**IOE Lab**

**ASSIGNMENT NO. 3**

**Aim**: Describe the IOT protocols: Physical Link layer to Data Link layer with respect to the attributes given below:

* Standardization and alliances
* Physical Layer
* MAC Layer
* Topology
* Security
* Working Principle
* Architecture
* Applications
* Pros and Cons
* Comparison with other protocol

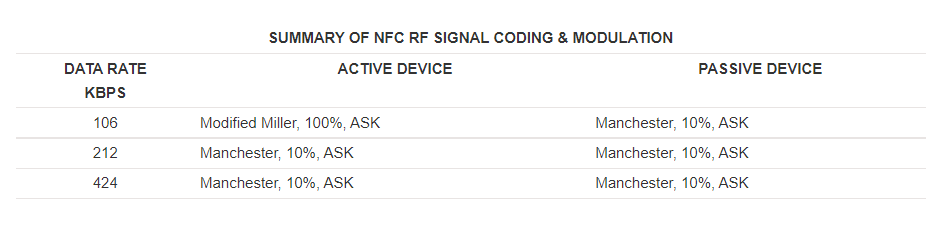
# **1. NFC and RFID**

**Standardization and alliances**: As an international standard, NFC specifies an RFID connection process for the electromagnetic near field. In accordance with ISO/IEC 180000-3, the standard frequency for NFC systems is 13.56 MHz, one of the ISM high-frequency bands available worldwide without a license.

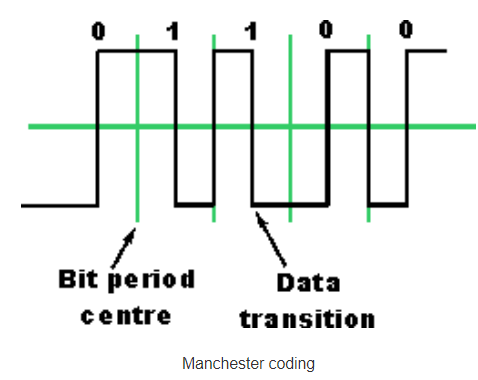
NFC standards cover communications protocols and data exchange formats and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. In addition to the NFC Forum, the GSMA group defined a platform for the deployment of GSMA NFC Standards within mobile handsets. GSMA's efforts include Trusted Services Manager, Single Wire Protocol, testing/certification and secure element.

**Physical Layer**: Physical layer takes care of modulation, coding and RF related parameters such frequency, power etc.

* **NFC RF signal parameters**: NFC uses the global 13.56 MHz allocation as this is an unlicensed radio frequency ISM band. Using ASK - amplitude shift keying, as the format for the NFC modulation, most of the RF energy is concentrated in the allowed 14 kHz bandwidth, although the sidebands may extend out as far as ± 1.8 MHz.
* **NFC RF signal coding & modulation**: NFC employs two different coding systems on the RF signal to transfer data. In most cases a level of 10% modulation is used, with a Manchester coding format. However for an active device transmitting data at 106 kbps, a modified Miller coding scheme is used with 100% modulation. In all other cases Manchester coding is used with a modulation ratio of 10%.

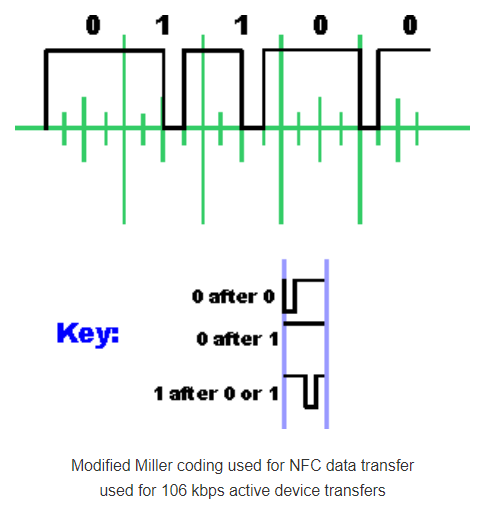


* **NFC and Manchester coding**: Manchester coding is used for the majority of cases for the NFC communications. The Manchester coding utilizes the two different transitions that may occur at the midpoint of a period. A low-to-high transition expresses a 0 bit, whereas a high-to-low transition stands for a 1 bit.



To achieve these conditions it is sometimes necessary to have a transition at the middle of a bit period. Transitions at the beginning of the period are disregarded.

* **NFC and Modified Miller coding**: The modified Miller code is a little less intuitive, but provides an efficient form of coding. It is characterized by the pauses occurring in the carrier at different positions of a period. Depending on the information to be transmitted, bits are coded as shown below. A high or "1" is always encoded in the same way, but a low or "0" is encoded differently depending upon what preceded it.



The NFC RF signal and physical layer is purposefully kept simple and straightforward to enable simple passive cards to be able to read and decode the information as required. As low data rates are used, this also enables the RF interface to be kept as simple as possible.

**MAC Layer**: The NFC MAC layer is also responsible for connection handling, message exchange, emulation modes, anti-collision bit transmission, activation procedures, data transport, and others.

**Topology**: NFC enables short range communication between compatible devices. At least one transmitting device and another receiving device is needed to transmit the signal. Many devices can use the NFC standard and are considered either passive or active. So NFC devices can be classified into 2 types:

* **Passive NFC devices**: These include tags, and other small transmitters which can send information to other NFC devices without the need for a power source of their own. These devices don’t really process any information sent from other sources, and can not connect to other passive components. These often take the form of interactive signs on walls or advertisements.
* **Active NFC devices**: These devices are able to both send and receive data. They can communicate with each other as well as with passive devices. Smartphones are the best example of active NFC devices. Card readers in public transport and touch payment terminals are also good examples of the technology.

**Security**: Although the range of NFC is limited to a few centimeters, standard plain NFC is not protected against eavesdropping and can be vulnerable to data modifications. Applications may use higher-layer cryptographic protocols to establish a secure channel.

The RF signal for the wireless data transfer can be picked up with antennas. The distance from which an attacker is able to eavesdrop the RF signal depends on multiple parameters, but is typically less than 10 meters. Also, eavesdropping is highly affected by the communication mode. A passive device that doesn't generate its own RF field is much harder to eavesdrop on than an active device. An attacker can typically eavesdrop within 10 m of an active device and 1 m for passive devices.

Because NFC devices usually include ISO/IEC 14443 protocols, relay attacks are feasible. For this attack the adversary forwards the request of the reader to the victim and relays its answer to the reader in real time, pretending to be the owner of the victim's smart card. This is similar to a man-in-the-middle attack.

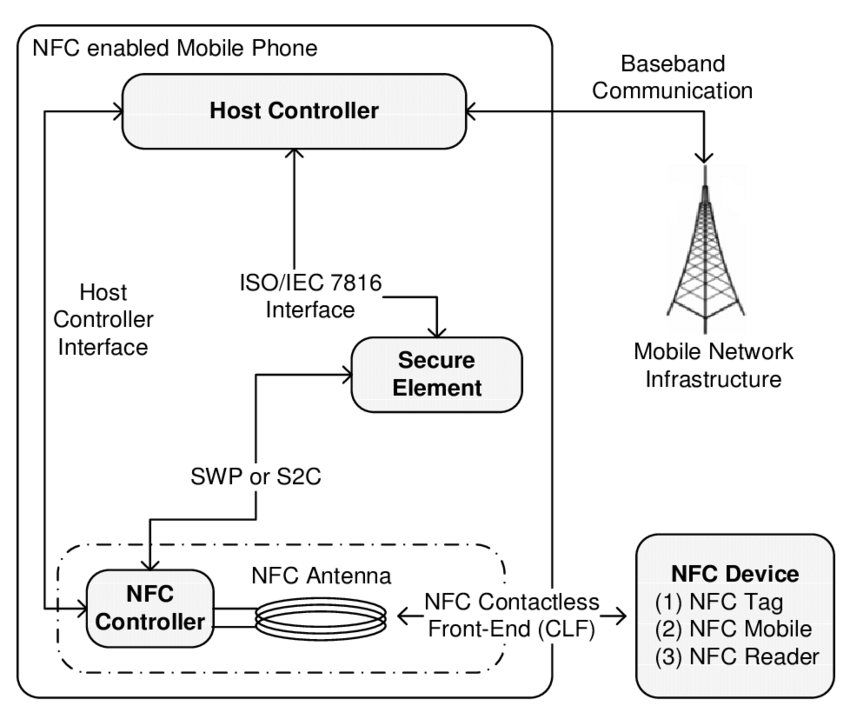
**Working Principle**: NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transition which means devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older technology which is the RFID (Radio-frequency identification) that uses electromagnetic induction in order to transmit information.

The NFC standard currently has three distinct modes of operation to determine what sort of information will be exchanged between devices.

* The most common used in smartphones is the peer-to-peer mode. Exchange of various pieces of information is allowed between 2 devices. In this mode both devices switch between active when sending data and passive when receiving.
* The second mode i.e. read/write mode is a one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advertisement tags use this mode.

* The third mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport systems.

**Architecture**:



NFC interface is composed of a contactless, analogue/digital front-end called as NFC Contactless Front-end (NFC CLF), an integrated circuit called as NFC controller to enable NFC transactions, and an NFC antenna. An NFC enabled mobile phone consists of secure element(s) for performing secure transactions using NFC devices as well as storing sensitive data in a secure environment. The mobile device may contain additional SEs based on the requirements. The NFC controller is connected to SEs through either Single Wire Protocol (SWP) or NFC Wired Interface (NFC-WI).

The SE can be accessed and controlled from the host controller (internally) as well as from the RF field (externally). The host controller, or baseband controller in other words, is the heart of the NFC mobile. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The host controller sets the operating modes of the NFC controller through HCI, processes data that is sent and received, and establishes the connection between the NFC controller and the secure element.

**Applications**: NFC allows one- and two-way communication between endpoints, suitable for many applications.

* **Commerce**: NFC devices can be used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards and allow mobile payment to replace/supplement these systems.
* **Bootstrapping other connections**: NFC offers a low-speed connection with simple setup that can be used to bootstrap more capable wireless connections. For example, Android Beam software uses NFC to enable pairing and establish a Bluetooth connection when doing a file transfer and then disabling Bluetooth on both devices upon completion.
* **Social Networking**: NFC can be used for social networking, for sharing contacts, text messages and forums, links to photos, videos or files and entering multiplayer mobile games.
* **Identity and access tokens**: NFC-enabled devices can act as electronic identity documents found in Passports and ID cards, and keycards for the use in Fare cards, Transit passes, Login Cards, Car key and Access badges. NFC's short range and encryption support make it more suitable than less private RFID systems.
* **Smartphone automation and NFC Tags**: NFC-equipped smartphones can be paired with NFC Tags or stickers that can be programmed by NFC apps. These programs can allow a change of phone settings, texting, app launching, or command execution. Such apps do not rely on a company or manufacturer, but can be utilized immediately with an NFC-equipped smartphone and an NFC tag.

**Pros and Cons**: We take a look at the pros and cons of NFC as a contactless or mobile payment portal. The advantages of NFC include:

* NFC makes it easy for users to make instant payments with their smartphone or tablet.
* It's also a highly versatile platform, in that it covers a range of services and industries.
* This system is beneficial for enterprises as well, as it presents a dynamic and forward-thinking mindset.
* NFC's advanced encryption allows institutions to use it to screen or admit student or employee IDs.

Some of the disadvantages and limitations include:

* NFC technology may be too expensive for some companies, as it usually involves a suite of related devices, equipment, and upgrade-dependent standards.
* While NFC transactions are undoubtedly more secure than regular credit card payments, this technology is not completely free of risk.

**Comparison with other protocol**: NFC and Bluetooth are both relatively short-range communication technologies available on mobile phones. NFC operates at slower speeds than Bluetooth and has a much shorter range, but consumes far less power and doesn't require pairing.

NFC sets up more quickly than standard Bluetooth, but has a lower transfer rate than Bluetooth low energy. With NFC, instead of performing manual configurations to identify devices, the connection between two NFC devices is automatically established in less than 0.1 second. The maximum data transfer rate of NFC (424 kbit/s) is slower than that of Bluetooth V2.1 (2.1 Mbit/s).

NFC's maximum working distance of less than 20 cm reduces the likelihood of unwanted interception, making it particularly suitable for crowded areas that complicate correlating a signal with its transmitting physical device (and by extension, its user).

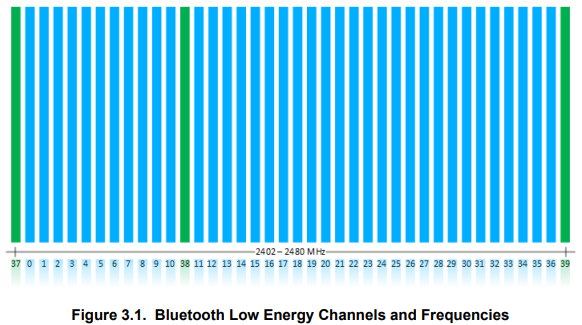
NFC is compatible with existing passive RFID (13.56 MHz ISO/IEC 18000-3) infrastructures. It requires comparatively low power, similar to the Bluetooth V4.0 low-energy protocol. However, when NFC works with an unpowered device (e.g. on a phone that may be turned off, a contactless smart credit card, a smart poster), the NFC power consumption is greater than that of Bluetooth V4.0 Low Energy, since illuminating the passive tag needs extra power.

# **2. BLE**

**Standardization and alliances**: BLE uses 2.4 GHz ISM frequency band either in dual mode or single mode. Dual mode supports both bluetooth classic and low energy peripherals. All BLE devices use the GATT profile (Generic Attribute Profile). The GATT protocol provides a series of commands for the client to discover information about the BLE server.

Bluetooth SIG introduced Bluetooth Low Energy with version 4.0 of the Bluetooth Core Specification. The specification had been several years in the making and most of the controversial sections and decisions were finally ironed out by the companies involved in the development process, with a few additional concerns left to be dealt with in subsequent updates of the specification.

**Physical Layer**: Bluetooth low energy operates in the 2.4 GHz ISM (Industrial Scientific Medical) band (2402 MHz - 2480 MHz), which is license-free in most countries. The Bluetooth 4 specification defines 40 RF channels with 2 MHz channel spacing (see the following figure). Three of the 40 channels are advertising channels (shown in green), used for device discovery, connection establishment, and broadcast. The advertising channel frequencies are selected to minimize interference from IEEE 802.11 channels 1, 6 and 11, which are commonly used in several countries.

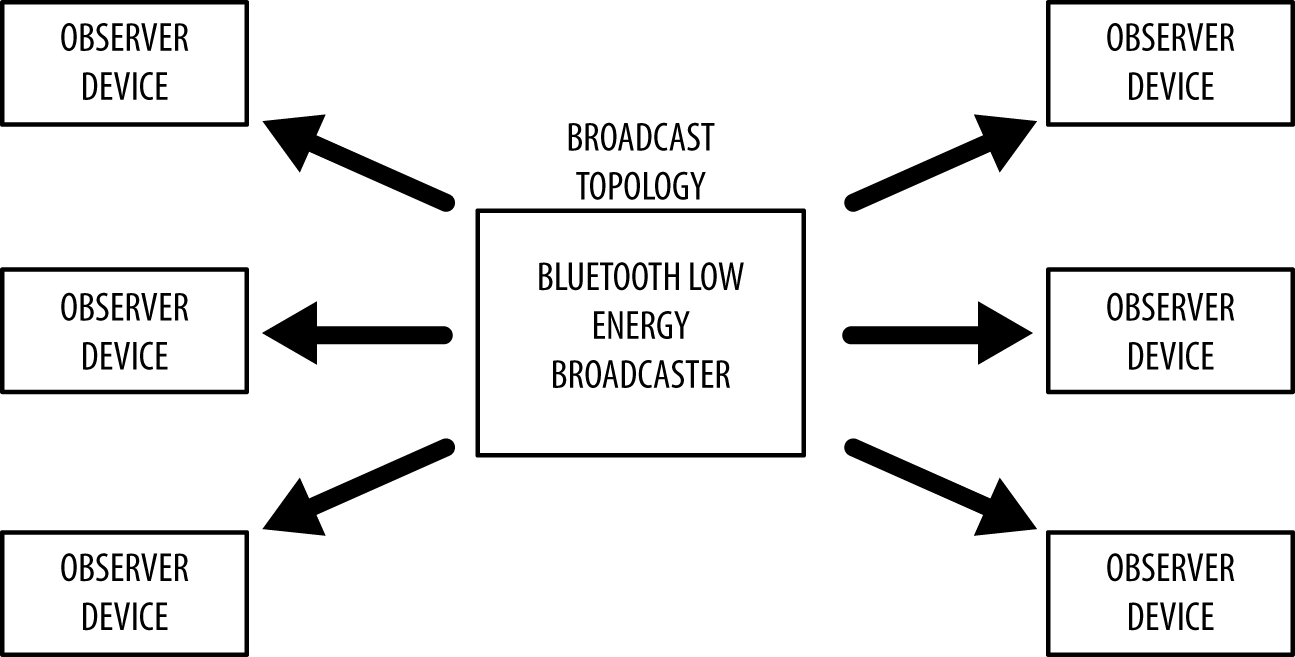


Data channels are used for bidirectional communication between connected devices. AFH (Adaptive FHSS) is used to select a data channel for communication during a given time interval. AFH is reliable, robust, and adapts to interference. All physical channels use GFSK (Gaussian Frequency Shift Keying) modulation, with a modulation index of 0.5, which allows reduced peak power consumption. In Bluetooth 4.0, 4.1, and 4.2 specification, the physical layer data rate is 1 Mbps.

