SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Low Network Power Challenges in IoT-Based Applications in Smart Cities

Muhammad Zunnurain Hussain[1,*], Zurina Mohd Hanapi[1], Muhammad Zulkifl Hasan[2]

[1] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[2] Faculty of Information Technology, Department of Computer Science, University of Central Punjab, Lahore, Punjab 54000, Pakistan

ARTICLE INFO

Article history:
Received 10 February 2024
Received in revised form 19 September 2024
Accepted 4 October 2024
Available online 31 December 2024

Keywords:

LoRaWAN; IoT; Security; LPWAN; Sigfox; Zigbee; Cyber-attacks; Smart cities; Low network power; Challenges; Applications; Energy-efficient technologies; Infrastructure planning; Technical innovations; Data loss; Slow response times; Poor device performance

ABSTRACT

The emergence of Internet of Things (IoT) technologies has led to the development of smart cities, potentially improving urban life through efficient and effective use of resources. The success of IoT-based applications in smart cities is contingent on several factors, including network power challenges. Deploying IoT-based applications in smart cities requires a reliable and efficient network infrastructure to ensure smooth and uninterrupted data communication. One of the significant challenges faced in this regard is low network power, which can significantly impact the performance of IoT devices and, consequently, the entire smart city system. This article addresses the issue of low network power in IoT-based applications in smart cities. It investigates the causes of this problem and the potential solutions that can be adopted to mitigate its impact. The article also highlights the importance of network power management in the context of IoT-based applications in smart cities. By implementing effective network power management techniques, it is possible to optimize the performance of IoT devices and extend their battery life, thus ensuring the overall efficiency and sustainability of the smart city system. The article concludes by emphasizing the need for continuous research and development to overcome the challenges of low network power and further enhance IoT technology's capabilities in smart cities.

1. Introduction

The rapid advancement of Internet of Things (IoT) technologies has been a cornerstone in the development of smart cities, aiming to enhance urban living through efficient resource utilization. However, the network power of IoT devices remains a critical challenge in this domain, which is essential for its operational efficiency and sustainability. This paper investigates this challenge, focusing on the following revised research question: "How are lighter and lower in power IoT devices shaping the smart city applications?" Inquiring into this question, we intend to provide an overview of where IoT technologies stand at present, with a focus on the latest developments concerning low-power devises for integrating them into smart cities. However, an important issue in this sector is how to control the network power of IoT devices for their effective and sustainable utility. This paper

* *Corresponding author.*
E-mail address: gs58270@student.upm.edu.my

https://doi.org/10.37934/araset.54.2.218237

investigates this challenge, focusing on the following revised research question: “What is cutting edge development of energy efficient, low weight IoT devices for the applications in smart cities?” In order to discover more on this issue, we would like to investigate the status quo of IoT technologies within smart cities and find out how evolutions concerning low-power devices are transforming what urban IoT networks look like.

Recent advancements in communication technology have given rise to Low-power Wide-area Networks (LPWANs) to enable the Internet of Things (IoT). In addition to cellular and current wireless technologies, LPWAN technologies provide low-power consumption, long-range, cheap cost for both devices and infrastructure and link many devices [1]. Nowadays, 7.5 billion of the total 30 billion IoT and Machine-to-Machine devices employing LPWA technologies are related to the Internet system via proprietary or cellular technologies. As we have seen [2], LPWA has gained popularity in the IoT. Besides, it raises various challenges, such as coexistence, mobility, spectrum limitation, scalability, etc. Low-power wireless area networks are vulnerable to identity theft and node simulation due to low power consumption. There is a real risk that these assaults may disrupt the network and compromise the integrity of the nodes, which would then compromise the user's ability to convert their data.

Network latency is an important factor which determines speed and reliability of Low-Power Wide-Area NetworksLPWAN and their applicability in smart cities. Network latency, sometimes referred to as “delay time” is just the amount of time it takes for a data file that starts in one place and ends up somewhere else. As to Internet of Things (IoT) applications, especially those based in smart cities where the people and things change constantly, latency is more than just a metric of time delay. It is one of the important differentiators which can make or mar real time data driven operations.

Latency has numerous impacts on IoT systems. Several years ago, answers to critical applications such as traffic management systems, emergency response services and real-time environmental monitoring could be late if there is too much latency. When data from numerous sensors and devices is used for rapid decisions and actions in smart cities, high latency can slow down similar processes making them less efficient and effective. For instance, in traffic management, late data might hinder the control of flow rates on roads leading to massive traffic jams and increased pollution level. Likewise, it becomes crucial to transfer data as quickly as possible during emergencies because sometimes a moment can make the difference between providing immediate assistance and missing out on an opportunity to reduce risks.

Another thing that ensures reliability of IoT systems is the fact that they do not have to work with significant delays. When real-time feedback and continuous monitoring are required, such as in the case of healthcare monitoring systems or building health monitoring, latency can impact how accurate and timely the data being analysed is going to be with which could lead to wrong conclusions or actions that they may take too late.

Consequently, an effective method for detecting and responding to such attacks is needed. One of the most important things to do to minimize the network's damage was to see and identify devices that the assault had infected. In addition, the devices were authenticated using biometrics, such as fingerprints and passwords. Communication technology has evolved exponentially over the past decades, impacting everyone's everyday life. The present era of numerous ways of communication has improved due to the progress of information technology [3]. Aside from that, technological advancements have resulted in essential improvements and innovations in the Internet of Everything (IoE) and the Internet of Things (IoT). The fast development of IoT technology has made global connections possible. Smart cities, intelligent transportation, smart homes, and intelligent systems are just some domains where the Internet of Things substantially impacts our everyday lives [4]. In

addition, the Internet of Things is vital in many fields, such as health care, industry, metals/oil/gas mining, and security [5]. As technology and IoT-based services progress, the number of IoT devices will continue to rise. By 2021, [6] predict that 35 billion IoT devices will be used.

More than 50 billion Internet of Things (IoT) devices are expected globally by 2025, according to [6]. Internet of Things (IoT) devices confront many obstacles and limitations due to their many communication needs, including concerns around power, data throughput, long-distance travel, cost, and coverage [7-9]. Network security, especially for wireless LANs, is a challenging endeavour. Countries are currently assessing ways to equip their cities for the expected surge in population, which will inevitably strain the existing city infrastructure. To support this infrastructure, Figure 1 illustrates the necessary applications of IoT.

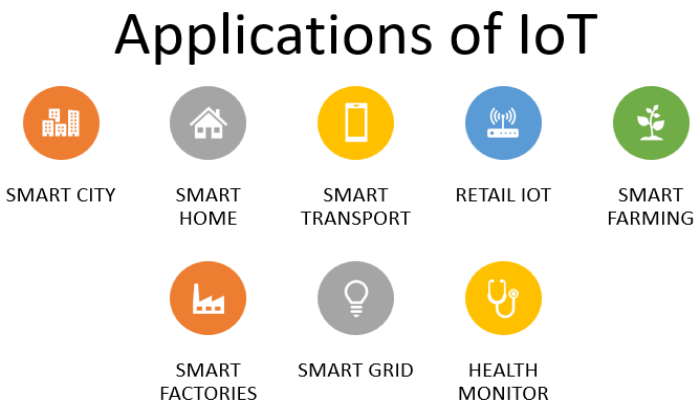

Fig. 1. Applications of IoT for supporting smart cities

Several issues may occur on a network, such as data loss, security breaches, viruses, and hackers [10]. Organizations' data is critical, and data security is a significant worry, leading researchers to offer innovative methods [11,12]. Ransomware, phishing, and data leakage are just some of the assaults that may compromise data security [13,14]. Wireless security is an uphill struggle because of the greater attack risk than LAN networks [15]. Whenever threads are detected in wireless networks, they become considerably more critical. Assaults like this are common on wireless devices:

These are common on wireless devices:

i. Configuration issues: Wireless devices frequently have configuration issues due to incorrect or insufficient configuration.
ii. Denial of Service: Issues with traffic, such as cyber-attacks, result in service interruptions.
iii. Passive Capturing: To gather information or acquire sensitive data, spying within range to gain access to the point.
iv. Rogue Access Point: Confronted with challenges relating to the connectivity of non-networked devices.
v. Stolen wireless devices: Manage the stolen devices through a wireless network and hack them to circumvent security tests.

