2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA),Tripoli, Libya, 19-21 May 2024.

6LoWPAN - Technical Features and Challenges in IoT: A Review

Albahlool M Abood
Faculty of Information Technology
Gharyan University
Gharyan, Libya
Albahlool.abood@gu.edu.ly

Walid K Hasan
Libyan National Authority for Scientific Research
Tripoli, Libya
w.hassan@nu.edu.ly

Haitham Khaled
School of Engineering
Edith Cowan University
Perth, Australia
h.khaled@ecu.edu.au

***Abstract*— The phrase "Internet of Things" (IoT) has been considered the next great prospect and a test for the Internet engineering community, technology users, society, and enterprises. The billions of physical devices are currently online, collecting and exchanging data globally. Anything as little as a pill or as large as an airliner can be made into a component of the IoT because of the development of affordable computer chips and the expansion of wireless networks. Devices that would otherwise be dumb are given a level of digital intelligence by connecting all these various components and attaching sensors to them, allowing them to communicate data in real time without human interaction. The difficulty of choosing the best wireless low-power area networks for IoT applications arises from the exponential expansion of wireless technologies connecting to the IoT. Therefore, this review investigates the importance of 6LoWPAN as a foundation for the IoT's future and reviews the history that led to IoT and the advantages of using 6LoWPAN-based IP networks. We also discuss the popular implementation and challenges of 6LoWPAN.**

Keywords—adaptation layer, fragmentation, header compression, IoT, IPV6, ML

I. INTRODUCTION

The IoT has emerged as a revolutionary force in today's era. It is characterized as a device that facilitates communication between objects [1]. IoT networks make use of small-sized and low-cost devices to interconnect and link billions of heterogeneous devices. It is expected that the majority of interconnected devices in the IoT will be low power and exhibit varying levels of complexity [2]. Due to the rapid expansion and integration of wireless technologies with IoT, selecting the appropriate wireless communication technology is a significant challenge. As a result of the proliferation of wireless communication standards in the market, different protocols and frequencies are used [3]. Wireless sensor networks (WSNs) have become increasingly important on the IoT [4]. An autonomous, battery powered WSN detects and monitors its surroundings. A variety of parameters could be captured, including motion, sound, temperature, vibration, and air quality. Protocols are being analysed and new ones are being developed to meet the growing demand for applications [5]. In addition to IEEE 802.15.4 for the physical and data link layers, RPL (IPv6 Routing Protocol for Low Power) for the network layer, and COAP for the application layer, the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE) have also developed several protocols. Network architecture depends heavily on routing, which determines routing decisions. Waste of network resources can result from incorrect decisions.

It is anticipated that the Internet of Everything (IoE) will supplant the IoT in the coming years . Each device within a network must possess its own unique Internet Protocol (IP) address to facilitate communication with other devices in the network.

Routing plays a crucial role in network architecture as it makes routing decisions. Incorrect decisions can waste network resources. It is expected that the IoE will replace the IoT in the coming years. Each device within a network must possess its own unique IP address to communicate with other devices within the network [6].

The most recommended solution to address this challenge is the adoption of IPv6 addressing, which provides a staggering 2^128 possible node or address combinations. The transmission of IPv6 packets over the Low Power Wireless Personal Area Network is abbreviated as 6LoWPAN, which is an IP IoT network designed specifically for low-rate, low-power WPANs using IPV6 Over IEEE 802.15.4 Networks.

There is a significant amount of effort being made by researchers to accommodate the demands of IoT applications and address the challenges presented by network devices used in IoT, such as power limitations, limited memory, and processing capabilities. Authors in [7] conducted a survey that primarily delved into network design (ND) techniques and header compression (HC) techniques within compressed Datagram Transport Layer Security (DTLS) in 6LoWPAN.the review in [8] offers a thorough analysis of attacks on the Routing Protocol for Low-Power and Lossy Networks (RPL) along with existing defense strategies. It also explores ongoing research challenges and suggests future directions to enhance RPL security. More recently authors in [9] conducts a research analysis of 6LoWPAN within the (IoT) domain over the past four years. It comprehensively assesses the system architecture, system components, and monitoring parameters of 6LoWPAN across various application scenarios. Another systematic literature review in [10] examines the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) and its security threats. It organizes relevant Intrusion Detection System (IDS) methods and highlights the need for further research in specific areas. Another systematic review in [11] presents a Machine Learning (ML) framework designed to enhance RPL functionalities within IoT-based networks. The review conducted in the paper highlights the potential of ML techniques in improving LLN performance by optimizing key parameters. This study has, however, made the following key contributions:

- We introduce a detailed and up-to-date study of the relevant aspects of previous research.
- We clarify essential concepts about 6LoWPAN and its impact of the 6LoWPAN efficiency. .

The reminders of this paper will be organized as follows: The semantics of 6LOWPAN will be explained in Section II. Section III describes the Architecture of 6LoWPAN.Section IV presents 6LOWPAN Protocol Stack, Fragmentation,

979-8-3503-7262-5/24/$31.00 ©2024 IEEE

Packet Reassembly, and Header Compression. Section V illustrates implementation and cachallenges of 6LoWPAN . Finally, Section VI provides the conclusion of this paper, along with a discussion on prospective avenues for future research.

II. OVERVIEW OF 6LOWPAN

In 2011, the Request for Comments (RFC) 6282 defined the open standard known as 6LoWPAN, which stands for "Compression format for IPv6 datagrams over IEEE 802.15.4 based networks." The aim of the IEFT working group that developed 6LoWPAN was to merge two distinct networks: IPv6 networks and the IEEE 802.15.4 link layer, resulting in IPv6 over Low Power Wireless Personal Networks .

The IEEE 802.154 standard, issued by the IEEE, defines the PHY and Media Access Control (MAC) layers for wireless communication. This wireless communication protocol was designed with low power consumption in mind and is suitable for applications that involve many nodes, most of which may run for years on battery power. To achieve low power consumption and minimize the Bit Error Rate (BER), smaller-sized packets must be broadcast over the air, which is one of its distinctive characteristics [13] . Depending on the security options and addressing type, the payload can reach a maximum of 127 bytes and 88 bytes at the PHY layer and the MAC layer, as depicted in Figure 1.

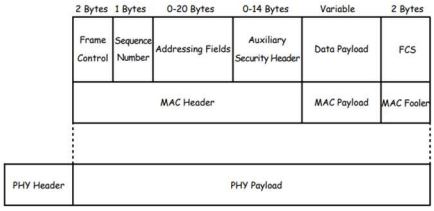

Fig. 1. 802.15.4 PHY and MAC Payloads

An analogy of 6LoWPAN is described as follows:

- Six (6); This refers to Internet Protocol (IP) version 6, the latest iteration of Internet protocols. IPv6 enables the identification of devices on the Internet for locating purposes. IP addresses are assigned to each Internet-connected device. IPV4 used a 32-bit address scheme, which could accommodate over 4.3 billion devices. However, due to the growth and development of IoT networks, the need for a significant number of devices to interact in the physical world, and the increase in users, computers, and mobile phones, there is a pressing need for more addresses. As a result of using 128 bits, IPv6 is able to accommodate approximately 340 trillion addresses. It is expected that this vast number will cover all nodes that will be part of the Internet of Things, as well as any future services that may require an IP address [12].
- Lo means low energy. IP connections are commonly vulnerable to conflicts and exhibit low power consumption. IPv4 was originally intended to serve as a standard for communication among universities rather than a global communication standard for billions of individuals when it was introduced in 1981. Furthermore, environmental consciousness was not as widespread three decades ago. In today's world, energy conservation is an important part of our daily routines, as we strive to reduce our impact on the environment [13]. Furthermore, wireless sensors heavily rely on battery power, necessitating the implementation of energy-saving practices to ensure their optimal functionality.
- With the proliferation of technology, energy costs have increased, prompting consumers to seek ways to reduce or control their energy consumption. The Internet of Things (IoT) has presented sophisticated methodologies for analysing, monitoring, and enhancing energy consumption at both the individual device and distribution network scales. 6LoWPAN offers energy savings as the energy overhead ranges from 2.8% for small data payloads of less than 10 bytes to under 2% for payloads close to frame capacity. Additionally, 6LoWPAN consumes minimal power as it leverages the current IP network infrastructure without the need for unique packet translation gateways or proxies [13].
- WPAN stands for Wireless Personal Area Networks. A Personal Area Network (PAN) is a group of interconnected devices cantered around an individual's workspace, linked together through a wireless medium, commonly known as short-range wireless connectivity. The range of a PAN typically spans from a few centimetres to a few meters. Wireless PANs (WPANs) are predominantly used for day-to-day applications and employ close-range wireless connectivity protocols like Bluetooth, primarily for connecting computer accessories or audio equipment, such as headsets or hands-free kits.

