IEEE 802.15.4

The IEEE 802.15.4 standard represents the most popular standard for low data rate wireless personal area networks (WPAN) [1]. 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. Figure 7.1 shows the IEEE 802.15.4 operational layers. The IEEE 802.15.4 standard was curated to operate in the ISM (industrial, scientific, and medical) band.

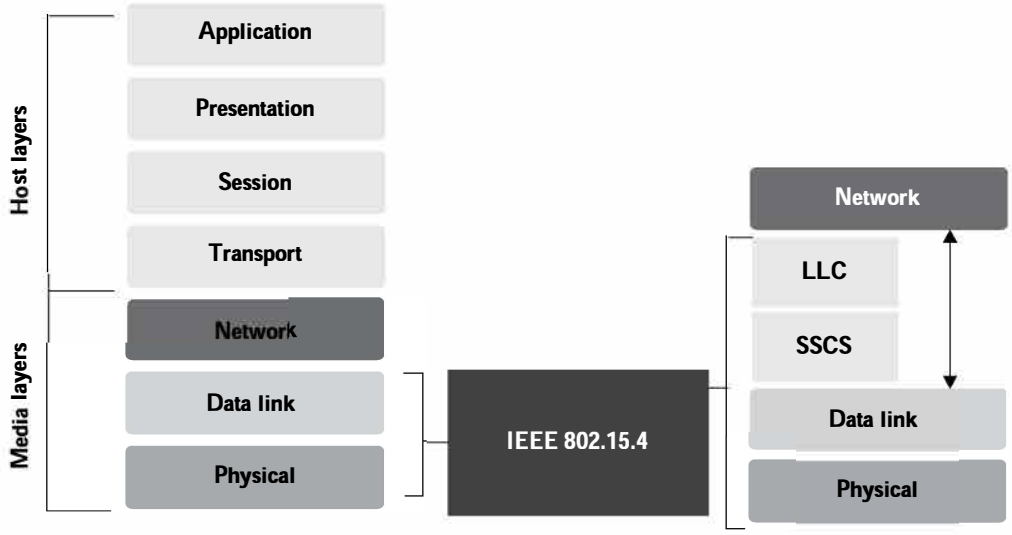


Figure 7.1 The operational part of IEEE 802.15.4's protocol stack in comparison to the OSI stack

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 the IEEE 802.15.4 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. Carrier sense multiple access with collision avoidance (CSMA-CA) is the channel access method used 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 [2] 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 –3 dBm or 0.5 mW for the radios utilizing this standard. The transmission, for most cases, is line of sight (LOS), with the standard transmission range varying between 10 m to 75 m. The best-case transmission range achieved outdoors can be up to 1000 m.

This standard typically defines two networking topologies: 1) Star and 2) mesh. There are seven variants identified with in IEEE 802.15.4—A, B. C, D, E, F, and G. Variants A/B are the base versions, C is assigned for China, and D for Japan. Variants E, F, and G are assigned respectively for industrial applications, active RFID (radio frequency identification) uses, and smart utility systems.

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 support 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. Figure 7.2 shows the device types and network types supported by the IEEE 802.15.4 standard.

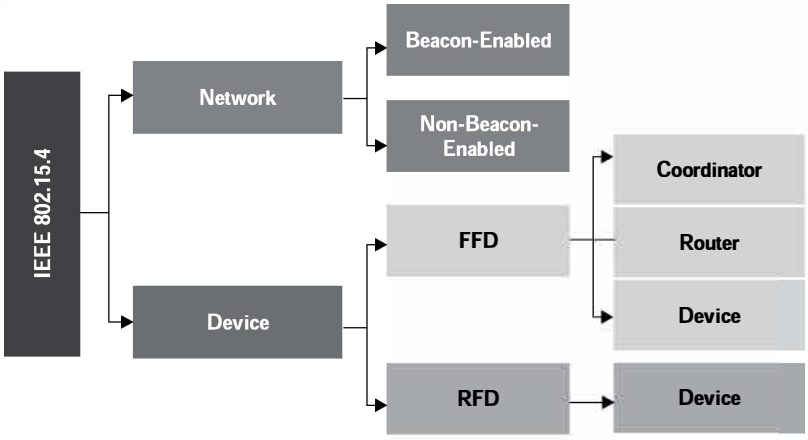


Figure 7.2 The various device and network types supported in the IEEE 802.15.4 standard

The IEEE 802.15.4 standard supports two network types: 1) Beacon-enabled networks and 2) non-beacon-enabled networks. The periodic transmission of beacon messages characterizes 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 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. 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.

Figure 7.3 shows the frame types associated with the IEEE 802.15.4 standard. Beacon frames are used for signaling and synchronization; data transmission is done through the data frames; and message reception is confirmed using the acknowledgment frames. MAC and command frames are used for association requests/responses, dissociation requests, data requests, beacon requests, coordinator realignment, and orphan notifications.

