IOT COMMUNICATION TECHNOLOGIES

Abstract

This chapter consists about the communication of IOT devices and the connectivity of different IOT devices in the network. The IOT communication is based on a framework called open-source interconnection which is comprised of seven layers. Those are physical layer, datalink layer, network layer, transport layer, session layer, presentation layer, application layer. Further, The connectivity of IOT devices in the network with the help of different technologies. In which the technologies are established by different organizations to connect the different types of IOT devices by applying the OSI model of different layers.

Keywords: IOT devices, Communication technologies, physical layer, datalink layer, network layer, transport layer, session layer, presentation layer, application layer.

Author

Dr. A. Jency Priyadharshany
Assistant Professor
School of Commerce & Economics
Presidency University
Bengaluru, Karnataka, India.

I. INTRODUCTION

Internet of Things consists of enabled technologies. It is the Combination of hardware and software that support the device for working. IOT took his part in all the devices from medical to smartphones, watches to security cameras, cars to factory. Primarily, IOT is made up of standard protocols and networking technologies. It takes the combination of Radio Frequency Identification Device (RFID), Near Field Communication (NFC), low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and Wi-Fi-Direct. A decade before all the devices is connected with the wire and through the connection of wire the communication was made possible. Nowadays all the devices are been connected through the wireless technology. To work with that there is a framework called Open System Interconnection (OSI).

II. OSI MODEL

The OSI Framework is defined as connections and task which helps to communicate the devices with one another. Its main purpose is to assist the vendors and soft ware developers to develop an intern operable network system. Due to the wireless technology, OSI Model replaced the other communication models. OSI model is based on the technique called layering. It is partitioned into a set of vertical layers. Each layer is responsible for group of functions and dependent on each layer. It is achieved through the following:

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

1. **Physical Layer:** It is the first and lowest layer in OSI Model. The takes the responsibility to connect the devices physically. It created the actual connection between the devices. The information in the physical layer in the form of BITS which will be transmitted from one node to another node. While sending the date, the layer will work by receiving the signals and convert the information into 0s and 1s.

   - **Functions**

   - **Bit synchronization:** The physical layer allows the bits in the layer to synchronize with the clock. It helps to synchronize both the sender and receiver at the bit level.
   - **Bit rate control**: It also performs the number of bits can be sent in per second
   - **Physical topologies**: It also understand the topologies of the device arrangement and the communication systems (i.e., bus, star, or mesh topology)
   - **Transmission mode**: it will confirm which way the data flow is processed (I.e Simplex, half-duplex and full-duplex)

2. **Data Link Layer:** It is responsible for node-to-node delivery of the message. The major function of this layer is to ensure the data is transferred error free from none node to another. Bits reached the data link layer is called as Frames. Network Interface Card and other device drivers of Host Machines such as Switches and Bridges are responsible for handling the frames in the data link layer. It is divided into two sublayers. Media Access Control (MAC) and Logical Link Control (LLC). MAC referred to a Hardware physical address of unique 12- character which is distributed as alphanumeric. It is used to identify the specific electronic device. (ex: 00-B0-D0-63-C2-26). Logical Link Control helps for synchronization, flow chart & Error checking

   - **Functions**

   - **Framing**: It is a function of converting the bits into frames. The frames are consisting of special bit patterns which is having the beginning and ending.
   - **Physical addressing**: Frames adds the physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
   - **Error control:** it controls the error while transmitting the data when there are damaged or lost frames.
   - **Flow Control:** sometimes the frames may get corrupted, to control the flow between the receiver and the sender, it helps to check the amount of data to be sent.
   - **Access control**: due to different type of topologies, the MAC layers help to confirm the device in the channel to send and receive the data.

3. **Network Layer:** It ensures the transmission of data from one node to other. It also considers the selection of the path in which the data can flow from one host to the other in different networks. Frames, once it reaches the Network layer called as Packets. The IP Address plays an important role in choosing the proper route to carry the packets.

   - **Functions**

   - **Routing:** It helps to choose the suitable route from source to destination.
   - **Logical Addressing**: In order to find the network, it gives separate address scheme. It will be mentioned in the header of the network layer. Such address will help to find the unique device in the universal.

4. **Transport Layer:** The Packets in the transport layer takes a form called Segments. This layer helps to deliver the complete message by providing and acknowledgement of the data transmission completion.

