UNIT IV

5 IoT Systems, Network and Protocols

Syllabus

Study of RF Wireless Sensors; Wireless networks; Wireless Sensor Networking (WSN); Cellular Machine-to- Machine (M2M) application networks; Computer Connected to Internet; Network Devices; Device configuration and management; Exchange information in real time without human intervention; IoT Protocols.

Contents

5.1 Study of RF

- Radio Frequency Identification (RFID) is a very simple and cost-effective way of item identification. RFID systems can be seen as a next-generation technology for bar-codes. RFID devices are wireless microchips used for tagging objects for automated identification.
- An RFID tag is a simplified, low-cost, disposable contactless smartcard. RFID tags include a chip that stores a static number (ID) and attributes of the tagged object and an antenna that enables the chip to transmit the store number to a reader.
- Tags are characterized by a unique identifier and are applied to objects. Readers trigger the tag transmission by generating an appropriate signal, which represents a query for the possible presence of tags in the surrounding area and for the reception of their IDs.
- Fig. 5.1.1 shows basic RFID system.

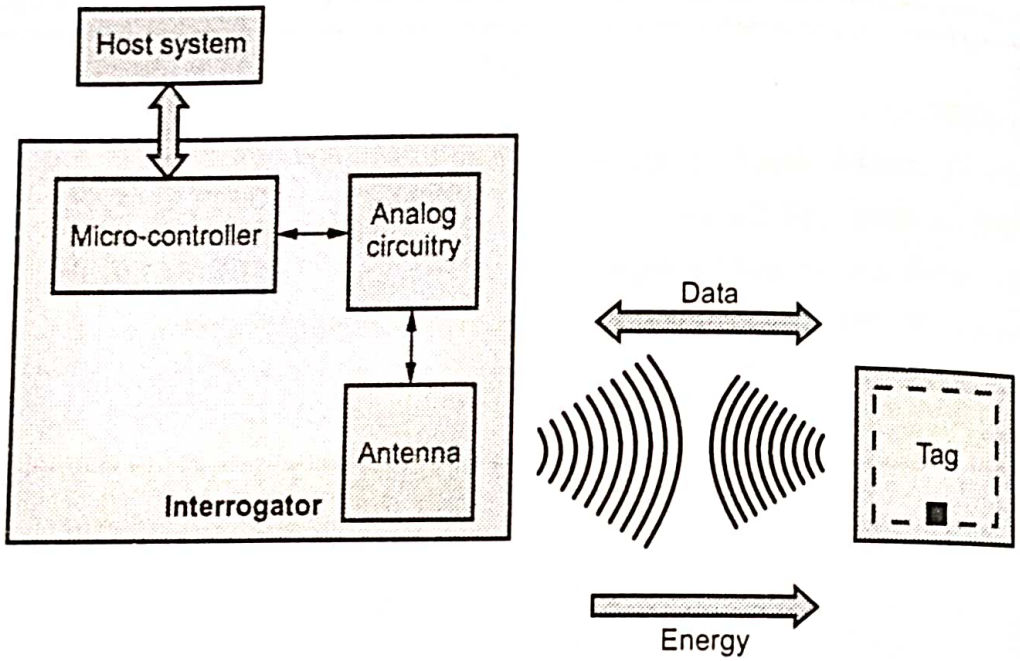


Fig. 5.1.1 : Basic RFID system

- RFID systems consist of a reading device called a reader and one or more tags. The reader is a powerful device with ample memory and computational resources.
- Passive tags have limited computational capacity, no ability to sense the channel, detect collisions and communicate with each other. They respond only at reader commands.
- Semi-passive tags have an on-board power source that can be used to energize their microchip. Active tags can sense the channel and detect collisions.

- Accordingly, RFID systems can be used to monitor objects in real-time, without the need of being in line-of-sight; this allows for mapping the real world into the virtual world.
- An RFID system involves hardware known as readers and tags, as well as RFID software or RFID middleware. Readers can also be mobile / hand-held.
- RFID systems operate in the Industry, Scientific and Medical (ISM) frequency band that ranges from 100 kHz to 5.8 GHz.

RFID Frequencies Range :

- RFID tags may operate in different frequencies with respect to their initial designs. Different frequencies and their respective devices offer different advantages.

RFID	Key Applications	Standard
125 kHz (Low Frequency)	Inexpansive passive RFID tags for identifying animals	ISO 18000-2
13.56 MHz (high Frequency)	Inexpansive passive RFID tags for identifying objects. Example : library book identification, clothes identification	ISO 14443
400 MHz	For remote control for vehicle centre locking systems	ISO 18000-7
868 MHz, 915 MHz and 922 MHz (UHF)	For active and passive RFID tags for logistics in Europe, US and Australia respectively.	
2.45 GHz (Microwave)	An ISM band, used for active and passive RFID tags. Used for temperature sensor or GPS collection	ISO 18000-5

- For example, RFID systems can track items in real-time with the help of Global Positioning System (GPS), which provides essential information about the objects like physical location or status. Sensor technologies are also emerging in this regard to collect and transmit the physical status or data from the objects or things.
- Reader functions :
  1. Remotely power tags
  2. Establish a bidirectional data link
  3. Inventory tags, filter results
  4. Communicate with networked server(s)
  5. Can read 100-300 tags per second

RFID Anti-Collision Protocols

- Collision due to simultaneous tag responses is one of the key issues in RFID systems. Tag collision results in wastage of bandwidth, energy and increases identification delays.
- RFID readers must use an anti-collision protocol to minimize collisions and hence help reduce identification delays. Fig. 5.1.2 shows tag collision problem.

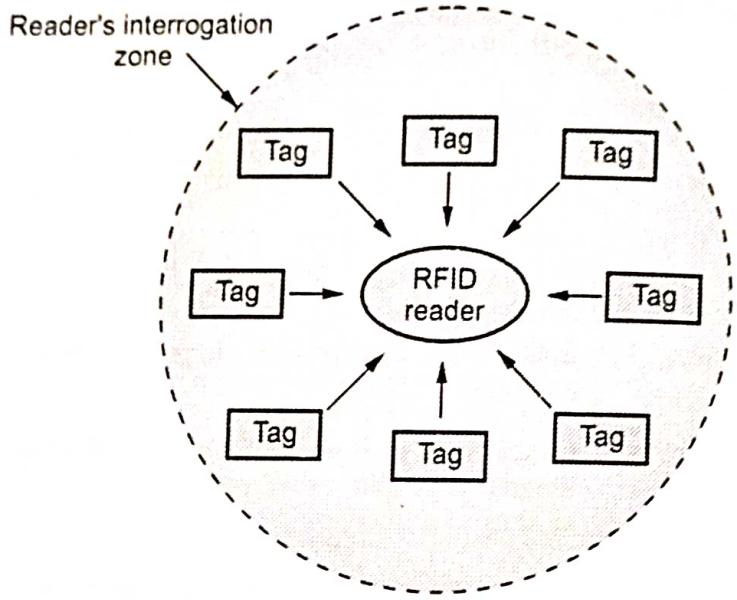


Fig. 5.1.2 : Tag collision problem

- RFID anti-collision protocols are often categorized as Aloha based protocols and tree based protocols. In pure Aloha based RFID systems, a tag responds with its ID randomly after being energized by a reader.
- In Slotted Aloha (SA) based RFID systems, tags transmit their ID in synchronous time slots. The collision occurs at slots boundary only, hence there are no partial collisions

RFID advantages over bar-codes

1. No line of sight required for reading
2. Multiple items can be read with a single scan
3. Each tag can carry a lot of data (read / write)
4. Individual items identified and not just the category
5. Passive tags have a virtually unlimited lifetime
6. Active tags can be read from great distances
7. Can be combined with barcode technology

RFID Middleware

- RFID middleware needs to allow users to configure, deploy and issue commands directly to readers through a common interface. For instance users should be able to tell a reader when to "turn off" if needed. Fig. 5.1.3 shows RFID middleware.

