Illapakurthi ,"ZigBee Based Multi-Level Parking Vacancy Monitoring System" 978-1-4244-6875-10/2010 IEEE pg 2563-2566

[6] Dunfan Ye, Daoli Gong, Wei Wang,"Application of Wireless Sensor Networks in Environmental Monitoring"2nd International Conference on Power Electronics and Intelligent Transportation SystemIEEE2009pg 2563-2567

[7] Ankur Tomar- Global technology Centre,Volume 1 july 2011.