ISSN 2350-1022

International Journal of Recent Research in Mathematics Computer Science and Information Technology
Vol. 8, Issue 1, pp: (23-33), Month: April 2021 – September 2021, Available at: www.paperpublications.org

Wireless Personal Area Network (WPAN) Bluetooth and ZigBee Survey

Abbas Atwan Mhawes

Ministry of Education 10065 Al Tarbawi,
Collection, Baghdad, 10001, Iraq

Abstract: **A wireless personal area network (WPAN) is a personal network, which is a network for interconnecting devices centred on an individual person's workspace, in which the connections are wireless. The WPAN introduced many different standards that depend on WPAN to work. In this paper, I concentrate on two of them, which are Bluetooth and ZigBee. I described their protocol stack, how they work, and at the end of this paper I made a comparison between these two standards in many different features. It is believed that the comparison presented in this paper would benefit application engineers in selecting an appropriate protocol.**

Keywords: **WPAN, Bluetooth, ZigBee.**

I. INTRODUCTION

The Wireless Personal Area Network (WPAN) is a personal area network using wireless to communicate within a small distance. Wireless Personal Area Network is based on the standard IEEE 802.15. The IEEE 802 committee designed a new standard for the Personal Area Networks at the end of the nineteenth of the last century. This new standard selected -802.15- working group for the Wireless Personal Area Networks (WPAN). This new technology has used to connect devices that using wireless for communication such as laptops, cell phones and many other devices. This technology is so easy to work, it just wants two or more devices to be close to each other and then they can communicate as they have a cable between them. In addition, it gives these devices the ability to choose the device that they want to communicate with, and this leads to prevent from the unauthorized access to the devices. The WPAN has many different standards. Bluetooth and ZigBee are two types of these standards that belong to WPAN. Bluetooth is a technology that uses wireless to send and receive information over small distance -10 meters-without needing wires and it has the standard 802.15.1. It uses a radio frequency to send and receive on a short-range network, and it is very secure to connect devices such as cell phones. Bluetooth is a good chose for sending files without using wires. Also, this paper talks about ZigBee technology, which has the standard 802.15.4 and it is a technology that works for low power radio waves Wireless Personal Area Network. ZigBee uses to create a network with energy efficiency. In addition, it covers a distance from 10 to 100 meters.

II. THE BLUETOOTH

Bluetooth is a wireless technology standard for exchanging data over short distances, 10 meters, using radio waves for this purpose, and it has been used for fixed and mobile devices.

III. HISTORY OF BLUETOOTH

Ericsson company was invented Bluetooth in 1994. Bluetooth took its named after King Harald Blaatand (Bluetooth), king of Denmark 940–981 A.D. Ericsson, IBM, Toshiba, Nokia, and Intel founded the Bluetooth Special Interest Group (SIG) in February 1998 to develop an open specification for short-distance wireless connectivity. 3COM, Microsoft, Lucent, and Motorola now also promote the group. Thousands of companies have joined the SIG. The following sections describe some things about Bluetooth such as the Bluetooth stack and how Bluetooth communicate some security aspects for Bluetooth [1].

IV. BLUETOOTH PROTOCOL OVERVIEW

The Bluetooth protocol stack divides into three logical groups. They are the Transport Protocol group, the Middleware Protocol group and the Application group [2]. As shown in Figure 1