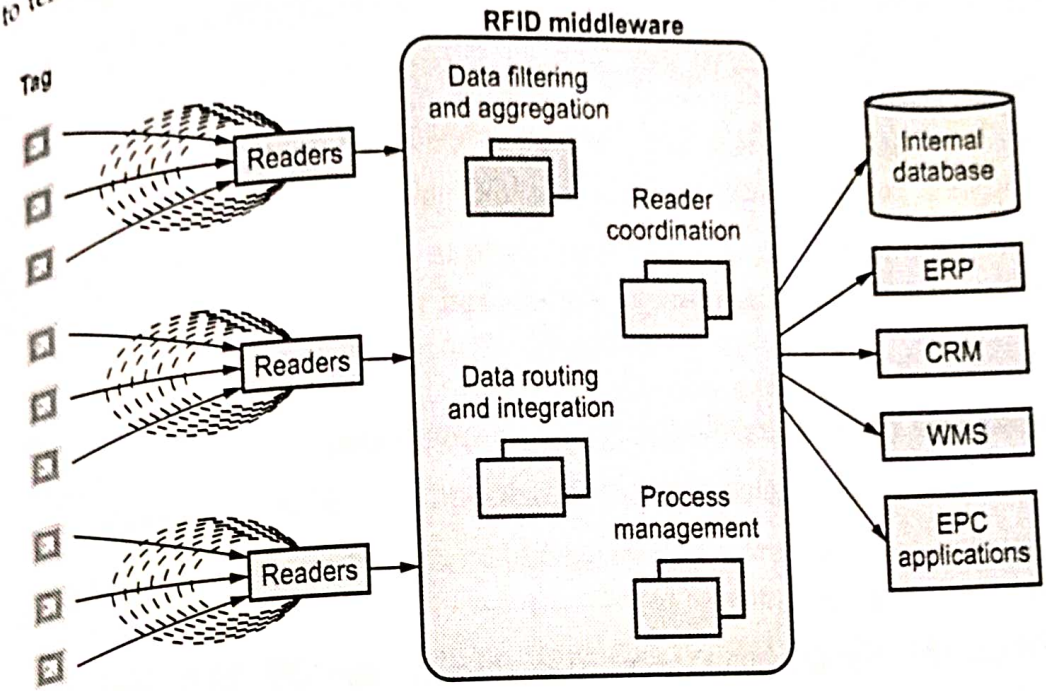


Fig. 5.1.3 : RFID middleware

- After RFID middleware captures EPC data from readers, it must be able to intelligently filter and route the data to the appropriate destinations.
- Look for middleware that includes both low-level logic and more complex algorithms. Comprehensive solutions also offer tools for aggregating and managing EPC data in either a federated or central data source.
- RFID middleware solutions need to provide the messaging, routing and connectivity features required to reliably integrate RFID data into existing SCM, ERP, WMS, or CRM systems. Ideally through a Services-Oriented Architecture (SOA).
- A services-oriented architecture is essentially a collection of services. These services communicate with each other. The communication can involve either simple data exchange or two or more services coordinating some activity, such as order placement or inventory control.
- Middleware needs to provide a library of adapters to popular WMS and SCM applications (e.g., SAP or Oracle E Business Suite). Application Programming Interfaces (APIs) and adapters for using standard technologies like JMS, XML and SOAP to integrate with other third-party applications.

- RFID middleware must provide :
  1. B2B integration features like partner profile management
  2. Support for B2B transport protocols
  3. Integration with a partner's data over communications such as EDI, Web-based systems like AS2,or a well engineered system specifically for EPC data RFID Middleware
- RFID middleware platforms that include packaged routing logic, product data schemas and integration with typical RFID-related applications and processes like shipping, receiving and asset tracking are major assets.
- RFID middleware platforms must include features for dynamically balancing processing loads across multiple servers and automatically rerouting data

RFID Middleware benefits

a. Minimized network traffic through intelligent filtering

b. Lower reader-management costs through centrally coordinated readers

c. Immediate visibility to pertinent RFID data through routing, filtering and track-and-trace tools

d. Minimized on-going integration costs through standard APIs and prepackaged application integration tools

e. Well-architected RFID middleware can enable more strategic opportunities that go way beyond these initial, rather obvious benefits

Industrial plants

- Smart environments also help in improving the automation in industrial plants with a massive deployment of RFID tags associated to the production parts. In a generic scenario, as production parts reach the processing point, the tag is read by the RFID reader.
- An event is generated by the reader with all the necessary data, such as the RFID number and stored on the network. The machine/robot gets notified by this event and picks up the production part.
- By matching data from the enterprise system and the RFID tag, it knows how to further process the part. In parallel, a wireless sensor mounted on the machine monitors the vibration and if it exceeds a specific threshold an event is raised to immediately stop the process.
- Once such an emergency event is propagated, devices that consume it react accordingly. The robot receives the emergency shut-down event and immediately stops its operation. The plant manager also immediately sees the status of the so

called Enterprise Resource Planning (ERP) orders, the production progress, the device status, as well as a global view on all the elements and the possible side effects of a production line delay due to shop-floor device malfunctions.

Weaknesses of RFID

1. Lack of industry and application standards
2. High cost per unit and high RFID system integration costs
3. Weak market understanding of the benefits of RFID technology

5.1.1 Wireless Sensor

- Wireless sensors are standard measurement tools equipped with transmitters to convert signals from process control instruments into a radio transmission. The radio signal is interpreted by a receiver which then converts the wireless signal to a specific, desired output, such as an analog current or data analysis via computer software.
- Wireless sensors gather data about local conditions and share findings with other powerful components or platforms for further processing. Sensors are typically distributed across large geographic areas and programmed to communicate with central hubs, gateways, and servers.
- A Wireless Sensor Network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc.
- WSNs nowadays usually include sensor nodes, actuator, nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area, form networks through self-organization.
- Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multi-hop routing and finally reach the management node through the internet or satellite.
- Standards for WSN technology have been well deployed, such as Zigbee (IEEE 802.15.4). The IEEE 802.15.4 is simple packet data protocol for lightweight wireless networks.
- It works well for long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics.

5.1.2 Wireless Networks

- Wireless local area network (WLAN) has data transfer speeds ranging from 1 to 54 Mbps. WLAN signal can be broadcast to cover an area ranging in size from a small office to a large campus. Most commonly, a WLAN access point provides access within a radius of 65 to 300 feet.
- IEEE 802.11 standard for WLANs.
- The 802.11 specifications were developed specifically for Wireless Local Area Networks (WLANs) by the IEEE and include four subsets of Ethernet-based protocol standards: 802.11, 802.11a, 802.11b, and 802.11g.
- 802.11 operated in the 2.4 GHz range and was the original specification of the 802.11 IEEE standards. This specification delivered 1 to 2 Mbps using a technology known as phase-shift keying (PSK) modulation.
- 802.11a operates in the 5 - 6 GHz range with data rates commonly in the 6 Mbps, 12 Mbps, or 24 Mbps range. Because 802.11a uses the orthogonal frequency division multiplexing (OFDM) standard, data transfer rates can be as high as 54 Mbps.
- The 802.11b standard operates in the 2.4 GHz range with up to 11 Mbps data rates and is backward compatible with the 802.11 standard. 802.11b uses a technology known as complementary code keying (CCK) modulation.
- 802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance.
- Fig. 5.1.4 shows WLAN.

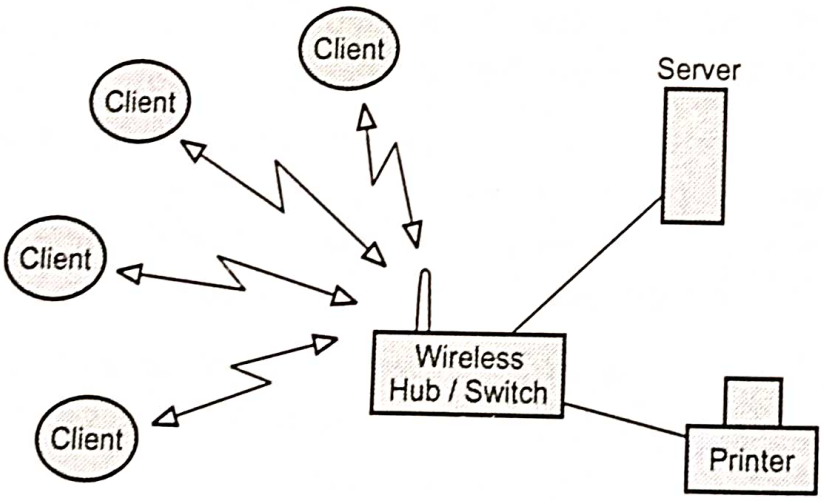


Fig. 5.1.4 Wireless LAN

- IEEE 802.11 defines the physical (PHY), logical link (LLC) and media access control (MAC) layers for a wireless LAN. Wireless Access Points (APs) is a small device that bridges wireless traffic to your network.

5.1.3 Wireless Sensor Networking

- A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc.
- WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area , form networks through self-organization.
- Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multi- hop routing, and finally reach the management node through the internet or satellite.
- Standards for WSN technology have been well developed, such as Zigbee (IEEE802.15.4). The IEEE 802.15.4 is simple packet data protocol for lightweight wireless networks.
- It works well for long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics.
- WSN is more for sensing and information-collecting purposes. Other networks include body sensor network (BSN), visual or video sensor network (VSN), vehicular sensor networks, underwater (acoustic) sensor networks, interplanetary sensor networks, fieldbus networks, and others.
- The extended scope of WSN is the USN, or ubiquitous sensor network, a network of intelligent sensors that could one day become ubiquitous.
- WSN developed at Linköping University in Sweden is based on the ZigBee specification and is an IoT solution. It provides nodes for monitoring temperature, relative humidity, carbon dioxide, VOC, PM and electricity consumption as well as for automatic control.
- A wireless sensor network is a network formed by a large number of sensor nodes where each node is equipped with some sensors to detect physical phenomena. In IoT, the sensor nodes and devices are interconnected to transmit useful measurement information via distributed sensor networks.
- Other networks are body sensor network (BSN), video sensor network (VSN), vehicular sensor network (V2V), interplanetary sensor network etc.
- VSN devices come with image sensors, adequate processing power and memory. They use wireless communication interfaces to collaborate and jointly solve tasks such as tracking persons within the network. In all applications, VSNs monitor a potentially large group of people and record sensitive image data which might contain identities of persons, their behaviour, interaction patterns or personal preferences.