**MAC Layer**: In Bluetooth Low Energy, there are no subdivisions in power classes but only the maximum and minimum output power values of the transmitter are provided. Only an approximate value of the maximum reachable distance can be predicted. The low power required for transmission is the main feature of the Bluetooth Low Energy standard and this result is due to enhancements made on the classic version. These enhancements include reduced frequency band and shorter PDU packets. The packet format is 2 PDUs for date and advertising channels of length 80-376 bits. There is only asynchronous logical transport along with the slot time variable packet transmission.

**Topology**: A Bluetooth Low Energy device can communicate with the outside world in two ways: broadcasting or connections. Each mechanism has its own advantages and limitations, and they are both subject to the guidelines established by the Generic Access Profile (GAP).

Using connectionless broadcasting, you can send data out to any scanning device or receiver in listening range. As illustrated, this mechanism essentially allows you to send data out one-way to anyone or anything that is capable of picking up the transmitted data.



Broadcasting defines two separate roles:

* **Broadcaster**: Sends non connectable advertising packets periodically to anyone willing to receive them.
* **Observer**: Repeatedly scans the preset frequencies to receive any non connectable advertising packets currently being broadcasted.

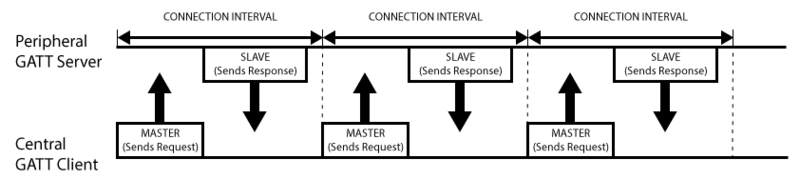
Broadcasting is fast and easy to use, and it’s a good choice if you want to push only a small amount of data on a fixed schedule or to multiple devices. A major limitation of broadcasting, when compared to a regular connection, is that there are no security or privacy provisions at all with it (any observer device is able to receive the data being broadcasted), so it might not be suited for sensitive data.

**Security**: The main security issues with the pairing process and BLE in general are passive eavesdropping, man in the middle (MITM) attacks and identity tracking. Passive eavesdropping is the process by which a third device listens in to the data being exchanged between the two paired devices. The way that BLE overcomes this is by encrypting the data being transferred using AES-CCM cryptography. While AES encryption is considered to be very secure, the key exchange protocols that BLE uses can introduce some severe security vulnerabilities which would allow an attacker to decrypt the data.

MITM attacks are when a third device, which we will call the malicious device, impersonates the other two legitimate devices, in order to fool these devices into connecting to it. In this scenario, both the GAP Central and GAP Peripheral will connect to the malicious device which in turn routes the communication between the two other devices. This gives the legitimate devices the illusion that they are directly connected to each other when in fact their connection has been compromised. As with passive eavesdropping, the pairing method used determines how resilient the BLE connection will be to MITM attacks.

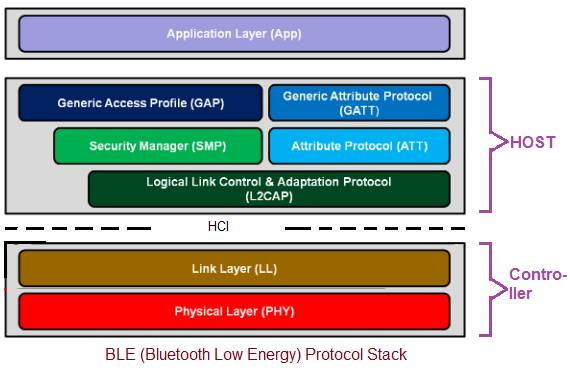
Identity tracking is where a malicious entity is able to associate the address of a BLE device with a specific user and then physically track that user based upon the presence of the BLE device. The way BLE overcomes this is by periodically changing the device address.

**Working Principle**: BLE Beacons broadcast data packets via wireless (through the 2,4GHz band) spaced out by configurable time frames (Broadcast Interval). This emitted data string is called an Advertising Packet. The connection to the Beacon occurs through the Master/Slave principle. (the same principle used by Bluetooth Classic). The Master has the job to handle the communication (start, synchronization, end), while the Slave only performs the Master orders. The Master can open multiple connections with Slaves at a time, but a Slave can be connected with only one Master at a time.



An example of Master/Slave architecture is the communication between Smartphone and Beacon: The smartphone (Master, with a Bluetooth 4.0 chip or higher) keeps listening to the channel where the Beacons (Slave) send their own Advertising. Once it receives an Advertising, the Smartphone can perform a connection with one or more Beacons at a time (maximum 8).

**Architecture**: Bluetooth Low Energy architecture is also described as the Bluetooth LE protocol stack. It describes the different parts of the Bluetooth LE system, their components, and how they interact to yield expected results.



The application layer of the Bluetooth Low Energy stack architecture is the part that interacts directly with the user. It contains the user interface, application logic, and general application architecture. Underneath this layer is the actual hardware, made of the host and controller layers.

The host layer follows the application layer. It consists of various structures:

* **Generic Access Profile (GAP)**: The GAP is a part of BLE architecture that describes how BLE devices communicate with each other. It includes peripheral or broadcaster devices, advertising information packets, and central device scanning for connection-ready devices.
* **Generic Attribute Profile (GATT)**: It describes how attributes are formatted, packaged, and transferred across connected devices following a set of rules. The devices communicate as a client or a server.
* **Attribute Protocol**: The attribute protocol lays the foundation for the GATT profile to function. It is a set of rules guiding how data is accessed. It defines the GATT protocol’s client-server rules, stating that a device can be a client, server, or function as both.
* **Security Manager Protocol**: This protocol ensures communication security between two or more BLE devices. It verifies and authenticates the pairing process. It can also prevent harmful tracking of a device’s Bluetooth address by hiding it.
* **Logical Link Controller And Adaptation Protocol (L2CAP)**: The L2CAP is vital to the BLE architecture. It functions as a protocol multiplexer by converting multiple protocols into standard BLE packets. It can also break down and recombine large data packets.

The controller is the physical part of the Bluetooth Low Energy architecture hardware component. It holds the circuit which decodes signals. The chip operates on the 2.4GHz radio band, which it effectively divides into 40 channels. The channels are used for data transmission and sending advertising packets to establish a connection. The controller consists of the physical layer already described and the link-layer that scans, advertises, creates, and monitors communication between BLE devices.

**Applications**: Bluetooth Low Energy has found applications in several areas. One major propelling factor is that it is easy to use without requiring complex or specialized hardware components.

* **Smart appliances and health or fitness trackers**: Fitness trackers and other smart appliances are some of the perfect use cases for Bluetooth Low Energy. The Bluetooth technology creates a wireless network where these devices can connect, transmit, and process information.
* **Tracking of assets and connected objects**: Asset tracking has become another significant application of BLE devices. Tags containing a BLE transmission device are simply attached to a valuable item, and the owners or those in charge are kept abreast of its location at all times.
* **Contact and employee tracing**: Bluetooth Low Energy has found another indoor application in contact and employee tracing. Just like item finding, employees and even visitors are given BLE-enabled tags that allow a central device managed by a person to record the location of employees at all times yet maintain their personal privacy.
* **Wayfinding and navigation**: Wayfinding and indoor navigation are widely used applications of BLE devices. It finds use in vast complexes and facilities such as hospitals, schools, airports, bus or train stations, etc.
* **Proximity marketing**: Proximity marketing is another use of BLE technology. It works based on location and closeness to a shop or business. So whenever Bluetooth-enabled devices, which cover virtually every smartphone, are close to a shop, targeted adverts showing their best deals are sent out to attract potential customers nearby.

**Pros and Cons**: Bluetooth Low Energy technology has revolutionized the approach to several issues in IoT and other industries. The advantages of BLE include:

* Its low energy consumption significantly prolongs the battery life of BLE-enabled devices.
* It provides encryption of data being transmitted between clients and servers, ensuring data security.
* It can withstand interference on 2.4 GHz because of the frequency hopping technology.
* The connection and data transfer between BLE devices are rapid (about 3 ms).

Some of the disadvantages and limitations include:

* BLE does not perform well over distances more than 25 meters. At optimal conditions, it may extend up to 100 meters but still falls short of the range provided by other technologies (e.g., wide area network or WAN).
* You cannot use it for the transmission of large data packets. Its data rate is limited to 1Mbps and 2Mbps and is not compatible with activities such as video streaming, large file sharing, etc.
* It is open to interference.

**Comparison with other protocol**: Bluetooth and Bluetooth Low Energy are similar in that they help users connect to their most favorite and important devices for both consumer and commercial use. The difference lies in how they distribute data for energy savings.

Standard Bluetooth is ideal for transmitting a lot of data, and BLE is better for saving power. Since BLE can only deliver up to 2 Mb/s, it’s not suitable for applications that need to exchange large files. By contrast, Bluetooth Classic will support heavier data loads but will drain battery life faster and could be more expensive.

At first, it may seem like standard Bluetooth isn’t ideal for IoT applications since it uses more power. Even small devices like smartwatches sometimes need to transfer files as large as 200 MB, though. That may not seem like a particularly massive file, but given BLE’s lower data rates, it could take a while to transfer, at least by today’s standards.

Many IoT processes don’t need to handle files that large. For these instances, BLE would be ideal since it uses considerably less energy than standard Bluetooth. Given how small the batteries are in some devices, even marginal power savings can make a difference.

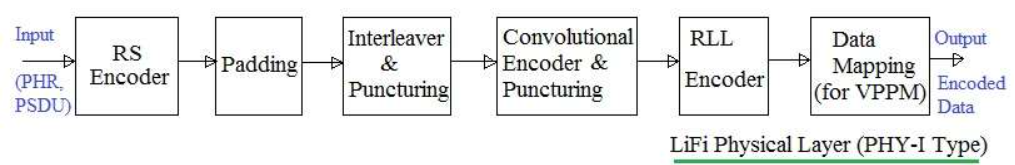
# **3. LiFi**

**Standardization and alliances**: Like Wi-Fi, Li-Fi is wireless and uses similar 802.11 protocols, but it also uses ultraviolet, infrared and visible light communication. Li-Fi is a light communication system that is capable of transmitting data at high speeds over the visible light, ultraviolet, and infrared spectrums. In its present state, only LED lamps can be used for the transmission of data in visible light.

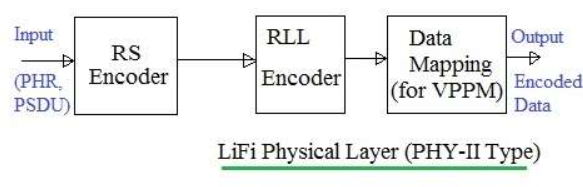
One part of VLC is modeled after communication protocols established by the IEEE 802 workgroup. However, the IEEE 802.15.7 standard is out-of-date: it fails to consider the latest technological developments in the field of optical wireless communications, specifically with the introduction of optical orthogonal frequency-division multiplexing (O-OFDM) modulation methods which have been optimized for data rates, multiple-access, and energy efficiency. The introduction of O-OFDM means that a new drive for standardization of optical wireless communications is required.

**Physical Layer**: LiFi Physical layer provides services to the upper layer. It is Used to provide error correction at the receiver by using FEC techniques such as Convolution encoding and RS encoding. It helps in synchronization at the receiver using preamble incorporated in the frame structure. It inserts a header (PHR) at the transmit end. This is decoded at the receive end to determine the length field of the PSDU. There are different LiFi physical layers based on different data rate and application of use such as indoor or outdoor.

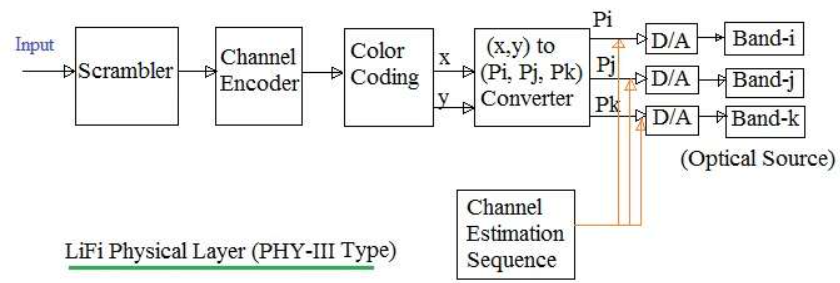
* **LiFi PHY-I**: LiFi PHY-I version is developed to meet low data rate requirements from 12 to 267 Kbps. It is ideally used for outdoor application.



* **LiFi PHY-II**: LiFi PHY-II version is developed to meet moderate data rate requirements from 1.25Mbps to 96 Mbps. It is ideally used for indoor application.



* **LiFi PHY-III**: LiFi PHY-III version is developed to meet data rate requirements of 12 Mbps to 96 Mbps. It is used in the systems where color source based on RGB and detectors are widely employed.

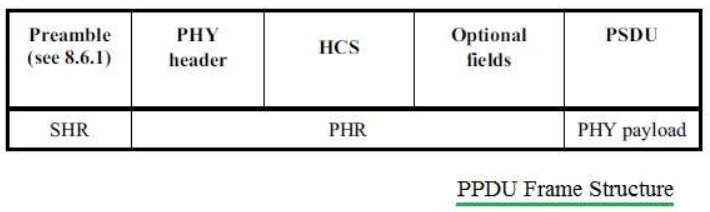


These are used to activate and deactivate VLC transceivers. It also provides WQI for all the received frames. It is used for channel selection as per requirement and RLL (Run Length Limited) Encoding helps in correcting DC balance, clock recovery and flicker mitigation.

**MAC Layer**: The LiFi standard uses following MAC modes for transmission of data and management frames:

* **Single mode**: In this mode, frames carry one PPDU per frame. It is used for short data communication e.g. ACK, Association, Beacon etc.
* **Packed mode**: In this mode, frames carry multiple PPDUs destined for the same destination. This mode improves the efficiency of the MAC layer as it eliminates repetitive PHY and MAC headers for the same destination.
* **Burst mode**: In this mode, the frame uses PHY preamble with reduced length after the 1st frame. Moreover it uses RIFS instead of SIFS. Hence this mode increases efficiency and also improves the throughput.
* **Dimmed OOK mode**: It is used for data transfer in dimming applications.

LiFi system uses PHY frame consisting of preamble, PHY header and PSDU. LiFi PHY Layer Frame Structure has the following structure:



Multiple octets are transmitted least significant octet first and in each octet least significant bit first.

* **Preamble**: It is used by the transceiver to perform optical clock synchronization.

Preamble = { FLP (64 to 16384 bits), TDP(15 bits each), ~TDP, TDP, ~TDP }

FLP (Fast Locking Pattern) consists of alternate one and zeros. Four TDPs (Topology Dependent Patterns) distinguish PHY modes used. Every alternate TDP pattern is inverted to achieve DC balance in the LiFi Physical layer.

* **PHY Header**: It is transmitted along with OOK modulation type. It carries burst mode, channel number, MCS ID (defines PHY type (PHY-I,II or III) and data rate), PSDU length etc.
* **HCS**: It is 16 bit in size. It is used to protect PHY header in LiFi Physical layer. There are optional fields in the frame used in PHY-I mode at a clock rate of 200 KHz.
* **PSDU Field**: This field has variable length. It carries data from the PHY frame.

PSDU: { MHR, MAC Payload i.e. MSDU, FCS, Tail Bits}

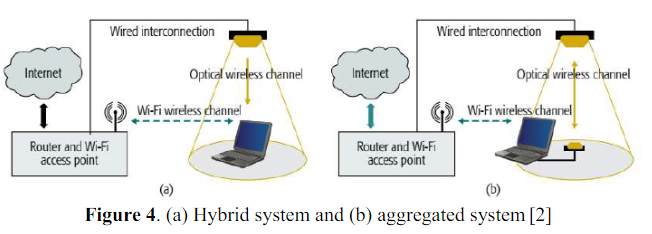
This is described below under the MAC frame section.

**LiFi MAC Layer Frame Structure** consists of MHR, MSDU and MFR. Frame control field carried in MHR is of size 2 octets.



It is composed of frame type, addressing fields, control flags. The MAC frame type is 3 bits long. It is used to differentiate different frame types e.g. Beacon, Data, Acknowledgment, Command, CVD etc. Source and destination addresses are 16 bit or 64 bit long in size.

**Topology**: LiFi has built a proof-of-concept prototype VLC HetNet. This prototype is a concept that uses a diverse spectrum to provide high quality of service in an indoor environment. There is an additional tier in the wireless HetNet using indoor gigabit small-cells to offer additional wireless capacity. The proof-of-concept experiment has two models such as hybrid model and aggregated model.



In the hybrid model, the system uses WiFi to connect to the internet but the downlink of a user is connected through a LiFi link. While the aggregated system is user connected on WiFi and LiFi in parallel. Unidirectional LiFi link is used in hybrid systems to supplement the WiFi downlink. In an aggregated system both WiFi and LiFi use bi-directional communication to improve the throughput and achieve robust connectivity.

**Security**: Radio frequency waves permit greater access of data as opposed to light transmissions used by LiFi. Due to this, LiFi’s light technology offers greater control over networks for its users. A LiFi channel is moderated and confined to the devices in a given area.

