SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.03 NO. 3 2024
DOI: 10.51984/SUCP.V3I3.3698

المؤتمر السادس للعلوم الهندسية والتقنية
The Sixth Conference for Engineering Sciences and Technology (CEST-6)
Confrence Proceeeding homepage: https://cest.org.ly

Implementing Zigbee Networks for Monitoring and Tracking Electricity Meters

*Mohamed A. Elalem, Mohammed Altayib, Milad Azzoka

Electrical and Computer Department, Elmergib University, Libya

Keywords:
IoT
M2M
Remotly electric meter measurments
Security
XBee
ZigBee

ABSTRACT

In order to lower electricity consumption, improve billing accuracy, and avoid customer issues, it is essential for residences, businesses, and factories to monitor their electrical meters. This paper introduces Zigbee technology as a standards-based wireless technology designed to facilitate low-power, low-cost wireless networks for the internet of things (IoT) and machine-to-machine (M2M). Zigbee is an open-source device for low-power, low-data-rate applications. Zigbee allows much lower data speeds and employs a mesh networking protocol. The goal of this work is to employ ZigBee networks to address earlier issues with electricity usage measurement. These networks eliminate the need for employees to carry out this procedure. Due to some technical and manufacturing issues with available reading meters, the practical portion of the work involved using an Arduino to simulate the operation of an electric meter. The reading has been successfully linked and transmitted, and a distance of 300 meters of transmission has been achieved via XBee. This confirms the process of using ZigBee networks to provide a wide and suitable network to monitor electrical meters in residential neighborhoods.

تنفيذ شبكات الزقبي لمراقبة وتتبع عدادات الكهرباء

*محمد العالم ومحمد الطيب و ميلاد عزوكة

جامعة المرقب، كلية الهندسة، الخمس، ليبيا

الكلمات المفتاحية:
الاتصالات بين الآلات
الاكسبي
الآمان
انترنت الأشياء
الزقبي
قياس عدادات الكهرباء عن بعد.

الملخص

من أجل خفض استهلاك الكهرباء وتحسين دقة الفواتير وتجنب مشاكل العملاء، من الضروري للمساكن والشركات والمصانع مراقبة عداداتها الكهربائية. يبدأ المشروع بلمحة موجزة عن أنواع عدادات الطاقة، وكيفية مراقبة العدادات، والتحديات الأساسية المرتبطة بأخذ القراءات، والتي تتطلب من قارئ العدادات الوصول فعليًا إلى العداد وأخذ القراءة يدويًا من أجل إصدار الفاتورة. يتم عرض بعض الإحصاءات عن سرقات الطاقة في بعض البلدان. يقدم هذا المشروع تقنية Zigbee كتقنية لاسلكية قائمة على معايير مصممة لتسهيل الشبكات اللاسلكية منخفضة الطاقة ومنخفضة التكلفة لإنترنت الأشياء (IoT) ومن الاتصالات بين الآلات (M2M) . هو جهاز مفتوح المصدر للتطبيقات منخفضة الطاقة ومنخفضة معدل البيانات. يسمح Zigbee بسرعات بيانات أقل بكثير ويستخدم بروتوكول الشبكات المتداخلة. الهدف من هذا المشروع هو استخدام شبكات ZigBee لمعالجة المشكلات السابقة المتعلقة بقياس استخدام الكهرباء. هذه الشبكات تلغي الحاجة إلى الموظفين لتنفيذ هذا الإجراء. وبسبب بعض المشكلات التقنية والتصنيعية في عدادات القراءة المتاحة، تضمن الجزء العملي من المشروع استخدام جهاز Arduino لمحاكاة تشغيل عداد كهربائي. وقد تم ربط القراءة وإرسالها بنجاح، وتم تحقيق إرسال مسافة 300 متر من الإرسال عبر .XBee وهذا يؤكد عملية استخدام شبكات ZigBee لتوفير شبكة واسعة ومناسبة لمراقبة العدادات الكهربائية في الأحياء السكنية.

1. Introduction

In recent decades, the world has witnessed a tremendous development in the field of telecommunications, leading the rest of the technical and scientific fields to develop dramatically and rapidly, which has provided quick and easy access to data and information from a long distance without any effort. And because of easy access to the Internet and its availability in most of the world's cities, the most available information is available to all. This contributes to improving the level of education, increasing people's confidence and awareness, and

*Corresponding author:
E-mail addresses: maelalem@elmergib.edu.ly, (M. Altayib,) mohammed4822531@gmail.com, (M. Azzoka) meeladiezouckah@gmail.com

Article History : Received 14 March 2024 - Received in revised form 29 August 2024 - Accepted 21 October 2024

increasing the performance and productivity of companies, thereby facilitating remote work and rapid access to data.