6LoWPAN enhances WPAN technology by facilitating the development of more extensive and interconnected networks. This technology enables improved building coverage through the utilization of 868/915 MHz frequency bands instead of the conventional 2400 MHz band. IoT involves local edge devices, often in the form of sensors, that collect data and transmit it to a central data centre or "the cloud" for processing. Using the standard IP protocol stack will facilitate communication and data transmission to the cloud. This objective can be achieved by adopting either the "cloud model," which involves directly connecting edge devices to data centres through the Internet, or the "fog model" .In the fog model, data from edge devices is routed to a collection point, commonly referred to as a border gateway, where it is then forwarded to the designated data centre [14]. Figure 2 illustrates this process.

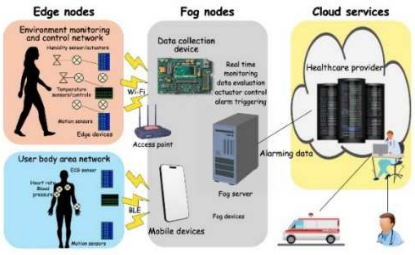

Fig. 2. Edge-to-Cloud Architecture Layers

One advantage of IP-based IoT is that it only requires an IP layer gateway, which makes it more flexible and lightweight. Additionally, because of the success of the IP, applications that use proven and existing protocol

applications can be reused in an IP IoT network, significantly reducing development time. However, the disadvantage of an IP IoT network is that TCP/IP is a relatively complex protocol suite compared to simpler IoT network protocols such as ZigBee, making it challenging to implement on constrained nodes. Nevertheless, with advancements in hardware, processing power has become more affordable, even for constrained devices, making IP IoT networks more reliable. LoWPAN is a network that runs IPv6 over IEEE 802.15.4 networks. The data transmission range of a packet in LoWPAN is small, ranging from 10m to 30m, with a transmission rate of 20 kbps to 240 kbps. Moreover, the memory of constrained devices is limited to 128 kb ROM and 16 kb RAM [15].

III. ARCHITECTURE OF 6LOWPAN

There are three types of LoWPANs: Adhoc LoWPANs, Simple LoWPANs, and Extended LoWPANs. Simple LoWPANs are connected to an IP network through a single LoWPAN edge router, while adhoc LoWPANs lack infrastructure and are not connected to the Internet. Extended LoWPANs consist of numerous edge routers and a backbone link connecting them, and the edge router's role is to direct traffic in and out of the LoWPANs. Figure 3 shows the 6LoWPAN architecture, which consists of several nodes that can function as a host or router, as well as one or more edge routers. The Neighbor Discovery (ND) is a critical term in 6LoWPAN, making it easier for nodes to register with the edge router and ensuring efficient network operation. In 6LoWPAN, the Neighbor Discovery protocol is essential for managing host and router interactions on a shared link. It not only defines communication rules within the network but also facilitates node mobility across various network segments, including edge routers and other LoWPANs, thereby promoting a flexible and dynamic network infrastructure.. [15].