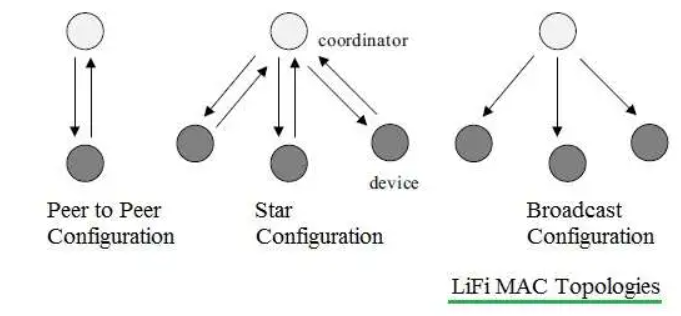
The security benefits surrounding LiFi are as follows:

* LiFi technology has rid any health concerns with wireless technology.
* Seen data rates at a peak of 10 Gbps.
* Access to more devices with Internet-of-Things.
* 10,000 times more capacity to eliminate the radio frequency spectrum crunch.
* Created a modified wireless infrastructure with more secure data transmission.

LiFi’s most efficient feature is its ability to operate on all visible light. Data can be transmitted with the very LED light bulbs in peoples’ homes, recreational centers, offices, and schools. LiFi’s efficient light technology blossoms the service into a cost-efficient and energy-efficient wireless system. When light is not necessary, the process will lessen to a point of seeming off, but in actuality is still navigating and computing. Efficiency paves way for another obvious benefit of LiFi: accessibility. Wherever emissions of light exist, internet services can exist. As light is usually found in all public places, these transmissions of data at high speeds can be accessible virtually anywhere and everywhere.

**Working Principle**: LiFi is the short form of “Light Fidelity”. It works on the principle of Visible Light Communication (i.e. VLC). The network is also referred to as VPAN or VLC Personal Area Network. The VLC transmits data by intensity modulation. It uses LEDs and Laser diodes(or photo detectors) at transmit and receive ends respectively. It works in a 380 nm to 780 nm optical band which is visible light and hence the name VLC.

The VLC standard or VPAN standard defines three classes of devices viz. infrastructure, mobile and vehicle. These devices operate in one of the three topologies mentioned below. The different devices have different coverage ranges, data rates and other requirements.

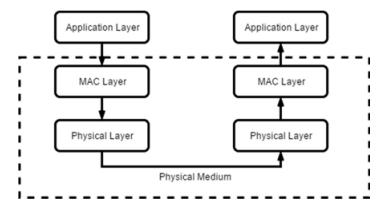


It works in three modes as mentioned above. In star topology, communication is established between the central controller (i.e. coordinator) and devices. In peer to peer topology, one of the devices should become coordinator at the time of establishing association.

Each device or coordinator has a unique 64 bit address. Devices can use 16 bit addresses also upon request at the time of establishing association with coordinator.

**Architecture**: In layered architecture, LiFi consist of 3 stages i.e. Application layer, MAC layer,

and Physical Layer.



PHY layer responsible for transmission and reception, activation and deactivation of optical transceiver, and detection of state of transmission channel, is it idle or busy state. There are 3 operation modes in the PHY layer.

Three network topologies are defined in MAC layer: Peer to peer, star, and broadcast.

* **Peer to peer**: There are two devices that communicate. One of them is to act as a coordinator.
* **Star**: Communication happens in several devices. One of them acts as a coordinator and it’s used as illumination infrastructure.
* **Broadcast**: One device i.e . a coordinator sends data to several devices. The communication is in a unidirectional way.

Propagation channel in LiFi is not different from VLC. Indoor environments characterized by six different link configurations refer to IR links. Transmitter and receiver communicate in two criterions, i.e. direct or indirect line-of-sight (LOS) that is required in the propagation channel. These two criterions are based on the degree of directionality of the transmitter and receiver (LOS) , others are based on the reflection of the light (non-LOS). In the LOS the links between the transmitter and receiver are pointing or directed at each other. While in the non-LOS the light is spreading by the reflection of the ceiling or diffusely reflecting surface.

**Applications**: LiFi applications are varied as a result of its key features, such as directional lighting, energy efficiency, intrinsic security, high data rate capability, signal blocking by walls and integrated networking capability.

* **Aircrafts**: In air crafts, passengers get high-charges on low-speed internet, but using Li-Fi provides affordable fees for high-speed internet.
* **Health technologies**: WI-Fi has been replaced by Li-Fi in many hospitals because use of Wi-Fi in hospitals interferes with mobile devices and computers that block the monitoring equipment signals.
* **Traffic Application**: Li-Fi can be used in traffic management, which interacts with LED lights of vehicles such as buses, which can help in dealing with traffic and can regulate accidents by warning other drivers when vehicles are excessively close.
* **Disaster management**: Li-Fi can be used as groundbreaking methods of correspondence in the midst of disaster, e.g. seismic tremor or, on other hand, hurricanes as subway stations and passages; common dead zones do not impede Li-Fi.
* **Power Plant application**: Li-Fi is progressively safe, bottomless availability in all regions of power plant as utilization of Wi-Fi and other radiation source isn’t acceptable.

**Pros and Cons**: Aside from it saving the world from spectrum crunch, LiFi comes with a lot of other benefits. Here are its major advantages:

* **Proficiency**: Energy utility can be minimized with use of LED illumination which are now accessible in homes, workplaces and malls and so on for lighting reasons. Consequently transmission of information requires negligible additional power, which makes it efficient in terms of costs as well as energy.
* **Cost**: Not only does Li-Fi need fewer components for its service, but it also requires only a small additional capacity for data transmission.
* **Availability**: Disponibility is not an issue as light sources are available all over the place. Along these lines, lights can be utilized as models for information transmission.
* **Security**: One principal advantage of Li-Fi is security. Since light can’t go through opaque structures, Li-Fi web is accessible just to clients inside a limited zone and can’t be intercepted and misused outside an area under operation.
* **High speed**: Combination of low interference, high bandwidths and high-intensity output, aids Li-Fi provides high data rates i.e., 1 Gbps or even beyond.

Disadvantages includes:

* The availability of light sources is necessary for internet access. This could restrict areas and situations where Li-Fi might be used.
* To trade data it requires a close or immaculate line of sight.
* Light waves can not penetrate walls and therefore Li-Fi has much shorter range than Wi-Fi.
* Opaque impediments affect data transmission on pathways.
* Normal light, sunlight, and ordinary electric light can influence information transmission speed.

**Comparison with other protocol**: Wi-Fi(wireless fidelity) and Li-Fi(light fidelity) are two different technologies that are used to send and receive data wirelessly. The main difference between Wifi and Lifi is, Wifi uses radio waves in order to transmit data at a slower data rate whereas Lifi uses visible light in order to transmit data at a much faster rate. Lifi is a groundbreaking technology which has been introduced recently in wireless communication. Through this technology, the bulbs at homes, offices and streets will not only be able to light and illuminate the environment but will also be able to transmit data wirelessly at high speed.

In Lifi, data can be transferred at 1Gbps. In Wifi, data can be transferred at 150Mbps with the use of WLAN -11n. The frequency that could be used in Lifi is ten thousand times the frequency of the radio spectrum. The frequency range used is between 400 and 800 terahertz on the visible light range. The frequency spectrum that could be used in Wifi is 2.4GHz, 4.9 GHz, and 5GHz.

It is evident that Lifi is a new technology which has the ability to surpass wifi easily due to its faster data rate and safety. Due to the above features and the simple hardware modification that needs to take place, it will be an ideal alternative to wifi. It will also be able to provide a greater range when compared with wifi.

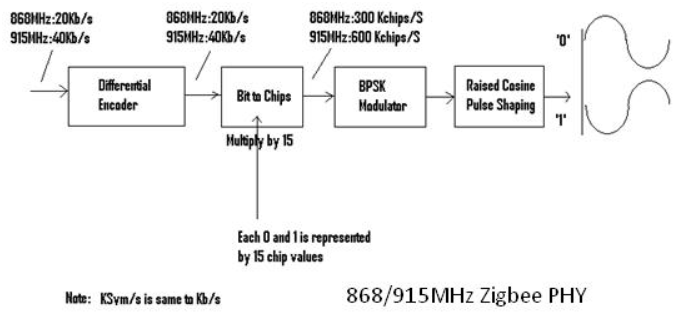
# **4. Zigbee**

**Standardization and alliances**: Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection. Hence, Zigbee is a low-power, low data rate, and close proximity (i.e., personal area) wireless ad hoc network.

Although numerous semiconductor manufacturers have registered with the ZigBee Alliance, only relatively few products have been announced so far. Freescale, a prominent member, has already launched a transceiver (MC13192), but also some smaller semiconductor manufacturers such as Chipcon (CC2430), Atmel (Z-Link) or Ember (EM2420) have already included products in their portfolio or stated that they will soon do so.

**Physical Layer**: There are two Physical layer formats one each for 868/915MHz and 2450MHz bands in Zigbee standard. 868-868.6 MHz zigbee band delivers about 20k Symbol/s with BPSK modulation employed. The 902-928 MHz band delivers about 40k Symbol/s with BPSK modulation. 2400-2483.5 MHz delivers about 62.5k Symbol/s with O-QPSK modulation.

* **868/915 PHY layer**: The first block is differential encoder. Bit to chips will convert each bit to 15 chip values, as mentioned in IEEE 802.15.4-2003 standard.



These chip values are BPSK modulated using a BPSK modulator block. The modulated signal is passed through the Raised cosine filters in the chain. This filtered signal is modulated using an RF carrier and transmitted over the air.

* **2450 PHY layer**: Each octet is divided into two nibbles of 4 bits each. These nibbles are converted to decimal values 0-15. This is fed as input to the symbol to chip and based on the Symbol-to-chip mapping table these decimal values are converted into chips. Later chips are passed through OQPSK modulator block and half sine wave pulse shaping filter before being converted to RF modulated waveform.

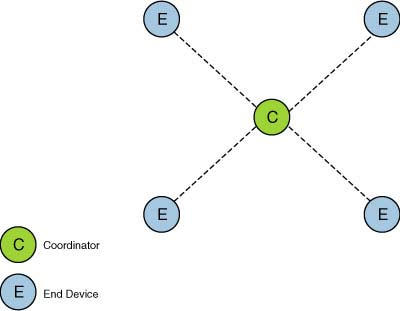


PPDU packet format which is transmitted is mentioned below. Zigbee PPDU Frame consists of SHR (Preamble 4 bytes, SFD 1 byte) + PHR(Frame length 1 bit, Reserved 1 bit) + PHY Payload(PSDU variable length)

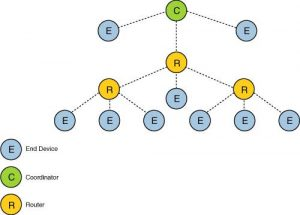
**MAC Layer**: This layer provides an interface between the physical and network layers. It defines how multiple 802.15.4 radios operating in the same area will share the airwaves. Data handling and data management are the two main functions of the MAC layer. Data handling includes functions such as “Data Request” and “Data Confirm”. The MAC layer adds a destination address and transmits options for the outgoing data frames.

When the Zigbee network layer calls the “data request” function, the data gets formatted into the relevant MAC header and frame length is added which is the physical header. The data frame is ready to be transmitted. The purpose of the “Data Confirm” function is to communicate the status of the transmitted data. It sends a fail status when the transmission frames exceed or when there is no response to transmitted data.

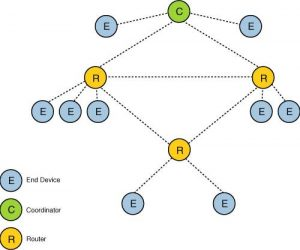
**Topology**: Zigbee network topology can be divided into three types. There are star topology, tree topology and peer-to-peer or mesh topology. Each topology will have a different effect on how the messages are routed and which devices connect to which devices.



The first topology is the star topology. Star topology consists of a coordinator and few end devices. It is the simplest and most limited one in the Zigbee. Devices are all connected to a single coordinator node and all communication goes via this coordinator.



The second topology is tree topology. It consists of a coordinator, a few routers and end devices that act as a central node or root tree. The routers operate as an extension for the network coverage. The end nodes that are connected to the parent (coordinators or routers) are called children. Only the end devices can communicate with the parent.



The third and last topology is peer-to-peer or mesh topology. This topology consists of a coordinator, a few routers and an end device. You can expand the network range by adding more devices into the network. If during the transmission one of the paths fails, the node will find the alternate path to reach to the destination therefore eliminating dead zones. Using this mesh topology it is easier for users to add or remove the device because they can communicate with any destination device in the network.

**Security**: Security in a ZigBee network is usually organized through a single node, the nominated Trust Center, which is often the ZigBee coordinator. The role of the Trust Center is to authenticate devices that attempt to join the network and distribute security credentials. The choice of Trust Center and the Trust Center policy is the most important decision in creating a ZigBee network.

As an alternative to the above centralized security network, ZigBee 3.0 allows de-centralized security management through a distributed security network. The two network security types are summarized below:

* **Centralized security**: Trust Center allows devices onto the network and distributes keys. It has a view of every node that has been authenticated onto the network.
* **Distributed security**: Every ZigBee router authenticates and distributes keys to devices that attempt to join the network as children of the router. In this case, there is no central node which has a view of all the authenticated nodes.

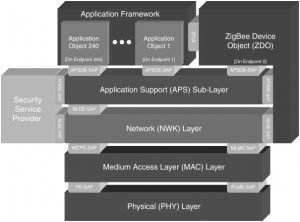
The authentication policies, the distribution and storage of authentication data, and the commissioning method all determine how secure a ZigBee network is. The ZigBee specification does not mandate any particular security policy and the choice is left to the solution providers.

**Working Principle**: Zigbee technology works with digital radios by allowing different devices to converse through one another. The devices used in this network are a router, coordinator as well as end devices. The main function of these devices is to deliver the instructions and messages from the coordinator to the single end devices such as a light bulb.

In this network, the coordinator is the most essential device which is placed at the origin of the system. For each network, there is simply one coordinator, used to perform different tasks. They choose a suitable channel to scan a channel as well as to find the most appropriate one through the minimum of interference, allocate an exclusive ID as well as an address to every device within the network so that messages otherwise instructions can be transferred in the network.

Routers are arranged among the coordinator as well as end devices which are accountable for messages routing among the various nodes. Routers get messages from the coordinator and store them until their end devices are in a situation to get them. These can also permit other end devices as well as routers to connect the network.

**Architecture**: Zigbee protocol architecture consists of a stack of various layers where IEEE 802.15.4 is defined by physical and MAC layers while this protocol is completed by accumulating Zigbee’s own network and application layers.



Physical Layer does modulation and demodulation operations upon transmitting and receiving signals respectively. This layer’s frequency, data rate, and a number of channels are given below.

MAC Layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidances (CSMA). This also transmits the beacon frames for synchronizing communication.

Network Layer takes care of all network-related operations such as network setup, end device connection, and disconnection to network, routing, device configurations, etc.

Application Support Sub-Layer enables the services necessary for Zigbee device objects and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

Application Framework provides two types of data services as key-value pair and generic message services. The generic message is a developer-defined structure, whereas the key-value pair is used for getting attributes within the application objects. ZDO provides an interface between application objects and the APS layer in Zigbee devices. It is responsible for detecting, initiating, and binding other devices to the network.

**Applications**: Zigbee protocols are intended for embedded applications requiring low power consumption and tolerating low data rates. The applications of ZigBee technology include the following:

* **Industrial Automation**: In manufacturing and production industries, a communication link continually monitors various parameters and critical equipment. Hence Zigbee considerably reduces this communication cost as well as optimizes the control process for greater reliability.
* **Home Automation**: Zigbee is perfectly suited for controlling home appliances remotely as a lighting system control, appliance control, heating, and cooling system control, safety equipment operations and control, surveillance, and so on.
* **Smart Metering**: Zigbee remote operations in smart metering include energy consumption response, pricing support, security over power theft, etc.
* **Smart Grid monitoring**: Zigbee operations in this smart grid involve remote temperature monitoring, fault locating, reactive power management, and so on.

**Pros and Cons**: There are some important advantages of zigbee which are given below:

* It is self-healing as well as more reliable.
* This network has a flexible network structure.
* Network setting is very easy as well as simple.
* Loads are evenly distributed across the network because it doesn’t include a central controller.
* Home appliances monitoring as well as controlling is extremely simple using remote.
* The network is scalable and it is easy to add/remote ZigBee end device to the network.

The disadvantages of Zigbee include the following:

* It needs the system information to control Zigbee based devices for the owner.
* The high replacement cost once any issue happens within Zigbee based home appliances
* It is so highly risky to be used for official private information.
* It is not used as an outdoor wireless communication system because it has less coverage limit.
* Similar to other types of wireless systems, this ZigBee communication system is prone to bother from unauthorized people.

**Comparison with other protocol**: Bluetooth is widely used to connect wireless devices in a short range. ZigBee too is a wireless technology standard for personal area networks but it is energy efficient as it uses low-power digital radio waves.

Zigbee employs the Direct Spread Spectrum technique. In the direct spread spectrum, the original signal is mixed and recovered from a pseudo random code at the transmitter and receiver. Bluetooth employs the Frequency Hopping Spread Spectrum. In frequency hopping, the carrier signal is made to fluctuate in frequency.

Systems built on the Zigbee protocol are intended for wireless sensor networking, and they are more popular with compact and energy-efficient gadgets. Zigbee-based networking is used in a variety of applications, including SCADA system sensors, medical devices, and television remote controls. Computer peripherals like wireless keyboards, mice, headsets, and other peripherals are the main use cases for Bluetooth-based applications. Additionally, several wireless remote controls and gesture-controlled devices communicate data via Bluetooth.

