Journal of Electronics and Electrical Engineering
https://ojs.wiserpub.com/index.php/JEEE/

Article

Wireless Sensor Network Based Gas Monitoring System Utilizing ZigBee Technology

Alberto Coboi[1], Minh T. Nguyen[1,*], Kien T. La[1] and Thang C. Vu[2]

[1]Department of Electrical Engineering, Thai Nguyen University of Technology, Thai Nguyen, Vietnam
[2]Department of Electronics Engineering, Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam
* E-mail: nguyentuanminh@tnut.edu.vn

Received: 22 July 2023; **Revised:** 9 October 2023; **Accepted:** 17 October 2023

Abstract: This paper presents a ZigBee-based wireless network gas monitoring system, utilizing ZigBee technology to enable reliable and low-cost communication. The system leverages small sensor nodes and ZigBee protocols to collect data on physical phenomena, particularly gas levels, in various environments. The network's low-power consumption and extended range capabilities allow for effective gas sensing within a radius of up to 300 meters. While interoperability with devices from different manufacturers remains a limitation, the system showcases the versatility of ZigBee technology in diverse fields. The study evaluates the system's performance through simulation and experimentation, addresses potential challenges, and proposes future developments to enhance ZigBee-based wireless network gas monitoring systems, offering improved remote monitoring and manipulation capabilities. Furthermore, our research contributes to the advancement of wireless sensor network technology by demonstrating the practicality of ZigBee in gas monitoring. The findings from our experiments and simulations provide valuable insights into the optimization of such systems, which can have far-reaching impacts on environmental monitoring, safety, and industrial processes. In addition, our proposed enhancements pave the way for more reliable and efficient remote monitoring and control, offering substantial benefits for various industries, including environmental management, industrial automation, and beyond.

***Keywords*:** ZigBee, wireless network, gas monitoring system, small sensor nodes, ZigBee protocols, data collection, physical phenomena, remote monitoring

1. Introduction

Our suggested approach is driven by the revolutionary potential of Wireless Sensor Network (WSN) technology. The advent of Wireless Sensor Networking technology has brought about significant changes to our everyday lives. The Internet of Things (IoT) is a rapidly developing technology that will allow us to connect multiple physical objects and transform our everyday interactions. As a result, seamless communication is becoming more and more necessary, particularly in fields with high activity levels [1,2].

We may now collect data on physical events that were previously difficult or impossible to capture using conventional approaches by leveraging networks of small sensor nodes [3]. There are a wide range of industries in which this technology finds use, including the military, healthcare, agriculture, home intelligence, home monitoring, industrial process control, warfare, child education, surveillance, and microsurgery [4,5].

Nodes in wireless sensor networks communicate without physical cables. Rather, transceivers facilitate wireless data and control signal transmission and reception to and from a central control center. Wireless sensor

Copyright ©2023 Alberto Coboi, et al.
DOI: https://doi.org/10.37256/jeee.2220233418
This is an open-access article distributed under a CC BY license
(Creative Commons Attribution 4.0 International License)
https://creativecommons.org/licenses/by/4.0/

networks use the frequency spectrum as their communication medium, and their nodes are battery-powered [6]. Many technologies are used in wireless sensor networks, including Bluetooth, ZigBee, Z-wave, Apple iBeacon, Wavenis, Wi-Fi, EnOcean, RFID, LoRaWAN, Insteon, Cisco Intelligent Proximity, x10, and many more. [6] and [7].

ZigBee, recognized as IEEE 802.15.4, is a universally accepted standard encompassing both hardware and software. It has been tailor-made to cater to the needs of wireless sensor networks characterized by their need for robust performance, affordability, energy efficiency, scalability, and limited data transfer speeds. To tackle the issues related to the compatibility of ZigBee/IEEE 802.15.4 protocol stacks, the ZigBee alliance is committed to finding solutions [8]. Networking and message routing techniques are used to optimize the performance of ZigBee applications, which build upon the physical layer. ZigBee includes various security provisions and options to ensure secure communication and device control, enhancing the overall security framework [9].

The ZigBee protocols are designed to facilitate the automatic establishment of low-speed ad-hoc networks comprising nodes. Within extensive networks, these nodes have the capability to create clusters, form a mesh, or function as a single cluster. ZigBee protocols offer support for both beacon-enabled and non-beacon-enabled networks. In non-beacon-enabled networks, channel mechanisms like CSMA/CA are employed. In such heterogeneous networks, ZigBee routers' receivers need to remain active consistently, which demands a robust power source. Conversely, other nodes can transmit data when they detect external stimuli [9].

ZigBee operates in three radio bands: 868MHz, 915MHz, and 2.4GHz. It offers a range of 300 meters and consumes low power. It can accommodate up to 6000 devices. However, one limitation is its lack of interoperability with devices from different manufacturers. Despite this limitation, ZigBee has relatively low installation costs [9].

It's crucial to remember that Bluetooth and Wi-Fi are not the same as ZigBee. ZigBee was created especially for simple data transfer via sensors, whereas Bluetooth and Wi-Fi were built for communication involving huge amounts of sophisticated data, such as media files and software [10].

The increasing demand for efficient wireless networking across a wide range of low-power devices led to the creation of ZigBee. Compact transmitters are integrated into production floor devices in the next generation of automated manufacturing, which is where ZigBee finds uses in industrial settings. Precise remote monitoring and control are made possible by this integration's smooth connectivity with a central computer [2–10].

ZigBee was developed in response to the growing need for effective wireless networking across a variety of low-power devices. ZigBee is used in industrial settings, where it is integrated into production floor devices in the next generation of automated manufacturing. The seamless connectivity of this integration with a central computer allows for precise remote monitoring and control [2–10].

The rest of this paper is organized as follows. We address different ZigBee applications in Section 2. ZigBee technologies are provided in Section 3. Different data routing mechanisms are considered in Section 4. Simulations and results are showed in Section 5. Finally, conclusions and future work are addressed in Section 6.

2. ZigBee Applications

ZigBee devices are employed in many automated systems because of their exceptional communication capabilities. Automation of buildings, medical monitoring, low-power sensors, HVAC control, embedded sensing, smoke and intruder alerts, home and office automation, industrial automation, remote wireless microphone configuration, smart irrigation, and smart agricultural [11].

2.1 *Home Automation*

Home automation was not first thought to be one of the commonly envisioned uses for sensor networking. Today, it may be the application with the greatest volume shipping volume of ZigBee mesh networks. This market is moving swiftly due to a number of variables, including how quickly consumer products are produced and introduced to the market. The two main categories of applications that were first introduced to the market were comfort and awareness/safety.

Sensor networking offers a wider range of uses within homes, whereas typical home automation chores like lighting and audio/video management have traditionally prioritized comfort and convenience in their products.

Certain items are designed to make homeowners more aware of the state of their house without requiring a full-fledged security system. Others, meantime, are starting to stress how sensor and control technologies might be used to encourage energy conservation [12,13].

2.2 *Monitoring and Controlling Power*

A smart grid is an electrical grid that has been upgraded such that generation, transmission, distribution, and customers are all connected not only electrically but also via a robust communication network with the market, with operators, and with service providers. It is crucial to identify an appropriate protocol in order to establish a strong communication link between them. A significant part of monitoring and direct load regulation for effective power utilization is played by ZigBee [14,15].

2.3 *Heating, Ventilation and Air Conditioning (HVAC Control)*

The advent of ubiquitous computing has resulted in our houses and buildings being heavily instrumented, with networks and devices being used to monitor and control a variety of building environment elements. This covers things like comfortable temperature, indoor air quality, illumination, and noise levels. Because smart energy systems continuously monitor, control, and utilize contextual information throughout these building environments, they have the potential to improve the energy efficiency of buildings. To fully utilize the potential of developing and implementing smart energy systems that aim to lower energy consumption while maintaining occupant comfort, it is imperative to conduct a thorough analysis of the building's surroundings [16,17].

This sophisticated type of agricultural automation requires close observation of meteorological conditions at the ground level and quick data transfer to a central database. Decisions and control over agricultural equipment are made on the central server, which has powerful processing power. The following elements make up the precision farming system [18]:

- Agricultural parameter sensing,
- Location identification and data collection,
- Data transfer from crop field to control station for decision-making,
- And calculation and control decisions based on sensed data are all included.

