ZigBee Communication Protocol

A study on the ZigBee Communication protocol

1st Yashodhan Vishvesh Deshpande
Electronic Engineering student
Hochschule Hamm-Lippstadt
Lippstadt, Germany
yashodhandesh@gmail.com

2nd Lochana Abhayawardana
Electronic Engineering student
Hochschule Hamm-Lippstadt
Lippstadt, Germany
lochana.abhayawardana@stud.hshl.de

3rd Emirkan Sali
Electronic Engineering student
Hochschule Hamm-Lippstadt
Lippstadt, Germany
emirkan.sali@stud.hshl.de

***Abstract*—Low-rate wireless personal area networks are common in many sections of today's society. ZigBee is a communication protocol that works under the IEEE 802.15.4 standard to provide an easy, low-cost way of connecting different sensors and actuators for a vast area of application. This paper explains the ZigBee communication protocol specifications and dives deeper into its advantages and challenges, as well as its various areas of application in industry, home, medicine, and many more.**

***Index Terms*—ZigBee, IEEE802.15.4, wireless, network, WPAN, layers, data, security, transmission, applications, comparison**

I. Introduction

Wireless communication technology is one of the most important technological areas of this century and is now so widespread and widely used that it is involved in almost any application one can imagine. Even today, wireless technology is still being improved in the hope of finding more prevalent ways to use it. One of these ways is the connection of sensors and actuators through a wireless network. Over the course of the years, so-called wireless sensor networks (WSN) have become more common in almost every section of today's modern world.

WSN consist of actuators and sensors that are physically distributed in different parts of the application area. Such sensors or actuators could be temperature sensors, electricity sensors, motors, LEDs, and more. The sensors gather necessary information about their environment, while actuators influence it based on the given information. In any case, all the information is communicated with the central node of the network. This central node contains a processing element that can be used to save information, analyze it, or even visualize it. [1].

In reference [1] some general examples of application for WSN are as follows:

- Gathering medical information about patients in so called "Body-Area-Networks" [1].
- Automation of buildings e.g. smart home systems
- Surveillance of harmful substances in chemical companies or animal migration
- Automation of merchandise management systems in stores and markets
- Controlling and querying electric systems in medical environments
- many more...

With more benefits in dozens of areas of application, WSN have become a part of our industry, homes, and cities. To be able to build a functioning WSN, a wireless communication protocol is needed. Therefore, different standards of communication have been specified by larger groups of companies to allow for an easier and more uniform use of wireless technology. ZigBee is a communication standard protocol that functions as a low-rate wireless personal area network (LR-WPAN), i.e., a type of WSN in which limited power consumption is prioritized [2]. In reference [2] the main objectives of LR-WPAN are as follows:

- Easy installation.
- Transferring data reliably while maintaining an extremely low cost
- Having a simple and flexible protocol with an adequate battery life

Zigbee is specifically applicable for use in automation and control.

A. History of Zigbee

The Zigbee Communication protocol was developed by Connectivity standards alliance (CSA), former known as ZigBee alliance [3]. It's first release was in 2005 known as ZigBee 2004 [1]. CSA is a group of companies that dedicated themselves to developing IoT solutions and promoting those and especially their Zigbee standards. They have 5000+ Zigbee certified Products and consist of 500+ member companies [3]

II. IEEE 802.15.4 Standard

ZigBee is a communication protocol that is based on the IEEE 802.15.4 network specification and therefore uses its transportation services. To gain a further understanding of how the ZigBee protocol works and how it is not the same as the IEEE 802.15.4 standard, this section will discuss the IEEE 802.15.4 standard first [4].

A. IEEE 802.15.4 structure

IEEE 802.15.4 is a network that allows two different types of devices to participate in it [2]:

1) A full-function device (FFD)
2) a reduced-function device (RFD)

An FFD acts as the central node of the network, or, in this case, specifically as the personal area network (PAN) coordinator. An RFD serves as a simple sensor or actuator in the network without being capable of being a coordinator, thus being able to be implemented without any high cost or usage of resources. In a system of this standard, several components with radio interfaces implementing a physical layer and a medium access control (MAC) layer are included. To have a WPAN, one of these devices has to be a FFD that is responsible for communication with RFDs. [2].

