A Survey of ZigBee Wireless Sensor Network Technology: Topology, Applications and Challenges

Omojokun G. Aju
Adekunle Ajasin University, Department of Computer Science
Akungba-Akoko, Ondo-State, Nigeria

ABSTRACT
ZigBee technology as a wireless sensor and control network is one of the most popularly deployed wireless technologies in recent years. This is because ZigBee is an open standard lightweight, low-cost, low-speed, low-power protocol that allows true operability between systems. It is built on existing IEEE 802.15.4 protocol and therefore combines the IEEE 802.15.4 features and newly added features to meet required functionalities thereby finding applications in wide variety of wireless personal area networked systems such as home/industrial automation and monitoring systems. Although the ZigBee design specification includes security features to protect data communication confidentiality and integrity, however, when simplicity and low-cost are the major goals, security suffers. This paper gives the general survey of the ZigBee as a wireless sensor network based technology which provides the readers with the general overview of ZigBee network technology including its topology, applications and challenges.

General Terms
Wireless Sensor Network, Mobile Network.

Keywords
ZigBee, IEEE 802.14.5, Wireless Sensor Network (WSN), topology, application, wireless technology.

1. INTRODUCTION
Wireless sensor networking is one of the most popular and active research areas in networking and communication field in recent years. Consequently, numerous workshops and conferences are being arranged annually on this emerging technology. This attraction resulted from the fact that the technology is exciting with unlimited potential for numerous applications that are been implemented based on wireless sensor networks (WSNs). Application areas include environmental, military, telecommunication, transportation, entertainment, crisis management, health, retail services and smart homes. The wireless technology deployed for a particular sensor network depends on the type of application. Common wireless technologies include Infrared, Bluetooth, WiFi, WiMax, ZigBee etc. However, this paper survey ZigBee technology as a Wireless Sensor Network with emphasis on its topology, application, and challenges.

Wireless sensor network (WSN) is a large number of nodes with sensing capabilities which gather information from physical processes/events (e.g. temperature, sound, vibration, pressure, motion, or pollutants) and communicate the processed data (information) cooperatively and wirelessly to the base station. The network is formed when the same or different types or group of sensors jointly monitor (and/or control) one or more physical environments [15].

Although, wired sensor networks are more reliable and secured in addition to having stable communication systems. However, the greatest advantage of wireless sensor devices is that they make installations possible where cabling is impractical, such as in large concrete structures and cargoes [17].

When ideal wireless sensors are networked, they perform smartly and are scalable. They consume very little power, software programmable, capable of fast data acquisition, reliable and accurate. Also, wireless sensors are relatively cheap and WSNs largely reduce long term maintenance cost, eases installation, eliminate the use of bundle of wires and fiber optic tails.

In WSN, the protocol stack helps to promote cooperative efforts of sensor nodes, enhance power efficiency and integrates data with networking protocols. The protocol stack is made up of the task management plane, mobility management plane, power management plane, application layer, transport layer, network layer, data link layer and physical layer. Although, some modifications may be applicable to the protocol depending on the wireless standard and technology used in designing the WSN. ZigBee, Bluetooth, WiFi, WiMax, ANT, WirelessHART, Z-Wave and 6LowPAN are some of the most popular technologies that are currently being deployed in WSNs.

Unlike LAN sensor network where sensors, controllers and processing stations are connected directly, in WSN, sensors interact wirelessly with central based (processing) stations [11]. The base station (can be a sink node) otherwise known as the gateway, communicates with the wireless sensors via radio link. Data from wireless sensor nodes is transmitted to the gateway (the sink node) directly or through other wireless sensor nodes using multi-hop communication system. Therefore, WSN enables information (data) to be obtained from remote and inaccessible locations for processing. A simple schematic diagram of a WSN is shown *in figure* 1.1.

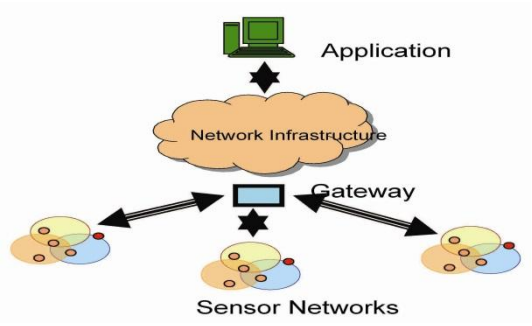

Fig. 1.1 A Wireless Sensor Network

Unlike other popular WSNs, ZigBee is an open standard protocol developed by ZigBee alliance using IEEE 802.15.4 wireless standard. It allows true operability between systems [1]. ZigBee is simpler, requires smaller power, more robust, less expensive, more reliable and secure, and has lower latency, energy efficiency with efficient wireless connectivity infrastructure. This accounts for its wide range of applications in wireless personal area networks and hence ZigBee WSN is one of the most popularly deployed technologies for home automation and monitoring systems.