As people become increasingly dependent on the Internet and communication networks, there is a need for fast Internet connectivity in most places. With the expansion and proliferation of 5G services in most modern cities, 5G provides high data transmission speeds with very little delay, and with increased demand for IoT devices, 5G technology has allowed us to get a great benefit from it as IoT provides us with remote interaction and automatically handles devices without the need for human intervention.

As the technical world develops, some of the problems people face in their daily lives continue. such as the problem of reading meters and overconsumption of energy. One of the problems faced by electrical technicians in reading meters is the difficulty of getting to me as hard as possible, being robbed or assaulted, and bad weather conditions. Other than the problems of monitoring reading, any error may lead to major problems. As populations grow and these problems worsen, it becomes necessary to research technical solutions to them.

The solution came from the use of various wireless communication technologies and the IoT Internet of Things to monitor and follow meters digitally and automatically without the need for human intervention, and this way the currencies can know their consumption permanently, allowing them to rationalize consumption and save energy and money.

Several studies have been performed on automatic electric meter reading in the last few decades. In [1], an automatic energy meter project was designed to simplify energy consumption monitoring and billing processes. By digitizing meter readings and eliminating manual efforts, it ensures accurate billing and timely payments. Benefits include enhanced consumer convenience, potential energy savings, reduced maintenance costs, increased safety, and improved control over energy usage. The system utilizes Wi-Fi connectivity and LCD displays to provide real-time data and facilitate prompt bill payments, ultimately saving time, costs, and resources for both consumers and energy providers.

The design project in [2] focuses on designing a single-phase smart energy meter using real-time sensors to calculate current, voltage, and power. Using an Arduino microcontroller, it measures circuit parameters like current, voltage, power factor, real power consumption, and reactive power. The system also includes WiFi-enabled switching for remote control of appliances. A mobile application named PMU is developed for remote operation. The smart meter replaces mechanical meters, providing advantages such as instant voltage and current readings as well as the ability to measure various electrical quantities. It offers remote control and monitoring of energy usage, enhancing convenience and efficiency.

The paper in [3] discusses the emergence of smart meters, driven by communication technology advancements. These meters automate energy consumption measurement, billing, and alerting using IoT and GSM techniques. They read current consumption units, calculate bills, and send alerts for excessive usage. Enabled by Arduino microcontroller technology, smart meters ensure accuracy and efficiency while providing real-time data transmission to users' smartphones and websites. Overall, they enhance energy management, promote efficiency, and improve customer convenience.

This paper aims to develop an intelligent system for measuring and monitoring electric power meters with simplicity, low cost, and high reliability, with the aim of improving energy management by the electricity company and by consumers. The overall objectives can be listed and clarified as follows:

- Replacing traditional methods of measuring electrical power by relying on a system to collect data without the need to read meters manually, providing accuracy for measuring and reducing human errors.
- Ability to track and manage energy and control consumption by both parties (electricity and consumer companies) by providing real-time consumption information to consumers.
- Reducing labors, following reading for counters, and keeping the time set for it.
- Using XBee as a transceiver and connecting it to mesh networks to provide wide coverage for reliability certification.

After this introduction, the rest of the paper is organized as follows: Section 2 introduces ZigBee technology, in which architecture, network layers, types of devices, network topology, and security are identified. Section 3 lists and briefly explains the components that are used in this work. In Section 4, the performance of Zigbee and real time measurements are taken. Finally, Section 5 draws the work conclusions.

2. Zigbee Technology

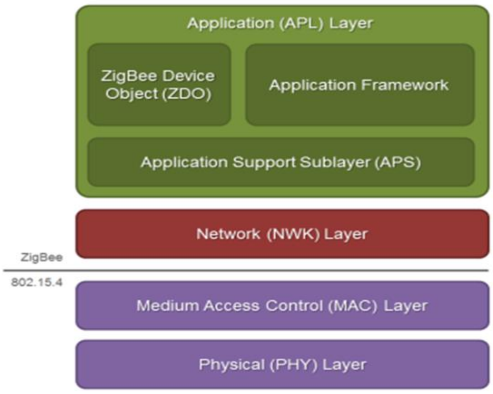
Zigbee is low-power, low-cost type of wireless technology that is commonly used in the Internet of Things. It is created in the beginning of 2000s to be an option to Wi-Fi or Bluetooth that would provide long battery life and guaranteed communication. Zigbee Alliance is a group of companies that develop Zigbee and maintain compatibility of all the devices based on open standards [10].