The high level of danger associated with wireless networks is due to various causes. There are several issues and new chances for attacks on wireless networking equipment since wireless networks are intended to make it easier for end-users to connect to them [16,17]. A security and privacy issue arises because of these desired qualities of wireless local area networks in low-area networks. Security is a significant challenge in IoT devices and wireless networks, such as low-power networking devices [18]. The problem of securing low-power networks becomes more challenging as

new technologies emerge. A network's limited resources are related to its low power consumption, such as the battery, memory, and computation power [19]. The primary goal is to keep low-power networks secure and reliable. The challenge of inadequate network capacity in Internet of Things (IoT) applications deployed in smart cities is a significant concern that requires meticulous attention and efficient resolution.

Smart cities are a growing trend, leveraging intelligent technologies to enhance urban infrastructure and improve the quality of life for citizens. These technologies include the Internet of Things (IoT), artificial intelligence (AI), and data analytics. The benefits of smart cities are vast and varied, ranging from energy conservation and pollution reduction to efficient traffic management and lighting. The primary objective of smart cities is to transform our current worldview, shifting from a traditional, centralized approach to a networked, decentralized model. This involves the integration of various technologies and services to create a seamless, interconnected system that can be managed and optimized in real-time. By leveraging data and insights, smart cities can respond to changing conditions and provide citizens with more personalized, efficient services. Smart cities aim to create a more sustainable, resilient, and liveable environment.

2. Survey Methodology

This study addressed the IoT security vulnerabilities in Low Power Networks (LPN). However, this research focuses on issues such as Configuration, Denial of Service, Passive Capturing, Rogue Access Points, and Stolen wireless devices. Further, this research also highlighted the challenges and future trends of LPWAN. Based on the preceding explanation, the suggested effort focuses on three questions and targets them as follows:

Q1. Which types of low-power devices exist?
Q2. How many types of security issues have existed in LPN/ LPWAN?
Q3. Which kinds of difficulties does LPWAN face?

2.1 Integration of IoT-Based Applications in Smart Cities

Integrating IoT-based applications in smart cities is crucial to achieving sustainable urban development. There are several approaches to incorporating IoT-based applications in smart cities, and they vary depending on the specific needs and objectives of the city. One standard method is establishing a comprehensive IoT infrastructure that can support various applications, such as traffic management, waste management, and public safety. This infrastructure typically consists of sensors, communication networks, and data processing systems that collect and analyse data from various sources. By leveraging this infrastructure, cities can gain valuable insights into their operations and make informed decisions to improve efficiency, reduce costs, and enhance the quality of life for their citizens. Various approaches can be taken to achieve this integration, each with its benefits and challenges. One method is to adopt a platform-based approach, where a centralized platform is used to manage various IoT devices and applications. This approach provides a high level of control and coordination, making it easier to manage the multiple components of a smart city ecosystem. However, developing and maintaining such a platform can also be complex and expensive.

Thoroughly analysed IoT's role in smart cities connected to Low Power Networks. The working mechanism of Low power devices is also mentioned. These devices are also utilized in smart cities and play an essential role in accessing devices remotely.

Table 1
Technical Specification & Security Issues of PAN and LAN

Type	Finding
Review Questions	Q1. What are the specific characteristics and applications of lightweight, low-power IoT devices in smart cities? Q2. How many types of security issues have existed in LPN/ LPWAN? Q3. Which kinds of difficulties does LPWAN face?
Research selection criteria	- Journal articles, conference papers, reports - Research published during the period between 2005-2022 - Researchers must provide the answers to the research questions. - Research also contains the title, year, and source. - The survey targeted LPN devices and the challenges of LPWAN attacks. - Research specifically addressing lightweight, low-power IoT devices and their applications in smart cities.
Research Exclusion criteria	- Summaries of events and seminars. - The publication is not in English.
Literature Search	- Source: IEEE, Springer, peerj, and Scopus - Search equations: "LPN issues" OR "LPN issues in IoT " OR "LPWAN" OR " LPWAN issues " OR " challenges of LPWAN " OR " Energy efficiency" OR " Scalability"OR "Lightweight IoT devices" OR " Security" OR " Sensor networks security " OR " sigfox" OR "WiFi" OR "NB-IoT" OR " LoRaWAN " OR " DASH7 " OR " Energy-efficient IoT technologies

Similarly, the challenges related to LPWAN are further associated with IoT brilliant cities in which confidentiality, Privacy, and integrity are the primary concern. For the in-depth examination, a review technique was adopted. The fundamental purpose of our study is to provide information to all users so they can analyse it quickly while working on LPN/LPWAN. Table 1 summarizes the investigation findings, and Figure 2 shows the paper selection mechanism regarding the targeted domain.

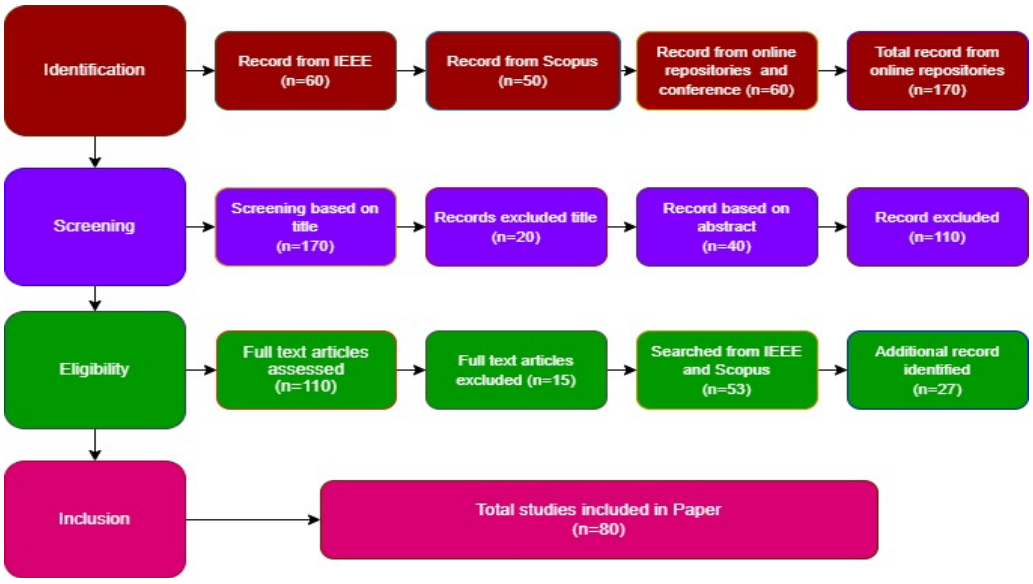

Fig. 2. Research selection mechanism

The rest of the Sections are organized as follows: The second section looks at the Literature review. Section 3 then discusses the Low power devices; Section 4 then discusses challenges and the future trend of LPWAN data. Section 5 provides the discussion, and Section 6 concludes the paper. This research gave a broad review of several approaches and techniques used in LPN. The academic

papers chosen for discussion in this review research year by year from 2005 to the present are shown in Figure 3.

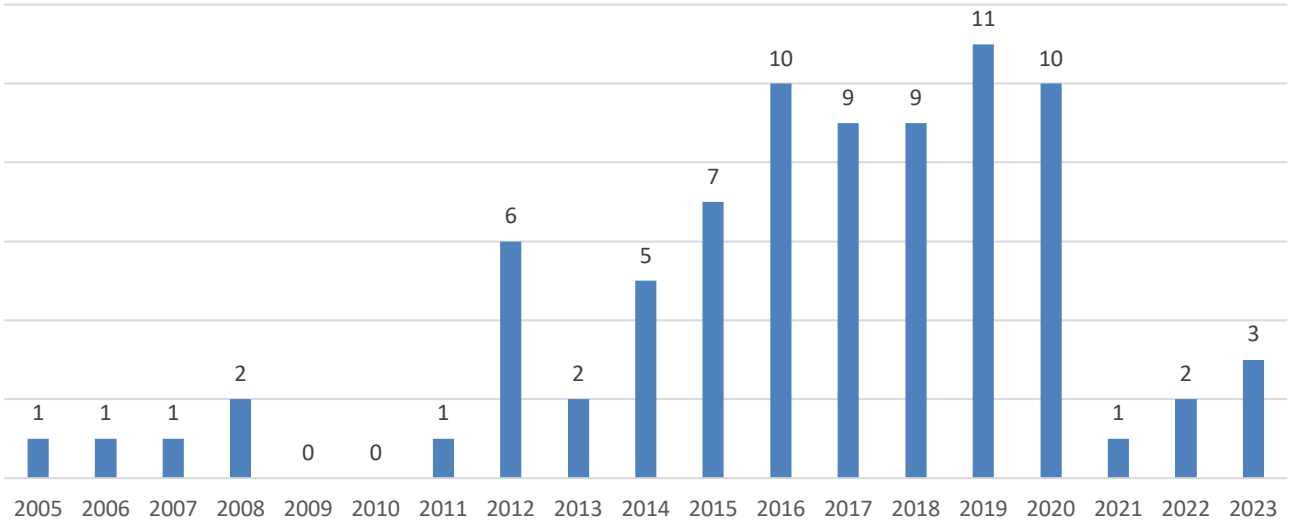

Fig. 3. Distribution of these review papers by year of publication

3. Literature Review

The literature review highlights the factors contributing to low network power, such as the location and density of IoT devices, network architecture, and device power consumption. This section concludes that the challenges associated with low network power are critical for successfully deploying IoT-based applications in smart cities.

