Connectivity Technologies

Computing for Internet of Things

Dr. Arijit Roy

Overview

1. IEEE 802.15.4
2. Zigbee
3. Wireless HART
4. RFID
5. NFC
6. Z-Wave
7. Sigfox
8. LoRa
9. NB-IoT
10. Wi-Fi

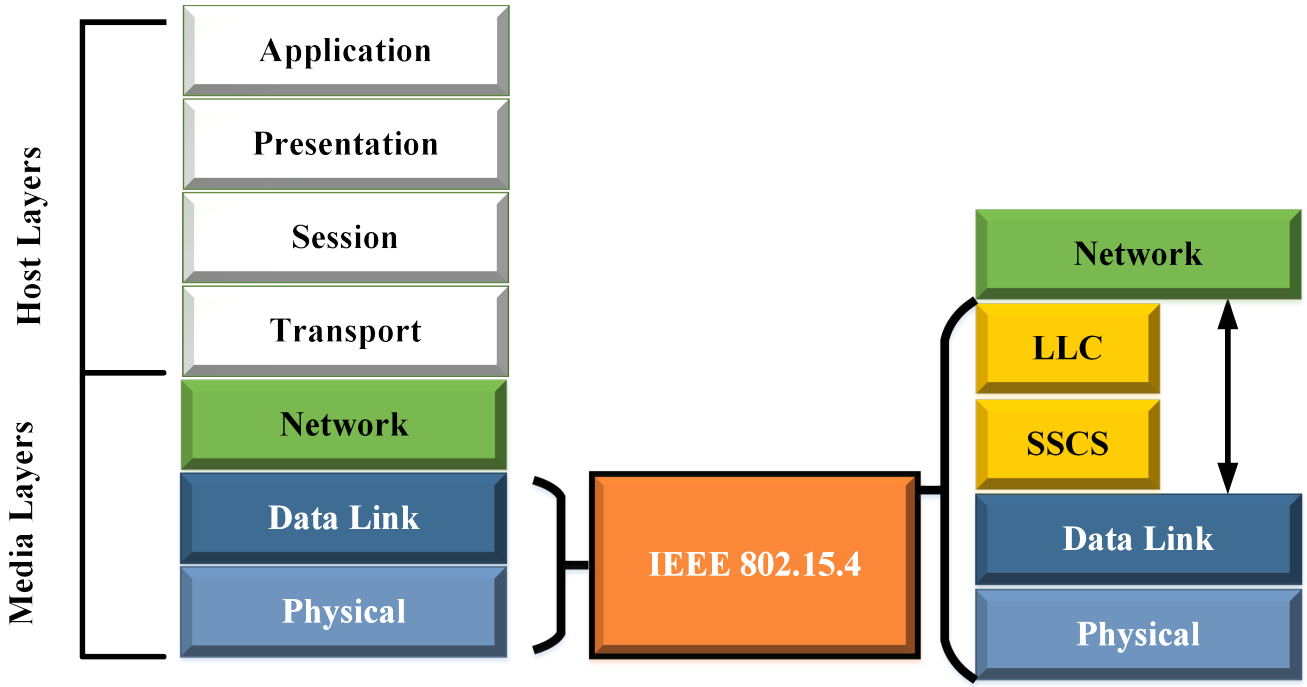
Introduction

- This chapter outlines the main features of eleven identified commonly used and upcoming IoT connectivity enablers.
- These connectivity technologies can be integrated with existing sensing, actuation, and processing solutions for extending connectivity to them.
- Some of these solutions necessarily require integration with some minimal form of processing infrastructure, such as Wi-Fi.
- In contrast, others can work in a standalone mode altogether, without the need for external processing and hardware support such as Zigbee.
- These solutions are outlined in the subsequent sections in this chapter.

IEEE 802.15.4

- The IEEE 802.15.4 standard represents the most popular standard for low data-rate wireless personal area networks (WPAN).
- This standard was developed to enable monitoring and control applications with lower data-rate and extend the operational life for uses with low-power consumption.
- This standard uses only the first two layers – Physical and Data Link – for operation along with two new layers above it – 1) logical link control (LLC), and 2) service-specific convergence sublayer (SSCS).
- The additional layers help in the communication of the lower layers with the upper layers.
- The IEEE 802.15.4 standard was curated to operate in the ISM band.

IEEE 802.15.4 protocol stack

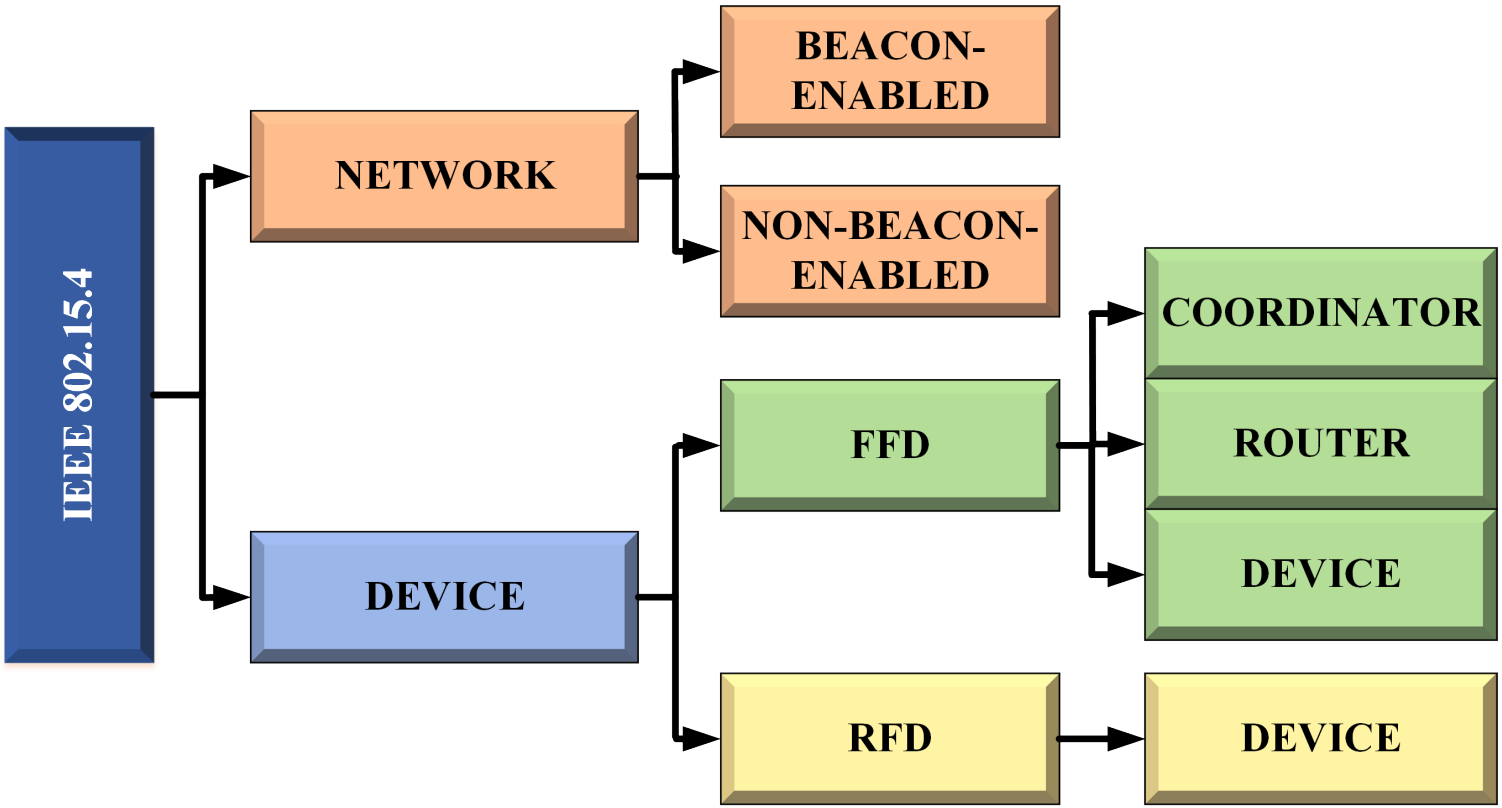


- The Direct Sequence Spread Spectrum (DSSS) modulation technique is used in IEEE 802.15.4 for communication purposes, enabling a wider bandwidth of operation with enhanced security by the modulating pseudo-random noise signal.
- This standard exhibits high tolerance to noise and interference and offers better measures for improving link reliability.
- Typically, the low-speed versions of this standard use Binary Phase Shift Keying (BPSK), whereas the versions with high data-rate implement Offset Quadrature Phase Shift Keying (O-QPSK) for encoding the message to be communicated.
- The method for channel access implements Carrier Sense Multiple Access with collision avoidance (CSMA-CA) for maintaining the sequence of transmitted signals and preventing deadlocks due to multiple sources trying to access the same channel.
- Temporal multiplexing enables access to the same channel by multiple users or nodes at different times in a maximally interference-free manner.