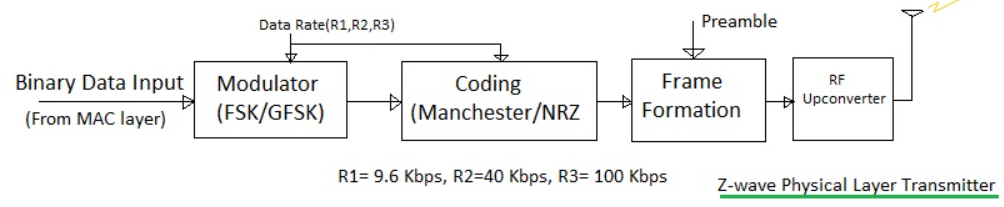
# **5. Z-Wave**

**Standardization and alliances**: Established in 2005 and re-incorporated as a non-profit in 2020, the Z-Wave Alliance is a member-driven standards development organization dedicated to market development, technical Z-Wave specification and device certification, and education on Z-Wave technology. Z-Wave Alliance is a consortium of over 300 companies in the residential and commercial connected technology market. Z-Wave Alliance certified devices to standards that guarantee interoperability with full backwards compatibility among all generations of Z-Wave devices.

In December 2019, the Z-Wave Alliance announced that the Z-Wave specification would become a ratified, multi-source wireless standard. It includes the ITU.G 9959 PHY/MAC radio specification, the application layer, the network layer, and the host-device communication protocol. Instead of being a single-source specification, it will become a multi-source, wireless smart home standard developed by collective working group members of the Z-Wave Alliance. August 2020, the Z-Wave Alliance officially became incorporated as an independent nonprofit standards development organization, with seven founding members under its new SDO structure.

**Physical Layer**: Z-wave physical layer (PHY) covers basic features of Z-wave physical layer and mentions Z-wave PHY transmitter block diagram.

There are three different data rates supported in the Z-wave Physical layer. They are 9.6 kbps (designated as 'R1'), 40 Kbps (designated as 'R2') and 100 Kbps (designated as 'R3'). Based on this data rate different physical layer configuration is made.



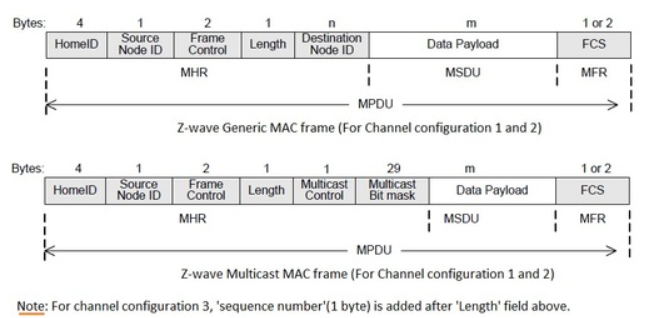
As shown in the Z-wave physical layer consists of modulation and coding blocks. After the modulation and coding of the input MAC layer data, the frame is formed as per format outlined in Z-wave tutorial. In order to do this a physical layer preamble is inserted before 'SOF' field.

FSK modulation is employed for R1 and R2 rates while GFSK is used for R3 data rate. For R1 manchester coding is used while for R2/R3 NRZ coding types is used. All the data is transmitted in little endian format. They are transmitted in blocks of 8 bit with MSB being sent first after manchester coding. Manchester coding will help in obtaining DC free signals.

At the Z-wave physical layer receiver, preamble is used for synchronization before decoding and demodulation is carried out to retrieve the MAC layer data. After the decoding of the data, they will be passed to the upper layers for further processing.

**MAC Layer**: The MAC layer has a collision avoidance mechanism that prevents nodes from starting to transmit while other nodes are transmitting. The collision avoidance is achieved by letting nodes be in receive mode when they are not transmitting, and then delay a transmit if the MAC layer is currently in the data phase in the receiver. The collision avoidance is active on all types of nodes when they have the radio activated.

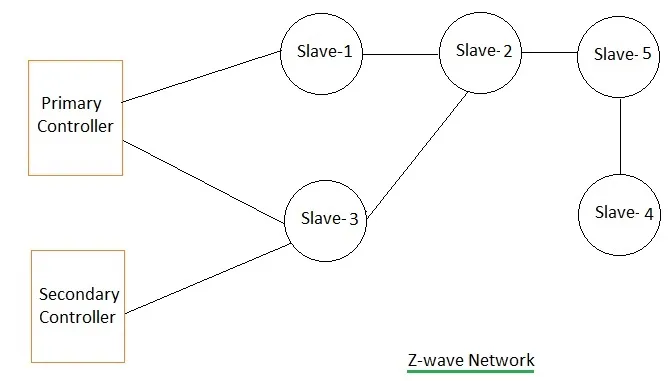
The MAC layer is independent of the RF media, frequency and modulation method but the MAC layer requires either access to the frame data when received or to the whole signal in binary form either as an decoded bit stream or to the Manchester coded bit stream.



The transmission of the frame is delayed a random number of milliseconds. The data stream is Manchester coded and consists of a preamble, start of frame (SOF), frame data and an end of frame (EOF) symbol. The frame data is the part of the frame that is obtained from the transport layer at the transmitter and given to the transport layer at the receiver. Each MAC frame (MPDU) consists of MHR, MAC payload and MFR.

* MHR consists of addresses, frame control and length information
* MAC payload contains data as per frame type. Ack frames do not have a payload field.
* MFR contains a FCS (Frame Check Sequence).

**Topology**: The topology of the Z-Wave mesh is shown in the following figure using some of the device types and attributes associated with slaves and controllers. A single primary controller manages the network and establishes the routing behaviors.



The z-wave network consists of controllers (one primary controller and more than one secondary controllers) and slaves. Controller devices are the nodes in a z-wave network which initiates control commands. It also sends out the commands to other nodes. The slave devices are the nodes which replies based on command received and also execute the commands. Slave nodes also forward the commands to other nodes in the network. This makes it possible for controllers to establish communication with the nodes who are not in the radio frequency region.

**Security**: The Z-Wave security solution comprises of two parts:

* Security elements implemented on application level provided by Silicon Labs
* Security elements implemented on application level provided by OEM

Each part or combination provides protection, detection or reaction against a number of security attacks.

* Facilities and systems to prevent people obtaining information.
* To find out if anybody has gained access, and compromised important information or processes.
* To allow the "bad guys" to be identified and their activity stopped.

Security is achieved by transforming outgoing messages using encryption and a message authentication code (MAC). To maintain backward compatibility and interoperability, both the secured and unsecured Z-Wave devices can operate in the same Z-Wave network.

The Z-Wave security solution supports networks with mixed secure and non-secure communication in order to leverage on the existing non-secure products. Both secure and non-secure nodes can participate in the routing algorithm.

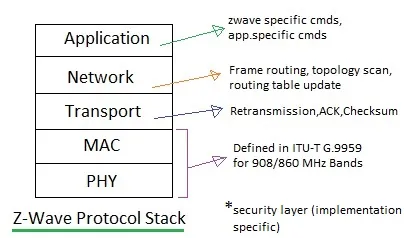
It is up to the implementation of each application to decide which commands should be supported using security encapsulation. For example, a device may choose to support all its command classes non-secure if it is being included to a non-secure network, but no command classes non-secure if it is included securely.

**Working Principle**: The concept of Z-Wave technology is that it uses a low-power RF radio circuitry which is embedded into home electronics devices and systems. Z-Wave technology is aimed at a number of wireless home automation areas including lighting, residential access control, entertainment systems and all forms of household appliances. Z-Wave can be used within a network (Home Area Network, HAN), and can therefore be used to set up all areas of home automation, possibly controlled by a single controller.

With many more home devices becoming remotely controlled, Z-Wave technology is seen as having a large market opportunity, especially with the talk about the Internet of Things, IoT becoming more widespread. Z-Wave modules are available from a variety of sources relatively cheaply and therefore they provide an excellent format for home automation.

The International Telecommunications Union, ITU has included the Z-Wave PHY and MAC layers as an option in its G.9959 standard. This defines a set of guidelines for sub-1-GHz narrowband wireless devices.

**Architecture**: The z-wave protocol layer's main function is to communicate very short messages of a few bytes long from a control unit to one or more z-wave nodes. It is a low bandwidth and half duplex protocol to establish reliable wireless communication. z-wave protocol stack need not have to take care of large amounts of data as well as any kind of time critical or streaming data.



As shown in the Z-wave protocol stack consists of 5 layers viz. PHY layer, MAC layer, Transport layer, network layer and application layer. The security layer is not defined in z-wave open protocol specifications and hence it is implementation specific. Following are the major functions of these protocol layers.

* Physical layer takes care of modulation and RF channel assignment as well as preamble addition at the transmitter and synchronization at the receiver using preamble.
* MAC layer takes care of HomeID and NodeID, and controls the medium between nodes based on collision avoidance algorithm and backoff algorithm.
* Transport layer takes care of transmission and reception of frames, takes care of retransmission, ACK frame transmission and insertion of checksum.
* Network layer takes care of frame routing, topology scan and routing table updates.
* Application layer takes care of control of payloads in the frames received or to be transmitted.

**Applications**: Z-wave offers smarter, safe and energy efficient solutions for smart homes, security and office automation.

* **Smart Hubs**: Smart hubs will be connected to the internet (using an Ethernet port or using wireless LAN) and all devices can be accessed from anywhere using an internet connection.
* **Smart Lighting**: Smart lighting is one of the most commonly used applications of smart home technologies like Z-wave. Light intensity can be wirelessly controlled and configured using a mobile phone app which can be accessed from anywhere.
* **Smart Locks**: Smart locks are getting popular nowadays. Z-wave technology offers a wide range of smart access control solutions with user friendly touch panels and keypad. Fingerprint scanners and highly secure mode of access can be configured using Z-wave technology.
* **Smart Sensors**: Smart sensors are inevitable components of any smart home and Internet of Things applications. Application areas of smart sensors uses Z-wave technology are thermostats, humidity sensors, proximity sensors etc.
* **Smart Home automation**: Z-wave provides advanced home automation solutions. Any appliances compatible with Z-wave technology can be added to smart home network. These devices and home appliances can be securely controlled using Smartphone apps.
* **Smart USB**: Smart USB will convert any personal computer running Z-wave software to a smart hub for home automation applications. Any compatible devices can be connected to the networks and easily control them.

**Pros and Cons**: Following are the advantages of Z-wave:

* The Z-wave network installation is simple and easy. It is also easy to add/remove Z-wave devices in the once installed system.
* The Z-wave devices consume less power and hence saves a great amount of cost in battery use.
* The home appliances are controlled remotely and this will add a great amount of comfort to the users.
* Z-wave devices are interoperable with other wireless devices in the IoT space.
* The Z-wave technology based devices are cheaper and hence technology is affordable to obtain great features/facilities once installed.
* It uses AES-128 type of encryption to provide secured wireless networks for the users.

Following are the disadvantages of Z-wave:

* The coverage is limited and hence requires more z-wave devices to cover larger regions. This increases the overall cost if more Z-wave repeaters or routers are employed.
* The technology requires knowledge to keep it secure from unauthorized people. This is due to the fact that Z-wave works on RF (Radio Frequency) and it is wireless in nature which can be accessed from anywhere.
* It supports only tree topology structure.
* It supports a limited number of nodes i.e. 232 which is less than 65000 nodes as supported by zigbee standard.
* It supports less data communication speed upto 100 kbps which is less compared to zigbee. Moreover due to less speed, Z-wave can only be used for small data size based communication needs such as monitoring and control.

**Comparison with other protocol**: For smart home wireless networking, there are numerous technologies working together. Z-Wave operates on the sub1GHz (low bandwidth) vs 2.4GHz (high bandwidth) to capitalize on the application-level benefits of low power, long range, and less RF interference. WiFi and Bluetooth operate on the 2.4GHz bandwidth which manages a lot of traffic among devices that consume a lot of power.

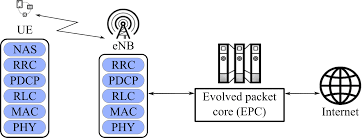
Other network standards include Bluetooth LE and Thread. Z-Wave has better interoperability than ZigBee, but ZigBee has a faster data transmission rate. Thread and Zigbee operate on the busy Wi-Fi standard frequency of 2.4 GHz, while Z-Wave operates at 908 MHz in the United States, which has reduced noise and congestion, and a greater coverage area. All three are mesh networks.

The Z-Wave MAC/PHY is globally standardized by the International Telecommunication Union as ITU 9959 radio, and the Z-Wave Interoperability, Security (S2), Middleware and Z-Wave over IP specifications were all released into the public domain in 2016, and Z-Wave has become a fully-ratified open-source protocol for development. Z-Wave networks have IP at the gateway level, enabling cloud connectivity to Matter. They can also work together at the local network level.

# **6. Narrow band IoT**

**Standardization and alliances**: Narrowband Internet of things (NB-IoT) is a low-power wide-area network (LPWAN) radio technology standard developed by 3GPP for cellular devices and services. The specification was frozen in 3GPP Release 13 (LTE Advanced Pro), in June 2016. Other 3GPP IoT technologies include eMTC (enhanced Machine-Type Communication) and EC-GSM-IoT.

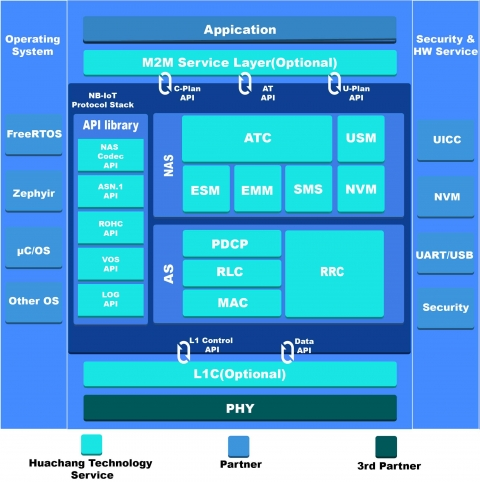
**Physical Layer**: NB-IoT protocol stack has been categorized into user plane and control plane. The user-plane LTE-NB protocol stack consists of a physical layer (PHY), MAC layer, RLC layer and PDCP layer. The control-plane LTE-NB protocol stack consists of PHY, MAC, RLC, PDCP, RRC and NAS layers.



Following are the functions of the physical layer:

* It enables exchange of data and control information between eNB and UE. It also enables transport of data to and from higher layers.
* The functions performed by PHY include error detection, FEC, antenna processing, synchronization etc.
* It consists of physical signals and physical channels. Physical signals are used for system synchronization, cell identification and channel estimation. Physical channels are used for transporting control, scheduling and user payload processing from higher layers etc.
* It uses OFDMA (with 15 KHz subcarrier spacing) in the downlink and SC-FDMA (with 3.75 KHz for single mode transmissions, 15 KHz for multi-tone transmissions) in the uplink.
* QPSK is used as the highest modulation scheme.
* HD FDD and TDD are supported.

**MAC Layer**: MAC layer takes care of cell access related messages between UE and network. This random access procedure helps in establishing RRC connection.



Moreover MAC layer performs following functions:

* Mapping of logical channels to transport channels.
* Multiplexing of MAC SDUs from one or different logical channels onto transport blocks to be delivered to the physical layer on the UE side.
* Error correction through HARQ retransmission.
* Priority handling between UEs by means of dynamic scheduling.
* Logical Channel prioritization.
* Transport format selection and TB size selection.

**Topology**: The NB-IoT system is made up of a high number of connected objects over a wide geographical area, mesh network topology not only suffers from high deployment costs, but it also suffers from the ‘‘bottleneck problem’’. This is due to the fact that as the traffic is forwarded over multiple hops towards a gateway, some devices become more congested than others depending on their location or network traffic patterns. This results in shortening of their battery lifetime which limits the overall network lifetime to only a few months or years.

Therefore, most NB-IoT systems use the star network topology by connecting end devices directly to base stations obviating the need for the dense and expensive deployments of relays and gateways altogether. This technique results in huge energy savings. Compared to the mesh topology, the devices need not waste precious energy in busy-listening to other devices that want to relay their traffic through them. In the star topology used by most LPWAN technologies in general and also used by NB-IoT systems in particular, the base station is always kept switched ON in order to provide convenient and quick access when required by end-devices.

It is important to point out that although most LPWA technologies use the star topology, some of them do make use of a tree or mesh topology. However, the latter often require considerably complex protocol designs in order to achieve a similar energy efficiency performance to that of the star network topology.

**Security**: Within a NB-IoT network the data travels encrypted and therefore in a secure way. The problem with the information appears once the data leaves the NB-IoT network and is sent over the Internet, from the servers of the network operator to the final cloud server where the client has installed its reception center and data processing.

Typically, the NB-IoT uses UDP protocol. It is a very simple protocol and is ideal for NB-IoT because of its low consumption, because it does not need to establish a connection in order to send data. When a flat UDP packet travels over the Internet, all of its data is visible to third parties.

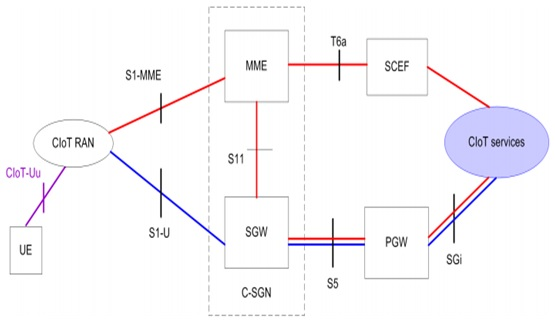
If we want to use one of the main features of NB-IoT: to have the lowest possible consumption of all LPWAN networks, we have to go through the UDP protocol and this is unsafe by nature. But we can still have low power consumption using UDP and ensure security in communications.

