Analysis of the Lora Wan structure and advantages of it over traditional iot networks

Jafarov N., Nasiyev M.

Abstract

In this article, we discuss traditional iot networks, the technologies behind them, and their structure. Our main goal here is to focus on Lora wireless technologies and explore their advantages and application areas. A detailed structural overview of Lora WAN networks is provided, and comparisons are made with traditional networks. Key elements of the system, such asLora nodes and gateways, were examined, and we provided the best possible connection diagrams throughout the material. Network bandwidth, security, energy efficiency, cost, and transmission speed characteristics of LPWAN were also analyzed. Range, transfer speed, topology, and band comparisons of Lora technology with Bluetooth Low Energy, Wi-Fi, LTE networks, Z-Wave, and zigbee were shown. We describe the Lora hardware structure, including the physical, MAC, and application layers, and provide a diagram that demonstrates the communication process. Although the Lora WAN protocol needs to be developed in terms of security, we foresee that it will continue to become widespread and that its place in our lives will gradually increase. According to the research conducted by multiple tests, the Lora WAN protocol is not yet fully secure and can be risky when sending critical information and using it in critical systems, but the risk of these vulnerabilities and attacks can be reduced with the precautions and suggestions presented in this study.

Keywords: iot network, LPWAN, sensor, TCP and UDP, Lora, MAC, UM and DL.

Iot technology connects millions of devices on different platforms and with different protocols, enabling them to communicate with each other and connect them directly or indirectly tothe internet. In this way, it makes our lives easier and aims to create smart environments that facilitate and accelerate work in agriculture, industry, health, transportation, and other areas used indaily life [2]. Iot devices, which have many application areas, appear in many areas such as smart

Cities, traffic density monitoring, monitoring the lives of wild animals, and military areas, and these areas are constantly expanding. It is estimated that 25 billion devices will be connected to the internet in 2021, and the number of peer-to-peer connections will reach 12.3 billion in 2024 and decrease by 1.5 devices per person. By 2030, the number of objects connected to the Internet is expected to exceed 500 billion [1].

The working principle of the iot ecosystem is to collect, process, send data, and act according to the received command. The components it needs to do these things are generally sensors, gateways, cloud platforms, and a user interface. While sensors are used to collect data, it is the job of the embedded systems to process this data. Sensors are devices that can measure many environmental events, such as heat, light, humidity, movement, and pressure, and have the ability to display or send these data. Data measured at a sensor is sent over the network. This is where gateways are needed. Gateways provide data communication between sensors and structures, such as the cloud, where data is to be transmitted and recorded. Many sensors can be connected to a gateway [4, 8]. Data transmission can be unidirectional or bidirectional. The data from the sensors can reach the destination through the gateways, and they also receive commands through them. Structures such as the cloud are used to store and process data from objects in a database. The interface allows users to monitor and control the devices from a single center and provides them with control mechanisms over the received data.

There are many network technologies and protocols for iot devices to communicate with each other. High reliability, application configuration capabilities, device-level traffic monitoring and management, real-time data transmission with minimal latency, multi-device connection capacity, communication range, interference immunity, battery life, network capacity, and security, single and dual channel settings such as one-way communication.

Solution for harsh environments.

Our main aim is to apply iot systems in harsh environments where traditional hardware installation is both efficient and costly to install and maintain. According to our research, network structures such as LAN (local area networks), PAN (personal area networks), WAN (wide area networks), and LPWAN (low power wide area networks) are the most suitable ones for these applications. Wireless network technologies used in these applications are Bluetooth, zigbee, Wi-Fi, cellular networks (2G, 3G, 4G, and 5G), NB-iot, Sigfox, and Lora WAN [4]. These network structures and technologies have some advantages and disadvantages among themselves. Therefore, the choice of network structure and technology is important in an iot application. While smart agriculture or military-grade applications require a network structure to meet requirements such as limited battery life and long range, speed may be the top priority for a smart building application.

Considering all of these parameters, the selection of a suitable network structure for iot cities, traffic density monitoring, monitoring the lives of wild animals, and military areas, and these areas are constantly expanding. It is estimated that 25 billion devices will be connected to the internet in 2021, and the number of peer-to-peer connections will reach 12.3 billion in 2024 and decrease by 1.5 devices per person. By 2030, the number of objects connected to the Internet is expected to exceed 500 billion [1].