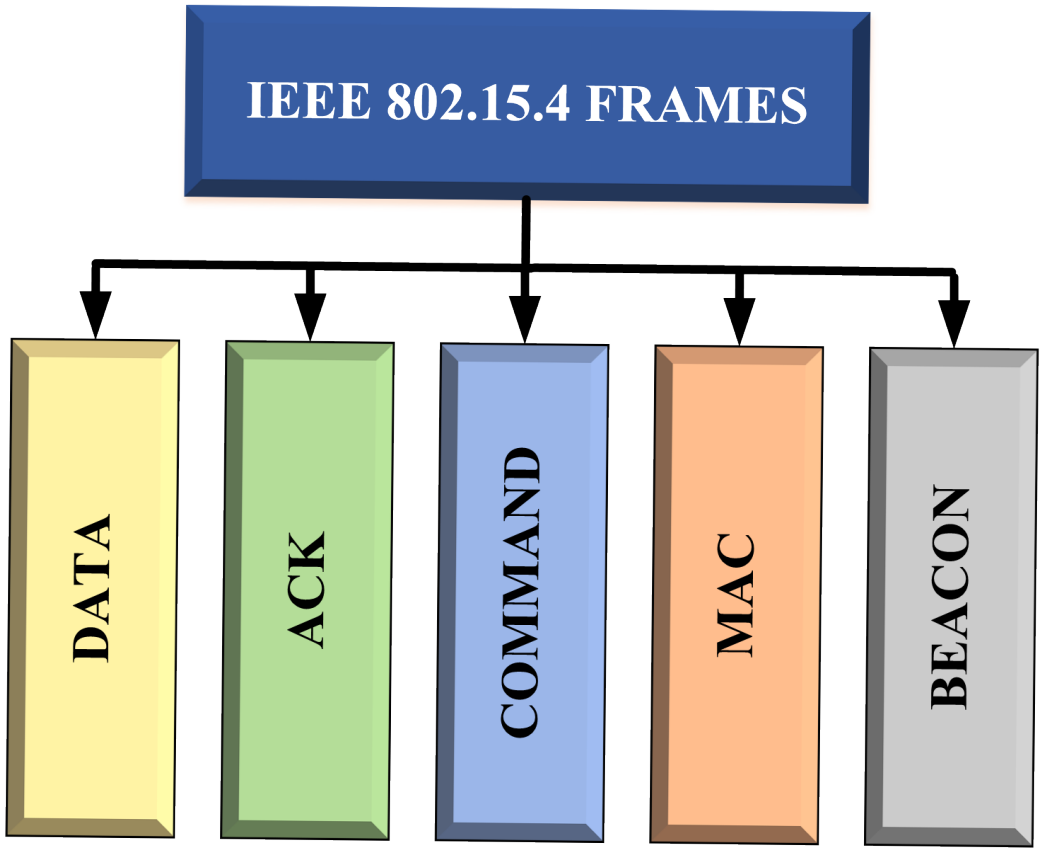
- The IEEE 802.15.4 standard utilizes infrequently occurring and very short packet transmissions with a low duty cycle (typically, $< 1\%$) to minimize the power consumption.
- The minimum power level defined is $-3dBm$ or $0.5mW$ for the radios utilizing this standard.
- The transmission, for most cases, is Line of Sight (LOS), with the standard transmission range varying between $10m$ to $75m$.
- The best-case transmission range achieved outdoors can be up to $1000m$.
- This standard typically defines two networking topologies – 1) Star, and 2) Mesh.

- The IEEE 802.15.4 standard supports two types of devices – 1) reduced function device (RFD), and 2) full function devices (FFD).
- FFDs can talk to all types of devices and supports full protocol stacks.
- However, these devices are costly and energy-consuming due to increased requirements for support of full stacks.
- In contrast, RFDs can only talk to an FFD and have lower power consumption requirements due to minimal CPU/RAM requirements.
- The IEEE 802.15.4 standard supports two network types – 1) beacon-enabled networks and 2) non-beacon-enabled networks.
- As the IEEE 802.15.4 is primarily a mesh protocol, all protocol addressing must adhere to mesh configurations such that there is a decentralized communication amongst nodes.

IEEE 802.15.4 device and network types



frame types

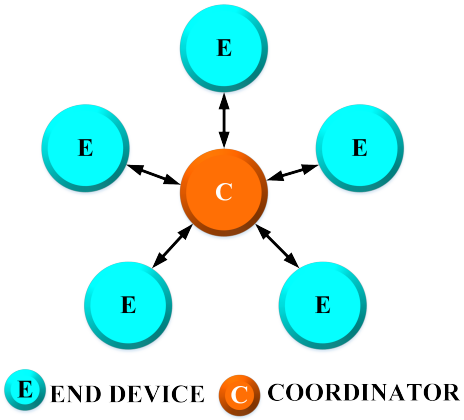


- The periodic transmission of beacon messages characterizes the beacon-enabled networks.
- Here, the data frames sent via slotted CSMA/CA with a superframe structure managed by a personal area network (PAN) coordinator.
- These beacons are used for synchronization and association of other nodes with the coordinator.
- The scope of operation of this network type spans the whole network.
- In contrast, for the non-beacon-enabled networks, unslotted CSMA/CA (contention-based) is used for transmission of data frames, and beacons are used only for link-layer discovery.
- This network typically requires both source and destination IDs of the communicating nodes.

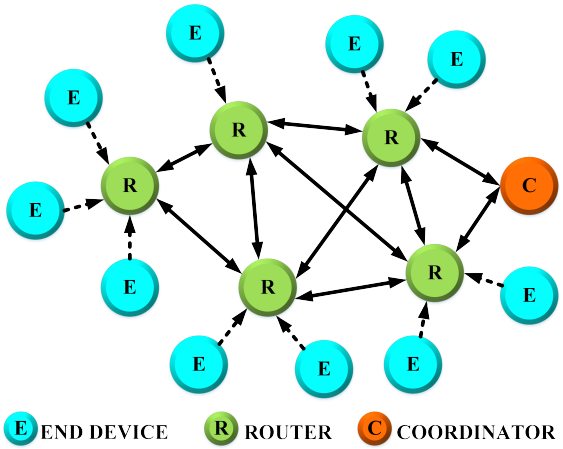
Zigbee

- The Zigbee radio communication is designed for enabling Wireless Personal Area Networks (WPANs). It uses the IEEE 802.15.4 standard for defining its physical and medium access control (layers 1 and 2 of the OSI stack).
- Zigbee finds common usage in sensor and control networks.
- Zigbee was designed for low-powered mesh networks at low cost, which can be broadly implemented for controlling and monitoring applications, typically in the range of 10-100 meters.
- The PHY and MAC layers in this communication are designed to handle multiple low data-rate operating devices.
- The frequencies of 2.4 GHz, 902-928 MHz or 868 MHz are commonly associated with Zigbee WPAN operations.
- The Zigbee commonly uses 250 kbps data-rate which is optimal for both periodic and intermittent full-duplex data transmission between two Zigbee entities.