   - **Functions**

   - **Segmenting**: break the message into smaller units. Each segment has a header.
   - **Service Point Addressing**: the smaller units are sent by breaking it into smaller units to the destination system by checking the service point address.

5. **Session layer:** This layer is ensuring the connection, session maintenance, authentication, and security.

   - **Functions**

   - **Session establishment, maintenance, and termination**: The layer performs two processes to establish, use and terminate a connection.
   - **Synchronization**: it also adds checkpoints to have concern on the synchronization in the data to identify the error so that the data is re-synchronized properly. By the way the messages are not cut prematurely and data loss is avoided.
   - **Dialog Controller**: It will also confirm the transmission mode.

6. **Presentation Layer:** It is also called the Translation layer. The data in this layer manipulated as per the required format to transmit over the network.

   - **Functions**

   - **Translation:** ASCII to EBCDIC.
   - **Encryption/ Decryption**: Data encryption translates the data into another form or code. The data encryption will take place in this layer as ciphertext and data decryption as plain text. A key value is been created here to encrypt and decrypt.
   - **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. **Application Layer:** The last layer of the OSI model is the Application layer implemented by the network applications. It will convert the data into the actual format which is required to be displayed. So it will be served as a window for the application services (Ex: Browsers, Skype Messenger, etc).

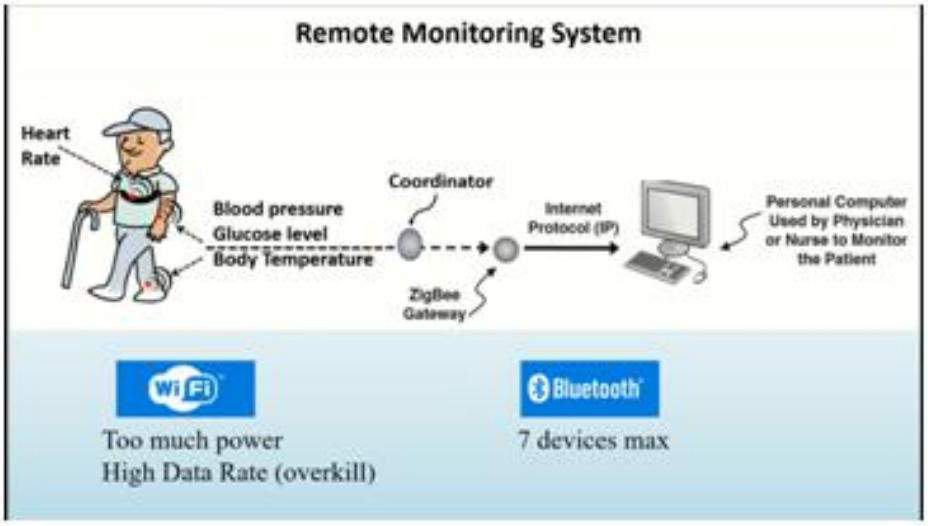
III. IOT COMMUNICATION AND TECHNOLOGIES

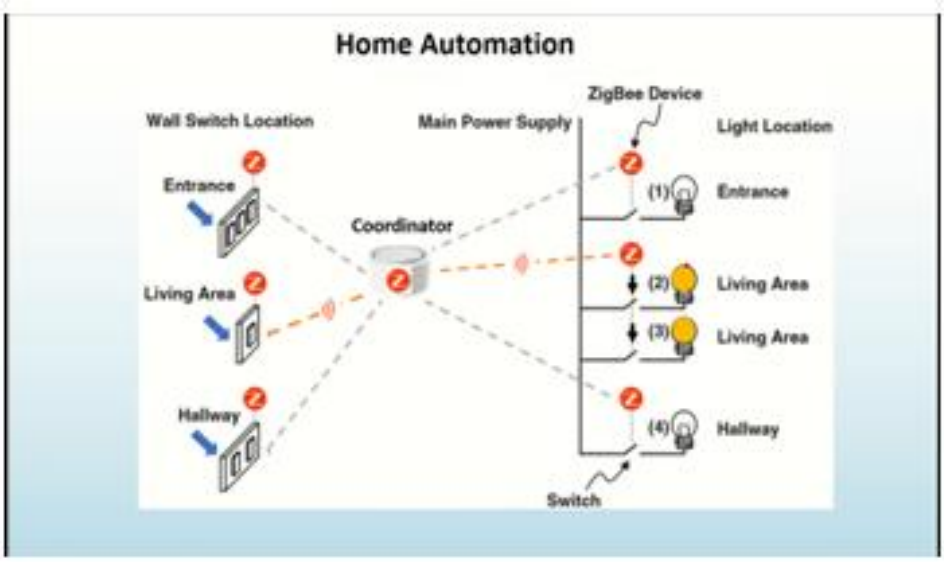
1. **Security of IEEE 802.15.4:** In the wired network, the sender and receiver have the communication through signals transmitted through wire. It will never be accessed by others. But in the wireless network, if coverage area consists of lots of devices connected, there will be possibility of the data can be accessed by others also. By controlling that the association called IEEE found a security technology called as IEEE 802.11. as like ethernet, IEEE 802.11 is designed to use in a limited geographical area. (Ex. home, office, campuses)

