1. IEEE 802.15.4 MAC

- The Institute of Electrical and Electronics Engineers (IEEE) released the 802.15.4 MAC standard for wireless personal area networks (WPANs) equipped with a duty cycle mechanism where the size of active and inactive parts can be adjustable during the PAN formation.

3.10.1 Network Architecture and Types/Roles of Nodes

The IEEE 802.15.4 MAC combines both the schedule-based and contention-based protocols and supports two network topologies, star and peer-to-peer as shown in Figure

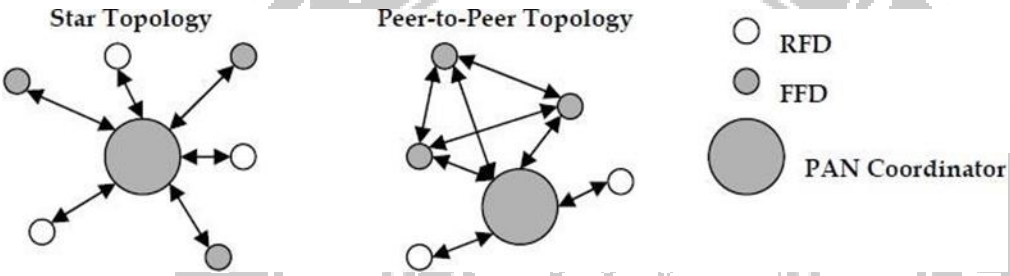

Figure 3.9 Topology configurations supported by IEEE 802.15.4 standard Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

Applications of IEEE 802.15.4

- Wireless sensor networks
- Home Automation
- Home Networking
- Connecting Devices to a PC
- Home security, etc.

- There are two special types of peer-to-peer topology. The first type is known as a cluster-tree network which has been used extensively in ZigBee. The other type is known as a mesh network which has been used extensively in IEEE 802.15 WPAN Task Group 5 (TG5).
- The standard defines two types of nodes namely the Full Function Device (FFD) and Reduced Function Device (RFD). The FFD node can operate with three different roles as a PAN coordinator, a coordinator and a device while RFD can operate only as a device.
- The devices must be associated with a coordinator in all network

conditions. The multiple coordinators can either operate in a peer-to-peer topology or star topology with a coordinator becoming the PAN coordinator.

- The star topology is more suitable for delay critical applications and small network coverage while the peer-to-peer topology is more applicable for large networks with multi-hop requirements at the cost of higher network latency.
- Furthermore, the standard defines two modes on how data exchanges should be done, namely, the beacon mode and the non-beacon mode. The beacon mode provides networks with synchronisation measures while the non-beacon mode provides the asynchronous features to networks.

2. Super frame Structure

- The beacon mode of IEEE 802.15.4 MAC defines a superframe structure to organise the channel access and data exchanges. The superframe structure is shown in Figure
  3.10 with two main periods; the active period and inactive period. The active period is divided into 16 time slots. Typically the beacon frame is transmitted in the first time slot and it is followed by two other parts, Contention Access Period (CAP) and Contention-Free Period (CFP) which utilise the remaining time slots. The CFP part is also known as Guaranteed Time Slots (GTS) and can utilise up to 7 time slots.

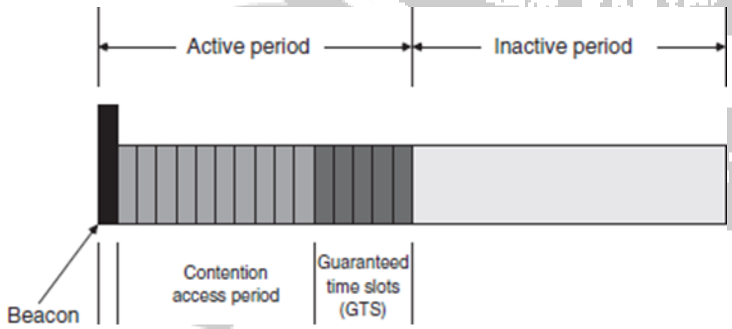

Figure 3.10 Super frame structure of IEEE 802.15.4

Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

- The length of the active and inactive periods as well as the length of a single time slot are configurable and traffic dependant.

- Data transmissions can occur either in CAP or GTS. In CAP, data communication is achieved by using slotted CSMA-CA while in GTS nodes are allocated fixed time slots for data communication.
- The strategy to achieve energy efficient operations in IEEE 802.15.4 MAC is by putting the nodes to sleep during the inactive period and when there is neither data to be transmitted nor any data to be fetched from the coordinator.
- However, the burden of energy cost is put on the coordinator where the coordinator has to be active during the entire active period

3. GTS Management

- The coordinator allocates GTS to devices only when the latter send appropriate request packets during the CAP. One flag in the request indicates whether the requested time slot is a transmit slot or a receive slot.
- In a transmit slot, the device transmits packets to the coordinator and in a receive slot the data flows in the reverse direction. Another field in the request specifies the desired number of contiguous time slots in the GTS phase.
- The coordinator answers the request packet in two steps: An immediate acknowledgment packet confirms that the coordinator has received the request packet properly but contains no information about success or failure of the request.
- After receiving the acknowledgment packet, the device is required to track the coordinator's beacons for some specified time (called aGTS Desc Persistence Time). When the

coordinator has sufficient resources to allocate a GTS to the node, it inserts an appropriate GTS descriptor into one of the next beacon frames. This GTS descriptor specifies the short address of the requesting node and the number and position of the time slots within the GTS phase of the superframe.

- A device can use its allocated slots each time they are announced by the coordinator in the GTS descriptor. If the coordinator has insufficient resources, it generates a GTS descriptor for (invalid) time slot zero, indicating the available resources in the descriptors length field. Upon receiving such a descriptor, the device may consider renegotiation.
- If the device receives no GTS descriptor within a GTS Desc Persistence Time time after sending the request, it concludes that the allocation request has failed. A GTS is allocated to a device on a regular basis until it is explicitly deallocated. The deallocation can be requested by the device by means of a special control frame.
- After sending this frame, the device shall not use the allocated slots any further. The coordinator can also trigger deallocation based on certain criteria. Specifically, the coordinator monitors the usage of the time slot: If the slot is not used at least once within a certain number of superframes, the slot is deallocated. The coordinator signals deallocation to the device by generating a GTS descriptor with start slot zero.

3. Data Transfer

- Assume that a device wants to transmit a data packet to the coordinator. If the device has an allocated transmit GTS, it wakes up just before the time slot starts and sends its packet immediately without running any carrier-sense or other collision-avoiding operations.
- However, the device can do so only when the full transaction consisting of the data packet and an immediate acknowledgment sent by the

coordinator as well as appropriate InterFrame Spaces (IFSs) fit into the allocated time slots.

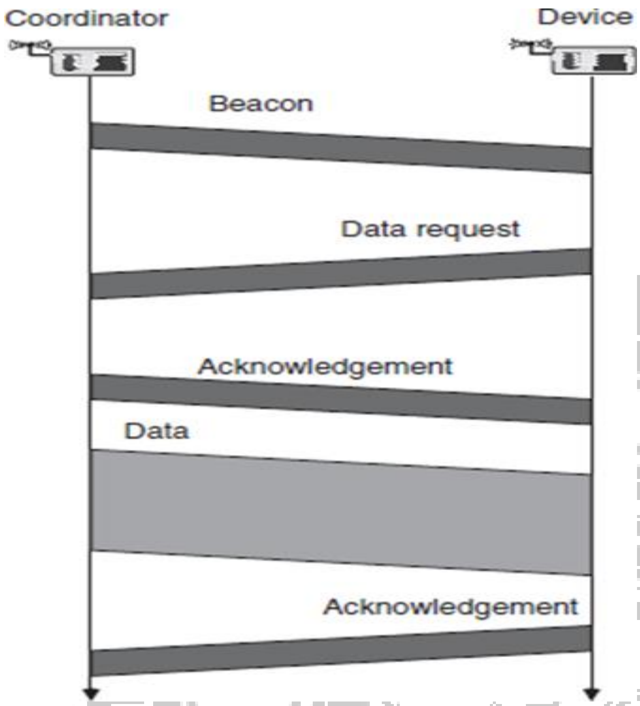

Figure 3.11 Handshake between coordinator and device when the device retrieves a packet

Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

- If this is not the case or when the device does not have any allocated slots, it sends its data packet during the CAP using a slotted CSMA protocol. The coordinator sends an immediate acknowledgment for the data packet.
- Now, assume the coordinator wants to send a data packet to the device. If the device has allocated a receive GTS and when the packet/acknowledgment/IFS cycle fits into these, the coordinator simply transmits the packet in the allocated time slot without further coordination.
- The device has to acknowledge the data packet. The handshake between device and coordinator is sketched in Figure 3.11
- The coordinator announces a buffered packet to a device by including the devices address into the pending address field of the beacon frame.
- When the device finds its address in the pending address field, it sends

a special data request packet during the CAP.

- The coordinator answers this packet with an acknowledgment packet and continues with sending the data packet.
- The device knows upon receiving the acknowledgment packet that it shall leave its transceiver on and prepares for the incoming data packet, which in turn is acknowledged.
- Otherwise, the device tries again to send the data request packet during one of the following super frames and optionally switches off its transceiver until the next beacon.

Slotted CSMA-CA Protocol

- When nodes have to send data or management/control packets during the CAP, they use a slotted CSMA protocol. The protocol contains no provisions against hidden- terminal situations.
- For example, there is no RTS/CTS handshake. To reduce the probability of collisions, the protocol uses random delays; it is thus a CSMA-CA protocol (CSMA with Collision Avoidance).
- The time slots making up the CAP are subdivided into smaller time slots, called back off periods. One back off period has a length corresponding to 20 channel symbol times and the slots considered by the slotted CSMA-CA protocol are just these back off periods.