ZigBee WSNs support three different network topologies, namely star, mesh and cluster tree, the cluster tree being a special case of mesh. Each of these topologies has its strengths and limitations which can be used to advantage in different situations. Although star is considered to be simpler, it has the limitation of ineffectiveness when multi-hop communication is required between nodes. In mesh, configuration of alternative paths is allowed in the network using the most cost effective path, thus allowing multi-hop communication. Hence, mesh connection is more secured, flexible, scalable and reliable.

Moreover, it should also be noted that the topology of a ZigBee network may change as a node moves from one point to another. Topology may also affect the correctness and accuracy of sensor readings, ease of network implementation and network security [19]. Therefore, this paper aims to evaluate these topologies and their corresponding trade-offs, while also looking at the various applications of the technology and the challenges facing the technology causing some constraints and limitations in its applications.

2. ZIGBEE TECHNOLOGY

ZigBee is a new open-standard wireless protocol developed by ZigBee Alliance (consisting of over 270 companies). ZigBee is particularly targeted at low-power, low-cost and low data rate wireless sensor and control networks, aimed at interoperability, it is easy to implement and can support up to 65,000 nodes depending on the type of topologies used [8].

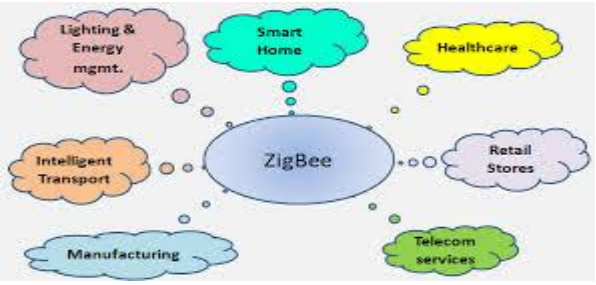

Fig. 1.2: ZigBee Technology Applications

ZigBee has a transmission range of 10 - 100metres. Comparing ZigBee with WiFi and Bluetooth, ZigBee stack is lighter weighted (about 120 KB). It has a maximum throughput of 250Kbps while Bluetooth (except 802.11n) and Wi-Fi transmit at 3Mbps and 54Mbps respectively. While WiFi devices (e.g. WiFi VoIP phones) are reported to have 8 – 12hours of battery lives and Bluetooth devices with a battery life of a few days, many ZigBee devices can boast of a battery life of up to 5years. The huge power saving resulted from relatively short-range of transmission, low data transfer rates and simple protocol stack of ZigBee. The characteristics of WiFi, Bluetooth and ZigBee are summarized and compare in table 1 [5]

Table 1. Characteristics of WiFi, Bluetooth and ZigBee

Features	**WiFi IEEE 802.11**	**Bluetooth IEEE 802.15.1**	**ZigBee IEEE 802.15.4**
Application	Wireless LAN	Cable Replacement	Control and Monitor
Frequency Bands	2.4GHz	2.4GHz	2.4GHz, 868MHz, 915MHz
Battery Life (Days)	0.1-5	1-7	100-7,000
Nodes Per Network	30	7	65,000
Bandwidth	2-100Mbps	1Mbps	20-250Kbps
Range (Metres)	1-100	1-10	1-75 and more
Topology	Tree	Tree	Star, Tree, Cluster Tree, and Mesh
Standby Current	20 * 10-3 amps	200 * 10-6 amps	3 * 10-6 amps
Memory	100KB	100KB	32-60KB

The history of ZigBee started back in 1998 when it was first conceived and supported from development perspective. Though, it was not until December 2004 that ZigBee Alliance published its first ratified specification. It only supported home control lighting [6]. However, ZigBee Alliance no longer supports 2004 specification. In 2006, the 2004 specification was modified to support group addressing, encryption and frame authenticity. In 2007, ZigBee 2007 and ZigBee Pro was published. ZigBee 2007 added new security model to ZigBee 2006 with "trust centre" while ZigBee-Pro has additional software features, more scalability, data fragmentation, stochastic addressing (automated address allocation mechanism) and enhanced security. ZigBee 2007 and ZigBee-Pro are interoperable [9].

2.1 ZigBee Device Types

The operation of a ZigBee node depends on whether it is a full-function device (FFD) or reduce-function device (RFD). The FFD performs all the tasks defined by ZigBee standard while the function performed by the RFD is limited. An FFD can form any type of network (such as star, tree or mesh) while a RFD can only connect to an FFD. With respect to these functionalities, ZigBee devices are classified as Coordinator, Router and End Devices [12].

i. ZigBee Coordinator (ZC)

It is an FFD and a network must contain only one. It starts the network and is responsible for the overall management of the network. In star topology, it is the central node while in tree or mesh topology, it is the root node. Its other functions include address allocation, granting permission to nodes to join or leave network, transfer application packets and keeping list of neighbours table. Because of it functions in the network, it must always be powered on.

ii. ZigBee Router (ZR)

It is also an FFD and can be absent in a network, a network can also contain just one or more depending on the size and topology of the network. It is not required in star topology

(figure 2.1). It is often used to expand ZigBee network (in tree and mesh). Basically, it performs all the functions of the coordinator except network establishment (start-up). Constant power source must also be provided for a ZR.

iii. ZigBee End Devices (ZEDs)

They are RFDs and are usually located at the extremities of a network. Their main task is in sending and receiving packets. Other devices cannot connect to the network through a ZED and it cannot relay messages. ZEDs often *sleep* when they are not transmitting or receiving in order to conserve power. At this point in time, they are said to be in *sleep mode*. Therefore they can be battery powered for ease of mobility.

iv. ZigBee Trust Centre (ZTC)

It is a dedicated device (node) in the network whose function is to provide security management, device authentication and key distribution. Where this is not available in the network, the coordinator performs these roles.

v. ZigBee Gateway

The main function of the gateway is to connect the ZigBee network to external network e.g. LAN using protocol conversion.

