Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 12, December -2017

Comparative Analysis Of Zigbee With Other Wireless Technologies - Survey

Komal D. Langalia[1]

[1]*Computer Science and Engineering, LD College Of Engineering, Ahmedabad*

Abstract — *Wireless communication includes different protocol standards for short range of connectivity such as Bluetooth, Wi-Fi, UWB, Zigbee etc. but they differ from an application point of view. In this paper we will evaluate the behavior and performance of these wireless communication standards in terms of different aspects. Here we will focus that how Zigbee is more useful than other wireless sensor network (WSN). This paper will also discuss about the basic architecture and security analysis of Zigbee. It is believed that the comparison presented in this paper would benefit application engineers in selecting an appropriate protocol for the specific task.*

Keywords *- Zigbee; Bluetooth; Wi-Fi; Wireless Sensor network; Short-range communication*

I. INTRODUCTION

From last few years, factory automation has been developed as one of the most attractive research area. Factory automation includes different modern disciplines such as communication, information, control and sensor etc. in integrated way. Integration of computer and actuator engineering with other disciplines leads to new solution, higher throughput, less complex & complete systems with better performance. Among all other components industrial communication is increasingly important component of factory automation [1]. For interconnection purposes, a factory automation system can be combined with various sensors, controllers, and heterogeneous machines using a common message specification. There exist different wireless networks to support short range wireless communication but selecting a most suitable network to achieve higher performance for a particular application is a critical issue to the industrial engineers. Zigbee style network became more attractive field of research when many installers realized that the technologies like Wi-Fi, Bluetooth, and UWB were going to be unsuitable for many applications because many network engineers saw the need for self-organizing ad-hoc digital radio network [2]. In particular, ZigBee over 802.15.4 standard can meet a wider variety of real industrial needs than Bluetooth and Wi-Fi due to its long-term battery operation, low data rate, greater useful range, flexibility in number of dimensions, self-healing capabilities and reliability in architectures like mesh networks.

II. COMPARATIVE STUDY OF EXISTING TECHNOLOGIES

2.1. The Existing Technology and Scheme

With the constant development of communication technology, all kinds of short-range wireless communication technologies are being innovated continuously.

Bluetooth is the open standard for short range radio frequency which is used as replacement of cable for many business and consumer devices. It provides a universal short range wireless capability. Bluetooth provide radio link power control for negotiating the radio link according to its signal strength measurement. The operating range for Bluetooth changes according to its power length from 1m to 100 m. Like for USB adapters, access points it is 100m, for mobile devices smart card readers it is up to 10m and for some Bluetooth adapters it is up to 1m. Bluetooth occupy a section of the 2.4 GHz ISM band that is 83 MHz-wide. So Interference is possible. Bluetooth operates Frequency Hopping Spread Spectrum (FHSS) and is allowed to hop between 79 different 1 MHz-wide channels in this band at a rate of 1600hops/s to avoid any interference. Bluetooth uses AFH (Adaptive Frequency Hopping) which classifies good and bad channels so that bad channels are avoided and replaced by pseudo randomly selecting out of the remaining good or free channels.

Wi-Fi [3] (Wireless Fidelity), namely IEEE 802.11 protocol, is a kinds of short-range wireless transmission technology capable to support the internet accessed radio signal within a few hundred feet. It has been developed to enable wireless local area networking in either the 2.4 GHz or 5.2 GHz ISM bands. The MAC and PHY layers are defined in the first version of Wi-Fi, published in 1997. The PHY is adopted with infrared, DSSS or FSSS technology. Its maximum transmission rate could reach 54Mb/s and it is widely capable to support data, image, voice and multimedia and other businesses. There are many security methods available, which is used to prevent Wi-Fi from unauthorized access or security threat such as Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) and WPA.