B. Network topologies

A WPAN in IEEE 802.15.4 can function in two types of network topologies, and with ZigBee in two more types of network topologies [2]:

1) Star topology
2) Peer-to-Peer topology
3) Tree topology (with ZigBee)
4) Mesh topology (with ZigBee)

The star topology has different devices communicating with a single controller in the center of the network. This controller is also referred to as the PAN coordinator, and it is the primary control point for the PAN. The peer-to-peer topology functions in a way that every device can communicate with the other device in range as long as it is an FFD, but it also has a PAN coordinator as a primary controller [2]. Both topology types are visualized in figure 1 from reference [2]

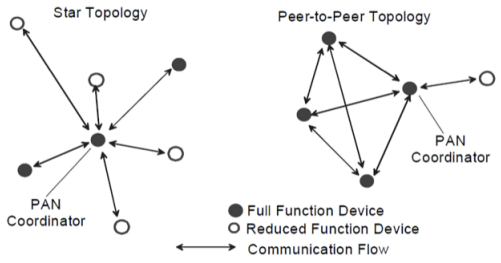

Fig. 1. Star Topology and Peer-to-Peer topology visualized [2]

C. Architecture

The architecture of IEEE 802.15.4 is simplified into different types of layers. To be specific, it contains at least one physical and one MAC layer, in which the physical layer is responsible for the radio frequency transceivers and low-level control and the MAC layer is responsible for transfer access [2]. A simple visualization is provided from [2] in figure 2

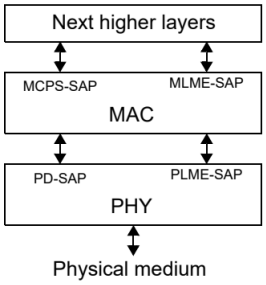

Fig. 2. Visualization of the layers in the IEEE 802.15.4 architecture [2]

III. ZigBee specifications

ZigBee expands on the two layers provided by the IEEE 802.15.4 standard by providing two additional layers above the MAC and physical layer: the network layer and the application layer [5]. This is visualized in figure 3 from reference [6].

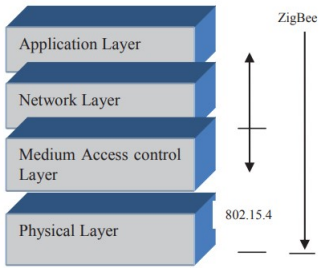

Fig. 3. Visualization of the layers in the ZigBee architecture from reference [6]

Each of the layers in the architecture have specific tasks to fulfill for the above layer. Every layer has an entity for data, which is responsible for data transmission, and an entity for managing every other task in the layer (management entity) [1]. ZigBee with all its layers is visualized in figure 4

Inside the application layer (APL), there is also the application support sub-layer (APS) and ZigBee device objects (ZDO), as well as the application framework [5].

A. Application Framework

The application framework consists of different application objects. Its main purpose is to embed the application that is to be developed. The application objects inside this framework can each fulfill a task that is important for the application. Each application object has a unique ID ranging from 1 to 240 [1].

B. ZigBee Device Object (ZDO)

ZDO inside the APL acts like an implemented application object with ID 0 that initializes the ZigBee layers and the security service provider of ZigBee. Furthermore, it also collects

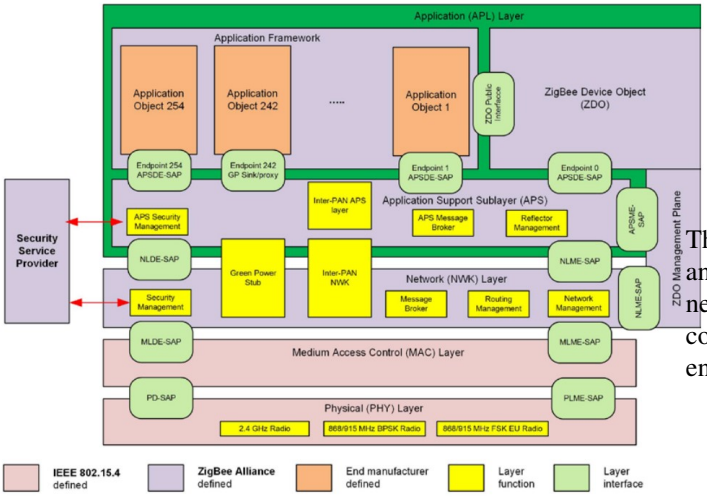

Fig. 4. Full visualization of the layers and sub-layers in the ZigBee architecture from reference [5]

information from several ZigBee end-devices that is necessary for management of the security, network, and binding [1].

C. Application support sub-layer

The APS layer uses a general set of services to provide an interface between the network layer and the application layer of ZigBee. Those services are provided by the APS Data entity and the APS Management entity, ultimately through service access points [5].