2.2 ZigBee Network Topologies

Three network topologies are specified for ZigBee network; star, tree and mesh. The depth of a network depends on the network topology and is determined by the number of routers (hops) in the network from the coordinator to the farthest node [8].

i. **Star Topology**

This topology consists of a coordinator and several end devices as shown *in figure* 2.1. It has no router and therefore a star network has a depth of one (1). End devices communicate with each other in the network only through the coordinator. Instead of end devices (*in figure* 2.1), routers can be used. However, router message relay functions will not be used, only its application functions will be used. The end devices or routers now become children to the coordinator

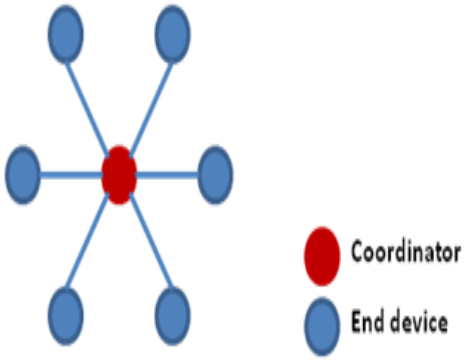

Fig. 2.1 ZigBee Star Topology

The major advantage of a ZigBee star network is its simplicity. The main disadvantage is that it does not provide alternative route for packet transmission and reception. All transmission and reception go through the coordinator. This may increase the burden on the coordinator and hence cause congestion in the network.

ii. **Tree Topology**

In the tree topology, the coordinator (at the top) is connected to several routers and end devices. In this case, the routers and the end devices are coordinator's children. The router is used to extend the network; a router can therefore connect to several other routers and/or end devices to form the router's children as shown *in figure* 2.2. Only the coordinator and the routers can have children and hence can become parents in a tree topology. The end devices cannot have children and therefore cannot become parents.

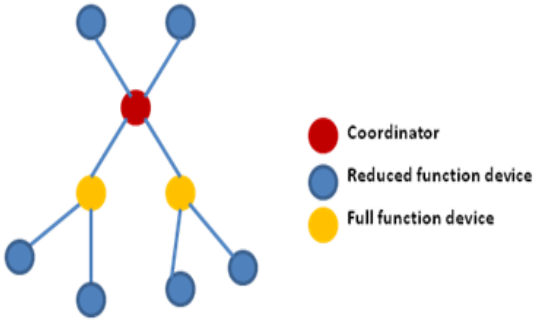

Fig. 2.2 ZigBee Tree Topology

A child is only permitted to communicate directly with its parent and not with any other nodes. Parents can communicate directly with their parents and children.

Like in star, there are no alternative paths to destinations. If a parent is down, its children cannot communicate with other nodes in the network. And even if two nodes in the network are geographically close, their direct communication is not guarantee.

iii. **Mesh Topology**

In mesh, the coordinator is also at the top like that of tree. It consists of a coordinator, several routers and end devices connected as shown *in figure* 2.3. Routers are used to extend network range like in tree. As shown, packets pass through multiple hops to reach destinations and communication between any source and destination in the network is realistic. Hence it is also called a peer-to-peer multi-hop network.

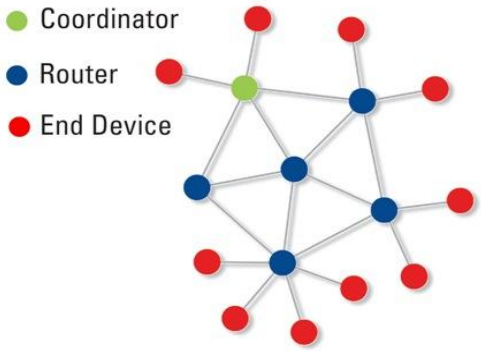

Fig. 2.3 ZigBee Mesh Topology

Moreover, a mesh network provides alternative paths for packet to reach its destination if a path fails. With reference to this, mesh network is usually also being described as a "self-healing" network. Thus adding or removing a node is made easier.

Compared to star and tree ZigBee network configurations, mesh network is more complex and therefore requires more overhead and uses more complex routing protocols.

2.3 ZigBee Protocol Stack

Two types of addresses are in use in ZigBee network; *IEEE address* and *network address.* The IEEE address is a unique 64-bit long address used to identify a ZigBee device. It is assigned to the device by the manufacturer and is also called MAC address or extended address. No two devices can have the same IEEE address in the entire world [12].