Currently available on the market are agricultural sensors, positioning systems for locating these sensors, and a variety of actuators such as foggers, sprinklers, and valve-controlled irrigation systems. The technology needed to transmit sensor data wirelessly from crop fields to distant servers, however, have not advanced much [18].

2.4 *Medical Monitoring*

Centralized data collection is made easier by giving medical equipment with wireless capabilities, such as infusion pumps, ventilators, and vital sign monitors. Numerous medical devices use ZigBee technology to handle issues with data frequency, patient data security, and the practicalities of patient mobility while linked to these devices. Other advantages that arise when these devices are integrated into a ZigBee or other wireless sensor network are the elimination of connections, improved mobility, and position management. Once connected to the network, these devices can also take advantage of the architecture of other nearby wireless sensor networks of a similar nature [19].

2.5 *Power Monitoring*

Wireless Sensor Networks (WSNs) have a plethora of industrial, consumer, and commercial applications that demonstrate their great potential. Utilizing the IEEE 802.15.4 standard, ZigBee offers specifications for Low Data Rate Wireless Personal Area Networks (LR-WPANs) that are designed to accommodate low-power control and monitoring devices. Compared to conventional wired networks, it has many benefits, including cost-effectiveness, low power consumption, minimum environmental impact, and ease of network organization. Long-term use and dependability are guaranteed by the smooth compatibility of ZigBee's two feature sets. The IEEE 802.15.4 standard is improved by the ZigBee specification, which adds network and security layers along with an application framework. Building on this base, the Alliance has created public application profiles, or standards, that make it possible to create interoperable solutions across several vendors. Manufacturers are free to create their own manufacturer-specific profiles for tailored applications in where interoperability is not required [15–21].

2.6 *For Smart Grid*

The Smart Grid represents the integration of cutting-edge sensor, network, communication, new energy, and IT technologies into the electric power system. This integration aims to empower the existing electrical network with capabilities like self-healing, interactivity, compatibility, integration, optimization, and security. ZigBee will harness its unique technical strengths to play a significant role in power grid development. This role encompasses network safety management, operations and maintenance, data collection, security surveillance, parameter measurement, and user engagement. ZigBee's adoption will provide robust support for enhancing power grid intelligence and achieving the integration of information, business processes, and power management [22].

3. The ZigBee Technology

While sensors and controllers don't need a lot of bandwidth, they do need very little delay and very little energy to guarantee longer battery life, particularly in situations where there are several devices involved [23]. ZigBee technology makes it possible to deploy trustworthy wireless networks widely while providing simple and affordable solutions. It is appropriate for the economical support of resilient mesh networking technologies since it enables devices to run for prolonged periods of time on reasonably priced primary batteries [23]. Figure 1's representation of the IEEE 802.15.4 standard lists the following layers of the Zigbee protocol:

- Network Layer (NWK): Supports various network typologies: star, tree, mesh.
- Application Layer: Houses ZigBee Device Objects (ZDOs) for device management.
- Security Layer: Implements AES encryption with 128-bit keys.
- Physical Layer (PHY): Utilizes DSSS modulation for data transmission.
- MAC Layer: Encapsulates data for transmission.

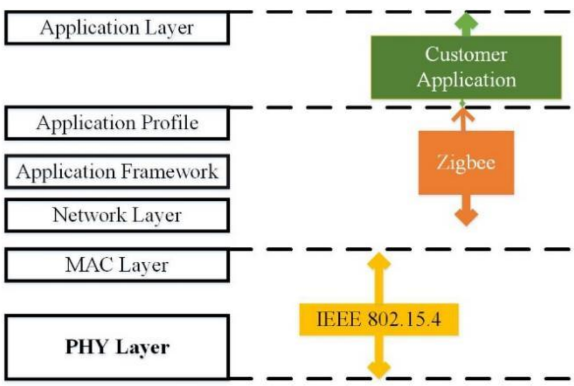


Figure 1. ZigBee stack

3.1 *Network Topologies Supported in Zigbee Technology*

Star topology, the network consists of one central controller that has dedicated point-to-point link with each device. Packets between the devices have to go through the ZigBee coordinator. This topology is very transparent and easy to expand and is used in industries where all the end point devices are needed to communicate with the controller [24].

Mesh topology, also known as a peer-to-peer network, in which numerous paths are established by connecting one device to other devices. There is just one controller, several routers, and an infinite number of end devices in this topology. Compared to star topology, it eliminates dead zones and makes adding or deleting end devices considerably simpler [24].

A cluster tree topology, is one in which clusters are created by establishing a parent-child relationship. A Cluster ID is given to each cluster. IEEE 802.15.4 does allow cluster tree structure, however ZigBee does not [24].

3.2 *ZigBee Network Devices and Their Operating Modes*

There are two kinds of devices in a Low-Rate Wireless Personal Area Network (LR-WPAN): Full Function Devices (FFDs) and Reduced Function Devices (RFDs). RFDs can only be used as end nodes and do not have routing capabilities. Their parent node, which granted them access to the network, is the only entity with which they can communicate. Conversely, FFDs can be set up to function as the PAN coordinator and have routing capabilities. Regardless of whether they are FFDs or RFDs, every node in a star network talks only with the PAN coordinator [25].

A single PAN coordinator remains in a peer-to-peer network, but it is accompanied by more FFDs. These FFDs are able to communicate with other FFDs and RFDs in addition to the PAN coordinator. Three operational modes are supported by IEEE 802.15.4: PAN coordinator, coordinator, and end device. Any of these modes of operation can be set up for FFDs. Within the ZigBee environment, the PAN coordinator is just called "coordinator." It is important to note that the IEEE term "coordinator" in ZigBee nomenclature refers to a "router" [25,26].

There are two communication modes in a ZigBee network: beacon mode (a) and non-beacon mode (b). A coordinator that runs on batteries will use beacon mode in an effort to save electricity. In this mode, a device watches for messages addressed to it and periodically receives beacons sent by the coordinator. The coordinator schedules the next beacon transmission for that particular device after message transmission is complete [26,27].

The device has the ability to switch to sleep mode once it recognizes the impending schedule. On the other hand, a coordinator running on the primary power source employs non-beacon mode. Within a mesh network, every device is aware of the timetable for communication between them, thus in order to avoid missing the signal, they must wake up at predefined intervals. As such, the gadgets need to be equipped with precise timing mechanisms [27].

This suggests that energy consumption will increase. For devices that are mostly in a "sleep" state, such as smoke detectors and burglar alarms, non-beacon mode communication is a good fit [27]. There are Zigbee features in Table 1.

Table 1. Features of the ZigBee technology

Parameter	Value
Data rate	250 kbs, 40 kb/s
Topology	Star or Peer-to-Peer
Addressing	16-bit (Short) or 64-bit (extend)
Multiple Access Technique	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Frequency	868 (Europe) 915 MHz (North America) 2.4 GHz (Worldwide)
Range	10–20 meter
Channels	11 channels (868/915 MHz) 16 channels (2.4 GHz)

3.3 *ZigBee Addressing Range*

The method by which a message travels throughout a network is called ZigBee Addressing. As Table 2 illustrates, postal (snail) mail utilizes a single address type that is widely recognized:

Table 2. ZigBee addressing

Name	Range	Description
Channel	11–26	A physical portion of the RF spectrum
PAN ID	0x0000–0x3fff	The address of a network within a channel
NwkAddr	0x0000–0xfff7	The address of a node within a network
Endpoint	1–240	The address of an application within a node
Cluster	0x00–0xff	The object within the application
Command	0x00–0xff	An action to take within the cluster
Attribute	0x0000–0xffff	A data item within the cluster

Both application layer and device addressing are supported by ZigBee. The destination address of the device to which a packet is intended is specified via device addressing. Application layer addressing provides a message type field called a Cluster ID in addition to identifying a specific application receiver, or ZigBee endpoint [28].