   It is Wireless Local Area Network Technology. It works on the principle for securing the communication called Carrier sense multiple access with collision avoidance (CSMA/CA). it cant perform the detection of collision because the signals are propagated through air. But the in the wired network, It works based on the Carrier sense multiple access with collision detection (CSMA/CD). It can easily detect the collision because the signals are propagated through wires.

   IEEE 802.11 is based on two modes.
   - Infrastructure mode (desktop-printer-server)
   - Adhoc Mode (no structure

2. **ZigBee Technology:** It's a open source standard which consists of set of communication protocols for short range only. It's a wireless technology specifically built to control and access the sensor networks. The main aim of this Zigbee technology to perform the task such as collect the information and control the devices inside the building. It was developed by a group of technologists called ZigBee Alliance in 2002. Its applications servers at home automation, Medical Data collection, Industrial Control Systems.



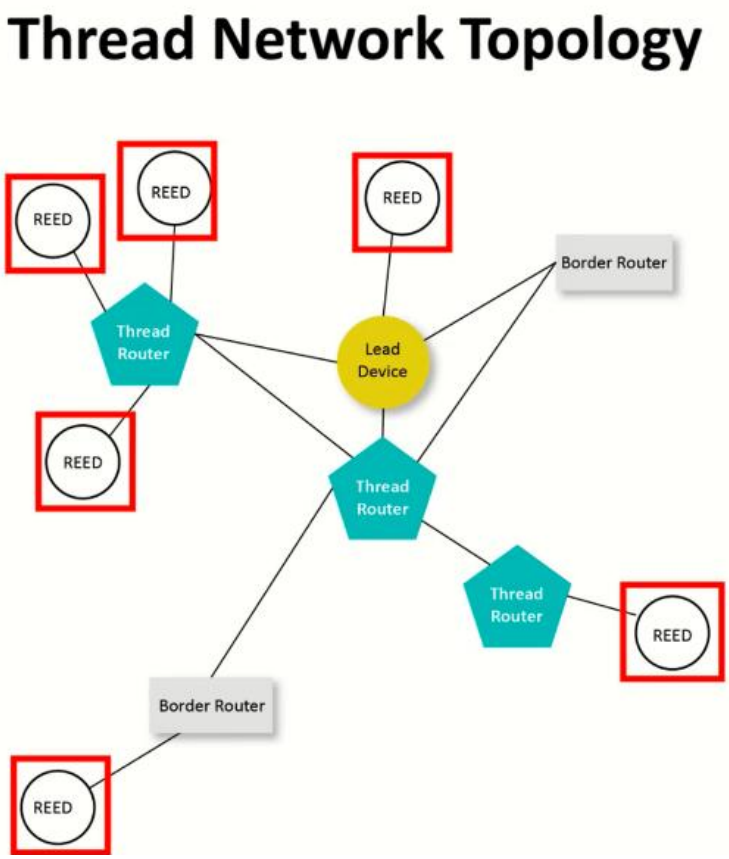


- Characteristics of ZigBee Standard

- It consumes low power to control the devices. It works for several years with a single battery.
- It consumes very less data
- It will operate in short range
- It takes very less time to get joined in the network.
- It also supports large and small networks
- It takes cheap cost for implementation

It enabled with advanced encryption standard which is an algorithm for data encryption and data authentication.

3. **Thread:** Thread is another framework developed by Thread Alliance Group in 2015. It will take the special configuration to mee the requirements of reliability, security, power efficiency and compatibility. It works on the topology called MESH where all the devices in the network are interconnected and allows self-hearing in the chances of failures. It is applicable for home appliances, climate and access control, lighting and energy management, safety and security. Thread Physical Layer of is based on IEEE 802.15.4, network layer access through the protocols such as IPv6, 6LowPAN.



