Zigbee Technology in Future Data Communication System

Sushila Gupta[1*]

ABSTRACT

As pervasive computing turns from the desktop model to the ubiquitous computing ideal, the development challenges become more complex than simply connecting a peripheral to a PC. A pervasive computing system has potentially hundreds of interconnected devices within a small area. This is not only a departure from the typical computer-peripheral model it is also a departure from the typical client-server model. ZigBee, based on IEEE 802.15.4, is an emerging standard within networked embedded systems. It has already been adopted by several major developers and the availability of devices and support systems is growing rapidly. This standard will become a foundation of future commonplace technologies. Topics in wireless mesh networking should be presented to Information Technology and Computer Engineering Technology students to ensure they are well-grounded in this emerging area. This paper describes an instructional module. It includes background information on the technology, the key concepts students must understand regarding ZigBee networking, the selection of a development environment, and the design of a hands-on lab experience. We briefly discuss the necessity of teaching this technology.

***Key words*:** Medium Access Control (MAC), Physical Layer (PHY), Wireless Personal Area Networking (WPAN), Open Systems Interconnection (OSI), ZigBee

1. INTRODUCTION

Wirless sensor networking (WSN) is a key technology for ubiquitous systems. The future widespread availability of wireless sensor networking requires application designers and embedded engineers to be familiar with it and its emerging standards. One such emerging standard is the recent protocol based on IEEE 802.15.4, called ZigBee.

ZigBee technology is a low date rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote applications. The market category ZigBee serves is called, "wireless sensor networking and control", or simply "wireless control". ZigBee is a standard networking protocol aimed at the wireless control market.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, 2.5 GHz in India, and 2.4 GHz in most jurisdictions worldwide. Data transmission rates vary from 20 to 900 kilobits/second. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory.

The reasons for using Zigbee are

- Reliable and self healing
- Supports large number of nodes.
- Easy to deploy
- Very long battery life
- Secure
- Low cost
- Can be used globally
- Vibrant industry support with thirty or more vendors supplying products and services
- Open Standards protocol with no or negligible licensing fees
- Chipsets available from multiple sources
- Remotely upgradeable firmware

1*. Sushila Gupta, Electronic and Communication, S.R.M.S.C.E.T. Bareilly, Uttar Pradesh (INDIA), e-mail : sushila.gupta784@gmail.com

- No new wires
- Low power
- Low maintenance

2. TRAFFIC TYPES

ZigBee/IEEE 802.15.4 addresses three typical traffic types. IEEE 802.15.4 MAC can accommodate all the types.

2.1 Data is periodic The application dictates the rate, and the sensor activates checks for data and deactivates.

2.2* Data is *intermittent The application, or other stimulus, determines the rate, as in the case of say smoke detectors. The device needs to connect to the network only when communication is necessitated. This type enables optimum saving on energy.

3. Data is repetitive, and the rate is fixed a priori. Depending on allotted time slots, called GTS (guaranteed time slot), devices operate for fixed durations.

ZigBee employs either of two modes, beacon or non-beacon to enable the to-and-fro data traffic. Beacon mode is used when the coordinator runs on batteries and thus offers maximum power savings, whereas the non-beacon mode finds favour when the coordinator is mains-powered.

In the beacon mode, a device watches out for the coordinator's beacon that gets transmitted at periodically, locks on and looks for messages addressed to it. If message transmission is complete, the coordinator dictates a schedule for the next beacon so that the device 'goes to sleep'; in fact, the coordinator itself switches to sleep mode.

While using the beacon mode, all the devices in a mesh network know when to communicate with each other. In this mode, necessarily, the timing circuits have to be quite accurate, or wake up sooner to be sure not to miss the beacon. This in turn means an increase in power consumption by the coordinator's receiver, entailing an optimal increase in costs.

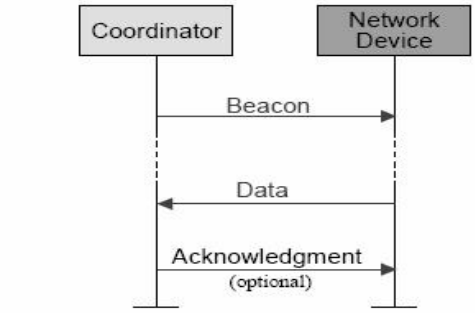

Fig. 1. Beacon Network Communication

The non-beacon mode will be included in a system where devices are 'asleep' nearly always, as in smoke detectors and burglar alarms. The devices wake up and confirm their continued presence in the network at random intervals.

