BEGHIN Léa
BRUGIERE Nathan
CHANFREAU Cédric
VALENTIN Maxime

5A PTP ISS

ZigBee Protocol

Introduction

Since the beginning of the internet of Things (IoT) in the 1980s, the number of communication protocols has grown consistently. Among them, ZigBee, introduced in 2003, has played a key role in enabling efficient communication between small devices.

Based on the IEEE 802.15.4 standard, ZigBee is renowned for its low power consumption and short-range capabilities, making it particularly suited for applications in smart homes and intelligent building systems. Supported by some of the world's largest companies, including Philips, Nest, Samsung, Texas, Siemens & Whirlpool, Zigbee technology is currently embedded in millions of smart home devices worldwide.

How does this protocol work, and what are the key advantages it offers in the IoT landscape? This report aims to present the characteristics of the ZigBee protocol, examining its structure and the specific advantages it offers in interconnected systems.

1. History and Evolution

In the 1990s, the first drafts of ZigBee-type networks appeared for applications where Wi-Fi and Bluetooth technologies were not usable. Based on Bluetooth technology, the ZigBee protocol was announced in May 2003. It is based on the Institute of Electrical and Electronics Engineers Standards Association's 802.15 specification.

ZigBbee technology is in constant evolution. Indeed, the ZigBee Alliance updates its specifications and boosts the IEEE 802.15.4 standard by adding network and security layers. Alliance members create standards that offer reliable, secure, low-power and easy-to-use wireless communication. The alliance is organized by committees, work groups, study groups, task forces and special interest groups.

For example, they recently implemented ZigBee PRO whose aim is to provide the foundation for IoT with features to support low-cost and highly reliable networks for device-to-device communication. ZigBee PRO also offers Green Power, supporting energy harvesting or self-powered devices that don't require batteries or AC power supply. There are also ZigBee RF4CE, designed for two-way device-to-device control applications, and ZigBee IP which optimizes the standard for IPv6-based full wireless mesh networks.

Figure1. ZigBee Alliance members [1]

ZigBee technology now consists of hundreds of companies across the world. It formed an alliance of companies that have signed up to use the protocol when they design and manufacture their products. The alliance now has over 400 members and between them, they have produced over 2,500 individual products that work with ZigBee.

2. Main Features

The ZigBee protocol has several features that distinguish it from other protocols, such as its topologies, low latency and low power consumption. ZigBee makes network configuration and device pairing quick and easy.

2.1. Range and frequency

Currently, there are 3 frequency bands that are assigned to ZigBee to use. The ZigBee WPANs operate on 2.4 GHz, 915 MHz and 868 MHz frequencies. The 868 MHz band is only available in Europe and the 915 MHz band in Australia and the US. The 2.4 GHz frequency band is the most commonly used because it can be used across the world.

The ZigBee technology is known for its very short range for transmission distances. Indeed, in order to limit power consumption, ZigBee only allows direct communication between products over limited distances from 10 to 100 meters depending on the obstacles present (e.g., partitions, walls, etc).

2.2. Connection time and number of participants

The time it takes to join a ZigBee network is also less than Wi-Fi and Bluetooth networks. It takes around 3 seconds to join a Wi-Fi network and 10 seconds for Bluetooth. ZigBee takes just 30 milliseconds to connect.

ZigBee also supports both small and large networks. In theory, 65,000 devices can be connected to a single ZigBee network but in reality, this is around 240.

2.3. Open Source

Being an open protocol, ZigBee has the advantage of being very accessible. However, since its inception, one of its greatest strengths has also been one of the biggest obstacles to its popularization. Since it is open source, ZigBee's specifications can be modified, improved and customized. This can affect its compatibility and therefore its accessibility. For a long time, ZigBee lacked a common foundation that would guarantee its use in all circumstances, and this is precisely what was resolved in 2015 with ZigBee 3.0. This feature makes ZigBee easy to implement for businesses.