D. ZigBee data transmission rates

Because ZigBee is a low-data-rate, low-power consumption type of data transmission, its maximum speed of data transmission is 250 kbps using a 2.4 GHz frequency band. ZigBee's PHY layer uses three different frequency bands in general, which are [6]:

1) 2.4 GHz (Worldwide) with 16 channels and a 250 kbps data rate
2) 915 MHz (USA) with 10 channels and a 40 kbps data rate
3) 868 MHz (Europe) with 1 channel and a 20 kbps data rate

With that being stated, Manufacturers of systems that use ZigBee for communication are also free to use the frequency bands 780 MHz and 950 MHz for China and Japan respectively [1].

E. ZigBee Topologies

Three Network topologies are supported by the ZigBee network layer:

1) Star topology
2) Mesh topology
3) Tree topology

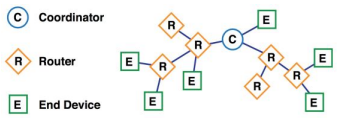

Fig. 5. ZigBee network [8]

The star topology is explained in Section 2, and in the mesh and tree topologies, the coordinator device chooses certain network parameters and starts the network [5]. Aside from the coordinator device, there are also ZigBee routers and ZigBee end-devices in the network topologies [1].

- ZigBee routers are responsible for routing in the network, i.e., determining the right path to the target device and passing on data packets [1].
- ZigBee end-devices are RFDs that are solely for communicating with the parent device, i.e., the router or coordinator. They are highly energy-saving and can switch to sleep mode when not in use [1].

IV. ZigBee Security Protocol

A. ZigBee Security Protocol Overview

ZigBee uses the basic security elements in IEEE Std. 802.15.4 security specification. It uses 128-bit encryption algorithms and has U.S. National Institute of Standards and Technology (NIST)-approved security features. Now ZigBee supports the **standard security**. Early versions of ZigBee security was divided into Residential security and High Security. [7]

B. ZigBee Security concepts and keywords

1) ZigBee's security policy: There are five key principles in ZigBee's security policy :

- Owner - The owner of ZigBee devices purchase the devices and needs to establish the network.
- Other user- Members of the household that would be using the system.
- Router - Routers in a Zigbee network act as intermediate nodes between the coordinator and the end devices.
- End device- End devices are user products such as motion sensors, contact sensors, and smart light bulbs. [8]

2) ZigBee security models: There are two different types of security models that ZigBee network is supporting those are centralised security model and distributed security model.

Centralized security model has the following features:

- Only coordinators/trust centers can start a network.
- Nodes join and receive the network key and establish a unique trust center key.
- Nodes must support install codes.

Distributed security model ha the following features:

- No central node/ trust center.
- Routers are able to start distributed networks.
- Nodes join and receive the network key. [8]

Security Key	Description	
Network-level Security		
Network key	• Essential key used to encrypt communications between all nodes of the network • Randomly generated by the Trust Centre • Distributed to joining nodes, encrypted with a pre-configured link key (see below)	
Application-level Security		
Global link key (pre-configured)	• Used between the Trust Centre and all other nodes • Pre-configured in all nodes (unless a unique link key is pre-configured - see below) • Also used in joining to encrypt network key transported from Trust Centre to joining node • If ZigBee-defined, allows nodes from all manufacturers to join the network • If manufacturer-defined, allows only nodes from one manufacturer to join the network • Touchlink Pre-configured Link Key is a key of this type • Distributed Security Global Link Key is a key of this type	
Unique link key	Optional key used to encrypt communications between a pair of nodes - may be one of:	
	Pre-configured unique link key	• Used between the Trust Centre and one other node • Pre-configured in Trust Centre and relevant node • Also used in joining to encrypt network key transported from Trust Centre to joining node • Install Code-derived Pre-configured Link Key is a key of this type
	Trust Centre Link Key (TCLK)	• Used between the Trust Centre and one other node • Randomly generated by the Trust Centre • Distributed to node encrypted with network key and pre-configured link key (if any) • Replaces pre-configured link key (if any) but application must retain the pre-configured key in case it needs to be reinstated
	Application link key	• Used between a pair of nodes, not including the Trust Centre • Randomly generated by the Trust Centre • Distributed to each node encrypted with network key and pre-configured link key (if any)

Fig. 6. Classification of the security key [8]

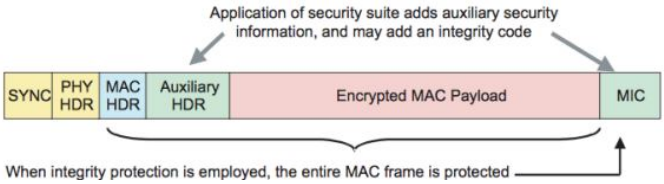

Fig. 7. MAC layer security of a frame [8]

3) ZigBee Security key: ZigBee uses 128-bit keys to communicate. The keys have two classifications which are network keys and link keys.