- A central idea of VSNs is to keep data processing local to reduce the amount of transmitted data. Fig. 5.1.5 shows VSN.

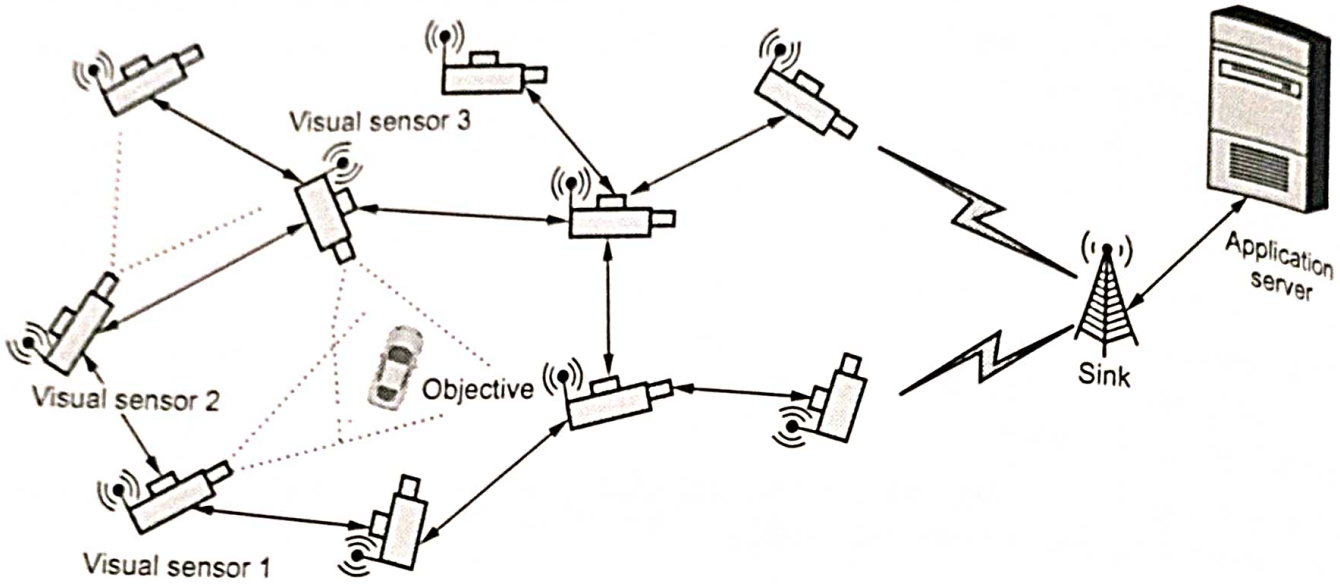


Fig. 5.1.5 : Example of wireless visual sensor networks

- A single VSN device has only a limited field of view but VSNs are typically designed to cover large areas. Therefore, multiple spatially distributed nodes are required. To avoid centralized control and data processing, VSNs use peer to peer communication for coordination, configuration, data exchange, handover of tracked objects or data fusion.
- To simplify deployment of spatially distributed VSNs, they rely no longer only on dedicated communication networks but make use of existing infrastructure which is not under full control of the VSN operators.
- Other VSN applications include environmental monitoring, smart homes and meeting rooms, entertainment and virtual reality as well as elderly care and assisted living.
- Body sensor network (BSN) is one of application of wearable computing device to enable wireless communication between several miniaturized body-sensor units and a single body central unit worn on the human body to transmit vital signs and motion readings to medical practitioners.
- Fig. 5.1.6 shows sources of body sensor network.

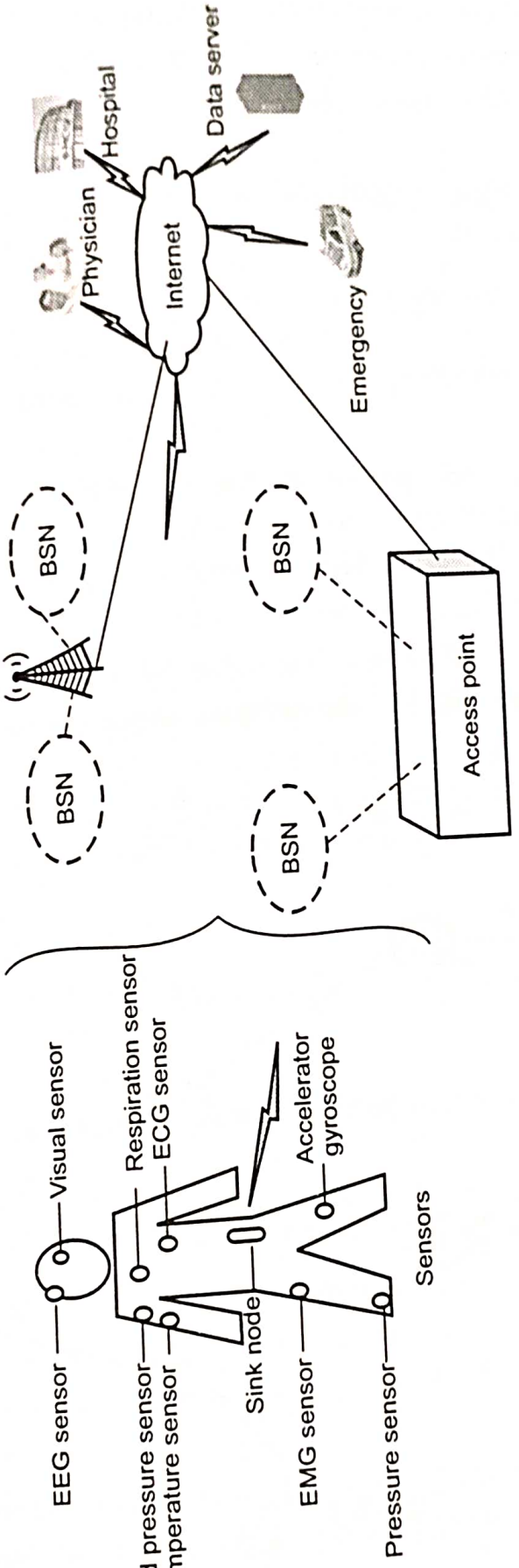


Fig. 5.1.6 : Source of body sensor network

- Sensor node electronics should be miniaturized, low power and detect medical signals such as electrocardiogram (ECG), photoplethysmogram (PPG), pulse rate, blood flow, pressure and temperature. The collected data from the control devices are then transferred to remote destinations in a wireless body area network for diagnostics.
- Most pupolar wireless technologies used for medical monitoring are ZigBee, WLAN, GSM, Bluetooth.
- Sensor nodes are designed to collect raw signals from a human body. A sensor node undertakes three functions: detecting signal via a front end, digitizing/coding/controlling for a multi access communication and finally wireless transmission.
- In data acquisition and processing, the microcontroller maintains a power management scheme to control the distribution of the energy from battery in an optimized manner. The signal from a human body is usually weak and coupled with noise.
- The development of WSNs was motivated by military applications such as battlefield surveillance. Fig. 5.1.7 shows typical sensor network.