The authors [20] propose an approach that combines IoT devices, data analytics, and intelligent algorithms to optimize energy usage across various domains, such as buildings, transportation, and street lighting. By emphasizing the role of IoT technologies in the smart city energy optimization field, the article makes a significant contribution to the smart city energy optimization field. Using IoT devices, data analytics, and intelligent algorithms, the proposed approach offers a comprehensive solution that can cover all aspects of IoT. The authors [21] discuss the challenges associated with reliability, including device failures, network congestion, and communication delays. The authors address several security concerns in the smart city applications based on IoT, such as unauthorized access, data breaches, and privacy risks, but also emphasize the importance of reliability and security in IoT-based smart city applications. IoT-based smart city applications use interconnected devices and sensors to improve urban services' efficiency, sustainability, and quality.

IoT-based smart city applications have prioritized efficient and secure wireless sensor network data link communication mechanisms. [22] discuss WSN and IoT framework data connection layer security protocols, emphasizing their importance in improving industrial resource flexibility and productivity in IoT applications. The IoT WSN architecture and significant research concerns and constraints in energy and power consumption, mobility, information transfer, quality of service (QoS), and security are described in this paper. This work highlights a WSN–IoT architecture that improves these elements and provides viable data connection layer solutions for future IoT applications.

In the world of IoT-based agriculture, [23] offers a broad insight on the application of various IoT technologies in Agri practices and network protocols necessary for their integration. Their research highlights the IoT’s capacity to redefine agricultural processes, increase growth rates of crops, and

decrease plantation costs. The article focuses on various IoT-agriculture network protocols, shedding light on the dual role of the Internet and IoT technologies in overall agricultural development. The authors also consider the problems and possible solutions of network protocols in agriculture, emphasizing the need for secure and efficient data transmission in this regard.

Provides [24] valuable insights into the challenges and strategies associated with using IoT systems within smart cities for energy management. Several techniques are proposed in research, such as energy-efficient protocols, adaptive power management, energy harvesting, and dynamic resource allocation, that can optimize energy consumption and enhance sustainability. Another study by [25] focused on the security and privacy challenges associated with smart cities and industry deployments. Several aspects of data protection are discussed in this research, including the mechanisms of authentication, secure communication protocols, access control, and detection and mitigation techniques for threats. In the era of smart cities and industries, security, and privacy must be protected since the proliferation of connected devices and data sharing will increase the chances of cyberattacks, unauthorized access, data breaches, and privacy breaches, among others.

Provides [26] a crucial study on machine learning algorithms that should help in strengthening IoT security within smart cities. Their research illuminates the increasing IoT cyber risks and the necessity of advanced security solutions. Modern cyberattacks are too sophisticated for traditional security frameworks that necessitate more dynamic and flexible approaches. This paper discusses the feasibility of these methods in threat detection and prevention as well as the challenges and opportunities of integrating machine learning into IoT security. This large-scale review emphasizes the effect machine learning has on the transformation of IoT security implementations and offers research for further development. It is of high relevance to smart cities, where numerous IoT devices are in use and network protection is an essential concern.

In this research, the author [27] provides valuable insights into applying AES-128 encryption to enhance security and minimize power consumption in LoRaWAN IoT systems. Throughout this research, the authors contribute to the existing body of knowledge by proposing an efficient and effective solution for securing communication in resource-constrained IoT environments. AES-128 is primarily designed to be scalable, low-latency, and have a high throughput in IoT deployments that use the LoRaWAN protocol, and future research can build upon these findings. The author [28] investigates a novel approach to multi-key exchange protocols utilizing Trusted Third Party (TTP) mechanisms. The authors highlight the benefits of leveraging a TTP, including reducing communication overhead and computational complexity.

The author [29] proposes a novel approach that leverages the timing information from network interactions to build a unique fingerprint for each device and actively explores timing analysis techniques to fingerprint 802.11 devices actively. A network device's active fingerprint identifies and characterizes that device based on its unique behaviour pattern or characteristic. By analysing the timing characteristics of network interactions, we can gain valuable insight into how 802.11 devices work internally, and we can also identify different types of devices, models, or even individuals by using the timing characteristics of network interactions. A comprehensive review [30,31] of the challenges and opportunities associated with device fingerprinting techniques in wireless networks was presented. Identifying and distinguishing individual wireless devices is known as device fingerprinting. The dynamic nature of wireless channels, device heterogeneity, and privacy and security concerns make device fingerprinting in wireless networks challenging.

The authors [32] highlight the advantages of their approach, such as improved synchronization accuracy, reduced energy consumption, and adaptability to changing network conditions. The adaptive nature of the proposed algorithm allows efficient synchronization with consideration of network conditions and energy constraints while considering the dynamic nature of IoT networks.

Optimizing synchronization intervals, reducing energy consumption, and accommodating varying network dynamics are the goals of adaptive synchronization algorithms. The authors demonstrate the effectiveness and efficiency of their adaptive algorithm in IoT-oriented LPWANs through simulations and comparisons.

The authors [33] offer Georgia Tech IDs (GTIDs) for device authentication; their efforts are admirable. The proposed paradigm for device authentication consists of four main components. Extracting a feature, creating a signature, calculating a similarity index, and enrolling are steps in the process. Node fingerprints were created using the preamble of signals to detect impostor nodes [34].

The network topology was limited to a hierarchical star structure. This paradigm decreases power consumption and complexity when compared to prior MAC protocols. Therefore, the proposed paradigm promotes the implementation of dense IoT sensor networks and simplifies the low-power network design [35]. The approach encouraged Long-Range (LoRa) nodes to join the network. The authors created a new technique of node joining based on the dual-key joining procedure due to the various flaws and difficulties connected with node joining. According to research, shared keys are being updated to enhance security. However, the proposed approach necessitates considerable power because two keys are pre-loaded. Increased security comes from each session's key being generated individually.

However, only LoRa nodes may be used in this setup [36]. LoRaWAN devices may interact with one another by using the key generation mechanism. To generate AES128 keys for LoRaWAN devices, there are seven unique processes. According to the study, the key was generated every three hours to keep the network secure [34]. For end-to-end verification, MAC communications were considered. An asymmetric key was used instead of the pre-shared key in that method. Their algorithm establishes a session key and user authentication in four phases. The Node and PAN ID are included each time a new key is created. According to the research, although registering a node took a long time, the authentication method was lightweight and accessible [37]. They demonstrated a scheme in which the devices and server produced the HD wallet's private and public key pairs using BIP32. Using the data from the devices, the server creates and saves a couple of root keys for communication. This advised technique improved the apparatus's security [38]. LoRa devices might benefit from an improved strategy that incorporates critical management. Root keys in LoRaWAN are suggested to pupate in a novel way. According to the researchers [39], the proposed solution uses considerably fewer resources than the HBK (hash-based key) mechanism now employed in LoRaWAN [40]. In manufacturing the two-step key, the rabbit stream pseudo-random number generator initiated and modified the root key. After that, the root key is used for data transfer and to generate session keys.

The authors [41] investigates the complexities of effective secure routing in low-powered IoT networks. Their study reinforces the ever-increasing problems prevalent in Wireless Sensor Networks WSN from IoT related to security issues such as sniffing, spoofing, and intrusions. The authors highlight that WSN-IoT networks are easy to be attacked because they consist of a numerous quantity of embedded devices with limited resources. importantly, Hussain and Hanapi’s study on the selective deployment of security mechanisms from Contiki operating system’s Routing Protocol for Low Power & Lossy Network (RPL) facilitates a promising perspective. However, their analysis is concise enough to state that such mechanisms are rather efficient when it comes to evaluating RPL’s security methods and thus helps in understanding IoT security principles in low power networks.