2.4. Data transfer

Whereas Wi-Fi uses around 11 Mbps and Bluetooth uses 1 Mbps, ZigBee uses between 20 Kbps and 250 Kbps. This is a very small amount of data, but it is still sufficient enough. Even at 250 Kbps, ZigBee transfers data around four times faster than Bluetooth and forty times faster than Wi-Fi.

2.5. Power consumption

One of the major advantages of using ZigBee is that it consumes considerably less power. Indeed, the devices spend the majority of their time in a power-saving mode, they will typically run for several years without the batteries needing to be changed.

The power consumption of a ZigBee device can be estimated based on its operation modes, namely the transmission mode and the idle or sleep mode. In this analysis, we will consider a typical ZigBee device that transmits data intermittently, with a maximum data rate of 250 kbps, while remaining in a low-power sleep state most of the time.

Assumptions:

- Maximum transmission rate: 250 kbps
- Data transmission: 100 bytes (800 bits) transmitted every 10 seconds
- Power consumption during transmission: 40 mW
- Power consumption in sleep mode: 50 µW
- Observation period: 1 hour

Step-by-step Calculations:

1. **Transmission Duration**:

The duration of each transmission is calculated based on the data rate:

$$t = \frac{800\ bits}{250\ kbps} = 0.0032 \text{ seconds}$$

Thus, each transmission takes 0.0032 seconds.

2. **Energy Consumption per Transmission**:

The energy consumed during each transmission is calculated by multiplying the power consumed during transmission by the transmission time:

$$E_{Transmission} = 40\ mW \times 0.0032\ s = 0.128 \text{ mJ}$$

Therefore, each transmission consumes 0.128 millijoules.

3. **Number of Transmissions per Hour**:

With one transmission every 10 seconds, the number of transmissions in one hour is:

$$\frac{3600\ seconds}{10\ seconds/transmission} = 360 \text{ transmissions}$$

4. **Total Energy Consumption for Transmissions**:

The total energy consumption for 360 transmissions in one hour is:

$$E_{Total\ transmission} = 360 \times 0.128\ mJ = 46.08 \text{ mJ}$$

5. **Energy Consumption in Sleep Mode**:

During sleep mode, the device consumes much less power. The total sleep time in one hour can be calculated as:

$$Sleep\ time = 3600\ seconds - (360 \times 0.0032\ seconds) = 3598.848\ seconds$$

The energy consumed during sleep mode is:

$$E_{Sleep} = 0.05\ mW \times 3598.848\ seconds = 179.94\ \text{mJ}$$

6. **Total Energy Consumption in One Hour**:

The total energy consumed in one hour is the sum of the energy consumed during transmission and in sleep mode:

$$E_{Total} = E_{Total\ transmission} + E_{Sleep} = 46.08\ mJ + 179.94\ mJ = 226.02\ \text{mJ}$$

7. **Total Number of Bits Transmitted in One Hour**:

Since each transmission consists of 800 bits, the total number of bits transmitted in one hour is:

$$Total\ bits\ transmitted = 360 \times 800 = 288\ 000\ bits$$

8. **Average Power Consumption per Bit**:

The average power consumption per bit is calculated by dividing the total energy consumed in one hour by the total number of bits transmitted:

$$Average\ energy\ per\ bit = \frac{226.02\ mJ}{288\ 000\ bits} = 784.72\ \text{nJ/bit}$$

Converting this to watts per bit:

$$P_{Average/bit} = \frac{Energy\ per\ bit}{Transmission\ time\ per\ bit} = \frac{784.72\ nJ}{\frac{1}{250\ kbps}} = 196\ \text{nW/bit}$$

This power efficiency is achieved by allowing ZigBee devices to operate primarily in low-duty-cycle modes, where nodes are inactive most of the time and only wake to transmit or receive data briefly. As a result, ZigBee networks can maintain long battery life across devices, even in noisy environments where retransmissions may be necessary, optimizing overall power use while keeping the per-bit energy cost low.