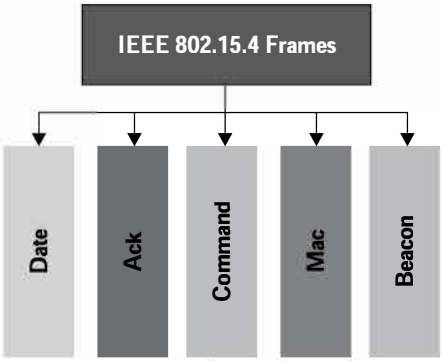
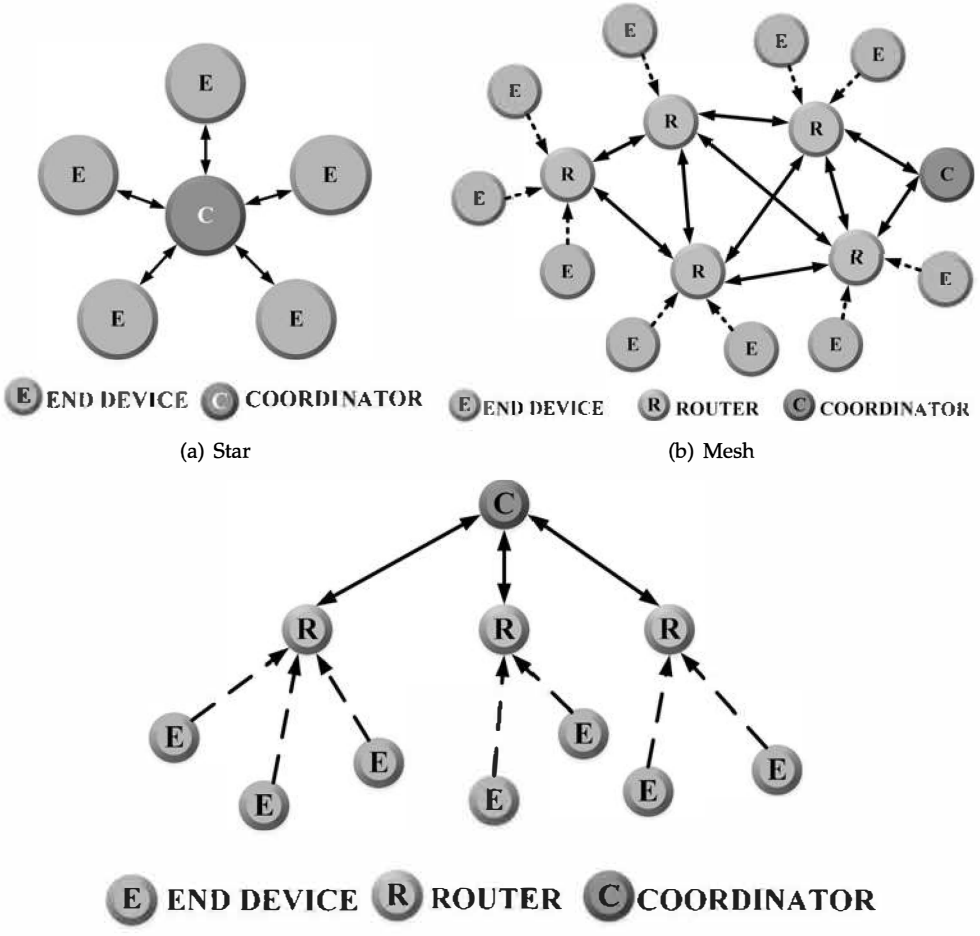


Figure 7.3 Various frame types supported in the IEEE 802.15.4 standard

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 [4]. It 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.

Zigbee supports various network configurations such as master-to-master communication or master-to-slave communication. Several network topologies are supported in Zigbee, namely the star (Figure 7.4(a)), mesh (Figure 7.4(b)), and cluster tree (Figure 7.4(c)). Any of the supported topologies may consist of a single or multiple coordinators. In star topology, a coordinator initiates and manages the other devices in the Zigbee network. The other devices which communicate with the coordinator are called end devices. As the star topology is easy to maintain and deploy, it finds widespread usage in applications where a single central controller manages multiple devices.



(a) Star

(b) Mesh

(c) Cluster tree

Figure 7.4 Various communication topologies in Zigbee

A network can be significantly extended in the Zigbee mesh and tree topologies by using multiple routers where the root of the topology is the coordinator. These configurations allow any Zigbee device or node to communicate with any other

adjacent node. In case of the failure of one or more nodes, the information is automatically forwarded to other devices through other functional devices. In a Zigbee cluster tree network, a coordinator is placed in the leaf node position of the cluster, which is, in turn, connected to a parent coordinator who initiates the entire network.

A typical Zigbee network structure can consist of three different device types, namely the Zigbee coordinator, router, and end device, as shown in Figure 7.4. Every Zigbee network has a minimum of one coordinator device type who acts as the root; it also 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; communication is limited to the parent nodes. This reduced functionality enables them to have a lower power consumption requirement, allowing 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.

The PHY and MAC layers of the IEEE 802.15.4 standard are used to build the protocol for Zigbee architecture; the protocol is then accentuated by network and application layers designed especially for Zigbee. Figure 7.5 shows the Zigbee protocol stack. The various layer of the Zigbee stack are as follows.