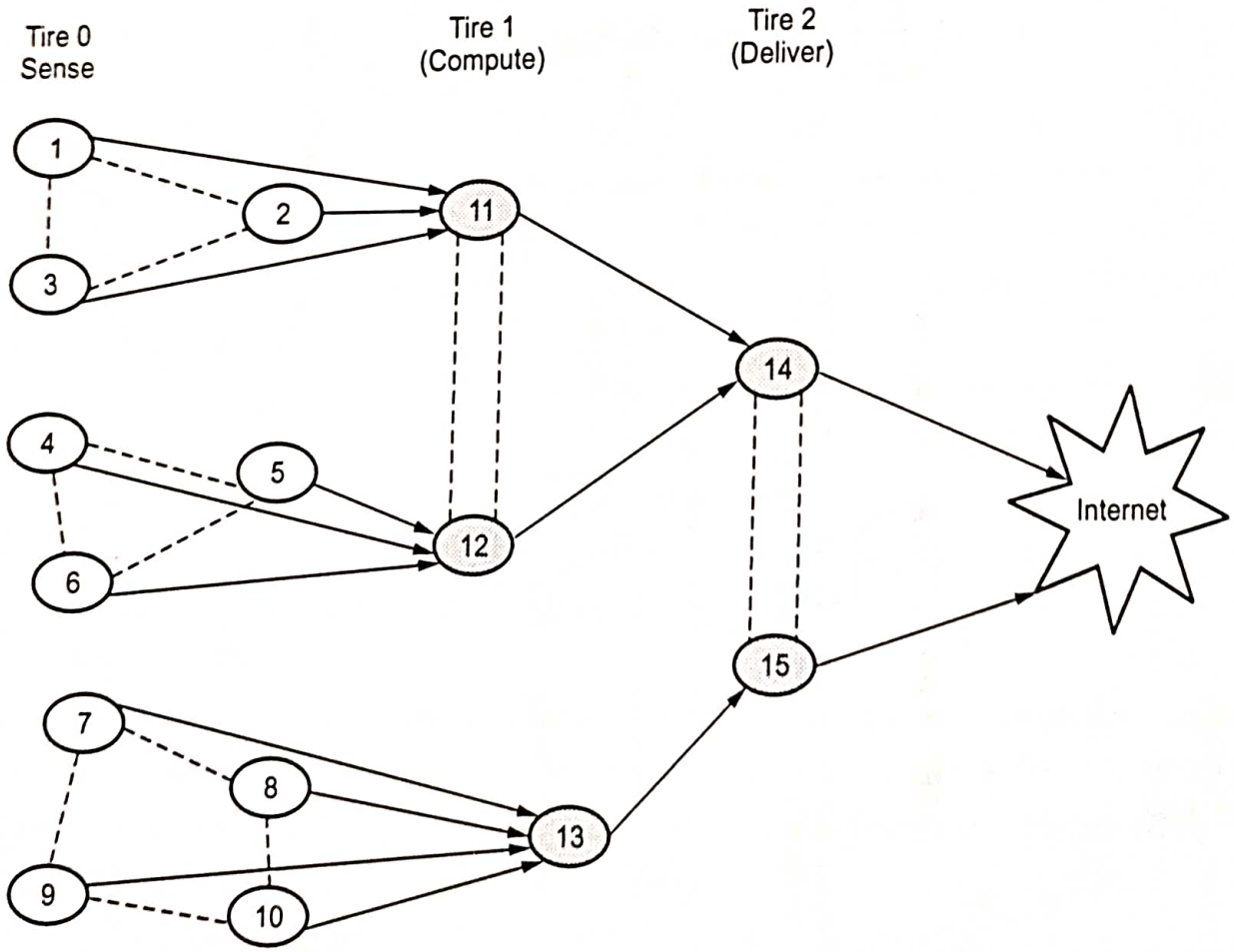


Fig. 5.1.7 : Sensor network architecture

- WSN is built of nodes, each node connected to one or more sensors. Each such sensor network node has typically several parts: a radio transceiver with an antenna, a microcontroller, an electronic circuit for interfacing with the sensors, and an energy source, usually a battery or an embedded form of energy harvesting.
- Topology of sensor network may be star topology or mesh topology. Following are the components used by sensor networks:
  1. Sensor node: sense target events, gather sensor readings, manipulate information, send them to gateway via radio link
  2. Base station/ sink: communicate with sensor nodes and user/ operator
  3. Operator/ user: task manager, send query
- For reliable data transmission in a WSN, routing method is used. Routing protocols are distributed and reactive. The nodes in the system start looking for a route only when they have application data to transmit.
- Commonly used routing algorithm for WSN are dynamic source routing (DSR) and Ad hoc on- demand distance vector (AODV).
- Energy is the scarcest resource of WSN nodes, and it deter-mines the lifetime of WSNs. WSNs are meant to be deployed in large numbers in various environments, including remote and hostile regions, with ad hoc communications as key. For this reason, algorithms and protocols need to address the following issues :
  1. Lifetime maximization
  2. Robustness and fault tolerance
  3. Self- configuration

5.2 Cellular Machine-to-Machine Application Network

- Machine to Machine (M2M) communication is the communication among the physical things which do not need human intervention.
- M2M communication is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. M2M is also named as Machine Type Communication (MTC) in 3GPP.
- M2M communication could be carried over mobile networks (e.g. GSM-GPRS, CDMA EVDO networks). In the M2M communication, the role of mobile network is largely confined to serve as a transport network.

- M2M is only a subset of IoT. IoT is a more encompassing phenomenon because it also includes Human-to-Machine communication (H2M).
- Radio Frequency Identification (RFID), Location-Based Services (LBS), Lab-on-a-Chip (LOC), sensors, Augmented Reality (AR), robotics and vehicle telematics, which are some of the technology innovations that employ both M2M and H2M communications.
- Reasons for shifting from M2M to IoT :
  1. It supports multiple application with multiple device.
  2. It is information and service centric.
  3. It supports open market place.
  4. IoT uses horizontal enabler approach.
  5. It requires generic commodity devices.
  6. Used in B2B and B2C.

Key features of M2M :

1. **Low mobility :** M2M Devices do not move and if moves only within a certain area.
2. **Time controlled :** Data can be sent or receive only at certain pre-defined time periods.
3. **Time tolerant :** Sometimes data transfer can be delayed.
4. **Packet switched :** Network operator to provide packet switched service.
5. **Online small data transmissions :** Devices frequently send or receive small amounts of data.
6. **Low power consumption :** To improve the ability of the system to efficiently service M2M applications.
7. **Location specific trigger :** Intending to trigger M2M device in a particular area e.g. wake up the device.

Six pillars of M2M :

- The six pillars of M2M are as follows :
  1. Remote monitoring is a generic term most often representing supervisory control, data acquisition and automation of industrial assets.
  2. RFID is a data-collection technology that uses electronic tags for storing data.
  3. A sensor network monitors physical or environmental conditions, with sensor nodes acting cooperatively to form/maintain the network.

4. The term smart service refers to the process of networking equipment and monitoring it at a customer's site so that it can be maintained and serviced more effectively.
5. Telematics to the integration of telecommunications and infomatics, but most often it refers to tracking, navigation and entertainment applications in vehicles.
6. Telemetry is usually associated with industrial, medical and wildlife-tracking applications that transmit small amounts of vehicles data.

5.2.1 Architecture and Components of M2M

- Fig. 5.2.1 shows M2M architecture.

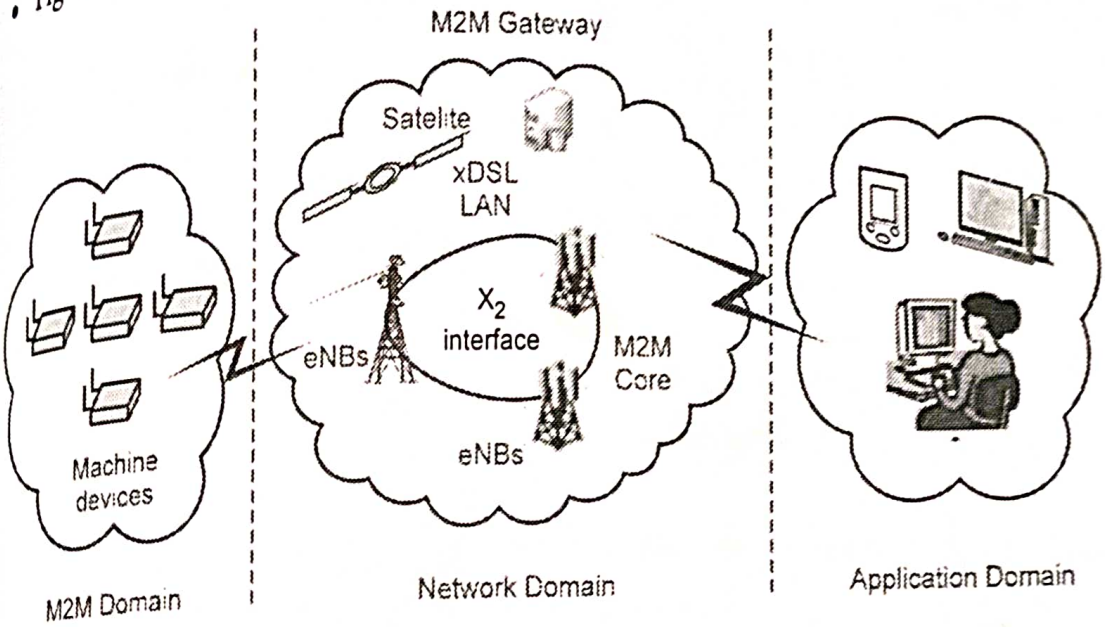


Fig. 5.2.1 : M2M architecture

- The system components of an M2M solution are as follows :

1. **M2M Device :** A device that runs application(s) using M2M capabilities and network domain functions. An M2M device is either connected straight to an access network or interfaced to M2M gateways via an M2M area network.
2. **M2M area network :** A M2M area network provides connectivity between M2M devices and M2M gateways. Examples of M2M area betworks include : Personal area network technologies such as IEEE 802.15, SRD, UWB, Zigbee, Bluetooth, etc or local networks such as PLC, M-BUS, Wireless M-BUS.
3. **M2M gateways :** Equipments using M2M capabilities to ensure M2M devices interworking and interconnection to the network and application do: ain. The M2M gateway may also run M2M applications.