In this paper, a node topology based on low-power and low-cost IoT sensors is developed to manage waste management in smart cities. This node has a single-chip microprocessor, an ultrasonic sensor for measuring garbage bin filling levels, and a data transmission module based on the LoRa LPWAN standard [42]. Proxy-based encryption was used to create a novel system that uses proxy

nodes to encrypt and distribute encrypted data. In such a setup, the end node and the proxy node have secure node connections. Finding a trustworthy node was necessary because the data's integrity and authenticity had to be ensured by an encryption approach [43]. A pre-computational technique was used to propose Attribute-Based Encryption (ABE) or the Cypher policy. Precomputing was utilized to save the data that had been gathered. Data from operations was used to speed up the computation of ECC. Despite the strategy's cost savings, memory was needed to store the precomputed data [44]. To keep tabs on Internet of Things (IoT) devices that use little power, the Integrated Beekeeping System of Holistic Management and Control (IBSMC) system was suggested. Safeguards were provided by the IBSMS system's intelligent monitoring behaviour. A strategy for protecting data was presented that employs a Swapped Huffman coding scheme to encode and compress the data using an encryption algorithm based on the secret key [45]. Even though it was a simple solution to data security, an attacker with sufficient data might decode the data pattern to decrypt the scheme and retrieve the plain text [46].

Side-channel assaults were detected using the method they described. South Korea accepted a Lightweight Encryption Algorithm (LEA) for the Internet of Things in 2013. (IoT). LEA used encryption to reassure them in a confined environment. XOR and addition rotation are used instead of the S-Box lookup as in AES to guard against ALE side-channel attacks. S-Box must be removed if there is an issue with the encryption [47]. It contrasts with [48], which uses a power adoption approach to create a wireless sensor network for encryption. The energy-adoptive technique alternates between a public key and symmetric cryptography depending on the need for node energy efficiency. Solar-powered nodes for cryptography are much more effective in terms of security and energy consumption than other traditional methods, such as public-key or symmetric-key encryption.

4. Low-Power Devices

Several devices can be used in a personal area network (PAN) and a local area network (LAN). A Personal Area Network (PAN) exchanges data between a personal device and another via ZigBee or Bluetooth. Wi-Fi is part of the wireless network to share files locally in the local areas. The low-power wireless area may be observed in the following sections, especially when considering the technologies of Bluetooth, ZigBee, and WiFi since they fall into the low-power wireless place.

4.1 ZigBee

Undoubtedly, ZigBee is commonly used in smaller networked devices. This low-power, low-data-rate wireless communication protocol is specifically designed for short-range wireless connectivity and minimal power consumption in applications requiring low-power and low-data-rate wireless communication. ZigBee technology operates on the globally available 2.4 GHz band, making it a popular choice for industrial, scientific, and medical devices. This allows the system to be adopted by various regions and become interoperable. The technology is particularly suited to small-scale projects where devices in a local area must communicate wirelessly to operate. Moreover, ZigBee incorporates various security features to ensure the integrity, confidentiality, and authenticity of data transmitted over its network. Encryption, authentication, and access [49-52].

4.2 Bluetooth

Short-range wireless technology standards like Bluetooth are common and well-established. It is intended for personal area networks with minimal power requirements. It utilizes the IEEE 802.15.4

standard for access control and runs in a private area network (PAN) using the 802.15.4 MAC protocol. Bluetooth uses a frequency of 2.4 GHz and a bandwidth of 1 MHz to transmit tiny data packets across a few meters range. When the two devices, Bluetooth, and ZigBee, are compared, they cover a range of just a few feet. Star topology was widely used in Bluetooth devices. A maximum of 1000 devices may communicate across a range of 30 meters at a maximum speed of 3 MBPS (MegaBytes per second). Frequency division multiple access (FDMA)/Frequency division multiple access (TDMA) is used in Bluetooth technology. Modulation utilizes 8DPSK (8 DPSK) and Gaussian frequency-shift keying (GFSK). Many gadgets, such as smartphones and other personal devices, are often found for communication [53-56].

4.3 Wi-Fi

Wireless fidelity is referred to as Wi-Fi. 802.11ac uses IEEE 802.11b and 802.11g standards to improve performance, speed, and management. Wireless communications technology lets wireless devices connect inside specific geographic regions, such as companies, schools, and houses. It works at 2.4 GHz-5 GHz and can transmit data between the two. Since ZigBee and Bluetooth only have a range of around 10 meters, this PAN technology has an incredible advantage. However, ZigBee devices do less regarding overall network dependability. Wi-Fi devices use more power than those connected through a Personal Area Network (PAN). When a network collision occurs, Carrier Sense Multiple Access and Collision Detection are used by Wi-Fi to detect it. Modulating a wide range of frequencies requires a significant amount of bandwidth. Compared to the PAN kinds, it has a maximum data throughput of 7 Gbps. If you compare the range and data rates of WAN devices to those of Bluetooth and ZigBee, you'll see they have an advantage over PAN. A comparison [55,56] of Bluetooth, ZigBee, and Wi-numerous Fi's technical properties is provided in Table 2.

Table 2
Technical Specification & Security Issues of PAN and LAN

Low-Power Devices	Frequency	Channel Access	Modulation	Maximum Data Rate	Maximum Range	Maximum Devices Support	Security Issues
Bluetooth	2.4 GHz	FDMA/TDMA	GFSK, 8DPSK	3 Mbps	30 m	1000	MAC Spoofing, Man in the middle attack
ZigBee	2.4 GHz	CSMA/CA	BPSK/QPSK	250 Kbps	10-100 m	255	Eavesdropping, DOS, Node compromise, Sink Hole, Warm hole, Physical Attacks
Wi-Fi	2.4 GHz, 5GHz	CSMA/CA	Various	7 Gbps	100 m	255	Limited Range, Data Protection, Connectivity issues.

4.4 NB-IoT

The 3GPP, also known as the Third Generation Partnership Project, has developed and standardized the LPWA network system NB-IoT, which utilizes the LTE (Long Term Evolution) spectrum for data transmission. Release 13 contains a detailed list of the standards included in this system. The term "5G" was coined the following year, and LPWANs, particularly NB-IoT, are becoming increasingly popular due to their versatility in new industrial and intelligent parking applications. The

primary objective of developing this technology is to provide long-distance coverage while keeping battery life and equipment expenses in check. [57-61].

4.5 Lora

LPWAN, also known as LoRaWAN, was developed and commercialized by Semtech Corporation. Recently, the LoRa Alliance announced the development of a MAC layer protocol for wireless devices that require battery power. One of LoRa's key features is using unlicensed 1 GHz frequency, allowing for wide-area network mobility. This device supports all frequencies from 433/868/915 to the border frequency, focusing on 868 MHz Uplink and downlink frequencies use frequency-shift keying (FSK) in conjunction with Chirp Spread Spectrum (CSS) spread spectrum modulation. LoRaWAN is a long-range communication technology with a maximum data rate of 50 kilobits per second and can cover up to 20 kilometres with a packet size of 2047 kilobytes. Every LoRaWAN node is safeguarded by AES 128-bit encryption, ensuring secure communication. The LoRaWAN network was launched in 2015 and is still evolving with the development of mesh and star topologies. LoRaWAN's security measures are becoming more robust as nodes use encrypted communication to communicate with servers and gateways. During network registration, no encryption is applied to speed up the process. However, once the server authenticates the node, communication is encrypted. LoRaWAN is an excellent solution for long-distance communication [62-65].

4.6 Sigfox

Sigfox is widely regarded as the most prominent transmission mode in low-power wide-area networks. It serves as a viable solution for the challenges surrounding LPWAN connections. Sigfox was established by a French telecom company in 2009 to address the issues faced by low-power network devices. The platform operates with Ultra-Narrow Band (UNB) modulation, which restricts broadcast frequencies to 200 kHz. With a range of up to 50 kilometres and UL to DL data speeds of up to 100 kbps, Sigfox offers USB-OTG compatibility for straightforward application integration. It takes 24 bytes to send a message with a payload of 12 bytes while up linking and 8 when downlinking. A typical communication travels from the base station to a satellite in 2 seconds or less. The 868/902 MHz spectrum modulates using a logical database (DBPSJ) and GFSK techniques. Less noise and a more accessible signal are decoding since Sigfox uses ultra-narrowband technology. In Sigfox, message signing is not enabled by default. Depending on the application, clients may choose between Sigfox's solution and end-to-end encryption [66-69].