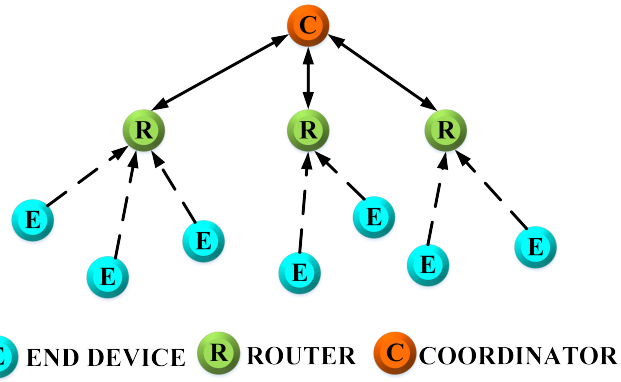
Communication topologies in Zigbee



(a) Star



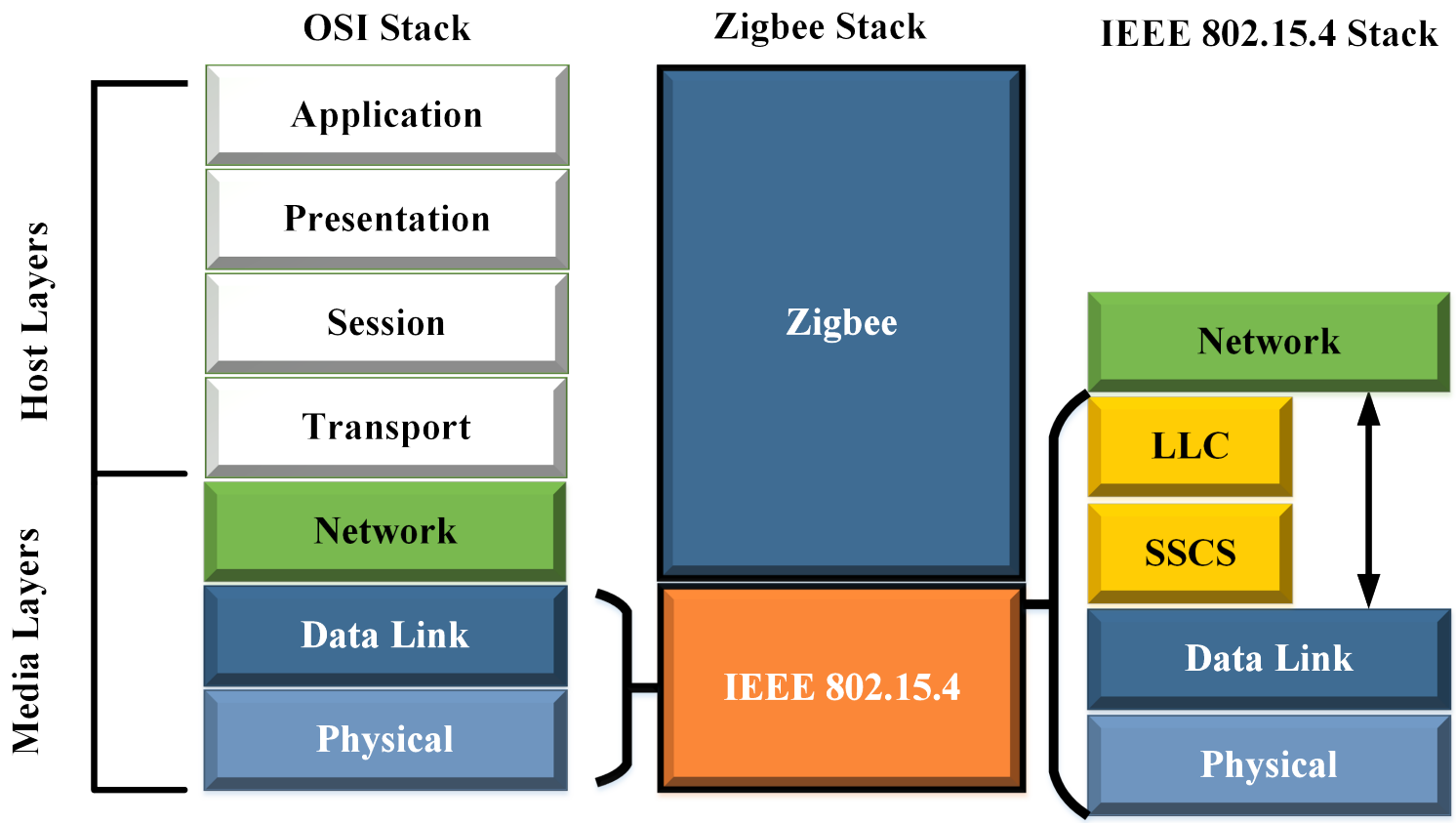
(b) Mesh



(c) cluster-tree

- A typical Zigbee network structure can consist of three different device types, namely Zigbee coordinator, Router, and End device.
- Every Zigbee network has a minimum of one coordinator device type who acts as the root as well as functions as the network bridge. The coordinator performs data handling and storing operations.
- The Zigbee routers play the role of intermediate nodes that connect two or more Zigbee devices, which may be of the same or different types.
- Finally, the end devices have restricted functionality, and communication is limited to the parent nodes. This reduced functionality enables them to have a lower power consumption requirement, enabling them to operate for an extended duration.
- There are provisions to operate Zigbee in different modes to save power and prolong the deployed network lifetime.

Zigbee protocol stack in comparison to the OSI stack



The various layer of the Zigbee stack are as follows:

- **Physical Layer**: This layer is tasked with transmitting and receiving signals, and performing modulation and demodulation operations on them, respectively. Zigbee physical layer consists of 3 bands made up of 27 channels – $2.4GHz$ band has 16 channels at 250 kbps, $868.3MHz$ has one channel at 20 kbps, and $902 - 928MHz$ has ten channels at 40 kbps.
- **MAC Layer**: This layer ensures the channel access and reliability of data transmission. CSMA-CA is used for channel access and intra-channel interference avoidance. This layer handles communication synchronization using beacon frames.
- **Network Layer**: This layer handles operations such as setting up the network, connecting and disconnecting the devices, configuring the devices, and routing.

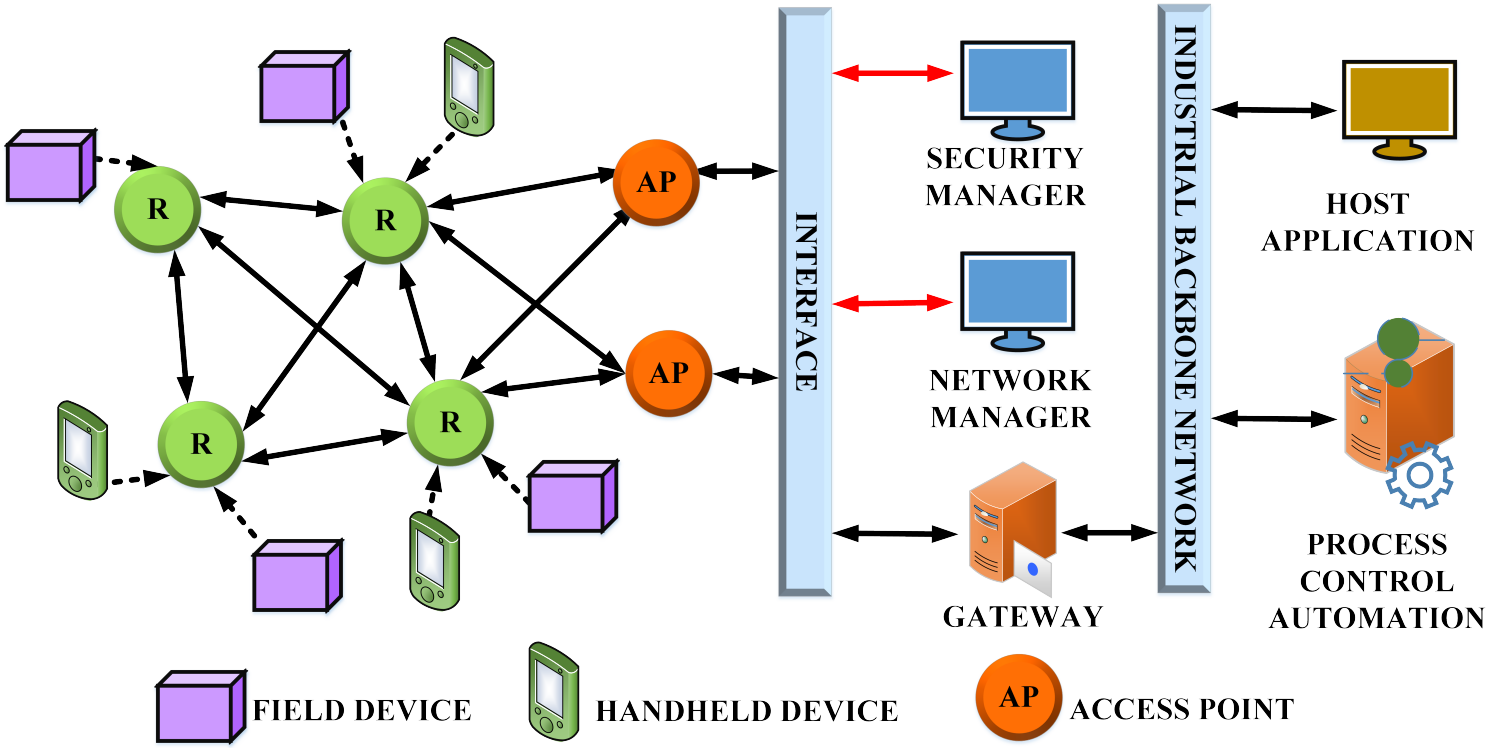
- **Application Support Sub-Layer**: This layer handles the interfacing services, control services, bridge between network and other layers, and enabling the necessary services to interface with the lower layers for Zigbee Device Object (ZDO), and Zigbee Application Objects (ZAO). This layer is primarily tasked with data management services and is responsible for service-based device matching.
- **Application Framework**: Two types of data services are provided by the application framework– as a key-value pair, and as generic message services. A key-value pair is used for getting attributes within the application objects, whereas a generic message is a developer-defined structure.

- Zigbee handles two-way data transfer using two operational modes – 1) Non-beacon mode, and 2) Beacon mode.
- As the coordinators and routers monitor the active state of the received data continuously in the non-beacon mode, it is more power-intensive. In this mode, there is no provision for the routers and coordinators to sleep.
- In contrast, a beacon mode allows the coordinators and routers to launch a very low-power sleep state, during the absence of data communication from end devices.
- The Zigbee coordinator is designed to periodically wake up and transmit the beacons to the available routers in the network.
- These beacon networks are used when there is a need for lower duty cycles and more extended battery power consumption.

Wireless HART

- WirelessHART can be considered as the wireless evolution of the Highway Addressable Remote Transducer (HART) Protocol.
- It is a license-free protocol, which was developed for networking smart field devices in industrial environments.
- The lack of wires makes the adaptability of this protocol significantly advantageous over its predecessor – HART, in industrial settings.
- By virtue of its highly encrypted communication, Wireless HART is very secure and has several advantages over traditional communication protocols.
- WirelessHART, similar to Zigbee, uses the IEEE 802.15.4 standard for its protocols designing.

