3 CONNECTIVITY TECHNOLOGIES

3.1 Introduction

In the previous Chapter, we have already discussed some important identification and data protocols like IPv4, IPv6, MQTT, CoAP, XMPP and AMQP. In this Chapter we will be discussing some other important communication protocols which have immediate importance to consumer and industrial IoTs. The connectivity technologies that will be discussed in this Chapter are IEEE 802.15.4, ZigBee, 6LoWPAN, Wireless HART, Z-Wave, ISA 100, Bluetooth, NFC and RFID. We will see each technology in detail.

3.2 IEEE 802.15.4

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of Wireless Personal Area Network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more.

IEEE 802.15.4 was developed for low data rate monitoring and control applications with extended life, low power consumption uses. This standard uses only the first two layers (PHY, MAC). In addition to this, the Logical Link Control (LLC) and Service Specific Convergence Sub-layer (SSCS) are used to communicate with all upper layers. This protocol operates in the ISM band. The industrial, scientific, and medical radio band (ISM band) refers to a group of radio bands or parts of the radio spectrum that are internationally reserved for the use of radio frequency (RF) energy intended for scientific, medical and industrial requirements rather than for communications. Devices are conceived to interact with each other over a conceptually simple wireless network. The definition of the network layers is based on the OSI model; although only the lower layers are defined in the standard, interaction with upper layers is intended, possibly using an IEEE 802.2 logical link control sub-layer accessing the MAC through a convergence sub-layer. Implementations may rely on external devices or be purely embedded, self-functioning devices. Figure 3.1 shows the architecture of IEEE 802.15.4.

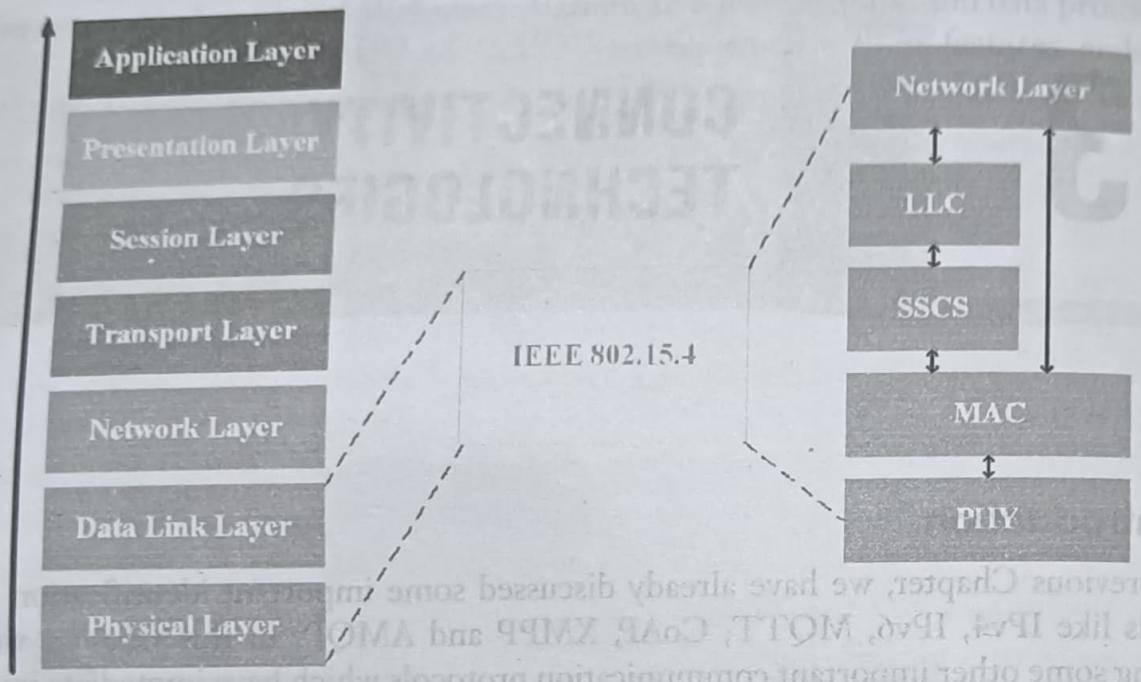


Fig.3.1: Architecture of IEEE 802.15.4

The standard uses Direct Sequence Spread Spectrum (DSSS) modulation. It is highly tolerant of noise and interference and offers coding gain to improve link reliability. Standard binary phase-shift keying (BPSK) is used in the two low-speed versions, while offset-quadrature phase-shift keying (O-QPSK) is used for the higher-data-rate version. O-QPSK has a constant wave envelope meaning that more efficient non-linear power amplification techniques can be used to minimize power consumption.

With regard to channel access, 802.15.4 uses carrier sense multiple access with collision avoidance (CSMA-CA). This multiplexing approach lets multiple users or nodes access the same channel at different times without interference. Most transmissions are short packets that occur infrequently for a very low duty cycle (<1 %), minimizing power consumption. The minimum power level defined is –3 dBm or 0.5 mW. Most modules use 0 dBm or 1 mW. However, some 20-dBm or 100-mW modules are available.

Transmission range varies considerably depending on the nature of the path that must for the most part be line of sight (LOS). Transmission power level and receiver sensitivity are also factors. Under the best conditions the range can be as great as 1000 meters with a clear outdoor path. Most applications cover a shorter range of 10 to 75 meters.

With regard to networking capability, 802.15.4 defines two topologies. One of them is a basic star topology given in Figure 3.2 (a). All communications between nodes must pass through the central coordinator node. A basic peer-to-peer (P2P) topology is also defined in IEEE 802.15.4 which is given in Figure 3.2(b). Any device may then talk to any other device. This basic topology may be expanded into other topologies in the upper network layers, such as the popular mesh topology.

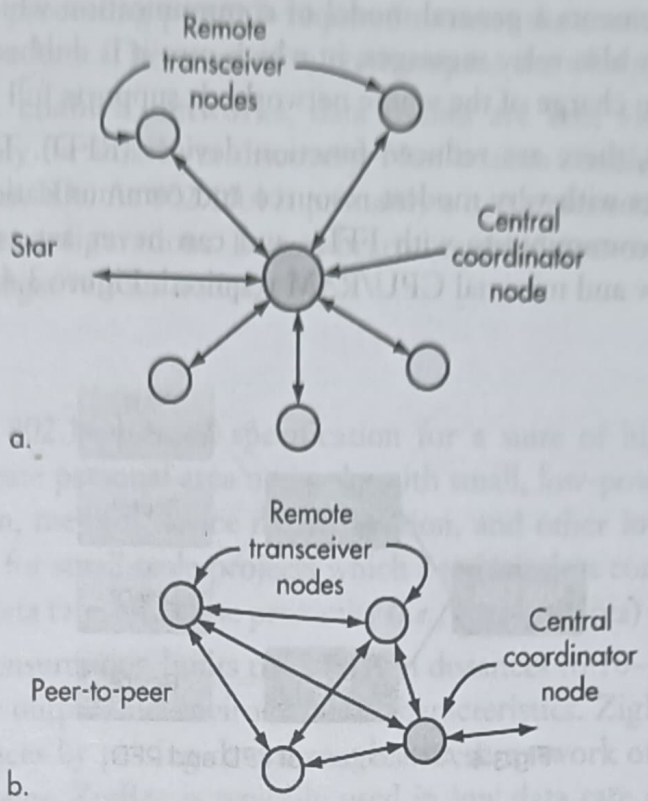


Fig.3.2: Star and Peer-to-Peer Topologies

There are different variants for IEEE 802.15.4. Figure 3.3 gives the different variants of IEEE 802.15.4.