All the characteristics seen above can be summarized in the table below.

Features	Description
Shorter delay	15ms—30ms
Low rate	1kB/S—250kB/S
Large capacity	Can support up to 255 devices
Multi-band	2.4GHz、868MHz and 915MHz
Security	Provides data integrity checking, and a AES-128 encryption algorithm
Low power consumption	Two ordinary route 5th battery can be used 6 months to 2 years (standby mode)

Figure 2. ZigBee most important features [1]

3. Physical Layer

The physical layer is the lowest protocol layer, and is responsible for controlling and activating the radio transceiver, and for selecting the channel frequency and monitoring the channel. It also enables communication with the radio devices. Communication of data or commands is done using packets. This layer does modulation and demodulation operations upon transmitting and receiving signals.

3.1. Modulation and Spectrum

ZigBee protocol uses the DSSS (direct-sequence spread spectrum). The direct-sequence modulation makes the transmitted signal wider in bandwidth than the information bandwidth. This spreading technique reduces the risk of interference, improving transmission reliability.

ZigBee uses offset quadrature phase shift keying (O-QPSK) to provide a balance between energy efficiency and interference resistance. This modulation method is based on QPSK and is used to transmit digital data. In conventional QPSK, data is encoded in phases (0°, 90°, 180°, 270°) but the transitions between these phases can be abrupt, causing sudden amplitude variations that make the signal more sensitive to interference. The OQPSK corrects this problem by introducing a time shift (an offset): the transitions of the two signal components (In-phase, I and Quadrature, Q) are shifted by half a bit period. This means that the two components never change simultaneously. This softens phase variations, reduces interference and makes the signal more stable, which is particularly useful in wireless environments.

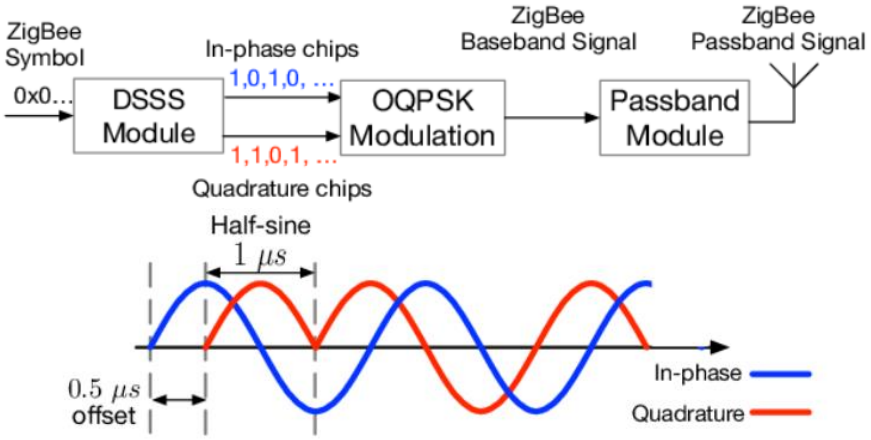

Figure 3. ZigBee transmitter architecture and baseband signal [2]

As said before, ZigBee operates on three frequency bands: 2.4 GHz with 16 channels, 915 MHz with 10 channels and 868 MHz with 1 channel in Europe. Thus, this protocol owns 27 channels that need to be managed. This is the role of the physical layer which defines and organizes them.

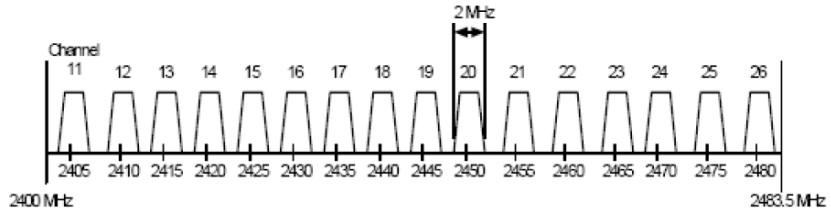

Figure 4. Channels on ISM band [3]

The transmit power is -3 dBm, and the receiver sensitivity reaches -85 dBm. Therefore, this protocol transmits a weak signal to save energy (0,5 mW), while the receiver is sensitive enough to pick up weak signals, enabling reliable communication over short to medium distances.