4.7 Weightless

Weightless-P, Weightless-W, and Weightless-N are Low Power Wide Area Network (LPWAN) technologies that enable the integration of weightless devices into a network. Commercialized initially by a non-profit organization in 2008, this technology has since been further developed by Neul and is currently being implemented in collaboration with Huawei. Weightless is one of the latest additions to the 802.11n family and incorporates advanced Ultra-narrowband technology, which boasts a 1 GHz spectrum and 24 uplink channel access. Combining BPSK, QPSK, and DBPSK can transmit at 10 Mbps across 5 kilometres. Our nodes are encrypted and authenticated using the AES 128-bit method for additional safety and protection. Using a star topology, a safe means of data transit is possible. Authentication and data encryption are improved due to nodes' use of AES 128. If

the session key is stolen in a physical attack, there is a risk that the node's security will be compromised [70,71].

4.8 DASH7

The DASH7 wireless protocol, which is open-source and operates in the 433/868/915 MHz frequency bands, is specifically designed for sensor applications. It was first introduced in 2003 and works in the ISM band. The system utilizes 128-bit AES symmetric key encryption for node authentication and relies on the network's security. Finally, the secret key is stored in the end node to conserve power. With recent technological advancements and the increasing adoption of IoT devices, LPWANs for small, battery-powered, compute, and memory-limited end devices such as wearables are vulnerable to security threats. LPWAN DASH7 may extend the battery life of end devices over many years. AES 128-bit data encryption is used to safeguard data transit. Using a packet size of 167kbps, DASH7 can transfer enormous amounts of data across a broad region. Three channels of GFSK modulation are supported. A network is built using a tree or star topology. DASH7 is made up of gateways, controllers, and endpoints. The gateway is considered responsible for transferring the data to the server if it actively collects end-to-end data. Like the gateway, it has a sleep cycle to save power. The DASH7's [72] energy efficiency is one of its features. Table 3 lists the technical parameters for LPWAN.

Table 3
Technical Specification of LPWAN

	NB-IoT	Lora	Sigfox	Weightless	DASH7
Channel Access	Multiple	10 (EUR), 8 (DL)	360	24 (UL)	3
Frequency	LET & GSM, USA	433/868/915 MHz	868/902 MHz	1 GHz	433/868/915 MHz
Modulation	QPSK	CSS/FSK	DBPSK & GFSK	BPSK, QPSK, DBPSK	GFSK
Maximum Data Rate	UL (158.5 kbps), DL (106 kbps)	50 Kbps	UL (100 kbps), DL (600 kbps)	10 Mbps	167 Kbps
Maximum Range	0-5 Km	5-20 Km	10-50 Km	5 Km	0-5 Km
Encryption	AES 128 bit	AES 128 bit	AES	AES 128 bit	AES 128 bit
Topology	Star	Star/Mesh	Star	Star	Star/Tree
Packet Size	2047 B	2047 B	UL (12 B), DL (8 B)	>10 Kb	256 B
Security	In development	Developed	Partially Afforested	Developed	N/A
Founded	2016	2015	2009	2012	2013
Security Issue	Insufficient authorization/authentication Poor application and end-point security Lack of physical security	MTM Attack Payload frame attacks network, flooding attack physical, RF attack, lamming attack	POC replay attack, SOD Attack	Key attack	authentication

5. Challenges in LPWAN and Future Trends

Scalability is a significant difficulty for LPWANs in dense networks. It enables several devices to connect to one base station, as well as the deployment of additional base stations across the network. Now a day, LPWAN is the most popular and more demanding among users. Therefore, more devices are required to meet the needs. As a result, structural scalability was already insufficient to accommodate LPWAN use cases.

Similarly, getting statistics on LPWAN performance is a significant challenge. Because data from major LPWANs (LoRaWAN, SigFox, and NB-IoT) is publicly accessible, acquiring data for others is far more complex due to fewer references. So, there is a need to develop more innovative methods to enhance personal and commercial operations.

But, in response to the complicated security challenges outlined above, new and promising trends of LPWAN technologies are emerging on the horizon. These developments are not only minor advancements but revolutionary because they promise to offer significantly stronger and more stable solutions that will fundamentally change the landscape of security in smart cities. As we explore these future trends, it becomes obvious that they have the potential of addressing current vulnerabilities and also opening new opportunities to developing smarter and more secure, efficient and scalable smart city applications.

In addressing the described complex security issues, new and promising trends are emerging in the horizon of LPWAN technologies. These are not just incremental enhancements but are likely to provide more robust and resilient solutions that could essentially transform the security scene of smart cities. As we explore these future trends, it also becomes self-evident that they have the potential to address existing vulnerabilities and lay a foundation for more secure, efficient and scalable smart city applications. This section delves into these emerging trends, implications for smart cities and how they are poised to change the way LPWAN fits within the IoT ecosystem.

However, there has been minimal attention on the security of LPWANs. Unauthorized access can quickly compromise the intelligent home controller's security. Using illegal access, criminals can steal information and gain complete control of household equipment, causing discomfort to users. Similarly, unlawful access to smart cities, agriculture, and inter-vehicle communication results in mortality and environmental damage. So, adequate security is required to verify the user/owner efficiently; otherwise, LPWANs are not commercially feasible. Some of the other security challenges are discussed below.

5.1 Confidentiality

Data transmission and reception must be secure enough for only the intended recipient and the sender to access the data via a network node to satisfy these essential criteria. When dealing with sensitive information, it's critical to safeguard the privacy of all parties. Because data is such an important asset, it must be protected at all costs. Man-in-the-middle attacks commonly use two common assaults: the compromised critical attack and the critical compromise attack. When attackers steal a key from the network, they use it to start an attack in the first example. For example, someone who steals a user's private key may obtain data, which they can subsequently edit or update and pass on to the receiver. When two nodes think their connections are secure, but a third party has access to the data, password, or code, a "man in the middle" attack is possible. Multiple devices, clients, and objects must authenticate each other to acquire system access through trustworthy administrations. The challenge is discovering how to securely deal with the client's personality,

items/articles, and devices. Many literary works have been proven to cope with them without worry in low-power networks.

5.2 Integrity

To protect the network from being disrupted by different types of threads. The integrity of the network is a significant concern. Ensuring the accuracy of data is a critical component of data integrity. Data manipulation may be prevented by mistake or intent using this strategy. Maintaining the network's integrity is essential to avoid deletions, tweaks, and modifications. Integrity is the primary concern in low-power networks because of the risk of wormholes or replay attacks. The wormhole attack cannot be carried out without a jammer and sniffer. The sniffer captures a data packet and decides whether to jam it. Problems with LPWAN are shown in Table 4.

Table 4
Attacks on LPWAN

	NB-IoT	Lora	Sigfox	Weightless	DASH7
Replay Attack	-	Frame Counter	Sequence Number	Data Frame Counter	N/A
Possible Attacks	Jamming	Jamming	Replay Attack	Jamming	Jamming
Possible Attacks	Physical attack, Port scanning, APR spoofing, DSN spoofing,	Network Flooding attack packet forging	POC attack	Key attack	

5.3 Privacy

People are linked together to transmit information through the internet safely, yet this poses several threats to sensitive data in various circumstances, such as sniffer and spoofing, data manipulation via unauthorized modification of IoT nodes, and unauthorized access [73,74]. The IoT device should determine if the user or machine has been authorized access to the system. A permission mechanism should be based on rules for accessing and manipulating data.

5.4 Trust Management

Nowadays, several distinct and diverse sets of IoT devices generate massive amounts of data daily, vulnerable to various threats, hazards, and problems. These problems extend to all IoT layers or devices and significantly impact information or administration quality [75,76]. Effective authorization processes that correctly verify both the sender and the receiver or other users in the network are required to offer a safe environment for users.

5.5 Vulnerabilities

Vulnerabilities are systematic flaws that allow unauthorized users and attackers to steal the user's personal information. However, these flaws occur at several levels, including user devices, scripts, hardware, and IoT devices' methodologies, negatively impacting the entire framework [77]. The application should have a straightforward development environment to use and comprehend. Simultaneously, it should be suitable for functioning in a high-pressure environment, and its working should be precise. Application engineers should concentrate on application validation tasks such as designing, data collection, and system management.

5.6 Interoperability

IoT devices that are poorly designed might harm network resources. However, security arises when devices are linked to the internet. The front-end interfaces of devices are connected to the Internet; if they are compromised, a substantial amount of data or information is lost [78]. As a result, customers never pay attention to products and services that are limited in their adaptability. To gain the user's attention, IoT devices must be designed to suit their needs while being safe from the abovementioned risks and assaults [79].