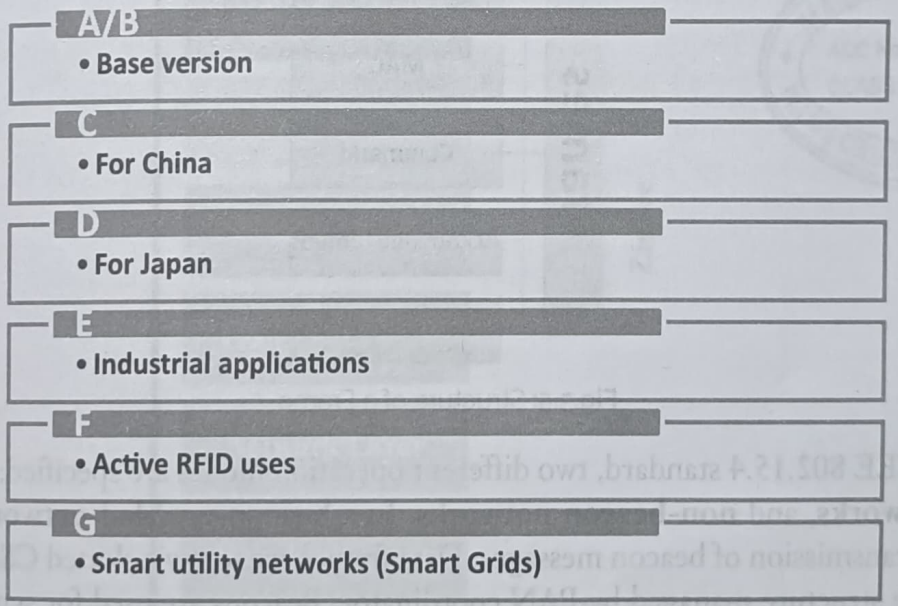


Fig.3.3: Variants of IEEE 802.15.4

IEEE 802.15.4 defines two types of network node. The first one is the full-function device (FFD). It can serve as the coordinator of a personal area network just as it may function as a

common node. It implements a general model of communication which allows it to talk to any other device. It may also relay messages, in which case it is dubbed a coordinator (PAN coordinator when it is in charge of the whole network). It supports full protocol.

On the other hand, there are reduced-function devices (RFD). These are meant to be extremely simple devices with very modest resource and communication requirements. Due to this, they can only communicate with FFDs and can never act as coordinators. Power consumption is very low and minimal CPU/RAM required. Figure 3.4 shows architecture of FFD and RFD.

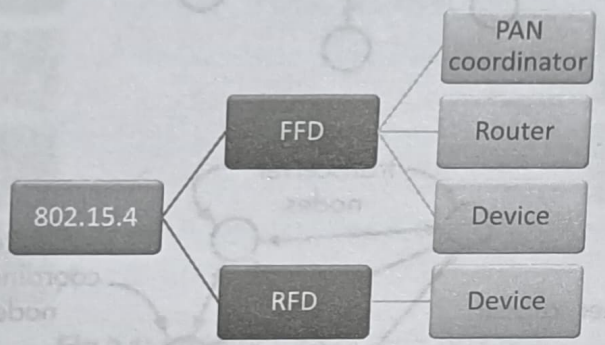


Fig.3.4: Architecture of FFD and RFD

Frames are the basic unit of data transport, of which there are four fundamental types (data, acknowledgment, beacon and MAC command frames), which provide a reasonable tradeoff between simplicity and robustness. Figure 3.5 shows the structure of a frame.

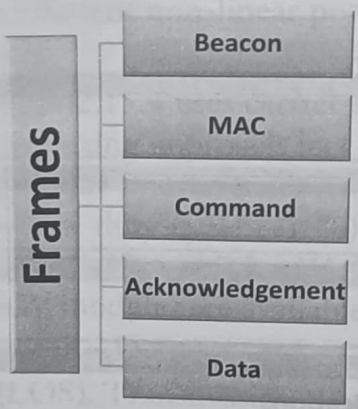


Fig.3.5: Structure of a Frame

In the IEEE 802.15.4 standard, two different operation modes are specified: the **beacon-enabled networks**, and **non-beacon networks**. In a **beacon-enabled network**, there will be periodic transmission of beacon messages. Data frames are sent via slotted CSMA/CA with a super frame structure managed by PAN coordinator. Beacons are used for synchronization and association of other nodes with the coordinator. The devices in a beacon-enabled network synchronize with each other and the beacon frame which is treated as synchronization signal also provides some extended features. On the other hand, a beacon-enabled device is hard

to implement. High processing power is required to meet the constrained timing events and process the beacon packets. The scope of operation spans the whole network.

In **non-beacon enabled networks**, data frames are sent via un-slotted CSMA/CA. Beacons are used only for link layer discovery. Non-beacon enabled networks require both source and destination IDs. As 802.15.4 is primarily a mesh protocol, all protocol addressing must adhere to mesh configurations. In non-beacon enabled networks, there is decentralized communication amongst various nodes.

3.3 ZigBee

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. It is 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.

It's low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics. ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. ZigBee is typically used in low data rate applications that require long battery life and secure networking. ZigBee networks are secured by 128 bit symmetric encryption keys. ZigBee has a defined rate of 250 Kbits/s, best suited for intermittent data transmissions from a sensor or input device.

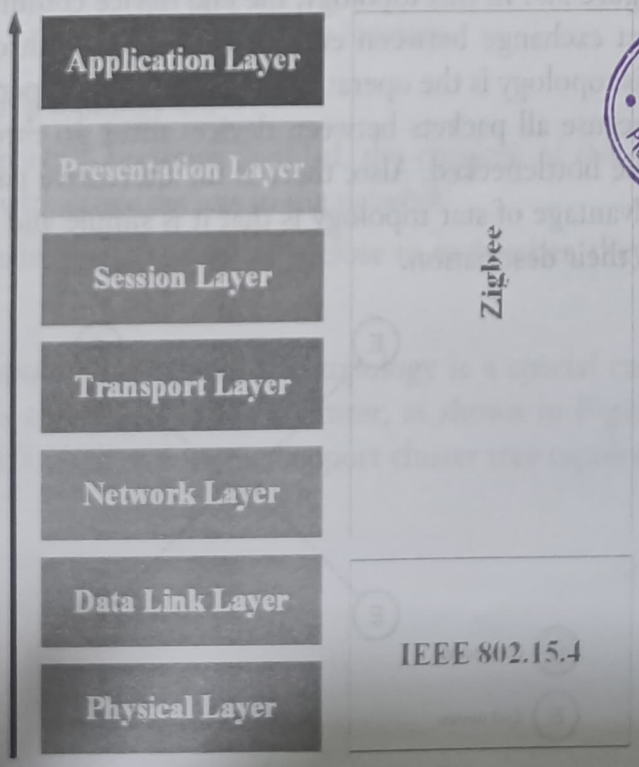


Fig.3.6: Structure of ZigBee

The most widely deployed enhancement to the 802.15.4 standard is ZigBee, which is a standard of the ZigBee Alliance. The organization maintains, supports and develops more sophisticated protocols for advanced applications. It uses layers 3 and above to define additional communication features as shown in Figure 3.6. It works with the 802.15.4 layers 1 and 2. These enhancements include authentication with valid nodes, encryption for security and a data routing and forwarding capability that enables mesh networking.

The ZigBee network layer uses Ad-hoc On Demand Distance Vector (AODV) routing. To find the final destination, The AODV broadcasts a route request to all of its immediate neighbours. The neighbours relay the same information to their neighbours eventually spreading the request throughout the network. Upon discovery of the destination, a low-cost path is calculated and informed to the requesting device via unicast messaging.

ZigBee has two important components. They are ZigBee Device Object (ZDO) and Application Support Sub-layer (APS). ZDO is responsible for device management, security and policies whereas APS is responsible for interfacing and controlling devices, bridge between network and other layers.

ZigBee Topologies

IEEE 802.15.4 offers star, tree, cluster tree, and mesh topologies. However, ZigBee supports only star, tree and mesh topologies. It uses an association hierarchy. A device joining the network can either be a router or an end device and routers can accept more devices.