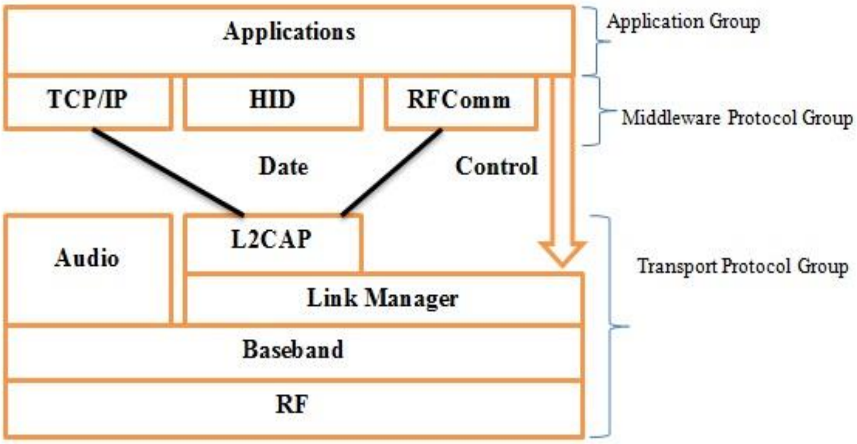

Figure 1

A. The Transport group protocols

This group of protocols allows devices that use Bluetooth to detect each other, and to manage physical and logical links with the above layer protocols and applications. Also, put in your mind that when we use the word "transport" in this group, we do not mean that this is the same as the transport layer on OSI model. Somewhat, these protocols are match to Physical and Data Link layers. The Radio, Baseband, Link Manager, Logical Link Control and Adaptation (L2CAP) layers and the Host Controller Interface (HCI) are built-in in the Transport Protocol group. These protocols work to provide support for both synchronous and asynchronous transmission. In addition, all of this group protocols have to provide a support for any communication between Bluetooth devices.

A short description for the Transport Group layer:

1) Radio Layer

The radio layer describes the technical features of the Bluetooth radios. A Bluetooth radio works on the range of 2.4 to 2.485 GHz ISM (industrial, scientific and medical) band. It employs a fast (1,600 hops/sec), frequency hopping, spread-spectrum (FHSS) technique – FHSS is a wireless technology that spreads its signal over rapidly changing frequencies. Each available frequency band is divided into sub-frequencies. Signals rapidly change among these in a pre-determined order. Interference at a specific frequency will only affect the signal during that short interval. The radio hops in a pseudo-random fashion on 79 one-MHz channels

2) Baseband Layer

This layer describes how devices that use Bluetooth look for and connect to other devices. The master and slave roles that a device may accept are describe here, as are the frequency-hopping sequences used by devices. The Bluetooth devices use a technology called time division duplexing (TDD), packet uses polling scheme to share the air-interface. The master and slave each connect only during their predetermined time slots. In addition, the Baseband layer describes the types of packets, packet-processing mechanisms and the approaches for error detection and correction, signal scrambling, encryption, packet transmission and retransmissions.

The Baseband layer provides support for two types of links, which are Synchronous Connection Oriented (SCO) and Asynchronous Connection-Less (ACL). SCO links are categorized by a periodic and single-slot packet assignment. It is mainly used for voice transmissions that need fast, reliable data transfer. A device that has established a Synchronous Connection Oriented link has reserved certain time slots for its use. Its packets are treated as high priority packets, and will be serviced before any Asynchronous Connection-Less packets. A device with an Asynchronous Connection-Less link can send fluctuate length packets of 1, 3 or 5 time-slot lengths. Nevertheless, it has no time slots reserved for it.

3) Link Manager Layer

This layer applies the Link Manager Protocol (LMP), which manages the properties of the air-interface link between Bluetooth devices. The Link Manager Protocol manages bandwidth share for general data, bandwidth reservation for audio traffic, authentication-using methods of challenge response, trust relations between devices, and encryption of data and control of power usage. Power usage control contains the negotiation of low power activity modes and the determination of transmission power levels.

4) L2CAP Layer

The Logical Link Control and Adaptation Protocol (L2CAP) layer provides interfacing between the above layer protocols and the bellow-layer transport protocols. The Logical Link Control and Adaptation Protocol provide support for multiplexing of some higher layer protocols, such as RFComm and SDP. This support allows many protocols and applications to share the air-interface. The Logical Link Control and Adaptation Protocol is also responsible for packet segmentation and reassembly, and for maintaining the negotiated service level between devices.

5) HCI layer

The Host Controller Interface (HCI) layer describes a standard interface for higher-level applications to access the lower layers of the stack. This layer is not a vital part of the specification. Its role is to enable interoperability among devices that use Bluetooth and the use of existing higher-level protocols and applications.