Thread Architecture is consisting of Border Router, Lead Devices, Thread Routers and REED**.**

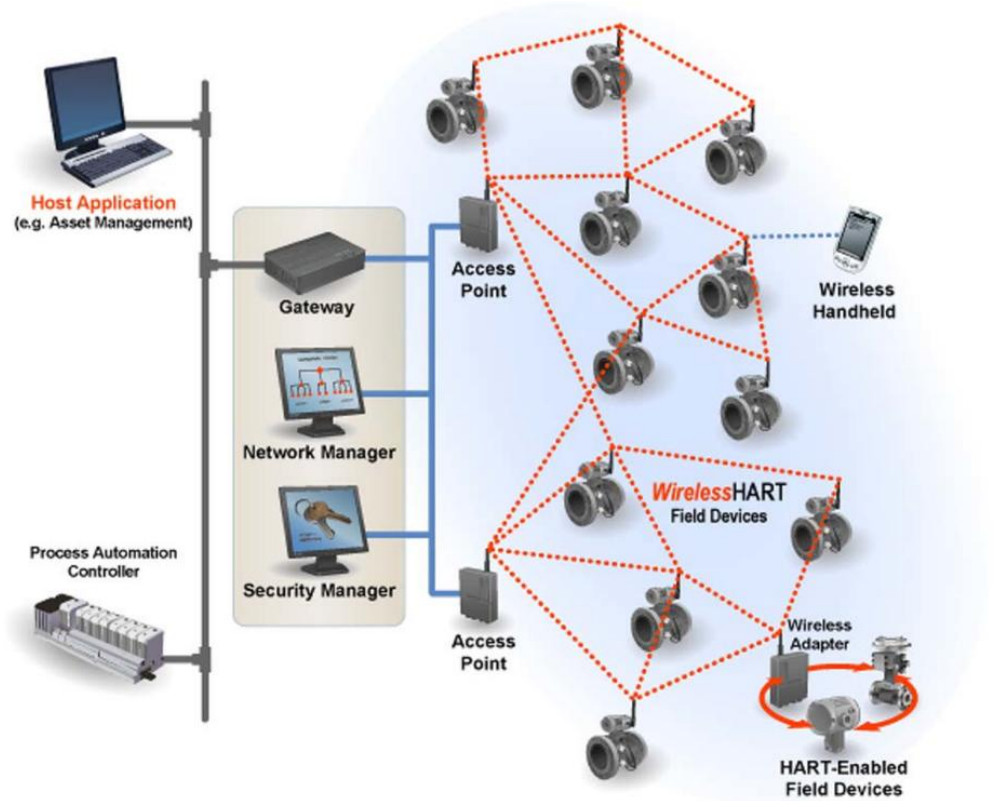
- **Borders Routers –** It has more than one border routers. It helps to prevent the data redundance and failure of network.
- **Lead Devices –** it manages a registry for the assigned routers. It also controls the end devices and allows those devices for self-healing in case of network failure.

- **Thread Routers –** it manages the path services of the mesh topology and always ensure the system in on mode or allowed or downgrade. Information also stored in Thread Device.

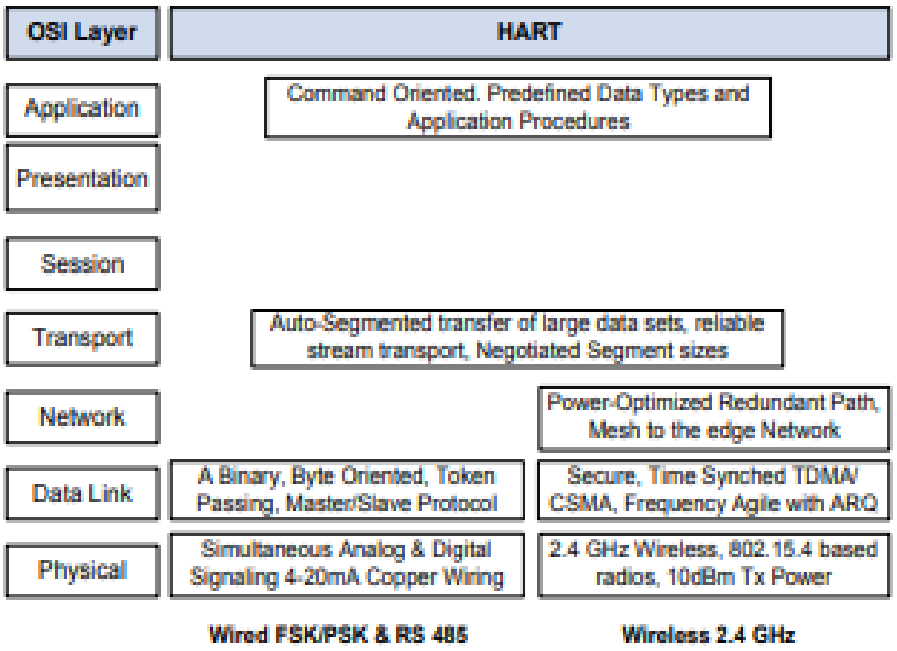
- **REED-** it is the end devices connected.