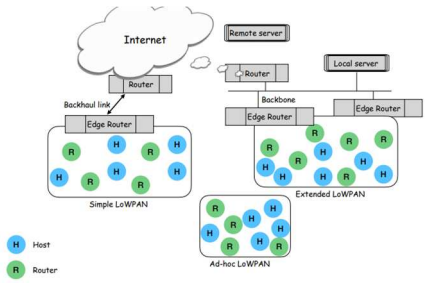

Fig. 3. Architecture of 6LoWPAN

Two types of network nodes are defined in IEEE 802.15.4: Reduced Function Devices (RFD) and Full Function Devices (FFD). FFDs have the capability to communicate with other FFDs or RFDs and can establish their networks. However, RFDs can only communicate with other RFDs. As shown in Figure 4, this hierarchy leads to a variety of topologies, including peer-to-peer meshes and star topologies.

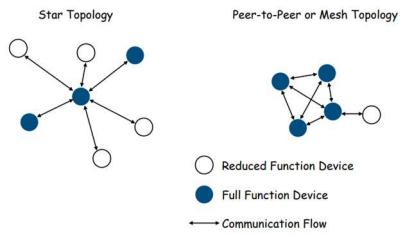

Fig. 4. IEEE 802.15.4 Network nodes

The star topology, with only one FFD needed, is the simplest and most cost-effective option. RFDs or FFDs can be used for the remaining devices, depending on implementation. However, The single-point dependency in star topology elevates the risk of network failure, limiting its suitability for multifaceted systems. Conversely, mesh topology, through its redundant communication routes, significantly enhances system reliability and message transmission efficiency. Additionally, its self-organizing feature in ad hoc settings reinforces its resilience and flexibility in evolving network landscapes. Therefore, connectivity can be maintained even when radio frequency propagation characteristics such as multipath change. The mesh topology is suitable for mobile nodes, as found in industrial robots [15].

IV. 6LOWPAN PROTOCOL STACK

The 6LoWPAN network allows wireless sensor nodes (WSN) to communicate over IP. However, there may be functional incompatibility issues between them. Two approaches were proposed to address this problem. The first approach involves modifying the existing layers of the TCP/IP protocol stack. The second approach involves adding a layer to the TCP/IP protocol stack without affecting the existing layers' functionality. The second approach was found to be more effective since it did not impact the current TCP/IP layer architecture. This additional layer is known as the adaptation layer and is required because using IPv6 for packet transfer over LoWPAN is not a natural fit. Therefore, the IETF recommends an adaptation layer to make IPv6 and 802.15.4 compatible [16]. In the 6LoWPAN protocol stack, this layer is located between the network layer and the data link layer, as shown in Figure 5.

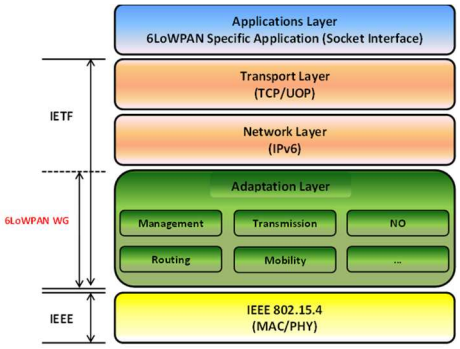

Fig. 5. 6lowpan adaptation layer

The adaptation layer in the 6LoWPAN protocol stack serves three primary functions, as well as several other networking-related tasks. The first two primary functions are header compression and decompression. This layer compresses the IPv6 and UDP headers using various methods that have been proposed. The second primary function is packet fragmentation and reassembly. The adaptation layer is responsible for breaking up large packets into smaller ones for transmission over the network and then reassembling them at the receiving end.

The third essential function of the adaptation layer is routing. Although routing is typically considered the network layer's primary function, the adaptation layer can also manage it. Mesh under routing refers to routing decisions made at the adaptation layer, while route over routing refers to routing decisions made at the network layer. The WSN border nodes

should be able to route internal traffic to external IP networks and IPv6 packets into the WSN nodes from the outside [16].