3.2. PHY Packet Structure

Each physical packet (PHY Packet) consists of three elements:

- Synchronization Header (SHR): Ensures reception synchronization, with a 4-byte (4B) preamble and a 1-byte packet delimiter.
    - Preamble ensures synchronization
    - Packet delimitation marks the start of the packet
- Physical Header (PHR): Specifies the length of the data unit and contains packet control information.
- PHY Payload (PSDU): Provided by the upper layers, it carries the data or commands. The total length of PPDU packets is typically 22 bytes (176 bits).

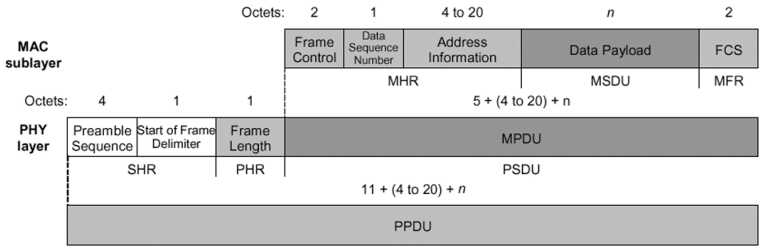

Figure 5. PHY/MAC Packet Structure [3]

These packets ensure efficient transmission with a packet error rate (PER) of 1%, corresponding to a bit error rate (BER) of 5.7e-5.

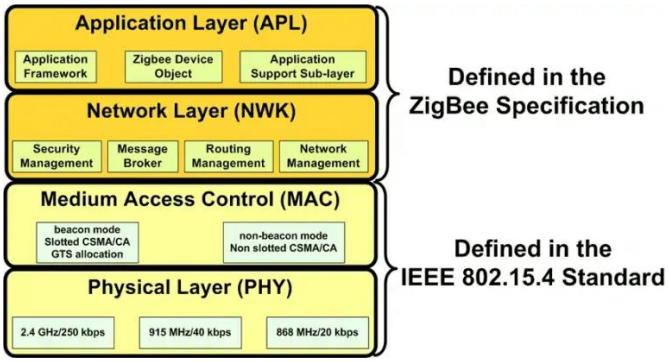

Figure 6. ZigBee Layers [4]

4. MAC Layer

The ZigBee MAC (Medium Access Control) layer coordinates access to the radio channel and guarantees reliable data transmission through a CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism, adapting to network configurations with or without beacons. As an interface between the physical and network layers, it synchronizes communication by generating beacon frames broadcast by the coordinator to align devices in a beacon-based network.

4.1. MAC Frame Structure

The structure of the MAC frame is divided into the following parts.

- MAC Header (MHR): Contains information about addressing, security, and control of the frame type (beacon, data, acknowledgement, or command).
- MAC Payload (MSDU): Contains data or commands from higher layers, of variable size.
- MAC Footer (MFR): Includes a 16-bit frame check sequence to validate the integrity of the transmitted data.

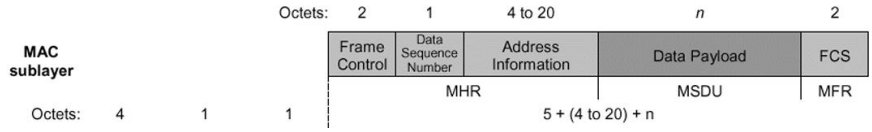

Figure 7. MAC Packet Structure [3]

Depending on their type, frames play essential roles.