4. **ISA 100.11.A:** It is another architecture which is designed specifically for large scale industries IOT. It is based on the tunnelled application layers. It works based on the support of Virtual Private area Networks. It has the ability to provides an interface between the wireless field network and the plant network, which connects the various controllers to the data and supervision

5. **Wireless HART:** It works on another technology called bi-directional (get and post). The HART Protocol is used for communicating information from one instrument to central control of monitoring systems. It is very successful for having the communication through wireless channel also. It is designed to serve with simple configuration, flexible and easy to access the instrument.



The OSI Model for HART with the physical layer adopts the IEEE 802.15.4-2006 .this also work on the MESH topology

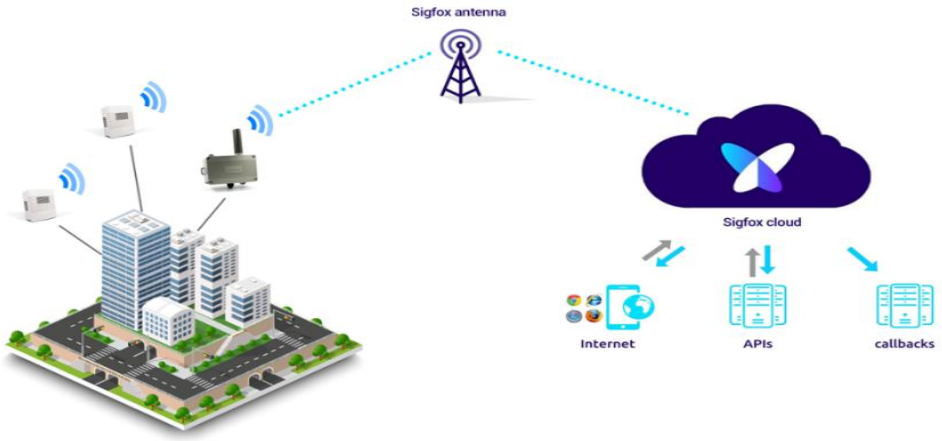


6. **Near Field Communication:** It has the speciation of contactless communication between two devices. NFC used the RFID and standard IS/IEC 18092. It is particularly work within the distance of 10cm. it serves its applications in making transactions, exchange digital content, and connect electronic devices with a touch. Because NFC has the ability to read and write to devices, it is believed that they will have a wider use in the future than standard smart cards. It will be working with an initiator and a target. The initiator has a name and generates Radio frequency signal and the control the exchange of data (a payment device) where the request is answered by a passive target (a Smartphone).