B. The Middleware Protocol group

This group of protocols allows current and any new applications to operate over Bluetooth links. Protocols like Point-to-Point Protocol (PPP), wireless application protocols (WAP), Transmission Control Protocol (TCP), Internet Protocol (IP), and object exchange (OBEX) protocols adopted from Infrared Data Association (IrDA). Bluetooth special interest group developed protocols contain

1) A serial port emulator (RFCOMM) that enables legacy applications to operate seamlessly over Bluetooth transport protocols.

2) A packet based telephony control signaling protocol (TCS) for managing telephony operations.

3) A service discovery protocol (SDP) that allows devices to obtain information about each other's available services. Reuse of existing protocols and seamless interfacing to existing applications was a high priority in the development of the Bluetooth specifications, as shown in Figure 2**.**

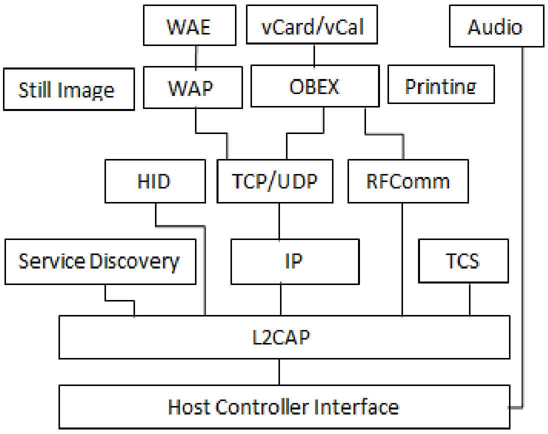

Figure 2. Interoperability with existing protocols and applications

C. The Application group

Consists of real applications that use Bluetooth [3].

V. HOW BLUETOOTH WORKS

Any two Bluetooth devices that become within a distance of each other can make an (ad-hoc) connection, which is called a piconet [4]. As shown in figure 3.

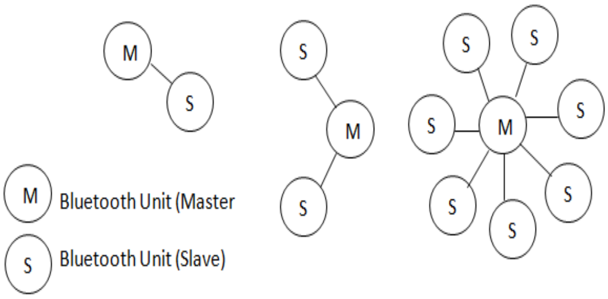

Figure 3. Piconet topology

Each piconet made up of up to eight units. One of these units called the Master unit and the rest called the Slaves. The unit that starts the piconet becomes the master unit. The master unit can be changed, but there cannot be more than one master. Several piconets can be found in the same area. This is called a scatternet as shown in figure 4. In one scatternet, all units share the same frequency range, but each piconet uses different hop sequences and transmits on different 1 MHz hop channels. All piconets share the 80 MHz band, and thus as long as the piconets choose different hop frequencies, no sharing of hop channels occur.

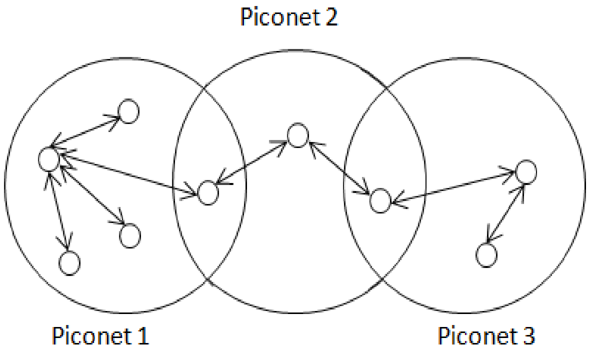

Figure 4. Scatternet

A) Bluetooth Addresses and Names

Each single Bluetooth device has a unique 48-bit address. This usually will be existing in the form of a 12-digit hexadecimal value. The most-significant half - 24 bits - of the address is an Organization Unique Identifier (OUI), which recognizes the manufacturers. The least significant half – 24 bits - are the more unique part of the address [5].