- Beacon frames: These frames are broadcast periodically by the coordinator to synchronize the devices on the network. They contain important information such as the PAN ID and synchronization parameters, enabling devices to organize themselves efficiently and save energy. For example, a sensor uses Beacon frames to know when to transmit or go into sleep mode.
- Data frames: These frames are used to transfer useful data between devices. They carry collected information, such as sensor readings (temperature, humidity, etc.), to the coordinator or between network nodes. For example, a sensor sends its readings to the gateway via a data frame.
- Acknowledgement frames (ACK): These frames are used to confirm that a frame has been received correctly. When a device sends data, the receiver returns an ACK frame to indicate that the transmission has been received without error. This ensures reliable communication and allows the sender to retransmit in the event of failure.
- Command frames: These frames are used to carry out specific operations required for the network to function. They are used for tasks such as requesting to join the network (association), leaving the network (disassociation), or changing certain parameters. For example, a newly activated device sends a command frame to ask the coordinator for authorization to connect.

4.2. MAC Layer Operating Modes

ZigBee offers two operating modes for the MAC layer, the beacon network and the non beacon network.

Beacon Mode:
Beacon Mode is an operating mode where communication is organized in superframes (16 equal slots). Nodes are coordinated using beacon frames. Here is a breakdown of its components:

- Superframe : The superframe structures time into 16 equal intervals called slots, and these intervals are coordinated by periodic beacons to synchronize the nodes in the network. Each superframe is delimited by a Beacon frame sent by the coordinator, which allows all the devices in the network to follow the same schedule and know when they can transmit or go to sleep.
- CAP (Contended Access Period): CAP is a contention period where multiple devices can attempt to access the communication channel at the same time. The devices must synchronize to avoid collisions by listening to the channel and transmitting when it is free. During this period, devices use a mechanism such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to manage access to the channel.
- CFP (Contention Free Period): The CFP is a contention-free period where devices have dedicated time slots to transmit their data. These slots are allocated in a predefined way by the coordinator, often using a time-division multiplexing (TDMA) mechanism. This enables more reliable and predictable communication, as each device knows exactly when it can transmit without interfering with the others.
- Synchronization Beacon: The Synchronization Beacon is a beacon frame sent at the start of each superframe to ensure network synchronization. It allows all the devices to be aligned to

the same calendar and to know exactly when to start the contention period or the non-contention period, as well as when to go into standby.

- Idle Period: The Idle Period is the period when devices have no data to send and can enter sleep mode to save energy. During this period, the nodes remain inactive until the next superframe starts. This mode extends the battery life of the devices without compromising the overall synchronization of the network.

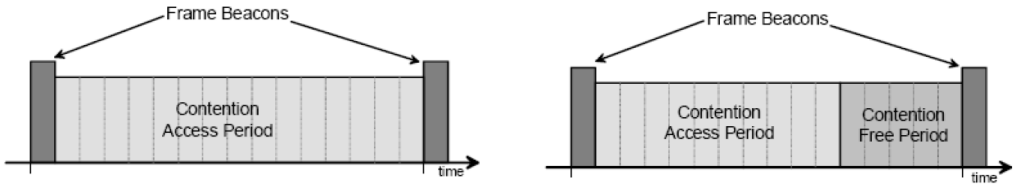

Figure 8. Tags and super frame [3]

Beaconless Mode:
In this configuration, there is no sending of a periodic beacon unless it is requested by a node. This allows more flexible channel access. Moreover, unslotted CSMA-CA are used without strict synchronization. It is suitable for applications requiring connection flexibility.

4.3. Data Transfer Methods

Data transfer varies depending on the type of communication. Direct transfer is suitable for exchanges between devices or between a device and the coordinator. Indirect transfer is used exclusively for coordinator-to-device communication, where the device periodically checks for data availability, allowing it to enter sleep mode between checks. Finally, in beacon networks, devices use gated time slots (GTS) for priority transmissions.