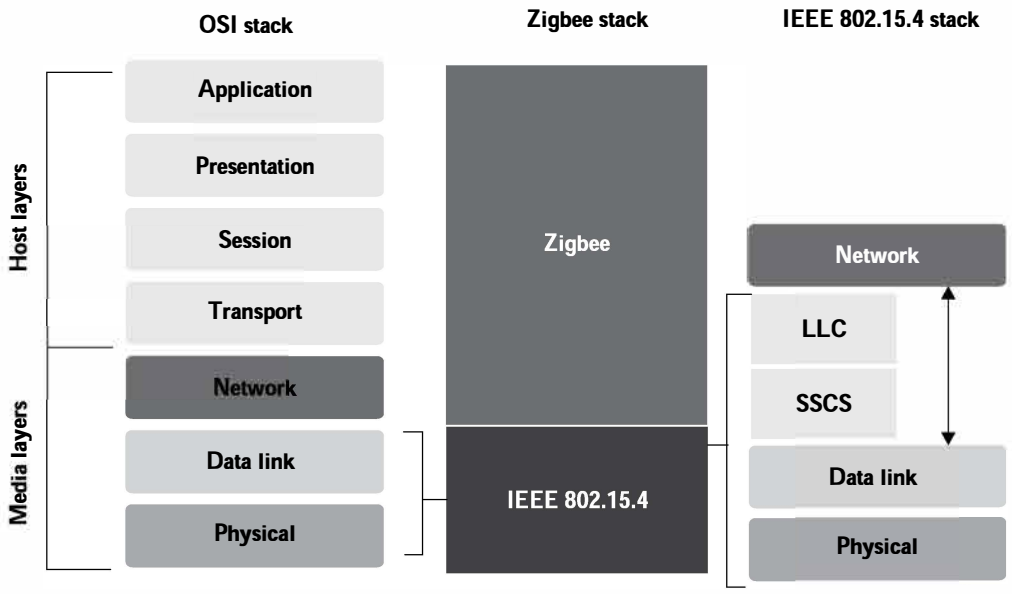


Figure 7.5 The Zigbee protocol stack in comparison to the OSI stack

- **Physical Layer**: This layer is tasked with transmitting and receiving signals, and performing modulation and demodulation operations on them, respectively. The

Zigbee physical layer consists of 3 bands made up of 27 channels: the 2.4 GHz band has 16 channels at 250 kbps the 868.3 MHz has one channel at 20 kbps; and the 902-928 MHz has ten channels at 40 kbps.

- **MAC Layer**: This layer ensures 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 enables 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: provision of a key-value pair and generation of generic messages. 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 into a very low-power sleep state in the absence of data communication from end devices. The Zigbee coordinator is designed to periodically wake up and transmit 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.

WirelessHART

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. Similar to Zigbee, wirelessHART uses the IEEE 802.15.4 standard for its protocols designing.

Figure 7.10 shows the WirelessHART network architecture. WirelessHART 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 until 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.

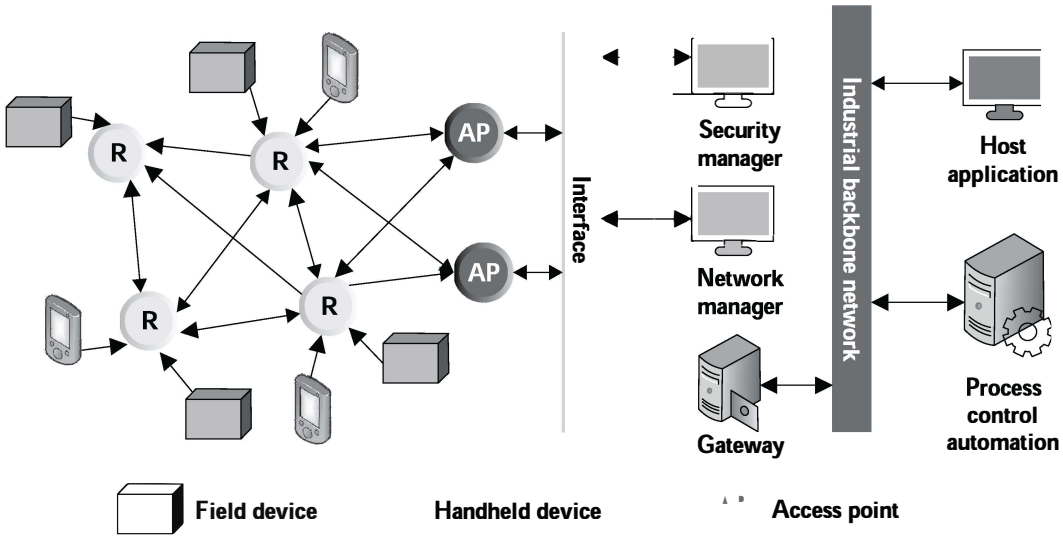


Figure 7.10 The WirelessHART network architecture

The HART encompasses the most number of field devices incorporated in any field network. WirelessHART makes device placements more accessible and cheaper, such as the top of a reaction tank, inside a pipe, or 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 2.4 Ghz 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 10 ms 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.

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 the destination. It 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. It also handles code-based network security and prevents unauthorized nodes from joining the network.