3.4 *ZigBee Protocol Specifies Two Address Types: 16-Bit and 64-Bit Addresses*

- ✓ Condensed address 16-bit Network Address: Upon entering a network, a node is given a 16-bit Network Address. Every node on the network has a unique network address, however it is subject to change. Data delivered to a destination device's 16-bit network address is required for ZigBee. This means that a procedure known as "Address Discovery" must be carried out in order to find the 16-bit network address before sending the data.
- ✓ 64-bit long addresses: Every node has a distinct 64-bit address. Because it uniquely identifies a node, the 64-bit address is permanent. It is a factory-assigned number that cannot be altered.

A distributed address assignment mechanism is used in ZigBee to assign network addresses to devices. The maximum number of children of a router (C_m), the maximum number of child routers of a router (R_m), and the network depth (L_m) are all determined by the coordinator prior to the network being formed. Keep in mind that a router's child can also be an end device, therefore $C_m \geq R_m$. At most Rm child routers and at least $C_m - R_m$ child end devices can be had by each coordinator and router. The assignment of device addresses occurs top-down.

The entire address space is rationally divided into $R_m + 1$ blocks for the coordinator. The coordinator's child routers are to be awarded the first Rm blocks, and the coordinator's own child end devices are to be allocated the last block. The following equation [29,30] explains how each router calculates a parameter called C_{skip} from C_m, R_m, and L_m to determine the starting addresses of its children's address pools.

$$C_{skip}(d) = \begin{cases} 1 + C_m x(L_m - d - 1) & if\ R_m = 1 \\ \dfrac{1 + C_m - R_m - C_m R_m^{L_m - d - 1}}{1 - R_m} & otherwise \end{cases} \quad (1)$$

4. Deploying Zigbee in WSNs

4.1 *Routing Protocols Used in Ad-Hoc WSN Especially in ZigBee Network*

A wireless sensor network uses a large number of dispersed sensors to perform wireless communication-based sensing tasks over a given geographic area. In order to facilitate the transfer of data from a source node to a destination (sink) node, a routing protocol that is capable of recognizing paths must be used. Owing to their restricted power source, these sensor nodes are widely dispersed and prone to malfunctions. As such, large, highly packed sensor networks may not be a good fit for many traditional ad-hoc routing techniques [31–33].

Research on routing protocols in sensor networks has recently exploded in activity and importance. To guarantee proper data delivery, sensor routing algorithms need to be resilient to failures, energy-efficient, and safe from hacked or malicious nodes [31,32]. As a result, we offer proactive, active, and hybrid protocols for the ZigBee Wireless Sensor Network. Figure 2 illustrates how these protocols might be simplified.

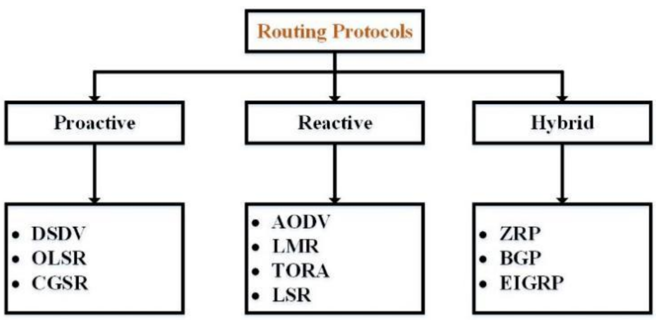


Figure 2. Routing protocols used in Ad-hoc WSN especially in ZigBee network

4.2 *Proactive*

Setting up routing paths before data transfer is part of the proactive routing strategy. The information about changes in the nodes' network structure is communicated to nearby nodes, who then update their own data. DSDV is a well-known illustration of a proactive routing technology [34]. Proactive routing protocols save routing information on each node for all other nodes in the network (or nodes located in a certain area). This routing data is usually kept in many tables [35].

4.2.1 Destination Sequence Distance Vector (DSDV)

The distance vector routing protocol is known as DSDV. The Bellman-Ford routing method serves as its foundation. A proactive routing protocol is called DSDV. With the hop-by-hop protocol known as DSDV, every network node keeps a routing table current. Every potential destination node and the number of hops needed to get there are listed in a routing table [25]. The destination node assigns a sequence number to each item in the routing table, indicating the route's recentness and preventing the creation of routing loops. Routing tables keep consistency by updating messages on a regular basis [25].

4.2.2 The Optimized Link State Routing Protocol (OLSR)

OLSR is designed for ad hoc mobile networks. It functions as a proactive, table-driven protocol, which means that it routinely exchanges topological data with other network nodes. A group of neighboring nodes is chosen by each node to serve as "multipoint relays" (MPR) [36]. Only nodes designated as these MPRs in OLSR are in charge of forwarding control traffic meant to be distributed throughout the network. By lowering the necessary number of transmissions, MPRs offer an effective method for flooding control traffic [36,37].

These routing algorithms' performances are compared with respect to energy consumption, packet loss, traffic load, and delay. As a result, the following parameters are briefly described: throughput, energy consumption, packet loss, delay, and network load [38].

4.2.3 Cluster-Head Gateway Switch Routing Protocol

A cluster head is chosen once the mobile nodes have been grouped together into clusters. Every node inside the cluster-head's communication range is a member of that cluster. Any node that can communicate with two or more cluster heads is considered a gateway node. Frequent cluster-head elections in a dynamic network can lead to a decline in performance [34–39].

The packet is sent to its cluster head by its source. The packet is forwarded from this cluster-head to the gateway node, which establishes a connection between this cluster-head and the subsequent cluster-head on the path to the destination. The gateway forwards it to that cluster-head and so forth, continuing in this manner until the destination cluster-head is reached. The packet is subsequently sent to the destination via the destination cluster-head. An illustration of a CGSR routing architecture is shown in Figure 3 [19–29].

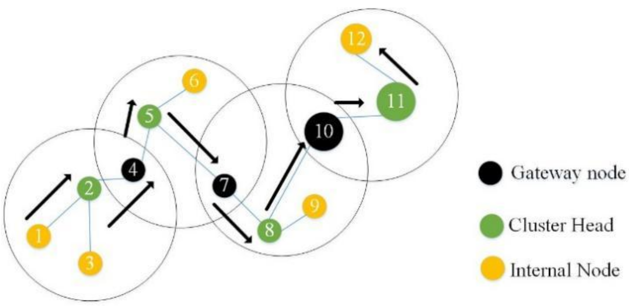


Figure 3. Cluster-head gateway switch routing protocol

4.3 *Reactive*

Only active routes are maintained by the reactive type, which sets the routing table on demand. AODV is a popular reactive routing protocol [40].

4.3.1 Ad-Hoc On-Demand Distance Vector (AODV)

Based on DSDV and DSR, AODV is an additional version of the standard distance vector routing technique. It uses a similar route discovery approach to find routes whenever needed because it shares the on-demand features of DSR. In contrast to DSR, which keeps several route cache entries for each destination, AODV uses traditional routing tables, with one item for each destination. After gaining experience with the DSDV routing algorithm, the first design of AODV is started. While repairing broken links, AODV offers loop-free routes similarly to DSDV, however it does not require global periodic routing announcements. AODV offers other noteworthy properties in addition to lowering the quantity of broadcasts that arise from a link break [41,42].

There is never any additional overhead for the packets when a route is available from source to destination. The route discovery process, however, is only started when a route is either not in use or has expired and is then deleted. This tactic lessens the consequences of outdated routes and the requirement for maintaining underutilized routes. The capability of AODV to facilitate broadcast, multicast, and unicast communication is another unique characteristic. The unicast route reply massage is used by AODV after a broadcast route discovery process. For a more detailed explanation of these methods, see Figure 4 [41–43].