The network address (otherwise known as short address) is a 16-bit address that identifies a node locally in the network. It is assigned by a parent to a node when the node joins the network. The advantage of using the 16-bit address is that it extends battery life. A 16-bit address reduces frame size compared to a 64-bit address size and hence reduces transmission time and consequently, increases battery life. The disadvantage is that it is possible for two nodes on different networks to have the same short address.

The ZigBee stack is formed on top of the IEEE 802.15.4 standard. The IEEE 802.15.4 consists of the Physical (PHY) and Media Access Control (MAC) layers while the ZigBee layer is made up of the Network (NWK) layer, the Application Support Sublayer (APS), the ZigBee Device Object (ZDO) and the Security Service as shown in figure 2.4 [20].

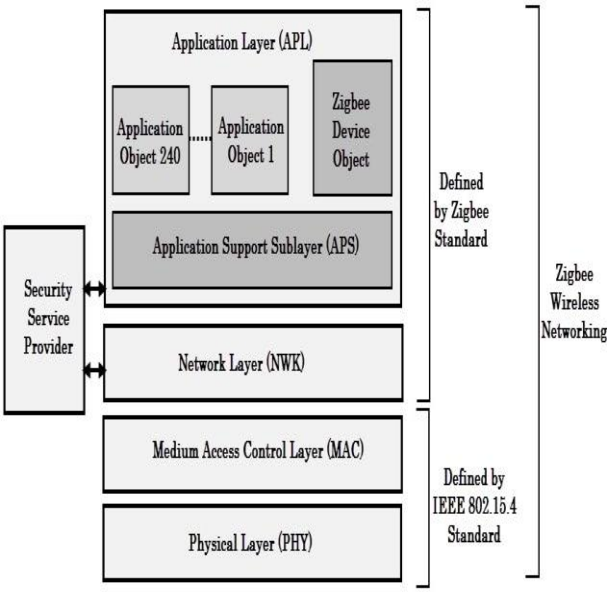

Fig. 2.4 ZigBee Protocol Architecture

ZigBee device manufacturers can use the ZigBee application profile to suite their design or they can develop their own application profile

i. ZigBee Physical Layer

The main function of the physical layer is to modulate outgoing signals and demodulates incoming signals. It also deals with transmission and reception of information from sources. The physical layer frequency band consists of 27 channels which are used worldwide [19]. How the bands are shared is shown in table 2.

Table 2. Physical Layer Frequency Band

Country	Channel	Channel Width	Frequency Band	Data Rate
Europe	0	600KHz	868-868.6MHz	100Kbps
USA	1-10	2MHz	902-928MHz	250Kbps
Worldwide	11-26	5MHz	2.4-2.4835GHz	250Kbps

Like IEEE 802.11, ZigBee uses mandatory DSSS (Distributed Sequence Spread Spectrum) and optional PSSS (Parallel Sequence Spread Spectrum). And similar to WiFi, a ZigBee network remains on a single frequency picked up automatically by the coordinator when creating the network. However, it can be reconfigured into another frequency by an administrator.

i. ZigBee MAC layer

This layer access the network using CSMA/CA (carrier-sense multiple access with collision avoidance) to enable beacon transmission for synchronization and hence provide reliable transmission. Other functions of this layer include assigning device roles (into ZC, ZR, or ZED), topology design and network association and disassociation.

At MAC layer, ZigBee traffics are carried by frames, unlike WiFi and Bluetooth. The frames are beacon frames, data frames, acknowledge frames and command frames. A frame format of the IEEE 802.15.4 MAC layer is shown *in figure* 2.5. The frame format is not constant (stable). It can change depending on the options that are set in the frame control header bits [22].

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

Fig. 2.5 ZigBee MAC Layer Frame Format

i. ZigBee Network Layer

As shown in *Figure 2.4*, this layer is located between MAC and Application layer. The main functions of the network layer includes network establishment, address assigning, routing and neighbour discovery, adding and removing devices from the network and applying security features to outgoing messages.

ii. ZigBee Application Layer

The application layer is the highest layer in the ZigBee protocol stack. It interfaces a ZigBee system (application object) with its end user. As shown *in Figure 2.4*, the application layer is made up of ZigBee Device Object (ZDO), Application Support Sublayer (APS) and Application Framework [14].

The ZDO Layer assigns functions to all ZigBee devices in the network. It determines whether a device is a coordinator, a router or an end device. It also performs security related functions (such as setting and removal of encryption key) and network management functions (such as network discovery).

The APS Layer enables the interfacing of ZigBee endpoints (application objects) and ZDO with the network layer for network services such as data and management services. This is achieved by receiving the required data (in the form of PDU) from either an application object or ZDO, add a header to create a data frame and then pass it down to the network layer. These services include *request*, *confirm* and *response*, which are provided to the objects for reliable and efficient data transfer [13].