**Working Principle**: NB-IoT is a data transmission standard designed to enable devices to operate in mobile carrier networks. NB-IoT technology uses low bandwidth signals to communicate within existing GSM and LTE technologies.

Specially designed devices and sensors are the basic components in NB-IoT systems. These devices collect information from their surroundings and transmit it to NB-IoT base stations or transmission nodes. Individual base stations are connected to an IoT gateway and IoT cloud application servers for centralized monitoring and data analysis.

NB-IoT employs a new physical layer with signals and channels to meet the requirements of extended coverage in rural areas and deep indoors, while enabling very low device complexity. The underlying technology is much less complex than that of GSM/GPRS modules.

**Architecture**: There are two main parts in the NB-IoT architecture access network and core network. UEs are connected to eNBs (i.e. base stations) using Uu interface. The eNBs are connected together via the X2 interface. The eNBs are connected to the Core network side using the S1 interface. This S1 interface carries either NB-IoT control packets or data packets. Though NB-IoT does not support handover, X2-interface is used to enable fast resume from IDLE state of UE. One can refer to the RRC Connection Establishment Procedure to know more about different states of UE.



There are two optimizations used in CIoT (Cellular IoT) based architecture such as NB-IoT. Control plane is marked in red and the user plane is marked in blue. In NB-IoT a new node called SCEF is designed to handle machine type data. It is used for delivery of non-IP data over control planes. It also provides an abstract interface for the network services such as authentication, authorization, discovery and access network capabilities. Above depicts data transmission and reception:

* UL data is transmitted from eNB to MME. From there it may either follow SGW to PGW path or to SCEF path. From this node, they are forwarded to the application server for CIoT services.
* DL data is transmitted over the same paths but in the reverse direction.
* This LTE NB-IoT architecture does not require data radio bearer setup. Data packets are sent on signaling radio bearer instead. Hence this architecture based solution is most ideal for transmission of infrequent and small data packets.

**Applications**: NB-IoT can be used for the following applications:

* **Smart metering**: NB‑IoT works well for monitoring water and gas meters via regular and small data transmissions. Network coverage is a major problem in rolling out smart metering as meters are often installed in difficult locations, such as deep underground, in cellars or in remote rural areas. NB‑IoT coverage and penetration are able to address this issue.
* **Smart cities**: NB‑IoT can help local governments control street lighting, determine when trash bins must be emptied, identify free parking spaces, monitor environmental conditions and survey road conditions.
* **Smart buildings**: NB‑IoT connected sensors can send alerts to facilities managers regarding building maintenance issues. There are also indoor temperature monitoring systems that are based on NB-IoT sensors. NB‑IoT can serve to back up a building's broadband connection.
* **Tracking**: NB‑IoT provides a secure, inexpensive way to track people, animals and assets when continuous tracking isn't necessary. NB-IoT is good for tracking objects that may not be moving all the time.
* **Smart farming**: NB‑IoT connectivity enables farmers and cities to capture data from environmental sensors containing NB‑IoT modules that can send alerts if anything out of the ordinary happens. These sensors could be used to monitor the temperature and humidity of the soil, as well as to track the attributes of land, pollution, noise and rain.

**Pros and Cons**: The benefits of NB-IoT include:

* **Ubiquitous coverage and connectivity**: NB-IoT can help support massive numbers of devices by establishing NB-IoT networks that can connect to billions of nodes. Designed for extended coverage indoors, the lower complexity of the devices provides long-range connectivity and communication.
* **Low power consumption**: NB-IoT doesn't need to run a heavy operating system, such as Linux, or do a lot of signal processing, which makes it more power efficient compared to other cellular technologies.
* **Low cost of devices**: Because it's easier to create devices with lower complexity, the cost of the devices is significantly low, around $5 per module.
* **Multiyear battery life**: The enhanced power consumption capability enables NB-IoT to support a multiyear battery life for devices.
* **Security**: NB-IoT is secured much like 4G, including all encryption and SIM-based authentication features.

The barriers to NB-IoT becoming a norm include:

* **Limited device mobility**: NB-IoT devices only remain connected within a finite environment and only to one network operator. This could mean limitations for such uses as wearables that leave specific perimeters.
* **Limited data transmission**: Voice or video transmission is not an option because NB-IoT can only transmit less than a kilobyte of data per day, about equal to a text message.
* **Lacks proof of concept**: Because commercial rollouts have been relatively limited, it's hard to determine if the technology has been a success.

**Comparison with other protocol**: Short for long range, LoRa is a low-power, long-range wireless communication protocol developed by the LoRa Alliance, a nonprofit organization dedicated to standardizing LPWAN technologies as a secure, energy-efficient IoT standard.

Although NB-IoT and LoRa are both low-power wide area network technologies created for low-power devices, NB-IoT has a lower latency compared to LoRa because of the higher device output power, which can offer higher data rates.

NB-IoT operates in the licensed spectrum. However, it can be deployed in-band within a normal LTE carrier or stand-alone for deployments in dedicated spectrum. Because the channel width is very small, it allows the NB-IoT signal to bury inside a larger LTE channel, replace a GSM channel or exist in the guard channels of regular LTE signals.

LoRaWAN is a spread spectrum modulation technique designed to facilitate communication between low-power devices and IoT applications. The LoRa wireless system uses unlicensed frequencies available worldwide to communicate with a network.

# **7. IP and TCP**

**Standardization and alliances**: Transmission Control Protocol/Internet Protocol (TCP/IP) is a group of communications protocols used to send and receive data over the Internet. Most networks support TCP/IP. You can access Sterling B2B CollaborationNetwork using a TCP/IP communications protocol. Many Internet users are familiar with the protocols that use TCP/IP to get to the Internet: Hypertext Transfer Protocol (HTTP) File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP).

TCP/IP is a two-layer program. The higher layer Transmission Control Protocol disassembles data into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original data. The lower layer Internet Protocol handles the address part of each packet so it gets to the right destination.

**Physical Layer**: The Physical Layer is the lowest layer of the TCP/IP model. It deals with data in the form of bits. This layer mainly handles the host to host communication in the network. It defines the transmission medium and mode of communication between two devices. The medium can be wired or wireless, and the mode can be simplex, half-duplex, or full-duplex.

It also specifies the line configuration(point-to-point or multiport), data rate(number of bits sent each second), and topology in the network. There are no specific protocols that are used in this layer. The functionality of the physical layer varies from network-to-network. Physical layer of the TCP/IP model is responsible for physical connectivity of two devices. Some of the devices used in Physical layers are:

* **Hubs**: Hubs are devices commonly used to connect segments of a LAN. It contains multiple input/output ports. When a signal is at any input port, this signal will be made at all output ports except the one it is coming from.
* **Cables**: In Wired network architecture (e.g Ethernet), cables are used to interconnect the devices. Some of the types of cables are coaxial cable, optical fiber cable, and twisted pair cable.
* **Modem**: Modem stands for MOdulator/DEModulator. A modem converts digital signals generated by the computer into analog signals which, then can be transmitted over cable line and transforms incoming analog signals into digital equivalents.
* **Repeaters**: Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters can only amplify the signal whereas digital repeaters can reproduce a signal to near its original quality.

**MAC Layer**: The Data-Link Layer is the second layer of the TCP/IP layer. It deals with data in the form of data frames. It mainly performs the data framing in which it adds some header information to the data packets for the successful delivery of data packets to correct destinations. For this, it performs physical addressing of the data packets by adding the source and the destination address to it.

The data-link layer facilitates the delivery of frames within the same network. It also facilitates the flow and error control of the data frames. The flow of the data can be controlled through the data rate. Also, the errors in the data transmission and faulty data frames can be detected and retransmitted using the checksum bits in the header information.

The Data Link layer is responsible for transferring data hop by hop (i.e within the same LAN, from one device to another device) based on the MAC address. Some of the devices used in Data Link layer are:

* **Bridges**: A bridge is a type of computer network device that provides interconnection with other networks that use the same protocol, connecting two different networks together and providing communication between them.
* **Switch**: A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.
* **Network interface card**: Network interface card is an electronic device that is mounted on the ROM of the com that connects a computer to a computer network, usually a LAN. It is considered a piece of computer hardware. Most modern computers support an internal network interface controller embedded in the motherboard directly rather than provided as an external component.

**Topology**: TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of protocols independent of the physical medium used to transmit data, but most data transmission for Internet communication begins and ends with Ethernet frames.

The Ethernet can use either a bus or star topology. A bus topology attaches all devices in sequence on a single cable. In a star topology all devices are wired directly to a central hub. 10Base-T uses a combination called a star-shaped bus topology because while the attached devices can share all data coming in on the cable, the actual wiring is in a star shape.



The access method used by the Ethernet is called Carrier Sense Multiple Access with Collision

Detect (CSMA/CD). This is a contention protocol, meaning it is a set of rules to follow when there is competition for shared resources.

In a star-shaped bus topology, all systems have access to the network at any time. Before sending data, a system must determine if the network is free or if it is already sending a frame. If a frame is already being sent, a system will wait. Two systems can “listen” on the network and “hear” silence and then proceed to send data at the same time. This is called a collision. Ethernet hardware has collision detection sensors to take care of this problem. This is the Collision Detect (CD) part of CSMA/CD. The colliding data is ignored, and the systems involved will wait a random amount of time before resending their data.

**Security**: The security features provided with TCP/IP, both in standard mode and as a secure system, and discusses some security considerations that are appropriate in a network environment. Therefore, the security setup for TCP/IP is quite different.

* **Client security in a TCP/IP network**: Different connectivity scenarios call for using different levels of authentication. Therefore, an administrator can set the lowest security authentication method required by the client when connecting to a server by setting the preferred authentication method field in each RDB directory entry.
* **Server security in a TCP/IP network**: The TCP/IP server has a default security of user ID with clear-text password. This means that, as the server is installed, inbound TCP/IP connection requests must have at least a clear-text password accompanying the user ID under which the server job is to run.
* **Connection security protocols**: Several connection security protocols are supported by the current DB2 for implementation of distributed data management (DDM) or Distributed Relational Database Architecture (DRDA) over TCP/IP.
* **Secure Sockets Layer**: DB2 for Distributed Relational Database Architecture (DRDA) clients & servers support Secure Sockets Layer (SSL). A similar function is available with Internet Protocol Security Architecture (IPSec).
* **Internet Protocol Security Architecture**: Internet Protocol Security Architecture (IPSec) is a security protocol in the network layer that provides cryptographic security services. These services support confidential delivery of data over the Internet or intranets.
* **Considerations for certain passwords being sent as clear text**: Although the IBM i operating system supports the encryption of connection passwords, one of the connection security options you can specify in setting up an RDB directory entry is \*USRIDPWD.
* **Ports and port restrictions**: With the advent of new choices for the security of distributed data management (DDM) communications, the system administrator can restrict certain communications modes by blocking the ports they use. This topic discusses some of these considerations.

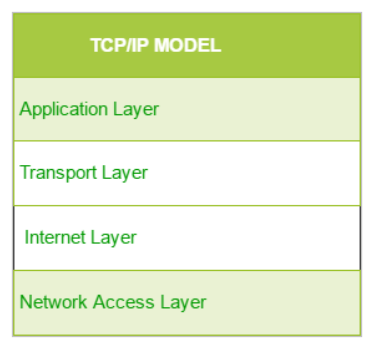
**Working Principle**: TCP/IP uses the client-server model of communication in which a user or machine (a client) is provided a service, like sending a webpage, by another computer (a server) in the network.

Collectively, the TCP/IP suite of protocols is classified as stateless, which means each client request is considered new because it is unrelated to previous requests. Being stateless frees up network paths so they can be used continuously.

The transport layer itself, however, is stateful. It transmits a single message, and its connection remains in place until all the packets in a message have been received and reassembled at the destination.

The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it. The OSI reference model defines how applications can communicate over a network.

**Architecture**: The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:



Network Access Layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

Internet Layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are:

* **IP**: It stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions which are IPv4 and IPv6.
* **ICMP**: It stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
* **ARP**: It stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

Host-to-Host Layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are:

* **Transmission Control Protocol (TCP)**: It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment features and controls the flow of the data through flow control mechanism.
* **User Datagram Protocol (UDP)**: On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is a connection-oriented protocol, UDP is connectionless.

Application Layer performs the functions of the top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Protocols other than those present in the linked article are :

* **HTTP and HTTPS**: HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer).
* **SSH**: SSH stands for Secure Shell. It is a terminal emulation software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
* **NTP**: NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions.

**Applications**: TCP/IP Protocols use both the server and client model of the communication in which it is a machine, or else the user is providing the services in computer networking. Some of the applications are:

* **Bootstrap Protocol**: Bootstrap Protocol (BOOTP) provides a dynamic method for associating workstations with servers. It also provides a dynamic method for assigning workstation Internet Protocol (IP) addresses and initial program load (IPL) sources.
* **Connecting to the Internet**: If you want to connect your IBM i operating system to an Internet service provider (ISP), or configure your operating system as a Web data server or application server, you can use the Internet Setup wizard to connect to the network.
* **Dynamic Host Configuration Protocol**: Dynamic Host Configuration Protocol (DHCP) is a TCP/IP standard that uses a central server to manage IP addresses and other configuration details for an entire network.
* **REXEC**: The remote execution server is having the transmission control protocols or else IP applications that will allow the client users to submit their remote system. It will enable the processing of both the programs and also a command to hosting on the internet.
* **Virtual Private Networking**: As a matter of fact it enables the stable ad to enlarge their private process over the existing framework of a public processor. Such as the VPN companies are controlling the networking traffic while providing the essential security types, i.e. data privacy.

**Pros and Cons**: The advantages of using the TCP/IP model include the following:

* Helps establish a connection between different types of computers.
* Works independently of the OS.
* Supports many routing protocols.
* Uses client-server architecture that is highly scalable.
* Can be operated independently.
* Supports several routing protocols.
* It is lightweight and doesn't place unnecessary strain on a network or computer.

The disadvantages of TCP/IP include the following:

* It is complicated to set up and manage.
* Transport layer does not guarantee delivery of packets.
* It is not easy to replace protocols in TCP/IP.
* It does not clearly separate the concepts of services, interfaces and protocols, so it is not suitable for describing new technologies in new networks.
* It is especially vulnerable to a synchronization attack, which is a type of denial-of-service attack in which a bad actor uses TCP/IP.

**Comparison with other protocol**: IP is limited by the amount of data that it can send. The maximum size of a single IP data packet, which contains both the header and the data, is between 20 and 24 bytes long. In contrast to IP, TCP/IP is a higher-level smart communications protocol that can do more things. TCP/IP still uses IP as a means of transporting data packets, but it also connects computers, applications, web pages and web servers.

As it does its work, TCP can also control the size and flow rate of data. It ensures that networks are free of any congestion that could block the receipt of data.

An example is an application that wants to send a large amount of data over the internet. If the application only used IP, the data would have to be broken into multiple IP packets. This would require multiple requests to send and receive data, since IP requests are issued per packet.

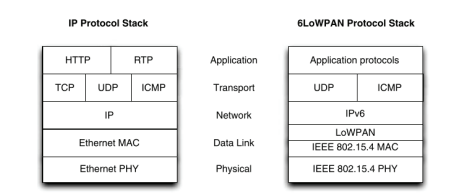
With TCP, only a single request to send an entire data stream is needed; TCP handles the rest. Unlike IP, TCP can detect problems that arise in IP and request retransmission of any data packets that were lost. TCP can also reorganize packets so they get transmitted in the proper order and it can minimize network congestion. TCP/IP makes data transfers over the internet easier.

# **8. 6LoWPAN**

**Standardization and alliances**: The 6LoWPAN group defined encapsulation, header compression, neighbor discovery and other mechanisms that allow IPv6 to operate over IEEE 802.15.4 based networks. Although IPv4 and IPv6 protocols do not generally care about the physical and MAC layers they operate over, the low power devices and small packet size defined by IEEE 802.15.4 make it desirable to adapt to these layers.

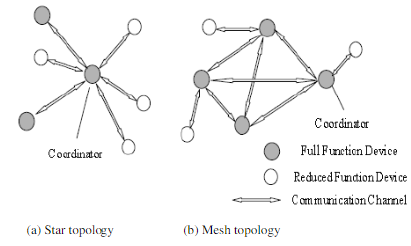
6LoWPAN standards enable the efficient use of IPv6 over low-power, low-rate wireless networks on simple embedded devices through an adaptation layer and the optimization of related protocols. The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices," and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.

**Physical Layer**: The physical layer converts data bits into signals that are transmitted and received over the air. In the 6LoWPAN example, IEEE 802.15.4 is used. In addition to the well-rounded 2006 version of the standard, two important amendments exist e and g. IEEE 802.15.4e is a MAC amendment and provides enhancements such as time slotted channel hopping (TSCH) and coordinated sampled listening (CSL). Both enhancements aim to further lower the power consumption and make the interface more robust. The IEEE 802.15.4g is a PHY (or physical layer) amendment and aims to provide an additional range of radio frequency bands to enable worldwide use even in the Sub-1 GHz frequency bands.



**MAC Layer**: The data link layer provides a reliable link between two directly connected nodes by detecting and correcting errors that may occur in the physical layer during transmission and receiving. The data link layer includes the media access layer (MAC) which provides access to the media, using features like carrier sense multiple access – collision avoidance (CSMA-CA) where the radio listens that no one else is transmitting before actually sending data over the air. This layer also handles data framing. In the 6LoWPAN example, the MAC layer is IEEE 802.15.4. The 6LoWPAN adaptation layer, providing adaptation from IPv6 to IEEE 802.15.4, also resides in the link layer.

**Topology**: 6LoWPAN supports both star and mesh network topology. Below shows the star and mesh network topology in 6LoWPAN. In a star network, the PAN coordinator is always one hop away from any sensor node because every node is directly connected with the PAN coordinator and there is no need for mesh header related fields in the 6LoWPAN header. However, in mesh topology, the 6LoWPAN adaptation layer needs an extra header to keep the originator and final destination address while the IEEE 802.15.4 MAC layer carries the source and destination node address that change at each hop.



For the routing aspect in 6LoWPAN, AODV has been considered as a strong candidate for 6LoWPAN. It enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network. A distinguishing feature of AODV is its use of destination sequence number for each route entry. For route discovery, AODV uses Route Requests (RREQs) messages and Route Replies (RREPs) messages. RREQ that is broadcast by the originator node contains the sequence number for route choosing purpose. RREP is to be unicast from the destination node or the intermediate node to the originator node to make the route available.

**Security**: State-of-the-art security schemes are necessary to be ahead of the pack. 6LoWPAN takes advantage of the strong AES-128 link layer security defined in IEEE 802.15.4. The link layer security provides link authentication and encryption. In addition to link layer security, transport layer security (TLS) mechanisms have been shown to work great in 6LoWPAN systems. TLS, as defined in RFC 5246, runs over TCP. For constrained environments and systems where UDP is chosen as the transport layer protocol, the RFC 6347 (datagram transport

layer security) can be used to provide security at the transport layer.

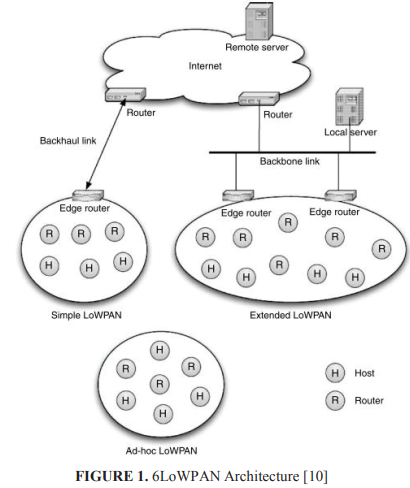
However, it should be noted that implementing TLS/DTLS requires the device to have necessary resources, such as a hardware encryption engine to enable the use of advanced cipher suites, etc. A device especially developed for this purpose is TI’s CC2538 wireless MCU, which integrates a powerful ARM® Cortex®-M3 CPU and an IEEE 802.15.4 radio. The device has up to 512kB Flash and 32kB RAM, and also features a hardware encryption engine capable of supporting TLS/DTLS

**Working Principle**: 6LoWPAN is an IPv6 protocol, and It’s extended from IPv6 over Low Power Personal Area Network. As the name itself explains the meaning of this protocol is that this protocol works on Wireless Personal Area Network i.e., WPAN.

IPv6 is Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. It is faster and more reliable and provides a large number of addresses. 6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks. It provides end-to-end IPv6 and as such it is able to provide direct connectivity to a huge variety of networks including direct connectivity to the Internet.

6LoWPAN initially came into existence to overcome the conventional methodologies that were adapted to transmit information. But still, it is not so efficient as it only allows for the smaller devices with very limited processing ability to establish communication using one of the Internet Protocols, i.e., IPv6. It has very low cost, short-range, low memory usage, and low bit rate.

**Architecture**: 6LoWPAN is a protocol specification to enable IPv6 standards to be used in low-power wireless networks, specifically with IEEE 802.15.4. The IETF 6LoWPAN working group maintains it. The rationale for introducing 6LoWPAN is that the existing IPv6 is too bulky for WSN. In 6LoWPAN, the IPv6 header is compressed to only a few bytes by introducing an adaptation layer that resides between network and MAC/PHY layer while retaining the main IPv6 functionality.



The 6LoWPAN architecture is made up of low-power wireless area networks (LoWPANs), which are IPv6 subnetwork. It means a LoWPAN is the collection of 6LoWPAN nodes, which share a common IPv6 address prefix (the first 64-bits of an IPv6 address). LoWPAN nodes may play the role of host or router, along with one or more edge routers. The transmission of 1280 bytes IPv6 Maximum Transmission Unit (MTU) over IEEE 802.15.4 is also made possible using fragmentation and reassembly provided by this adaptation layer. The detailed specification of this protocol is described in IETF standard RFC4944.

There are three types of LoWPANs which are Simple LoWPANs, Extended LoWPANs, and Ad hoc LoWPANs. A Simple LoWPAN is connected through one LoWPAN Edge Router to another IP network. An Extended LoWPAN consists of multiple edge routers along with a backbone link to interconnect them. An Ad hoc LoWPAN is not connected to the Internet and operates without an infrastructure.

**Applications**: While there are many forms of wireless networks including wireless sensor networks, 6LoWPAN addresses an area that is currently not addressed by any other system, for example, that of using IP, and in particular IPv6 to carry the data.

The overall system is aimed at providing wireless internet connectivity at low data rates and with a low duty cycle. However, there are many applications where 6LoWPAN is being used:

* **Automation**: There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
* **Industrial monitoring**: Industrial plants and automated factories provide a great opportunity for 6LoWPAN. Major savings can be made by using automation in everyday practices. Additionally, 6LoWPAN can connect to the cloud which opens up many different areas for data monitoring and analysis.
* **Smart Grid**: Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator’s monitoring and billing system using the IPv6.
* **Smart Home**: By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

**Pros and Cons**: Following are the benefits or advantages of 6LoWPAN:

* 6LoWPAN is a mesh network which is robust, scalable and self healing.
* It offers a long range of communication which detects signals below noise level.
* It consumes less power as it uses reduced transmission time (using short time pulses). Hence this saves energy and consecutively the battery can be used for a very long duration.
* It offers a large network which can be used by millions of devices.
* It delivers low cost and secure communication in IoT devices.
* It offers one to many and many to one routing. Hence transparent internet integration is possible.
* It uses IPv6 protocol and hence can be routed directly to cloud platforms.

Following are the drawbacks or disadvantages of 6LoWPAN:

* It is less secure than zigbee.
* It has less immunity to interference than wifi or bluetooth devices.
* It supports short range without mesh topology.

**Comparison with other protocol**: The comparative study of ZigBee standard and 6LoWPAN reveals that 6LoWPAN adds IP functionality to WPANs and consumes little power, while ZigBee supports many more nodes operates at low power and requires a low cost. ZigBee can be used in HAN networks, as well as for smart metering, if it is used in a mesh structure. It can also provide remote intelligent meter monitoring and other devices.

ZigBee has reliable security and uses powerful encryption techniques. It has a networking technique far superior to that of other technologies that avoids the collision of channels. On the other hand, 6LoWPAN is suitable for IP-based low power devices such as sensors and controllers. The main attributes of these technologies have been summarized in Table 2. In terms of power consumption, 6LoWPAN and ZigBee are designed for portable devices and limited battery power. Thus, it offers low power consumption.

In the context of the comparison between ZigBee IP and 6LoWPAN, ZigBee IP is considered the first open standard of ZigBee compatible with IPv6 protocol. It provides seamless connection with low-power, low-cost devices. The 6LoWPAN adaptation layer built into ZigBee IP ensures interoperability between the link layer defined by the 802.15.4 standard and the network layer that supports IPv6, this is to bind any which device to the internet.

# **9. Cellular Connectivity LTE**

**Standardization and alliances**: LTE is a packet switch IP technology based on OFDM digital modulation scheme to supports channels bandwidth up to 20 MHz and antenna techniques with multiple-input multiple-output (MIMO), such that multiple data streams are delivered and received on a given frequency time by multiple antennas.

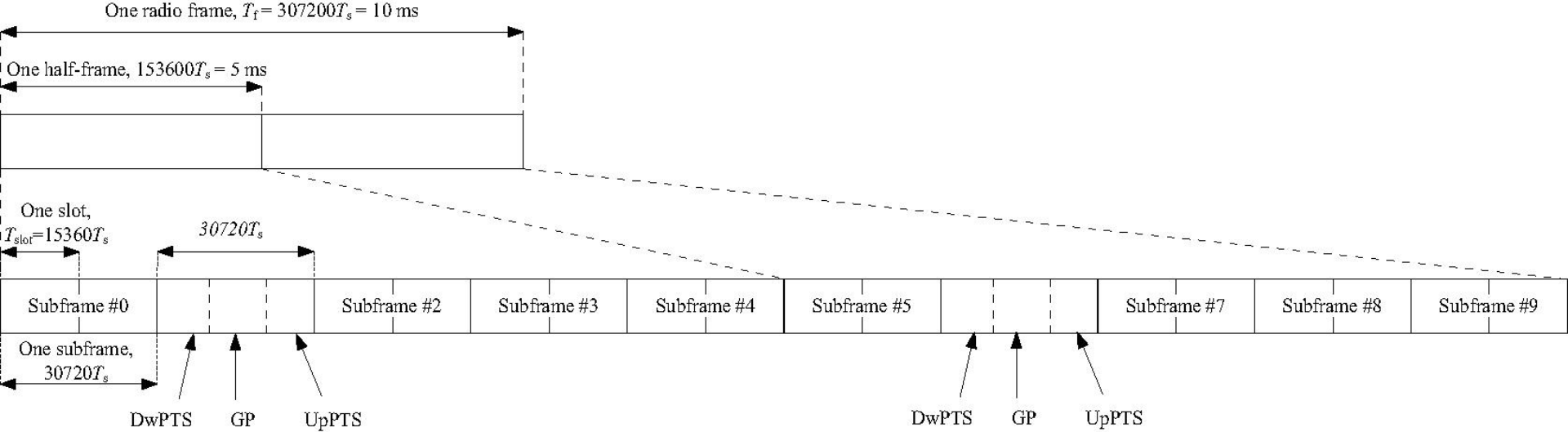
The standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9. LTE is also called 3.95G and has been marketed as "4G LTE" and "Advanced 4G" but it does not meet the technical criteria of a 4G wireless service, as specified in the 3GPP Release 8 and 9 document series for LTE Advanced.

The requirements were set forth by the ITU-R organization in the IMT Advanced specification but, because of market pressure and the significant advances that WiMAX, Evolved High Speed Packet Access, and LTE bring to the original 3G technologies, ITU later decided that LTE and the aforementioned technologies can be called 4G technologies.

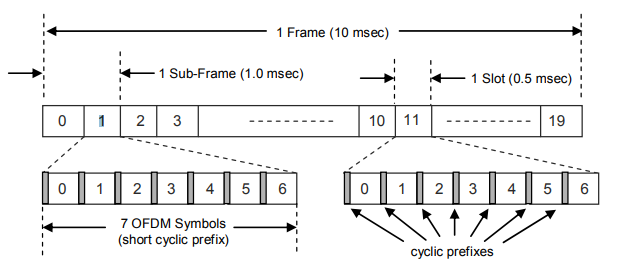
**Physical Layer**: Physical Layer carries all information from the MAC transport channels over the air interface. Takes care of the link adaptation (AMC), power control, cell search (for initial synchronization and handover purposes) and other measurements (inside the LTE system and between systems) for the RRC layer.

The LTE physical layer supports two types of frame structures as types 1 and 2. The type 1 structure is used for Frequency Division Duplex (FDD) mode however, the type 2 structure is applied to Time Division Duplex (TDD) mode maintaining only full duplex operation. Type 1 lasts 10 ms equivalent to 10 subframes (each 1 ms long) or 20 slots (each 0.5 ms long). As in FDD, each frame consists of 10 subframes of 1 ms long and each subframe consists of two concatenated slots of 0.5 ms long. The radio frame used in TDD mode (type 2) also has a length of 10 ms, but it is divided into two half-frames of length 5 ms. Just like the FDD, each subframe of type 2 frame structure also consists of two slots of length 0.5 ms. The special subframe in each half-frame includes three fields DwPTS (Downlink Pilot Time Slot), GP (Guard Period) and UpPTS (Uplink Pilot Time Slot).



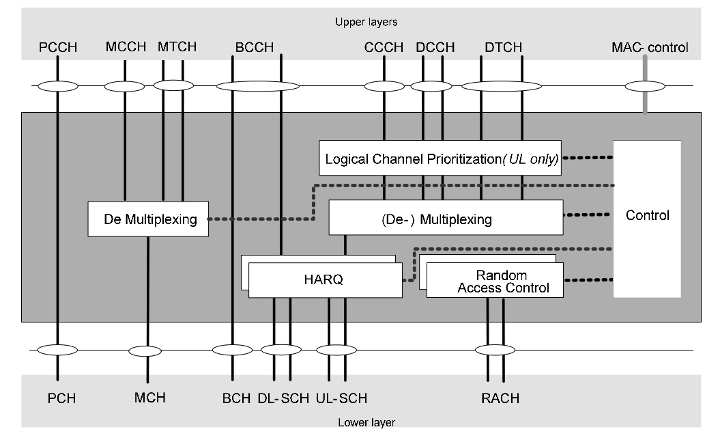


The capabilities of the eNodeB and UE are obviously quite different. Not surprisingly, the LTE PHY DL and UL are quite different. The DL and UL are treated separately within the specification documents. Therefore, the DL and UL are described separately in the following sections.



One element shared by the LTE DL and UL is the generic frame structure. As mentioned previously, the LTE specifications define both FDD and TDD modes of operation. This paper deals exclusively with describing FDD specifications. The generic frame structure applies to both the DL and UL for FDD operation.

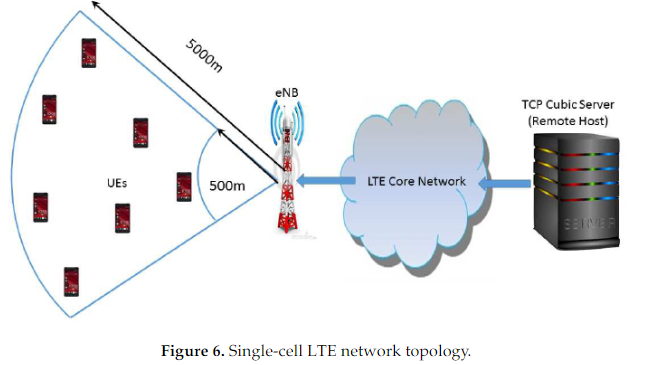
**MAC Layer**: MAC layer is responsible for Mapping between logical channels and transport channels, Multiplexing of MAC SDUs from one or different logical channels onto transport blocks (TB) to be delivered to the physical layer on transport channels, de multiplexing of MAC SDUs from one or different logical channels from transport blocks (TB) delivered from the physical layer on transport channels, Scheduling information reporting, Error correction through HARQ, Priority handling between UEs by means of dynamic scheduling, Priority handling between logical channels of one UE, Logical Channel prioritization.



E-UTRA defines two MAC entities; one in the UE and one in the E-UTRAN. Here is how it looks for the user plane and control plane. The MAC layer is composed of a Hybrid Automatic Repeat request (HARQ) entity, a multiplexing/demultiplexing entity, a logical channel prioritization entity, and a control entity. MAC layer performs the following functions:

* Mapping between logical channels and transport channels
* Multiplexing of MAC SDUs from one or different logical channels onto transport blocks (TB) to be delivered to the physical layer on transport channels
* Demultiplexing of MAC SDUs from one or different logical channels from transport blocks (TB) delivered from the physical layer on transport channels
* Scheduling information reporting
* Error correction through HARQ
* Priority handling between UEs by means of dynamic scheduling and between logical channels of one UE

**Topology**: In order to systematically explore the interactions between the AQM-based buffer management and scheduling algorithm, we have to delve deeper to consider mobile network elements and protocols. We used the LTE/EPC Network Simulator and Analysis (LENA) module to create an end-to-end LTE network. The LENA module has all the major elements of a real LTE system including the Evolved Packet Core (EPC) and air interface Evolved UMTS Terrestrial Radio Access(E-UTRA). The LTE model in ns3 provides a detailed implementation of various aspects of the LTEstandard such as adaptive modulation and coding, Orthogonal Frequency Division Multiple Access (OFDMA), hybrid Automatic Repeat Request (ARQ) etc.



The guaranteed bit rate video trafﬁc is simulated, the remote host on the right side acts as sources,and the UEs on the left side act as sinks. TCP data senders are of the TCP-Cubic type. We used TCP-Cubic as it is the default TCP congestion control algorithm in Linux OS in real networks. The TCPpacket sizes are 1000 bytes.

**Security**: The typical services are voice and/or data used by the users. Different systems employ security in different ways. As we know, the LTE network consists of various system elements connected using various interfaces. The network elements are UE, eNB, MME, HSS and AuC. Following to be considered in order to provide LTE security. Nodes should be able to exchange signaling data and user data securely. Following vulnerable positions should be made secure in the LTE system.

* Protection at the LTE network access interfaces as mentioned.
* Protection on the wireline network.
* Secured access to mobile stations by the user domain.
* Enable application domain security for applications and messages.
* Provide provision to the user to configure the security feature. This helps users know whether the security is supported or not by the network service provider.

**Working Principle**: LTE transports big data packets to an internet protocol system (IPS). The previous generations of data transmission standards. The global system for mobile communications (GSM) and code-division multiple access (CDMA) only carried small quantities of data compared to LTE.