Figure 7.11 shows the comparison of the wirelessHART protocol stack against the standard ISO-OSI stack. The various layers of the wirelessHART stack are outlined as follows:

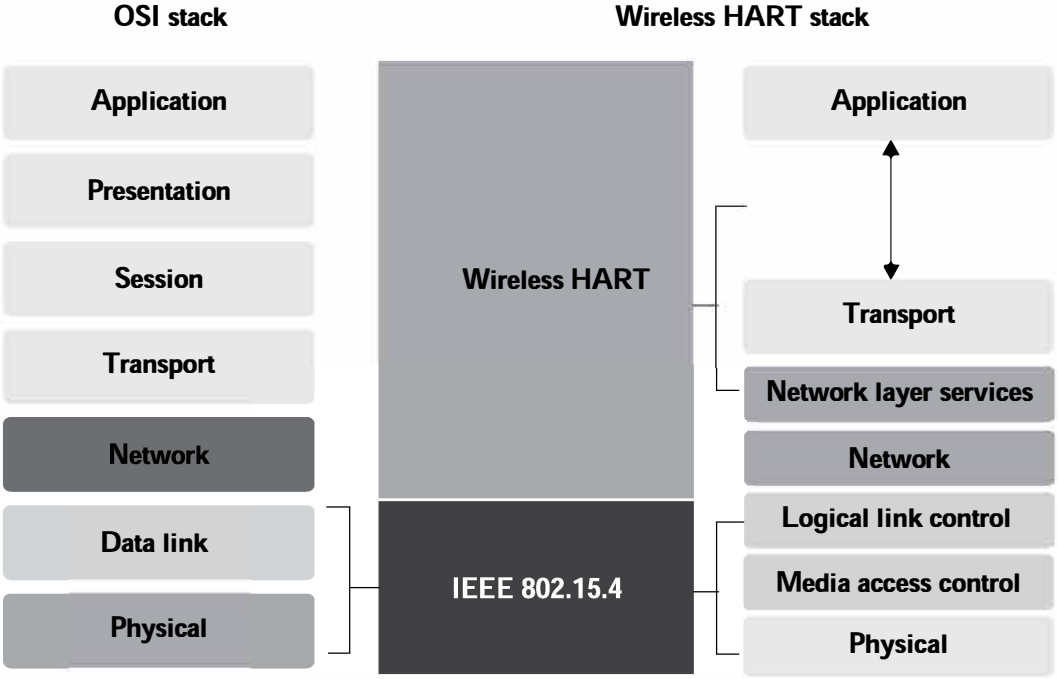


Figure 7.11 The WirelessHART protocol stack in comparison to the OSI stack

- **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.

WirelessHART superframes consist of 10 ms wide time-slots that 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 the wirelessHART 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 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 WirelessHART'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. This technology uses tags and readers for communication. RFID tags have data encoded onto them digitally [8]. 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. Typically, RFID systems are made up of three components: 1) RFID tag or smart label, 2) RFID reader, and 3) an antenna. Figure 7.12 shows the various RFID components.

In RFID, the tags consist of an integrated circuit and an antenna, enclosed in a protective casing to protect from wear and tear and environmental effects. These

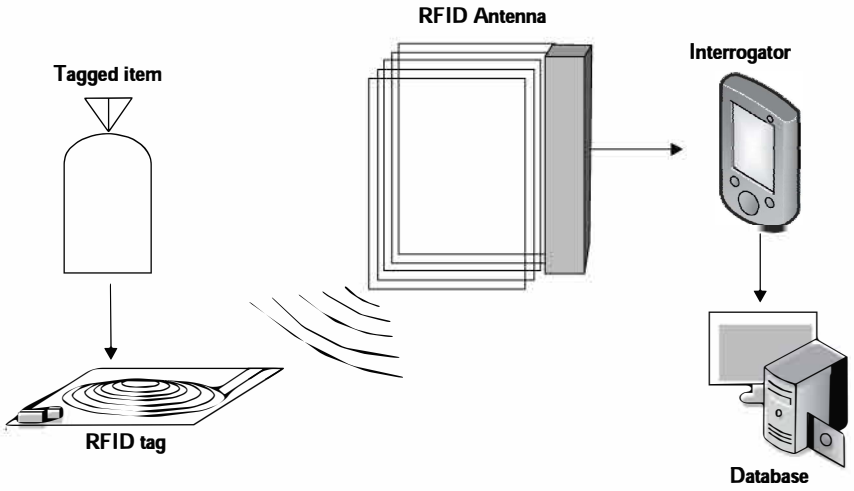


Figure 7.12 An outline of the RFID operation and communication

tags can be either active or passive. Passive tags find common usage in a variety of applications due to its low cost; however, 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 Wi-Fi or Ethernet. The data on the host system is finally updated onto 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 [9]. NFC can also be used with other wireless technologies such as Wi-Fi 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. Figure 7.13 shows the various NFC types, components, and its usage.

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 (electromagnetic) 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.