The Application Framework enables different ZigBee devices from different manufacturers to interoperate. For interoperability to be achieved, ZigBee manufacturers must strictly adhere to the application profiles specified by ZigBee Alliance (2006). The two sets of data services specified in the application framework are Generic Message (GM) and Key Value Pair (KVP) services. Using KVP, object attributes can be configured through a simple XML interface. Unlike KVP, GM is more general and as such it uses arbitrary payloads and skips overheads. Exchange of actual data is achieved through ZDO interface using services such as *request*, *confirm* and *indicate*.

ii. Security Service

The security service plane spans and interacts with the NKW and APS layers. It is the security service provider layer of the stack. ZigBee security provides authentication, integrity, freshness and privacy in a ZigBee network. Security is provided using counter mode encryption and cipher block chaining message authentication code (CCM) at different levels with 128 bit Advanced Encryption Standard (AES) algorithm [21].

For all level of security, ZigBee uses symmetric key and applies cryptography and frame integrity to network and application layers. It is the responsibility of an application developer to decide the level of security to apply. A layer is also responsible to protect (secure) a frame that it generated.

ZigBee uses 3 types of keys for security. They are: link, network and master keys.

a) ***Link Key:*** This is used by the APS layer to protect confidentiality and integrity of unicast traffic between two devices. Link key may be preconfigured by device manufacturer, distributed by trust centre, generated from master key or installed on devices using SKKE (Symmetric-Key Key Establishment). In standard security environments, the key can be distributed in plain text [22].

b) ***Network Key:*** This is used to protect and secure group or broadcast traffic in the network. The network key is shared by all network devices. The key can be preconfigured or transported by the trust centre. Over-the-air key transport is not recommended for security reasons. Like the link key, the network key can also be distributed in plain text, however, in a standard security environment.

c) ***Master Key:*** This key is optional. It can be preinstalled or installed by the trust centre. Where applicable, it can be used to generate other keys (network and link keys).

3. ZIGBEE APPLICATIONS

ZigBee technology has find its applications in wide variety of wireless personal area networked systems such as home/industrial automation and monitoring systems due to attracting features to various industries and sectors. Some of the areas in which its applications are found are:

i. ***Home Automation:*** This defines ZigBee applications for automated residential management. ZigBee can be used to remotely control doors, lightings, security alarm, heating, cooling and other residential applications.

ii. ***Commercial Building Automations:*** ZigBee provides means for easy management and maintenance of buildings. An example is found in the monitoring of fire-door positions and smoke detectors operation. With ZigBee all the smoke detectors in a building can be remotely monitored and managed from a central location [17].

iii. ***Smart Energy:*** ZigBee enables wireless communication between home area networks (HAN) and advanced metering infrastructure thereby enhancing quick reading of water, gas and electrical meters. It also helps utility companies to effectively manage services provided to their customers especially during peak demands.

iv. ***Health Care:*** This profile enables remote monitoring of patients in the hospitals and health care centres. Hence, mobility of patients does not affect monitoring. For example, patients' blood pressure can be monitored remotely using ZigBee wireless sensor technology.

v. ***Industrial Process Monitoring and Control:*** With ZigBee, industrial processes are now being controlled and monitored wirelessly. An example is found in industrial inventory tracking where equipment are tagged with wireless sensors and can be located by a ZigBee node.

vi. ***Remote Control for Consumer Electronics:*** Most remote controllers for consumer electronics now uses radio frequency (RF) instead of infrared (IR) with the help of ZigBee RF4CE technology. The limitation of IR remote controller *line of sight* operation is therefore eliminated.

vii. ***Telecommunication Applications:*** Here, ZigBee devices are embedded in smart phones and PDAs thus enabling their communication with other ZigBee enabled devices

4. CHALLENGES OF ZIGBEE SENSOR NETWORK

Despite their countless practical applications in our modern society, however, because of their peculiarity in terms of their non-conventional protocol design, complexity, long network lifetime, bandwidth constraint of communication channel between nodes and fusion canter, balance between communication and data processing, signal processing techniques, etc., WSNs offer numerous and formidable challenges. In order to overcome these challenges, huge efforts are now being placed in research activities,

standardization process and industrial investments of wireless sensor networking. The following are some of the challenges and constraints pose by WSNs when compared to other distributed (existing) systems especially in terms of design with respect to protocol and algorithms.

i. ***Energy Limitation***: Wireless sensor nodes are usually powered with batteries and replacing batteries in the field is often not practicable. Since a WSN must operate for a given network operation time or as long as possible, meeting the energy requirement with batteries becomes a challenge [3]. Energy limitation can be improved by the use of solar cells, which can be charged as the battery is being in use. However, this is only applicable to applications in light exposed environments. Also, sensor nodes are now been designed with improved energy efficiency and balanced energy harvesting techniques to enable them operate for several years without battery replacement [10].

ii. ***Self-Management*:** WSNs are usually deployed in remote and harsh environments (which may not be predetermined or engineered) and often without infrastructural support, repair and maintenance. Consequently, sensor nodes are exposed to system and environmental dynamics thus posing a significant challenge for building reliable sensor networks [11]. Therefore the need to build a self-managed WSN network in terms of self-organization, self-optimization, self-protection and self- healing becomes a necessity.