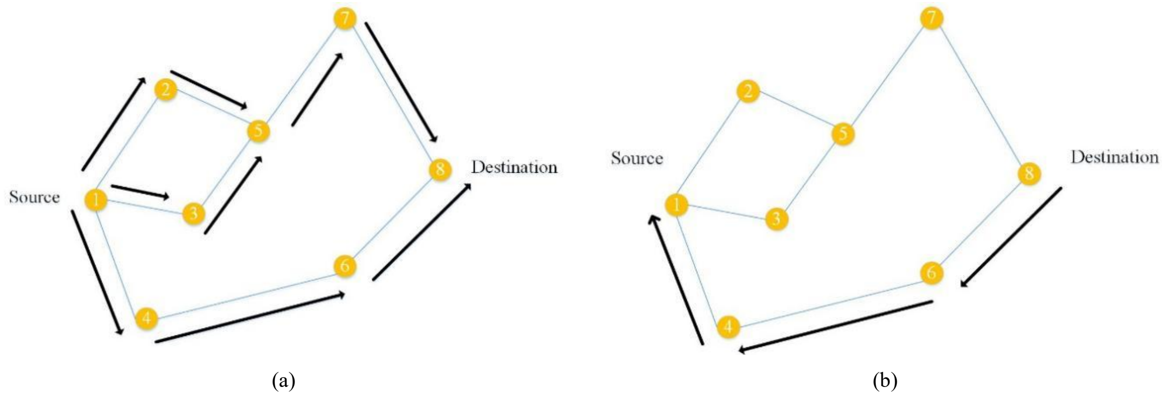


Figure 4. (a) Propagation of route request (RREQ) packet, (b) Path taken by the route reply (RREP) packet. Route discovery in AODV.

4.3.2 Light-Weight Mobile Routing (LMR)

Another on-demand routing technology that uses a flooding strategy to create routes is the LMR protocol. Nodes in the LMR have several paths to every place they need to go. By allowing nodes to select the next accessible route to a given destination without starting a route discovery process, this improves the resilience of the protocol. The fact that each node in this protocol only keeps routing data for its close neighbors is an added bonus. By using this method, further delays and storage costs related to keeping routes complete are avoided. However, it's important to remember that LMR might sometimes produce temporary invalid routes, which can cause further delays in figuring out the right path [35].

4.3.3 The Temporally-Ordered Routing Algorithm (TORA)

Figure 5 shows TORA, which is an extremely flexible distributed routing method used in Mobile Ad hoc Networks (MANETs). Its main purpose is to create several paths to a location while making sure none of them are circular. To carry out its primary functions, which include route creation, maintenance, and erasure, TORA mostly depends on the services offered by the Internet MANET Encapsulation Protocol (IMEP) [43]. One of TORA's most notable features is its capacity to lower the amount of control messages that are sent throughout the network. This is accomplished by asking nodes to submit a path request only in the event that they genuinely need to send a packet to a given location [43].

The node first sends a QUERY packet to its neighbors in order to establish a route. Until it reaches the target or an intermediary node with a path to it, this QUERY is repeated throughout the network. Subsequently, the UPDATE packet, which specifies its height relative to the destination, is broadcast by the QUERY packet recipient. Each node that gets the UPDATE packet during packet propagation in the network adjusts its height to a number higher than the neighbor from whom the UPDATE was received [43].

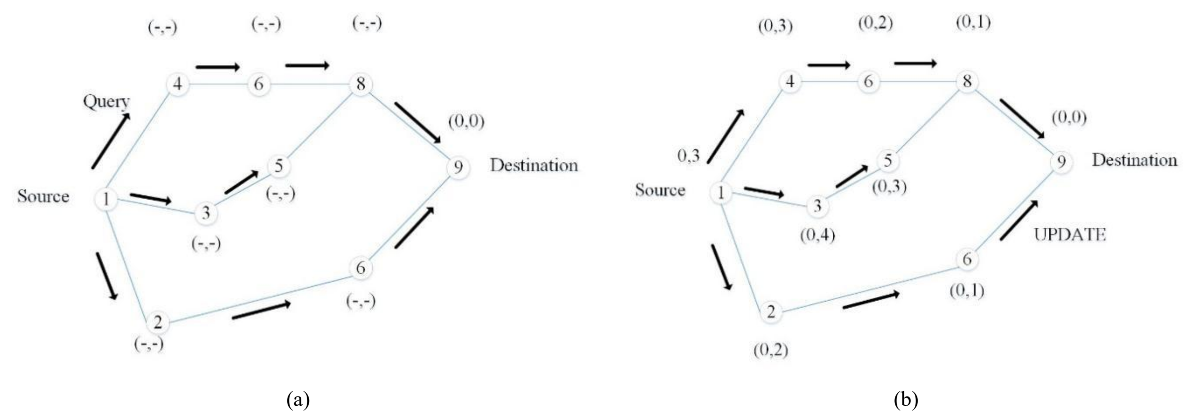


Figure 5. (a) Route creation in TORA. (b) Route creation in TORA. The Temporally ordered routing algorithm (TORA).

4.4 *Hybrid Routing Protocols*

Certain hybrid routing methods are suggested to combine the benefits of proactive and reactive protocols, based on a combination of demand-driven and table-driven routing protocols. Zone routing protocol is the most common hybrid [25–44].

4.4.1 Zone Routing Protocol (ZRP)

In ZRP, every node adopts a proactive stance by exclusively preserving topological data inside the boundaries of its designated routing zone, which is a predetermined area surrounding it. ZRP makes use of this routing zone structure by using a method called border-casting. By using border-casting, a node can send messages only to its peripheral nodes—that is, the nodes that are located at the perimeter of its routing zone. Most importantly, it keeps these signals out of the hands of non-peripheral nodes. ZRP effectively obtains route discovery by starting border-casting of a route query to all of the source node's periphery nodes. If the destination node is beyond of these peripheral nodes' individual routing zones, they will continue to border-cast the query to their own peripheral nodes [45,46]. This process is repeated recursively.

5. Simulations and Results

5.1 *System design of Gas Monitoring System ZigBee*

This is the general schematic for the Gas Monitoring System using Zigbee Technology. Designing a gas monitoring system using ZigBee technology requires careful consideration of the requirements, sensor selection, network topology, node design, communication protocol, and central monitoring system design as it is at Figure 6.

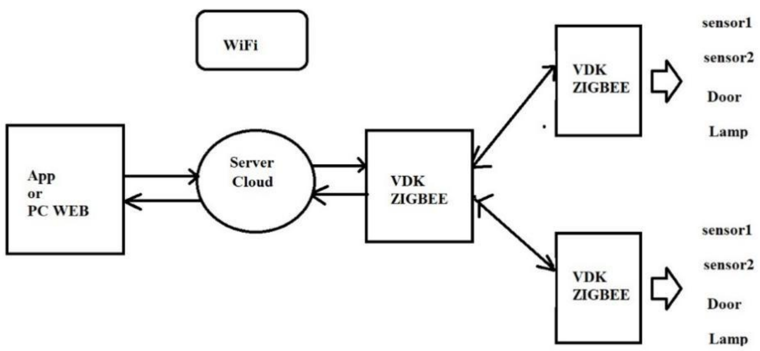


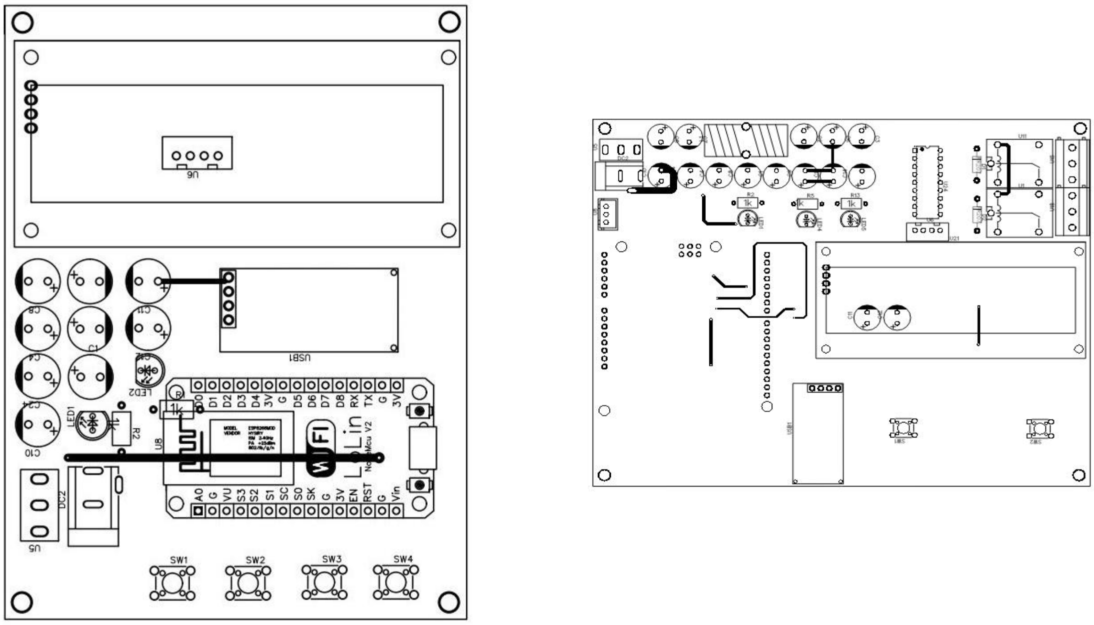
Figure 6. System design of gas monitoring system using ZigBee technology

The first step is to identify the requirements of the gas monitoring system, including the types of gases to be monitored, the measurement range, the accuracy required, the sampling frequency, and the communication range.