2.1 ZigBee Architecture

The Zigbee device operates within the IEEE 802.15.4 framework, tailored for Wireless Personal Area Networks (WPANs), ensuring efficient and reliable communication. Utilizing the IEEE 802.15.4 standard's physical and MAC layers, Zigbee supports low-power, short-range applications across various frequency bands, including 868 MHz, 902-928 MHz, and 2.4 GHz, with a data rate of 20-250 kbps. This makes Zigbee ideal for control and sensor networks, contributing to its popularity in home automation, industrial automation, and healthcare [11].

Zigbee extends the IEEE 802.15.4 standard by incorporating additional layers, including a network layer for data routing, an application layer for specific behaviors, and a security layer for encrypted transmissions. Operating in the 2.4 GHz band, Zigbee efficiently supports numerous devices while minimizing power consumption, making it widely adopted in wireless communication standards [11].

Expanding upon this foundation, the Zigbee specification introduces additional layers to manage higher-level functionalities. The Network Layer (NWK) is responsible for network architecture, routing, and security, while the Application Layer (APL) framework encompasses the Application Support Sublayer (APS), Zigbee Device Objects (ZDO), and user-defined applications. This is shown in Fig. 1. Together, these layers provide the device with its specific functionality and enable it to interact within the Zigbee network [12].



a.

Fig. 1: Zigbee device object as apart of communication layers [13]

2.2 ZigBee Network Layers

The PHY layer defines the actual operation of Zigbee devices, including receive sensitivity, channel rejection, output power, number of channels, chip modulation, and transmission rate specifications. Most Zigbee applications operate on the 2.4 GHz ISM band at a data rate of 250 kb/s. Detailed specifications can be found in the IEEE 802.15.4 standard [14].

The MAC layer manages wireless data transactions between neighboring devices in a Zigbee network in a point-to-point manner. It provides services such as transmission retry, acknowledgment management, and collision avoidance techniques like Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) [14].

The network layer adds routing capabilities to Zigbee, allowing wireless data packets to traverse multiple devices (multiple hops) to reach their destination in a peer-to-peer manner [15].

The application support sublayer (APS) is located within the application layer, it defines various addressing objects including profiles, clusters, and endpoints. It facilitates communication and interaction for applications [15]. While Zigbee device object (ZDO) is also, within the application layer, it provides device and service discovery features, as well as advanced network management capabilities. It helps Zigbee devices discover and join networks, manage network parameters, and perform other administrative functions [15].

2.3 ZigBee devices

ZigBee networks include the following three main device types. The first is the coordinator which is he node responsible for organizing the network. It is the one that determines the network security policy, allowing or denying the connection of new devices to the network, and in the event of radio interference, it begins the process of transferring all devices on the network to another frequency channel [16]. The second is the router, it is the node with constant power that can constantly participate in the operation of the network. A coordinator is also a router. Nodes of this type are responsible for routing network traffic. Routers constantly maintain special routing tables, which are used to plot the optimal path and find a new path if any device suddenly fails. For example, routers on a ZigBee network can be smart plugs, lighting controllers, or any other device with a power connection [16]. The third device that the ZigBee can be configured is what called end-device, it is the device that connects to the network through a parent node - a router or coordinator - the difference between it and the earlier is that it does not participate in directing traffic. Network connectivity for it is limited only to sending packets to the “parent” node or reading data received from it. The "parent" of these devices can be any router or coordinator. Peripheral devices spend most of their time in sleep mode to conserve power and send control or information messages [12,16]. There are two types of terminal devices: sleeping devices which turn off their radio when they are idle, thus conserving resources. However, they must poll their parent node to receive incoming messages and acknowledgments; no data is sent to an end device is sleepy until the end device requests it. Sleeper devices are sometimes known as Rx-off-when-idle devices. The other device is the inactive device, which does not forward messages to other devices but are still supported during operation. These devices are known as Rx-on-when-idle devices [17].