Table 5
Summary of Challenges in LPWAN

Challenge	Implications	Potential Solutions/Mitigations
Limited Range	Reduced connectivity in larger areas	Use of repeaters, development of more powerful transmitters
Security Vulnerabilities	Risk of data breaches and unauthorized access	Implementation of advanced encryption techniques, regular security audits
Interference Issues	Signal disruption leading to data loss	Utilizing adaptive frequency hopping, improving signal processing algorithms
Energy Consumption	Shortened lifespan of IoT devices	Energy-efficient protocols, use of renewable energy sources
Scalability Concerns	Difficulty in managing a large number of devices	Cloud-based management solutions, development of scalable network architectures
Data Throughput Limitations	Inability to handle large volumes of data	Optimization of data transmission protocols, use of data compression techniques
Network Congestion	Slower data transmission rates	Implementing traffic management strategies, increasing network bandwidth

6. Discussion

The LPWAN technologies landscape is changing at a fast pace and as time goes by, new protocols and breakthroughs appear. Future developments are likely to involve making security measures better, increasing energy efficiency, as well as creating more resilient and adaptive protocols. For instance, a combination of AI and machine learning algorithms could result in smarter, self-tuning networks that dynamically adapt to changes triggered by the environment or different patterns of use.

These technological developments are promising in terms of smart cities. Security measures in LPWAN technologies would also need to be improved as they are important for protecting sensitive data and privacy within urban networks of IoT. Improved connectivity and energy efficiency will allow IoT devices to be deployed on a greater scale in various urban applications, ranging from traffic control to environmental monitoring without overwhelming the city’s power supply. IoT solutions in urban areas are expected to witness a spike in adoption from LPWAN technologies advancements.

6.1 Implications for Smart Cities

These are the anticipated trends in LPWAN technologies that will revolutionize how smart cities would be managed and run. Quality and efficiency IoT networks in the cities will make data collection and analysis a better process, resulting in a higher level of informed decision-making. This could lead to more efficient use of resources, better public services, and increased quality of urban life.

However, the incorporation of such sophisticated LPWAN technologies into already developed urban structures will not be without obstacles. Cities must expect potential cyber threats

accompanying the implementation of more connected devices. There is also need for standardization and interoperability between various IoT devices and networks so that there can be smooth integration and communication.

For instance, a hypothetical situation could be one in which a city installs an LPWAN-based air quality monitoring system. This system might involve energy-efficient sensors that communicate over an AI-readable, secure network providing real time information to city officials. Such a system would not only facilitate better environmental monitoring but also allow quick responses to pollution incidents, showing the various practical uses of these technologies for future LPWAN.

7. Conclusion

LPWAN technologies offer cost-effective wireless communication solutions. With the growing popularity of the Internet of Things, wireless local area networks (WLANs) have become increasingly problematic for IoT devices. This study investigates the potential security issues associated with using low-power wireless LANs for local networking. Our research delves into various aspects of wireless technology, focusing on improving the standards for IoT devices to ensure their integrity and confidentiality. We tackle key management, authentication, and encryption issues for low-power networks. Low network power poses a significant challenge for IoT-based applications in smart cities, affecting their efficiency and reliability. Our findings aim to address these challenges and support the development of more secure and reliable wireless networks for IoT devices.

Acknowledgment

Geran Putra Berimpak Universiti Putra Malaysia, Vote Number 9659400, supported this work. Our sincere thanks to Geran Putra Berimpak Universiti Putra Malaysia for their support.

References

[1] Nguyen, Huy, Nam Tuan Le, Pham Tung Lam, Nguyen Cong Hoan, Thanh Luan Vu, Minh Duc Thieu, and Yeong Min Jang. "The next generation architecture of low power wide area network for energy platform." In *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 144-147. IEEE, 2019. https://doi.org/10.1109/ICUFN.2019.8806189

[2] Ismail, Dali, Mahbubur Rahman, and Abusayeed Saifullah. "Low-power wide-area networks: opportunities, challenges, and directions." In *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*, pp. 1-6. 2018. https://doi.org/10.1145/3170521.3170529

[3] Cho, Jaehee. "Roles of smartphone app use in improving social capital and reducing social isolation." *Cyberpsychology, behavior, and social networking* 18, no. 6 (2015): 350-355. https://doi.org/10.1089/cyber.2014.0657

[4] Bogatinoska, Dijana Capeska, Reza Malekian, Jasna Trengoska, and William Asiama Nyako. "Advanced sensing and internet of things in smart cities." In *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 632-637. IEEE, 2016. https://doi.org/10.1109/MIPRO.2016.7522218

[5] Namasudra, Suyel, Ganesh Chandra Deka, Prashant Johri, Mohammad Hosseinpour, and Amir H. Gandomi. "The revolution of blockchain: State-of-the-art and research challenges." *Archives of Computational Methods in Engineering* 28 (2021): 1497-1515. https://doi.org/10.1007/s11831-020-09426-0

[6] Ejaz, Waleed, Alagan Anpalagan, Waleed Ejaz, and Alagan Anpalagan. "Dimension reduction for big data analytics in internet of things." *Internet of Things for Smart Cities: Technologies, Big Data and Security* (2019): 31-37. https://doi.org/10.1007/978-3-319-95037-2_3

[7] Yaacoub, Elias, and Mohamed-Slim Alouini. "A key 6G challenge and opportunity—Connecting the base of the pyramid: A survey on rural connectivity." *Proceedings of the IEEE* 108, no. 4 (2020): 533-582. https://doi.org/10.1109/JPROC.2020.2976703

[8] Shen, Hang, Guangwei Bai, Yujia Hu, and Tianjing Wang. "P2TA: Privacy-preserving task allocation for edge computing enhanced mobile crowdsensing." *Journal of Systems Architecture* 97 (2019): 130-141. https://doi.org/10.1016/j.sysarc.2019.01.005

[9] Pant, Vinay Kumar, Jyoti Prakash, and Amit Asthana. "Three step data security model for cloud computing based on RSA and steganography." In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 490-494. IEEE, 2015. https://doi.org/10.1109/ICGCIoT.2015.7380514

[10] Choubey, Siddharth Dutt, and Mohit Kumar Namdeo. "Study of data security and privacy preserving solutions in cloud computing." In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1101-1106. IEEE, 2015. https://doi.org/10.1109/ICGCIoT.2015.7380627

[11] Mohan, N. Ram, and N. Praveen Kumar. "Predicting and Analysis of Phishing Attacks and Breaches In E-Commerce Websites." *International Journal of Scientific Research in Science, Engineering and Technology* (2020): 170-175. https://doi.org/10.32628/IJSRSET207443

[12] Cheng, Long, Fang Liu, and Danfeng Yao. "Enterprise data breach: causes, challenges, prevention, and future directions." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7, no. 5 (2017): e1211. https://doi.org/10.1002/widm.1211

[13] Khan, Shafiullah, Kok-Keong Loo, Tahir Naeem, and Mohammad Abrar Khan. "Denial of service attacks and challenges in broadband wireless networks." *8; 7* (2008).

[14] Akyildiz, Ian F., and Xudong Wang. "A survey on wireless mesh networks." *IEEE Communications magazine* 43, no. 9 (2005): S23-S30. https://doi.org/10.1109/MCOM.2005.1509968

[15] Li, Xiaomin, Di Li, Jiafu Wan, Athanasios V. Vasilakos, Chin-Feng Lai, and Shiyong Wang. "A review of industrial wireless networks in the context of industry 4.0." *Wireless networks* 23 (2017): 23-41. https://doi.org/10.1007/s11276-015-1133-7

[16] Yaqoob, Ibrar, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges." *IEEE wireless communications* 24, no. 3 (2017): 10-16. https://doi.org/10.1109/MWC.2017.1600421

[17] Akinyele, Daniel O., and Ramesh K. Rayudu. "Review of energy storage technologies for sustainable power networks." *Sustainable energy technologies and assessments* 8 (2014): 74-91. https://doi.org/10.1016/j.seta.2014.07.004

[18] Nikravan, Mohammad, Ali Movaghar, and Mehdi Hosseinzadeh. "A lightweight defense approach to mitigate version number and rank attacks in low-power and lossy networks." *Wireless Personal Communications* 99 (2018): 1035-1059. https://doi.org/10.1007/s11277-017-5165-4

[19] Chen, Zhong, C. B. Sivaparthipan, and BalaAnand Muthu. "IoT based smart and intelligent smart city energy optimization." *Sustainable Energy Technologies and Assessments* 49 (2022): 101724. https://doi.org/10.1016/j.seta.2021.101724

[20] Tragos, Elias Z., Vangelis Angelakis, Alexandros Fragkiadakis, David Gundlegard, Cosmin-Septimiu Nechifor, George Oikonomou, Henrich C. Pöhls, and Anastasius Gavras. "Enabling reliable and secure IoT-based smart city applications." In *2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS)*, pp. 111-116. IEEE, 2014. https://doi.org/10.1109/PerComW.2014.6815175