Bluetooth devices can also have easy names given to them. These are usually offered to the user, in place of the address, to help find which device it is. The rules for device names are less strict. They can be up to 248 bytes long, and two devices can use the same name. Sometimes the distinctive digits of the address might be included in the name to help differentiate devices.

B) Connection Process

Making a Bluetooth connection between two devices is a multi-step process including three states [6], which are:

1) Inquiry: if two Bluetooth devices don not know anything about each other, one must run an inquiry to try discovering the other. One device sends out the inquiry request, and any device listening for such a request will respond with the device address, and its name and other information.

2) Paging (Connecting): paging is the process of creating a connection between two Bluetooth devices. Before this connection can be started, each device needs to know the address of the other, which can be found in the inquiry process.

3) Connection: after a Bluetooth device has completed the paging process, it goes to the connection state. Either while connected, a device can be actively contributing or it can be entering into a low power sleep mode.

C) Bonding and Pairing

When two Bluetooth devices share a distinct affinity for each other, they can be together [7]. Bonded Bluetooth devices automatically establish a connection whenever they are close enough to each other. For example When anyone has a phone and become so close to his wife phone, the phone of this person immediately connects to his wife' phone because they share a bond.

Bonds are made through a process called pairing. When Bluetooth devices pair up, they share their addresses, names, and profiles, and usually store them in memory. They also share a common secret key, which permits them to bond when they are together in the future.

Pairing usually needs an authentication process where a user has to authenticate the connection between devices. The flow of the authentication process differs and usually depends on the interface abilities of one device or the other. Sometimes pairing is a simple operation, where the click of a button is all it takes to pair. Other times pairing includes matching 6-digit numeric codes. Older, legacy (v2.0 and earlier), pairing mechanisms involve the entering of a common PIN code on each device. The PIN code can vary in length and difficulty from four numbers to a 16-character alphanumeric string.

VI. THE ENERGY MANAGEMENT IN BLUETOOTH

Bluetooth has four different energy management modes [8], which are:

A) Active Mode: This is the normal connected mode, where the device is actively sending or receiving data.

B) Sniff Mode: This mode is the power-saving mode, where the device is less active. It sleeps and only listens for transmissions at a set interval, for example every 100ms.

C) Hold Mode: Hold mode is a temporary power-saving mode where a device sleeps for a well-defined period and then goes back to active mode when that interval has passed. The master can order a slave device to hold.

D) Park Mode: Park is the deepest of sleep modes. A master can order a slave to "park", and that slave will be not active until the master orders it to wake up again.

VII. BLUETOOTH SECURITY

In every Bluetooth device, there are four units used for maintaining the security at the link level [9], which are:

A) The Bluetooth device address (BD_ADDR), which is a 48-bit address that is distinctive for each Bluetooth device and defined by Institute of Electrical and Electronics Engineers (IEEE).

B) Private authentication key, which is a 128-bit random number used for authentication purposes.

C) Private encryption key, 8-128 bits in length that is used for encryption.

D) Random number (RAND), which is a regularly changing 128-bit random or pseudo-random number that is made by the Bluetooth device itself.

In Bluetooth Generic Access Profile, the Bluetooth security is divided into three modes:

- Security Mode 1: non-secure

- Security Mode 2: service level enforced security
- Security Mode 3: link level enforced security

The difference between Security Mode 2 and Security Mode 3 is that in Security Mode 3 the Bluetooth device starts security procedures before the channel is established. There are also different security levels for devices and services. For devices, there are 2 levels, "trusted device" and "untrusted device". The trusted device clearly has unrestricted access to all services. For services, 3 security levels are described: services that require authorization and authentication, services that require authentication only and services that are open to all devices.

VIII. THE ZIGBEE

ZigBee is a wireless technology standard used for exchanging data over distance varies from 10 to 100 meters with efficient using power. It uses radio wave for this purpose.

IX. HISTORY OF ZIGBEE

ZigBee was developed for the first time in beginning of the nineteenths of the last century. The IEEE organization was approved the 802.15.4 ZigBee specification in 2004. From that time, a group of companies has worked together to develop and provide support for a set of open, global and low power consumer technology depends on 802.15.4, and this group is called Zigbee Alliance.