Star Topology: The star topology consists of a coordinator and several end devices (nodes), as shown in Figure 3.7. In this topology, the end device communicates only with the coordinator. Any packet exchange between end devices must go through the coordinator. The disadvantage of this topology is the operation of the network depends on the coordinator of the network, and because all packets between devices must go through coordinator, the coordinator may become bottlenecked. Also, there is no alternative path from the source to the destination. The advantage of star topology is that it is simple and packets go through at most two hops to reach their destination.

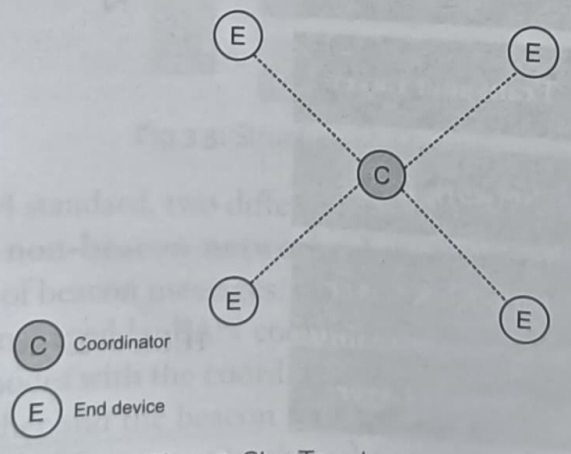


Fig.3.7: Star Topology

Tree Topology: In this topology, the network consists of a central node (root tree), which is a coordinator, several routers, and end devices, as shown in Figure 3.8. The function of the router is to extend the network coverage. The end nodes that are connected to the coordinator or the routers are called children. Only routers and the coordinator can have children. Each end device is only able to communicate with its parent (router or coordinator). The coordinator and routers can have children and, therefore, are the only devices that can be parents. An end device cannot have children and, therefore, may not be a parent. A special case of tree topology is called a cluster tree topology.

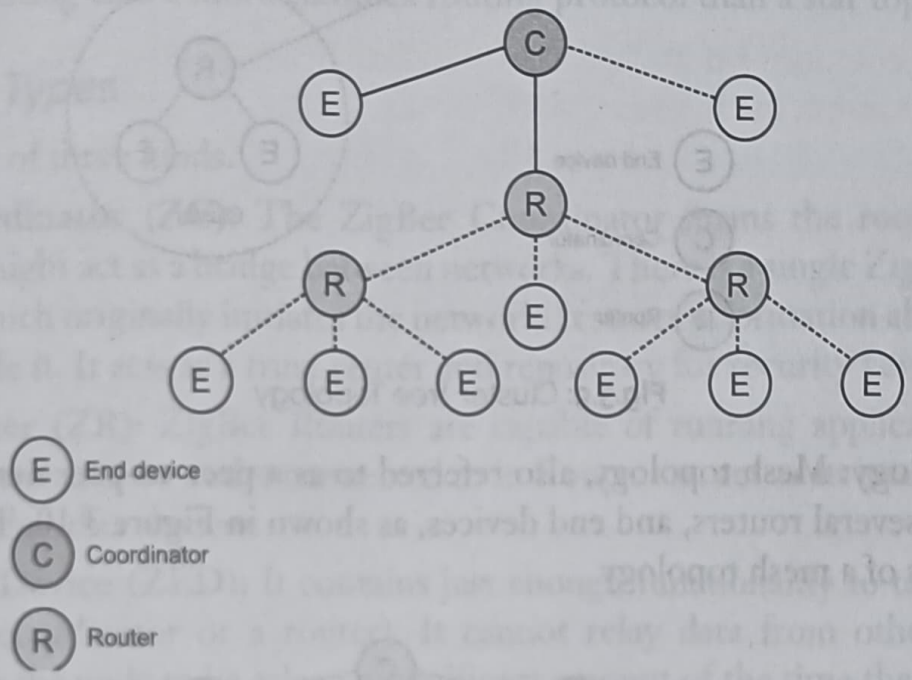


Fig.3.8: Tree Topology

The disadvantages of tree topology are—

a. If one of the parents becomes disabled, the children of the disabled parent cannot communicate with other devices in the network.

b. Even if two nodes are geographically close to each other, they cannot communicate directly.

Cluster Tree Topology: A cluster tree topology is a special case of tree topology in which a parent with its children is called a cluster, as shown in Figure 3.9. Each cluster is identified by a cluster ID. ZigBee does not support cluster tree topology, but IEEE 802.15.4 does support it.

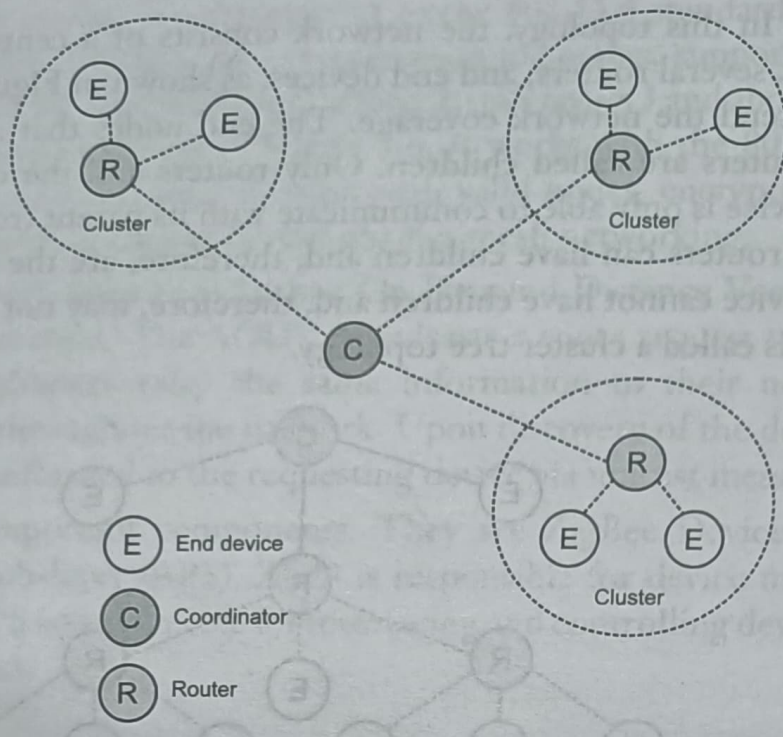


Fig.3.9: Cluster Tree Topology

Mesh Topology: Mesh topology, also referred to as a peer-to-peer network, consists of one coordinator, several routers, and end devices, as shown in Figure 3.10. The following are the characteristics of a mesh topology.

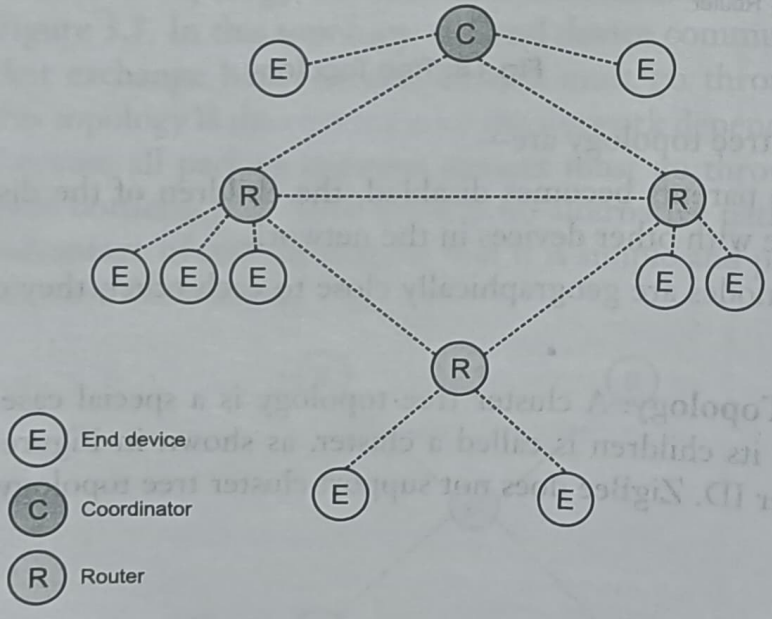


Fig.3.10: Mesh Topology

a. A mesh topology is a multi-hop network. Packets pass through multiple hops to reach their destination.

b. The range of a network can be increased by adding more devices to the network.

c. It can eliminate dead zones.
d. A mesh topology is self-healing, meaning during transmission, if a path fails, the node will find an alternate path to the destination.
e. Devices can be close to each other so that they use less power.
f. Adding or removing a device is easy.
g. Any source device can communicate with any destination device in the network.