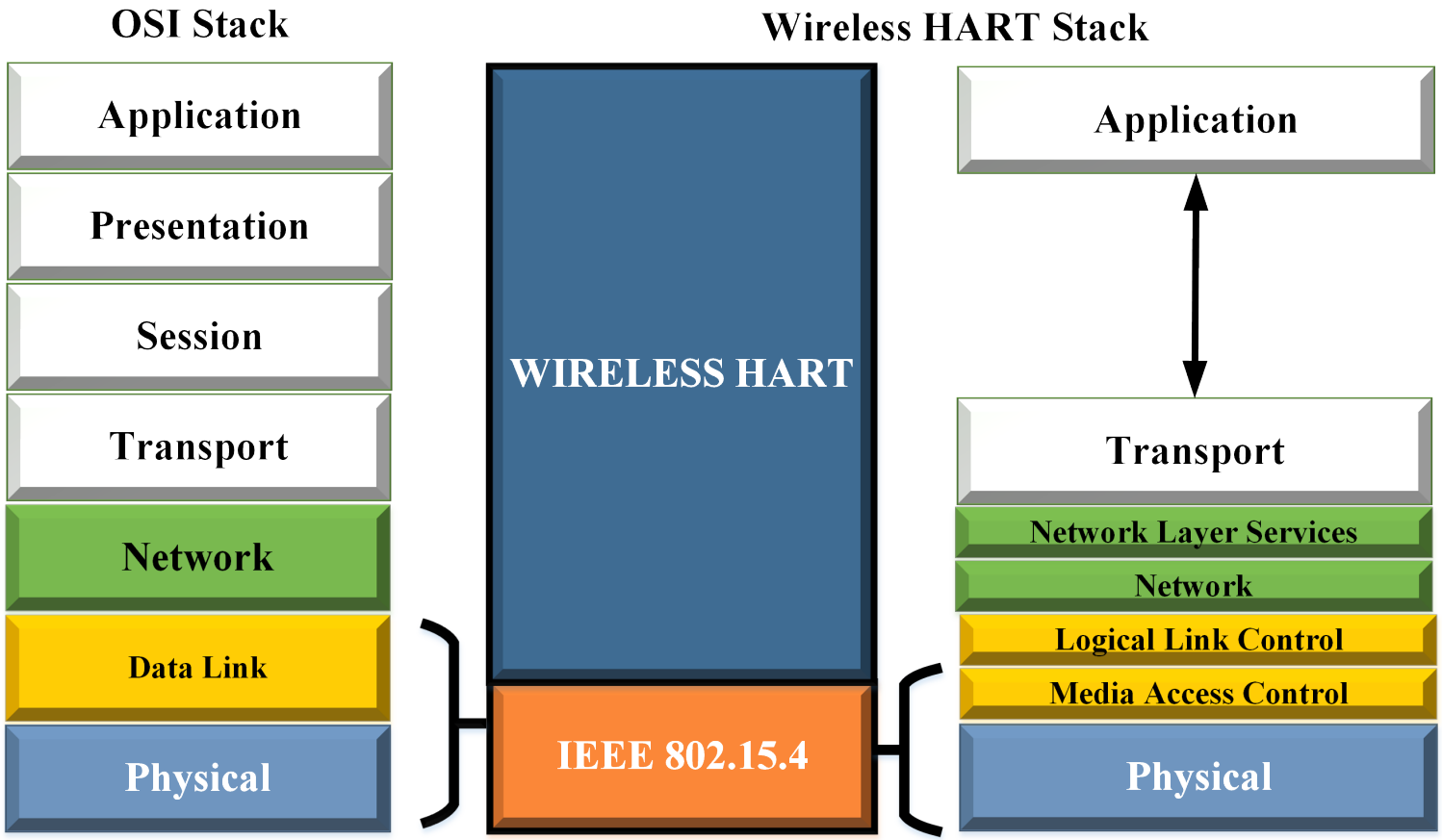
Wireless HART network architecture



- Wireless HART can communicate with a central control system in any of the two ways – 1) direct and 2) indirect.
- Direct communication is achieved when the devices transmit data directly to the gateway in a clear LOS (typically 250 m).
- Indirect communication is achieved between devices in a mesh and a gateway when messages jump from device to device till it reaches the gateway.
- WirelessHART communication is 99.999% reliable due to the maintenance of a tight schedule between message transmissions.
- All wirelessHART devices are back-compatible and allow for the integration of legacy devices as well as new ones.

- The HART encompasses most number of field devices incorporated in any field network. Wireless HART enables device placements more accessible and cheaper– such as the top of a reaction tank, inside a pipe, or at widely separated warehouses.
- The wired and unwired versions differ mainly in the network, data link, and physical layer. The wired HART lacks a network layer.
- HART ensures congestion control in the 2.4Ghz ISM band by eliminating channel 26 because of its restricted usage in certain areas.
- The use of interference-prone channels is avoided by using channel switching after every transmission.
- The transmissions are synchronized using 10ms time-slots. During each time-slot, all available channels can be utilized by the various nodes in the network, allowing for the simultaneous propagation of 15 packets through the network, which also minimizes the risk of collisions between channels.

Wireless HART protocol stack in comparison to the OSI stack



- A network manager supervises each node in the network and guides them on when and where to send packets.
- This network manager allows for collision-free and timely delivery of packets between a source and destination.
- The network manager updates information regarding neighbors, signal strength, and information needing a delivery receipt.
- This network manager also decides which nodes transmit, which nodes listen, and the frequency to be utilized in each time-slot.
- This also handles code-based network security and prevents unauthorized nodes from joining the network.

The various layers of the Wireless HART stack are outlined as follows:

- **Physical Layer**: The IEEE 802.15.4 standard specification is used for designing the physical layer of this protocol. Its operation is limited to the use of the 2.4 GHz frequency band. The channel reliability is significantly increased by utilizing only 15 channels of the 2.4 GHz band.
- **Data Link Layer**: The data link layer avoids collisions by the use of TDMA. The communication is also made deterministic by the use of superframes. The Wireless HART superframes consist of 10ms wide timeslots, which are grouped together. The use of superframes ensures better controllability of the transmission timing, collision avoidance, and communication reliability. This layer incorporates channel hopping and channel blacklisting to increase reliability and security. A characteristic feature of this protocol is Channel blacklisting. This feature identifies channels consistently affected by interference and removes them from use.

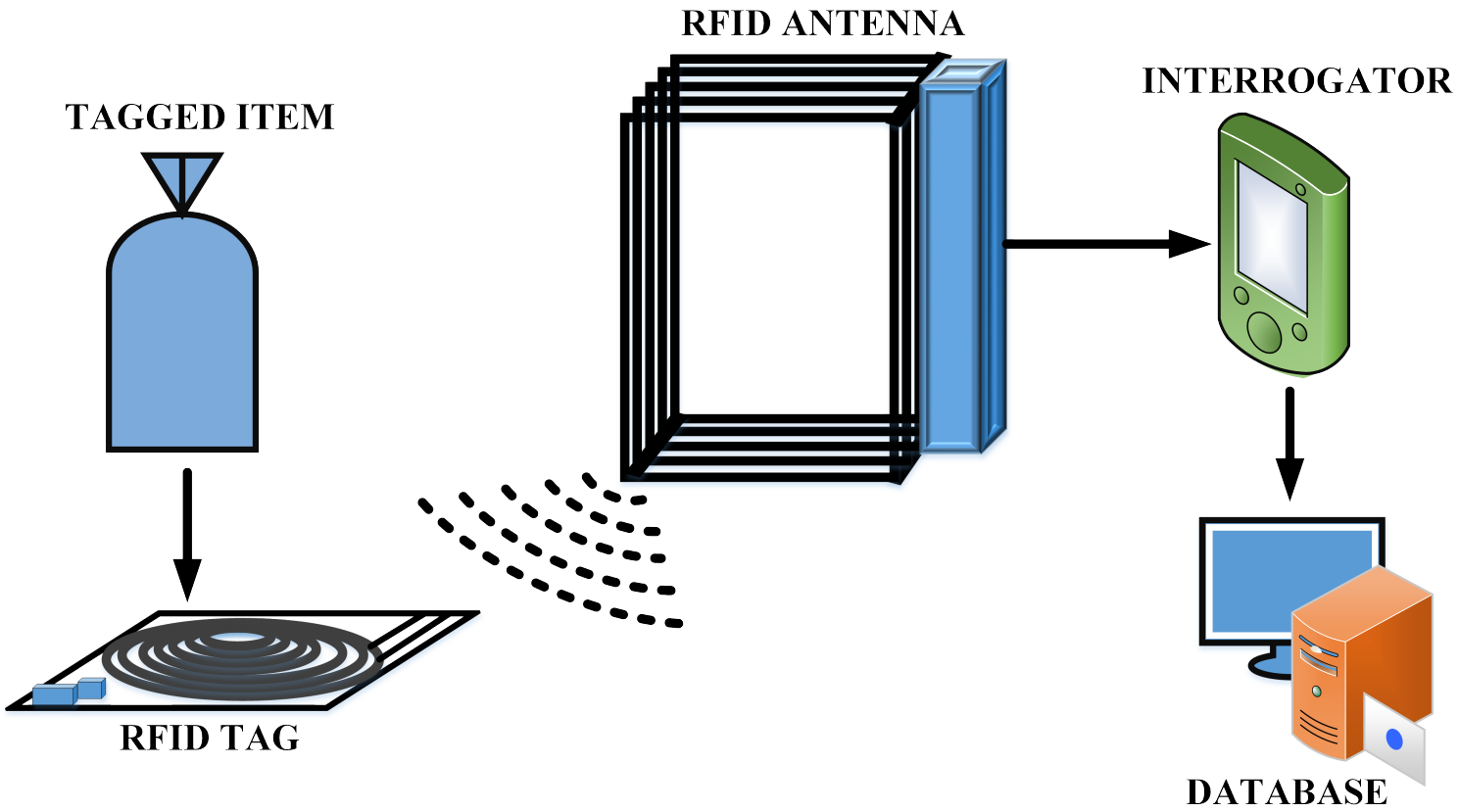
- **Network and Transport Layers**: The network and the transport layer work in tandem to address the issues of network traffic, security, session initiation/termination, and routing. WirelessHART is primarily a mesh-based network, where each node can accept data from other nodes in range and forward them to the next node. All the devices in its network have an updated network graph, which defines the routing paths to be taken. Functionally, the OSI stack's network, transport, and session layers constitute the Wireless HART's network layer.
- **Application Layer**: The application layer connects gateways and devices through various command and response messages. This layer enables back-compatibility with legacy HART devices as it does not differentiate between the wired and wireless versions of HART.

RFID

- RFID stands for Radio Frequency Identification. RFID uses tags and readers for communication. RFID tags have data encoded onto them digitally.
- The RFID readers can read the values encoded in these tags without physically touching them.
- RFIDs are functionally similar to barcodes as the data read from tags are stored in a database. However, RFID does not have to rely on line of sight operation, unlike barcodes.
- The Automatic Identification and Data Capture (AIDC) technology can be considered as the precursor of RFID. Similar to AIDC techniques, RFID systems are capable of automatically categorizing objects.
- Categorization tasks such as identifying tags, reading data, and feeding the read data directly into computer systems through radio waves outline the operation of RFID systems.

RFID operation and communication

Typically, RFID systems are made up of three components – 1) RFID tag or smart label, 2) RFID reader, and 3) an antenna.



- In RFID, the tags consist of an integrated circuit and an antenna, encased in a protective case
- These tags can be either active or passive. Passive tags find common usage in a variety of applications due to its economical cost, but it has to be powered using an RFID reader before data transmission.
- Active tags have their own power sources and do not need external activation by readers.
- Tags are used for transmitting the data to an RFID interrogator or an RFID reader. The radio waves are then converted to a more usable form of data by this reader.
- A host computer system accesses the collected data on the reader by a communication technology such as WiFi or Ethernet. The data on the host system is finally updated on a database.
- RFID applications span across domains such as inventory management, asset tracking, personnel tracking, and supply chain management.