4.4. Unsplit CSMA-CA algorithm

The non-split CSMA-CA allows access to the channel in case of inactivity. In case of collision, the device waits for a random back-off delay before retrying access. The BE (Back-Off Exponent) determines the length of this delay. It is calculated by choosing a random number in a time interval. This interval becomes wider with each new transmission attempt after a collision.The number of back-offs (NB) is a variable that tracks the number of failed attempts to access the channel, and the waiting time becomes longer with each new attempt. This mechanism makes it possible to manage channel conflicts effectively and improve network performance.

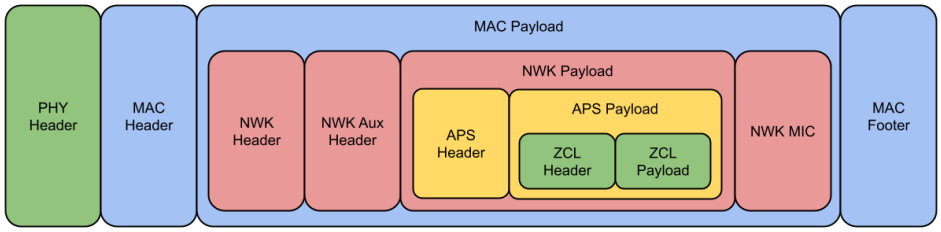

Figure 9. Frame Structure [5]

There are other layers quite important in ZigBee protocol such as the network layer and the application layer.

The network layer handles all network-related operations, such as network setup, connection and disconnection of end devices, routing, and device configurations. The application layer, being the highest layer in the network, is responsible for hosting application objects that include user applications and ZigBee Device Objects (ZDOs).

The ZigBee PHY layer is optimized for reliable and energy-efficient communication, while the MAC layer provides efficient and secure channel access, with mechanisms to save energy and adapt the network configuration. The choice of the operating mode (with or without beacon) depends on the application needs, such as the need for synchronization or the flexibility of the connections.

5. Topology

As seen above, one of the main characteristics of ZigBee is its ability to support multiple topologies. Indeed, there are three main types of ZigBee network topologies: star, mesh, and tree. A topology simply refers to the layout and arrangement of different elements within a communication network.

A key component of the ZigBee protocol is the ability to support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node. Connections between nodes are dynamically updated and optimized.

A mesh network employs one of two decentralized connection arrangements: full mesh topology or partial mesh topology. In a full mesh topology, each network node is connected directly to other nodes. In a partial mesh topology, some nodes are connected to all the others, but some are only connected to nodes they exchange the most data with.

The ZigBee protocol defines three types of nodes: coordinators, routers and end devices. Although all nodes can send and receive data, they each play a different role. There is one coordinator in each network whose job is to store information about the network, including security keys. Routers are intermediate nodes, relaying data from other devices. End devices can talk to the coordinator or a router, but can't relay data from other devices.

This operation is transparent to the user and greatly increases communication distances and reliability. The mesh topology is well suited for smart homes as they will usually have more devices than other topologies.

The star topology is the least expensive type of ZigBee to implement. There are no routers and all of the end devices communicate directly with the coordinator. The problem with this setup is that if the coordinator fails, the whole network will crash and none of the end devices will work given that there is no one there to give them their instructions. Star networks are also limited by the range of the coordinator itself and therefore really only suitable for the smallest of networks that consist of just a couple of devices.

The tree topology is very similar to the mesh topology with the only difference being that the routers are not interconnected. The coordinator connects to all of the nearby routers and the routers connect with the nearby end devices. The routers don’t associate themselves with each other and only communicate with the coordinator and the end devices.