The disadvantages are compared with star topology, mesh topology requires greater overhead. Mesh routing uses a more complex routing protocol than a star topology.

ZigBee Device Types

ZigBee devices are of three kinds.

ZigBee Coordinator (ZC): The ZigBee Coordinator forms the root of the ZigBee network tree and might act as a bridge between networks. There is a single ZigBee coordinator in each network which originally initiates the network. It stores information about the network under it and outside it. It acts as a trust center and repository for security keys.

ZigBee Router (ZR): ZigBee Routers are capable of running applications as well as relaying information between nodes connected to it. Router can act as an intermediate router, passing on data from other devices.

ZigBee End Device (ZED): It contains just enough functionality to talk to the parent node (either the coordinator or a router). It cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires least amount of memory and therefore can be less expensive to manufacture than a ZR or ZC.

Applications

ZigBee finds application in the following domains.

a. Building automation.
b. Remote Control (RF4CE or RF for consumer electronics).
c. Smart energy for home energy monitoring.
d. Healthcare for medical and fitness monitoring.
e. Home automation for control of smart homes.
f. Light link for control of LED lighting.
g. Telecom services.

3.4 6LoWPAN

6LoWPAN is an acronym of IPv6 over Low-Power Wireless Personal Area Networks. 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. It allows low power devices to connect to the Internet. 6LoWPAN was created by Internet Engineering Task Force (IETF). The 6LoWPAN protocol is based on IPv6 and operates in a fully asynchronous way. It adopts a mesh topology and uses a routing algorithm which does not take care of the sleeping node thus requiring approaches such as low-power listening for energy saving purpose.

The features of 6LoWPANs are the following:

a. It allows IEEE 802.15.4 radios to carry 128 bit addresses of Internet Protocol Version 6 (IPv6).
b. Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the Internet.
c. IPv6 packets are compressed and reformatted to fit the IEEE 802.15.4 packet format.
d. Requires low bandwidth.
e. Consumes low power and typically battery operated.
f. Supports star and mesh topologies.
g. Relatively low cost with other technologies.

The 128 bits of IPv6 addresses are divided in two parts: The network prefix (64 bits) and the host address (64 bits). The 6LoWPAN header compression mechanism omits the 64 most significant bits (network prefix) because they're fixed for a given 6LoWPAN. Moreover, the 64 least significant bits can address very large address space (up to 1.84467441×1019). Therefore, 6LoWPAN provides options for compressing the host address (the common usage is 16 bits). In a nutshell, a 128-bit IPv6 address can be compressed down to 16 bits using 6LoWPAN. Figure 3.11 shows the packet format of 6LoWPAN.

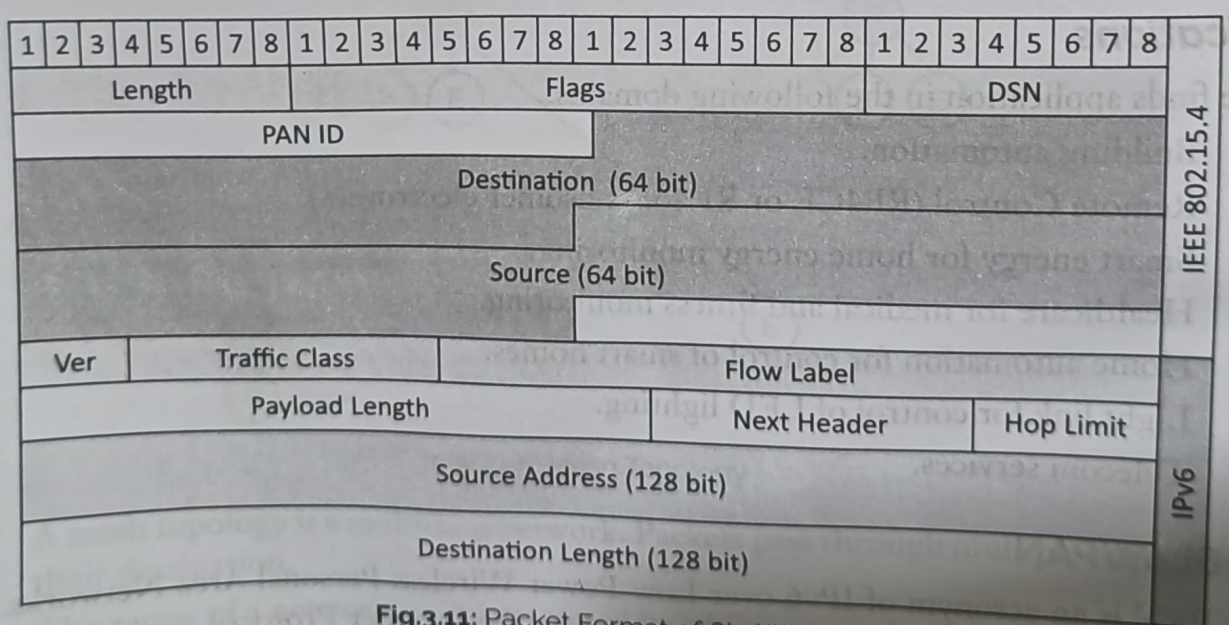


Fig.3.11: Packet Format of 6LoWPAN

Version – 4-bit Internet Protocol version number = 6.
Traffic Class – 8-bit traffic class field.
Flow Label – 20-bit flow label.
Payload Length – 6-bit unsigned integer. Length of the IPv6 header is in octets.
Next Header – 8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 protocol field.
Hop Limit – 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if hop limit is decremented to zero.
Source Address – 128-bit address of the originator of the packet.
Destination Address – 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient, if a routing header is present).

6LoWPAN Headers

There are 3 types of header for 6LoWPAN—Dispatch header, Mesh addressing header and Fragmentation header.

Dispatch Header

It is a 32-bit header. 0, 1 is the identifier for dispatch type. Dispatch initiates communication. This is a 6-bit and identifies the next header type. The Type Specific Header is determined by Dispatch header. Figure 3.12 shows the dispatch header.

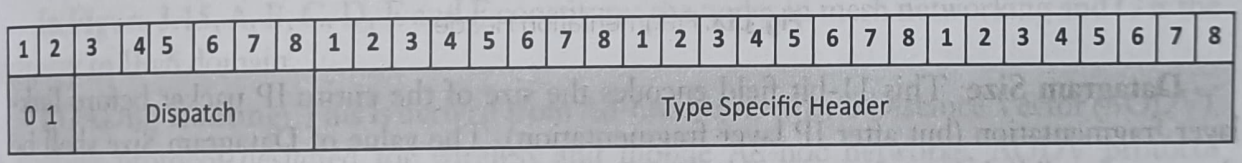


Fig.3.12: Dispatch Header

Mesh Addressing Header

It is a 32-bit header. 1, 0 is the identifier for mesh addressing header. V has 2 values 0 and 1. The value of V is 0, if originator is 64-bit extended address and 1 if 16-bit address. Similarly F has 2 values 0 and 1. The value of F is 0 if destination is 64-bit address and 1 if 16-bit address. Hops Left is decremented by each node before sending to next hop. Originator address is the source address and Final address is the destination address. Figure 3.13 shows the mesh addressing header.