- Network key: Network key is shared by all devices in the network and is used for broadcasting communications. Used in centralized security model and at network layer. The network key also has a sequence number attached to it. This sequence number is used to identify a specific instance of the key. The sequence number is updated to identify which instance of the key is used so the data packet could be secured. The sequence number ranges from 0 to 255 and restart to 0 upon reaching 255.
- Link key: A link key is shared by two devices. Used in application layer security. [7]
  The figure 6 shows further classification of the security key and its applications.

C. MAC layer security

The MAC layer security is based on the security of IEEE 802.15.4 augmented with CCM (enhanced counter with CBC-MAC mode) . The MAC layer is responsible for its own security processing but the upper layers determine which keys or security levels to use. The figure 7 shows MAC layer security of a frame. [8]

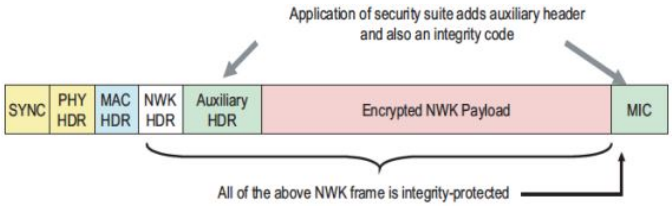

Fig. 8. Network layer security of the frame [8]

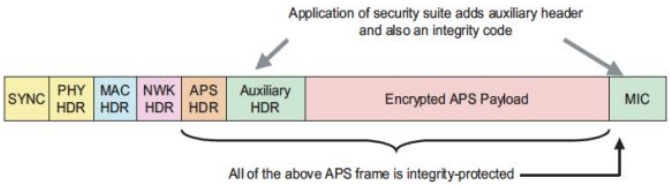

Fig. 9. Application layer security of the frame [8]

D. Network layer security

The Network layer is responsible for the processing needed to transmit outgoing frames and receive incoming frames. The frame format explicitly indicates the key used to protect the frame. Figure 8 shows the packet of network layer security. [8]

E. Application layer security

Earlier versions of ZigBee such as ZigBee 1.2 used a Trust Center Link Key for securing communications with a new device. This security feature had a "moment of insecurity" as the key was symmetric encryption key which could be decoded in that moment.

ZigBee 3.0 version replaced this security feature. The new feature has a process that requires a per-device installation code that is used to generate a unique joining key. Figure 9 shows the application layer security of the frame. [8]

F. Hop-by-Hop Security and MIC

Network security is secured through hop-by-hop process in ZigBee protocol. Every router verifies the encrypted packet before further processing. The router decrypts the package then checks the integrity of the packet. The router then re-encrypts the package with its own network parameters and then sends it to the next hop [7] .

Message Integrity Code (MIC) and is used to authenticate the message to check if the message has not been modified. A receiving device decodes the MIC encryption and verifies the value against the value appended to the message. If the value is incorrect the entire message is discarded. [7]

V. Application of ZigBee

A. Smart Home

Modern day smart homes are based on Internet of Things (IoT). The smart home system uses multiple sensors to collect data. The data can be from user input also. The system consists of actuators that respond to the incoming commands of the system or its user. ZigBee communication protocol can be

used to connect multiple devices to a hub in a mesh network. The hub is the master coordinator of the system that gives instructions to every other device.The ZigBee Alliance has developed a Home Automation standard [9].Manufactures of smart home devices use these standard for communications and operations with other devices. The following are the specifications for ZigBee Home automation.

B. Home Automation Clusters

The Home Automation clusters are group of smart home systems or sensors. They are classified based on their function: **General clusters** are common to all ZigBee Alliance profiles. **Measuring and sensing clusters** are used for measurement and sensing only. Examples of measuring and sensing clusters are luminance measurement, pressure measurement and temperature measurement. **HVAC clusters** (Heating, Ventilation and air conditioning) : HVAC clusters are used for controlling heating and cooling. Examples are a thermostat and fan control. **Security and safety cluster** are responsible for operations for security applications. Examples are intruder alarm system device.