And not far from the above idea, our system contains a Zigbee base station (Coordinator), two Router directly connected with DHT sensors. On other hand, the Zigbee coordinator is connected to the cloud through Wi-Fi, so that the data will be shown in PC Website.

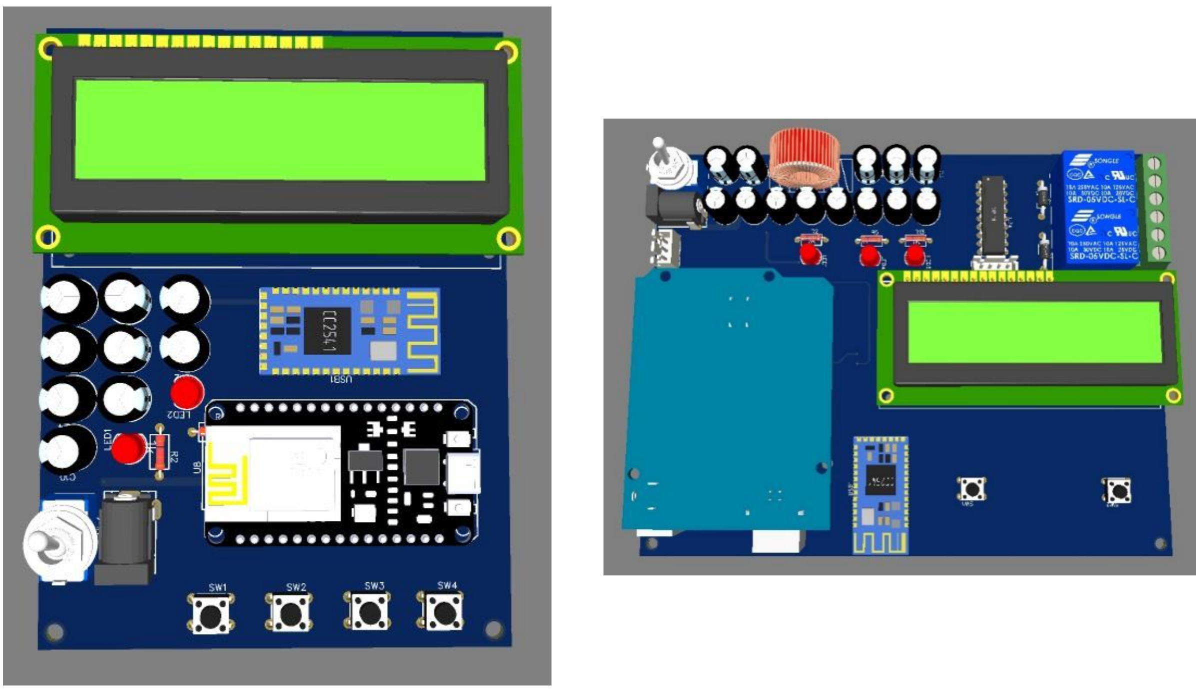
5.2 *Hardware Design*

The hardware design does go far from the idea of a Central Monitoring System, a design that will receive the data from the ZigBee nodes and display the gas concentration levels. The central monitoring system should include a ZigBee coordinator, a microcontroller, and a display unit. Figure 7 and Figure 8, shows the PCBs designed from software https://easyeda.com/page/download. Zigbee Coordinator and Router are designed.



(a) (b)

Figure 7. PCBs in PDF version. From left to right, there is (a) Zigbee coordinator and (b) Zigbee router.



(a) (b)

Figure 8. PCBs captured from easyeda version, (a) Zigbee coordinator and (b) Zigbee router.

Following (Figure 9), is the Node Design that will be used in the gas monitoring system. Each node should include a ZigBee transceiver (Zigbee UART CC2530) defined as a coordinator, a microcontroller (Wi-Fi Model ESP8266 Node MCU), a monitoring system (LCD) and a gas sensor. The microcontroller will read the gas sensor data and transmit it to the ZigBee network using the transceiver. The last and not least, is the system of power supply.

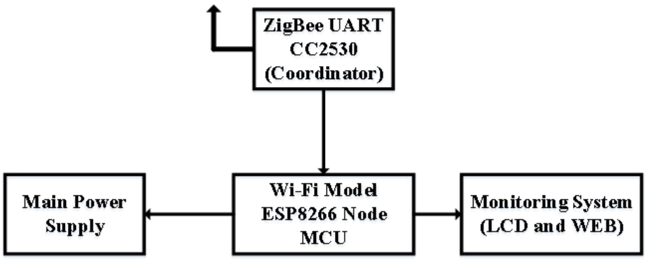


Figure 9. ZigBee coordinator system using the ESP8266 model as Wi-Fi provider for IOT

Two Router containing a two Zigbee UART CC2530 connected with an Arduino R3, DHT11 at Figure 10, ULN2303APG that can withstand large currents and high voltages. A monitoring system and a main power supply.

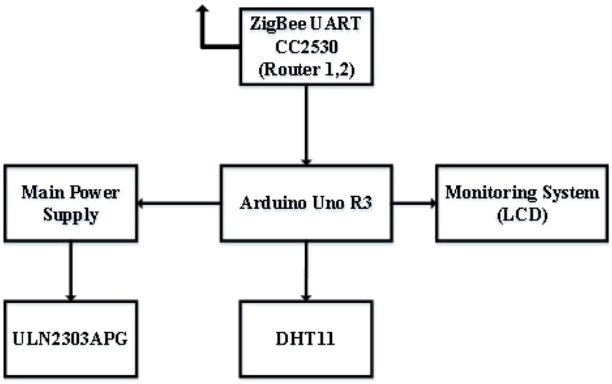
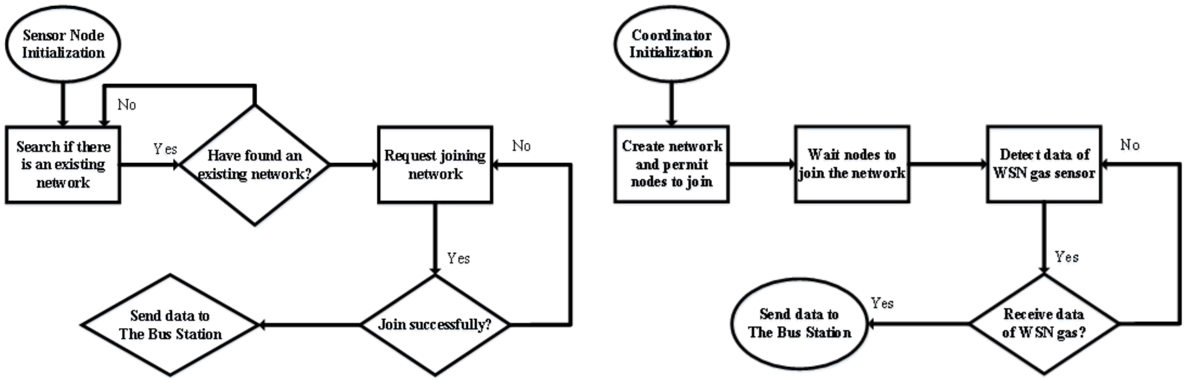


Figure 10. ZigBee router system with a DHT11 sensor

5.3 *Software Design*

The software design (Using Arduino IDE) of the gas monitoring system. Software design defines the architecture, components, modules, interfaces, and algorithms of a software system. In the case of a gas monitoring system using ZigBee technology, the communication protocol is a crucial part of the software design, as it defines how the nodes in the network will communicate and exchange data. The communication protocol also defines the data format and error correction mechanism, which are important considerations for the overall performance and accuracy of the gas monitoring system.