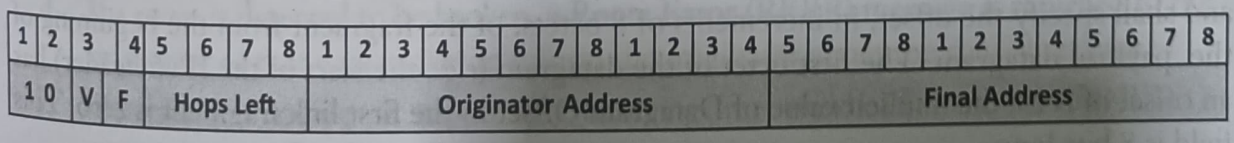
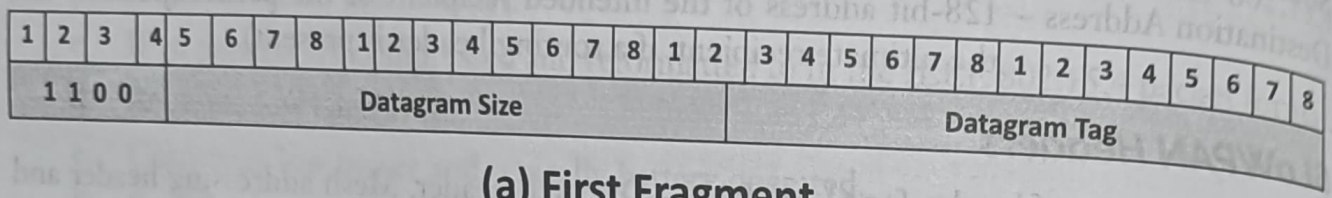


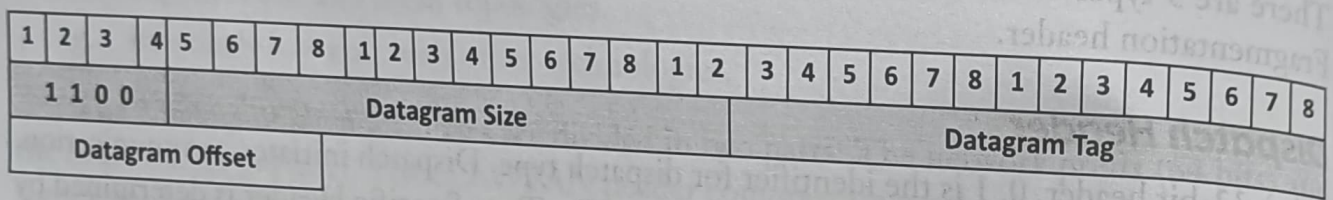
Fig.3.13: Mesh Addressing Header

Fragmentation Header

In fragmentation header, the first fragment is 32 bits and the subsequent fragment is also 32 bits. If an entire payload (*e.g.*, IPv6) datagram fits within a single 802.15.4 frame, it is unfragmented and the 6LoWPAN encapsulation should not contain a fragmentation header. If the datagram does not fit within a single IEEE 802.15.4 frame, it shall be broken into link fragments. As the fragment offset can only express multiples of eight bytes, all link fragments for a datagram except the last one must be multiples of eight bytes in length. The first link fragment shall contain the first fragment header and the second and subsequent link fragments (up to and including the last) shall contain a fragmentation header that conforms to the format shown in Figure 3.13.



(a) First Fragment



(b) Subsequent Fragment

Fig.3.14: Fragmentation Header

Datagram Size: This 11-bit field encodes the size of the entire IP packet before link-layer fragmentation (but after IP layer fragmentation). The value of Datagram Size shall be the same for all link-layer fragments of an IP packet. For IPv6, this shall be 40 octets (the size of the uncompressed IPv6 header) more than the value of Payload Length in the IPv6 header [RFC2460] of the packet. Note that this packet may already be fragmented by hosts involved in the communication, *i.e.*, this field needs to encode a maximum length of 1280 octets.

Datagram Tag: The value of Datagram Tag shall be the same for all link fragments of a payload (*e.g.*, IPv6) datagram. The sender shall increment Datagram Tag for successive, fragmented datagrams. The incremented value of Datagram Tag shall wrap from 65535 back to zero. This field is 16 bits long, and its initial value is not defined.

Datagram Offset: This field is present only in the second and subsequent link fragments and shall specify the offset, in increments of 8 octets, of the fragment from the beginning of the payload datagram. The first octet of the datagram (*e.g.*, the start of the IPv6 header) has an offset of zero; the implicit value of Datagram Offset in the first link fragment is zero. This field is 8 bits long.

6LoWPAN Routing

Routing is a two phased problem that is being considered for low-power IP networking. Mesh routing in the Personal Area Network (PAN) space and routing of packets between the IPv6 domain and the PAN domain. There are several protocols used but the commonly used ones are LOADng and RPL. Figure 3.14 shows the architecture of 6LoWPAN routing.

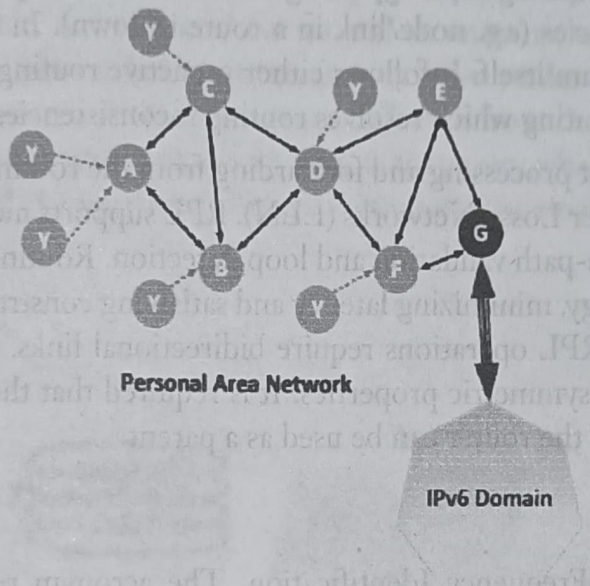


Fig.3.15: Architecture of 6LoWPAN Routing

In Figure 3.15, A, B, C, D, E and F constitutes the nodes in mesh networking and G is the gateway to IPv6 domain.

LOADng Routing: This is derived from Ad-hoc On-Demand Distance Vector (AODV), a routing protocol designed for wireless and mobile Ad-hoc networks. AODV protocol establishes routes to destinations on demand and supports both unicast and multicast routing. LOADng routing is extended for use in IoT. Basic operations of LOADng include the following.

a. Generation of Route Requests (RREQs) by a LOADng router (originator) for discovering a route to a destination.
b. Forwarding of such RREQs until they reach the destination LOADng router.
c. Generation of Route Replies (RREPs) upon receipt of an RREQ by the indicated destination and unicast hop by hop forwarding of these RREps towards the originator.
d. If a route is detected to be broken, a Route Error (RERR) message is returned to the originator of that data packet to inform the originator about the route breakage.
e. Optimized flooding is supported, reducing the overhead incurred by RREQ generation and flooding.
f. Only the destination is permitted to respond to an RREQ.

g. Intermediate LOADng routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.
h. RREQ/RREP messages generated by a given LOADng router share a single unique monotonically increasing sequence number.

RPL Routing: RPL stands for IPv6 Routing Protocol for Low-Power and Lossy Networks. This routing maintains routing topology using low rate beaconing. Beaconing rate increases on detecting inconsistencies (*e.g.* node/link in a route is down). In this, routing information is included in the datagram itself. It follows either proactive routing that maintains a routing topology or a reactive routing which resolves routing inconsistencies.

RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low-power Lossy Networks (LLN). RPL supports message confidentiality and integrity. It supports data-path validation and loop detection. Routing optimization objectives include minimizing energy, minimizing latency and satisfying constraints with respect to node power, band width etc. RPL operations require bidirectional links. In some LLN scenarios, those links may exhibit asymmetric properties. It is required that the reachability of a router should be verified before the router can be used as a parent.