C. Home Automation Network Requirements

The ZigBee standard recommended some requirements for Home Automation systems. They are as follows:

- Device polling rate is 7.5 second, except for commissioning, which can be higher.
- Channels 11, 14, 15, 19, 20, 24, and 25 are recommended to be used as the operating channels.
- HA uses standard security.
- ZigBee Standard defines the following startup attributes for different ZigBee devices : Short address set to 0xFFF, PAN ID set to 0, channel masks such as all channels in frequency band protocol version 2006 or higher

D. Commissioning

Commissioning is a method to setup a device in ZigBee network. Commissioning is a process that allows the installer to install devices, check networks operations and troubleshoot. This tool can be simple push button switch or laptop also. The ZigBee alliance uses three main types of commissioning modes:

- Automatic mode : Plug and play. In this mode the device configures itself.
- Easy mode : The devices contains some switches that the user configures to setup the device.
- System mode : A laptop or PDA device is used to install the device.

In smart home applications mainly the easy mode commissioning is used.

E. Smart Home ZigBee products

1) Amazon Echo (Fourth Generation): Amazon echo is a smart device that has various autonomous capabilities. It has various technologies in-built, such as WiFi connectivity and Bluetooth connectivity. The important feature of smart home uses the ZigBee standard for its operations. This product makes use of the ZigBee standard to control smart devices such as light bulbs, door locks and plugs. [10]

Fig. 10. Amazon Echo (Fourth Generation) [11]

This product makes use of the low-power consumption and close-proximity features of the ZigBee standard in the home automation applications.

- ZigBee versions 1.2 and 3.0 are supported and enabled as per the regulations of the ZigBee Alliance.
- This product uses 2.4 GHz frequency and has a range of 50 to 100 feet.
- This product has a built-in hub that enables it to control other home automation devices. It has enabled a custom ZigBee cluster called Works With All Hubs (WWAHu). The WWAHu is a standardized ZigBee cluster with the goal of improving interoperability between various IOT devices and major consumers and commercial platforms. The WWAHu is driven by ZigBee Alliance and has companies including Amazon, NXP, Samsung Smart Things and others. [12]. Figure 10 shows the product visual of the Amazon Echo (Fourth Generation).

VI. Advantages of ZigBee

1) Low power consumption
   One of the ZigBee's primary advantages is, it is designed to function on low-power and battery-efficient devices such as sensors, switches and remotes. This means that the user doesn't require to change the battery regularly. [13]
2) mesh capability
   Because of the mesh capability of ZigBee, the ZigBee devices can operate as a signal repeater by extending the signal range and its dependability. [13]
3) High Compatibility
   Next advantage of ZigBee is that it is based on a single standard, ensuring interoperability and compatibility among various devices and manufacturers. Without depending on the manufacturer, branding and model ZigBee devices may share commands and information using a common language and protocol. This provides you with additional options and flexibility for the users. Furthermore, there are more than 65000 ZigBee-enabled devices globally, which is greater than other protocols like Wi-Fi and Bluetooth. [13]

4) Security and Privacy
When compared with the other protocols, ZigBee has certain benefits regarding security and privacy. To safeguard the data and orders transferred between devices and the hub or the collector, ZigBee employs encryption and authentication. ZigBee has a different frequency than Wi-Fi, therefore it reduces signal interferences. Furthermore, ZigBee does not require Internet connections to function. Because of that it is restricted to its own network and the probability of getting data breach or the risks are minimum. [13]

VII. Disadvantages and Challenges to ZigBee

1) Security, privacy and compatibility.
ZigBee has plenty of security issues. If there is a lack of services or a theft to a certain node, it will affect whole entire node. If a hacker got access to the node he can manipulate a node in an illegal way. [14]
2) Implementation of the ZigBee network might be costly. There are several use cases for this. The availability of compatible items and the equipment also influence the price. The level of compatibility also influences the cost of a specific application. [14]
3) Channel noise
Because the most common protocols and devices like Bluetooth, cordless phones, microwaves and other wireless devices share the common band of 2.4 GHz, there may be channel noise appear. [14]
4) Low transmission rate
Because ZigBee is designed for low-rate data transmission, the technology used in it has a low bit rate. As a result, it has a lower transmission rate than WiFi and Bluetooth. Therefore ZigBee is unsuitable for high-speed data transmission. [14]
5) Incompatibility:
ZigBee has some incompatibility with common devices like smartphones and computers. [14]

VIII. Comparison to other wireless network protocols

This section is a comparison of ZigBee technology with Bluetooth, BACnet, HART protocol, RFID, z-wave and ISA-100 technologies.

Each protocol has its advantages and disadvantages. We should know them before designing a new IOT network.