A. Fragmentation & Reassembly of packets

While the allowed packet size for 802.15.4 is just 127 bytes, the maximum transmission unit (MTU) for IPv6 packets is 1280 bytes. IPv6 packets must be fragmented to support 802.15.4 MTU to be transported over it in 6LoWPAN. Therefore, to encapsulate IPv6 large-sized packets onto 802.15.4, they must be divided, sent, and put back together once they have arrived at their destination. When the IPv6 packet size is larger than the maximum link-layer payload size, the 6LoWPAN fragmentation mechanism kicks in at the sender node. It will iteratively divide the IPv6 packet's single data field into smaller pieces. The maximum frame size at the data link layer will determine the size of the fragments. Before being transmitted, each fragment will then contain a fragment header. The adaptation layer is responsible for segmenting and reassembling packets. The adaption layer receives packets from the source node's network layer and determines their size. A larger packet will be fragmented and forwarded to the MAC layer Each fragment is delivered with a fragment header, as seen in Fig. 6. Three fields are present in the fragment header: (Datagram Size, Datagram Tag, and Datagram Offset) [10].

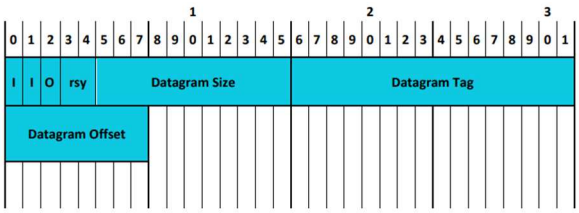

Fig. 6. 6LoWPAN Fragment Header.

Datagram Size, which is given with every fragment to make buffer allocation at the receiver easier when pieces come out of order, specifies the total size of the unfragmented payload. When matching up fragments of the same payload, Datagram Tag identifies the fragments corresponding to a specific payload. Offset is a value produced during the PDU payload segmentation process. This value specifies the relative position of a specified fragment concerning the rest of the fragments within the original payload. The offset value is necessary to complete the reassembly process. Without it, the parts cannot be reassembled in the correct order to reproduce the original fragmented PDU [8].

B. Header Compression

A significant reduction in the size of the IPv6 header is essential for the effective transmission of data using 6LoWPAN, especially when employing IEEE 802.15.4 or other 6Lo technologies. This is because the standard 40-byte IPv6 header can consume a substantial portion of the frame payload and valuable energy and bandwidth resources. To address this concern, a lightweight encoding technique for the IPv6 header was developed using 6LoWPAN HC, primarily for IEEE 802.15.4. The approach employs both stateless and stateful compression methods. The stateless approach utilizes various IPv6 header fields, such as IIDs and datagram length, which can be derived from the link layer header. The stateful method, on the other hand, assumes that some IPv6 header fields have default values. In addition, 6LoWPAN HC necessitates nodes to share context, which enables address prefixes or complete addresses to be replaced by short identifiers. Although each technology has unique features that require adaptation, 6LoWPAN HC has served as the basis for header compression in all 6Lo technologies [9]. Figure 7 provides an example of 6LoWPAN operation.

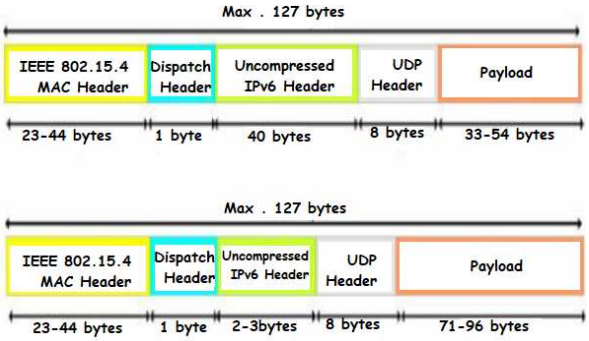

Fig.7. 6LoWPAN frames without and with Ipv6 header compression.

The maximum transmission unit (MTU) for packets in 6LoWPAN is 127 bytes. Alternatively, IPv6 packets can contain 1280 bytes. According to 802.15.4's frame format (shown in Figure 8), the link layer header is assigned 23 bytes, the security header is assigned 21 bytes, the fragment header is allocated 5 bytes, and the footer is allocated 2 bytes. Therefore, only 76 bytes are available for upper-layer headers and payloads. When transmitting an IPv6 packet via TCP, one only has 16 bytes remaining for the payload due to the header lengths of IPv6, TCP, and UDP. As shown in Figure 5, UDP only provides 28 bytes for the payload. To increase the capacity of payload transmission, it is necessary to use techniques that compress IPv6, UDP, and TCP headers. In the context of 6LoWPAN, UDP is preferred over TCP due to its simpler and smaller header. Moreover, 6LoWPAN is commonly used in applications that require real-time data transmission, making connection-oriented protocols less desirable and UDP more suitable [10].