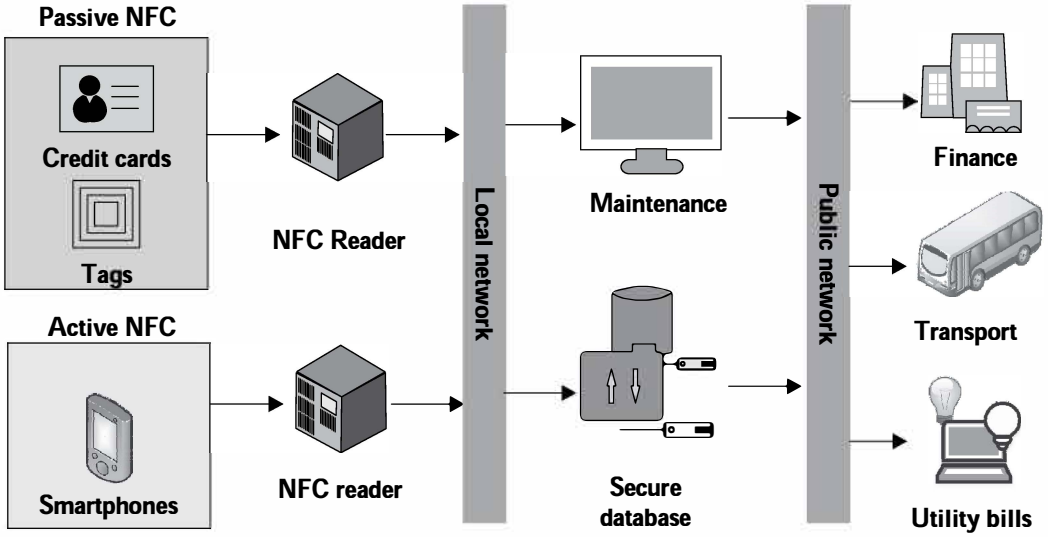


Figure 7.13 An outline of the NFC operation and communication

Passive NFC devices do not need a power source for communicating with the NFC reader. Tags and other small transmitters can act as passive NFC devices. 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 as 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; it 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.

7.10 Z-Wave

Z-Wave is an economical and less complicated alternative to Zigbee. It was developed by Zensys, mainly for home automation solutions [11]. It boasts of a power consumption much lower than Wi-Fi, but with ranges greater than Bluetooth. This feature makes Z-Wave 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. Figure 7.16 shows the network architecture of the Z-Wave protocol.

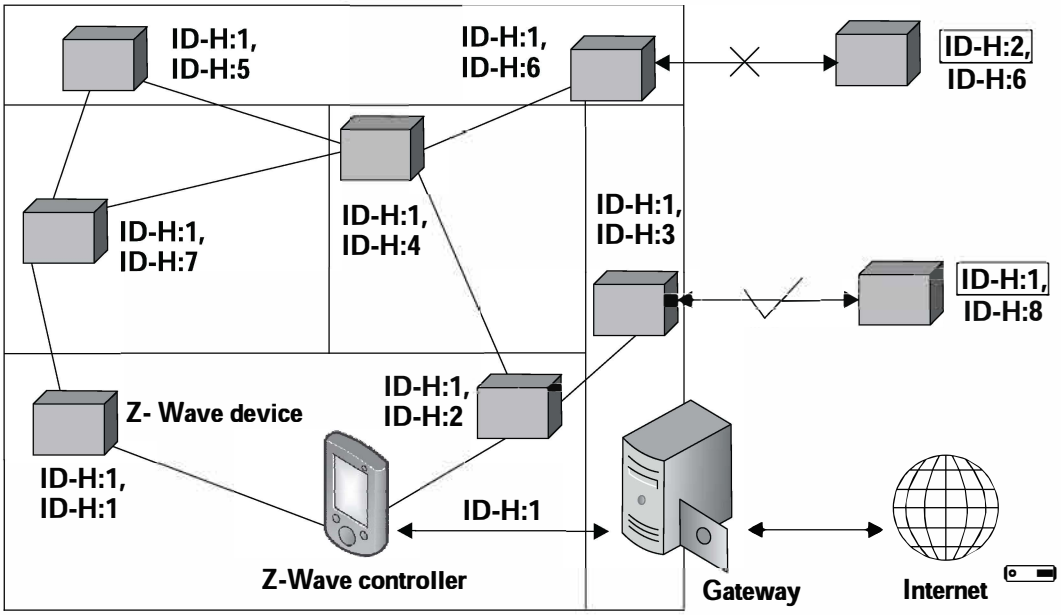


Figure 7.16 A typical Z-Wave deployment and communication architecture

Figure 7.17 shows the stack for this protocol. The Z-Wave operational frequency is in the range of 800–900 MHz, which makes it mostly immune to the interference effects of Wi-Fi and other radios utilizing the 2.4 GHz frequency band. Z-wave utilizes gaussian frequency shift keying (GFSK) modulation, where the baseband pulses are passed through a Gaussian filter before modulation. The 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.