2.4 ZigBee Network Topologies

ZigBee network can be connected in star topology which is characterized by a single coordinator and a variable number of end devices. It adopts a master-slave network model where the ZigBee coordinator serves as the master, functioning as a Full Function Device (FFD), while the slaves can be either FFDs or Reduced Function Devices (RFDs). Physically and electrically isolated from each other, ZigBee end devices pass information exclusively through the coordinator. Communication is restricted to devices interacting solely with the coordinator, without supporting multi-hop or mesh networking capabilities [18,19]. Cluster tree topology can closely resembles the star topology, with the key distinction being that node, other than the coordinator, can communicate with each other. This allows for additional connections of RFDs and FFDs to non-coordinator FFDs, enabling potential geographical expansion of the network. The primary advantage of this topology lies in its ability to facilitate communication between nodes beyond a direct link to the coordinator [18,19].

Mesh topology permits each node to communicate with any other node within its operational range. While this topology is intricate to maintain and does not support beaconing, it offers increased robustness and fault tolerance. The complexity arises from the extensive connectivity between nodes, allowing for more diverse communication paths and enhanced reliability [18,19].

2.5 ZigBee Security

ZigBee security, which is based on a 128-bit AES algorithm, adds to the security model provided by IEEE 802.15.4. ZigBee’s security services include methods for key establishment and transport, device management, and frame protection. The ZigBee specification defines security for the MAC, NWK and APS layers. Security for applications is typically provided through Application Profile [21,24]. The Trust Center decides whether to allow or disallow new devices into its network. The Trust Center may periodically update and switch to a new Network Key. It first broadcasts the new key encrypted with the old Network Key. Later, it tells all devices to switch to the new key. The trust center is usually the network coordinator, but is also able to be a dedicated device. It is responsible for several security roles, such as authentication that requests to join the network, network management for maintaining and distributing network keys configuration management, to enable end-to-end-security between devices [21, 25]. In ZigBee, there are three types of keys to manage security. The first is the master keys, which are optional keys and not used to encrypt frames. Instead, they are used as an initial shared secret between two devices when they perform the key establishment procedure. Keys that originate from the trust center are called trust center master keys, while all other keys are called application layer master keys.

The second security keys are the network keys. These keys perform security network layer security on a ZigBee network. All devices on a ZigBee network share the same key. High security network keys must always be sent encrypted over the air.

The third keys in ZigBee security are the link keys. These keys are used to secure communication between network devices, encrypted by either the master key or the network key. It ensures data confidentiality and communication security within the network [21,25].

3. Components and Project Methodology

The proposed work layout can be configured as a mesh network consisting of a coordinator, which will be present in the control device, and routers or end devices in terms of meters. Fig. 2 illustrates the block diagram used in this experiment. The Zigbee coordinator is responsible for sending commands issued by the control office or user to perform any power on/off operation. It receives readings sent from the meters and displays them at the control office and at the users. The block diagram for the monitoring device is as shown in Fig. 3.

The electric meter sends the actual reading of the electricity consumption and the meter ID to the precision controller, which in turn sends the reading to the ZigBee transceiver to be sent to the monitoring device. For the event of receiving an order from a monitoring device, the ZigBee transceiver sends the meter readings to the microcontroller, which in turn controls the relay and connects or disconnects the electricity from the consumer. The main components used in this work are described in the following subsections.

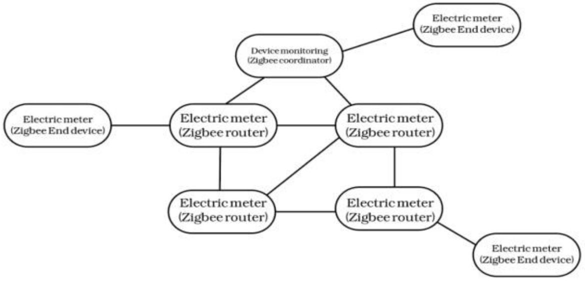

Electric meter (Zigbee End device)
Device monitoring (Zigbee coordinator)
Electric meter (Zigbee End device)
Electric meter (Zigbee router)
Electric meter (Zigbee router)
Electric meter (Zigbee router)
Electric meter (Zigbee router)
Electric meter (Zigbee End device)