2.2. Shortcomings of the Existing Technologies

Although Bluetooth and Wi-Fi technologies avoid the barrier of data transmission, makes low-power design, and the communication distance reaches to the higher range, their defects are still obvious and they're not suitable for smart home design. Their defects are mainly shown in the following three aspects:

1. Inadequate anti-interference capability
2. Poor self-organized networking
3. Inadequate security [4].

Table 1. Comparative study of Bluetooth, Zigbee and Wi-Fi

	BLUETOOTH	ZIGBEE	WI-FI
FREQUENCY BAND	2.4 GHz	868/915 MHz; 2.4 GHz	2.4 GHz; 5.2 GHz
MAX SIGNAL RATE	1 Mb/s	250 Kb/s	54 Mb/s
NOMINAL RANGE	10m	10 - 100 m	100 m
NUMBER OF RF CHANNELS	79	1/10; 16	14 (2.4 GHz)
CHANNEL BANDWIDTH	1 MHz	0.3/0.6 MHz; 2 MHz	22 MHz
MODULATION TYPE	GFSK	BPSK (+ ASK), O-QPSK	BPSK, QPSK COFDM, CCK, M-QAM
SPREADING	FHSS	DSSS	DSSS, CCK, OFDM
COEXISTENCE MECHANISM	Adaptive freq. hopping	Dynamic freq. selection	Dynamic freq. selection, transmit power control (802.1 1 h)
BASIC CELL	Piconet	Star	BSS
EXTENSION OF THE BASIC CELL	Scatternet	Cluster tree, Mesh	ESS
MAX NUMBER OF CELL NODES	8	> 65000	2007
ENCRYPTION	EQ stream cipher	AES block cipher (CTR, counter mode)	RC4 stream cipher (WEP), AES block cipher
AUTHENTICATION	Shared secret	CBC-MAC (ext. of CCM)	WPA2 (802.11i)
DATA PROTECTION	16-bit CRC	16-bit CRC	32-bit CRC
POWER PROFILE	Days	From months to years	Hours
LATENCY	Enumeration up to seconds	Enumeration 30ms	Enumeration up to 3 seconds
EXTENDIBILITY	No	Yes	Roaming possible

III. ZIGBEE OVER IEEE 803.15.4

ZigBee is IEEE 802.15.4 wireless PAN standard for short range wireless communication. Compared with other wireless communication technology, Zigbee has the following technological advantages:
(1) Low-power dissipation.
(2) Low cost
(3) Low rate
(4) Short time delay
(5) High security
(6) Self-Healing capability
(7) High density of network
(8) Greater Battery Life
(9) Simple protocol with global implementation

These advantages make ZigBee popular in wireless automation systems at industries and homes where remote monitoring and controlling is used, including smart home automation, Smart Energy, Telecommunication Application, Personal Home, Hospital care. Applications also include wireless light switches, electrical meters with in-home-displays, traffic management systems, and other consumer and industrial equipment that requires short-range wireless transfer of data at relatively low rates for longer distance. Zigbee provides wider range for research in the field of wireless sensors and control networks.

The key component of ZigBee is its ability to support mesh networking. ZigBee devices are often used in mesh network form to transmit data over longer distances, passing data through intermediate devices to reach more distant ones, which provides it larger range. In mesh networking communicating nodes make multiple pathways by interconnecting with other nodes. Connections between nodes are dynamically updated and optimized through sophisticated, built-in mesh routing table. Mesh networks are decentralized in nature; each node is capable of self-discovery on the network. Also, as nodes leave the network, the mesh topology allows the nodes to reconfigure routing paths based on the new network structure. There for mesh topology and ad-hoc routing have greater stability in changing conditions or failure at single nodes. These features of mesh network provide self-healing capability and more reliability to ZigBee than other wireless standards. The low cost allows it to be widely deployed in wireless control and monitoring and low power consumption allows it to have longer life with smaller batteries [1].

3.1. Characteristics of Zigbee

(1) Frequency agile solution operating over 16 channels in the 2.4GHz frequency
(2) Incorporates power saving mechanisms for all device classes
(3) Discovery mechanism with full application confirmation
(4) Pairing mechanism with full application confirmation
(5) Multiple star topology and inter-personal area network (PAN) communication
(6) Various transmission options including broadcast
(7) Security key generation mechanism
(8) Ease of deployment

3.2. Types of Zigbee devices

3.2.1 ZigBee coordinator (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. Communication between computer and ZigBee can be achieved through co-ordinate. Two types of co-ordinate are available AT and API. AT uses terminals like AT commands to communicate with ZigBee. API uses bytes and checksums to communicate with ZigBee. It stores information about the network, including acting as the Trust Center & repository for security keys.