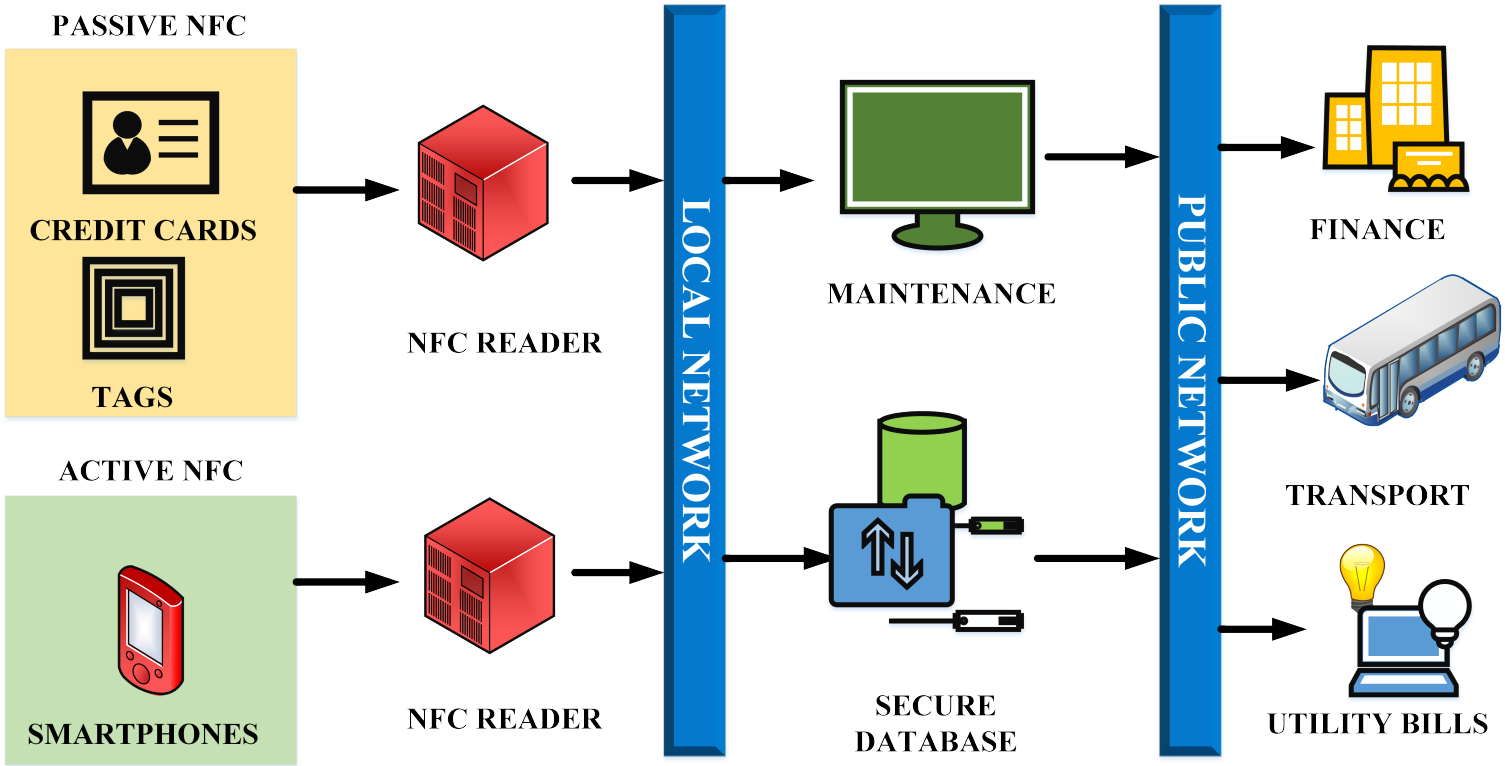
NFC

- Near Field Communication (NFC) was jointly developed by Philips and Sony as a short-range wireless connectivity standard, enabling peer-to-peer (P2P) data exchange network.
- Communication between NFC devices is achieved by the principle of magnetic induction, whenever the devices are brought close to one another.
- NFC can also be used with other wireless technologies such as WiFi after establishing and configuring the P2P network.
- The communication between compatible devices requires a pair of transmitting and receiving devices.
- The typical NFC operating frequency for data is 13.56 MHz, which supports data-rates of 106, 212, or 424 Kbps.
- NFC devices can be grouped into two types – 1) passive NFC and 2) active NFC.

- A small electric current is emitted by the NFC reader, which creates a magnetic field that acts as a bridge in the physical space between two NFC devices.
- The generated EM field is converted back into electrical impulses through another coil on the client device.
- Data such as identifiers, messages, currency, status, and others can be transmitted using NFCs.
- NFC communication and pairing are speedy due to the use of inductive coupling and the absence of manual pairing.

You can see: https://www.youtube.com/watch?v=QISeei0R-KQ

NFC operation and communication



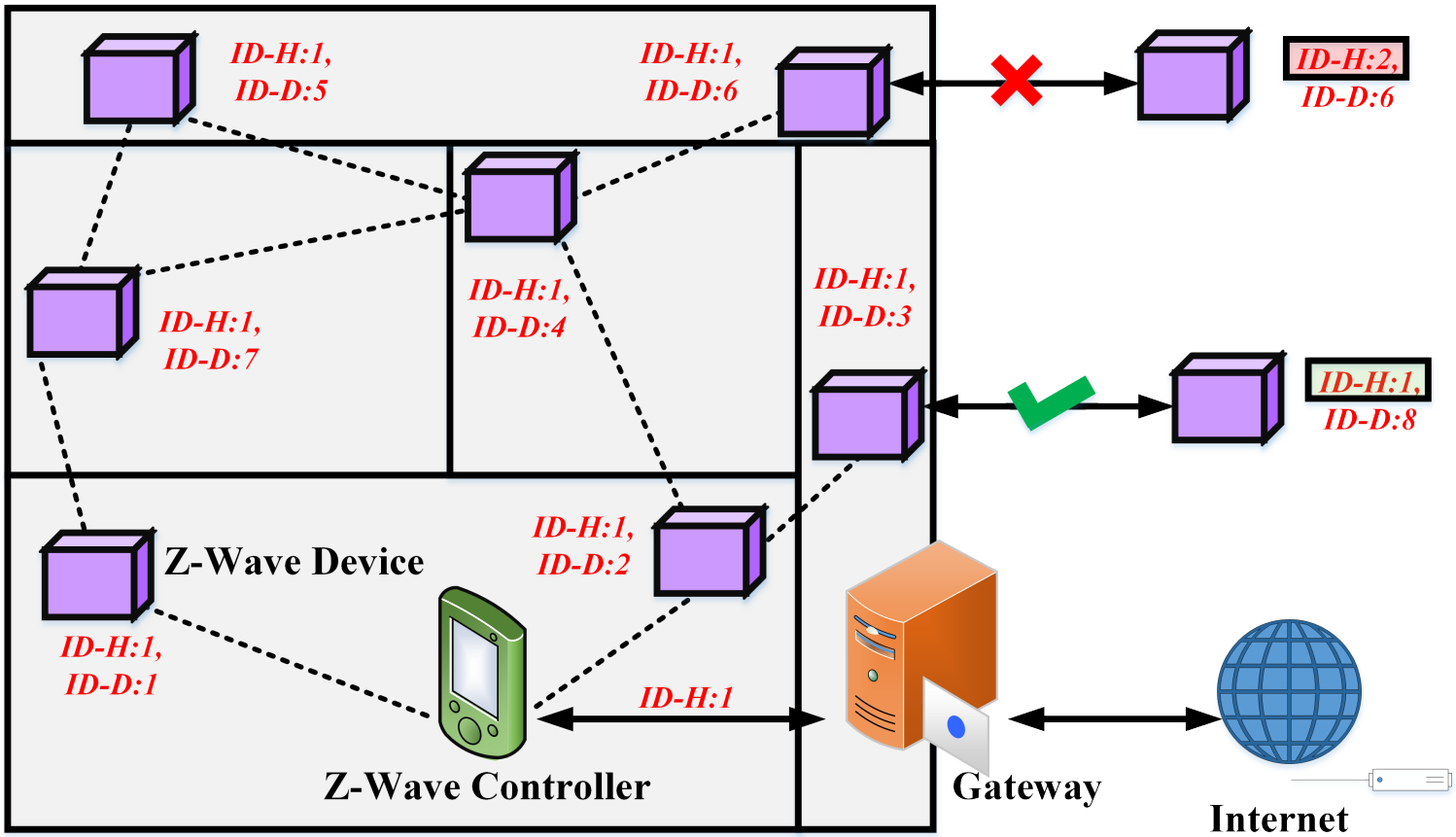
- Passive NFC devices do not need a power source for communicating with the NFC reader.
- Tags and other small transmitters can act as a passive NFC device.
- However, passive devices cannot process information; they simply store information, which is read by an NFC reader.
- In contrast, active NFC devices can communicate with active as well s passive NFC devices.
- Active devices are capable of reading as well as writing data to other NFC terminals or devices.
- Some of the most commonly used NFC platforms are smartphones, public transport card readers, and commercial touch payment terminals.

- NFC currently supports three information exchange modes – 1) peer-to-peer, 2) read/write, and 3) card emulation.
- The peer-to-peer mode is commonly used in NFC modes, which enables two NFC devices to exchange information.
- In the peer-to-peer mode of information exchange, the transmitting device goes active while the receiving device becomes passive.
- During the reverse transfer, both devices change roles. The read/write mode of information exchange allows only one-way data transmission.
- An active NFC device connects to a passive device to read information from it.
- Finally, the card emulation mode enables an NFC device (generally, smartphones) to act as a contactless credit card and make payments using just a simple tap on an NFC reader.

Z-Wave

- Z-Wave is an economical and less complicated alternative to Zigbee. It was developed by Zensys, typically for home automation solutions.
- It boasts of power consumption much lower than WiFi, but with ranges greater than Bluetooth.
- This feature makes Z-Wave be significantly useful for home IoT use by enabling inter-device communication between Z-wave integrated sensors, locks, home power distribution systems, appliances, and heating systems.