The communication protocol used in a gas monitoring system using ZigBee technology is based on the ZigBee protocol, which is a low-power wireless networking protocol that is designed for use in industrial and commercial applications and Figure 11 can show how it is in the flow chart. The ZigBee protocol is based on the IEEE 802.15.4 standard and provides a robust and reliable communication mechanism for low-power devices.



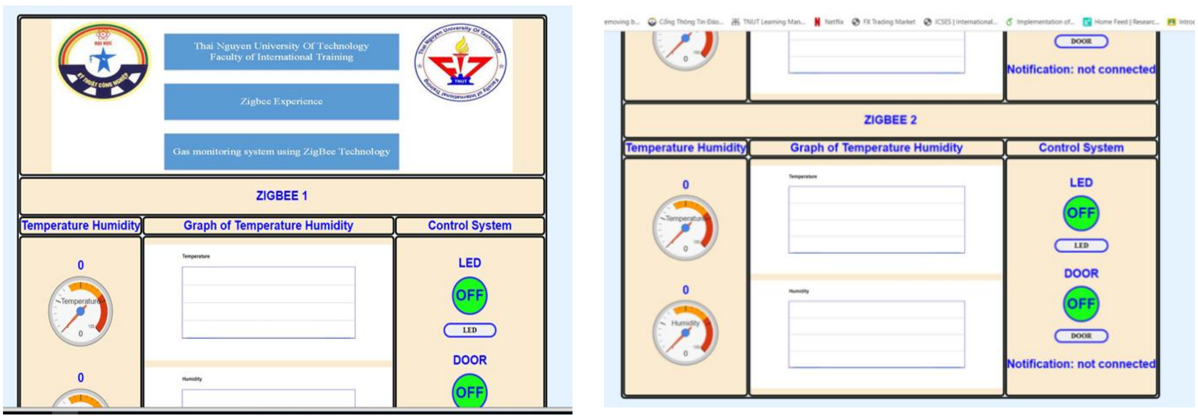
(a) (b)

Figure 11. (a) Flow chart of the router software design, (b) Flow chart of the coordinator software design.

5.4 *Website Design*

The web application (using Notepad +++ software) is designed to communicate with the central monitoring system (Coordinator interfaced by the Wi-Fi ESP8266 Node MCU, which collects the data from the ZigBee nodes and stores it in the cloud. The web application would need to access the cloud database to retrieve the data and display it to the user in a meaningful way.

The design of the graphical user interface is friendly and easy to navigate. The interface provides the user with an overview of the gas concentrations measured by the system, as well as detailed information about individual nodes (Zigbee 1 and Zigbee 2, at Figure 12) and their readings. The interface also includes charts and graphs to visualize the data collected by the system from Humidity and Temperature and allow users to perform various types of analysis on the data, such as trend analysis and statistical analysis. Apart from that, there is a light and a door directly connected at the modules, so that the user may open or close from the Web, Modules (Zigbee 1 and Zigbee 2) or also known as Router.



(a) (b)

Figure 12. (a) and (b) A view of the Website

5.5 *Results on Practical Devices*

We tested the system to see if the functions were working as intended and met the requirements that were specified during the design phase. Therefore, the system connects properly and sends data as well to the cloud as shown in the design of the website, and it is illustrated in Figure 13.

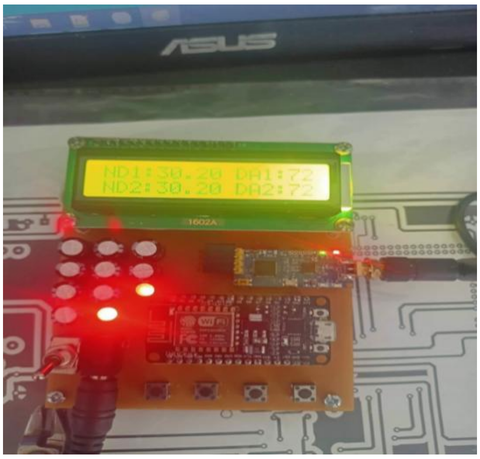
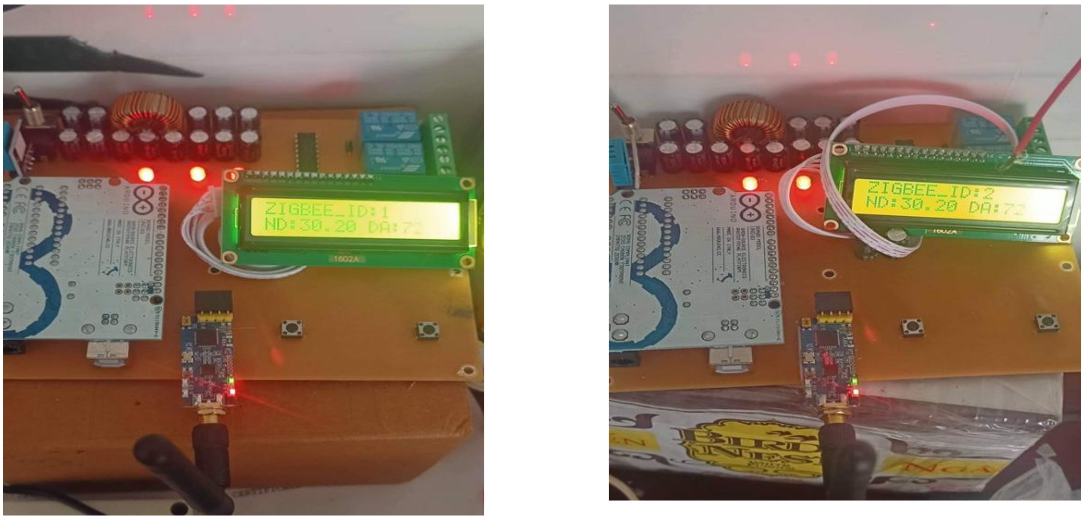


Figure 13. ZigBee coordinator system

In Figure 14, the ZigBee Coordinator System successfully connects with to the home Wi-Fi and starts receiving the Temperature and Humidity of the room that it has been connected in. As it can be seen, the Node number 1 shows a room temperature of 30.20 °C and 72 kg/m³ and at Node 2 the same temperature and Humidity as the two devices are connected in the same room.



(a) (b)

Figure 14. (a) Node 1 or Zigbee 1, (b) Node 2 or Zigbee 2.

Figures 15, the Nodes are sending data to Figure 13 (The coordinator system). And they measure the Temperature and Humidity as well as the commands for doors and lamps in the system.

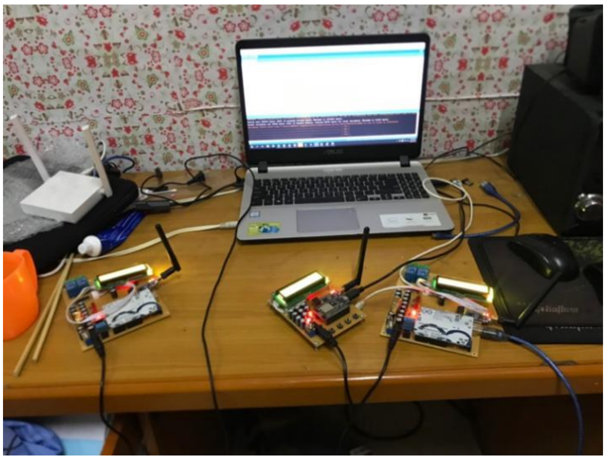


Figure 15. Interface of the software with the hardware devices connected

5.6 *Results on the Website*

When all devices are connected, the Base station will connect to the website and show the results or graphs of the received data (temperature, humidity, door closed or opened as well as the lamp if it is connected or not, this data coming from Zigbee 1 and Zigbee 2. And it will also interface if there are any issues with the devices. If the Zigbee 1 and 2 are connected or disconnected, it will show. Figure 16 and Figure 17 are the result in the website.