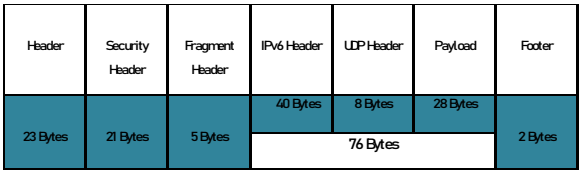

Fig. 8. 802.15.4 Frame Format

V. 6LOWPAN IMPLEMENTATIONS AND CHALLENGES

A. 6LOWPAN Implementations

6LoWPAN has many open-source and commercial implementation. Thread, Contiki OS, TinyOS, and Open thread are the most well-liked. Many different hardware platforms and architectures have had them ported. Here is a list of some recent 6LoWPAN Applications.

1) Thread: Thread is an open IoT protocol collaboratively developed by entities including Google and Samsung, grounded in the 6LoWPAN architecture. It is designed as a low-power, wireless device-to-device communication standard, emphasizing reliability and cost-efficiency. The Thread Specification is particularly tailored for Connected Home applications that prioritize IP-based networking. Key attributes of Thread include its open-standard framework, energy efficiency, and suitability for home-based IoT implementations:

a) Simplicity: Easy setup, operation, and installation.

b) Scalability: Thread networks can support up to hundreds of devices.

c) Reliability: To ensure reliability, spread-spectrum techniques, and self-healing mesh networking with no single point of failure are used. Low-power efficiency, Thread gadgets have long battery life and can sleep.

d) Security: In a Thread network, every device is authenticated, and all communications are encrypted.

Nest released an open-source thread implementation called Open ich [17].

2) Contiki: Contiki is a lightweight, open-source operating system that supports 6LoWPAN and is licensed under BSD. It can operate on nodes with highly restricted resources and IEEE 802.15.4 wireless communication capabilities, with as little as 20 KB RAM and 100 KB ROM. Contiki is coded in C and has been adapted to several hardware platforms, including those utilizing Atmel AVR, MSP430, and ARM Cortex-M3 architectures. By turning off wireless transceivers for up to 99% of the time, Contiki achieves low power consumption. Cooja, a network simulator, is also included in Contiki.

3) TinyOS: An open-source operating system with LGPLv2 licensing that was created expressly for the Internet of Things.

4) RIOT: An open-source operating system with LGPLv2 licensing that was created expressly for the Internet of Things. RIOT uses a microkernel architecture, supports standard C and C++ programming, offers real-time capabilities as well as multithreading, and only requires a minimum of 1.5 KB of RAM [18].

5) OpenWSN: UC Berkeley has pioneered the creation of an open-source Internet of Things (IoT) operating system, namely OpenWSN. The primary goal of the OpenWSN project is to provide freely available and open-source implementations of a comprehensive protocol stack, adhering to IoT standards, for utilization on diverse computer hardware and software platforms. OpenWSN is fully compatible with 6LoWPAN and CoAP protocols and enjoys extensive support from a wide range of motes, including the OpenMote.

6) Zephyr: WindRiver System created a new IoT operating system called Zephyr. The Apache 2.0 license governs Zephyr, which is open source. The Zephyr kernel is compatible with various architectures, including RISC-V 32, ARC, Intel x86, Tensilica Xtensa, NIOS II, and ARM Cortex-M. Zephyr supports multithreading and includes POSIX threads compatible API support. Zephyr supports 6LoWPAN with its IP networking stack.

7) Mbed OS: Mbed OS, specifically designed for internet-connected devices, is built upon 32-bit ARM Cortex-M microcontrollers. Developed collaboratively by ARM and its partners, Mbed OS not only provides native support for 6LoWPAN but is also a certified Thread component. This certification as a Thread Certified Component signifies its full compliance with the Thread specification, reinforcing its suitability for advanced connected systems [19].