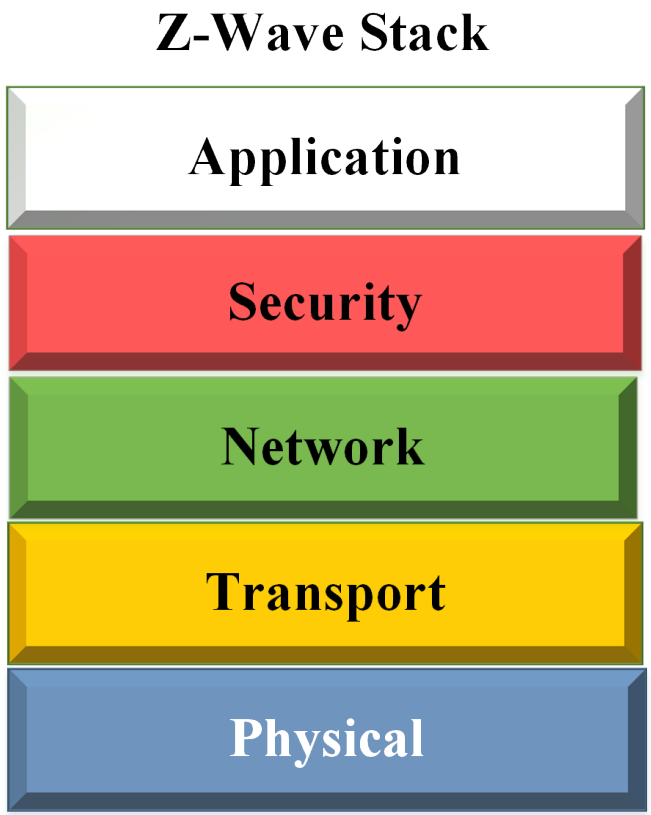
Z-Wave deployment and communication architecture



- The Z-Wave operational frequency is in the range of $800 - 900MHz$, which makes it mostly immune to the interference effects of WiFi and other radios utilizing the $2.4GHz$ frequency band.
- Z-wave utilizes Gaussian Frequency Shift Keying (GFSK) modulation, where the baseband pulses are passed through a Gaussian filter before modulation.
- A filtering operation smoothens the pulses consisting of streams of -1 and 1 (known as pulse shaping), which limits the modulated spectrum's width.
- A Manchester channel encoding is applied for preparing the data for transmission over the channel.

- The Z-wave devices are mostly configured to connect to home-based routers and access points.
- These routers and access points are responsible for forwarding Z-wave messages to a central hub.
- Z-wave devices can also be configured to connect to the central hub directly if they are in range.
- Z-wave routing within the home follows a source-routed mesh network topology.
- When the Z-wave devices are not in range, messages are routed through different nodes to bypass obstructions created by household appliances or layouts.
- This process of avoiding radio dead-spots is done using a message called Healing. Healing messages are characteristic of Z-wave.

Z-Wave protocol stack

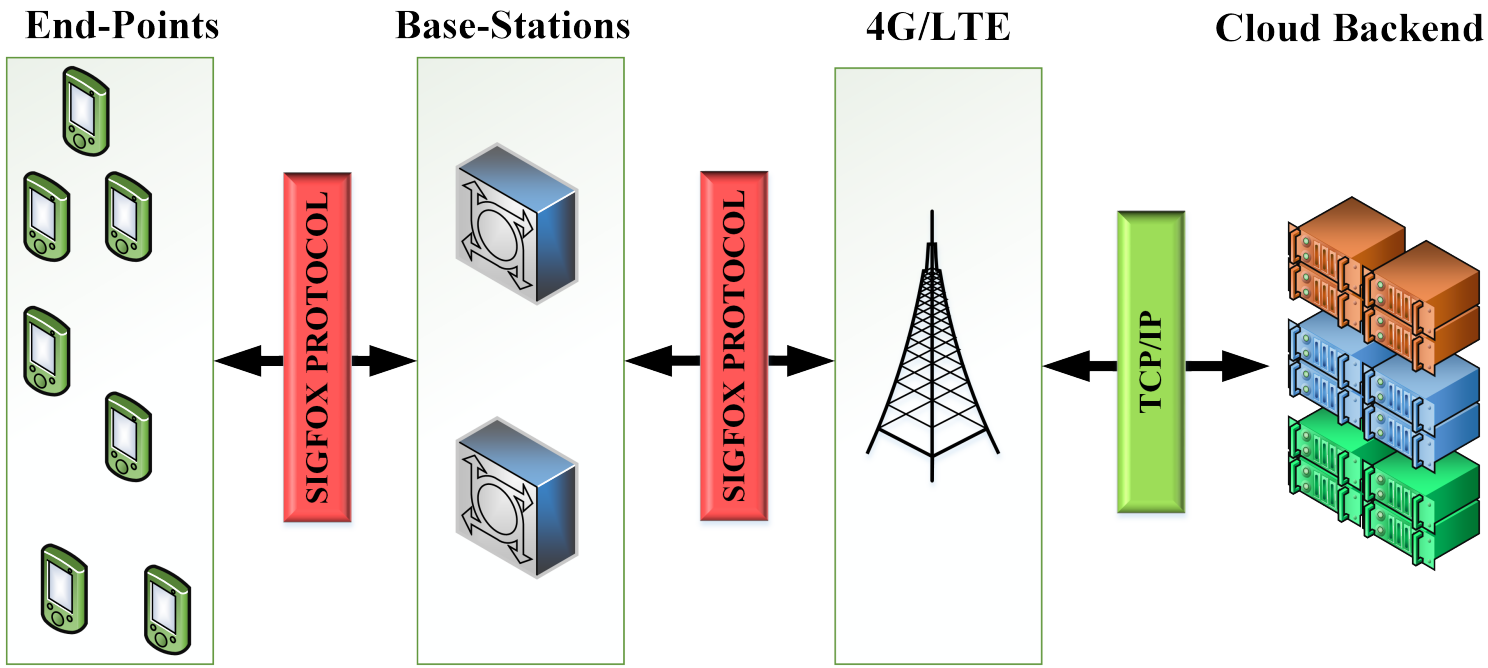


- A central network controller device sets-up and manages a Z-wave network, where each logical Z-wave network has one home (network) ID and multiple node IDs for the devices in it.
- Each network ID is 4 bytes long, whereas the node ID length=1 Byte.
- The Z-Wave nodes with different home IDs cannot communicate with one another.
- The central hub is designed to be connected to the Internet, but their quantities are limited to one hub per home.
- Each home can have multiple devices, which can talk to the hub using Z-Wave. However, the devices themselves cannot connect to the Internet.
- The Z-wave can support 232 devices in a single home deployment (a single hub).
- This technology has been designed to be backward compatible. As Z-wave uses a source-routed static network, mobile devices are excluded from the network, and only static devices are considered.

Sigfox

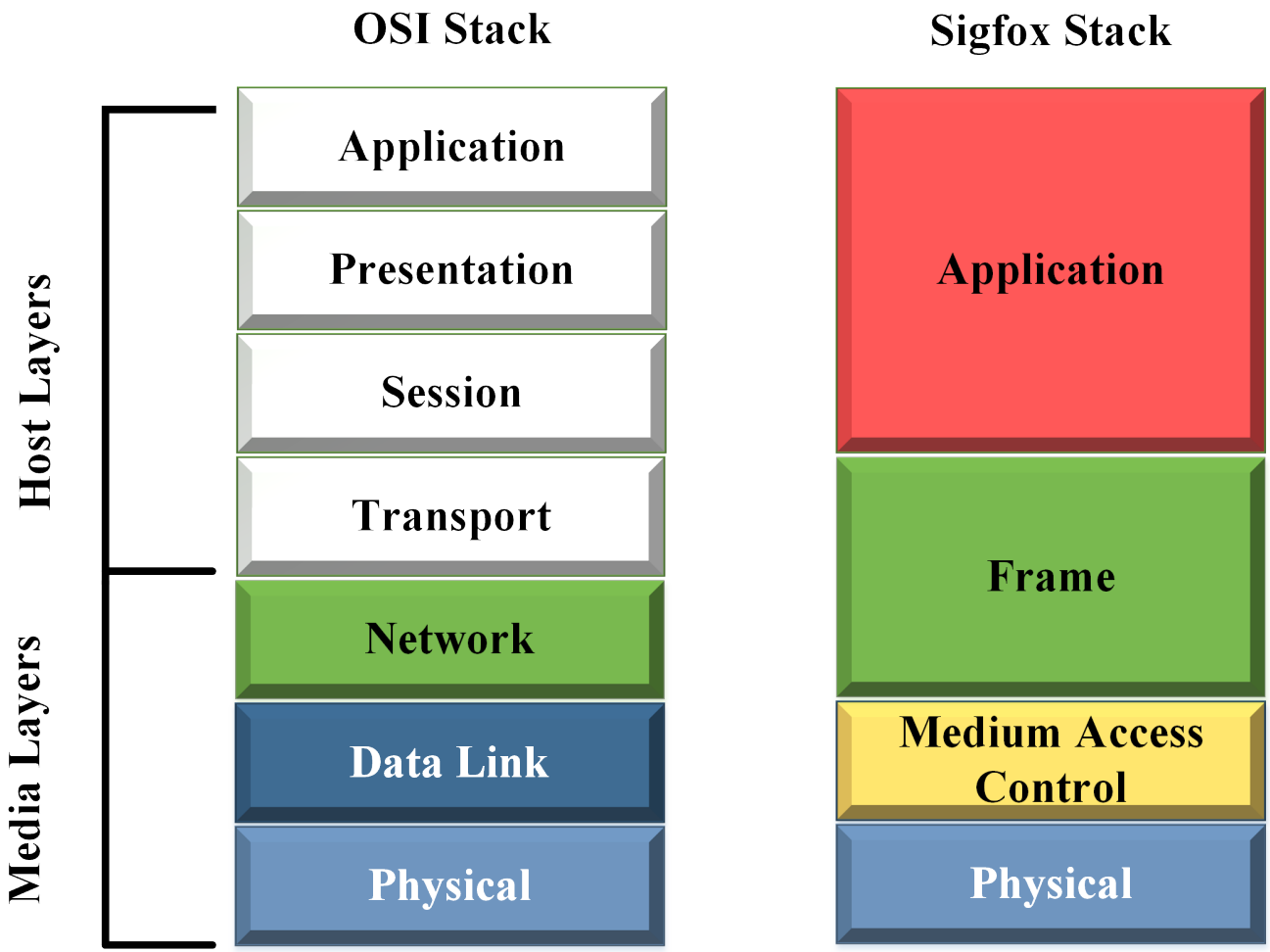
- Sigfox is a low-power connectivity solution, which was developed for various businesses such as building automation and security, smart metering, agriculture, and others.
- It uses ultra-narrowband technology (192 kHz wide) for accessing and communicating through the radio spectrum.
- The typical data rates achieved in Sigfox ranges from 100-600 bits per second. Sigfox in Europe utilizes the 868 and 868.2 MHz spectrum, whereas it uses 902 and 928 MHz elsewhere.
- A binary phase-shift keying (BPSK) is used for encoding the message transmission by changing the phase of the carrier waves, where each message is 100 Hz wide.
- As the Sigfox receiver has to access only a very tiny part of the spectrum for receiving messages, the effects of noise are significantly reduced, and enables it to communicate in the presence of jamming signals, making this standard quite resilient.