LTE allows you to transfer far more data and improves your service. Conventional phone calls are only available in 2G and 3G networks through the circuit-switched portion of the network. LTE is a revamped version of the 3G standard designed to meet the need for high-speed data transmission in the age of hyperconnectivity. The revamp incorporates the following features:

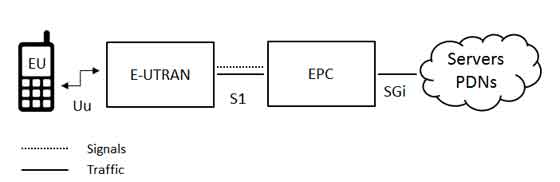
* A core network based on IP addresses
* A network architecture that has been simplified
* A brand-new radio user interface
* A novel modulation technique

The main advantage of LTE is that it minimizes data transmission delay. Time delay duplex (TDD) is used by GSM, whereas code division duplex (CDD) is used by CDMA. They are both ways of encoding data for transmission over radio waves, and although CDD has shown to be speedier in experimental environments, the world still runs on GSM technology.

**Architecture**: The high-level network architecture of LTE is comprised of following three main components:

* The User Equipment (UE).
* The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
* The Evolved Packet Core (EPC).

The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below



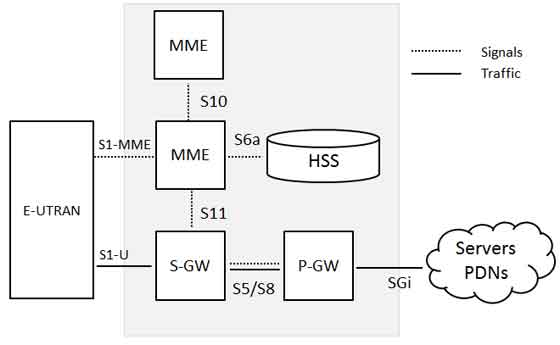
The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME). The mobile equipment comprised of the following important modules:

* **Mobile Termination (MT)**: This handles all the communication functions.
* **Terminal Equipment (TE)**: This terminates the data streams.
* **Universal Integrated Circuit Card (UICC)**: This is also known as the SIM card for LTE equipment. It runs an application known as the Universal Subscriber Identity Module (USIM).

The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called eNodeB or eNB. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB. LTE Mobile communicates with just one base station and one cell at a time and there are following two main functions supported by eNB:

* The eBN sends and receives radio transmissions to all the mobiles using the analogue and digital signal processing functions of the LTE air interface.
* The eNB controls the low-level operation of all its mobiles, by sending them signaling messages such as handover commands.

The architecture of Evolved Packet Core (EPC) has been illustrated below. There are a few more components which have not been shown in the diagram to keep it simple. These components are like the Earthquake and Tsunami Warning System (ETWS), the Equipment Identity Register (EIR) and Policy Control and Charging Rules Function (PCRF).



The interface between the serving and PDN gateways is known as S5/S8. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

**Applications**: Systems are employed in almost every industry. The critical LTE-enabled internet of things (IoT) use cases include:

* **Transport**: Buses, passenger trains, and other types of public transportation rely on LTE data and connections to deliver data on vehicle performance, passenger levels, and passenger Wi-Fi to dispatchers and network administrators.
* **Smart cities**: Smart lighting for streets and public spaces, charging stations for electric cars, and high-speed LTE systems that connect traffic signals to drive real-time adaptive traffic control are a few smart city applications that use LTE technology.
* **Industrial applications**: In industrial applications, wireless Ethernet technologies such as Wi-Fi or low-bandwidth 900 MHz systems can be difficult and expensive to implement.
* **Precision agriculture**: LTE-enabled irrigation equipment and other infrastructural facilities can save farmers substantial time and money. This ensures the reliability of agricultural data transfer, access to farm information fusion, and real-time control transmission of information back to intelligent terminals.
* **Waste management**: IoT apps with LTE connections allow wireless surveillance for wells, lift channels, sewers, and other water supply and wastewater system components 24 hours a day, 7 days a week.

**Pros and Cons**: Following are the advantages of LTE:

* Data, as well as voice, can be exchanged between participants. This is because LTE supports packet switching.
* High amounts of data can be transferred between the sender and the receiver.
* All data exchange occurs with very less power consumption. This leads to a better life for smartphone batteries.
* It has a high speed of file upload and download.
* It releases the network usage faster. This decreases the load on the network.

Following are the disadvantages of LTE:

* This service is not currently available in all cities.
* More towers and fresh technologies need to be developed for better signals while in transit e.g., in buses and trains.
* LTE being complex needs only skilled people to manage the system. They even need to be paid a higher salary.
* This technology cannot be used in old versions of smartphones.
* Buying new smartphones for LTE is a costly affair.

**Comparison with other protocol**: Global System for Mobile communication mobile network widely used by mobile phone users around the world. In this, the information of the customer is put on a sim card that can be carried in the new mobile handset. It is operated on either 900 MHz or 1, 800 MHz frequency band. In GSM, two technologies are used which are: FDMA and TDMA. Long Term Evolution is a standard for high-speed data communication. It delivers download speeds of around 100 Mbps and upload speeds of around 50 Mbps. It does not deliver good voice call quality while using the data services. It needs a sim card to validate the handset.

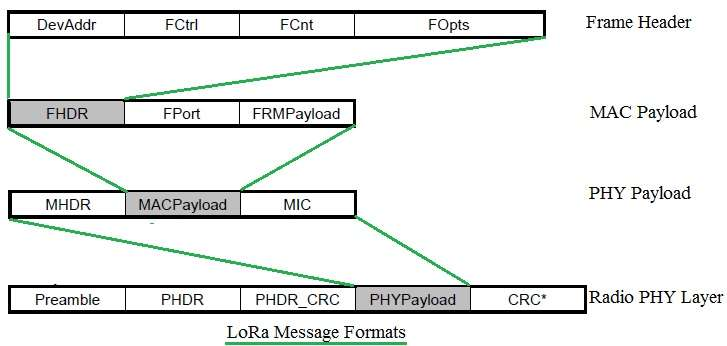
In GSM, information is transported through channels that are separated into physical and logical channels. Whereas in LTE, information is carried out using physical, logical, and transport channels. GSM is used for voice calls, GPRS, and data communications, and it includes new capabilities including SAIC, VAMOS, and MSRD. LTE is designed for data calls and includes MIMO, carrier aggregation, beamforming, and enhanced release ten versions.

# **10. LoRa**

**Standardization and alliances**: LoRa is an RF modulation technology for low-power, wide area networks (LPWANs). The name, LoRa, is a reference to the extremely long-range data links that this technology enables. Created by Semtech to standardize LPWANs, LoRa provides for long-range communications: up to three miles (five kilometers) in urban areas, and up to 10 miles (15 kilometers) or more in rural areas (line of sight).

A key characteristic of the LoRa-based solutions is ultra-low power requirements, which allows for the creation of battery-operated devices that can last for up to 10 years. The patented LoRa wireless radio frequency technology stands for the physical layer protocol while LoRaWAN, developed by the LoRa Alliance, stands for the media access control layer protocol, which leverages and includes the physical LoRa modulation of Semtech.

**Physical Layer**: LoRa RF physical layer uses a form of spread spectrum modulation. The LoRa modulation scheme uses wide-band linear frequency modulated pulses. The level of frequency increase or decrease over time is used to encode the data to be transmitted, i.e. a form of chirp modulation.



This form of modulation enables LoRa wireless systems to demodulate signals that are 20dB below the noise floor when the demodulation is combined with forward error correction, FEC. This means that the link budget for a LoRa system can provide an improvement of more than 25dB when compared to a traditional FSK system.

Following are the functions of LoRa Physical Layer (PHY):

* Physical Layer constructs the frame in order to transmit payload from MAC layer over RF link.
* It inserts PHDR, PHDR\_CRC, preamble and CRC for the entire frame. CRC field is available in uplink message only.
* As a preamble specific constant sync words are used based on modulation technique either LORA, GFSK or FSK. This preamble will help in synchronization at the receiver as it is known to the receiver.
* PHY layer uses specific RF bands as per countrywide requirement.

**MAC Layer**: The packet processed in the MAC layer consists of a MAC Header , a MAC Payload, and a Message Integrity Code (MIC). MAC header defines protocol version and message type, i.e., whether it is a data or a management frame, whether it is transmitted in uplink or downlink, whether it shall be acknowledged.

MAC Header can also notify that this is a vendor specific message. In a join procedure for end node activation, the MAC Payload can be replaced by join request or join accept messages. The entire MAC Header and MAC Payload portion is used to compute the MIC value with a network session key (Nwk\_SKey). The MIC value is used to prevent the forgery of messages and authenticate the end node.



Following MAC messages are used in LoRa for establishing communication between end device and server.

* Join request (From End device to Server)
* Join accept (from network server to End device)
* Beacon frame (from gateway to End device) for scheduling slot for reception by End devices.
* Confirmed Data Up/Down (These messages are to be acknowledged by LoRa receiver)
* Unconfirmed Data Up/Down (These messages do not require any ack).

**Topology**: LoRa uses a star topology. For long range, star architecture makes the most sense for preserving battery lifetime when long-range connectivity can be achieved. The nodes in a LoRa network are asynchronous and communicate when they have data ready to send whether event-driven or scheduled.

This type of protocol is typically referred to as the Aloha method. In a mesh network or with a synchronous network, such as cellular, the nodes frequently have to ‘wake up’ to synchronize with the network and check for messages. This synchronization consumes significant energy and is the number one driver of battery lifetime reduction. In a recent study and comparison done by GSMA of the various technologies addressing the LPWAN space, LoRa showed a 3 to 5 times advantage compared to all other technology options.

**Security**: Any communication technology dealing with many connected nodes needs robust end-to-end security. LoRa achieve this by implementing security at two different layers:

* One for the network
* One for the application

Network security ensures authenticity of the node in the network and application security ensures the operator does not have access to end user’s application data. LoRa uses AES (Advanced Encryption Standard) security keys. To achieve the required levels of security for LoRa networks, several layers of encryption have been employed:

* Unique Network key (EUI64) and ensure security on network level
* Unique Application key (EUI64) ensure end to end security on application level
* Device specific key (EUI128)

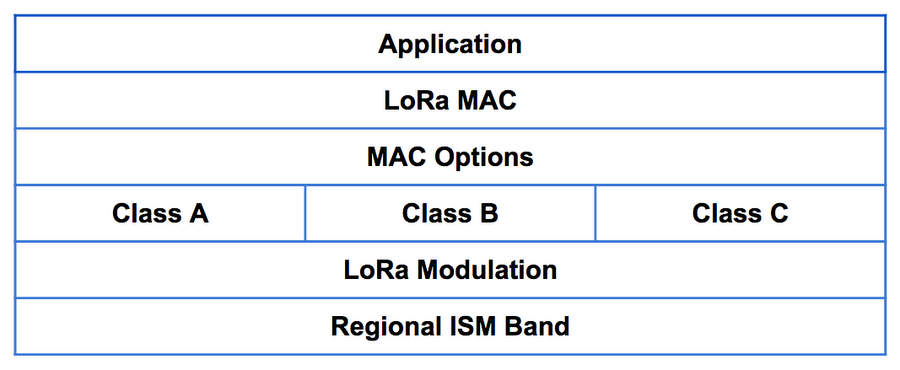
The LoRa Alliance has always kept security front and center in its development of the LoRaWAN specification and has been highly transparent about the protocol’s security features. The LoRaWAN specification has been designed from the outset with security as an essential aspect, providing state-of-the-art security properties that meet the needs of highly scalable low-power IoT networks. Unlike many other IoT technologies, the LoRaWAN specification already offers dedicated end-to-end encryption to application providers.

**Working Principle**: LoRa is a wireless modulation technique derived from Chirp Spread Spectrum (CSS) technology. It encodes information on radio waves using chirp pulses similar to the way dolphins and bats communicate. LoRa modulated transmission is robust against disturbances and can be received across great distances.

LoRa is ideal for applications that transmit small chunks of data with low bit rates. Data can be transmitted at a longer range compared to technologies like WiFi, Bluetooth or ZigBee. These features make LoRa well suited for sensors and actuators that operate in low power mode.

LoRa can be operated on the license free sub-gigahertz bands, for example, 915 MHz, 868 MHz, and 433 MHz. It also can be operated on 2.4 GHz to achieve higher data rates compared to sub-gigahertz bands, at the cost of range. These frequencies fall into ISM bands that are reserved internationally for industrial, scientific, and medical purposes.

**Architecture**: LoRa network uses a star topology in which an end node can send messages to multiple gateways that communicate with the network server. Since an end node does not belong to a specific gateway, more than one gateway can receive a message sent by an end device. LoRa radio access technology is used in communications between an end device and the gateways. The gateways and network server are connected via standard IP connections.



The LoRa network consists of several elements.

* **LoRa Nodes/End Points**: LoRa end points are the sensors or application where sensing and control takes place. These nodes are often placed remotely. Examples, sensors, tracking devices, etc.
* **LoRa Gateways**: Unlike cellular communication where mobile devices are associated with the serving base stations, LoRaWAN nodes are associated with a specific gateway. Instead, any data transmitted by the node is sent to all gateways and each gateway which receives a signal transmits it to a cloud based network server.
* **Network Servers**: The network server has all the intelligence. It filters the duplicate packets from different gateways, does security checks, and sends ACKs to the gateways. In the end if a packet is intended for an application server, the network server sends the packet to the specific application server.
* **Application Server**: An Application Server is the end server where all data sent by End Device is post processes and necessary action being taken.

**Applications**: LoRa can be used on a great many different applications where long-distance device communication and cabling cost reduction are required in an efficient way. Even so, there are five applications where LoRa is truly beneficial at the level of both performance and cost reduction.

* **Smart agriculture**: LoRa technology can be used in smart agriculture and farming applications by helping in smart farming and livestock management, temperature and moisture monitoring and checking water level sensors and irrigation control.
* **Smart buildings**: In the future, billions of smart devices and home appliances will be connected to the internet. It helps in enhanced home security and home automation for IoT enables smart appliances
* **Smart energy**: Smart energy metering deserves its own section as one of the best applications for LoRa technology. With no need of installing cables, LoRa™ allows to collect data from energy meters along huge areas and installations where submetering is required.
* **Solar power generation**: It is important to remember that one of the LoRa ’s main strengths is the low consumption that is required to collect and send data which is ideal for applications powered by batteries or 12/24 Vdc power supplies. Kilometers of solar panels being wireless monitored using low consumption devices.
* **Smart water and gas monitoring**: Water and gas monitoring is a sector that has been waiting a long time for a technology such as LoRa to minimize costs and maximize efficiency on their automation solutions. It meets the requirements of high penetration and low cost technology to control wells, pumps, pipes, silos, irrigation and water treatment.

**Pros and Cons**: Currently, one of the most representative communication technologies in low-power wide area networks is used in various industries. Following are the advantages of LoRa:

* **Long transmission distance**: Sensitivity -148dBm, communication distance up to 15 kilometers.
* **Low working energy consumption**: Aloha method only connects when there is data, and the battery can work for several years.
* **Multiple network nodes**: Flexible networking mode, multiple nodes can be connected.
* **Strong anti-interference**: The protocol has the function of LBT, based on the aloha method, with automatic frequency jump and rate adaptation functions.
* **Low cost**: Unlicensed spectrum, low node/terminal cost shortcoming.

Following are the disadvantages of LoRa:

* **Spectrum interference**: With the continuous development of LoRa, LoRa equipment, and network deployment continue to increase, and certain spectrum interference will occur between each other.
* **Need to build a new network**: During the LoRa deployment process, users need to build their own network.
* **Small payload**: The payload of LoRa transmission data is relatively small and has a byte limit.

**Comparison with other protocol**: LoRa has a star topology, which means each node needs to communicate directly with a gateway and is used for low cost sensing applications. LoRa is well suited for simple sensing applications, where sensors are battery powered and have slow poll rates (data update rate) in the range of a few times per day up to 2-5 minute intervals.

Zigbee has a more flexible, reliable and expandable mesh network topology, built for reliability with ‘self-healing’ capabilities and nodes that can communicate with any other node on the mesh network, multi-hopping for very long distances and used for monitoring, control and automation applications. Zigbee is also low power and with the correct device design, is ideal for battery operated sensing applications, including applications requiring high speed polling and high reliability, such as control/automation in addition to real-time sensing requirements such as equipment condition monitoring or process instrumentation.

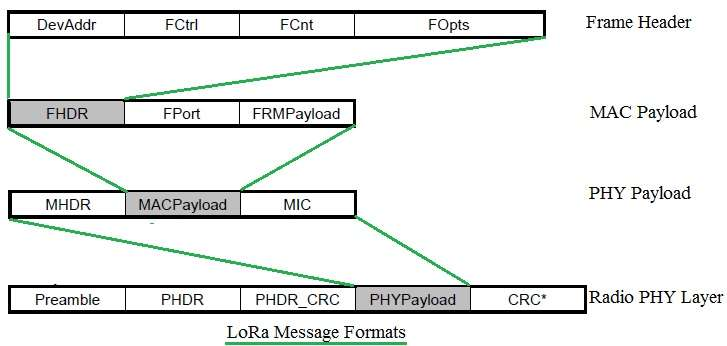
LoRa might have received a lot more media attention in recent years, as compared with Zigbee, however they are both low power IoT networks and Zigbee also has long range options that can rival the distances of LoRa or even exceed the range with multi-hopping in the mesh networks. Zigbee is also a more reliable protocol, with a longer standing history in industry, used for both monitoring and control, whereas LoRa is limited to the use of low cost, low power sensing.

# **11. LoRaWAN**

**Standardization and alliances**: Long range wide area networking (LoRaWAN), a communications system for connecting internet of things (IoT) devices at long distances, has been formally approved as a standard by the International Telecommunication Union (ITU), the United Nations agency for information and communication technologies.