X. ZIGBEE PROTOCOL OVERVIEW

The ZigBee protocol stack divides into four layers. They are the Application layer, the Network layer, the MAC layer and the Physical layer [10]. As shown in Figure 5

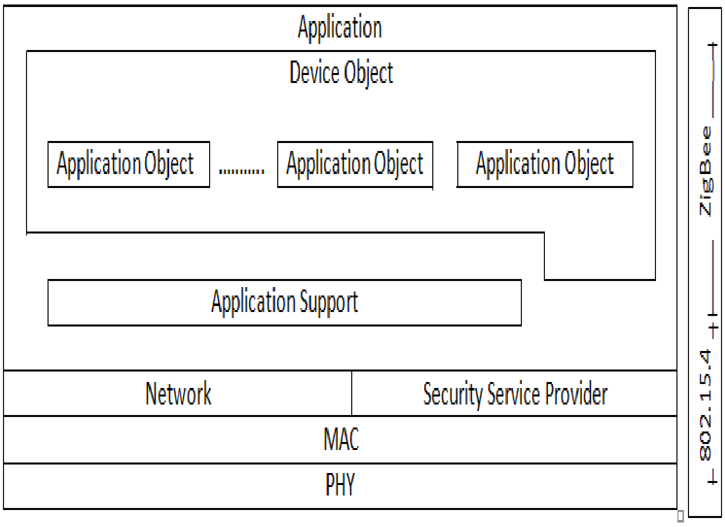

Figure 5. The ZigBee architecture.

A) Application Layer

The application Layer is contains the application objects. ZigBee splits the application layer into three different sub-layers: the Application Support Sub layer, the ZigBee Device Objects, and Application Framework having manufacturer defined Application Objects.

1) The application objects (APO)

It works like a controller and manager for the protocol layers in ZigBee device. It is a software that controls the hardware. Each application objects allocated a unique end point number that other applications objects can use an extension to the network device address to interact with it. There can be up to 240 application objects in one ZigBee device. A ZigBee application must follow to an existing application profile that is accepted ZigBee Alliance.

An application profile describes message formats and protocols for communications between applications objects. The application profile allows different vendors to freely build and sell ZigBee devices that can interoperate with each other in a given application profile.

2) ZigBee Device Object

The main part of ZigBee is the ZigBee device object, which addresses three main operations, service discovery, security and binding.

What service discovery does is to find nodes and ask about MAC address of coordinator or/and router by unicast messages. The service discovery is also enabling the procedure for locating some services through their profile identifiers. Therefore, profile plays an important role.

The security services in the ZigBee device object have the role to derive and authenticate the necessary keys for data encryption. The network manager is applied in the coordinator and its role is to select an existing PAN to connect. It also supports the creation of new PANs.

The binding manager role is binding nodes to recourses and applications also binding devices to channels.

3) Application support sub layer

The Application Support sub layer provides an interface between the Network and the Application layers. The application support sub layer processes leaving/arriving frames in order to securely send and receive the frames and create and manage the cryptographic keys.

Application support sub Layer Security includes the following services: Establish Key, Transport Key, Update Device, Remove Device, Request Key, Switch Key, Entity Authentication, and Permissions Configuration Table.

4) Security service provider

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

B) Network Layer

Network layer provide interfaces between application layer and MAC Layer. Network layer is responsible for network formation and routing. Routing is the process of selection of path to send the messages to its destination. This shaping the network involving joining and leaving of nodes, maintaining routing tables for the router, actual routing and address allocation. ZigBee coordinator or router will do the route discovery. This layer provides network security and allows low power devices to increase their batteries life.

C) MAC Layer

This layer is responsible for providing interface between network layer and physical layer.

The MAC layer provides two services; MAC data services and MAC management service. The MAC data service enables the send and receives of MAC protocol Data Units across the PHY data service. MAC layer is provide the ability for generating beacons and synchronizing devices to the beacon signal. It is also doing association and dissociation function.