Figure 16. The graphs of temperature and humidity

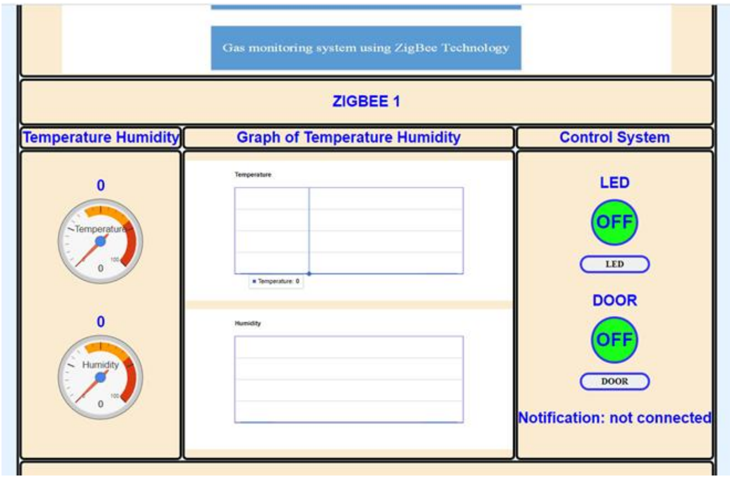


Figure 17. The graphs of temperature and humidity

5.7 *Discussions*

In summary, gas monitoring systems using ZigBee technology offer several advantages, including wireless connectivity, low power consumption, real-time monitoring, and scalability. However, they also have some disadvantages, such as limited range, interference, security concerns, and high initial costs.

While ZigBee modules are useful for providing wireless connectivity in a local area network, they cannot directly send data to the internet because they operate on a different protocol than the internet protocol. To connect a ZigBee network to the internet, a gateway or hub is required to bridge the two networks and translate the ZigBee protocol into IP protocol.

6. Conclusions and Future Development

In conclusion, the gas monitoring system using ZigBee technology is a wireless sensor network that uses ZigBee modules to transmit data from gas sensors to a central hub. The hub collects and stores the data, which can then be accessed and analyzed by authorized personnel through a cloud-based platform.

ZigBee technology is well-suited for this application because it is a low-power, low-bandwidth wireless communication protocol that is designed for short-range communication between devices in a local area network. This makes it an ideal choice for a wireless sensor network that needs to be deployed in an industrial setting where power and bandwidth limitations are a concern.

Using a cloud-based platform to display and analyze the data from the gas monitoring system provides several benefits, including remote accessibility, scalability, and real-time monitoring. However, there are also some potential drawbacks, such as security concerns and data privacy issues, that need to be addressed.

To mitigate these risks, it is important to implement appropriate security measures, such as encryption and authentication protocols, and to ensure that the data is stored and transmitted securely. Regular testing and validation of the system can also help to identify and address any potential issues before they become a problem.

In addition, by keeping the ZigBee network separate from the internet, it helps to improve the security of the system. ZigBee networks typically have their own security protocols, which can help to prevent unauthorized access to the network. By using a gateway or hub to bridge the two networks, it allows for additional security measures to be implemented, such as encryption and authentication protocols, to protect against potential security threats.

Acknowledgments

The authors would like to thank Thai Nguyen University of Information and Communication Technology, Thai Nguyen University, Ministry of Education and Training (Project B2023-TNA-16), Viet Nam for the support.

Conflict of Interest

There is no conflict of interest for this study.

Abbreviations

Term	Description
AODV	Ad-hoc On-Demand Distance Vector
CGSR	Cluster-head Gateway Switch Routing
C_m	Maximum number of children a router can have
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing
FFD	Full Function Device
GHz	Gigahertz
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IMEP	Internet MANET Encapsulation Protocol
IoT	Internet of Things
kbps	Kilobits per second
L_m	Network depth
LMR	Loop-free Multipath Routing
LR-WPAN	Low-Rate Wireless Personal Area Network
MANET	Mobile Ad hoc Network
MPR	Multipoint Relays
NWK Add	Network Address
OLSR	Optimized Link State Routing
PHY	Physical Layer
RFD	Reduced Function Device
R_m	Maximum number of child routers a router can have
TORA	Temporally-Ordered Routing Algorithm
T_{pause}	Pause Time
V_{max}	Maximum Speed Attainable
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol

References

[1] Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wire less sensor network techniques in Internet of Things (IoT). **2021**, *51*, 161–165, https://doi.org/10.1016/j.mat pr.2021.05.067.

[2] Nguyen, M.T.; Teague, K.A. Compressive sensing based energy-efficient random routing in wireless sensor networks. In Proceedings of 2014 International Conference on Advanced Technologies for Communication s (ATC). Hanoi, Vietnam, 15–17 October 2014, https://doi.org/10.1109/atc.2014.7043381.

[3] Perillo, M.A.; Heinzelman, W.B. Wireless Sensor Network Protocols. https://doi.org/10.1201/97814200350 94.sec8.

[4] Sahoo, B.M.; Pandey, H.M.; Amgoth, T. GAPSO-H: A hybrid approach towards optimizing the cluster bas ed routing in wireless sensor network. *Swarm Evol. Comput.* **2020**, *60*, 100772, https://doi.org/10.1016/j.sw evo.2020.100772.

[5] Prasanna, S.; Rao, S. An overview of wireless sensor networks applications and security. *Int. j. soft comput. eng,* **2012***, 2,* 2231–2307.

[6] Sharma, H.; Sharma, S. A review of sensor networks: Technologies and applications. In Proceedings of 2014 Recent Advances in Engineering and Computational Sciences (RAECS), Chandigarh, India, 6-8 March 2014, https://doi.org/10.1109/raecs.2014.6799579.

[7] Nguyen, M.; Cheng, Q. Efficient data routing for fusion in wireless sensor networks. *Signal* **2012**, *8*, 11.

[8] Pan, M.S.; Tseng, Y.C. ZigBee and their applications. In *Sensor networks and configuration: Fundamentals, standards, platforms, and applications*. Springer: Heidelberg, Germany, 2007. https://doi.org/10.1007/3-540-37366-7_16.

[9] Danbatta, S.J.; Varol, A. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. In Proceedings of 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019, https://doi.org/10.1109/isdfs.2019.8757472.

[10] Thakur, D.S.; Sharma, A. Voice Recognition Wireless Home Automation System Based on Zigbee. *IOSR J. Electron. Commun. Eng.* **2013**, *6*, 65–75, https://doi.org/10.9790/2834-616575.

[11] Anurag, D.; Roy, S.; Bandyopadhyay, S. Agro-sense: Precision agriculture using sensor-based wireless mes h networks. In Proceedings of 2008 First ITU-T Kaleidoscope Academic Conference - Innovations in NGN: Future Network and Services, Geneva, Switzerland, 12–13 May 2008, https://doi.org/10.1109/KINGN.200 8.4542291.

[12] Wheeler, A. Commercial Applications of Wireless Sensor Networks Using ZigBee. *IEEE Commun. Mag.* **2007**, *45*, 70–77, https://doi.org/10.1109/mcom.2007.343615.

[13] Coboi, A.E.; Tran, T.A.; Tran, S.Q.; Nguyen, M.T. Security Problems in Smart Homes. *ICSES Trans. Comput. Netw. Commun.* **2021**, *10*, 1–9.

[14] Javaid, N.; Sharif, A.; Mahmood, A.; Ahmed, S.; Qasim, U.; Khan, Z. Monitoring and Controlling Power Using Zigbee Communications. In Proceedings of 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications, Victoria, BC, Canada, 12–14 November 2012, https://doi.org/10.1109/BWCCA.2012.107.

[15] Alimoradi, P.; Barati, A.; Barati, H. A hierarchical key management and authentication method for wireless sensor networks. *Int. J. Commun. Syst.* **2021**, *35*, e5076, https://doi.org/10.1002/dac.5076.

