Role of ZigBee Technology in Wireless Networking

Himakshi, Deepak Sharma

Department of Computer Science and Engineering, RBIENT Hoshiarpur, Punjab, India
Department of Computer Science and Engineering, DBFGI Moga, Punjab, India

Abstract—*Zigbee technology is a kind of newly arisen wireless network technology has low frequency, short distance communication, low speed, low power consumption, and low cost, wireless mesh networking Technology. It, Application of Zigbee wireless communication technology, is Industrial control and monitoring sensor networks, building automation, home control and automation, toys and games etc. and With the rapid development of IT industry and the strong functional expansion of SCM, Zigbee wireless communication technology will play an important role in wireless sensor network (WSN). In this paper, Zigbee wireless communication technology and the process of establishing Zigbee network are introduced, the application of Zigbee wireless communication technology is studied in the real world. The ZigBee standard provides network, security, and application support services operating on top of the IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer (PHY) wireless standard. It employs a suite of technologies to enable scalable, self-organizing, self-healing networks that can manage various data traffic patterns.*

Keywords— Zigbee, Stack Protocols, Applications, Wireless Communication Techology.

I. INTRODUCTION

ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology is intended to be simpler and cheaper than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications which require a low data rate, long battery life, and secure networking.[4]

ZigBee is the wireless language that everyday devices use to connect to one another. In fact, ZigBee could be at work in your home right now. It is a mesh network specification for low-power wireless local area networks (WLANs) that cover a large area and was designed to provide high data throughput in applications where the duty cycle is low and low power consumption is an important consideration. (Many devices that use ZigBee are powered by battery.) Because ZigBee is often used in industrial automation and physical plant operation, it is often associated with machine-to-machine communication and the Internet of Things (IoT). ZigBee is based on the Institute of Electrical and Electronics Engineers Standards Association's 802.15 specification. It operates on the IEEE802.15.4 physical radio specification and in unlicensed radio frequency bands, including 2.4GHz, 900 MHz and 868 MHz. The specifications are maintained and updated by the ZigBee Alliance. There are three ZigBee pecifications: ZigBee, ZigBee IP and ZigBee RF4CE. ZigBee IP optimizes the standard for IPv6full mesh networks and ZigBee RF4CE optimizes the standard for partial mesh networks.[1]

ZigBee is a low data rate, two-way standard for home automation and data networks. The standard originates from the Firefly Working Group and provides a specification for up to 254 nodes including one master, managed from a single remote control. Real usage examples of ZigBee includes home automation tasks such as turning lights on, turn up the heat, setting the home security system, or starting the VCR. With ZigBee all these tasks can be done from anywhere in the home at the touch of a button. ZigBee also allows for dial-in access via the Internet for automation control.

The ZigBee standard uses small very low-power devices to connect together to form a wireless control web. A ZigBee network is capable of supporting up to 254 client nodes plus one full functional device (master). ZigBee protocol is optimized for very long battery life measured in months to years from inexpensive, off-the-shelf non-rechargeable batteries, and can control lighting, air conditioning and heating, smoke and fire alarms, and other security devices. The standard supports 2.4 GHz (worldwide), 868 MHz (Europe) and 915 MHz (Americas) unlicensed radio bands with range up to 75 meters.[2]

II. HISTORY OF ZIGBEE

Wi-Fi and Bluetooth were not good enough and suitable for some applications, it was decided to have ZigBee style networks in 1998, actually it was realized that need for self-organizing ad-hoc digital radio networks. There was a problem with Philips because Philips semiconductors stopped the investment. On the other hand, Philips lighting kept being a promoter member of ZigBee Alliance board of directors. Officially, ZigBee Alliance was announced in October 2004. It had more than 100 member companies almost all over the world. Also, number of members were increased almost double of previous years. In addition, next year (after December 2005), more than 200 companies became member which is quite high number.