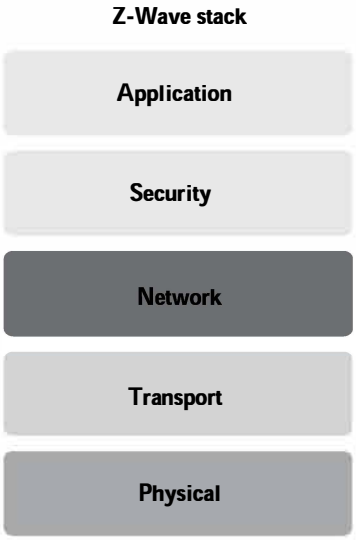


Figure 7.17 The Z-Wave protocol stack

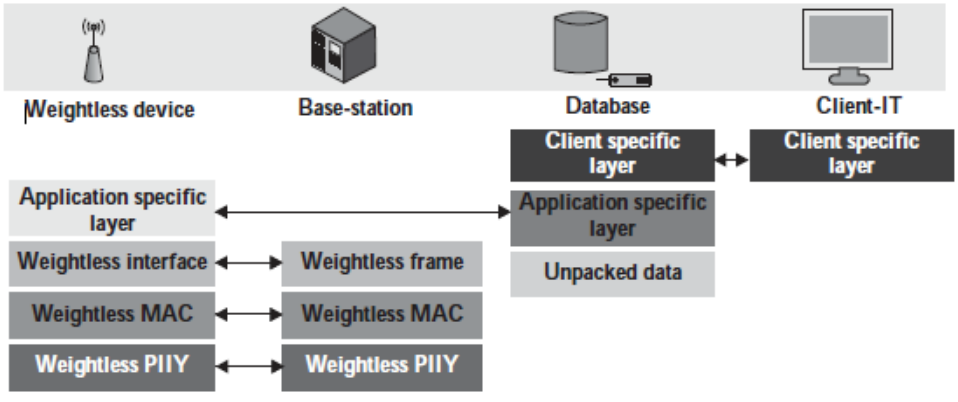
Z-wave devices are mostly configured to connect to home-based routers and access points. These routers and access points are responsible for forwarding Z-wave messages to a central hub. Z-wave devices can also be configured to connect to the central hub directly if they are in range. Z-wave routing within 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 a characteristic of Z-wave.

A central network controller device sets up and manages a Z-wave network (Figure 7.16), 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 is 1 byte. 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; only static devices are considered.

7.11 Weightless

Weightless is yet another emerging open standard for enabling networked communication in IoT; it is especially useful for low-power wide area networks [12]. It was designed for useful for low-power, low-throughput, and moderate to high latency applications supporting either or both public and private networks. The operating frequency of Weightless is restricted to sub-GHz bands, which are also exempted from the requirements of licensing such as 138 MHz, 433 MHz, 470 MHz, 780 MHz, 868 MHz, 915 MHz, and 923 MHz. Initially, three standards were released for Weightless: Weightless P, Weightless N, and Weightless W. Weightless P is the only currently accepted and used standard as it has features for bi-directional communication over both licensed as well as unlicensed ISM bands. Weightless N was designed as an LWPAN uplink-only technology, whereas Weightless W was designed to make use of the TV whitespace frequencies for communication.

As Weightless P was the most commonly adopted and accepted standard among the three Weightless standards, it came to be referred to merely as Weightless. Weightless provides a true bi-directional and reliable means of communication, where each message transaction is validated using an acknowledgment message. As it was designed initially for dense deployments of low-complexity IoT end devices, its payload size was limited to less than 48 bytes. Weightless networks can be optimized to attain ultra-low-power consumption status compared to cellular networks. However, this is at the cost of network latency and throughput with data rates in the range of 0.625 kbps to 100 kbps. Weightless has been identified with three architectural components: end devices, base stations, and base station network (Figure 7.18). The end devices (ED) form the leaf nodes in the Weightless network. These devices are typically low complexity and low cost. The duty cycle of EDs is also low, with a nominal transmiting power of 14 dBm (which can be increased up to 30 dBm).The base stations (BS) act as the central coordinating node in each cell. A star topology is deployed to connect the EDs to the BS. The transmit powers of a typical BS lie in the range of 27 dBm to 30 dBm. Finally, the base station network (BSN) is responsible for connecting all the BS of a single network. This enables the BSN to manage the allocation and scheduling of radio resources across the network. Additional tasks of the BSN include addressing authentication, roaming, and scheduling responsibilities.



7.13 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 [14]. It is a sub-GHz wireless technology that operationally uses the 169 MHz, 433 MHz, 868 MHz, and 915 MHz frequency bands for communication. LoRa uses bi-directional communication links symmetrically and 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 of devices. Figure 7.21 shows the LoRa network architecture.

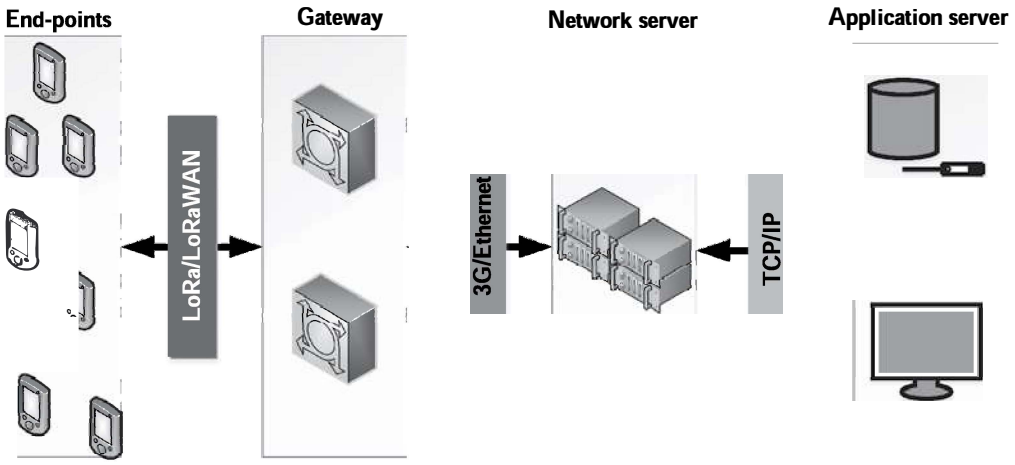


Figure 7.21 A typical LoRa deployment and communication architecture

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. Figure 7.22 shows the LoRa protocol stack.

