COMMUNICATION TECHNOLOGIES

Physical cum data-link layer in the model consists of a local area network/personal area network. A local network of IoT or M2M device deploys one of the two types of technologies— wireless or wired communication technologies. Figure 2.4 shows connected devices (1st to ith) connectivity using different technologies for communication of data from and to devices to the local network connectivity to a gateway.

Here follows the technologies and standards recommended for the communication.

Wireless Communication Technology

Physical cum data-link layer uses wired or wireless communication technologies. Examples of wireless communication technologies are NFC, RFID, ZigBee, Bluetooth (BT), RF transceivers and RF modules. Following subsections describe these wireless communication technologies.

Near-Field Communication

Near-Field communication (NFC) is an enhancement of ISO/IEC214443 standard for contact-less proximity-card. NFC is a short distance (20 cm) wireless communication technology. It enables data exchange between cards in proximity and other devices. Examples of applications of NFC are proximity-card reader/RFID/IoT/M2M/mobile device, mobile payment wallet, electronic keys for car, house, office entry keys and biometric passport readers.

NFC devices transmit and receive data at the same instance and the setup time (time taken to start the communication) is 0.1 s. The device or its reader can generate RF fields for the nearby passive devices such as passive RFID. An NFC device can check RF field and detect collision of transmitted signals. The device can check collision when the received signal bits do not match with the transmitted signal bits.

Features of an NFC device are:

Range of functioning is within 10 to 20 cm. The device can also communicate with Bluetooth and Wi-Fi devices in order to extend the distance from 10 cm to 30 m or higher. The device is able to receive and pass the data to a Bluetooth connection or standardized LAN or Wi-Fi using information handover functions. Device data transfer rates are 106 kbps, 212 kbps, 424 kbps and 848 kbps (bps stands for bit per second, kbps for kilo bit per second). Three modes of communication are:

1. Point-to-point (P2P) mode: Both devices use the active devices in which RF fields alternately generate when communicating.

2. Card-emulation mode: Communication without interruption for the read and write as required in a smart card and smart card reader. FeliCa™ and Mifare™ standards are protocols for reading and writing data on the card device and reader, and then the reader can transfer information to Bluetooth or LAN.

3. Reader mode: Using NFC the device reads passive RFID device. The RF field is generated by an active NFC device. This enables the passive device to communicate.

RFID

Radio Frequency Identification (RFID) is an automatic identification method. RFIDs use the Internet. RFID usage is, therefore, in remote storage and retrieval of data is done at the RFID tags. An RFID device functions as a tag or label, which may be placed on an object. The object can then be tracked for the movements. The object may be a parcel, person, bird or an animal. IoT applications of RFID are in business processes, such as parcels tracking and inventory control, sales log-ins and supply-chain management.

Bluetooth BR/EDR and Bluetooth Low Energy

Bluetooth devices follow IEEE 802.15.1 standard protocol for L1 (physical cum data-link layer). BT devices form a WPAN devices network. Two types of modes for the devices are Bluetooth BR/EDR (Basic Rate 1 Mbps/Enhanced Data Rate 2 Mbps and 3 Mbps) and Bluetooth low energy (BT LE 1Mbps). A latest version is Bluetooth v4.2. BT LE is also called Bluetooth Smart. Bluetooth v4.2 (December 2014) provides the LE data packet length extension, link layer privacy and secure connections, extended scanner and filter link layer policies and IPSP. BT LE range is 150 m at 10 mW power output, data transfer rate is 1Mbps and setup time is less than 6s.

Bluetooth v5, released in June 2016, has increased the broadcast capacity by 800%, quadrupled the range and doubled the speed. A device may have provisions for single mode BT LE or dual mode BT BR/EDR (Mbps stands for Million Bits per second).