MAC layer defines four frame structures, which are Beacon frame, Data frame, Acknowledge frame, and MAC command frame. One of the advantages of ZigBee protocol stack is Interoperability. ZigBee has wide range of applications, so different companies provide ZigBee devices. ZigBee devices can interact with each other regardless of the company

D) Physical Layer

The physical layer is the closest layer to the hardware. This layer controls and communicates with the radio transceiver directly. It deals with all tasks involving the access to the ZigBee hardware, which includes initialization of the hardware, channel selection, link quality estimation, energy detection measurement, and clear channel assessment to assist the channel selection. The physical layer supports three frequency bands, which are 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.

XI. HOW ZIGBEE WORKS

ZigBee uses the IEEE 802.15.4 2003 specification for its physical layer and MAC layer. IEEE 802.15.4 offers star, tree, cluster tree, and mesh topologie while ZigBee supports only star, tree, and mesh topologies [11].

ZigBee uses an association hierarchy; a device joining the network can be either a router or an end device, and routers can accept more devices.

A) ZigBee Star topology

The star topology consists of a coordinator and several end devices (nodes), as shown in Figure 6. In star topology, the end device communicates only with the coordinator. Any packet exchange between end devices has to go through the coordinator. The disadvantage of this topology is the operation of the network depends on the coordinator of the network, and because all packets between devices must go through coordinator, if any failure happens to the coordinator, the whole network goes down. The advantage of star topology is that it is really simple and packets go travel at most two hops to reach their destination.

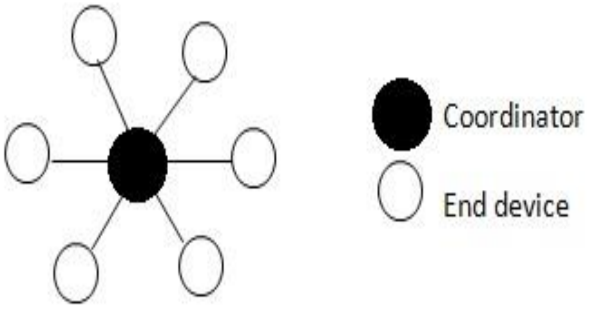

Figure 6. Star topology

B) ZigBee Tree topology

The tree topology consists of a central node (root tree), which is a coordinator, several routers, and end devices, as shown in Figure 7. The purpose of the router is to increase the network coverage. The end devices that are connected to the coordinator or the routers are called children. Only the routers and the coordinator can have children, so they are called parents. Every end device is only able to communicate with its parent.

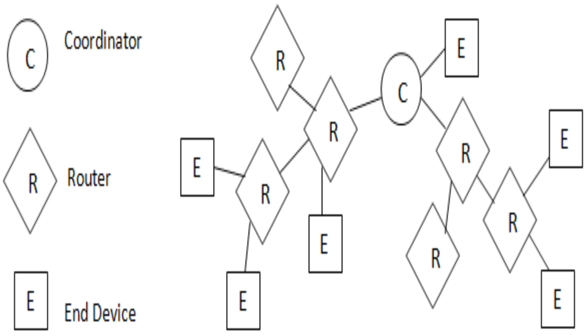

Figure 7. Tree topology

The tree topology has disadvantages, which are if one of the parents becomes deactivated; the children of the deactivated parent cannot communicate with other devices in the network, and the other disadvantage is even if two devices are close to each other, they cannot communicate directly.

C) Zigbee Mesh topology

The mesh topology consists of one coordinator, several routers, and end nodes, as shown in Figure 8. In the mesh topology, the packet travels through many hops to reach its destination. Also, the distance that this network covers can be extended by adding more nodes to the network. In addition, a mesh topology is self-healing, meaning during transmission, if a path fails, the device will find an alternative path to the destination. It is easy in these kinds of network to add or remove a device