iii. ***Connectivity Challenge*:** The fact that WSNs use wireless communication system also poses a number of challenges to their design especially when maintaining a balance between signal strength, power (transmitted and received) and distance. Increasing the distance between a sensor node and a base station increases the required transmission power and decreases signal strength. For energy and connectivity efficiency, the need to split large distance into several shorter distances using multi hop communication and routing becomes essential. Moreover, in an attempt to conserve energy, some sensor nodes do switch off their radios when they are not in use (*duty cycling*) thereby preventing them from receiving message from neighbours during down time and creating synchronization and connectivity problems. Arbitrary long sleep periods can also reduce the responsiveness and effectiveness of a sensor. However, sensor nodes now use *wake up on demand* strategies and *adaptive duty cycling* to conserve power and still maintain connectivity in WSNs [2, 4]. In *adaptive duty cycling*, some nodes sleep while others are active to form network backbone.

iv. ***Decentralized Management:*** Another challenge to WSN is its infeasibility of centralized management functions such as topology management and routing. This resulted from the fact that WSNs are often large scaled and usually affected by energy constraints. Hence WSN management is usually decentralized to ensure that sensor nodes collaborate with neighbours to make localized decisions. Thus management overhead is consequently reduced although may lead to non-optimal routes.

v. ***Privacy and Security:*** The fact that information collected by a WSN is sensitive, of large scale and sensor nodes are often located in remote, unattended and hostile environments poses privacy and security challenges [21]. Therefore, they are prone to malicious intrusions and attacks such as Denial of Services (DoS), Interrogation, Sybil, Wormhole, Acknowledgement Spoofing, Hello Flood, Routing Information Manipulation and Impersonation [15]. Although, several techniques such as channel hopping and blacklisting, key manipulation, cyclic redundancy check (CRC) and time diversity etc. are in place to tackle these threats, the computational, communication and storage requirements of these techniques still remain a challenge [13]. Hence the need to develop new and better solutions to guarantee the security of WSNs.

5. SOME OTHER WSN STANDARDS AND TECHNOLOGIES

As the applications of WSNs are increasing, different protocols and standards are being researched and created to enhance the efficiency of the network. The decision to select a particular standard/protocol over the other is determined by the target application requirements and some other factors such as network size, network environment and network duration. Once the application requirements are set, then the engineer will select the technology which satisfies these requirements. The following are overview of the features of other popular WSN technologies.

i. Bluetooth Technology

Bluetooth is a robust, low power, low cost, short-range wireless communication technology intended to replace cables in wireless personal area networks (WPANs). Initially created by Ericsson Microelectronics in 1994, its specifications are driven by a consortium that was founded by Ericsson, Nokia, Toshiba, IBM and Intel. The IEEE standard for Bluetooth (WPAN) is called The IEEE Project 802.15.1 and is based on the Bluetooth v 1.1 Foundation (Bluetooth^{TM}, 2004). It allows product differentiations because some of its core specifications are optional. It can communicate (pass and synchronize data) between up to seven devices using 868MHz, 915MHz and 2.4GHz radio bands at 1GHz per second using frequency-hopping spread-spectrum (FHSS) and up to a range of 10 meters [5]. Bluetooth only supports star topology, uses master-slave based MAC protocol and full duplex transmission through the use of time-division duplexing.

The simplified version of Bluetooth was released to the public in 2006 and is called Bluetooth Low Energy Technology. Designed to be more efficient (about 15 times than existing Bluetooth), however, it interoperate with existing Bluetooth. This efficiency is achieved by improvement on number of packets transmitted during connection, node discovery and the size of each individual packet [8].

In WSNs, applications of Bluetooth technology are increasing drastically. Bluetooth technology finds application in smart home, automation, health and fitness, mobile telephony, PC and peripherals etc. "*Bluetooth Low Energy will be a significant contributor to the overall Wireless Sensor Network market, representing nearly half of all shipments in 2015*" [23].

ii. WiFi

Based on IEEE 802.11 standards, WiFi is a WLAN technology that allows electronic devices to exchange data over a network such as internet and uses a radio band of 2.4GHz. WiFi is robust, easily expandable and cost effective. WiFi data transfer rate is up to 300Mbps depending on the standard and has about 100 to 150Mbps through-put. It also has a broad coverage area, some non-line-of-sight (NLOS) transmission capacity, small disturbance of links, and supports mesh networking.

A WiFi-based WSN is a combination of traditional WiFi mesh network and WSN and hence possesses both the features of WiFi mesh network and WSN. Therefore, it is both network-centred and data-centred.

WiFi-based WSNs are used in smart grid, smart agriculture and intelligent environment protection. Also because of WiFi's high bandwidth, fast transmission rate, long transmission distance and NLOS, WiFi-based WSN is being deployed in video monitoring which requires data transition and good-real time.

iii. Z-Wave

Z-Wave is a proprietary low-power and low data wireless communication technology specifically designed for home automation and control. Initially developed by a Danish company, Zen-Sys, it was later acquired by Sigma Designs in 2008 and is now been standardized by Z-Wave Alliance. It uses the 868MHz ISM band and hence unsusceptible to interference due to 802.11 and 802.15.1 devices. Z-Wave uses 9.6kbps and 40kbps with 1% duty cycle limitation and allows up to 100 meters outdoor range. It also supports source-routed mesh networking and allows 232 maximum nodes.

Comparing ZigBee and Z-Wave, they are similar in many respects including areas of application. They are both designed for low power and low through-put. They also both support mesh topology. However, ZigBee is more robust and provides a higher data rate [16].

Z-Wave chips are embedded in consumer electronic products such as TV, remote controls and lighting and thus they can easily form a WSN to enhance home automation, for monitoring and controlling residential, and to light commercial environments.

iv. *ANT Technology*

ANT is another proprietary wireless technology that is designed using microcontrollers and transceivers operating in the 2.4GHz ISM for reliable, flexible and adaptive data communication with ultra-low power consumption in WSN applications. This technology is simply and efficiently designed to maximize battery life, simplify network design and minimize implementation cost. It has low latency, supports broadcast and burst with a data rate of up to 20 kbps. It also supports star, tree and mesh topologies and its nodes can act as slaves or masters in a network of tens to hundreds of nodes in personal area networks and practical WSNs. ANT also provides cross-talk immunity [3].

One feature of ANT that must be emphasized is its extremely low power consumption compared to other wireless technologies and standards. This is achieved by allowing a system to spend most of its time in an ultra-low sleep mode, wake up quickly, transmit for the shortest possible time and then quickly return back to an ultra-low power sleep mode. Bluetooth power consumption is 10 times higher with 90% higher hardware cost. When compared to ZigBee, ANT is relatively less complex and presents a larger data rate of 1 Mbps [8]. However, ANT lacks interoperability because it is a proprietary technology.

Applications of ANT technology are found in various aspects of WSNs including sport, fitness and wellness applications, home health monitoring and industrial automation.

v. *WirelessHART*

It is an open wireless industrial sensor network standard that is based on the Highway Addressable Remote Transducer (HART) Protocol using the 802.15.4 – 2006 standard. Officially released in 2007 and majorly used for industrial control process and monitoring, WirelessHART is a secure and TDMA-based (usng10*ms* time slot) mesh networking technology that operates in the 2.4 GHz ISM band [11]. Other key features of WirelessHART includes network wide time synchronization, channel hopping, channel blacklisting, and industry standard AES-128 ciphers and keys.

WirelessHART provides a centralized WSN. The eight types of network devices defined by WirelessHART are network manager, network security, gateway, access point, field device, adapter, router and handheld device. These devices are connected to support network formation, maintenance, reliability, routing and security. The network manager is centralized and maintains up-to-date routes and communication schedules for the network, thereby guaranteeing the network performance. Features common to WirelessHART, Bluetooth, WiFi and ZigBee include the sharing of the unrestricted 2.4 GHz ISM band. But then, they are different from each other in some other aspects. Both WirelessHART and ZigBee are based on IEEE 802.15.4 standard. WirelessHART additionally uses channel hopping and channel blacklisting (useful to minimise persistence noise which is common in industrial set up) while ZigBee only utilizes Direct Sequence Spread Spectrum (DSSS) provided by IEEE 802.15.4. Like ZigBee, WiFi too does not support channel hopping. Like WirelessHART, Bluetooth supports time slots and channel hopping. But while Bluetooth is targeted at Personal Area Network (PAN) with a limited range of 10 metres and only supports star topology, WirelessHART network supports all types of network topology to enhance network scalability. These features make WirelessHART more suitable for industrial applications.

vi. *6LoWPAN*

IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is another open wireless communication protocol that is targeted on low-power applications that requires wireless internet connectivity at lower data rate and limited form factor. It was released by the IETF in 2007. It allows IPv6packets to be sent to and received from

low rate WPAN (IEEE 802.15.4) based networks, thus bringing IP to small devices such as sensor and controllers [18].

Comparing with ZigBee, they are both based on IEEE 802.15.4 standard. However, while 6LowPAN devices can interoperate with other IP-enabled devices, ZigBee node needs an 802.15.4 IP gateway to communicate with an IP network [8]. This IP interoperability makes 6LoWPAN a better option when considering applications that requires interfacing with IP devices or small packet sizes.

Popular wireless network standards such as WirelessHART utilize 6LowPAN to achieve fragmentation and reassembly. Applications of 6LoWPAN inWSNs are found in automation and entertainment applications in home, office and factory environments, security and safety, asset management, heath care and wellbeing etc.

6. CONCLUSION

ZigBee technology as a wireless sensor and control network is being considered as one of the most deployed wireless technologies in recent times as results of its attractive features to the users such as: open standard lightweight, low-cost, low-speed, low-power, interoperability protocol, among others. It is built on existing IEEE 802.15.4 protocol and therefore combines the IEEE 802.15.4 features and newly added features to meet required functionalities thereby finding applications in wide variety of wireless personal area networked systems. This paper has provided a general overview of the ZigBee sensor networking technology in which its definition, topology, applications and challenges have been presented.

Furthermore, the ZigBee stack protocol and other wireless sensor networking technologies were also discussed; this together with the general overview of the technology is to assist the users in considering the necessary factors when adopting the technology while allowing the vendors and the manufacturer of various ZigBee devices to work out the necessary improvements in the areas with deficiencies.

7. REFERENCES

[1] ZigBee Alliance.: Low-Power, IPv6 Networking for Home Energy Management. (2014). (Online). ZigBee Press, California. Available at: http://www.zigbee.org/920ip-low-power-ipv6-networking-for-home-energy-management-by-zigbee-alliance/ (Accessed 20 September, 2015).

[2] Abbagnale, A, Cipollone, E, Cuomo, F.: A case study for evaluating IEEE 802.15.4 wireless sensor network formation with mobile sinks, IEEE ICC, Rome. (2009)

[3] ANT.: Multi-Channel Design Considerations. (2012). (online). Dynastream Innovations Inc., Alberta. Available at: file:///C:/Users/Owner/Downloads/ANT_AN15_Multi_Channel_Design_Considerations%20(1).pdf (Accessed 23 July, 2015).

[4] Bell, B. S, Kanar, A. M, Kozlowski, S. W.: Current issues and future directions in simulation-based training in North America. The International Journal of Human Resource Management, Vol. 19, 1416–1436. (2008)

[5] Bluetooth T M.: Specification of the Bluetooth System; Bluetooth SIG Inc., Kirkland. (2005)

[6] Blum, B. M.: ZigBee and ZigBee PRO: Which feature set is right for you? EE Times. (2008). [online]. Available at: http://www.eetimes.com/design/microwave-rf-design/4019000/ZigBee-and-ZigBee-PRO-Which-feature-set-is-right-for-you- (Accessed 8 June, 2015)

[7] Bowers, B.: ZigBee Wireless Security: A New Age Penetration Tester's Toolkit. Cisco Press, (2012). (Online): Cisco Press. [Online]. Available at: http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4 (Accessed 2 July, 2015).

[8] Buratti, C, Conti, A, Dardari, D.: 2009. An overview on wireless sensor networks technology and evolution. (Online). (2009). Sensors 2009.9. 6869-6896. (2009)

[9] Cache, J, Wright, J, Liu, V.: Hacking Exposed Wireless: Wireless Security Secrets and Solutions. (2nd ed). McGraw Hill, London. (2010)

[10] Chandane, M, Bhirud, S, Bonde, S.: Performance Analysis of IEEE 802.15.4. International Journal of Computer Applications, (e-journal). Vol.40, No.5. (2012)

[11] Dargie, W, Poellabauer, C.: Fundamentals of wireless sensor networks: theory and practice. (e-book). John Wiley & Sons Inc., New Jersey. (2010)

[12] Johnstone, M. N, Jarvis, J. A.: Penetration of ZigBee-based Wireless Sensor Networks. A Proceeding of *Australian information Warfare and Security Conferenece*. (Online). (2011). Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1044&context=isw (Accessed 25 August, 2015).

[13] Kalita, H.K, Kar, A.: 2009. Wireless Sensor Network Security Analysis. International Journal of Next-Generation Networks (IJNGN). (e-journal), (2009). Vol.1, No 1. 1-10.

[14] Karl, H, Willing, A.: 2007. Protocols And Architectures For Wireless Sensor Networks. John Wiley & Sons, New Jersey. (2007).

[15] Kim, H, Caytiles, R.D, Kim, T.: Design of an Effective WSN-Based Interactive u-Learning Model. International Journal of Distributed Sensor Networks, (e-journal). (2012).

[16] Knight, M.: Wireless security-How safe is Z-wave?. Computing & Control Engineering Journal, (e-journal). (2006). Vol. 17, No. 6. 18-23.

[17] Ruiz-Garcia, L.: 2009. A review of wireless sensor technologies and applications in agriculture and food industry: state of the art and current trends. *Sensors*, Vol. 9, No. 6. 4728-4750. (2009)

[18] Shelby, Z, Bormann, C.: 6LoWPAN: The Wireless Embedded Internet. John Wiley & Sons, New Jersey. (2009)

[19] Silva, I, Guedes, L, Portugal, P, Vasques, F.: Reliability and Availability Evaluation of Wireless Sensor Networks for Industrial Applications. *Sensors, Vol.* 12, No. 1. 806-838. (2012)

[20] IEEE 802.15.4 Standard. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) IEEE; Piscataway, New Jersey. (2006)

[21] Loukas, G., Oke, G, Gelenbe, E.: Defending against Denial of Service in a Self-Aware Network: A Practical Approach. NATO Symposium on Information Assurance for Emerging and Future Military Systems. Ljubljana, Slovenia.(2008)

[22] Radmand, P.: ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys. Proceeding of International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. (2010). 465-470

[23] SNRG.: Smart Network Research Group. (Online), (2012). Available at: http://www.pafkiet.edu.pk/ Default.aspx?tabid=696 (Accessed 24 August 2015].