Most importantly, ZigBee specification was approved on 14 December 2004 which is named as ZigBee 2004 Specification. After improvement, its public availability was announced 13 June 2005. In September 2006, ZigBee 2006 Specification was announced with member availability version. After all these developments, through the end of 2007, ZigBee PRO which is final version was announced. It contains enhanced ZigBee specification.[3]

The relationship between IEEE 802.15.4-2003 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The ZigBee 1.0 specification was ratified on December 14, 2004 and is available to members of the ZigBee Alliance. An entry level membership called Adopter, in the ZigBee Alliance costs US$ 3500 annually and provides access to the specifications and permission to create products for market using the specifications. For non-commercial purposes, the ZigBee specification is available to the general public at the ZigBee Specification Download Request. Most recently, the ZigBee 2006 specification was posted in December 2006. ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in countries such as USA and Australia, and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and cheaper than other WPANs such as Bluetooth. The most capable ZigBee node type is said to require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2%[citation needed]. However, actual code sizes are much higher, closer to 50% of Bluetooth code size. ZigBee chip vendors have announced 128-kilobyte devices.

III. ZIGBEE CHARACTERSTICS

The ZigBee core system consists of an RF transceiver and the protocol stack, which is depicted in Figure1. The system offers low rate services that enable the connection of possibly mobile low-complexity devices based on the carrier sensing multiple access with collision avoidance (CSMA/CA) channel access technique.

ZigBee physical layer The ZigBee physical layer operates in three different unlicensed bands with different modalities according to the geographical area where the system is deployed. However, direct sequence spread spectrum (DS-SS) is wherever mandatory to reduce the interference level in shared unlicensed bands.

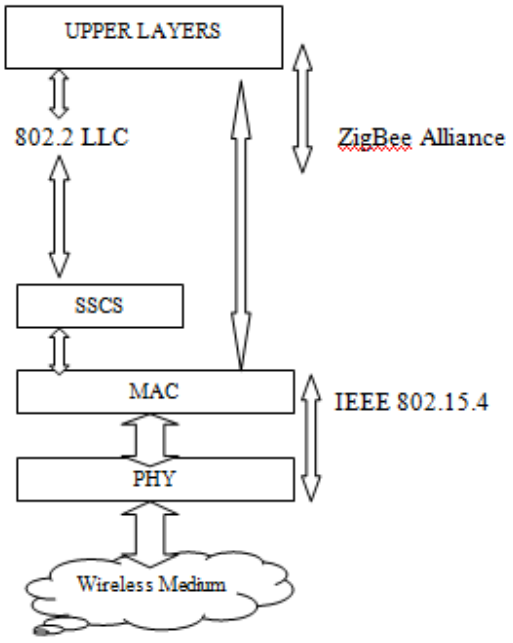

Fig.1: ZigBee Protocol Stack

The PHY layer provides the interface with the wireless medium. It is in charge of radio transceiver activation and deactivation, energy detection, link quality, clear channel assessment, channel selection, and transmission and reception of the message packets. Moreover, it is responsible for the establishment of the RF link between two devices, bit modulation and demodulation, synchronization between the transmitter and the receiver, and, finally, for packet level synchronization. Zigbee uses three frequency bands for transmission- 868 MHz band with a single channel has a raw data rate of 20 kb/s. The 915MHz band with 10 channels has each channel's central frequency separated from the adjacent band by 2 MHz and data rate of 40 kb/s. BPSK modulated symbols are transmitted at 1 bit per symbol using Direct Sequence Spread Spectrum (DSSS) technique with 15 bit chips. The 2.4 GHz ISM band with 16 channels, 5 MHz wide offers 250 kb/s data rate. It employs O-QPSK modulation with 4 bits/symbol transmitted using DSSS with 32 Bit chips. To reduce the transmitted power, the Zigbee transmitters use Energy Detection (ED) and Link Quality Indication (LQI). It

is the responsibility of the physical layer to perform channel assessment.[7]