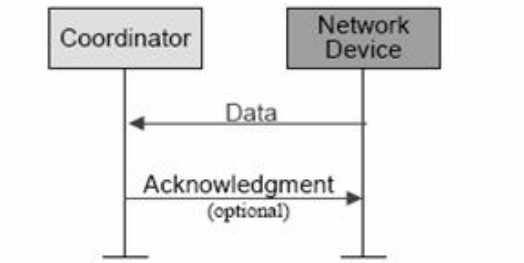

Fig. 2. Non-Beacon Network Communication

3. ARCHITECTURE

Protocol architecture is based on Open system interconnection (OSI). ZigBee builds on IEEE standard 802.15.4 which defines the physical and media access control (MAC) layers. ZigBee alliance defines the network layer and application layer. Fig. shows protocol stack of ZigBee system.

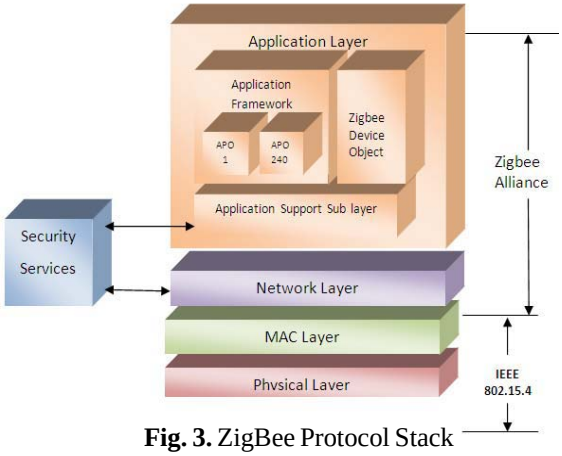

Fig. 3. ZigBee Protocol Stack

S-JPSET : ISSN : 2229-7111, Vol. 3, Issue 2

3.1 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 using 16 channels, 915MHz band which using 10 channels and 868MHz band using 1 channel. All three using Direct Spread Spectrum Sequencing (DSSS) access mode.

3.2 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 if the message is encrypted).

3.3 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, cluster tree and mesh.

3.4 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.

3.4.1 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. 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.

3.4.2 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.

3.4.3 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 299 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 Conguration Table.

3.4.4 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.

4. TOPOLOGIES

4.1 Star Topology

Star topology consists of one coordinator and any number of end devices. In star topology a master-slave network model is adopted where master is the ZigBee coordinator which is FFD and slave will be either FFD or RFD. ZigBee end devices are physically and electrically separated from each other end devices and pass information through coordinator. Devices can only communicate with the coordinator. This is does not provide multi-hop networking and mesh networking.

4.2 Cluster Tree Topology

The cluster tree topology is similar to the star topology. The difference is that other nodes can communicate with each other so that more RFD/FFDs can be connected to non-coordinator FFDs. The advantage of this topology is the possible geographical expansion of network.

4.3 Mesh Topology

In mesh topology, each node can communicate any other node within its range. Mesh topology is complex to maintain and beaconing is not allowed here. But it is more robust and tolerance to fault.

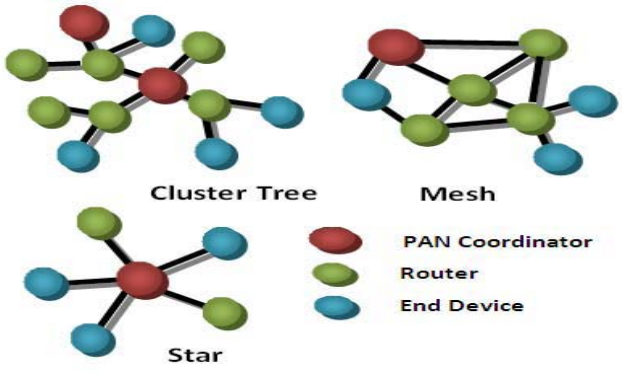

Fig. 4. Topologies

5. DEVICE TYPES

There are three categories of nodes in a ZigBee system. They are Coordinator, Router and End devices.