3.5 RFID

RFID stands for Radio-Frequency Identification. The acronym refers to small electronic devices that consist of a small chip and an antenna. The chip typically is capable of carrying 2,000 bytes of data or less. The RFID device serves the same purpose as a bar code or a magnetic strip on the back of a credit card or ATM card. It provides a unique identifier for that object. And, just as a bar code or magnetic strip must be scanned to get the information, the RFID device must be scanned to retrieve the identifying information.

Data read from RFID tags are stored in a database by the reader. As compared to traditional bar codes and QR codes, RFID data can be read outside the line of sight. RFID tag consists of an integrated circuit and an antenna. The tag is covered by a protective material which also acts as a shield against various environmental effects. Tags may be passive or active. Passive RFID tags are the most widely used. Passive tags have to be powered by a reader inductively before they can transmit information, whereas active tags have their own power supply. The applications of RFID can be found in various domains as follows.

- Inventory management
- Asset tracking
- Personnel tracking
- Controlling access to restricted areas
- ID badging
- Supply chain management
- Counterfeit prevention (*e.g.* In the pharmaceutical industry)

Working of RFID

RFID technology is derived from Automatic Identification and Data Capture (AIDC) technology. AIDC performs object identification, object data collection and mapping of the collected data to computer systems with little or no human intervention. AIDC uses wired communication. RFID uses radio waves to perform AIDC functions. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which is used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time. Figure 3.16 shows the working principle of RFID.

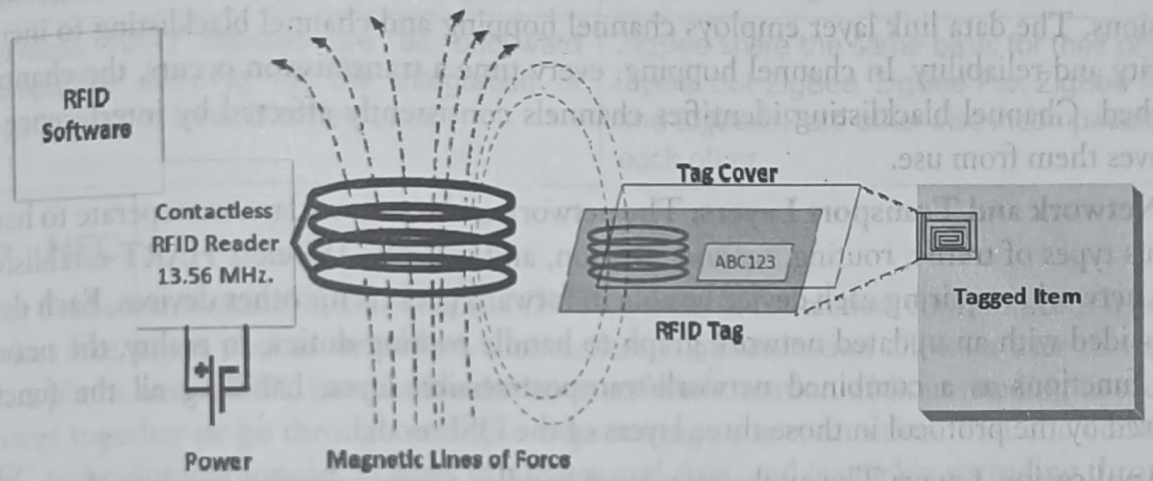


Fig.3.16: Working Principle of RFID

3.6 HART and Wireless HART

HART is the acronym for Highway Addressable Remote Transducer Protocol. Wireless HART is the latest release of HART protocol. HART standard was developed for networked smart field devices. The wireless protocol makes the implementation of HART cheaper and easier. HART encompasses the 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. Figure 3.17 shows various layers in HART.

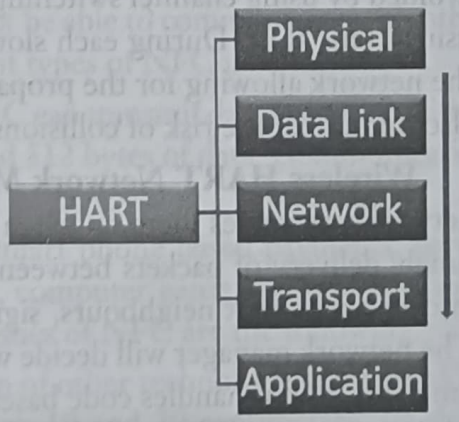


Fig.3.17: Various Layers in HART

HART includes five layers of the OSI model: physical layer, data link layer, network layer, transport layer, and application layer. The main difference

between the wired and unwired versions is in the physical layer, data link layer and network layer. In fact, wired HART does't have a network layer.

Physical Layer: The physical layer of the protocol is derived from the IEEE 802.15.4 standard. Basically, it is a subset of the IEEE standard with modifications. It only operates in one of the bands specified in the IEEE 802.15.4 standard – the 2450MHz ISM band. The physical layer employs 15 channels of the band which the data link layer exploits to increase reliability. Several transceivers developed to meet the IEEE standard have also been approved for use with Wireless HART, reducing development time and cost.

Data Link Layer: The data link layer introduces the use of superframes and Time Dimension Multiple Access (TDMA) technology to provide collision free, deterministic communication. Timeslots 10ms in length are grouped into superframes. These superframes are used to control the timing of transmissions to insure reliable communication and reduce collisions. The data link layer employs channel hopping and channel blacklisting to increase security and reliability. In channel hopping, every time a transmission occurs, the channel is switched. Channel blacklisting identifies channels consistently affected by interference and removes them from use.

Network and Transport Layers: The network and transport layers cooperate to handle various types of traffic, routing, session creation, and security. Wireless HART establishes a mesh network, requiring each device be able to forward packets for other devices. Each device is provided with an updated network graph to handle routing duties. In reality, the network layer functions as a combined network/transport/session layer, handling all the function required by the protocol in those three layers of the OSI model.

Application Layer: The application layer handles communication between the gateway and devices through a series of commands and responses. This layer extracts the command from a message, executes the command and generates a response. At this level, there is really no difference between the wired and wireless versions of the HART protocol.

HART Congestion Control: Due to its restricted use in certain areas, HART is restricted to 2.4 GHz ISM band with channel 26 removed. Interference-prone channels are avoided by using channel switching after every transmission. Transmissions are synchronized using 10ms slots. During each slot, all available channels can be utilized by various nodes in the network allowing for the propagation of 15 packets through the network at a time, which also minimizes the risk of collisions.

Wireless HART Network Manager: The network manager supervises each node in a network and guides them on when and where to send packets. It allows for collision-free and timely delivery of packets between a source and destination. The network manager updates information about neighbours, signal strength and information needing delivery or receipt. The network manager will decide who will send, who will listen and at what frequency is each time-slot. It also handles code based network security and prevents unauthorized nodes from joining the network.

Wireless HART versus ZigBee

Wireless HART	ZigBee
A wireless HART node hops after every message, changing channels every time it sends a packet.	ZigBee does not feature hopping at all and only hops when the entire network hops.
At the MAC layer, wireless HART utilizes Time Division Multiple Access (TDMA) allotting individual time slots for each transmission.	ZigBee applies Carrier Sense Multiple Access with Collision Detection. (CSMA/CD)
Wireless HART represents a true mesh network where each node is capable of serving as a router so that if one node goes down, another can replace it ensuring packet delivery.	ZigBee utilizes a tree topology which makes nodes along the trunk critical.
Wireless HART devices are all backward compatible allowing for the integration of legacy devices as well as new ones.	ZigBee share the same basis for their physical layers, but ZigBee, ZigBee Pro, ZigBee RF4CE and ZigBee IP are otherwise incompatible with each other.

3.7 NFC

Near field communication, abbreviated NFC, is a form of contactless communication between devices like smart phones or tablets. Contactless communication allows a user to wave the smart phone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection. Fast and convenient, NFC technology is popular in parts of Europe and Asia, and is quickly spreading throughout the United States. Near field communication maintains interoperability between different wireless communication methods like Bluetooth and other NFC standards including FeliCa which is popular in Japan.

The NFC forum enforces strict standards that manufacturers must meet when designing NFC compatible devices. This ensures that NFC is secure and remains easy-to-use with different versions of the technology. Compatibility is the key to the growth of NFC as a popular payment and data communication method. It must be able to communicate with other wireless technologies and be able to interact with different types of NFC transmissions.

NFC's data transmission frequency is 13.56 MHz. NFC can transmit data at a rate of either 106, 212 or 424 Kbps. Tags typically store between 96 and 512 bytes of data. Communication range is less than 20 cms.

NFC finds application in various domains such as smart phone based payments, parcel tracking, information tags in posters and advertisements, computer game synchronized toys, low power home automation systems etc. The characteristics of NFC are the following.

Wireless Connection: It is similar to the connection of other technologies such as WiFi or Bluetooth but with a shorter range, generally between 10 and 20 centimetres. Its short range allows for avoiding possible security problems such as the reading of our transmission.

Connection Speed: It has almost immediate connection with a transfer rate that can reach 424 Kbit/s.

Autonomy: The chips included in NFC technology do not need to be connected to a main battery.

Working of NFC

NFC works on the principle of magnetic induction. Figure 3.18 shows the working of NFC. A reader emits a small electric current which creates a magnetic field that in turn bridges the physical space between the devices. The generated field is received by a similar coil in the client device where it is turned back into electrical impulses to communicate data such as identification number status information or any other information.

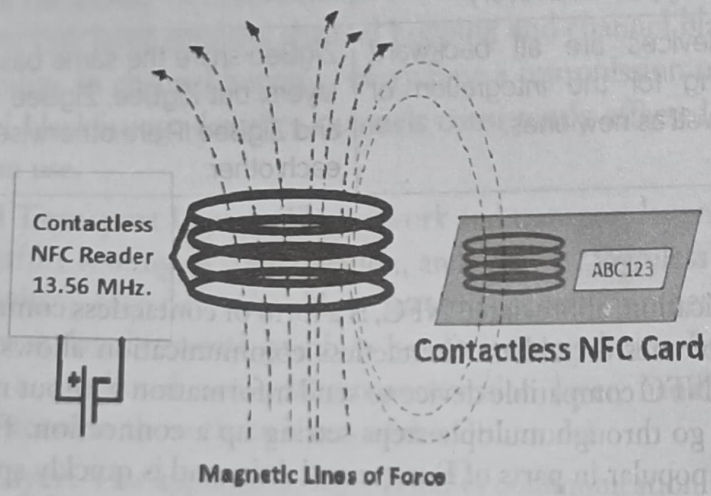


Fig.3.18: Working of NFC

Passive NFC tags use the energy from the reader to encode their response while active or peer-to-peer tags have their own power source.

NFC Types

There are two types of NFC devices–**passive devices** and **active devices**. Passive devices contain information which is readable by other devices. However, it cannot read information itself. NFC tags found in supermarket products are examples of passive NFC. Active devices are able to collect as well as transmit information. Smart phones are good examples of active devices. NFC tags are passive devices that can be used to communicate with active NFC devices (an active NFC reader/writer). The NFC tags can be used within applications such as posters and other areas where small amounts of data can be stored and transferred to active NFC devices. Within the poster the live area can be used as a touch point for the active NFC device.

The stored data on the NFC tag may contain any form of data, but common applications are for storing URLs from where the NFC device may find further information. NFC tags

may also be used. The NFC tag is a passive device with no power of its own. Accordingly when one is used, the users touch an NFC enabled device onto the tag. A small amount of power is taken by the NFC tag from the reader/writer to power the tag electronics. The tag is then enabled to transfer a small amount of information to the reader/writer.

The data stored in the tag memory is transferred to the NFC enabled device. Normally there will be a small amount of data in the tag memory and this may be used to direct the device to a website URL.

Modes of Operation

There are three modes of operation for NFC. They are **reader/writer, peer-to-peer** and card **emulation**. The different operating modes are based on the ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 contactless smart card standards.

In **reader/writer** mode, the NFC device is capable of reading NFC Forum-mandated tag types, such as a tag embedded in an NFC smart poster. The reader/writer mode on the RF interface is compliant with the ISO 14443 and FeliCa schemes.

In **Peer-to-Peer** mode, two NFC devices can exchange data. For example, we can share Bluetooth or WiFi link set-up parameters or we can exchange data such as virtual business cards or digital photos. Peer-to-Peer mode is standardized on the ISO/IEC 18092 standard.

In **Card Emulation** mode, the NFC device appears to an external reader much the same as a traditional contactless smart card. This enables contactless payments and ticketing by NFC devices without changing the existing infrastructure.

3.8 Bluetooth

Bluetooth wireless technology is a short range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Pico nets, which is a local area network with a very limited coverage. Bluetooth finds applications in audio players, home automation, smart phones, toys, hands free headphones and sensor networks.

Features of Bluetooth

1. Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
2. Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
3. Low power consumption of Bluetooth technology and an offered range of up to ten meters have paved the way for several usage models.
4. Bluetooth offers interactive conference by establishing an Ad-hoc network of laptops.
5. Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Bluetooth technology operates in the unlicensed industrial, scientific and medical ISM band at 2.4 to 2.485 GHz. It uses spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. Bluetooth supports 1 Mbps data rate for version 1.2 and 3 Mbps data rate for version 2.0 combined with error data rate. Bluetooth operating range depends on the device. The transmit power and therefore range of a Bluetooth module is defined by its power class. There are three defined classes of power as given below.

Class Number	Max. Output Power (dBm)	Max. Output Power (mW)	Max. Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	100 cm

- Class 3 radios have a range of upto 1 meter or 3 feet.
- Class 2 radios are most commonly found in mobile devices having a range of 10 meters or 30 feet.
- Class 1 radios are primarily in industrial use cases having a range of 100 meters or 300 feet.

Bluetooth Connection

Every single Bluetooth device has a unique 48-bit address, commonly abbreviated BD_ADDR. This will usually be presented in the form of a 12-digit hexadecimal value. The most-significant half (24 bits) of the address is an organization unique identifier (OUI), which identifies the manufacturer. The lower 24-bits are the more unique part of the address. This address should be visible on most Bluetooth devices.

Creating a Bluetooth connection between two devices is a multi-step process involving three progressive states. Figure 3.19 shows the connection establishment in a Bluetooth.

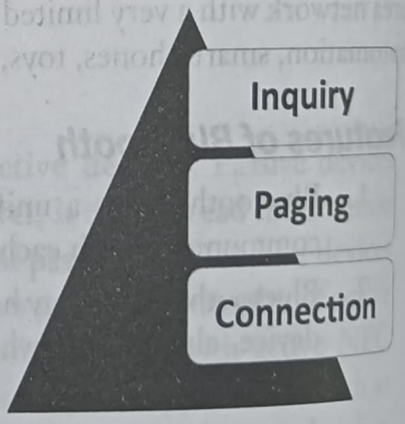


Fig.3.19: Connection Establishment in Bluetooth

Inquiry – If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to discover the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.

Paging (Connecting) – Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).

Connection – After a device has completed the paging process, it enters the connection

state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.

- **Active Mode:** This is the regular connected mode, where the device is actively transmitting or receiving data.
- **Sniff Mode:** This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (*e.g.* every 100 ms).
- **Hold Mode:** Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed. The master can command a slave device to hold.
- **Park Mode:** Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up.

When two Bluetooth devices share a special affinity for each other, they can be bonded together. Bonded devices automatically establish a connection whenever they are close enough. For example, when I start up my car, the phone in my pocket immediately connects to the car's Bluetooth system because they share a bond. No Unique Identifier interactions are required in this case. Bonds are created through one-time a process called **pairing**. When devices pair up, they share their addresses, names, and profiles, and usually store them in memory. They also share a common secret key, which allows them to bond whenever they're together in the future.

Pairing usually requires an authentication process where a user must validate the connection between devices. The flow of the authentication process varies and usually depends on the interface capabilities of one device or the other. Sometimes pairing is a simple "Just Works" operation, where the click of a button is all it takes to pair (this is common for devices with no UI, like headsets). Other times pairing involves matching 6-digit numeric codes. Older, legacy (v2.0 and earlier), pairing processes involve the entering of a common PIN code on each device. The PIN code can range in length and complexity from four numbers (*e.g.* "0000" or "1234") to a 16-character alphanumeric string.

Bluetooth Protocol Stack

The Bluetooth protocol stack allows devices to locate, connect and exchange data with each other and to execute interoperable, interactive applications against each other. Figure 3.20 shows the Bluetooth protocol stack.

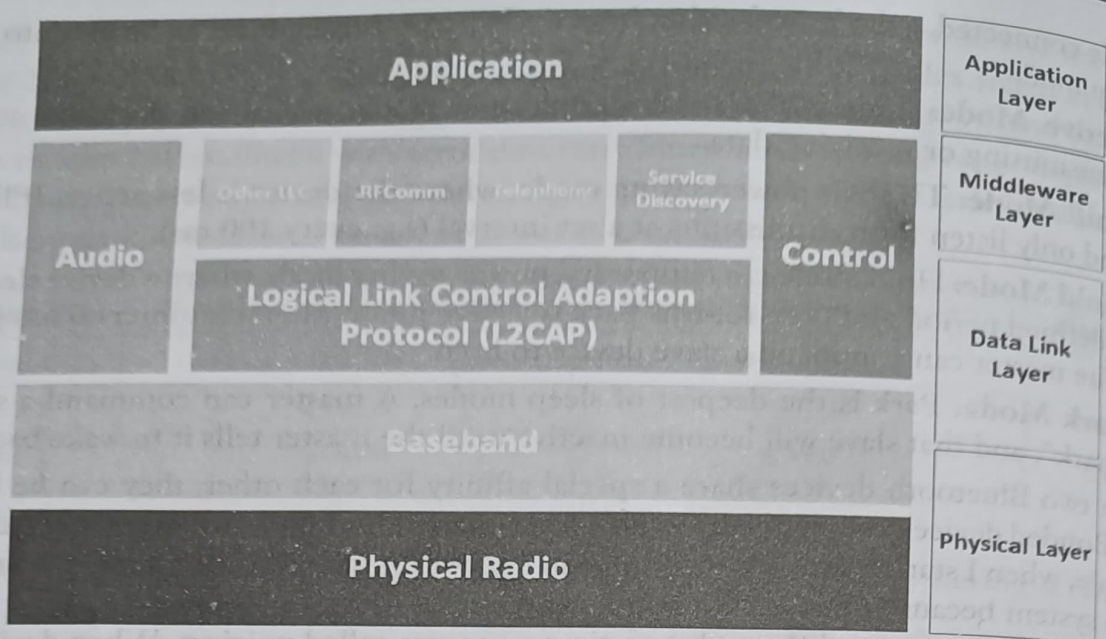


Fig.3.20: Bluetooth Protocol Stack

(a) Physical Radio and Baseband

The physical radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band. The baseband layer describes the specification of the Bluetooth Link Controller (LC), which carries out the baseband protocols and other low-level link routines. It specifies piconet/channel definition, "low-level" packet definition and channel sharing. Physical radio and baseband forms the physical layer of the Bluetooth. Other services of this layer include error correction, data whitening, hop selection and Bluetooth security. The baseband layer is responsible for searching other devices, assigning master and slave roles. It manages link between devices and determines packet types supported for synchronous and asynchronous traffic.

(b) Logical Link Control Adaptation (L2CAP)

L2CAP is layered over the baseband protocol and resides in the data link layer. All data traffic is routed through this layer. This layer shields higher layers from details of lower layers. It segments larger packets from higher layers into smaller packets that can be easily handled by lower layers. It facilitates maintenance of desired grade of service in two peer devices.

This protocol is used to multiplex multiple logical connections between 2 devices. It provides connection-oriented and connection-less data services to upper layer protocols. (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly and conveys quality of service information.

(c) RFComm

RFComm stands for Radio Frequency Communication. It is a cable replacement protocol used for generating a virtual data stream. It provides a virtual serial port for applications needed for scenarios like dial-up networking, etc. RFComm provides for binary data transport. It emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, *i.e.* it is serial port emulation. RFComm provides a simple, reliable data stream to the user similar to TCP. It supports up to 60 simultaneous connections between 2 Bluetooth devices.

(d) Service Delivery Protocol (SDP)

The Service Delivery Protocol (SDP) provides a means for applications to discover, which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services. It addresses the unique characteristics of Bluetooth environment such as dynamic changes in the quality of services in Radio Frequency proximity of devices in motion. SDP can function over a reliable packet transfer protocol. It uses a request/response model.

(e) Telephone Control Specifications Layer (TCS) and Audio

This layer is designed to set up voice calls. It supports functions like call control and group management. TCS can also be used to set up data calls. TCS protocols are compatible with International Telecommunication Union (ITU) specifications. Bluetooth audio communication takes place at rate of 64Kbps.

(f) Application

This group of protocols consists of actual applications that make use of Bluetooth links and refers to software that exists above protocol stack. The Bluetooth does not define any application protocols nor does it specify any API. Bluetooth profiles are developed to establish a base point for use of a protocol stack to accomplish a given usage case.

Bluetooth Topology: Piconet and Scatternet

Bluetooth enabled electronic devices connect and communicate wirelessly through short range devices known as Piconets. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as **master** or **slave** the specification allows a mechanism for master and slave to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a **Piconet**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the master. The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme.

The features of Piconets are as follows:

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique 48-bit address of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several Piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave Piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.
- Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
- A device can be a member of two or more Piconets, jumping from one Piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second Piconet.
- It can be a slave in one Piconet and master in another. It however cannot be a master in more than once Piconet.

Devices resident in adjacent Piconets provide a bridge to support inner-Piconet connections, allowing assemblies of linked Piconets to form a physically extensible communication infrastructure known as **Scatternet**. The Figure 3.21 shows the diagram of Piconets and Scatternet.

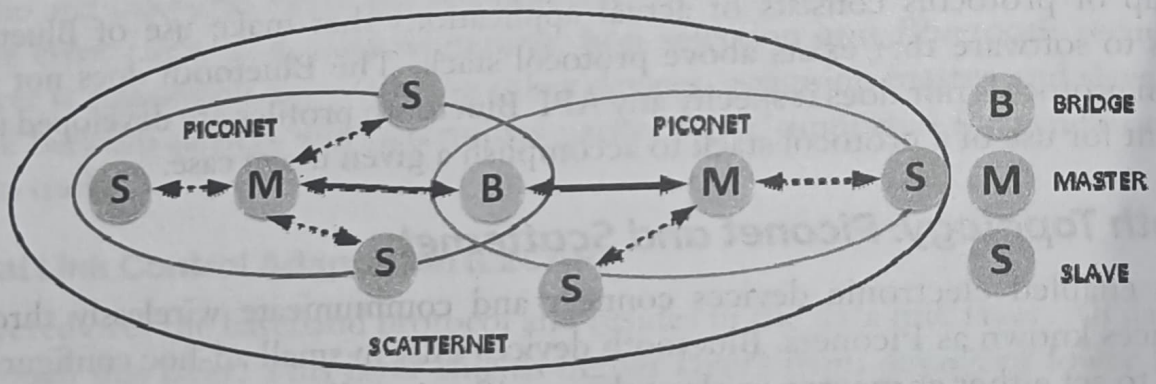


Fig.3.21: Diagram of Piconets and Scatternet

3.9 Z-wave

Z-wave (or Z wave or Zwave) is a protocol for communication among devices used for home automation. It uses RF for signaling and control. Z-wave was developed by Zensys, Inc. a start-up company based in Denmark. Z-wave was released in 2004. Based on the concepts of ZigBee, Z-wave strives to build simpler and less expensive devices than ZigBee.