[21] Ejaz, Waleed, Muhammad Naeem, Adnan Shahid, Alagan Anpalagan, and Minho Jo. "Efficient energy management for the internet of things in smart cities." *IEEE Communications magazine* 55, no. 1 (2017): 84-91. https://doi.org/10.1109/MCOM.2017.1600218CM

[22] Hasan, Muhammad Zulkifl, and Zurina Mohd Hanapi. "Efficient and secured mechanisms for data link in IoT WSNs: A literature review." *Electronics* 12, no. 2 (2023): 458. https://doi.org/10.3390/electronics12020458

[23] Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, Summaira Nosheen, Ali Moiz Qureshi, Adeel Ahmad Siddiqui, Muhammad Atif Yaqub, Saad Hussain Chuhan, Afshan Belal, and Muzammil Mustafa. "IoT Security Implementation using Machine Learning." *Research Briefs on Information and Communication Technology Evolution* 9 (2023): 116-119. https://doi.org/10.56801/rebicte.v9i.161

[24] Rao, P. Muralidhara, and Bakkiam David Deebak. "Security and privacy issues in smart cities/industries: technologies, applications, and challenges." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 8 (2023): 10517-10553. https://doi.org/10.1007/s12652-022-03707-1

[25] Tsai, Kun-Lin, Yi-Li Huang, Fang-Yie Leu, Ilsun You, Yu-Ling Huang, and Cheng-Han Tsai. "AES-128 based secure low power communication for LoRaWAN IoT environments." *Ieee Access* 6 (2018): 45325-45334. https://doi.org/10.1109/ACCESS.2018.2852563

[26] Tsai, Kun-Lin, Yi-Li Huang, Fang-Yie Leu, and Ilsun You. "TTP based high-efficient multi-key exchange protocol." *IEEE Access* 4 (2016): 6261-6271. https://doi.org/10.1109/ACCESS.2016.2613442

[27] Sieka, Bartlomiej. "Active fingerprinting of 802.11 devices by timing analysis." In *CCNC 2006. 2006 3rd IEEE Consumer Communications and Networking Conference, 2006.*, vol. 1, pp. 15-19. IEEE, 2006.
[28] Xu, Qiang, Rong Zheng, Walid Saad, and Zhu Han. "Device fingerprinting in wireless networks: Challenges and opportunities." *IEEE Communications Surveys & Tutorials* 18, no. 1 (2015): 94-104. https://doi.org/10.1109/COMST.2015.2476338
[29] Xing, Kai, Fang Liu, Xiuzhen Cheng, and David HC Du. "Real-time detection of clone attacks in wireless sensor networks." In *2008 The 28th International Conference on Distributed Computing Systems*, pp. 3-10. IEEE, 2008. https://doi.org/10.1109/ICDCS.2008.55
[30] Petroni, Andrea, Francesca Cuomo, Leonisio Schepis, Mauro Biagi, Marco Listanti, and Gaetano Scarano. "Adaptive data synchronization algorithm for iot-oriented low-power wide-area networks." *Sensors* 18, no. 11 (2018): 4053. https://doi.org/10.3390/s18114053
[31] Radhakrishnan, Sakthi Vignesh, A. Selcuk Uluagac, and Raheem Beyah. "GTID: A technique for physical device and device type fingerprinting." *IEEE Transactions on Dependable and Secure Computing* 12, no. 5 (2014): 519-532. https://doi.org/10.1109/TDSC.2014.2369033
[32] Rehman, Saeed Ur, Kevin W. Sowerby, Peter Han Joo Chong, and Shafiq Alam. "Robustness of radiometric fingerprinting in the presence of an impersonator." In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1-5. IEEE, 2017.
[33] Petrosky, Eric E., Alan J. Michaels, and Joseph M. Ernst. "A low power IoT medium access control for receiver-assigned CDMA." *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 11, no. 2 (2019): 24-41. https://doi.org/10.4018/IJITN.2019040103
[34] Kim, Jaehyu, and JooSeok Song. "A dual key-based activation scheme for secure LoRaWAN." *Wireless Communications and Mobile Computing* 2017 (2017). https://doi.org/10.1155/2017/6590713
[35] Ruotsalainen, Henri, Junqing Zhang, and Stepan Grebeniuk. "Experimental investigation on wireless key generation for low-power wide-area networks." *IEEE Internet of Things Journal* 7, no. 3 (2019): 1745-1755. https://doi.org/10.1109/JIOT.2019.2946919
[36] Roselin, Annie Gilda, Priyadarsi Nanda, and Surya Nepal. "Lightweight authentication protocol (LAUP) for 6LoWPAN wireless sensor networks." In *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 371-378. IEEE, 2017. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.260
[37] Wuille, Pieter. "Bip32: Hierarchical deterministic wallets." *https://github. com/genjix/bips/blob/master/bip-0032. md* (2012).
[38] Parhami, Behrooz. "Data Longevity and Compatibility." (2019). https://doi.org/10.1007/978-3-319-77525-8_331
[39] Xing, Jinyu, Lu Hou, Kuan Zhang, and Kan Zheng. "An improved secure key management scheme for LoRa system." In *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, pp. 296-301. IEEE, 2019. https://doi.org/10.1109/ICCT46805.2019.8947215
[40] Cerchecci, Matteo, Francesco Luti, Alessandro Mecocci, Stefano Parrino, Giacomo Peruzzi, and Alessandro Pozzebon. "A low power IoT sensor node architecture for waste management within smart cities context." *Sensors* 18, no. 4 (2018): 1282. https://doi.org/10.3390/s18041282
[41] Hussain, Muhammad Zunnurain, and Zurina Mohd Hanapi. "Efficient secure routing mechanisms for the low-powered IoT network: A literature review." *Electronics* 12, no. 3 (2023): 482. https://doi.org/10.3390/electronics12030482
[42] Naoui, Sarra, Mohamed Elhoucine Elhdhili, and Leila Azouz Saidane. "Enhancing the security of the IoT LoraWAN architecture." In *2016 international conference on performance evaluation and modeling in wired and wireless networks (PEMWN)*, pp. 1-7. IEEE, 2016. https://doi.org/10.1109/PEMWN.2016.7842904
[43] Oualha, Nouha, and Kim Thuat Nguyen. "Lightweight attribute-based encryption for the internet of things." In *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-6. IEEE, 2016. https://doi.org/10.1109/ICCCN.2016.7568538
[44] Kontogiannis, Sotirios. "An internet of things-based low-power integrated beekeeping safety and conditions monitoring system." *Inventions* 4, no. 3 (2019): 52. https://doi.org/10.3390/inventions4030052
[45] Jang, Yun Seong, Muhammad Rehan Usman, Muhammad Arslan Usman, and Soo Young Shin. "Swapped Huffman tree coding application for low-power wide-area network (LPWAN)." In *2016 international conference on smart green technology in electrical and information systems (ICSGTEIS)*, pp. 53-58. IEEE, 2016. https://doi.org/10.1109/ICSGTEIS.2016.7885766
[46] Choi, Jaehak, and Youngseop Kim. "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system." In *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pp. 1-4. IEEE, 2016. https://doi.org/10.1109/APSIPA.2016.7820845

[47] Kim, Jong Min, Hong Sub Lee, Junmin Yi, and Minho Park. "Power adaptive data encryption for energy-efficient and secure communication in solar-powered wireless sensor networks." *Journal of Sensors* 2016 (2016). https://doi.org/10.1155/2016/2678269

[48] Di Francesco, Mario, Giuseppe Anastasi, Marco Conti, Sajal K. Das, and Vincenzo Neri. "Reliability and energy-efficiency in IEEE 802.15. 4/ZigBee sensor networks: An adaptive and cross-layer approach." *IEEE Journal on selected areas in communications* 29, no. 8 (2011): 1508-1524. https://doi.org/10.1109/JSAC.2011.110902

[49] Song, Aijuan, and Guangyuan Si. "Remote monitoring system based on Zigbee wireless sensor network." In *2017 29th Chinese Control And Decision Conference (CCDC)*, pp. 2618-2621. IEEE, 2017. https://doi.org/10.1109/CCDC.2017.7978956

[50] Zhao, Lingjiang, and Yufa Xu. "Artificial Intelligence Monitoring System Using ZigBee Wireless Network Technology in Warehousing and Logistics Innovation and Economic Cost Management." *Wireless Communications and Mobile Computing* 2022 (2022). https://doi.org/10.1155/2022/4793654