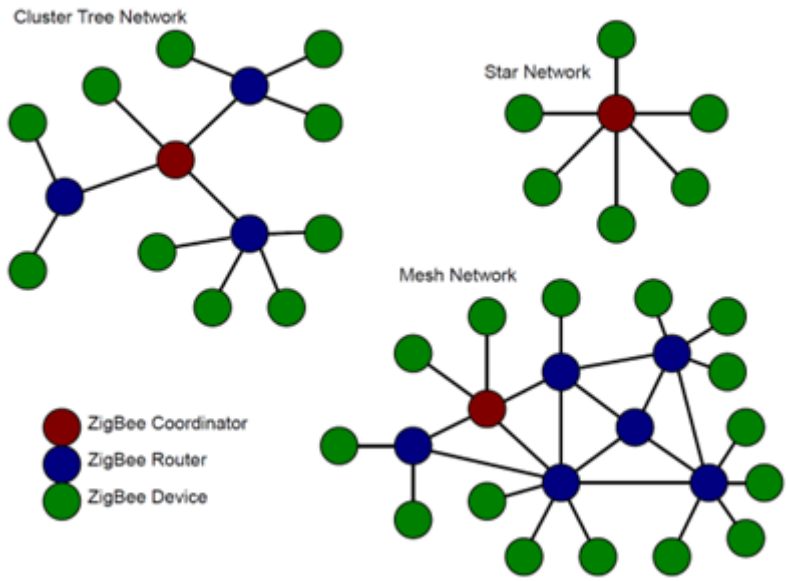

Figure 10. Graphic of the three topologies [6]

6. Security

Security in ZigBee is essential due to its widespread use in sensitive applications like smart homes, and healthcare. ZigBee includes several security mechanisms to protect data and ensure the reliability of communication within its networks. However, given the open-source nature of ZigBee and its adoption across various devices, some vulnerabilities and risks still exist.

6.1. Key Management and Security Layers

ZigBee's security architecture builds on the IEEE 802.15.4 standard with layered security at both the network and application levels:

- Network Layer: Manages access and encrypts messages with network keys shared among all devices and device keys unique to each device. A central coordinator distributes the network key to authenticated nodes.
- Application Layer: Provides end-to-end encryption between devices to add protection in sensitive applications, with custom security based on each application's needs.

6.2. Encryption and Authentication

ZigBee uses AES-128 encryption to secure data during transmission, a widely accepted standard for its strength and efficiency. Mutual Authentication is employed so both sender and receiver verify each other's identity, preventing unauthorized access.

6.3. Access Control and Data Integrity

Access control ensures only authorized devices communicate within the network, while Message Integrity Codes (MICs) maintain data integrity, verifying that messages haven't been altered in transit.

6.4. Security Modes

ZigBee supports two security modes:

- Standard Mode: Uses shared network keys, suitable for basic applications.
- High-Security Mode: Used primarily in ZigBee PRO networks, with link keys added for specific device-to-device encryption.

6.5. Vulnerabilities in ZigBee

Despite strong security measures, ZigBee faces a few vulnerabilities:

- Network Key Exposure: If one device is compromised, shared network keys can be exposed, threatening the whole network.
- Replay Attacks: Attackers can intercept and replay data packets to disrupt network operation, though MICs mitigate this.
- Key Reuse: Using the same network key across devices or networks increases vulnerability.
- Device Management: Retiring devices improperly can create lingering access points for attackers.

6.6. ZigBee 3.0 Security Enhancements

ZigBee 3.0 strengthens security by standardizing protocols for improved interoperability and updating its key exchange mechanisms to reduce risks during key distribution. Enhanced compatibility for updates and patches also allows for better security across devices.

7. Some applications

Example 1: Smart Lighting in a Connected Home

A smart lighting system using ZigBee allows for controlling and automating the lighting in a home. In this setup, several connected light bulbs and a smart wall switch are linked through a ZigBee network. A central hub connected to Wi-Fi enables control of the lighting via a mobile app.