4. **M2M applications server :** Applications that run the service logic and use service capabilities accessible via open interfaces.
5. **M2M application :** The application component of the solution is a realization of the highly specific monitor and control process. The application is further integrated into the overall business process system of the enterprise.

- Fig. 5.2.2 shows generic M2M solution.

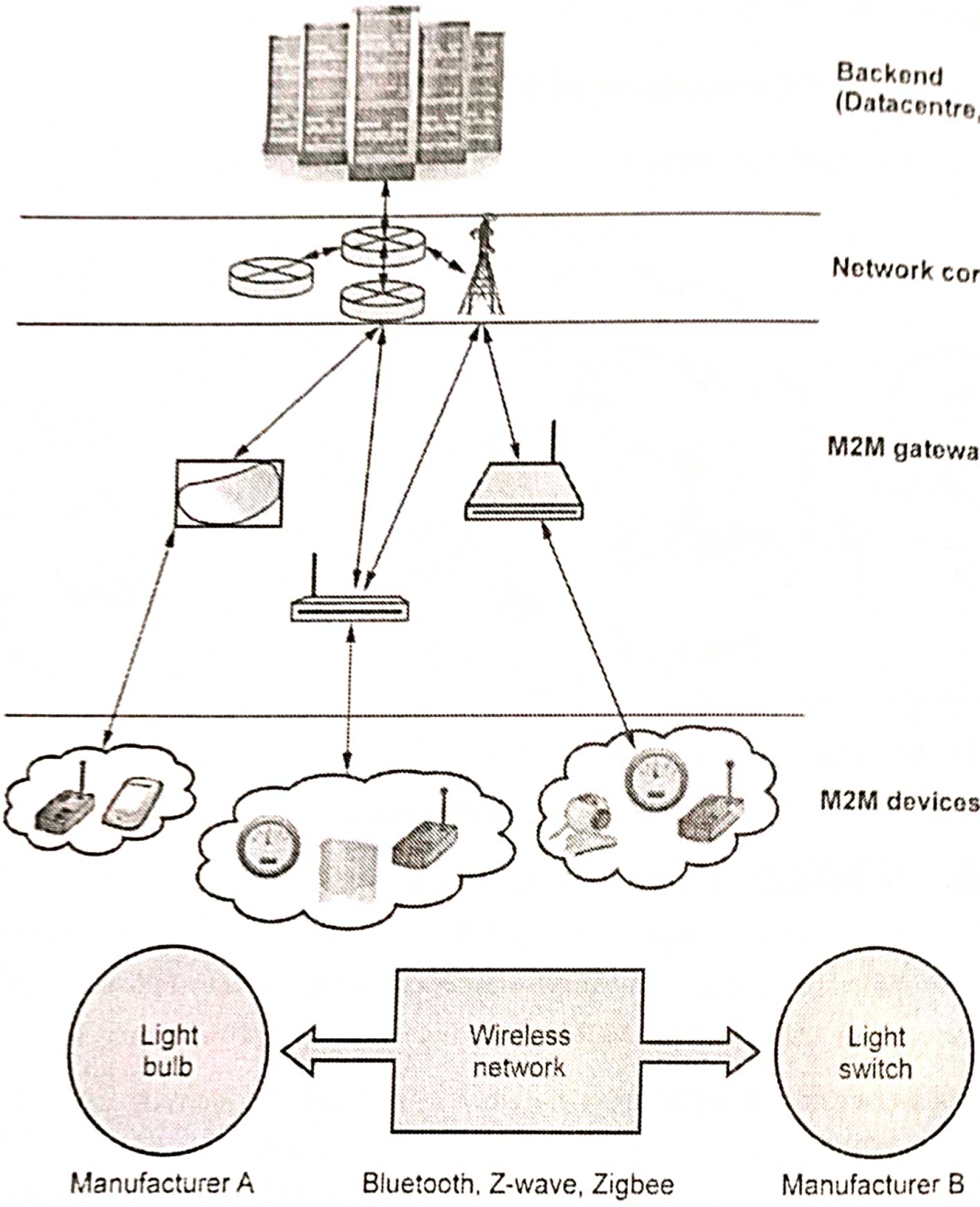


Fig. 5.2.2 Generic M2M solution

- A number of sub-sets of users of M2M services can be identified : Consumers in the home, business users and facility managers, city governments, logistics businesses, energy providers and more.

5.2.2 Difference between M2M and IoT

Machine-to-Machine	Internet of Things
It support single application with single device.	It support multiple application with multiple device.
It is communication and device centric.	It is information and service centric.
It support closed business operations.	It support open market place.
M2M uses vertical system solution approach.	IoT uses horizontal enabler approach.
It requires specialized device solutions.	It requires generic commodity devices.
Used in B2B.	Used in B2B and B2C.

5.2.3 Key Application Area

1. Security : Surveillances, Alarm systems, Access control, Car/driver security
2. Tracking and tracing : Fleet Management, Order Management, Pay as you drive, Asset Tracking, Navigation, Traffic information, Road tolling, Traffic optimization/steering
3. Payment : Point of sales, Vending machines, Gaming machines.
4. Health : Monitoring vital signs, Supporting the aged or handicapped, Web Access Telemedicine points, Remote diagnostics.
5. Remote maintenance/control : Sensors, Lighting, Pumps, Valves, Elevator control, Vending machine control, Vehicle diagnostics.
6. Metering : Power, Gas, Water, Heating, Grid control, Industrial metering.
7. Manufacturing : Production chain monitoring and automation.
8. Facility management : Home / building / campus automation.

Sr. No.	Industry/Vertical	M2M applications
1.	Automotive	Passenger vehicle anti theft/recovery, monitoring/ maintenance, safety/control, entertainment.
2.	Transportation	Fleet management, asset tracking telematics manufacturing and logistics.
3.	Utilities/ Energy	Smart metering, smart grid, electric line monitoring , gas/oil/water pipeline monitoring.
4.	Security	Commercial and home security monitoring, surveillance applications, fire alarm, police/medical alert.
5.	Financial/Retail	Point of sale (POS), ATM Kiosk, vending machines, digital signage and handheld terminals.

6	Healthcare	Remote monitoring of patient after surgery (e-health), remote diagnostics, medication reminders, tele-medicine.
7.	Public safety	Highway, bridge traffic management, homeland security, police, fire and emergency services.

India Market Scenario

- As per projections by Ericssion, Indian M2M market may rise from 30 Million in 2013 to more than 250 million in 2020. Automotive (connected vehicles) is having a market share of 45 % and Energy (smart meters) 23 %.
- Other applications are Point of sale (POS), healthcare, security and surveillance, intelligent buildings, smart homes etc. M2M applications will make the living smart and improve the quality of life.

5.2.4 M2M Value Chains

- The "value chain" has been a basic business concept for many years. Each link in the chain "adds value" in a somewhat linear progression from raw materials to finished products or services. It is a useful concept for identifying key elements in the route to market for new product ideas and for highlighting where new profits can be made.
- Fig. 5.2.3 shows M2M value creation chain.