5.1 Coordinator

Forms the root of the network tree and might bridge to other networks. There is exactly one coordinator in each network. It is responsible for initiating the network and selecting the network parameters such as radio frequency channel, unique network identifier and setting other operational parameters. It can also store the information about network, security keys.

5.2 Router

Router acts as intermediate nodes, relaying data from other devices. Router can connect to an already existent network, also able to accept connections from other devices and be some kind of re-transmitters to the network. Network may be extended through the use of ZigBee routers.

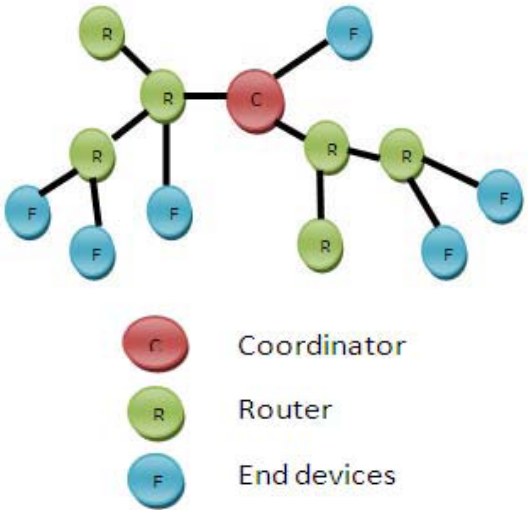

Fig. 5. ZigBee Network

5.3 End Devices

End Device can be low-power /battery-powered devices. They can collect various information from sensors and switches. They have sufficient functionality to talk to their parents (either the coordinator or a router) and cannot relay data from other devices. This reduced functionality allows for the potential to reduce their cost. They support better low power models. These devices do not have to stay awake the whole time, while the devices belonging to the other two categories have to. Each end device can have up to 240 end nodes which are separate applications sharing the same radio.

6. SECURITY

Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:

- Access control—the device maintains a list of trusted devices within the network.
- Data encryption, which uses symmetric key 128-bit advanced encryption standard.
- Frame integrity to protect data from being modified by parties without cryptographic keys.
- Sequential freshness to reject data frames that have been replayed—the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value.

The actual security implementation is specified by the implementer using a standardized toolbox of ZigBee security software.

7. CONCLUSION

Since there are no global standards so far in wireless sensor networks, the ZigBee plays vital role in most of the wireless application. In most industries it is observed, there is an increasing demand of ZigBee based wireless applications.

In terms of protocol stack size, ZigBee's 32 KB is about one-third of the stack size necessary in other wireless technologies (for limited capability end devices, the stack size is as low as 4 KB). The IEEE 802.15.4–based ZigBee is designed for remote controls and sensors, which are very many in number, but need only small data packets and, mainly, extremely low power consumption for long life.

REFERENCES

[1] ZigBee Alliance, ZigBee Specification. Version 1.0 ZigBee Document 053474r06, December 14th, 2004.

[2] P. Kinney, ZigBee Technology: Wireless Control that Simply Works, White Paper dated 2 October 2003.

[3] S.-W. Lee *et al.*, "802.11 TGs MAC Enhancement Proposal," IEEE 802 11-05/0589r0, June2005.

[4] *ZigBee Specification v1.0*, ZigBee Alliance, December 14th, 2004.

[5] Chen, B., Wu, M., Yao, S., & Binbin, N. (2006). ZigBee technology and its application on wireless meterreading system. *Industrial Informatics, 2006 IEEE International Conference on*, August 2006, 1257-1260.

[6] Xiuping Zhang; Guangjie Han; Changping Zhu; Yan Dou; Jianfeng Tao;" Research of Wireless Sensor Networks based on ZigBee for Miner Position", [J] International Symposium on Computer, Communication, Control and Automation, IEEE. 29 July 2010Pg1 - 5

[7] 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

[8] ShizhuangLin; JingyuLiu; YanjunFang; Wuhan Univ., Wuhan" ZigBee Based Wireless Sensor Networks and Its Applications in Industrial", IEEE International Conference on Automation and Logistics18-21Aug.2007Pg1979-1983.