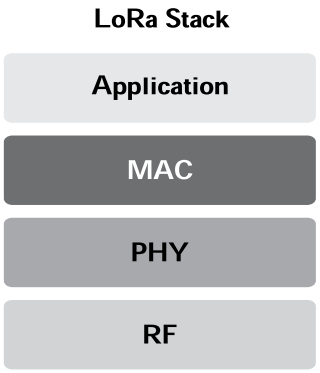


Figure 7.22 The LoRa protocol stack

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 solved using 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 an architecture that makes 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.

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 (Figure 7.21). 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 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, and 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, which ensures security on the network level, unique application key, which ensures an end-to-end security on the application level and device specific key.

7.15 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 (Figure 7.25). 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 [16]. 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.

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 5 GHz band using OFDM for communication. IEEE 802.11b achieves a data rate of 11 Mbps and operates on the 2.4 GHz band. Similarly, IEEE 802.11g also works on the 2.4 GHz band but achieves higher data rates of 54 Mbps using OFDM. Finally, the newest version, IEEE 802.11n, can transmit data at a rate of 140 Mbps on the 5 GHz band.

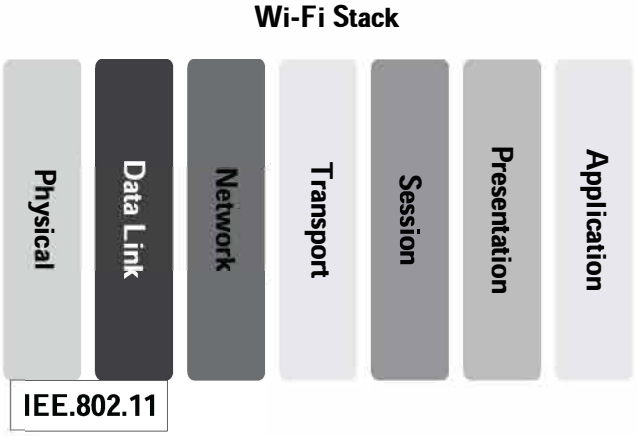


Figure 7.25 The IEEE 802.11 Wi-Fi stack

Wi-Fi devices can network using a technology referred to as wireless LAN (WLAN), as shown in Figure 7.26. A Wi-Fi enabled device has to connect to a wireless access point, which connects the device to the WLAN. WLAN is then responsible for forwarding the messages from the devices to and fro between the devices and the Internet.

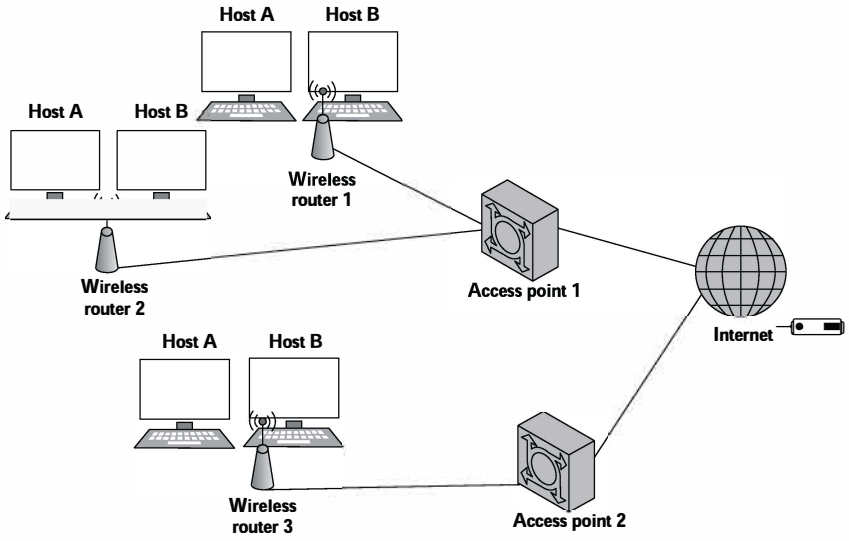


Figure 7.26 The Wi-Fi deployment architecture

Bluetooth

Bluetooth is defined by the IEEE 802.15.1 standard and is a short-range wireless communication technology operating at low power to enable communication among two or more Bluetooth-enabled devices [17]. It was initially developed as a cable replacement technology for data communication between two or more mobile devices such as smartphones and laptops. This standard allows the transmission of data as well as voice-over short distances. Bluetooth functions on the 2.4 GHz ISM band and has a range of approximately 10 m. The transmission of data is done through frequency hopping spread spectrum (FHSS), which also reduces the interference caused by other devices functioning in the 2.4 GHz band. The data is divided into packets before transmitting them by Bluetooth. The packets are transmitted over the 79 designated channels, each 1MHz wide in the 2.4 GHz band. Adaptive frequency hopping (AFH) enables this standard to perform 800 hops per second over these channels. Initial versions of this standard followed Gaussian frequency shift keying (GFSK) modulation, which was known as the basic rate (BR) mode, and was capable of data rates of up to 1 Mbps. However, with the development of newer variants, modulation schemes such as $\pi/4$ DQPSK (differential quadrature phase shift keying) and 8-DPSK (differential phase shift keying) were adopted, which enabled data rates of 2 Mbps and 3 Mbps respectively.