Its features are:

- Auto-synchronisation between mobile and other devices when both use BT. BT network uses features of self-discovery, self-configuration and self-healing.
- Radio range depending on class of radio; Class 1 or 2 or radios: 100 m, 10 m or 1 m used in device BT implementation.
- Support to NFC pairing for low latency in pairing the BT devices.
- Two modes—dual or single mode devices are used for IoT/M2M devices local area network.
- IPv6 connection option for BT Smart with IPSP (Internet Protocol Support Profile).
- Smaller packets in LE mode.
- Operation in secured as well as unsecured modes (devices can opt for both link-level as well as service-level security or just service level or unsecured level).
- AES-CCM 128 authenticated encryption algorithm for confidentiality and authentication.
- Connection of IoT/M2M/mobile devices using BT EDR device to the Internet with 24 Mbps Wi-Fi 802.11 adaptation layer (AMP: Alternative MAC/PHY layer) or BT-enabled wire-bound connection ports or device. MAC stands for media access control sub layer at a data-link layer/sublayer.

ZigBee IP/ZigBee SE 2.0

ZigBee devices follow the IEEE 802.15.4 standard protocol L1 (physical cum data-link layer). ZigBee devices form a WPAN devices network. ZigBee end-point devices form a WPAN of embedded sensors, actuators, appliances, controllers or medical data systems which connect to the Internet for IoT applications, services and business processes.

ZigBee Neighbourhood Area Network (NAN) is a version for a smart grid. ZigBee smart energy version 2.0 has energy management and energy efficiency capabilities using an IP network.

The features of ZigBee IP are:

- L1 layer PDU = 127 B
- Used for low-power, short-range WPAN
- The device can function in six modes—end point, ZigBee-ZigBee devices router, ZigBee network coordinator, ZigBee-IP coordinator, ZigBee-IP router and IP host.
- ZigBee IP enhancement provisions the IPv6 connectivity. A ZigBee IP device is a Reduced Function Device (RFD). RFD means one that functions for the 'sleepy'/ battery-operated device. Sleepy means one that wakes up infrequently, sends data and then goes back to sleep. ZigBee IP supports IPv6 network with 6LoWPAN header compression, connection for Internet communication and control of low power devices, TCP/UDP transport layer and TLSv1.2 public key (RSA and ECC) and PSK cipher suite for end-to-end security protocol, end-to-end means application layer to physical layer.
- The ZigBee router uses reactive and proactive protocols for routing mode, which enable applications in big-scale automation and remote controls.
- A self-configuring and self-healing dynamic pairing mesh network, supports both multicast and unicast options.
- Multicast forwarding to support multicast Domain Name System (mDNS) based service discovery (SD)
- Support to development of discovery mechanism with full application confirmation
- Support to pairing of coordinator with end-point devices and routers in star topology
- Provides bigger network using multiple star topology and inter-PAN communications
- Support to sensor nodes and sensor (or appliances) network integration, sensor and appliances devices configured as router or end-devices
- Low latency (< 10 ms) link layer connection
- Range is 10–200 m, data transfer rate is 250 kbps, low power operation
- ISM band frequencies direct sequence spread spectrum 16-channel radio, and provide link level security using AES-CCM-128
- Includes RFD in ZigBee SE 2.0 ZigBee NAN is for devices which are used for smart-metering, distribution automation devices and smart grid communication profile. NAN enables a utility's last-mile at HAN (Home Area Network), outdoor access network that connects smart meters to WAN (wide area network) gateways.

Features of a ZigBee network:

- A router in star network connects to 6LoWPAN, which connects an IEEE 802.15.4 devices network to IPv6 network.
- 1000s of byte communicate between the network layer and IoT web objects.
- 127 B communication between the adaptation layer IEEE 802.15.4 devices at single data transfer.
- IETF ND (Neighbour Discovery), ROLL (Routing Over Low power Loss Network), RPL routing, IPv6/IPv4 network, TCP/UDP/ICMP transport, SSL/TLS security layer protocols for the communication between web object/application and ZigBee devices.

Wi-Fi

Wi-Fi is an interface technology that uses IEEE 802.11 protocol and enables the Wireless Local Area Networks (WLANs). Wi-Fi devices connect enterprises, universities and offices through home AP/public hotspots. Wi-Fi connects distributed WLAN networks using the Internet.

Automobiles, instruments, home networking, sensors, actuators, industrial device nodes, computers, tablets, mobiles, printers and many devices have Wi-Fi interface. They network using a Wi-Fi network. Wi-Fi is very popular. The issues of Wi-Fi interfaces, APs and routers are higher power consumption, interference and performance degradation. Wi-Fi interfaces connect within themselves or to an AP or wireless router using Wi-Fi PCMCIA or PCI card or built-in circuit cards and through the following:

● Base station (BS) or AP
● A WLAN transceiver or BS can connect one or many wireless devices simultaneously to the Internet.
● Peer-to-peer nodes without access point: Client devices within Independent Basic Service Set (IBSS) network can communicate directly with each other. It enables fast and easy setting of an 802.11 network.
● Peer to multipoint nodes with Basic Service Sets (BSSs) using one in-between AP point or distributed BSSs connect through multiple APs.
● Connectivity range of each BSS depends on the range of wireless bridges and antennae used and environmental conditions.
● Each BSS is a Service Set Identifier (SSID).

The Wi-Fi interfaces, access points, routers features are as follows:
● Generally used are the 2.4 GHz IEEE 802.11b adapters or 5 GHz (802.11a or 802.11g) or 802.11n or other 802.11 series protocols.
● Interfaces use 2.4 GHz or 5 GHz antenna
● Offers mobility and roaming.
• Have easy installation simplicity and flexibility
● Coverage range is 30 m to 125 m
● Used in a room having the limited-coverage 802.11a which coexists with b, coexists with b and g
● Uses the 802.11b in wider coverage range because that is unaffected by walls and is meant for hotspots for public usage having range data rate 11 Mbps (802.11b) within 30 m
● Uses 802.11g for high data rates up to 54 Mbps, and 802.11n for very high 600 Mbps, using multiple antennas to increase data rates
● Interoperable with wireless as well as wired infrastructure which ensures compatibility and enables easier access and hides complexity when enabling the wireless access to data, media and streams, and applications and services.
● Provides a dynamic environment of network expendability and scalability. Scalability means a system can have a large number of smaller interfaces, routers and APs
● Provides security, integrity and reliability
● Uses Wireless Protected Access (WPA) and Wired Equivalent Privacy (WEP) security sub layers

RF Transceivers and RF Modules

RF transmitters, receivers, and transceivers are the simplest RF circuits. A transceiver transmits the RF from one end and receives the RF from the other end, but internally has an additional circuit, which separates the signals from both ends. An oscillator generates RF pulses of required active duty cycle and connects to a transmitter. BT, ZigBee, and Wi- Fi radios deploy ISM band transceivers, which have comparatively complex circuits.

IoT/M2M applications deploy ISM band RF modules with transceivers or just transmitter or receiver. A number of systems use RF modules for applications needing wireless connectivity; for example, security, telemetry, telematics, fleet management, home automation, healthcare, automobiles wireless tire pressure monitors, back-up cameras and GPS navigation service, payment wallet, RFID and maintenance.

RF technology consists of the following elements:

● RF interface/physical layer, RF signals transmit between the nodes or endpoints, i.e. the sensors, actuators, controllers and a gateway where signals are received. Physical layer specifications consist of signal aspects and characteristics, including the frequencies, modulation format, power levels, the transmitting and receiving mode and signaling between end-point elements.

● RF network architecture includes the overall system architecture, backhaul, server and bidirectional end-devices with radio duty cycling in the applications. Radio duty cycling means managing the active intervals, transmission and receiving schedule, and time-intervals actions on an event during the active intervals and actions during the inactive (sleep) intervals using the RF Integrated Circuits (RFICs).

GPRS/GSM Cellular Networks-Mobile Internet

An IoT/M2M communication gateway can access a Wireless Wide Area Network (WWAN). The network access may use a GPRS cellular network or new generation cellular network for Internet access.

A mobile phone provisions for a USB wired port, BT and Wi-Fi connectivity. Wireless connectivity for Internet uses data connectivity using GSM, GPRS, UMTS/LTE and WiMax services of a mobile service provider or Wi-Fi using a modem. A phone, generally, provisions for number of sensors also; for example, acceleration, GPS and proximity.

Wireless USB

Wireless USB is a wireless extension of USB 2.0 and it operates at ultra-wide band (UWB) 5.1 GHz to 10.6 GHz frequencies. It is for short-range personal area network (high speed 480 Mbps 3 m or 110 Mbps 10 m channel). FCC recommends a host wire adapter (HWA) and a device wire adapter (DWA), which provides wireless USB solution. Wireless USB also supports dual-role devices (DRDs). A device can be a USB device as well as limited capability host.

Data enrichment, data consolidation and device management at gateway

A gateway at a data-adaptation layer has several functions. These are data privacy, data security, data enrichment, data consolidation, transformation and device management. ITU-T reference model's lowest layer is the device layer. This layer has device and gateway capabilities. A gateway consists of the data enrichment, consolidation and IoT communication frameworks.
The communication gateway enables the devices to communicate and network with the web. The communication gateway uses message transport protocols and web communication protocols for the Internet. Gateway includes the provisions for one or more of the following functions: transcoding and data management. Following are data management and consolidation functions:

- Transcoding
- Privacy, security
- Integration
- Compaction and fusion

Transcoding

Transcoding means data adaptation, conversion and change of protocol, format or code using software. The gateway renders the web response and messages in formats and representations required and acceptable at an IoT device. Similarly, the IoT device requests are adapted, converted and changed into required formats acceptable at the server by the transcoding software.
Transcoding involves formats, data and code conversion from one end to another when the multimedia data is transferred from a server to the mobile TV, Internet TV, VoIP phone or smartphone as the client devices. Transcoding applications also involve filtering, compression or decompression.
A transcoding proxy can execute itself on the client system or the application server. A transcoding proxy has conversion, computational and analysing capabilities, while a gateway has conversion and computational capabilities only.

Privacy

Data such as patient medical data, data for supplying goods in a company from and to different locations, and changes in inventories, may need privacy and protection from conscious or unconscious transfer to untrustworthy destinations using the Internet. Privacy is an aspect of data management and must be remembered while designing an application. The design should ensure privacy by ensuring that the data at the receiving end is considered anonymous from an individual or company. Following are the components of the privacy model:

- Devices and applications identity-management
- Authentication
- Authorization
- Trust
- Reputation

A suitable encryption of identification of data source enforces privacy. Device ID management provides for privacy. The analysed decrypted data is an input to application, service or process. IoT or M2M data have to be for the beneficiary individual person or company only.

When data is transfered from one point to another, it should be ensured that the stakeholder in future may not misuse the device end data or the application data. These static and dynamic relationships are components which depend on trust and reputation.

Secure Data Access

Access to data needs to be secure. The design ensures the authentication of a request for data and authorization for accessing a response or service. It may also include auditing of requests and accesses of the responses for accountability in future. End-to-end security is another aspect while implies using a security protocol at each layer, physical, logical link and transport layers during communication at both ends in a network.

Data Gathering and Enrichment

IoT/M2M applications involve actions such as data-gathering (acquisition), validation, storage, processing, reminiscence (retention) and analysis. Data gathering refers to data acquisition from the devices/devices network. Four modes of gathering data are:

1. Polling refers to the data sought from a device by addressing the device; for example, waste container filling information in a waste management system
2. Event-based gathering refers to the data sought from the device on an event; for example, when the device reaches near an access point or a card reaches near the card reader or an initial data exchange for the setup of peer-to-peer or master-slave connection of BT device using NFC
3. Scheduled interval refers to the data sought from a device at select intervals; for example, data for ambient light condition in Internet of streetlights
4. Continuous monitoring refers to the data sought from a device continuously; for example, data for traffic presence in a particular street ambient light condition in Internet of streetlights
Data enrichment refers to adding value, security and usability of the data.

Data Dissemination

Consider the following three steps for data enrichment before the data disseminates to the network as aggregation, compaction and fusion. Aggregation refers to the process of joining together present and previously received data frames after removing redundant or duplicate data.
Compaction means making information short without changing the meaning or context; for example, transmitting only the incremental data so that the information sent is short. Fusion means formatting the information received in parts through various data frames and several types of data (or data from several sources), removing redundancy in the received data and presenting the formatted information created from the information parts. Data fusion is used in cases when the individual records are not required and/or are not retrievable later.