The standard, named Recommendation ITU-T Y.4480, is for low power protocols for wide area wireless networks and is under the responsibility of Study Group 20 of the ITU Telecommunication Standardization Sector for IoT and smart cities and communities. Designed to wirelessly connect battery operated things to the internet in regional, national or global networks, the LoRaWAN standard meets key Internet of Things (IoT) requirements such as bidirectional communication, end-to-end security, mobility, and geolocation services.

**Physical Layer**: Physical Layer constructs the frame in order to transmit payload from MAC layer over RF link. It inserts PHDR, PHDR\_CRC, preamble and CRC for the entire frame. CRC field is available in uplink message only.

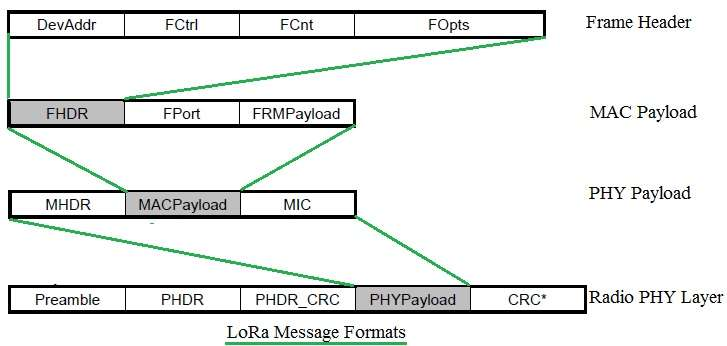


LoRa uses wideband linear frequency modulated chirp pulses to encode information bits. Chirp is called sweep signal which is a tone in which frequency increases with time (called up-chirp) or decreases with time (called down-chirp). In up-chirp frequency increases in time and in down-chirp frequency decreases in time. These chirp signals are used as carrier signals where a message is encoded on. Following figure depicts encoding of messages on chirp signals. As shown the starting part is a preamble sequence followed by two down chirps and encoded payload.

The PHY layer passes the modulated signal to the RF transceiver for up conversion to higher frequencies as per country specific LoRaWAN bands. Similarly down conversion is carried out at the other end before demodulation to raw information bits.

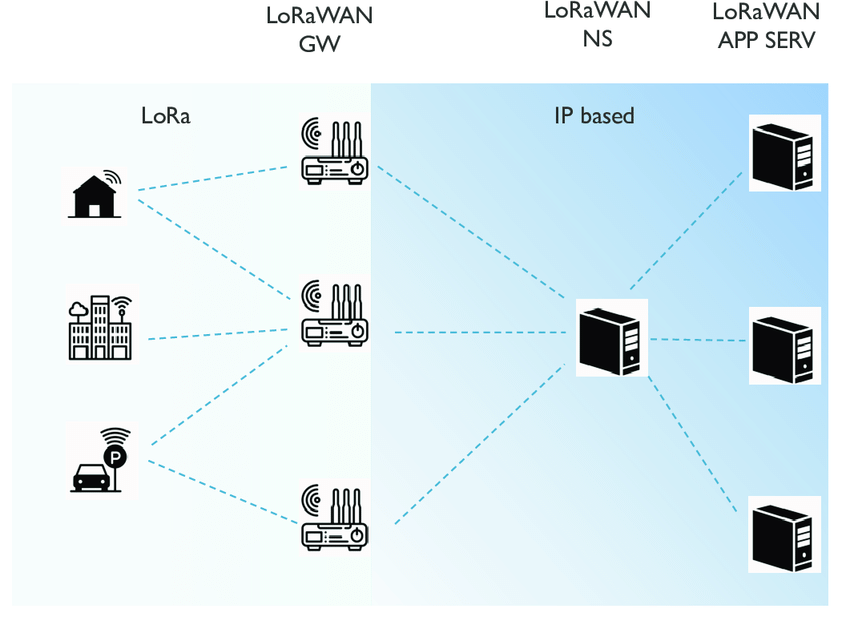
**MAC Layer**: LoRaWAN is a Media Access Control (MAC) protocol for wide area networks, the second layer of Open Systems Interconnection (OSI) model. The LoRaWAN MAC layer performs the following functions.

* Establishes connection between MAC layer of peers (i.e. between LoRa Gateway and End device).
* The MAC layer handles transmission and reception of MAC commands and data from the application layer. All the LoRaWAN MAC messages are identified based on MAC message types. This is shown in table-1.
* MAC layer adds MHDR (MAC header) and MIC (message integrity code) at the beginning and end of MAC payload. MAC header is 1 octet in size and MIC is 4 octet in size. As mentioned MAC payload carries either MAC commands or data.
* The MAC layer data is used by PHY layer which incorporates Preamble, PHY header at the beginning and PHY header CRC and entire frame CRC at the end while constructing PHY payload at the transmit end. The reverse process i.e. stripping of preamble, PHY header and CRC is done at the receive end.



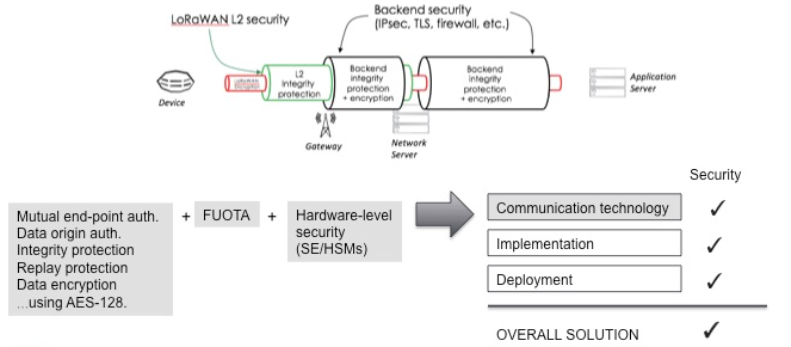
MAC commands are used for network administration between server (i.e. Gateway) and end device. These commands are non visible to applications running in the LoRa server and end devices. A single data frame consists of one or multiple MAC commands (either piggybacked or transmitted as a separate frame). MAC commands are segregated based on a CID field of size 1 octet long. CID stands for Command IDentifier. These mac commands are used by the end device or by gateway or by both.

**Topology**: LoRaWAN uses a star topology where the nodes in a LoRaWAN network are asynchronous and communicate when they have data ready to send whether event-driven or scheduled. This type of protocol is typically referred to as the Aloha method. In a mesh network or with a synchronous network, such as cellular, the nodes frequently have to ‘wake up’ to synchronize with the network and check for messages.



LoRaWAN network architecture is deployed in a star-of-stars topology in which gateways relay messages between end-devices and a central network server. The gateways are connected to the network server via standard IP connections and act as a transparent bridge, simply converting RF packets to IP packets and vice versa. The wireless communication takes advantage of the Long Range characteristics of the LoRaÒ physical layer, allowing a single-hop link between the end-device and one or many gateways. All modes are capable of bi-directional communication, and there is support for multicast addressing groups to make efficient use of spectrum during tasks such as Firmware Over-The-Air (FOTA) upgrades or other mass distribution messages.

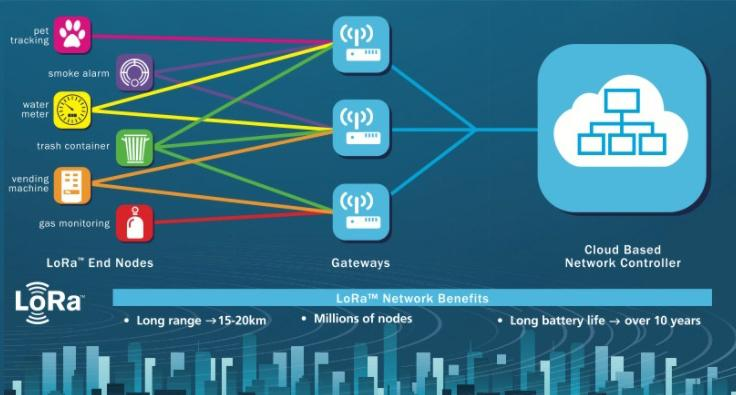
**Security**: LoRaWAN is by design very secure authentication and encryption are, in fact, mandatory but networks and devices can be compromised if security keys are not kept safe, not randomized across devices or if cryptographic numbers used once (nonces) are reused, as is shown by numerous blog posts. That’s why it is critical to look for LoRaWAN CertifiedCM devices to ensure the device has been tested against the standard and works as expected.



AES algorithms are used to provide authentication and integrity of packets to the network server and end-to-end encryption to the application server. By providing these two levels, it becomes possible to implement “multi-tenant” shared networks without the network operator having visibility of the users’ payload data. The devices can be activated by Personalization on the production line or during commissioning, or can be over the air activated (OTAA) in the field. OTAA allows device sessions to be rekeyed if necessary.

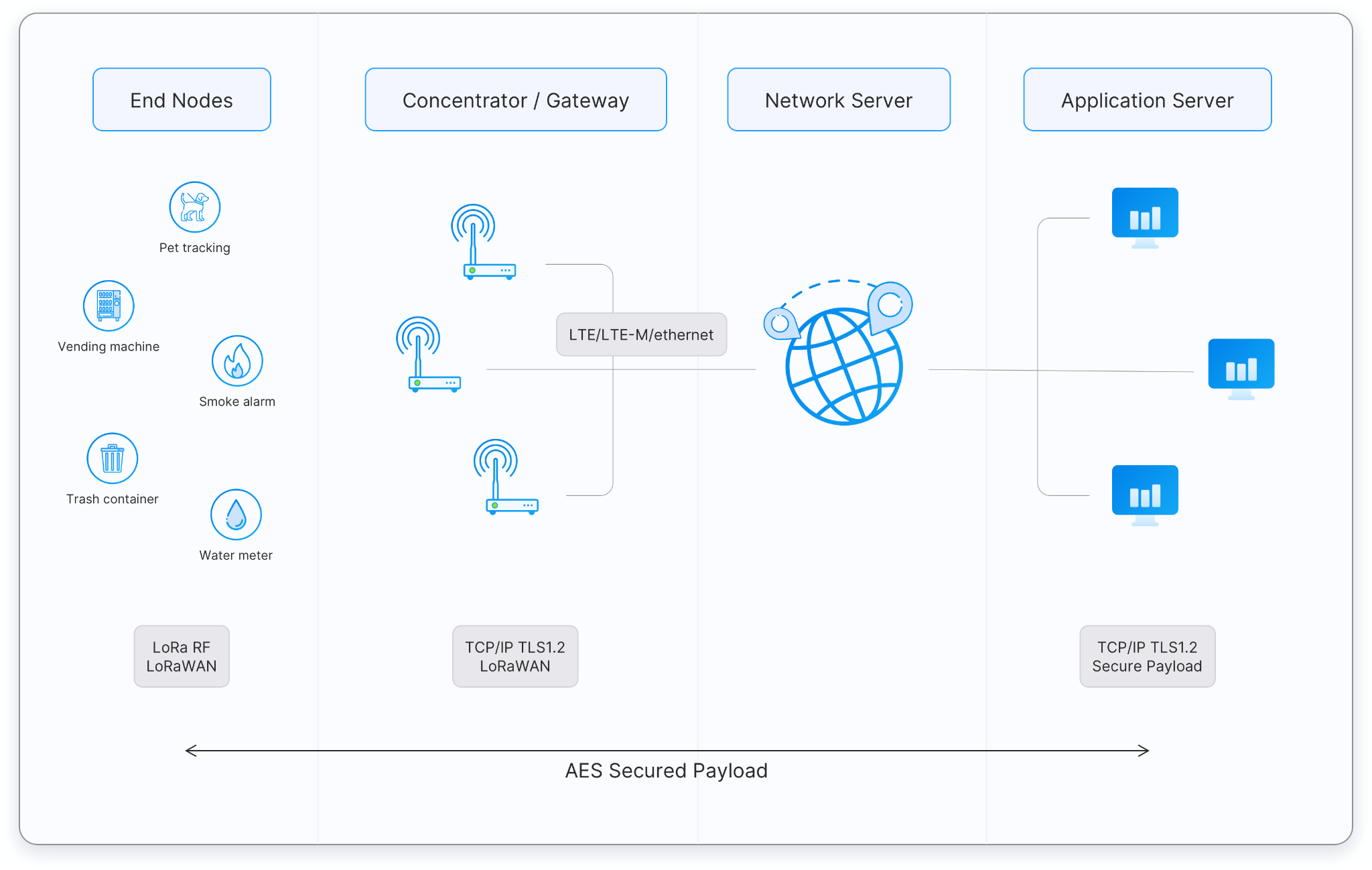
LoRaWAN has all the fundamental building blocks required and used by any modern wireless communications technology, and does so at AES-128 strength. LoRaWAN’s inherent security, as provided in the specification, needs to be accompanied by secure implementation and secure deployment of these devices and/or networks to maintain the protocol’s built-in security mechanisms. It should be pointed out that this is true of all secure device implementations using any communication technology.

**Working Principle**: Whenever the sensor reads data, the device conditionally sends a signal (data packet) that the gateway captures data. Now the data on the gateway uses FSK (Frequency Shift Keying) to transfer data to the server as efficiently as possible, this process is called Chirp Spread Spectrum (CSS). When a packet from a terminal device enters the circuit of the gateway, it enters "chirp" or symbol indicating the digital information. The chirp is then parsed into the frequency domain and the modulated signal is then demodulated for efficient data transmission.



After converting the input signal to the frequency domain, the LoRa hardware searches within the frequency band for other better frequency channels that can carry the signal. Once the gateway finds one, the entire process modulates the frequency of the input signal to make it more energy efficient, and then "shifts" the signal to the channel for fast data transfer. Once the gateway finds one, the entire process modulates the frequency of the input signal to make it more energy efficient, and then "shifts" the signal to the channel for fast data transmission.

**Architecture**: LoRaWAN networks are deployed in a star-of-stars topology. A typical LoRaWAN network consists of the following elements.



* **End points**: The endpoints are the elements of the LoRa network where the sensing or control is undertaken. They are normally remotely located.
* **LoRa gateway**: The gateway receives the communications from the LoRa endpoints and then transfers them onto the backhaul system. This part of the LoRa network can be Ethernet, cellular or any other telecommunications link wired or wireless. The gateways are connected to the network server using standard IP connections.
* **LoRa Network Server**: The LoRa network server manages the network and as part of its function it acts to eliminate duplicate packets, schedules acknowledgement, and adapts data rates. In view of the way in which it can be deployed and connected, it makes it very easy to deploy a LoRa network.
* **Remote computer**: A remote computer can then control the actions of the endpoints or collect data from them - the LoRa network being almost transparent.

End devices communicate with nearby gateways and each gateway is connected to the network server. LoRaWAN networks use an ALOHA based protocol, so end devices don’t need to peer with specific gateways. Messages sent from end devices travel through all gateways within range. These messages are received by the Network Server. If the Network Server has received multiple copies of the same message, it keeps a single copy of the message and discards others.

Communication to end point nodes is generally bi-directional, but it is also possible to support multicast operation, and this is useful for features such as software upgrades and the like or other mass distribution messages.

**Applications**: Here are a few great LoRaWAN use cases provided by Semtech, to give you some insight into how LoRaWAN can be applied:

* **Vaccine cold chain monitoring**: LoRaWAN sensors are used to ensure vaccines are kept at appropriate temperatures in transit.
* **Animal conservation**: Tracking sensors manage endangered species such as Black Rhinos and Amur Leopards.
* **Dementia patients**: Wristband sensors provide fall detection and medication tracking.
* **Smart farms**: Real time insights into crop soil moisture and optimized irrigation schedule reduce water use up to 30%.
* **Water conservation**: Identification and faster repair of leaks in a city’s water network.
* **Food safety**: Temperature monitoring ensures food quality maintenance.
* **Smart waste bins**: Waste bin level alerts sent to staff optimize the pickup schedule.

**Pros and Cons**: Following are the advantages of LoRaWAN:

* It uses Adaptive Data Rate technique to vary output data rate/Rf output of end devices. This helps in maximizing battery life as well as overall capacity of the LoRaWAN network.
* It is widely used for M2M/IoT applications.
* It delivers orthogonal transmissions at different data rates. Moreover it provides processing gain and hence transmitter output power can be reduced with the same RF link budget and hence will increase battery life.
* It uses LoRa modulation which has constant envelope modulation similar to FSK modulation type and hence available PA (power amplifier) stages having low cost and low power with high efficiency can be used.
* It has a very wide coverage range, about 5 km in urban areas and 15 km in suburban areas.

Following are the disadvantages of LoRaWAN:

* It can be used for applications requiring low data rate i.e. upto about 27 Kbps.
* LoRaWAN network size is limited based on parameters called duty cycle. It is defined as the percentage of time during which the channel can be occupied. This parameter arises from the regulation as a key limiting factor for traffic served in the LoRaWAN network.
* It is not an ideal candidate to be used for real time applications requiring lower latency and bounded jitter requirements.

**Comparison with other protocol**: Wi-Fi is superior when it comes to bandwidth, it suffers when it comes to battery life and range. Most networks might struggle to work past 15 meters, which makes it unsuitable for scattered IoT devices.

In comparison, the low power and long-range nature of LoRa make it ideal for these devices. However, LoRa will struggle to send a single image, let alone large files. It thrives at sending small packets of data, such as temperature and humidity.

5G is superior to LoRaWAN, but the latter is meant to replace the former before 5G can become more widespread. Ideally, 5G has the ability to send more data faster and with little hassle. However, setting up the infrastructure required for 5G requires time and a lot of investment before it can become a viable option.

On the flip side, LoRaWAN has been the go-to network for IoT devices, especially in the industrial setup. These are devices that can reliably send very small data packets, from temperature to humidity.