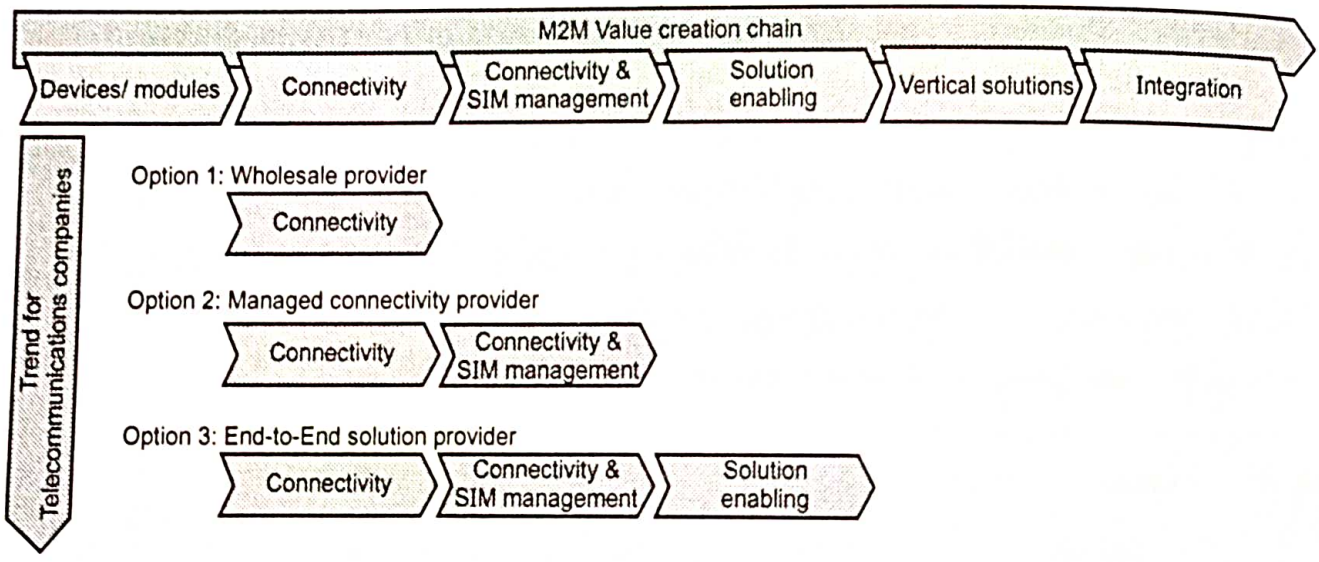


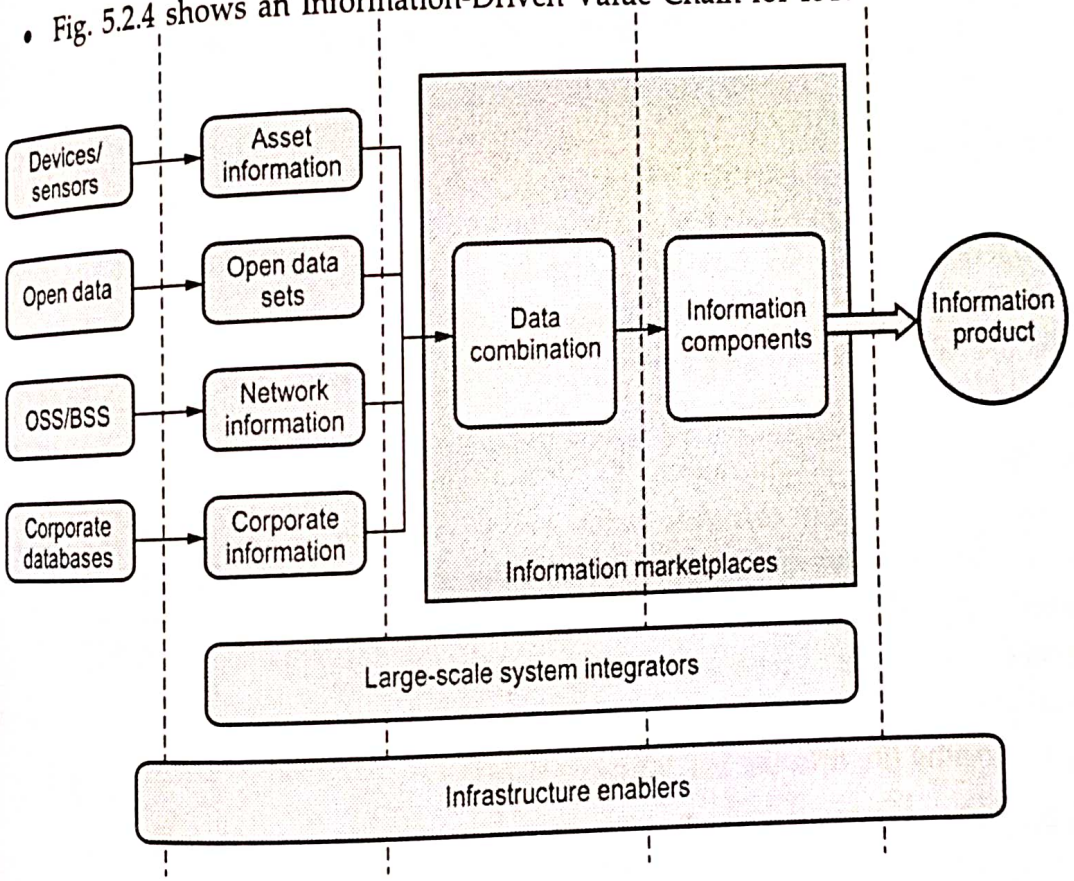
Fig. 5.2.3 : M2M value creation chain

- **Inputs :** It is raw material which converted into product. For example : Information is converted into required data. Coal mined for making domestic steel.
- **Production or manufacture :** It processes the raw inputs which becomes a part of a value chain. Data from an M2M solution, meanwhile, needs to be verified and tagged for provenance.

- **Processing :** Product is prepared for sale.
- **Packaging :** Packaging refers to the process whereby a product can be branded as would be recognizable to end-user consumers.
- **Distribution/Marketing :** This process refers to the channels to market for products.

5.2.5 IoT Value Chains

- IoT value chains based on data are to some extent enabled by open APIs and the other open web-based technologies.
- Required data is collected from publicly available resources and take from other company data. An information marketplace is available in world for getting data.
- It should be noted that such a marketplace could still be internal to a company or strictly protected between the value chains of several companies.
- Open APIs allow for the knowledge contained within different technical systems to become unembedded, creating the possibility for many different economic entities to combine and share their data as long as they have a well-defined interface and description of how the data is formatted.
- Fig. 5.2.4 shows an Information-Driven Value Chain for IoT.



Input ⇨ Production ⇨ Processing ⇨ Packaging ⇨ Distribution & marketing

Fig. 5.2.4 : Information-driven value chain for IoT

M2M value chain	IoT value chain	Description
Input	Sensors	Similar to M2M device solution.
	Open data	Provided by government and city organizations.
	Operational support systems / business support systems	Used increasingly in tightly closed information marketplaces.
	Corporate database	Contains various database like supply chain management, payroll, accounting etc.
Production	Asset Information	It store information like temperature over time of container during transit or air quality during a particular month.
	Open data sets	It may include maps, rail timetables or demographics about a certain area.
	Network information	Contains GPS data, services accessed via the mobile network.
	Corporate information	Current state of demand for a particular product in the supply chain at a particular moment in time.
Processing	Data combination	Data is mixed together from various sources.
Packaging	Information components	Packaging section of the information value chain creates information components.
Distribution and marketing	Information product	Company may have market information about a certain area of town.

- 'Intelligence' is imparted through a process of generating and sharing information between these 'things'. Therefore connectivity is an essential element where today there are a number of open and proprietary standards governing connectivity between devices and networks.
- Connectivity enables applications that take advantage of the connected devices to create value to the end user. The applications are managed through platforms that provide critical and value added business support services such as device management, security, accounting and billing, data management and analytics, etc., to breathe life into the IoT infrastructure.
- Fig. 5.2.5 shows IoT value stack.

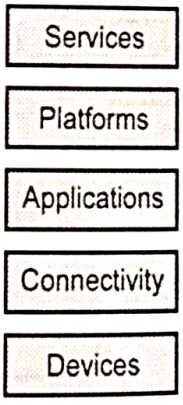


Fig. 5.2.5 : IoT value stack

- From a value perspective, value will be appropriated by each layer of the IoT model : Device, connectivity, applications, platforms and services. Devices and connectivity are viewed as commodities with consequently low value appropriation whereas in applications, platforms and services is where the value lies because that's where the 'brains' of the operation resides as opposed to the connected limbs and veins that represent devices and connectivity.

5.3 Network Devices : IoT Device

- IoT devices have unique identity and they are refer as "things" in IoT. Device can perform remote sensing, actuating and monitoring.
- IoT devices can exchange data between them and process data or send to centralized location for processing and storage. Fig. 5.3.1 shows block diagram of IoT device.

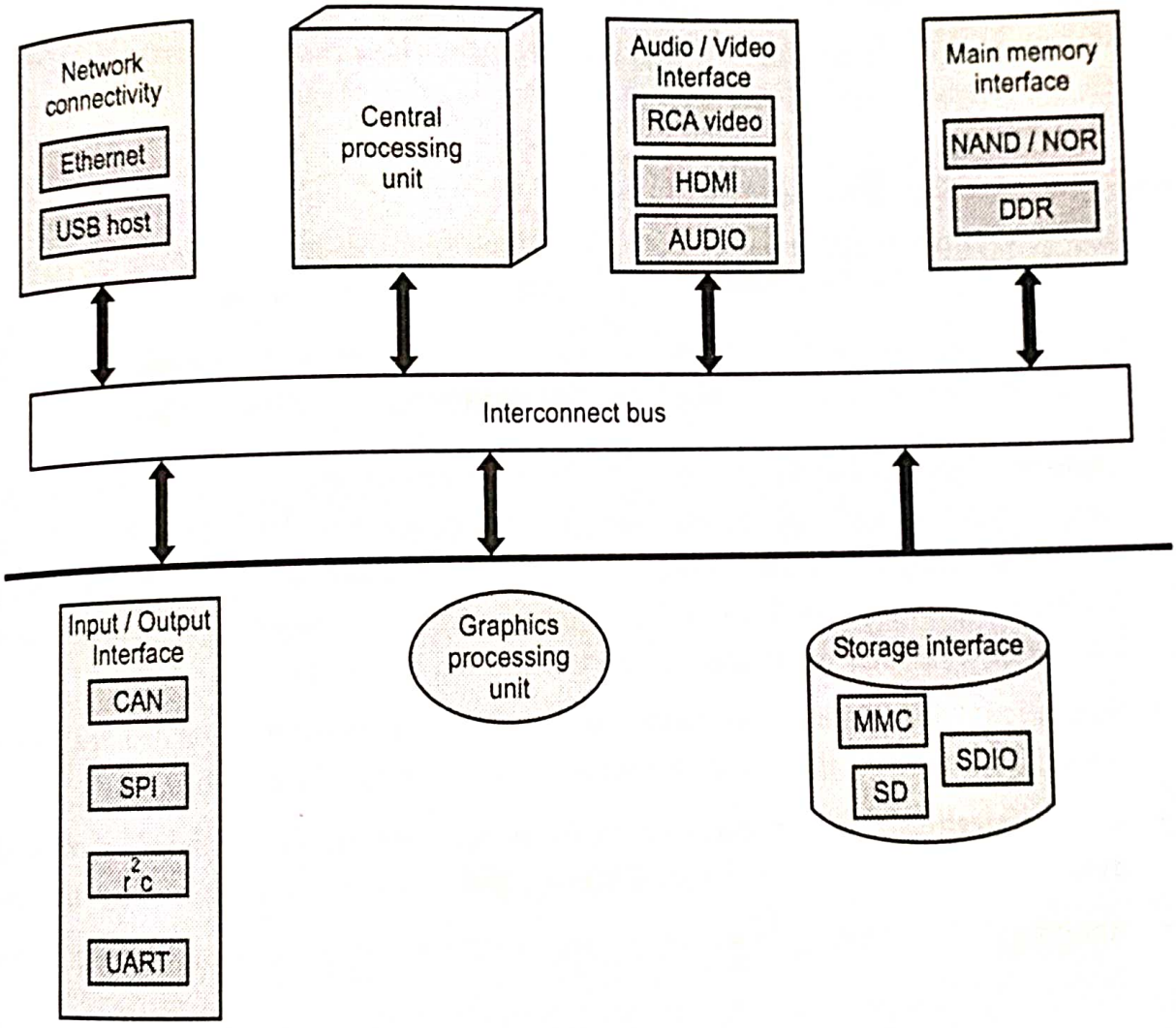


Fig. 5.3.1 : Block diagram of IoT device

- IoT devices provide interface to various wire and wireless devices. Interface includes memory interface, I/O interface for sensors, Internet connectivity interface, storage interface etc.
- Using sensors, IoT collects various information like temperature, light intensity, humidity, air pressure. Some application used cloud based storage. Collected information is stored in cloud and transmitted to other devices.
- Various types of IoT devices are smart clothing, smart watch, wearable sensors, LED lights, automobile industry etc. Fig. 5.3.2 shows IoT devices.

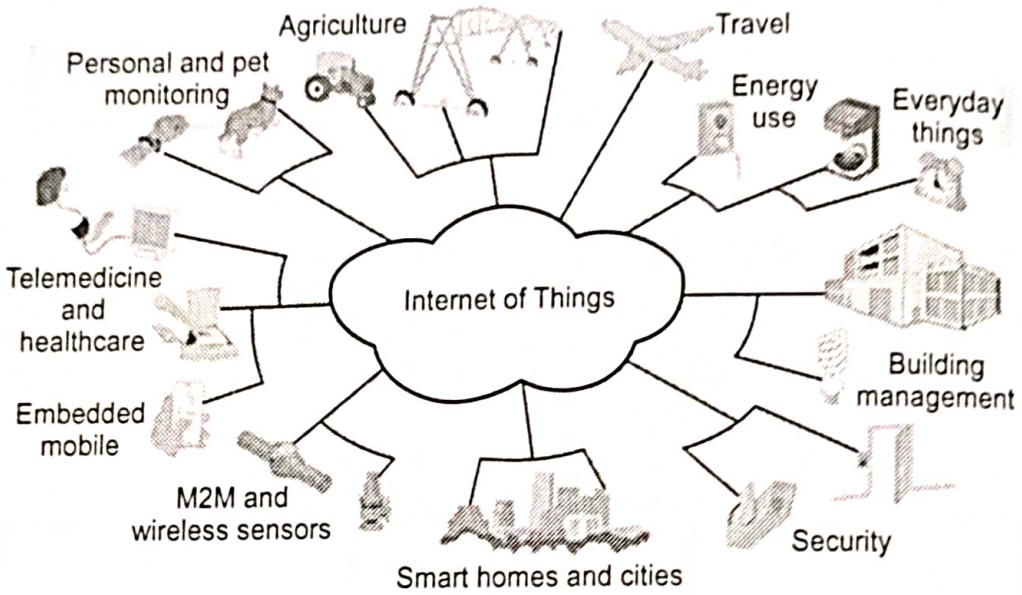


Fig. 5.3.2 : IoT devices

- **Sensor :** Devices that can measure a physical quantity and convert it into a signal, which can be read and interpreted by the microcontroller unit. These devices consist of energy modules, power management modules, RF modules and sensing modules. Most sensors fall into 2 categories : Digital or analog. An analog data is converted to digital value that can be transmitted to the Internet.
- **Actuation :** IoT devices can have various types of actuators attached that allow taking actions upon the physical entities in the vicinity of the device.
- **Communication :** Communication modules are responsible for sending collected data to other device or cloud based servers and receiving data from other devices.
- Analysis and processing modules are responsible for making sense of the collected data.

IoT Device Life Cycle :

- IoT devices are generally more like single-purpose computers. The first life cycle, for example, includes four steps :

1. **Boot-up :** The device loads the firmware and starts to work as defined.
2. **Initialization :** Once boot-up is completed, the system reads the configuration, established connections, syncs up data, etc.
3. **Operation :** The device performs its designed purpose continually.
4. **Update :** New firmware is installed, the device reboots and then starts to load the new firmware.

- The device should complete its previous life cycle before starting the next life cycle every time the firmware is updated. Eventually, the device will be retired for whatever reason. When it does, it reaches the end of the device life cycle called termination.

5.3.1 IoT System Building Blocks

- The hardware utilized in IoT systems includes devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication, and detection to support-specific goals and actions.
- Major components of IoT devices are as follows :

1. **Control units :** A small computer on a single integrated circuit containing processor core, memory and a programmable I/O peripheral. It is responsible for the main operation.
2. **Sensor :** Devices that can measure a physical quantity and convert it into a signal, which can be read and interpreted by the microcontroller unit. These devices consist of energy modules, power management modules, RF modules, and sensing modules. Most sensors fall into 2 categories: Digital or analog. An analog data is converted to digital value that can be transmitted to the Internet.
   a. Temperature sensors : accelerometers
   b. Image sensors: gyroscopes
   c. Light sensors : acoustic sensors
   d. Micro flow sensors : humidity sensors
   e. Gas RFID sensors : pressure sensors
3. **Communication modules :** These are the part of devices and responsible for communication with rest of IoT platform. They provide connectivity according to wireless or wired communication protocol they are designed. The communication between IoT devices and the Internet is performed in two ways :

A) There is an Internet-enable intermediate node acting as a gateway;

B) The IoT Device has direct communication with the Internet.

- The communication between the main control unit and the communication module uses serial protocol in most cases.

4. Power sources : In small devices the current is usually produced by sources like batteries, thermocouples and solar cells. Mobile devices are mostly powered by lightweight batteries that can be recharged for longer life duration.

- **Communication Technology and Protocol :** IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

Working :

1. Collect and transmit data : The device can sense the environment and collect information related to it and transmit it to a different device or to the Internet.
2. Actuate device based on triggers : It can be programmed to actuate other devices based on conditions set by user.
3. Receive information : Device can also receive information from the network.
4. Communication assistance : It provides communication between two devices of same network or different network.

- Fig. 5.3.3 shows working of IoT.