[51] Zhang, Ting, Jiang Lu, Fei Hu, and Qi Hao. "Bluetooth low energy for wearable sensor-based healthcare systems." In *2014 IEEE healthcare innovation conference (HIC)*, pp. 251-254. IEEE, 2014. https://doi.org/10.1109/HIC.2014.7038922

[52] Sonawane, Asmita Pandit, Janhavi Sanjay Pradhan, Vaibhavi Prakash Waghmare, Saurabh Kesari, Shashank Kumar Singh, and Prashant Pal. "Complete Data Transmission using Li-Fi Technology with Visible Light Communication." In *2022 International Conference on Futuristic Technologies (INCOFT)*, pp. 1-5. IEEE, 2022. https://doi.org/10.1109/INCOFT55651.2022.10094453

[53] Dolińska, Iwona, Mariusz Jakubowski, and Antoni Masiukiewicz. "Interference comparison in wi-fi 2.4 ghz and 5 ghz bands." In *2017 International Conference on Information and Digital Technologies (IDT)*, pp. 106-112. IEEE, 2017. https://doi.org/10.1109/DT.2017.8024280

[54] Kharel, Jeevan, Haftu Tasew Reda, and Soo Young Shin. "Fog computing-based smart health monitoring system deploying lora wireless communication." *IETE Technical Review* 36, no. 1 (2019): 69-82. https://doi.org/10.1080/02564602.2017.1406828

[55] Chaudhari, Bharat S., Marco Zennaro, and Suresh Borkar. "LPWAN technologies: Emerging application characteristics, requirements, and design considerations." *Future Internet* 12, no. 3 (2020): 46. https://doi.org/10.3390/fi12030046

[56] Anand, Sharath, and Sudhir K. Routray. "Issues and challenges in healthcare narrowband IoT." In *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 486-489. IEEE, 2017. https://doi.org/10.1109/ICICCT.2017.7975247

[57] Alagarsamy, Gautami, J. Shanthini, and G. Naveen Balaji. "A survey on technologies and challenges of LPWA for narrowband IoT." *Trends in cloud-based IoT* (2020): 73-84. https://doi.org/10.1007/978-3-030-40037-8_5

[58] Qadir, Qahhar Muhammad, Tarik A. Rashid, Nawzad K. Al-Salihi, Birzo Ismael, Alexander A. Kist, and Zhongwei Zhang. "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs." *IEEE Access* 6 (2018): 77454-77473. https://doi.org/10.1109/ACCESS.2018.2883151

[59] Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094. https://doi.org/10.1016/j.comnet.2019.107094

[60] Sanchez-Gomez, Jesus, Dan Garcia-Carrillo, Rafael Marin-Perez, and Antonio F. Skarmeta. "Secure authentication and credential establishment in narrowband IoT and 5G." *Sensors* 20, no. 3 (2020): 882. https://doi.org/10.3390/s20030882

[61] Ribeiro, Lucas Eduardo, Davi Wei Tokikawa, Joao Luiz Rebelatto, and Glauber Brante. "Comparison between LoRa and NB-IoT coverage in urban and rural Southern Brazil regions." *Annals of Telecommunications* 75 (2020): 755-766. https://doi.org/10.1007/s12243-020-00774-3

[62] Sinha, Rashmi Sharan, Yiqiao Wei, and Seung-Hoon Hwang. "A survey on LPWA technology: LoRa and NB-IoT." *Ict Express* 3, no. 1 (2017): 14-21. https://doi.org/10.1016/j.icte.2017.03.004

[63] Dasiga, Sankar, Aditya Akash Rajeev Bhatia, Atul Bhirangi, and Ayesha Siddiqua. "LoRa for the last mile connectivity in IoT." In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pp. 195-200. IEEE, 2020. https://doi.org/10.1109/SMART50582.2020.9337114

[64] Drăgulinescu, Ana Maria Claudia, Adrian Florin Manea, Octavian Fratu, and Andrei Drăgulinescu. "LoRa-based medical IoT system architecture and testbed." *Wireless Personal Communications* (2020): 1-23. https://doi.org/10.1007/s11277-020-07235-z

[65] Ikpehai, Augustine, Bamidele Adebisi, Khaled M. Rabie, Kelvin Anoh, Ruth E. Ande, Mohammad Hammoudeh, Haris Gacanin, and Uche M. Mbanaso. "Low-power wide area network technologies for Internet-of-Things: A comparative review." *IEEE Internet of Things Journal* 6, no. 2 (2018): 2225-2240. https://doi.org/10.1109/JIOT.2018.2883728

[66] Buurman, Ben, Joarder Kamruzzaman, Gour Karmakar, and Syed Islam. "Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges." *IEEE Access* 8 (2020): 17179-17220. https://doi.org/10.1109/ACCESS.2020.2968057

[67] Aernouts, Michiel, Rafael Berkvens, Koen Van Vlaenderen, and Maarten Weyn. "Sigfox and LoRaWAN datasets for fingerprint localization in large urban and rural areas." *Data* 3, no. 2 (2018): 13. https://doi.org/10.3390/data3020013

[68] Poursafar, Noushin, Md Eshrat E. Alahi, and Subhas Mukhopadhyay. "Long-range wireless technologies for IoT applications: A review." In *2017 Eleventh International Conference on Sensing Technology (ICST)*, pp. 1-6. IEEE, 2017. https://doi.org/10.1109/ICSensT.2017.8304507

[69] Stoynov, Viktor, Vladimir Poulkov, and Zlatka Valkova-Jarvis. "Low power wide area networks operating in the ism band-overview and unresolved challenges." In *Future Access Enablers for Ubiquitous and Intelligent Infrastructures: 4th EAI International Conference, FABULOUS 2019, Sofia, Bulgaria, March 28-29, 2019, Proceedings 283*, pp. 96-109. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-23976-3_10

[70] Weyn, Maarten, Glenn Ergeerts, Luc Wante, Charles Vercauteren, and Peter Hellinckx. "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication." *International Journal of Distributed Sensor Networks* 9, no. 12 (2013): 870430. https://doi.org/10.1155/2013/870430

[71] Ergeerts, Glenn, Maciej Nikodem, Dragan Subotic, Tomasz Surmacz, Bartosz Wojciechowski, Paul De Meulenaere, and Maarten Weyn. "DASH7 alliance protocol in monitoring applications." In *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pp. 623-628. IEEE, 2015. https://doi.org/10.1109/3PGCIC.2015.93

[72] Ling, Zhen, Kaizheng Liu, Yiling Xu, Yier Jin, and Xinwen Fu. "An end-to-end view of IoT security and privacy." In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1-7. IEEE, 2017. https://doi.org/10.1109/GLOCOM.2017.8254011

[73] Dalipi, Fisnik, and Sule Yildirim Yayilgan. "Security and privacy considerations for iot application on smart grids: Survey and research challenges." In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 63-68. IEEE, 2016. https://doi.org/10.1109/W-FiCloud.2016.28

[74] Sicari, Sabrina, Alessandra Rizzardi, Daniele Miorandi, and Alberto Coen-Porisini. "REATO: REActing TO Denial of Service attacks in the Internet of Things." *Computer Networks* 137 (2018): 37-48. https://doi.org/10.1016/j.comnet.2018.03.020

[75] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an analysis of security issues, challenges, and open problems in the internet of things." In *2015 ieee world congress on services*, pp. 21-28. IEEE, 2015. https://doi.org/10.1109/SERVICES.2015.12

[76] Mahmoud, Chaira, and Sofiane Aouag. "Security for internet of things: A state of the art on existing protocols and open research issues." In *Proceedings of the 9th international conference on information systems and technologies*, pp. 1-6. 2019. https://doi.org/10.1145/3361570.3361622

[77] Ahsan, Talha, Farrukh Zeeshan khan, Zeshan Iqbal, Muneer Ahmed, Roobaea Alroobaea, Abdullah M. Baqasah, Ihsan Ali, and Muhammad Ahsan Raza. "IoT devices, user authentication, and data management in a secure, validated manner through the blockchain system." *Wireless Communications and Mobile Computing* 2022 (2022): 1-13. https://doi.org/10.1155/2022/8570064

[78] Ziegeldorf, Jan Henrik, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: threats and challenges." *Security and Communication Networks* 7, no. 12 (2014): 2728-2742. https://doi.org/10.1002/sec.795

[79] Al-Kashoash, Hayder AA, and Andrew H. Kemp. "Comparison of 6LoWPAN and LPWAN for the Internet of Things." *Australian Journal of Electrical and Electronics Engineering* 13, no. 4 (2016): 268-274. https://doi.org/10.1080/1448837X.2017.1409920