3.2.2 ZigBee Router (ZR)

As well as running an application function, a router can act as an intermediate router, passing on data from other devices. It is mainly used to extend the network range. It can also act as ZED. It has two methods of routing. Mesh routing and Tree routing. Mesh router is used as extender for wireless monitors to allow transmission and receipt of monitor readings. It is also used for finding the optimal location for monitors. Up to 3 mesh routers can be combined to extend communication range.

3.2.3 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. It is responsible for requesting pending messages from its parent and also for finding and joining the correct network. It also helps in finding new parent if old parent is lost. ZigBee end device is portable. 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 [5] [2].

3.3. Zigbee Architecture

ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60 KB and 256 KB flash memory. Specifications for Zigbee lay down standards for the Physical and MAC layers.

3.3.1 PHY Layer

It is designed to accommodate the need for low cost yet allowing for high level of integration. The use of DSSS allows the analog circuitry to be very simple and very tolerant towards inexpensive implementations.

3.3.2 MAC Layer

It is designed to allow multiple topologies without complexity. The power management operation doesn't require multiple modes of operation. The MAC allows a reduce functionality device (RFD) that needn't have flash nor large amounts of ROM or RAM. The MAC is designed to handle large numbers of devices without requiring them to be "parked". The network layer has been designed to allow the network to spatially grow without requiring high power transmitters. The network layer also can handle large amounts of nodes with relatively low latencies.

The protocol stack is completed by adding ZigBee's own Network Layer (NWK) and Application Layer (APL) on top of PHY and MAC. Drawing analogies from the OSI protocol stack simplifies the study of ZigBee protocol.

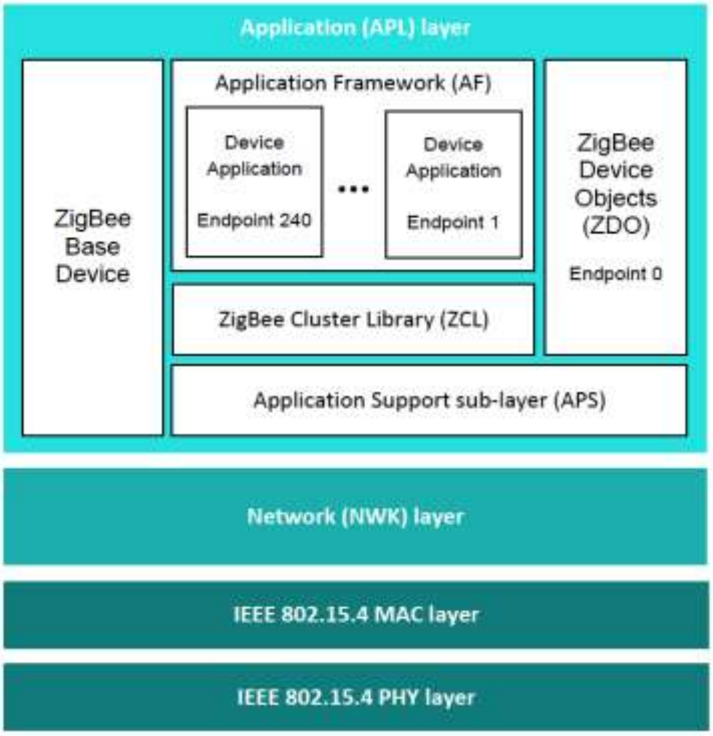

Figure 1. Zigbee architecture

3.4. How ZigBee works?

ZigBee operates in 16 channels of 2.4GHz unlicensed ISM band and provides a data rate of 250 Kbps. It has been designed for single channel 868 MHz, which provides 20 kbps in Europe. ZigBee device can function either as a node or a coordinator. A node is like a client or slave device that receives commands/data from a coordinator. A node cannot initiate connection with another node. The coordinator device is the master or the slaved device that can control up to 255 active nodes. The networking and message routing is used to enhance the performance of the application. ZigBee devices can form PAN using: star, cluster tree or mesh topology. Multi network coordinators can be linked together to form a large network to control up to 65536 devices. The air interface is direct sequence spread spectrum (DSSS) using BPSK for 868 MHz and 915 MHz and O-QPSK for 2.4 GHz. The access method in IEEE 802.15.4-enabled networks is carrier sense multiple access with collision avoidance (CSMA-CA). Profile will provide highly inter operable products and solutions [2].