The working principle of the iot ecosystem is to collect, process, send data, and act according to the received command. The components it needs to do these things are generally sensors, gateways, cloud platforms, and a user interface. While sensors are used to collect data, it isthe job of the embedded systems to process this data. Sensors are devices that can measure many environmental events, such as heat, light, humidity, movement, and pressure, and have the ability todisplay or send these data. Data measured at a sensor is sent over the network. This is where gateways are needed. Gateways provide data communication between sensors and structures, such as the cloud, where data is to be transmitted and recorded. Many sensors can be connected to a gateway [4, 8]. Data transmission can be unidirectional or bidirectional. The data from the sensors can reach the destination through the gateways, and they also receive commands through them. Structures such as the cloud are used to store and process data from objects in a database. The interface allows users to monitor and control the devices from a single center and provides themwith control mechanisms over the received data.

There are many network technologies and protocols for iot devices to communicate with each other. High reliability, application configuration capabilities, device-level traffic monitoring and management, real-time data transmission with minimal latency, multi-device connection capacity, communication range, interference immunity, battery life, network capacity, and security,single and dual channel settings such as one-way communication.

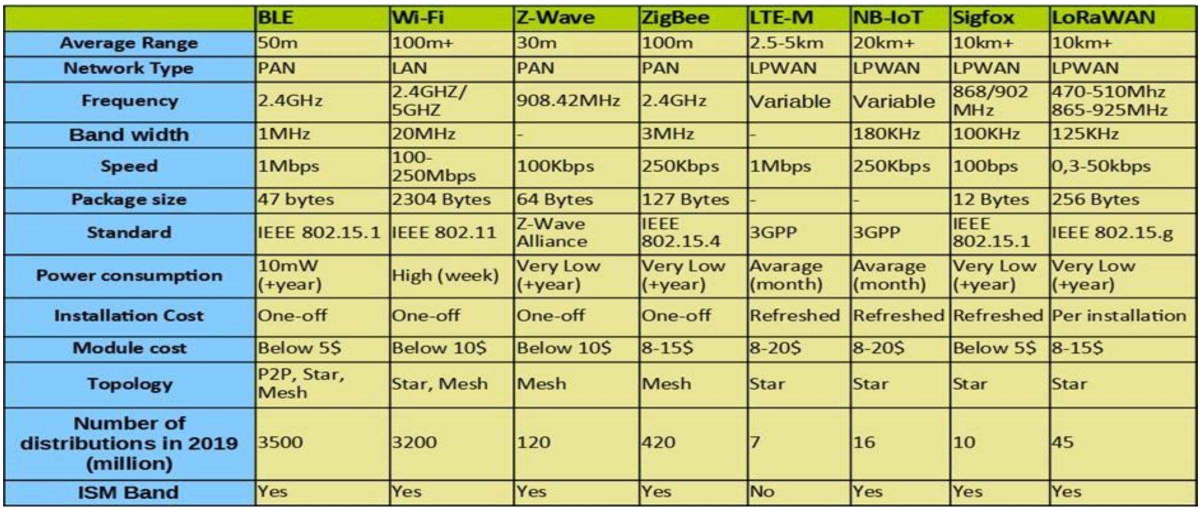
Solution for harsh environments.

Our main aim is to apply iot systems in harsh environments where traditional hardware installation is both efficient and costly to install and maintain. According to our research, network structures such as LAN (local area networks), PAN (personal area networks), WAN (wide area networks), and LPWAN (low power wide area networks) are the most suitable ones for these applications. Wireless network technologies used in these applications are Bluetooth, Zigbee, wifi,cellular networks (2G, 3G, 4G, and 5G), NB-iot, Sigfox, and lorawan [4]. These network structures and technologies have some advantages and disadvantages among themselves. Therefore, the choice of network structure and technology is important in an iot application. While smart agriculture or military-grade applications require a network structure to meet requirements such as limited battery life and long range, speed may be the top priority for a smart building application.

Considering all of these parameters, the selection of a suitable network structure for iot

Applications may vary according to the needs, taking into account factors such as low energy, long range, speed, and the size of the data packet that can be transported at once [1]. Table 1. Shows the comparison of network systems. As a result of the rapid development and spread of iot technology, some protocols were found to be limited and insufficient, and some solutions were presented for this situation. For example, due to the host size limits of the ipv4 protocol, the transition to the ipv6 protocol is required. On the other hand, the spread of these devices may result in the attention of malicious people and the increase of malicious software [8].