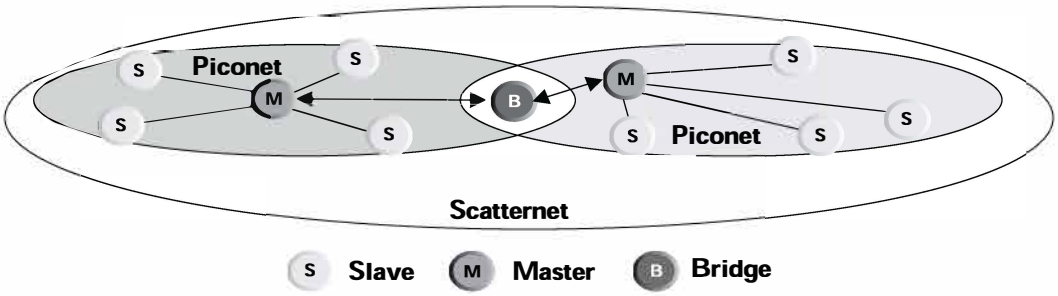


Figure 7.27 The Bluetooth device network architecture

Bluetooth follows a master–slave architecture (Figure 7.27). It enables a small network, which can accommodate seven slave devices simultaneously with a single master node. A slave node in one piconet cannot be part of another piconet at the same time, that is, it can have a single master node at a time. This network is known as a personal area network (PAN) or piconet. All the devices in a piconet share the master node's clock. Two piconets can be joined using a bridge. The whole network is also referred to as a scatternet.

Bluetooth Low Energy (BLE), the advanced variant of Bluetooth has 2 MHz wide bands, which can accommodate 40 channels. Its features include low energy consumption, low cost, multivendor interoperability, and an enhanced range of operations.

Bluetooth connections are encrypted and prevent eavesdropping of communications between devices. The inclusion of service-level security adds an additional layer of security by restricting the usage and device features and activities.

The Bluetooth standard consists of four parts: 1) core protocols, 2) cable replacement protocols, 3) telephony control protocols, and 4) adopted protocols. Figure 7.28 shows the Bluetooth protocol stack. Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), Host Controller Interface (HCI), Radio Frequency Communications (RFCOMM), and Service Discovery Protocol (SDP) are some of the well-known protocols associated with Bluetooth. These protocols can be enumerated as follows:

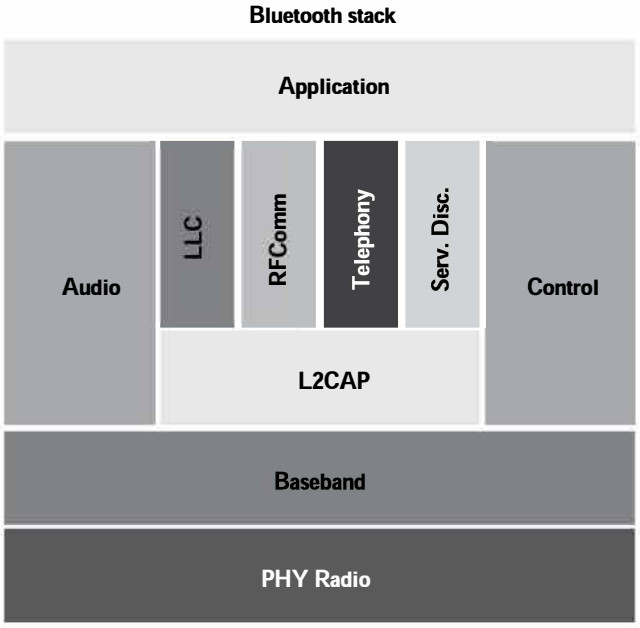


Figure 7.28 The Bluetooth protocol stack

(i) **Link Manager Protocol:** It manages the establishment, authentication, and links configuration. LMPs consist of some protocol data units (PDU), between which transmission occurs for availing services such as name requests, link address requests, connection establishment, connection authentication, mode negotiation, and data transfer.

(ii) **Host Controller Interface:** It enables access to hardware status and control registers and connects the controller with the link manager. The automatic discovery of Bluetooth devices in its proximity is one of the essential tasks of HCI.

(iii) L2CAP: It multiplexes logical connections between two devices. It is also tasked with data segmentation, flow control, and data integrity checks.

(iv) Service Discovery Protocol: It is tasked with the discovery of services provided by other Bluetooth devices.

(v) Radio Frequency Communications: It is a cable replacement protocol, which generates a virtual stream of serial data. This protocol supports many telephony related profiles as AT commands and Dbject Exchange Protocol (DBEX) over Bluetooth.

(vi) Telephony Control Protocol - Binary (TCS BIN): It is a bit-oriented protocol to control call signaling prior to initiation of voice or data communications between devices.