Sigfox communication architecture



- Sigfox has an exciting message forwarding principle called random access, which ensures the high quality of services in this standard.
- Each Sigfox device emits a message at an arbitrary frequency and simultaneously sends two replicas of the same message at different frequencies and time using a principle known as time-frequency diversity.
- Although the Sigfox devices are relatively less complicated, however, the base-stations are very complicated as they monitor the whole 192 kHz spectrum looking for UNB transmissions for demodulation.
- The base-stations in Sigfox follow a cooperative reception principle.
- The messages in Sigfox are not attached to any base station, and any base-station in the vicinity of the device can receive messages from it.
- This is called the principle of spatial diversity in Sigfox.
- The time and frequency diversity, along with the spatial diversity, ensures excellent quality of service for Sigfox.

Sigfox protocol stack in comparison to the OSI stack

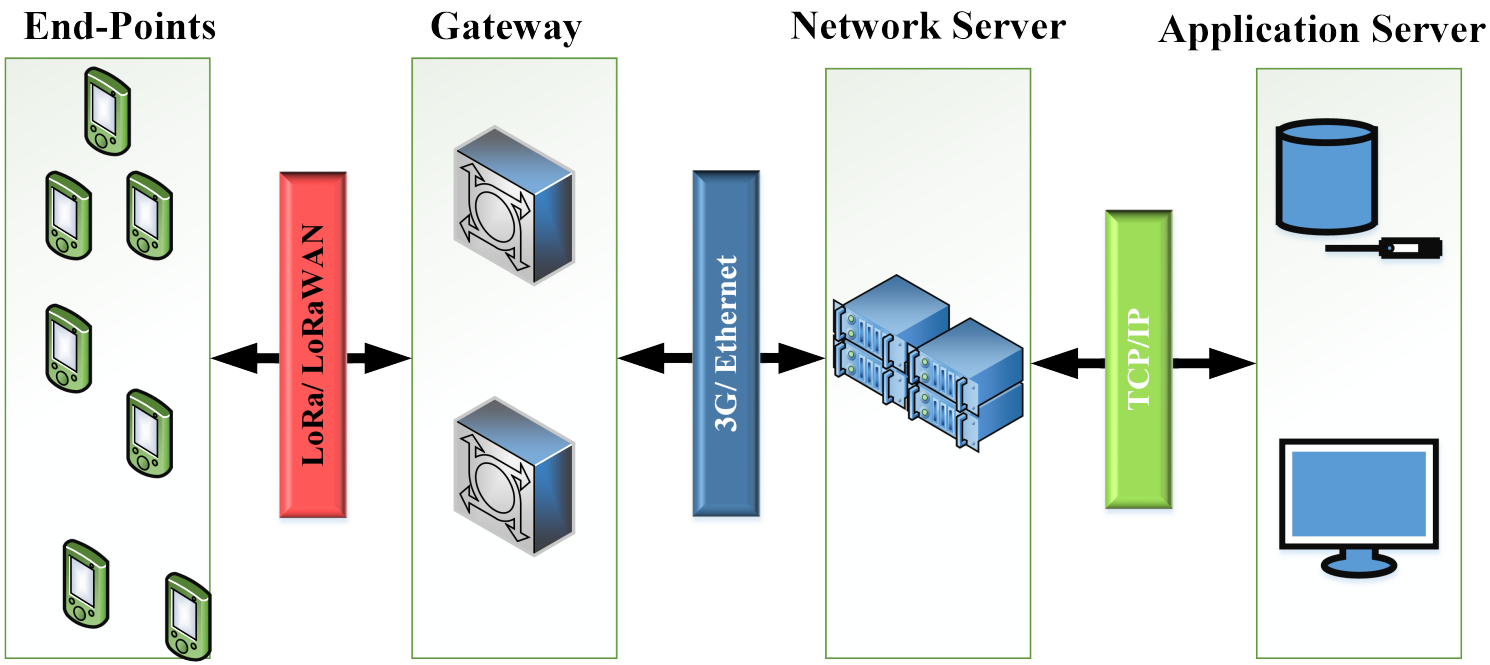


- The Sigfox communication is bidirectional and asynchronous with a significant difference between the uplink and downlink speeds.
- As the devices are less complex than the base stations, the uplink budget (device to base station) is high compared to the downlink budget (device to base station). It is mainly due to this reason that the Sigfox was designed to have small message lengths ranging from 0 to 12 bytes.
- This 12-byte payload supports the simultaneous transfer of sensor data, the status of an event/ alerts, GPS coordinates, and even application data.
- Sigfox boasts of excellent security features with support for authentication, integrity, and anti-replay on messages transmitted through the network. AES is supported by this standard.
- All these collective features of Sigfox enables it to be a low-power and resilient standard.
- However, due to the low data rates and asynchronous links, its use is better utilized in applications requiring infrequent communication with small bursts of data.

LoRa

- LoRa or Long Range is a patented wireless technology for communication, developed by Cycleo of Grenoble, France for cellular-type communications aimed at providing connectivity to M2M and IoT solutions.
- It is a sub-GHz wireless technology that operationally uses the 169 MHz, 433 MHz, 868 MHz, and 915 MHz frequency bands for communication.
- It uses bi-directional communication links symmetrically and uses a spread spectrum with a 125 kHz wideband for operating.
- Applications such as electric grid monitoring are typically suited for utilizing LoRa for communications.
- Typical communication of LoRa devices ranges from 15 to 20 km, with support for millions for devices.

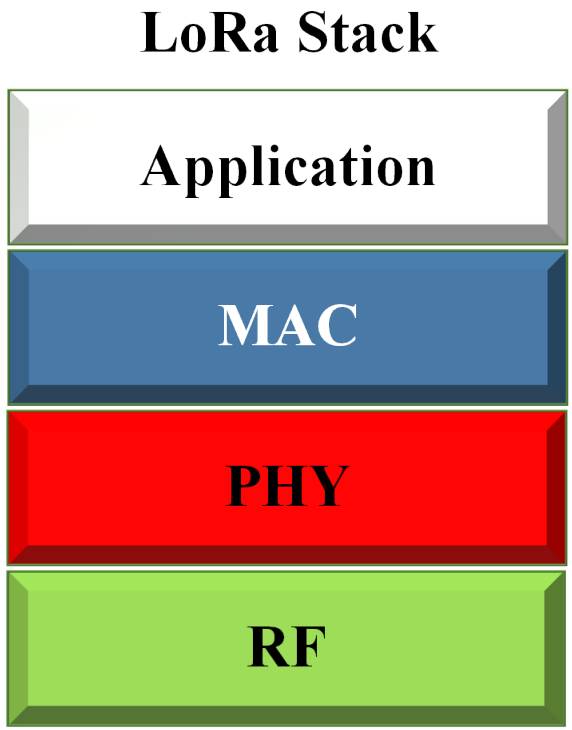
LoRa deployment and communication architecture



- It is a spread-spectrum technology with a broader band (usually 125 kHz or more). LoRa achieves high receiver sensitivity by utilizing frequency-modulated chirp coding gain.
- LoRa devices provide excellent support for mobility, which makes them very useful for applications such as asset tracking and asset management.
- In comparison with similar technologies such as NB-IoT, LoRa devices have significantly higher battery lives, but these devices have low data rates (27 to 50 kbps) and longer latency times.

- LoRa devices make use of a network referred to as LoRaWAN, which enables the routing of messages between end-nodes and the destination via a LoRaWAN gateway.
- Unlike Sigfox, LoRaWAN has a broader spectrum resulting in interference, which is handled employing coding gains of the chirp signals.
- Additionally, unlike Sigfox, the LoRaWAN end-nodes and the base stations are quite inexpensive.
- The LoRaWAN protocol is designed for WAN communications and is the architecture making use of LoRa, whereas LoRa is used as an enabling technology for a wide area network.
- Messages transmitted over LoRaWAN is received by all base stations in proximity to the device, which induces message redundancy in the network.
- However, this enhances the resilience of the network by ensuring more messages are successfully delivered between entities in the network.