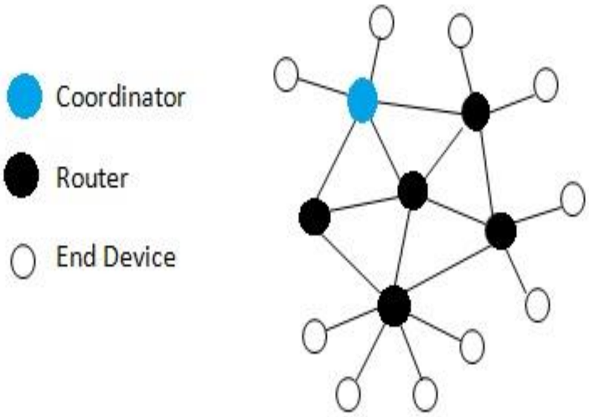

Figure 8. Mesh topology

XII. ZIGBEE SECURITY

ZigBee provides security based on three main principles. First is simplicity: Every layer initiating a frame is responsible for securing it, rather than having many layers do so. Second is directness: Keys are traveled directly between each source and destination device. Third is end-to-end security: Data proceeds without having to be decrypted and re-encrypted at each hop [12].

Security aspects of ZigBee technology are specifically described in the following features:

A) ZigBee provides sequential freshness. Sequential freshness is a security facility that uses an ordered sequence of inputs to reject frames that have been replayed. It can avoid the forwarding of attack. ZigBee devices keep the input and output freshness counter, when there is a new key is created, the counter will reset.

B) ZigBee offers frame integrity checking function. It uses a message integrity code (MIC) to protect data from being modified by parties without the cryptographic key. It further offers assurance that data came from a party with the cryptographic key. This feature stops an attacker to modify the data. The bit-length of the MIC may take the values 0, 32, 64 or 128.

C) ZigBee offers entity authentication service. The entity authentication service provides a secure means for a device to synchronize information with another device while concurrently providing authenticity based on a shared key. The NWK (network) layer authentication is by an active network key. The APS (application support sublayer) layer authentication is through using the link key between devices.

D) ZigBee provides data encryption. Data encryption is a security service that uses a symmetric cipher to keep data from being read by parties without the cryptographic key. Data may be encrypted using a key shared by a set of devices or using a key shared between two peers.

E) ZigBee describes the role of Trust Center. The Trust Center decides whether to allow or disallow new devices into its network. The Trust Center occasionally update and switch to a new Network Key. It first broadcasts the new key encrypted with the old Network Key. Later, it informs all devices to switch to the new key. All members of the network shall recognize exactly one Trust Center, and there shall be exactly one Trust Center in each secure network. The Trust Center is usually the network coordinator, but is also able to be a dedicated device. It is responsible for the following security roles:

1) Trust Manager, to authenticate devices that ask to join the network.

2) Network Manager, to keep and distribute network keys.

3) Configuration Manager, to enable end-to-end security between nodes.

F) ZigBee adopts CCM* (counter with CBC-MAC) encryption algorithm. CCM* is a minor modification of CCM (counter with CBC-MAC). It includes all of the features of CCM and additionally offers encryption-only and integrity only capabilities. Unlike other MAC layer security modes which need a different key for every security level, the use of CCM* enables the use of a single key for all CCM* security levels. With the use of CCM* throughout the ZigBee stack, the MAC, NWK, and APS layers can reuse the same key.

XIII. COMPARISON BETWEEN BLUETOOTH AND ZIGBEE

Below is a comparison between Bluetooth and ZigBee in different features [13], which are:

A) Frequency Band

Bluetooth works on the unlicensed 2.4 GHz spectrum, while ZigBee can also operate at reduced speeds at 915MHz and 868 MHz.

B) Power and Battery Life

ZigBee, aimed to be a low-power alternative to Bluetooth, offers 30mW performance compared to Bluetooth’s 100mW. This results from its ability to lock into a transmission time slot and sleep in between. Bluetooth, nevertheless, must stay awake for the suitability of quick response time, which results in battery life on the order of days.

C) Range

Bluetooth is designed to operate within a 10m range, but many new Bluetooth devices reach to a maximum range of 30m. Zigbee is designed to reach a maximum range of 75m.

D) Data Rate

Bluetooth has designed to reach maximum rates of 3Mbps while ZigBee loses his data rate to save power, so it transmits only 20-250Kbps.