MAC Layer Channel access is primarily through Carrier Sense Multiple Access- Collision Avoidance (CSMA-CA). On a node hop to hop basis, the MAC layer can take care of transmitting data. Depending on the mode of transmission, i.e. Beacon or Non-Beacon mode, the MAC layer decides whether to use slotted or unslotted CSMA-CA. The MAC layer takes care of scanning the channel, starting PANs, detecting and resolving PAN ID conflicts, sending beacons, performing device discovery, association and disassociation, synchronizing network device and realigning orphaned devices on the network. Along with this, the MAC layer also provides some standard security features like access control, encryption of data, duplicate rejection and frame integrity. Like in the case of the standard OSI MAC Layer, MAC layer in Zigbee also cannot take care of the situation when the nodes have intermediate nodes between them. This functionality of routing the packets to their destinations is provided in the network layer.[7]

The IEEE 802.15.4 specifications on PHY and MAC layer, the ZigBee Alliance defines the network layer and the framework for the application layer. The responsibilities of the ZigBee network layer include: mechanisms to join and leave a network, frame security, routing, path discovery, one-hop neighbours discovery, neighbour information storage. The ZigBee application layer consists of the application support sub-layer, the application framework, the ZigBee device objects, and the manufacturer-defined application objects. The responsibilities of the application support sub-layer include: maintaining tables for binding (defined as the ability to match two devices together based on their services and their needs) and forwarding messages between bound devices. The responsibilities of the ZigBee device objects include: defining the role of the device within the network (e.g., PAN coordinator or end device), initiating and/or responding to binding requests, establishing secure relationships between network devices, discovering devices in the network, and determining which application services they provide.[6]

IV. TRAFFIC TYPES

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

1. **Data is periodic**. The application dictates the rate, and the sensor activates checks for data and deactivates.
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.[8]

V. DEVICE TYPES

These devices have 64-bit IEEE addresses, with option to enable shorter addresses to reduce packet size, and work in either of two addressing modes – star and peer-to-peer. ZigBee networks use three device types:

- **ZigBee Coordinators (ZC)**: The most capable device, the Coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee Coordinator in each network since it is the device that started the network originally (the ZigBee Light Link specification also allows operation without a ZigBee Coordinator, making it more usable for over-the-shelf home products). It stores information about the network, including acting as the Trust Center & repository for security keys.[11][12]
- **ZigBee Router (ZR):** Running an application function, a Router can act as an intermediate router, passing on data from other devices.
- **ZigBee End Device (ZED)**: Contains just enough functionality to talk to the parent node (either the Coordinator or a Router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of

memory, and therefore can be less expensive to manufacture than a ZR or ZC.

VI. COMPARISON AMONG TECHNOLOGY

Different technologies, comprising Bluetooth, Zigbee and UWB among others, are compared in the following.[6]

1. **Zigbee** The nine promoter companies of the ZigBee Alliance include Philips, Honeywell, Mitsubishi Electric, Motorola, Samsung, BM Group, Chipcon, Freescale and Ember; then are more than 70 members:
   - Capacity of 250 Kbit/s at 2.4 GHz, 40 Kbit/s at 915 Mhz, and 20 Kbit/s at 868 Mhz with a range of 10–100 metres.
   - Its purpose is to become a wireless standard for remote control in the industrial field.
   - The ZigBee technology is targeting the control applications industry, which does not require high data rates, but must have low power, low cost and ease of use (remote controls, home automation, etc.).
   - Security was not considered in the initial development of the specification. Currently there are three levels of security.
   - It operates in the 3.2 – 10.2 GHz band.
   - ZigBee chips are low cost.