ZigBee-connected bulbs allow for switching on/off, adjusting brightness, and changing color. The ZigBee wall switch replaces a traditional switch and enables control of the lights without needing a smartphone. The ZigBee hub acts as the network coordinator and connects to Wi-Fi, allowing for remote control through a mobile app. The mobile app provides configuration, scheduling, and control of the lighting.
The central hub establishes the ZigBee network by connecting all the bulbs and switches and communicates with Wi-Fi to enable remote control. When a command is sent from the mobile app (for example, to turn on all lights in the living room), the hub transmits this command to the bulbs via the ZigBee network. If a bulb does not directly receive the hub signal, it can receive it via another bulb that relays the signal through the mesh network.

Advantages of ZigBee in This Context:
The system is energy-efficient, which extends the lifespan of the devices. The mesh network extends coverage, allowing each bulb to relay the signal. Additionally, thanks to its interoperability, devices from different brands can communicate within the same network.

Example 2: Temperature/Humidity Monitoring System in a Factory

A ZigBee network is used in a factory to monitor temperature and humidity conditions in sensitive areas. Temperature and humidity sensors send real-time data to a ZigBee coordinator, which then transmits the data to a central server for analysis.

Temperature and humidity sensors equipped with ZigBee are installed in critical areas of the factory. ZigBee routers serve as relay nodes, strategically placed to extend network coverage. The ZigBee coordinator connects to a central server to collect and send monitoring data. The monitoring server receives the data and triggers alerts if abnormal conditions are detected.

The sensors collect temperature and humidity data and periodically send it to the coordinator. If a sensor is too far from the coordinator for direct transmission, it sends its data through a ZigBee router that relays the information. The monitoring server analyzes the data in real time and can trigger an alert if thresholds are exceeded. The mesh network structure ensures reliable data transmission even in the complex environment of a factory.

Advantages of ZigBee in This Context:
The sensors are battery-operated with low energy consumption, minimizing maintenance. The mesh network structure allows data to circumvent obstacles within the factory, ensuring transmission even in dense environments. Finally, the deployment is flexible, with sensors and routers easily added or repositioned according to needs.

Conclusion

In summary, ZigBee stands out as an ideal wireless communication technology for applications requiring low energy consumption and reliable connectivity within extensive networks. With its strengths in energy efficiency, network meshing, and interoperability, ZigBee simplifies the integration and control of numerous devices, especially in smart home automation, industrial applications, intelligent lighting, and energy management. Its flexibility and robustness make it an especially relevant choice for improving equipment management and automation while optimizing energy resources and reducing operational costs. ZigBee, therefore, represents an essential asset in the development of modern and sustainable connected solutions, adaptable to the current and future needs of both our daily lives and infrastructure.

Image References

[1] What is Zigbee? | Definition from TechTarget
[2] What is ZigBee Technology and How does it works? Electrical Technology
[3] Poly_reseau_mobile
[4] Zigbee Stack Layers
[5] Autopsie of a Zigbee Frame
[6] How Does Zigbee Work? Everything You Need to Know - Home Network Geek

References Used Throughout the Report

The sources listed below have been consulted for all sections of the report and serve as general references for understanding the ZigBee protocol, its structure, applications, and comparisons with other wireless technologies.

Qu'est-ce que Zigbee ? En savoir plus sur la technologie de maillage sans fil Zigbee | Digi International
ZigBee — Wikipédia
How Does Zigbee Work? Everything You Need to Know - Home Network Geek
ZigBee Technology : Architecture, Working and Its Applications
Bluetooth contre WiFi contre Zigbee: Quelle technologie sans fil est la meilleure
Protocole ZIGBEE : Définition et produits compatibles
Domotique : mais au fait, c'est quoi le protocole ZigBee ?
Qu'est-ce que Zigbee ? Explication sur la technologie de réseau de lumière intelligente la plus populaire au monde | Homey
ZigBee : découvrez le protocole de communication pour l'IoT
Tips for Optimizing Performance and Energy Use of ZigBee Radios
How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4 | IEEE Conference Publication | IEEE Xplore
Zigbee Technique de l'ingénieur