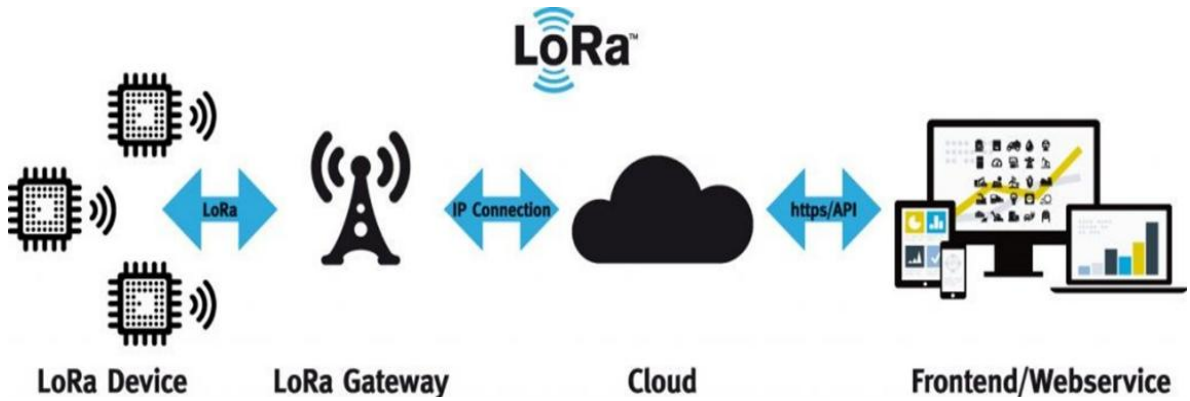
7. **Z-Wave:** Z-Wave is an new wireless home automation technology. It works on very low power. It communicates in the frequency of 900MHz and range of around 30 meters. It makes devices double as repeaters and also has network reliability that enables commercial applications. It is widely used for controlling and monitoring purpose only. It

won't allow the devices to work with any wireless technology. It has the application for energy saving and lowe power consumption.

8. **SIGFOX:** Sigfox works on the software-based communication solution. Its networking and computing are managed in the cloud only. Sigfox is a narrowband (or ultra-narrowband) technology. It uses a standard radio transmission method called binary phase-shift keying (BPSK). It is the radio transmission signals coming from over-the-air. Ex: radio and television stations, cellular phones, or walkie-talkies.



9. **LoRA - Long range Radio:** It's a wireless platform of Internet of Things (IoT). LoRaWAN is the communication protocol It was developed by LoRa-Alliance. Semtech's LoRa chipsets connect sensors to the Cloud and it enables real-time communication of data and analytics.



LoRa works on the spread spectrum technology using the unlicensed sub-GHZ band. The LoRa chirp spread spectrums (CSS) modulations ensure full bidirectional communication (get and Post), The LoRa Signals are generated at very low noise levels. It enables high interference resilience but very difficult to detect or jam.

10. **Narrowband IoT:** Narrowband IoT (NB-IoT) is a wireless IOT . It uses the low-power wide area network (LPWAN) technology. It was developed by 3GPP (3rd Generation Partnership Project) for cellular wireless communication. NB-IoT reduces the power

consumption of connected devices, whereas increasing the capacity and bandwidth efficiency of system specifically in the in locations where the traditional cellular technologies are covered the range. NB-IOT work based on the carrier network. A telecommunications carrier network is the collection of devices and underlying infrastructure used to transmit data from one location to another).

	Sigfox	LoRaWAN	NB-IoT
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868MHz in Europe, 915MHz in North America, and 433MHz in Asia)	Unlicensed ISM bands (868MHz in Europe, 915MHz in North America, and 433MHz in Asia)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Bidirectional	Limited / Half-duplex	Yes / Half-duplex	Yes / Half-duplex
Maximum messages/day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interference immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End-devices do not join a single base station	End-devices do not join a single base station	End-devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network	LoRa-Alliance	3GPP

REFERENCES

[1] Stiller, B., Schiller, E., Schmitt, C., Ziegler, S., & James, M. (2020). An overview of network communication technologies for IoT. *Handbook of Internet-of-Things, 12*.

[2] Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.

[3] Herrero, R. (2022). *Fundamentals of IoT communication technologies*. Cham: Springer.

[4] Kumar, S., Dalal, S., & Dixit, V. (2014). The OSI model: Overview on the seven layers of computer networks. *International Journal of Computer Science and Information Technology Research*, *2*(3), 461-466.

[5] Florencio, H., & Neto, A. D. D. (2019). Method for link stability evaluation of industrial wireless sensor networks (ISA 100.11 a). *Prz. Elektrotechniczny*, *11*, 176-183.

[6] Want, R. (2011). Near field communication. *IEEE Pervasive Computing*, *10*(3), 4-7.

[7] Danbatta, S. J., & Varol, A. (2019, June). Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

[8] Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017, May). Internet of Things (IoT) communication protocols. In *2017 8th International conference on information technology (ICIT)* (pp. 685-690). IEEE.

[9] Lauridsen, M., Nguyen, H., Vejlgaard, B., Kovacs, I. Z., Mogensen, P., & Sorensen, M. (2017, June). Coverage comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² area. In *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)* (pp. 1-5). IEEE.