Table. 1. Comparison of iot Network Technologies



	BLE	Wi-Fi	Z-Wave	ZigBee	LTE-M	NB-IoT	Sigfox	LoRaWAN
Average Range	50m	100m+	30m	100m	2.5-5km	20km+	10km+	10km+
Network Type	PAN	LAN	PAN	PAN	LPWAN	LPWAN	LPWAN	LPWAN
Frequency	2.4GHz	2.4GHZ/ 5GHZ	908.42MHz	2.4GHz	Variable	Variable	868/902 MHz	470-510Mhz 865-925MHz
Band width	1MHz	20MHz	-	3MHz	-	180KHz	100KHz	125KHz
Speed	1Mbps	100-250Mbps	100Kbps	250Kbps	1Mbps	250Kbps	100bps	0,3-50kbps
Package size	47 bytes	2304 Bytes	64 Bytes	127 Bytes	-	-	12 Bytes	256 Bytes
Standard	IEEE 802.15.1	IEEE 802.11	Z-Wave Alliance	IEEE 802.15.4	3GPP	3GPP	IEEE 802.15.1	IEEE 802.15.g
Power consumption	10mW (+year)	High (week)	Very Low (+year)	Very Low (+year)	Avarage (month)	Avarage (month)	Very Low (+year)	Very Low (+year)
Installation Cost	One-off	One-off	One-off	One-off	Refreshed	Refreshed	Refreshed	Per installation
Module cost	Below 5$	Below 10$	Below 10$	8-15$	8-20$	8-20$	Below 5$	8-15$
Topology	P2P, Star, Mesh	Star, Mesh	Mesh	Mesh	Star	Star	Star	Star
Number of distributions in 2019 (million)	3500	3200	120	420	7	16	10	45
ISM Band	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Wireless network technologies currently used in iot - LPWAN (Low Power Area Networks)

As the scope of iot applications expands, new needs continue to emerge. As the distances between the sensors increase in an iot application, some difficulties arise, and the need for new communication technologies and sensors that can transmit data with low power consumption over long distances is increasing. LPWAN, which was developed to fill this gap, is a wireless communication protocol [7]. Another factor that distinguishes LPWAN technologies, which enablebattery-powered and low-power consumption-oriented iot sensors to send small-sized data packetsover long-range distances, is that these sensors make them work with a single battery for a long time with power optimization techniques [8]. Therefore, large iot networks can be established economically without the need for cellular connections and operators [3].

LPWAN increases its dominance, especially in the industrial field, with its low power usage, low cost, and long range. The fact that it has a communication range of up to 40 km in rural areas and up to 5 km in urban areas, as well as a battery life of up to 10 years, explains its popularity in these areas [4]. Today, many LPWAN technologies have emerged in licensed and unlicensed frequency bands. Sigfox, Lora, and NB-iot technologies are among the leading ones. Lora technology was first developed in 2009 by France-based Cycleo. After being acquired by US-based Semtech three years later, Lora was standardized by Lora-Alliance in 2015. It is already being used and becoming widespread in 42 countries after receiving investments from various mobile operators [5]. One of the main differences between Lora and other LPWAN technologies is that Lora is resistant to the Doppler effect and multipath fading.

Lora can provide communication over long distances thanks to low data rates and radio bands below ghz. The range is often dependent on environmental conditions and obstacles. With a gateway, it can cover an entire city or an area of kilometers. Communication between end devices and gateways spans different data rates and different frequency channels. This data rate is determined by the propagation factor parameter. The propagation (also called spread factor) factor (SF) balances the message duration with the communication range, thus avoiding the communication of signals and messages with different data rates. Simultaneous communication on the same frequency channel is possible using different propagation factors (SF7–12). Lora uses unlicensed ISM bands. These are 433 mhz in Asia, 915 mhz in North America, and 868 mhz in Europe. The data rate of Lora technology is between 0.3 and 50 kbps. The maximum payload length is 243 bytes.

Lora WAN is an LPWAN protocol running at the MAC layer. Lora WAN is equivalent to the network layer and data layer of the OSI model, while Lora is equivalent to the physical layer of the OSI model. Lora WAN networks are usually set up according to star topology. In this way, the end device can be connected to one or more gateways over a Lora connection in a single hop. Gateways in Lora WAN network design are responsible for routing messages between the end devices and the network server. While the end devices can be connected to many gateways with single-hop FSK or Lora protocols, the network server and gateways are connected to each other via IP connections. Communication is provided in a two-way direction, but in messaging, communication is predominantly in the form of an uplink from the end device to the gateway [6]. In Lora WAN communication, communication can be established between end devices and gateways with different frequency channels and different propagation factors (SF). Message duration and range are effective in determining the propagation factor (SF). In addition, different propagation factors can operate simultaneously on the same channel without any problems. There is a correlation between data transmission rate, range, and propagation factor. Lora technology supports six channel propagation factors ranging from 0.3 kbps to 50 kbps. In this way, Lora WAN can use the adaptive data rate (ADR) structure it supports to change the diffusion factor of each device and adjust it to increase network capacity or battery efficiency.