LoRa protocol stack



- A LoRa network follows the star topology and is made up of four crucial entities – end-points/nodes, gateways, network server, and a remote computer.
- The end-nodes deal with all the sensing and control solutions. The gateways forward messages from end-nodes to a backhaul network.
- The LoRa network can comprise of both or either of wired and wireless technologies. The gateways themselves are connected to the network server utilizing IP-based connections (either private or public).
- The LoRa network server is responsible for scheduling message acknowledgments, modifying data-rates, removing message redundancies.
- Finally, the remote computers have control over the end-nodes and act as data sinks for data originating from these nodes.
- The LoRa network security is achieved through various mechanisms such as Unique Network key – ensures security on the network level, Unique Application key – ensures an end to end security on the application level and Device-specific key.

NB-IoT

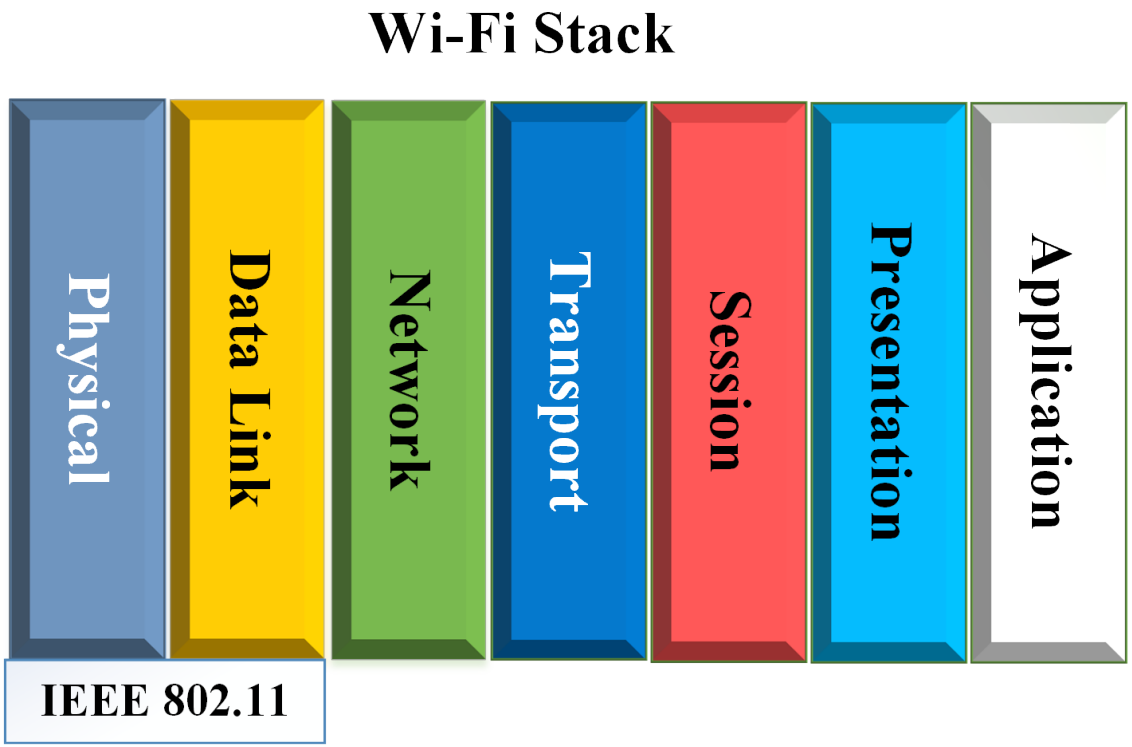
- NB-IoT or Narrowband IoT is an initiative by the Third Generation Partnership Project (3GPP) to develop a cellular standard, which can coexist with cellular systems (2G/3G/4G), be highly interoperable and that too using minimum power.
- It is reported that a major portion of the NB-IoT applications can support the battery life of up to ten years.
- NB-IoT also boasts of significant improvements in reliability, spectrum efficiencies, and system capacities.
- NB-IoT uses Orthogonal Frequency Division Multiplexing (OFDM) modulation, which enhances the system capacity and increases spectrum efficiency.
- However, device complexities are quite high. NB-IoT also provides support for security features such as confidentiality, authentication, and integrity.

- The coverage of NB-IoT supports deployments in indoor environments as well as in dense urban areas.
- When compared with technologies such as LoRa, NB-IoT ensures a higher quality of service as well as reduced latencies. As because of its design principles, the transfer of large messages is not efficient.
- NB-IoT is better suited for static deployments such as energy metering, fixed sensors, and others.
- Mobility support is not provided in this standard. NB-IoT communication can either make use of the available 200-kHz GSM (Global System for Mobile Communications) bands or be allocated resource blocks on the guard bands by LTE base stations. This ensures that the NB-IoT can achieve more extensive coverage while coexisting with cellular systems.
- NB-IoT was developed for non-IP based applications requiring quite small volumes of daily data transactions, typically in the range of a few tens to a hundred bytes of data per device daily.

Wi-Fi

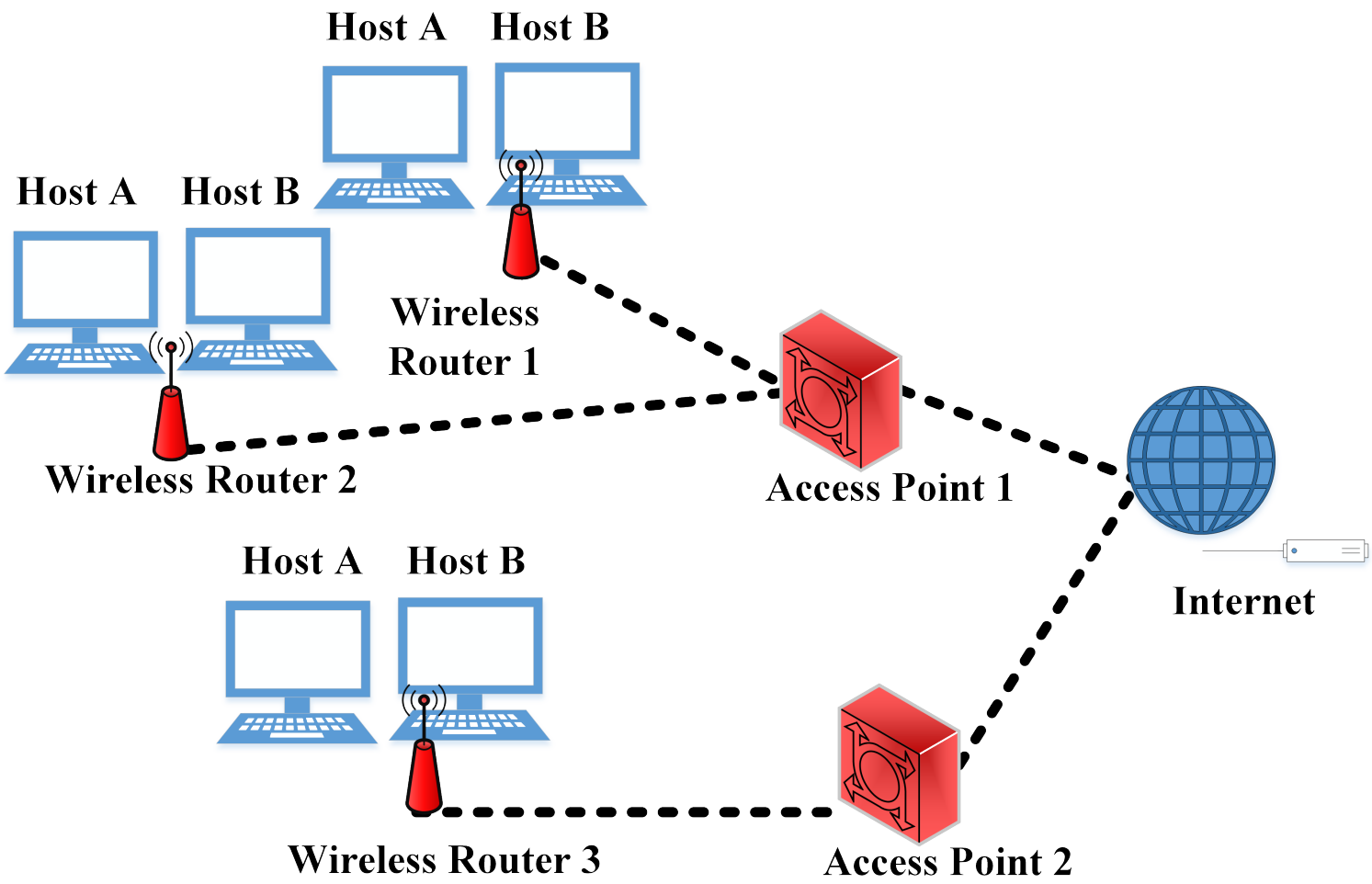
- Wi-Fi or WiFi is technically referred to by its standard – IEEE 802.11 and is a wireless technology for wireless local area networking of nodes and devices built upon similar standards.
- Wi-Fi utilizes the 2.4 GHz Ultra High frequency (UHF) band or the 5.8 GHz Super High Frequency (SHF) ISM radio bands for communication.
- For operation, these bands in Wi-Fi are subdivided into multiple channels.
- The communication over each of these channels is achieved by multiple devices simultaneously using time-sharing based TDMA multiplexing. It uses CSMA/CA for channel access.

IEEE 802.11 Wi-Fi stack



- Various versions of IEEE 802.11 have been popularly adapted, such as a/b/g/n.
- The IEEE 802.11a achieves a data rate of 54 Mbps and works on the 5GHz band using OFDM for communication.
- IEEE 802.11b achieves a data rate of 11 Mbps and operates on the 2.4GHz band.
- Similarly, IEEE 802.11g also works on the 2.4GHz band but achieves higher data rates of 54Mbps using OFDM.
- Finally, the newest version – IEEE 802.11n – can transmit data at a rate of 140Mbps on the 5GHz band.

Wi-Fi deployment architecture



The End