E) Component Cost

At the beginning of the third millennium, while ZigBee was targeting 2 dollars component

Cost, Bluetooth supports a 5 dollars cost per device. In now days, Bluetooth price has reached to 3 dollars while ZigBee costs remain same.

F) Network Topologies

Bluetooth operates primarily in ad-piconets, where one master device controls multiple slaves. These piconets are limited to 8 devices. ZigBee has much more flexibility the area of topology, supporting star, tree, and mesh topologies.

G) Time to Wake and Transmit

One of the best features that ZigBee has is freedom to sleep often while Bluetooth does not have this. This comes from its quick wake-from-sleep mechanism. A ZigBee device “can wake up and get a packet across a network connection in around 15 milliseconds,” while a Bluetooth device would take 3 seconds.

The above comparison is summarized in the below table 1.

Table I: Comparison between Bluetooth and Zigbee

	Bluetooth	ZigBee
Band	2.4 GHz	2.4 GHz , 868 MHz , 915 MHz
Power	100 mW	30 mW
Target battery life	Days - months	6 month – 2 years
Range	10 - 30 m	10 - 75 m
Data rate	1 - 3 Mbps	25 - 250 Kbps
Component cost	3 $	2 $
Network Topologies	Ad hoc , point to point , star	Mesh , ad hoc , star
Time to wake and transmit	3 s	15 ms

XIV. CONCLUSION

This paper has talked at the beginning about the wireless personal area network, then it concentrate about two specific standards, which are Bluetooth and Zigbee, also it has given a brief description of both Bluetooth and ZigBee, and it explains the protocol stack, the mechanisms of their working, and some security features for them. At the end of the paper, a comparison has done between the two technologies. From all of that we can know that for Bluetooth and ZigBee there are advantages and disadvantages, but in case of saving power and sending data for long distance, ZigBee has won that. On the other hand Bluetooth has won the amount of data that has to send.

REFERENCES

[1] K. V. S. S. S. S. Sairam, N. Gunasekaran and S. R. Redd, "Bluetooth in wireless communication," in IEEE Communications Magazine, vol. 40, no. 6, pp. 90-96, Jun 2002.

[2] P. McDermott-Wells, "What is Bluetooth?," in IEEE Potentials, vol. 23, no. 5, pp. 33-35, Dec. 2004-Jan. 2005.

[3] C. Bisdikian, "An overview of the Bluetooth wireless technology," in *IEEE Communications Magazine*, vol. 39, no. 12, pp. 86-94, Dec. 2001.

[4] Rumiana Krasteva, Ani Boneva, Vesselin Georchev, Ivilin Stoianov, “Application of Wireless Protocols Bluetooth and ZigBee in Telemetry System Development,” in Problems of Engineering, Cybernetics, and Robotics, vol 55, pp. 30-38, 2005.

[5] Developer.bluetooth.org. (2016). Pages-. [Online] Available at: https://developer.bluetooth.org/gatt/characteristics/ Pages/CharacteristicViewer.aspx?u=org.bluetooth.characteristic.system_id.xml [Accessed 17 Apr. 2016].

[6] Kansal, A, "Bluetooth Primer,” 2002.

[7] Bluetooth.com. (2016). Bluetooth Technology Website. [online] Available at: https://www.bluetooth.com/ [Accessed 17 Apr. 2016].

[8] Cano, J., Cano, J., Gonz´alez, E., Calafate, C., & Manzoni, P, “How Does Energy Consumption Impact Performance in Bluetooth?,” vol 35, 2007.

[9] J. Vainio, “Bluetooth Security.”

[10] Somani, N., & Patel, Y, “.ZIGBEE: A LOW POWER WIRELESS TECHNOLOGY FOR INDUSTRIAL APPLICATIONS,” vol 2, 2012.

[11] Elahi, A., Gschwender, A., “Introduction to the ZigBee Wireless Sensor and Control Network”, 2009.

[12] H. Li, Z. Jia and X. Xue, "Application and Analysis of ZigBee Security Services Specification," *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on*, Wuhan, Hubei, 2010, pp. 494-497.

[13] Kooker, J., “Bluetooth, ZigBee, and Wibree: A Comparison of WPAN Technologies,” 2008.