2. **Ultra Wideband:-** UWB is a revolutionary wireless technology for transmitting digital data over a wide spectrum of frequency bands with very low power. It can transmit data at very high rates (for WPAN applications).
   - It will have low power consumption, low price, high speed, use a wide swath of radio spectrum, carry signals through obstacles (doors, etc.) and apply to a wide range of applications (defense, industry, home, etc.).
   - Currently, there are two competing UWB standards for WPAN applications: the UWB Forum is promoting one standard based on direct sequence (DS-UWB), while the WiMedia Alliance is promoting another standard based on multiband OFDM.
   - Each standard allows for data rates from approximately 0 to 500 Mbps at a range of 2 metres and a data rate of approximately 110 Mbps at a range of up to 10 metres.
   - The Bluetooth SIG announced in May 2005 its intentions to work with both groups behind UWB to develop a high rate Bluetooth specification on the UWB radio.
   - For application to WSANs the standard proposed, which can be used as the PHY layer of the ZigBee protocol stack, is the IEEE 802.15.4a based on IR-UWB. It allows for typical data rate of 850 Kbit/s (up to 27 Mbit/s optional) with a range of 10 – 50 metres and location capability.

3. **Bluetooth Wireless Technology** Bluetooth wireless technology is geared towards voice and data applications.
   - It operates in the ISM unlicensed 2.4 GHz spectrum. Typically, it can operate over a distance of few metres (up to 10 metres, depending on the device class also up to 100 metres). The peak data rate with EDR is 3 Mbps.
   - It is omni-directional and in some conditions can work also in NLOS.
   - The Bluetooth specification allows for three modes of security.
   - The cost of Bluetooth chips is actually under 3USD.
4. **Infrared (IrDA)** IrDA is used to provide wireless connectivity for devices that would normally use cables to connect. IrDA is a point-to-point, narrow angle (30 cones), ad hoc data transmission standard designed to operate over a distance of 0 to 1 metre and at speeds of 9600 bps to 16 Mbps.
   - IrDA is not able to penetrate solid objects and has limited data exchange applications compared to other wireless technologies.
   - IrDA is mainly used in payment systems, in remote control scenarios or when synchronizing two PDAs with each other.
5. **Radio Frequency Identification (RFID)** There are over 140 different ISO standards for RFID for a broad range of applications.
   - With RFID, a passive or unpowered tag can be powered at a distance by a reader device. The receiver, which must be within a few feet, pulls information off the tag, and then looks up more information from a database. Alternatively, some tags are self-powered, active tags that can be read from a greater distance.
   - RFID can operate in low frequency (less than 100 MHz), high frequency (more than 100 MHz), and UHF (868 to 954 MHz).

- Uses include tracking inventory both in shipment and on retail shelves.

VII. SECURITY SERVICES

ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, cyphering frames and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies.[13]

Security Model: The ZigBee network model must take particular care of security considerations, as ad hoc networks may be physically accessible to external devices and the particular working environment cannot be foretold; likewise, different applications running concurrently and using the same transceiver to communicate are supposed to be mutually trustworthy: for cost reasons the model does not assume a firewall exists between application-level entities.

Within the protocol stack, different network layers are not cryptographically separated, so access policies are needed and correct design assumed. The open trust model within a device allows for key sharing, which notably decreases potential cost. Nevertheless, the layer which creates a frame is responsible for its security. If malicious devices may exist, every network layer payload must be ciphered, so unauthorized traffic can be immediately cut off. The exception, again, is the transmission of the network key, which confers a unified security layer to the network, to a new connecting device.

Security Architecture: ZigBee uses 128-bit keys to implement its security mechanisms. A key can be associated either to a network, being usable by both ZigBee layers and the MAC sub-layer, or to a link, acquired through pre-installation, agreement or transport. Establishment of link keys is based on a master key which controls link key correspondence. Ultimately, at least the initial master key must be obtained through a secure medium (transport or pre-installation), as the security of the whole network depends on it. Link and master keys are only visible to the application layer. Different services use different one-way variations of the link key in order to avoid leaks and security risks.

Key distribution is one of the most important security functions of the network. A secure network will designate one special device which other devices trust for the distribution of security keys: the trust center. Ideally, devices will have the trust center address and initial master key preloaded; if a momentary vulnerability is allowed, it will be sent as described above. Typical applications without special security needs will use a network key provided by the trust center (through the initially insecure channel) to communicate.