Lora data transmission layers.

Lora WAN packets and messages are of two different types. One of them is the downlink (Up Link), and the other is the uplink (Down Link) message. The uplink message (UM) is the message that goes from the end device to the gateway, while the downlink message (DM) is the message that goes from the gateway to the end device. UM and DL messages are also divided into two different types. These are confirmed (confirmed) and unconfirmed (unconfirmed) messages. The difference between these two types is that while the relevant device gives feedback that the message has been received in the approved message, there is no feedback in the unconfirmed message [7]. This analogy is the same as the TCP and UDP protocols used in the OSI model.

There are two different header types in message format. These include information about payload length, forward error correction (FEC), and optionally CRC for payloads in open header types. The maximum error correction code is transmitted as 4/8. It also has its own CRC for the receiver to detect and destroy invalid headers [7, 8]. The layers have the frame structure shown in Figure 1. Lora WAN message headers have a preamble, payload header, data, and additionally a CRC.

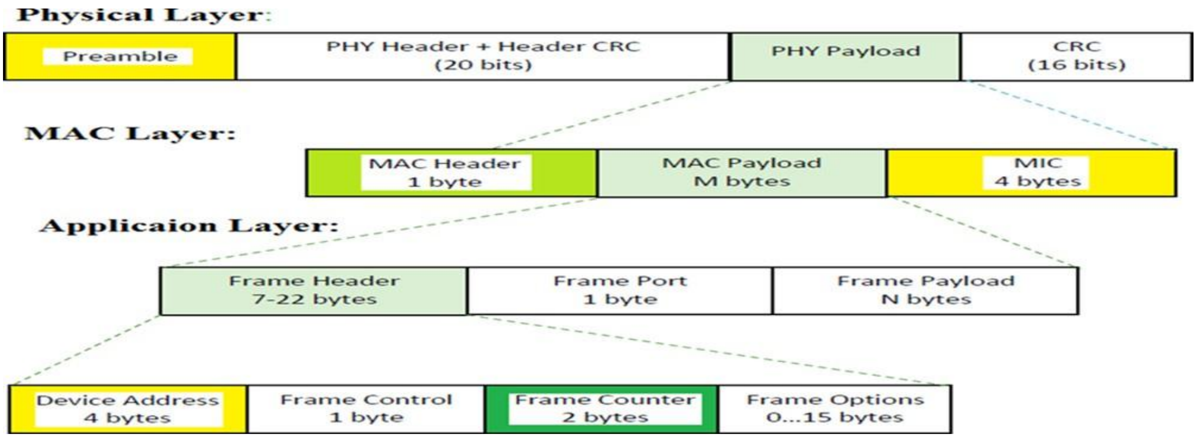


Figure 1. Lora WAN Frame Structures

Security aspects of Lora WAN

This section examines Lora WAN security. Different activation methods, key management, authentication, and activation by air (OTAA) explained. In the Lora WAN network, an end device can be connected to the network with two different activation methods. These are the activation by air (OTAA) and activation by personalization (ABP) methods. The main difference between these methods is that in the OTAA method, session keys derived after the join procedure, while in the ABP method, these keys are already present on the devices. Therefore, the generation of session keys in these two activation methods differs [6, 3].

In the OTAA activation method, the participation procedure must followed before the end device and the server can exchange data between themselves. Each time the end device loses session information, it must perform the rejoin procedure. This procedure consists of a join request and a join acceptance between the end device and the server. According to the join procedure, first the end device initiates the procedure by sending a join request message to the network server. This message contains deveui, appeui, and devnonce information stored on the end device. Appkey keys with AES-128 root keys are stored on the end device and network server. This key used between the end device and the network server, as seen in Figure 2. Before starting the activation procedure in the OTAA method, the end device must contain deveui, appeui, and appkey. EUI stands for extended unique identifier, is 64 bits long, and generally serves as an identifier for network elements. Deveui, which is the ID of the end device, is similar to the MAC address structure, while appeui, which is the ID of the application server, is similar to the port number.