B. Challeneges of 6LOWPAN

The creation and implementation of 6LoWPAN face various challenges, particularly due to the constrained resources such as processing power, memory, and energy, in the IPv6 nodes. For instance, 6LoWPAN's link layer only supports an MTU of 127 bytes, compared to IPv6's minimum MTU of 1280 bytes with a 40-byte header. Thus, the transmission of standard IPv6 packets through IEEE 802.15.4 is inefficient, requiring frequent fragmentation and defragmentation, and resulting in a high header/payload ratio [20].

To address these challenges, the 6LoWPAN Task Group is exploring different areas, such as Secure Neighbour Discovery, Service Discovery, and Neighbour Discovery, to locate IPv6 network prefixes, local routers, and other network configuration parameters. Security is also a significant concern, but commonly used security measures such as IPSec and TLS require more resources than what IoT devices can provide [21].

In addition, the design of routing protocols is a significant challenge due to the unreliable nature of lossy networks caused by factors such as mobility and interference. Most routing protocols rely on a relatively stable and slowly changing network topology, which is not feasible in such networks . One possible solution is to use the Representational State Transfer (REST) architecture based on HTTP, which has become popular in web services due to its ability to reduce latency and network communication while increasing component independence and scalability [22]. As many RESTful web services are based on HTTP, it is an attractive option for 6LoWPAN applications. However, standard HTTP and TCP may be too complex and resource intensive for the restricted networks that 6LoWPAN operates on.

I. CONCLUSION AND FUTRE WORK

Although 6LoWPAN may not be as well-known as other wireless standards like Zigbee, its use of IPv6 gives it a clear advantage. As the world moves toward packet data, technologies like 6LoWPAN offer several benefits for low-power wireless sensor networks. End users stand to benefit the most from this competition. In contrast, competing technologies like ZigBee and Z-Wave, which seek to exchange wireless remote-controlled objects for smart homes, may struggle to keep up.

This paper's primary focus is on the meaning of 6LoWPAN, including a survey of its architecture, different classes, and disparities between them in terms of infrastructure and network nodes. It also explains how each class works and outlines options used to make 6LoWPAN compliant with IP communications while ensuring compatibility with the existing TCP/IP layer architecture. Header compression techniques have the potential to substantially decrease the size of the IPv6 header, thereby enabling a larger allocation of bytes for transporting the payload in 6LoWPAN. In all these techniques, link-local addresses can be completely excluded as they can be derived from the link layer header.

Further studies will focus on developing routing protocols, addressing the energy drain problem, improving. Routing performance and enhancing 6LoWPAN's security. While 6LoWPAN offers significant benefits and opportunities performance and enhancing 6LoWPAN's security. While 6LoWPAN offers significant benefits and opportunities

transporting the payload in 6LoWPAN, researchers must carefully consider and address the identified challenges to achieve further improvements in the future. Routing performance and enhancing 6LoWPAN's security.

ACKNOWLEDGMENT

The authors express profound appreciation to Miss. Somaia Almalloshi for her indispensable support in the creation of the figures for this paper. Her exceptional skills and commitment have greatly enhanced the quality of this work.

REFERENCES

[1] W. K. A. Hasan, Y. Ran, J. Agbinya, and G. Tian, "A Survey of Energy Efficient IoT Network in Cloud Environment," in 2019 Cybersecurity and Cyberforensics Conference (CCC), 8-9 May 2019 2019, pp. 13-21, doi: 10.1109/CCC.2019.00-15.

[2] W. K. A. Hasan, A. Alraddad, A. Ashour, Y. Ran, M. A. Alkelsh, and R. A. M. Ajele, "Design and Implementation Smart Transformer based on IoT," in 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 22-23 Aug. 2019 2019, pp. 16-21, doi: 10.1109/iCCECE46942.2019.8941980.

[3] W. K. A. Hasan, A. M. Abood, and M. Habbal, "A Review of Blockchain-based on IoT applications (challenges and future research directions)," in 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), 25-27 Nov. 2020 2020, pp. 1-7, doi: 10.1109/CITISIA50690.2020.9371814.