A. Bluetooth

Bluetooth Technology was introduced by the Bluetooth Special Interest Group (SIG) [15]. Bluetooth is the most common and widely available technology which is used mostly as a connectivity method, Industry and home automation. Because it is easy to access because Bluetooth is enabled by default in most consumer devices like smartphones, laptops, headphones etc. There are three types of Bluetooth protocol. First is Classic Bluetooth, Bluetooth Low Energy and Bluetooth mesh.

Bluetooth classic is always short ranged technology and has higher bandwidth than ZigBee, is relatively power-hungry, and is designed for devices which can be recharged easily and regularly. [15]

However there is Bluetooth Low Energy (BLE) technology, it is also a low-energy, low-bandwidth, long-lasting battery. applications are similar to ZigBee. It is used in smartwatches, temperature monitors, cook pots etc. In most cases, it is used in tiny devices in which the battery need to last long. BLE has a range of 10m, therefore it is not usable for the long-range operabiliy required fields like agriculture or weather monitoring. [15]

Mesh capability: ZigBee configures it automatically. If the node is disabled or removed it has the ability to reconfigure it. No need to charge daily. ZigBee is open source. Therefore different manufacturers can communicate seamlessly. [15]

Both IoT protocols are vastly used for local communications

B. BACnet

Building Automation and Control Network (BACnet) is used in the Building Automation field. It is a worldwide standardized protocol. The common implementations of BACnet are Heating, Ventilation, air conditioning, elevator monitoring, Lightning control, access controls and security fire alarm systems monitoring. [16]

1) Comparison of BACnet and ZigBee: Mostly BACnet technology is a wired technology but ZigBee technology is wireless 900 MHz and 2.4GHz band. BACnet devices are functioning only in wired networks and required a line power connection. But, ZigBee works both wireless and wired and it is capable of being operated by battery. BACnet devices are always powered on devices. But ZigBee devices can either be turned on when required or also switch to sleeping mode when the service is not required. In this method, ZigBee is more power efficient than BACnet.

BACnet protocol has the Following data rates. 9.6 to 76.8 kbps (MS/TP), 9.6 to 56.0 kbps (PTP), Data Rates 78.8 kbps (LonTalk), 256 kbps156 kbps (A rcnet),10 to 100+ Mbps (BACnetIP) [17]. On the other hand, ZigBee uses 256 kbps which is way higher than BACnet. BACnet can be a Broadcast, multicast or unicast call. All the nodes on the Personal Area Network(PAN) can receive and reply through the BACnet network. ZigBee devices and the ZigBee coordinator must search and recognise each other o establish a connection. The connection will be encrypted and more secure than BACnet. The bandwidth of BACnet is a lot higher than ZigBee. [17]

C. The HART Protocol

Highway Addressable Remote Transducer (HART) is a globally standard bi-directional communication protocol which is functioning through analogue wires between smart devices. There are more than 20 million HART-enabled devices globally [18]. Different industries can implement HART

	BACNet	ZigBee
Governance	ASHRAE	ZigBee Alliance
Standard Established	1995	2004
Markets	Commercial Buildings	Commercial and Residential Buildings
Object Model	Well-Defined	Work-in-Progress
Network	Work various wired media No wireless	Wireless 900 mHz and 2.4gHz
Power	Line Powered Devices	Battery powered, Line Powered
Availability	Devices Always On	Devices Always On or Sleeping
Data Rates	9.6 to 76.8 kbps (MS/TP) 9.6 to 56.0 kbps (PTP) 78.8 kbps (LonTalk) 156 kbps (Arcnet) 10 to 100+ mbps (BACnet IP)	256 kbps
Network Technology	Multiple	Mesh

Fig. 11. comparison of BACnet and ZigBee [17]

in their preferred methods. This protocol can be used in the machines on the assembly lines, and manufacturing floor to communicate with each other [18].

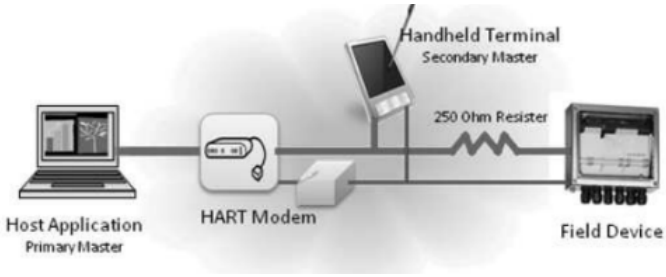

Fig. 12. The HART System [17]

HART is a low-risk and highly accurate, robust and reliable system. It's mostly used in industries and suppliers and it is not suitable for smart home applications. HART has some similarities to ZigBee, such as it functioning in the same 2.4GHz band, encryption enabled, and physical and MAC layers also sharing IEEE 802.15.4 standards. [18]