Fig. 2: Network topology of the project

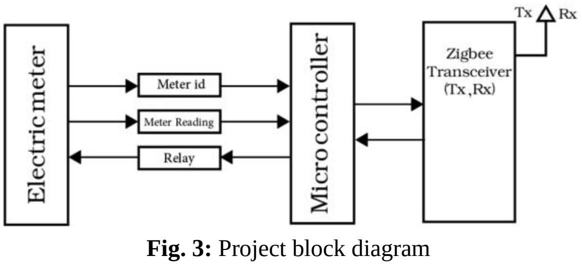


Fig. 3: Project block diagram

3.1 XBee S2C

Digi XBee S2C, shown in left side of Fig. 4, provides an excellent option to create Zigbee P2P or mesh networks and connect microcontrollers. It acts as a coordinator for the monitor and as a router or end device for the electrical meter. It supports 2.4 GHz and 900 MHz frequencies and includes UART and SPI interfaces with programmable and adjustable transmitting power. The internal and external coverage range is up to 300 feet (90 meter), with an RF data rate of 250 Kbps and a power sensitivity of about -102 dBm. It requires a voltage of +2.1 V to +3.6 V and an operating current between 33 mA and 45 mA; providing ESD protection up to 3000V; and operating at a temperature between - 40 °C to 85 °C. It can be programmed and configured using XCTU software, which provides an easy-to-use interface to manage settings and download software. The coordinator will be in the monitoring device and the router or end device.

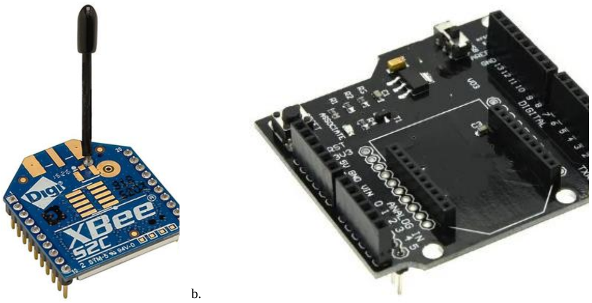


Fig. 4: Digi XBee S2C and XBee ZigBee Shield V03 module wireless control

3.2 Arduino Uno

The Arduino is a straightforward microcontroller designed for basic electrical tasks with programmable circuitry facilitated through an Integrated Development Environment (IDE). It utilizes a microcontroller processor that can be programmed to execute a variety of tasks, making it suitable for a wide range of electronic applications. The Arduino Uno is utilized here as a simulator for the electricity meter from the customer's perspective. It is used to simulate real-meter actions to assess the performance of electricity systems without the necessity of an actual meter. Moreover, when employed as a power consumption monitor, the Arduino Uno can be programmed to read and analyses data from electrical devices, enabling intelligent and precise control of power consumption and thus providing insightful reports on power usage.

3.3 XBee Shield

The XBee shield is an interface device with Arduino that makes it easy to connect the XBee module. It rides over the top of the Arduino panel and has pins that correspond to those in the panel below, as well as a socket to which the XBee module is connected. This shield simplifies connecting XBee units to Arduino by dealing with power regulation, level conversion, and other hardware requirements. The right side of Fig. 4 illustrates the XBee shield used in this project.

3.4 Screen-LCD-16x2

The 16x2 LCD display is a popular display unit featuring 16 characters across 2 lines. Liquid Crystal Screen (LCD) technology is used to provide a simple and effective way to view text and simple graphics. The module typically includes a built-in controller that interacts with miniature controllers such as Arduino, allowing for easy integration into projects. The 16x2 LCD screen is commonly used in various applications, including displaying sensor readings, messages, menus, and other information in Arduino projects. It is used here to display meter readings/customer ID on the meter side and on the monitor side.

4. ZigBee Performance Study and Results

In this section, the communication performance of the XBee is studied and analyzed during real-time transmission of packets of 4-byte-length. Two different transmission environments are used. Line of Sight (LOS) and Non-Line of Sight (NLOS) scenarios are tested. The measurements are recorded in Table (1). In LOS case, as expected, the best received power is obtained. The lowest number for packet loss is obtained compared with the other scenario. The packets start to be lost at a distance greater than 140 meters. Up to 300 meters, all packets are lost. During this experiment measurement, the bite error rate was roughly calculated and found to be equal to 1×10^{-2}.

For the case of NLOS, the received power dramatically attenuates compared with the previous case. The power is not dropping quite as linearly. Some packets start to be lost beyond 20 meters. Higher than 60 m, all sent packets are lost. The bit error rate is found to be nearly double that of the previous case, i.e. 2×10^{-2}.

Table 1: The experiment measurements

Distance (m)	**Received power (dBm)**	
	LOS	**NLOS**
1	-34	-52
5	-51	-57
10	-54	-63
25	-57	-78
50	-59	-88
60	-60	-90
90	-63	-
110	-68	-
130	-73	-
170	-81	-
230	-84	-
270	-88	-
300	-91	-

ZigBee is utilized as a communication gateway, which is used as a coordinator and/or a router according to the setting configuration given in Table (2). This gives electrical consumers comprehensive data about their power usage, including on a day-by-day or month-by-month basis. The instantaneous meter readings as well as the meter ID are displayed on the LCD screen, therefore, the electrical consumption of energy can be monitored, controlled, and displayed.

Table 2: Device configurations as: a Coordinator and a Router

	Coordinator	Router
PAN ID	1111	1111
Coordinator Enable CE	Enable [1]	-
Destination Address High DH	0	0
Destination Address Low DL	FFFF	0000
Node identifier	COORDINATOR	ROUTER
API Enable AP	Transparent mode [0]	Transparent mode [0]

5. Conclusions

With the increase in population and electricity demand, the energy consumption problem has become one of the biggest problems facing electric production, making it necessary to seek out more effective solutions to monitor and follow up on electrical meters in an easy and safe way. This paper introduces easy and fast meter reading procedures by implementing Zigbee networks for monitoring and tracking electric meters. This gives great benefit to addressing the problems of monitoring electric meters. Using Arduino and XBee devices eases the task of taking these readings personally. The obtained observations show very good results in terms of the distance that these networks can cover. High reliability in accessing readings from surveillance devices is guaranteed. The proposed system works individually on any other existing networks, even though it does not depend on the Internet. It provides a high level of security against hacking or sabotage and is under full control by the operating company.

6. References

[1] Prachi Bramhe, Akshay Sarode, Vicky Bonde, Rachana Mankar, Ayushi Kesharwani, and Samiksha Dhengale (2019), Automatic Electric Meter Reading Using WIFI, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 04, pp. 343-346.

[2] Khalid Al-Otaibi, Ahmed Ananzi, Abdullah Abaoud, and Mohammed Dhameri, "Smart Energy Metering and Control System", Senior Design Project Report, Prince Mohammed Bin Fahd University, College of Engineering, Spring 2018-2019.

[3] M. Rupesh and N. Anbu Selvan, (2001), Design of IoT Based Smart Energy Meter for Home Appliances, Journal of Physics, Volume 1964, DOI 10.1088/1742-6596/1964/5/0520.

[4] V. Agarwal, S. A. Mahmud, S. Kasera, and M. Ji, (2023), Experimental Evaluation of Interference in 2.4 GHz Wireless Network, Idaho National Laboratory (INL), Idaho Falls, ID (United States).

[5] N. Abdulrahman and F. A. Yaseen, (2015), Performance Evaluation of Zigbee Routing Protocol under Various Conditions using OPNET Modeler, International Journal of Computer Applications, vol. 117, no. 18.

[6] C. M. Ramya, M. Shanmugaraj, and R. Prabakaran, (2011), Study on ZigBee technology, 3rd international conference on electronics computer technology, vol. 6: IEEE, pp. 297-301.

[7] K. S. Harris. "Exploiting the IoT Through Network-based Covert Channels," Accessible at https://scholar.afit.edu/etd/5322?utm_source=scholar.afit.edu%2Fetd%2F5322&utm_medium=PDF&utm_campaign=PDFCoverPages.

[8] Koubâa, M. Alves, and E. Tovar, (2005), IEEE 802.15. 4 for wireless sensor networks: a technical overview.

[9] Wang, T. Jiang, and Q. Z. Zhang, (2016), Network Protocols and Applications, Auerbach Publications: Boca Raton, FL, USA.

[10] S. Safaric and K. Malaric, (2006), ZigBee wireless standard," in Proceedings ELMAR 2006, IEEE, pp. 259-262.

[11] M. Benini and L. Vanzago, "Optimizing ZigBee for data streaming in body-area bio-feedback applications."

[12] J. Li, X. Zhu, N. Tang, and J. Sui, (2010), Study on ZigBee network architecture and routing algorithm, 2nd International Conference on Signal Processing Systems, vol. 2: IEEE, pp. V2-389-V2-393.

[13] D. Vishwakarma, (2012), IEEE 802.15. 4 and ZigBee: A conceptual Study, Channels, vol. 868, pp. 868-6.

[14] D. N. Inc. "Getting Started with ZigBee and IEEE 802.15.4" Accessible at: https://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/Zigbee%20GettingStarted.pdf .

[15] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, (2014), Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned, 14th international conference on hybrid intelligent systems, IEEE, pp. 199-206.

[16] Z. Alliance, Zigbee specifications: Zigbee and zigbee pro," ed. 2012.