The nwkskey used here is used in the calculation of the MIC value (message integrity code), which has an important place in data exchanges between the end device and the network server. In addition, nwkskey used to encrypt or decrypt the payload. Appskey, on the other hand, is responsible for ensuring the security of end-to-end communication between the end device and the application server. The payload between the end device and the application server is end-to-end encrypted, and encryption and decryption done with appskey. Another point is that there is no MIC in the data exchange between the end device and the application server, and therefore message integrity checking cannot done.

There is no participation procedure in the ABP activation method. Therefore, the end device does not have the values used in the join procedure, like appeui and appkey. In this method, instead of deriving session keys with the end device activation joining procedure, it has four personalized nwksenckey, appskey, snwksintkey, and fnwksintkey keys from the first time it opened. They are ready for direct communication through the keys they contain. Each end device has its own four session keys, so if one end device is compromised, other end devices are not affected [6].

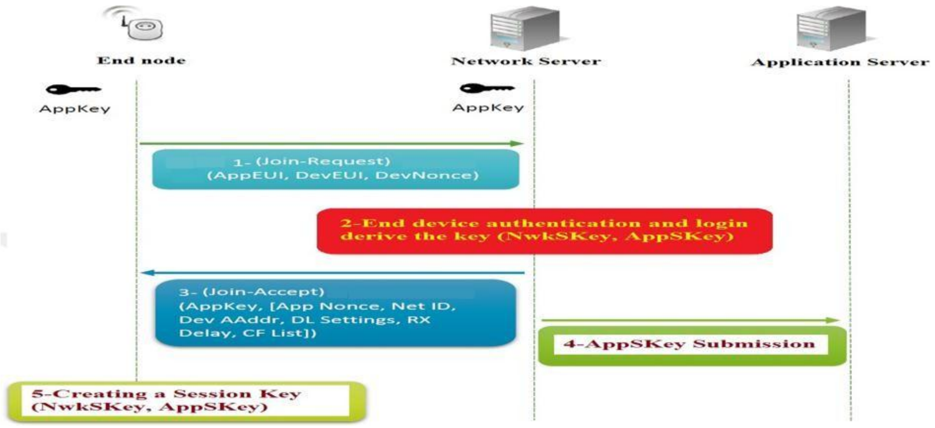


Figure 2. Key management and authentication methods

Conclusion

In this study, the lorawan protocol, which is one of the networks used in the internet of things and is discussed in this context, is examined due to its long range and low power operation, which has started to gain popularity in recent years. When the lorawan protocol security is examined, it is seen that OTAA and ABP activation methods are used to securely establish communication between the end device and the servers. Activation methods are responsible for deriving session keys used when establishing a connection to the network. If we focus on the advantages and disadvantages of these two methods, in the OTAA method, the keying process is used to transmit securely over the air between the end device and the server. It is used on both the end device and server sides, and it is used for message encryption and signing on both sides. While confirming the message through the counter used in the message acceptance procedure, it generates the key required to ensure message security with AES-128 and uses the cipher block mode for signing and encrypting the message.

References

[1] Jafarov N, Nasiyev M. Application of lora Wireless Technology in IOT Networks. Sciences of Europe, 2022, No. 108, 42–45.

[2] Jafarov N, Nasiyev M. Experimental analysis of lora/lorawan based iot networks in indoor and outdoor environments: Performance and limitations. III International Scientific Conference for

[3] Information the Systems and Technologies Achievements and Perspectives, 2022, No. 9, 273–277.

[4] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything,https://www.cisco.com/c/dam/en_us/about/ac79/docs/innoviot_IBSG_0411FINAL.pdf. Cisco, Cisco Visual Networking Index: Forecast and Trends, 2017–2022, Available: https://cyrekdigital.com/uploads/content/files/white-paper-c11-741490.pdf.

[5] K. Matthews. (2019, Nov.) 5 iot use cases that will shape the future of agriculture.

[6] A.F.Ağrak,Security analysis of lorawan wireless communication protocol and review and analysis of attacks against lorawan using iot devices.

[7] Raza, U., Kulkarni, P., and Sooriyabandara, M.(2017). Low power wide area networks: An overview. IEEE Communications Surveys&Tutorials, 19(2), 855–873.

[8] Semtech Corporation, lora and lorawan: A Technical Overview, 2019. Available: https://lora-developers.semtech.com/uploads/documents/files/lora_and_lorawan- A_Tech_Overview-Downloadable.pdf.