[4] O. A. Zargelin, F. M. Lashhab, and W. K. Hasan, "Localization Methods based on Error Analysis and Modeling in Two Dimensions," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020: IEEE, pp. 0690-0699.

[5] O. A. Zargelin, F. M. Lashhab, and W. K. Hasan, "Localization Methods based on Error Analysis and Modeling in One Dimension," in 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020: IEEE, pp. 0674-0683.

[6] M. Al-Fawa'reh, J. Abu-Khalaf, P. Szewczyk, and J. J. Kang, "MalBoT-DRL: Malware Botnet Detection Using Deep Reinforcement Learning in IoT Networks," IEEE Internet of Things Journal, 2023.

[7] H. Shah, R. Shrimali, and V. Parikh, "Header Compression and Neighbor Discovery in 6LoWPAN based IoT - a survey," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 23-25 March 2016 2016, pp. 306-311, doi: 10.1109/WiSPNET.2016.7566144.

[8] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," IEEE Sensors Journal, vol. 20, no. 11, pp. 5666-5690, 2020, doi: 10.1109/JSEN.2020.2973677.

[9] L. Zhao and G. Wang, "Research Status of 6LoWPAN in the Field of Internet of Things," in 2020 5th International Conference on Automation, Control and Robotics Engineering (CACRE), 19-20 Sept. 2020, 2020, pp. 739-743, doi: 10.1109/CACRE50138.2020.9230293.

[10] A. M. Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, "Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review," IEEE Sensors Journal, vol. 21, no. 11, pp. 12940-12968, 2021, doi: 10.1109/JSEN.2021.3068240.

[11] M. E. Ekpenyong, D. E. Asuquo, I. J. Udo, S. A. Robinson, and F. F. Ijebu, "IPv6 Routing Protocol Enhancements over Low-power and Lossy Networks for IoT Applications: A Systematic Review," New Review of Information Networking, vol. 27, no. 1, pp. 30-68, 2022/01/02 2022, doi: 10.1080/13614576.2022.2078396.

[12] R. Garg and S. Sharma, "Comparative study on techniques of IPv6 header compression in 6LoWPAN," in Proc. of the Intl. Conference on Advances in Information Processing and Communication Technology-IPCT, 2016, pp. 34-38.

[13] Z. Yang and C. H. Chang, "6LoWPAN Overview and Implementations," in EWSN, 2019, pp. 357-361.

[14] S. M. Kumar and D. Majumder, "Healthcare solution based on machine learning applications in IOT and edge computing," International Journal of Pure and Applied Mathematics, vol. 119, no. 16, pp. 1473-1484, 2018.

[15] G. Mulligan, "The 6LoWPAN architecture," in Proceedings of the 4th workshop on Embedded networked sensors, 2007, pp. 78-82.

[16] C. Yibo et al., "6LoWPAN stacks: A survey," in 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, 2011: IEEE, pp. 1-4.

[17] A. Ortega i Blasi, "Evaluating Thread protocol in the framework of Matter," Universitat Politècnica de Catalunya, 2022.

[18] M. A. Elsadig, A. Altigani, and M. A. Baraka, "Security issues and challenges on wireless sensor networks," Int. J. Adv. Trends Comput. Sci. Eng, vol. 8, no. 4, pp. 1551-1559, 2019.

[19] M. H. Qutqut, A. Al-Sakran, F. Almasalha, and H. S. Hassanein, "A Comprehensive Survey of the Internet of Things Open Source Operating Systems."

[20] A. J. Albarakati, J. Qayyum, and K. A. Fakeeh, "A survey on 6LowPAN & its future research challenges," International Journal of Computer Science and Mobile Computing, vol. 3, no. 10, pp. 558-570, 2014.

[21] M. A. Seliem, K. M. Elsayed, and A. Khattab, "Optimized neighbor discovery for 6LoWPANs: Implementation and performance evaluation," Computer Communications, vol. 112, pp. 73-92, 2017.

[22] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, "From 6LoWPAN to 6Lo: Expanding the universe of IPv6-supported technologies for the Internet of Things," IEEE Communications Magazine, vol. 55, no. 12, pp. 148-155, 2017.