ZigBee Alliance is a group of more than 300 companies including industry majors like Philips, Mitsubishi Electric, Epson, Atmel, Texas Instruments etc. which are committed towards developing and promoting this standard. The alliance is responsible for publishing and maintaining the ZigBee specification and has updated it time and again. The manufacturers which are members of the Alliance provide software, hardware and reference designs to anyone who wants to build applications using ZigBee.

3.5. Security

Zigbee claims to provide state-of-art security tools allowing its member companies to create some of the most secure IOT devices. Symmetric-key cryptography is used in Zigbee where same keys are shared between two communicating parties. 128-bit advanced encryption standards (AES) based encryption will enable highly secure networks and applications[7].

3.5.1. Security Architecture

As mentioned before, Zigbee builds NWK and APL layers on top of the IEEE 802.15.4 PHY and MAC layers. The APL layer includes Application Support (APS) sublayer, the Zigbee Device Object (ZDO), and applications. The ZDO is responsible for managing the security policies and the security configuration of a device. The APS layer provides a foundation for servicing ZDO and Zigbee applications. The architecture includes security mechanisms at three layers of the protocol stack: the MAC, NWK, and APS layers.

Even though Zigbee was designed with the importance of security in mind, there have been tradeoffs made to keep the devices low-cost, low-energy and highly compatible. Some parts of the standard's security controls are poorly implemented, which inevitably lead to security risks.

3.5.2. Recommendations

Here some recommendations are listed to improve the security of Zigbee over the different attacks [6]
Out-of-band key loading method
Secure network admission
Dynamic device ID rotation

IV. CHALLENGES DESIGNING ZIGBEE TECHNOLOGY

However, there are still some challenges in designing ZigBee-based home network system and applications. Firstly, according to the current situation, the ZigBee-based service terminals need to provide the total solution to improve the integrated efficiency. Meanwhile, the ZigBee module will be used as a supplementary means of integration. Secondly, the ZigBee-based service node uses a limited power resource, such as a battery. Thus, the network lifetime is greatly influenced by the battery lifetime. Last but in no means least, compared with the ZigBee network itself, users are more concerned about the visual perception. For example, how to effectively monitor model, and manage monitoring processes is a critical task for current situation.

V. CONCLUSION

This paper has presented a broad overview of the three most popular wireless standards, Bluetooth, ZigBee, and Wi-Fi with a quantitative evaluation in terms of the transmission time, data coding efficiency, protocol complexity, and power consumption. Furthermore, the radio channels, coexistence mechanism, network size, and security are also preliminary compared. This paper shows that suitability of network protocols is greatly influenced by practical applications, of which many other factors such as the network reliability, roaming capability, recovery mechanism, chipset price, and installation cost need to be considered in the future. ZigBee has a great deal to offer in industrial automation applications such as low cost deployment and redeployment, mesh networking to cover entire industrial plants and factories, an open standard with multiple vendors, battery operation. The different ZigBee products are designed to function and survive in industrial settings like high RF noise floor, temperature extremes, rough handling. At last this paper shows some security tradeoffs in Zigbee technology and the recommendations against different attacks.

REFERENCES

[1] R. Zurawski, "Guest editorial of special section on factory communication systems," IEEE Trans. Ind. Electron., vol. 49, no. 6, pp.1186-1188, Dec. 2002.

[2] Akshay Kanwar, Aditi Khazanchi, “Zigbeee : The New Bluetooth Technology”, International Journal Of Engineering And Computer Science ISSN:2319-7242,page no 3,4 , 2012.

[3] K. Lian, “Intelligent multi,-sensor control system based on innovative technology integration via ZigBee and Wi-Fi networks”, Elsevier, (2013), p. 2.

[4] J. Peng, “Research and Design of Bluetooth Home Control Network”, Journal of Dalian University of Technology, **(2006)**, p. 1.

[5] http://en.wikipedia.org/wiki/ZigBee

[6] Xueqi Fan, Fransisca Susan, William Long, Shangyan Li, “Security analysis of Zigbee”, 2017

[7] Inc. Zigbee Alliance, Zigbee 3.0 Stack User Guide JN-UG-3113 (October 5, 2016).