D. RFID

Radio Frequency Identification (RFID) is a communication protocol that is used to uniquely identify an object, animal or human. This wireless communication method uses electromagnetic or electrostatic coupling in the radio frequency section of the electromagnetic spectrum. [19] A RFID system always contains a scanning antenna, a transceiver and a transponder RFIDs are classified into two types. They are mobile readers and fixed readers. The devices should be connected to the network or to the internet and They can scan /activate different kinds of tags, which then transmit data back to the antenna. [19] Therefore it is used mainly in tracking and monitoring, Identification and authentication, Transport payments, passports or for location-based services [17]. RFID is functioning mostly in the frequency range of 13MHz to 900MHz frequency range. When the tag is surrounded by several things/obstacles 13MHz range is useful because it can pass through. But the drawback is it has a shorter range. However, 900MHz may transverse a wider range but has low penetrating power. Any type of data can be fed and saved into the RFID tags. [17]

1) Comparison between ZigBee and RFID: RFID and ZigBee are not competitors. As a matter of fact, there are circumstances where RFID is used to detect and identify objects. However, ZigBee technology is used for RFID to connect with non-RFID devices. As mentioned before these two technologies are working on different frequency ranges. ZigBee has a significantly greater range and has higher security mechanisms than RFID. Not like ZigBee, RFID is only a one-way communication protocol [17] .

E. Z-wave

Zensys, a Danish corporation, invented Z-wave. It has the same motivation as ZigBee which was It was created for wireless communication for Home automation. Z-wave is a low-bandwidth, half-duplex protocol and works at a frequency lower than 1 GHz, making it immune to interference from WiFi frequencies and Bluetooth frequencies. This technology is intended for modest data flow. It is typically used to deliver command messages like on-off, high-low and so on. The standard is provided under the non-disclosure agreement.

The z-wave protocol was made up of two sorts of devices. They are the controller and the slave. Controller devices are in charge of delivering orders to the nodes, slave nodes should execute the command or transmit it to devices that are outside the controller's immediate range. The controller has access to the whole network's routing table, allowing it to issue orders to any device on the network. The primary controller is the only one who has the power to add or remove devices from the network.

1) Comparison of Z-wave and ZigBee: The ZigBee alliance supports ZigBee, whilst the Z-wave alliance supports Z-wave. Both protocols are supported by a large number of market participants. Zigbee is supported by the key players such as Freescale, TI , etc. It is compliant with the IEEE 802.15.4 standards, whereas z-wave, created by Zensys is supported by the companies like Intel, Cisco, etc. The goal of ZigBee and Z-wave is to provide smart home automation and monitoring but, ZigBee offers a wider range of applications. Z-wave has 30 meters of range Without multihop, ZigBee has a wider range of 10 to 75 meters in the absence of multihop. Two technologies are incompatible with one another. [17]

F. ISA-100

The International Society of Automation (ISA) covers wireless manufacturing and control systems. The applications of this technology are Field sensors that can be Vertically linked from the field to business systems for monitoring, alarm, control and shutdown. REa-time field-to-business systems for example wireless equipment controlling work order systems, control LAN, etc are among the applications of this wireless technology. This technology can applied to fluid and material

	ZigBee	Z-Wave
Applications	Large	Mainly home and small industry automation
Data rate	250kbps	40kbps
Frequency	2.4GHz/900MHz	99MHz
Range	10-75m	30m
Cost	Cheaper	Expensive than zigbee
Nature	Openly Available	Proprietary to zensys

Fig. 13. comparison of Z-wave and ZigBee [17]

processing, and discrete components manufacturing sectors. [20]

1) Comparison of ISA-100 with ZigBee: The main advantage of using ZigBee because ZigBee-enabled devices have significantly longer battery life compared with ISA-100. ISA-100 is designed for industrial standards and the architecture is for wireless sensing in industries.[5] However, the main focus of the ZigBee is home automation.

IX. Conclusion

Considering all the information in this paper, ZigBee is an efficient low-data-rate communication protocol that is constantly updated and supported even to this day. Using the IEEE 802.15.4 standard of radio communication, ZigBee provides a reliable and power-saving method of creating networks with actuators and sensors and enables a way of communicating wirelessly with devices in these networks using low data rates.

The security protocol has been explained in this paper and consists of firstly, the security protocol overview and concepts and keyword related to the protocol. Then it also explains the ZigBee security models and security key features used. Security at every layer of the architecture is also explained.