Thus, the trust center maintains both the network key and provides point-to-point security. Devices will only accept communications originating from a key provided by the trust center, except for the initial master key. The security architecture is distributed among the network layers as follows:

- The MAC sub-layer is capable of single-hop reliable communications. As a rule, the security level it is to use is specified by the upper layers.
- The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.
- The application layer offers key establishment and transport services to both ZDO and applications. It is also responsible for the propagation across the network of changes in devices within it, which may originate in the devices themselves (for instance, a simple status change) or in the trust manager (which may inform the network that a certain device is to be eliminated from it). It also routes requests from devices to the trust center and network key renewals from the trust center to all devices. Besides this, the ZDO (ZigBee Device Object) maintains the security policies of the device.

VIII. SECURITY ISSUES

Zigbee communicates via a wireless RF network, it is vulnerable to the same attacks as a tradition 802.11 network. Though, the alliance has done much work in making the network safe by implementing AES 128 bit encryption (Zigbee 2006). Atmel Corporation has added additional encryption to its Zigbee compatible products by providing an onboard crypto engine which also increases the speed of the AES encryption by up to ten times (Atmel, 2011). Despite these efforts, Zigbee is vulnerable in two ways: stealing the cryptographic key and packet capture (Radmand, unk). The cryptographic key can be stolen by either a remote or physical attack and packets can be captured for the purposes of eavesdropping, spoofing, replaying, and denial of service attacks (Radmand, unk). Keeping this in mind, a homeowner would need to consider what devices he/she hooks up to the Zigbee network with the same prudence given to what kind of information he/she would send across his/her wireless home computer network.[14]

IX. CONCLUSION

ZigBee Technology has presented many features which are highlighted in this paper. Although the ZigBee has a lots of applications, we limit this effort only to its application in WHAS. The performances of the ZigBee based WHAS have been compared with those of other competing technologies including UWB, RFIDe, IrDA, Insteon, Waveins, WiFi, and Bluetooth. Zigbee is bright; companies are jumping on the Zigbee bandwagon left and righ, just like the startup company Tendril networks that introduced its Zigbee compliant home energy monitor network (LaMonica, 2008). This protocol is so adaptable, the possibilities for application is extending quickly outside the home, in the healthcare realm, and other industries. Anyplace where RF transmitters and receivers can be placed may take advantage of the Zigbee wireless network protocol.

REFERENCES

[1] http://www.zigbee.org/what-is-zigbee
[2] http://searchmobilecomputing.techtarget.com/definition/ZigBee
[3] http://sercolaywireless.blogspot.in/2011/06/history-of-zigbee-alliance.html
[4] http://www.zigbees.com/
[5] http://www.ieee802.org/15/pub/TG4.html
[6] http://www.zigbee.org/en/index.asp
[7] http://www.engineersgarage.com/articles/what-is-zigbee-technology?page=3
[8] http://www.jatit.org/volumes/researchpapers/Vol5No2/5Vol5No2.pdf
[9] http://:www.zigbee.org/en/resources
[10] http://www.zigbee.org/en/resources
[11] "Wireless Sensor Networks Research Group". Sensor-networks.org. 2010-04-15. Retrieved 2012-10-18.
[12] "Wireless Sensor Networks Research Group". Sensor-networks.org. 2009-02-05. Retrieved 2012-10-18.
[13] https://en.wikipedia.org/wiki/ZigBee
[14] https://sites.google.com/site/zigbeewirelessmeshprotocol/home/security-issues
[15] ZigBee Document 053474r06, Version 1.0, ZigBee Specification. ZigBee Alliance. 2004.
[16] "IEEE 802.15.4". Ieee 802. Retrieved 2012-10-18.
[17] "ZigBee Wireless Networking", Drew Gislason (via EETimes)
[18] "ZigBee Specification FAQ". *Zigbee Alliance*. Retrieved 14 June 2013.
[19] "The ZigBee Alliance". Zigbee. Retrieved 2012-10-18.