[16] Yun, J.; Won, K.-H. Building Environment Analysis Based on Temperature and Humidity for Smart Energy Systems. *Sensors* **2012**, *12*, 13458–13470, https://doi.org/10.3390/s121013458.

[17] Nguyen, C.V.; Coboi, A.E.; Bach, N.V.; Dang, A.T.; Le, T.T.; Nguyen, H.P.; Nguyen, M.T. ZigBee based data collection in wireless sensor networks. *Int. J. Informatics Commun. Technol. (IJ-ICT)* **2021**, *10*, https://doi.org/10.11591/ijict.v10i3.pp212-224.

[18] Kalra, A.; Chechi, R.; Khanna, R. Role of Zigbee Technology in agriculture sector. In Proceedings of 2010 National Conference on Computational Instrumentation, Chandigarh, India, 19–20 March 2010.

[19] Frehill, P.; Chambers, D.; Rotariu, C. Using Zigbee to Integrate Medical Devices. In Proceedings of 2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Lyon, France, 22–26 August 2007, https://doi.org/10.1109/IEMBS.2007.4353902.

[20] Somani, N.A. Zigbee: A Low Power Wireless Technology for Industrial Applications. *Int. J. Control. Theory Comput. Model.* **2012**, *2*, 27–33, https://doi.org/10.5121/ijctcm.2012.2303.

[21] Nguyen, M.T.; Teague, K.A.; Rahnavard, N. CCS: Energy-efficient data collection in clustered wireless sen sor networks utilizing block-wise compressive sensing. *Comput. Networks* **2016**, *106*, 171–185, https://doi.org/10.1016/j.comnet.2016.06.029.
[22] Zhang, Q.; Sun, Y.; Cui, Z. Application and analysis of ZigBee technology for Smart Grid. In Proceedings of 2010 International Conference on Computer and Information Application, Tianjin, China, 3-5 December 2010, https://doi.org/10.1109/ICCIA.2010.6141563.
[23] Suhendar, E.; Sukardi. Situation analysis of fulfillment of beef needs and opportunities for beef cattle partnership. *IOP Conf. Ser.: Earth Environ. Sci.* **2022**, *1063*, 012027, https://doi.org/10.1088/1755-1315/1063/1/012027.
[24] Kharb, L. Proposing a Comprehensive Software Metrics for Process Efficiency. *Int. J. Eng. Res.* **2014**, *5*, 78–80.
[25] Tomar, A. Introduction to ZigBee technology. *Glob. Technol. Centre* **2011**, *1*, 1–24.
[26] Nguyen, M.T.; Teague, K.A. Neighborhood based data collection in Wireless Sensor Networks employing Compressive Sensing. In Proceedings of 2014 International Conference on Advanced Technologies for Co mmunications (ATC 2014), Hanoi, Vietnam, 15–17 October 2014, https://doi.org/10.1109/ATC.2014.7043383.
[27] Kriška, M.; Janitor, J.; Fecilak, P. Dynamic Routing of IP Traffic Based on QOS Parameters. *Int. J. Comput. Netw. Commun.* **2014**, *6*, 11–22, https://doi.org/10.5121/ijcnc.2014.6402.
[28] Tsai, C.-H.; Tseng, Y.-C. A Path-Connected-Cluster Wireless Sensor Network and Its Formation, Addressi ng, and Routing Protocols. *IEEE Sensors J.* **2012**, *12*, 2135–2144, https://doi.org/10.1109/jsen.2012.2183348.
[29] Nezhad, M.A.; Barati, H.; Barati, A. An Authentication-Based Secure Data Aggregation Method in Internet of Things. *J. Grid Comput.* **2022**, *20*, 1–28, https://doi.org/10.1007/s10723-022-09619-w.
[30] Pan, M.-S.; Fang, H.-W.; Liu, Y.-C.; Tseng, Y.-C. Address Assignment and Routing Schemes for ZigBee-B ased Long-Thin Wireless Sensor Networks. In Proceedings of VTC Spring 2008 - IEEE Vehicular Technol ogy Conference, Marina Bay, Singapore, 11–14 May 2008, https://doi.org/10.1109/VETECS.2008.48.
[31] Kuppaswamy, K. Maximizing the system lifetime in wireless sensor networks using improved routing algorithm. Master Thesis, Southern Illinois University at Carbondale, Carbondale, IL, USA, August 2011.
[32] Ravilla, D. Hybrid Routing Protocols for Ad hoc Wireless Networks. *Int. J. Ad hoc, Sens. Ubiquitous Comput.* **2011**, *2*, 79–96, https://doi.org/10.5121/ijasuc.2011.2407.
[33] Rezaeipour, K.H.; Barati, H. A hierarchical key management method for wireless sensor networks. *Microprocess. Microsystems* **2022**, *90*, 104489, https://doi.org/10.1016/j.micpro.2022.104489.
[34] Anitha, P.; Chandrasekar, C. Energy aware routing protocol for zigbee networks. *J. Comput. Appl.* **2011**, *4*.
[35] Abolhasan, M.; Wysocki, T.; Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks* **2004**, *2*, 1–22, https://doi.org/10.1016/s1570-8705(03)00043-x.
[36] Sharei-Amarghan, H.; Keshavarz-Haddad, A.; Garraux, G. Routing Protocols for Border Surveillance Using ZigBee-Based Wireless Sensor Networks. In Proceedings of Computer Networks: 20th International Conference, CN 2013, Lwówek Śląski, Poland, 17–21 June, 2013.
[37] Nguyen, M.T. An energy-efficient framework for multimedia data routing in Internet of Things (IoTs). *EAI Endorsed Trans. Ind. Networks Intell. Syst.* **2019**, *6*, https://doi.org/10.4108/eai.13-6-2019.159120.
[38] Dehkordi, E.G.; Barati, H. Cluster based routing method using mobile sinks in wireless sensor network. *Int. J. Electron.* **2022**, *110*, 360–372, https://doi.org/10.1080/00207217.2021.2025451.
[39] Chatterjee, M.; Das, S. K.; Turgut, D. WCA: A weighted clustering algorithm for mobile ad hoc networks. *Clust. Comput.* **2002**, *5*, 193–204.
[40] Ramesh, V.; Subbaiah, D.P.; Rao, N. K.; Raju, M.J. Performance Comparison and Analysis of DSDV and AODV for MANET. *Int. J. Comput. Sci. Eng.* **2010**, *2*, 183–188.
[41] Lim, K.H.; Datta, A. An In-depth Analysis of the Effects of IMEP on TORA Protocol. In Proceedings of 2012 IEEE Wireless Communications and Networking Conference (WCNC), Paris, France, 1–4 April 2012, https://doi.org/10.1109/WCNC.2012.6214328.
[42] Nguyen, M.T.; La, H.M.; Teague, K.A. Collaborative and Compressed Mobile Sensing for Data Collection in Distributed Robotic Networks. *IEEE Trans. Control. Netw. Syst.* **2017**, *5*, 1729–1740, https://doi.org/10.1109/tcns.2017.2754364.
[43] Nguyen, M.T. Data collection algorithms in wireless sensor networks employing compressive sensing. PhD Thesis, Oklahoma State University, Stillwater, OK, USA, December 2015.

[44] Kuppusamy, P.; Thirunavukkarasu, K.; Kalaavathi, B. A study and comparison of OLSR, AODV and TORA routing protocols in ad hoc networks. In Proceedings of 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011, https://doi.org/10.1109/ICECTECH.2011.5941974.
[45] Nguyen, M.T.; Teague, K.A. Compressive sensing based random walk routing in wireless sensor networks. *Ad Hoc Networks* **2017**, *54*, 99–110, https://doi.org/10.1016/j.adhoc.2016.10.009.
[46] Nguyen, M.T.; Teague, K.A. Tree-based energy-efficient data gathering in wireless sensor networks deploying compressive sensing. In Proceedings of 2014 23rd Wireless and Optical Communication Conference (WOCC), Newark, NJ, USA, 9–10 May 2014, https://doi.org/10.1109/WOCC.2014.6839920.