The smart home applications of ZigBee are explained in this paper. It explains the home automation clusters and related concepts. Amazon echo product has been used as case study for real life application of ZigBee based smart home network. ZigBee protocol has its own advantages and disadvantages. It will depend on the application use case. The section like Advantages, Disadvantages and the challenges to ZigBee provides a clear idea that and It is a guide to select which protocol is to be best for each situation. Protocols like Bluetooth low energy have almost the same characteristics and have slightly more advantages than ZigBee and in the future, there is always room for upgrade.

X. Contributions to this paper

- Yashodhan Vishvesh Deshpande: wrote **ZigBee Security Protocol** section and **Application of ZigBee** section.
- Emirkan Sali: Wrote **Abstract**, **Introduction** section, **IEEE 802.15.4 Standard** section and **ZigBee Specifications** section.
- Lochana Abhaywaradana: Wrote **Advantages of ZigBee, Disadvantages and challenges to ZigBee, Comparison to other wireless network protocols** section.

References

[1] M. Krauße and R. Konrad, *Drahtlose Zigbee-Netzwerke Ein Kompendium*. Springer Vieweg, 2014, relevancy for paper: An entire german book with the topic of ZigBee, IEEE802.15.4 and WPAN.

[2] IEEE, "Ieee standard for low-rate wireless networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020, relevancy for paper: The newer IEEE802.15.4 standard from 2020 with all its specifications.

[3] Website of csa. Relevancy for paper: Main website of the developers of the ZigBee protocol. Information about its history etc. [Online]. Available: https://csa-iot.org/

[4] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, "Study on zigbee technology," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 6, 2011, pp. 297–301, relevancy for paper: A small study on the ZigBee technology with compact, useful information.

[5] ZigBee Alliance/Connectivity Standards Alliance. (2017) Zigbee specification. [accessed 31-May-2023, Relevancy for paper: The official Zigbee specs by the main developers of the protocol]. [Online]. Available: https://csa-iot.org/wp-content/uploads/2022/01/docs-05-3474-22-0csg-zigbee-specification-1.pdf

[6] Manpreet and J. Malhotra, "Zigbee technology: Current status and future scope," in *2015 International Conference on Computer and Computational Sciences (ICCCS)*, 2015, pp. 163–169.

[7] S. labs. An1233: Zigbee security. [Online]. Available: https://www.silabs.com/documents/public/application-notes/an1233-zigbee-security.pdf

[8] Xueqi Fan, Fransisca Susan, William Long, Shangyan Li. Security analysis of zigbee. [Online]. Available: https://courses.csail.mit.edu/6.857/2017/project/17.pdf

[9] A. Elahi, *Zigbee wireless sensor and Control Network*. Pearson, 2009.

[10] 1990. [Online]. Available: https://developer.amazon.com/en-US/docs/alexa/smarthome/zigbee-support.html

[11] Amazon. (2023) Amazon echo. [Online]. Available: https://www.amazon.de/-/en/generation-Smart-speaker-Alexa-Charcoal/dp/B085FXHR38

[12] Z. Alliance. The alliance announces the all hubs initiative. [Online]. Available: https://csa-iot.org/newsroom/all-hubs-initiative/

[13] P. Hub. (2022) Advantages and disadvantages of zigbee. [Online]. Available: https://www.polytechnichub.com/advantages-disadvantages-zigbee/

[14] (2022) Zigbee technology advantages and disadvantages — zigbee technology architecture and its applications. [Online]. Available: https://www.aplustopper.com/zigbee-technology-advantages-and-disadvantages/

[15] D. International. (2021) Zigbee vs. bluetooth: Choosing the right protocol for your iot application. [Online]. Available: https://www.digi.com/blog/post/zigbee-vs-bluetooth-choosing-the-right-protocol

[16] B. Committee. (2023) About bacnet. [Online]. Available: https://bacnet.org/about/

[17] C. Wang, T. Jiang, and Q. Zhang, *ZigBee Network Protocols and Applications*. CRC Press, 2014, ch. 11. [Online]. Available: https://learning.oreilly.com/library/view/zigbee-network-protocols/9781439816028/chapter-04.html

[18] I. Tools. (2023) What is hart protocol? [Online]. Available: https://instrumentationtools.com/what-is-hart-protocol/

[19] TechTarget. (2023) What is rfid (radio frequency identification)? [Online]. Available: https://www.techtarget.com/iotagenda/definition/RFID-radio-frequency-identification

[20] ISA. (2023) Isa100, wireless systems for automation. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa100