UNIT III

Zigbee/IEEE 802.15.4

The commercialization of consumer-based IoT services requires the introduction of wireless, low-power, battery-powered sensors and actuators in people's premises.

• ZigBee's focus aimed at the "little devices" (things, objects) like light switches, thermostats, electricity meters, remote controls (RCs), as well as more complex sensor devices found in the healthcare, commercial building, and industrial automation sectors.

• To avoid multiple separate consumer networks, a PHY/MACagnostic solution is needed upon which IP standards and other wellknown higher-layer protocols can run with little changes.

• ZigBee is one such open standard, as discussed below. ZigBee IP (ZIP) is an example where Zigbee systems operate in an IP context. • Here we focus more on the wireless lower-layer aspects of Zigbee and not the IP part.

• ZigBee utilizes the globally available, licensefree 2.4 GHz industrial, scientific, and medical (ISM) frequency band to provide low data rate wireless applications

• IEEE 802.15.4, wireless links can operate in three unlicensed frequency bands, namely the 858 MHz band, the 902-to-928 MHz band, and the 2.4 GHz band

• IEEE 802.15.4 defines a robust radio PHY (physical) layer and MAC (medium access l)

• ZigBee networks support star, mesh, and cluster-tree topologies.

• These capabilities enable a network to have over 65,000 devices on a single wireless network.

• ZigBee offers low-latency communication between devices without the need for the initial network synchronization delays as required by Bluetooth. • ZigBee can create robust self-forming, self-healing wireless mesh networks. The ZigBee mesh network connects sensors and controllers without being restricted by distance or range limitations;

• ZigBee mesh networks allow all participating devices to communicate with one another and act as repeaters transferring data between devices.

• ZigBee is available as two feature sets, – ZigBee PRO and ZigBee. • Both feature sets define how the ZigBee mesh networks operate.

• ZigBee PRO, the most widely used and optimized for low-power consumption and to support large networks with thousands of devices.

• The ZigBee Alliance announced an expanded set of features for the ZigBee protocol. – This new stack profile is universally referred to as ZigBee PRO and for the most part defines specific stack settings and makes mandatory many of the features. • ZigBee PRO also used in some new application like automatic meter reading, commercial building automation, and home automation.

• ZigBee PRO features implement support for larger networks, – for example stochastic addressing to assign addresses using probability analysis to simplify network formation.

• ZigBee PRO implements a technique known as frequency agility (not hopping): – a network node is able to scan for clear spectrum (with a choice of 16 available channels) and communicate its findings back to the ZigBee coordinator so that a new channel can be used across the network.

• ZigBee PRO networks have the ability to aggregate routes through the use of "many-to-one" routing; – this allows each device to share the same routing path reducing broadcast and network traffic and greatly improves the efficiency and stability of the network routing table.

• The ZigBee 802.15.4 spec defines a maximum packet size of 128 octets; – this packet size is optimal for short control messages, but there may be instances where the network needs to send larger messages;

• therefore, ZigBee PRO now has the means to automatically fragment and reassemble a message at a receiving node relieving the host application of this overhead.

• The ZigBee Alliance is a global ecosystem of 400+ companies in the M2M/IoT space developing standards and producing products for use in commercial building automation, consumer electronics, health care and fitness, home automation, energy management, retail management, and wireless telecommunications.

• LR-WPANs (Low-Rate Wireless Personal Area Networks) applications require a low-cost, small-size, highly reliable technology which offers long battery life, measured in months or even years, and automatic or semiautomatic installation.

• ZigBee is a low-power wireless specification that introduces mesh networking to the low-power wireless space and is targeted toward applications such as smart meters, home automation, and RC units. ZigBee technology provides reasonably efficient low-power connectivity and ability to connect a large number of devices into a single network.

• Some studies have shown that for the home, two wireless PHY layer communications technologies that best meet the overall

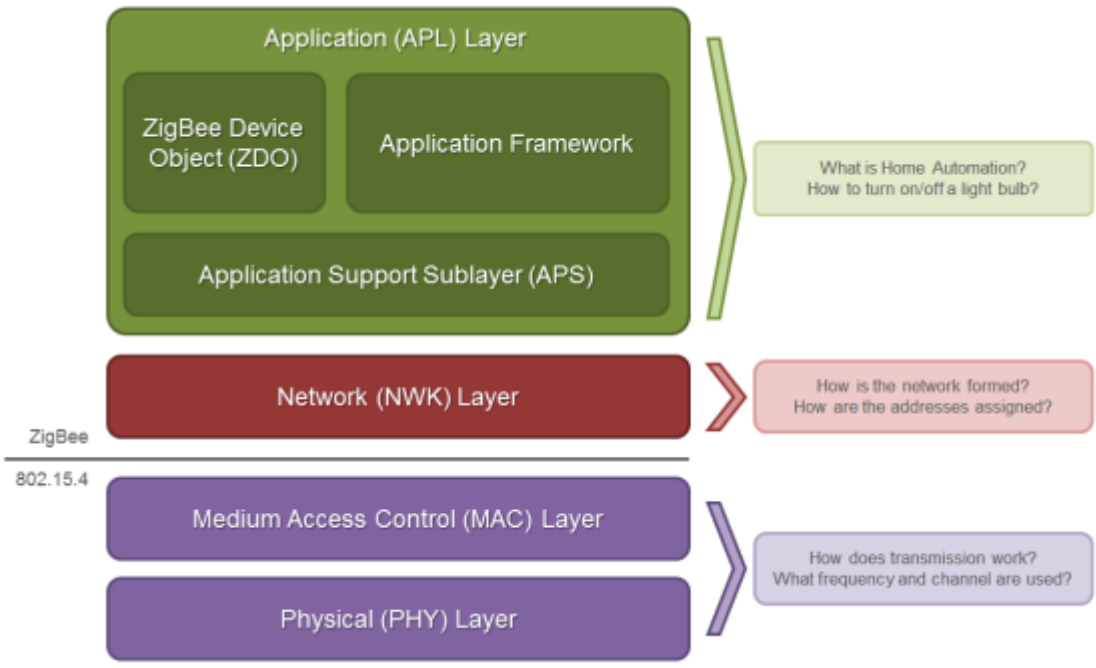
• performance and cost requirements are Wi-Fi (802.11/n) and ZigBee (802.15.4).

Disadvantages:

• ZigBee's relative complexity (as seen in the protocol stack) and the apparent fact that the power consumption of ZigBee devices is higher than the consumption of some alternatives (e.g., BLE) tend to make ZigBee not always the most ideal solution for unmaintained devices that need to operate for extensive periods of time from a limited power source;

• hence, while many home applications make ideal use of ZigBee, other IoT/M2M applications can also be supported by other approaches.

• ZigBee makes use of the physical radio specified by IEEE 802.15.4; it adds logical network capabilities, and security and application software.



The PHY layer of the reference model specifies the network interface components, parameters, and operation.

• The PHY layer includes a variety of features, such as – receiver energy detection (RED), – link quality indicator (LQI), – clear channel assessment (CCA).

• The PHY layer is also including low-duty cycle operations, strict power management, and low transmission overhead.

• IEEE 802.15.4 defines several addressing modes: – it allows the use of either IEEE 64-bit extended addresses or 16- bit addresses unique within the PAN.

MAC layer handles network association and disassociation.

• It also regulates access to the medium; this is achieved through two modes of operation: – beaconing – nonbeaconing.

• The beaconing mode is specified for environments where control and data forwarding is achieved by an always active device.

• The nonbeaconing mode specifies the use of unslotted, non persistent CSMA-based MAC protocol.

• The network layer provides the functionality required to support network routing capabilities, configuration and device discovery, association and disassociation, topology management, MAC layer management, and routing and security management.

• Three network topologies, namely star, mesh, and cluster tree, are supported.

• The security layer leverages the basic security services specified by the IEEE 802.15.4 security model to provide support for infrastructure security and application data security.

• The application layer consists of the application support sublayer (APS), the ZigBee device object (ZDO), and the manufacturerdefined application objects. – The responsibilities of the APS sublayer include maintaining tables for binding devices together, based on their services and their needs, and forwarding messages between bound devices.

• ZigBee is not a frequency-hopping technology; therefore, it requires careful planning during deployment in order to ensure that there are no interfering signals in the vicinity.

• The design of the PHY layer is driven by the need for low-cost, powereffective PHY layer for cost-sensitive, low data rate monitoring and control applications.

• Under IEEE 802.15.4, wireless links can operate in three unlicensed frequency bands, namely in the 858 MHz band, in the 902-to-928 MHz band, and in the 2.4 GHz band.

• Based on these frequency bands, the IEEE 802.15.4 standard defines three physical media: – Direct sequence spread spectrum (DSSS) using binary phase shift keying (BPSK), operating in the 868 MHz at a data rate of 20 Kbps; – DSSS using BPSK, operating in the 915 MHz at a data rate of 40 Kbps – DSSS using offset quadrature phase shift keying (O-QPSK), operating in the 2.4 GHz at a data rate of 140 Kbps

• IEEE 802.15.4 defines four types of frames: – beacon frames, – MAC command frames, – acknowledgement frames, – data frames

• IEEE 802.15.4 networks can either be nonbeacon enabled or beacon enabled.

• The latter is an optional mode in which devices are synchronized by a so-called coordinator's beacons. – This allows the use of super frames within which a contentionfree guaranteed time service (GTS) is possible.

• In nonbeacon-enabled networks, data frames are sent via the contention-based channel access method of unslotted carrier sense multiple access/collision detect (CSMA/CD). – In nonbeacon-enabled networks, beacons are not used for synchronization; however, they are still useful for link-layer device discovery to aid in association and disassociation events

• The first field of this structure contains a 32- bit preamble; this field is used for symbol synchronization.

• The next field represents the start of packet delimiter; this field of 8 bits is used for frame synchronization. – The 8-bit PHY header field specifies the length of the PHY service data unit (PSDU).

• The PSDU field can carry up to 127 bytes of data.

• In order to accommodate the MAC protocol, the IEEE 802.15.4 standard distinguishes devices based on their hardware complexity and capability.

• The standard defines two classes of physical devices, namely: – a full function device (FFD) – a reduced function device (RFD).

• These device types differ in their use and how much of the standard they implement.

• An FFD is equipped with the adequate resources and memory capacity to handle all the functionalities and features specified by the standard.

• An RFD is a simple device that carries a reduced set of functionalities, for lower cost and complexity.

• Based on these physical device types, ZigBee defines a variety of logical device types. There are three categories of logical devices:

• Network coordinator: An FFD device responsible for network establishment and control. The coordinator is responsible for choosing key parameters of the network configuration and for starting the network. It also stores information about the network and acts as the repository for security keys.

• Router: An FFD device that supports the data routing functionality, including acting as an intermediate device to link different components of the network and forwarding message between remote devices across multihop paths. A router can communicate with other routers and end devices.

• End Devices: An RFD device that contains (just) enough functionality to communicate with its parent node, namely the network coordinator or a router. An end device does not have the capability to relay data messages to other end devices.

• A PAN coordinator is the designated principal controller of the WPAN. Every network has exactly one PAN coordinator, selected from within all the coordinators of the network. A coordinator is a network device configured to support network functionalities and additional responsibilities, including: – Managing a list of all associated network devices; – Exchanging data frames with network devices and peer coordinator; – Allocating 16-bit short addresses to network devices. The short addresses, assigned on-demand, are used by the associated devices in lieu of the 64-bit addresses for subsequent communications with the coordinator; – Generating, on a periodic basis, beacon frames. These

frames are used to announce the PAN identifier, the list of outstanding frames, and other network and device parameters.

• The ZDO (ZigBee device object) represents a predefined base class of functionality upon which all applications are written.

• The ZDO creates an abstraction so that the developer can focus on writing application-specific code rather than dealing with the low-level details.

• The ZDO provides an interface between the application objects, the profile (e.g., the ZigBee Health Care), and the APS.

• The ZDO is responsible for initializing the APS, the network layer, and the security service provider

• ZigBee is designed for low-to-very-low-duty cycle static and dynamic environments with many active nodes;

• Bluetooth, is designed for high QoS, variety of duty cycles, and moderate data rates in networks with limited active nodes.