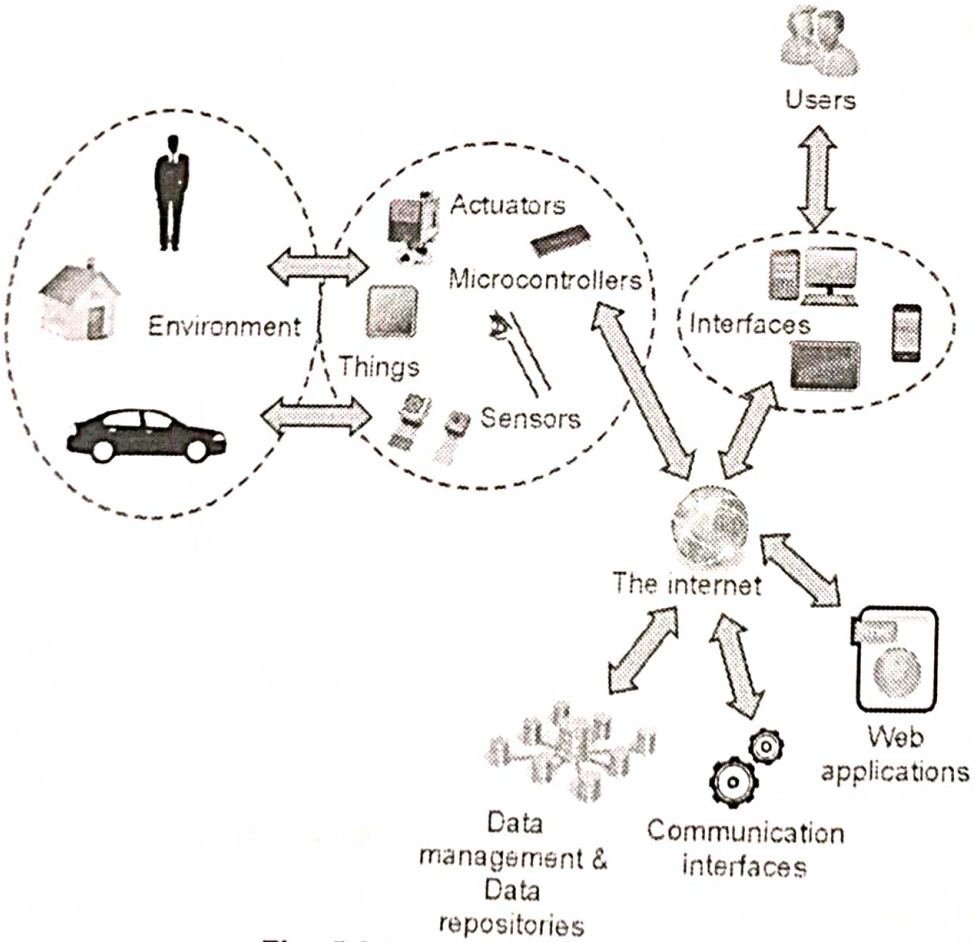


Fig. 5.3.3 : Working of IoT

- Sensors for various applications are used in different IoT devices as per different applications such as temperature, power, humidity, proximity, force etc.
- Gateway takes care of various wireless standard interfaces and hence one gateway can handle multiple techologies and multiple sensors. The typical wireless technologies used widely are 6LoWPAN, Zigbee, Zwave, RFID, NFC etc. Gateway interfaces with cloud using backbone wireless or wired technologies such as WiFi, Mobile , DSL or Fibre.

5.4 Device Configuration and Management

Need for IoT Systems Management :

- IoT system management is required for following :
  a. Automating Configuration
  b. Monitoring Operational and Statistical Data
  c. Improved Reliability
  d. System Wide Configurations
  e. Multiple System Configurations
  f. Retrieving and Reusing Configurations

5.4.1 Simple Network Management Protocol (SNMP)

- SNMP is a well-known and widely used network management protocol that allows monitoring and con?guring network devices such as routers, switches, servers, printers, etc.
- SNMP component include Network Management Station (NMS), Managed Device, Management Information Base (MIB) and SNMP Agent that runs on the device.
- Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions.
- SNMP provides a common language for network devices to relay management information in a local area network (LAN) or wide area network (WAN).
- SNMP has a simple architecture based on a client-server model. The servers, called managers, collect and process information about devices on the network.
- The clients, called agents, are any type of device or device component connected to the network. They can include not just computers but also network switches, phones, printers, and so on.
- Some devices may have multiple device components. For example, a laptop typically contains a wired as well as a wireless network interface.

Strength of SNMP :

1. It is simple to implement.
2. Agents are widely implement.
3. Agent level overhead is minimal.
4. It is robust and extensible.
5. Polling approach is good for LAN based managed object.
6. It offers the best direct manager agent interface.
7. SNMP meet a critical need.

Limitation of SNMP :

1. It is too simple and does not scale well.
2. There is no object orietned data view.
3. It has no standard control definition.
4. It has many implementation specific (private MIB) extensions.
5. It has high communication overhead due to polling.

5.4.2 Network Operator Requirements

- Ease of use
- Distinction between configuration and state data
- Fetch configuration and state data separately
- Configuration of the network as a whole
- Configuration transactions across devices
- Dump and restore configurations
- Support for both data-oriented and task oriented access control

5.4.3 NETCONF

- Network Configuration Protocol (NETCONF) is a session-based network management protocol. NETCONF allows retrieving state or configuration data and manipulating configuration data on network devices.
- NETCONF is the standard for installing, manipulating and deleting configuration of network devices.
- Fig 5.4.1 shows NEFCONF protocol layers.

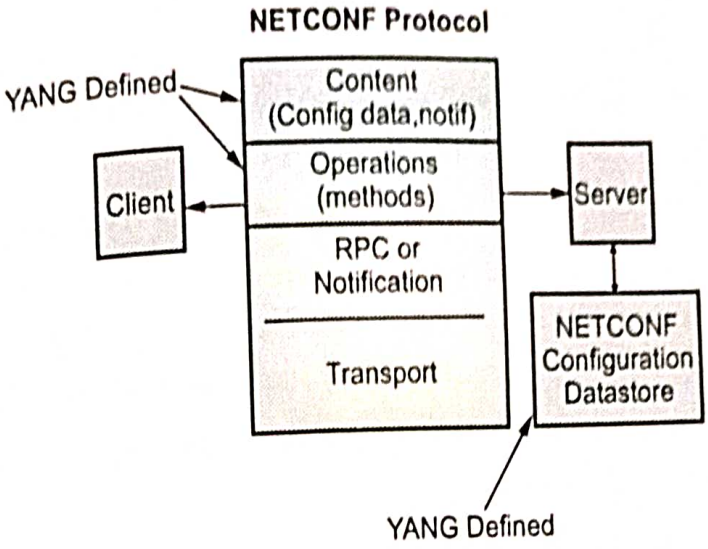


Fig. 5.4.1 : NEFCONF protocol layers

- NETCONF is defined for transaction-safe configuration of devices. This means that scenarios like setting up initial configuration for a range of devices, changing ACLs and adding VPNs, can be performed automatically, while keeping flexibility and vendor independence.
- It uses an Extensible Markup Language (XML) based data encoding for the configuration data as well as the protocol messages.
- NETCONF uses a simple Remote Procedure Call (RPC) based mechanism to facilitate communication between a client and a server. The server is a network device and client can be a script or application running as part of a network manager.
- It uses Secure Shell(SSH) as the transport layer across network devices.
- NETCONF provides various operations to retrieve and edit configuration data from network devices.
- The Content Layer consists of configuration and state data which is XML-encoded.
- The schema of the configuration and state data is defined in a data modeling language called YANG.
- NETCONF provides a clear separation of the configuration and state data. The configuration data resides within a NETCONF configuration datastore on the server.
- All NETCONF devices must allow the configuration data to be locked, edited, saved, and unlocked. In addition, all modifications to the configuration data must be saved across a reboot in non-volatile storage

5.4.4 YANG

- YANG is a data modeling language used to model configuration and state data manipulated by the NETCONF protocol.
- YANG is used to model both configuration and state data of network elements.
- YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints.
- YANG data definitions are contained in modules and provide a strong set of features for extensibility and reuse.
- YANG modules defines the data exchanged between the NETCONF client and server. A module comprises of a number of 'leaf' nodes which are organized into a hierarchical tree structure.

5.5 Exchange Information in Real Time without Human Intervention

- Integration of different cyber-physical systems involves a development process that takes into account some solutions for intercommunicating and interoperating heterogeneous devices. Each device can be managed as a thing within the Internet-of-Things concept by using web technologies.

1. Machine-Machine Interaction

- Reasons for requiring holistic information management :
  a) Increase of flexibility in complex production systems of manufacturing companies by enabling in-process planning, reconfiguration and control.
  b) Decentralization of responsibilities in terms of planning and execution of production tasks to reach the aimed flexibility and customization in production processes.
  c) Enabling methods of learning and the usage of enhanced process knowledge directly between machines and throughout the entire information and communication supply chain of a manufacturing enterprise.
- The most common representatives of the semantic approaches are the Data Distribution Service (DDS) for Real-Time Systems (RTS) and the OPC Unified Architecture (OPC UA) standard as a successor of the well-known and within the industrial reality well-established OLE for Process Control (OPC) standard

2. Field Bus Systems and the Industrial Ethernet

- A field bus is a serial bus system used in machines and systems to connect sensors and actuators (motors) to each other and to one or multiple masters. The hardware level determines fundamental bus properties, such as cable lengths and transmission capacity.

- Field bus protocols work according to master-slave principles and are intended to optimize the communication in centralized automation environments. Field bus systems emphasize on the networking with Programmable Logic Controllers (PLC) or Supervisory Control and Data Acquisition (SCADA) systems.
- In the traditional view, an industrial automation system, such as a manufacturing assembly line, needs an organized hierarchy of controller systems to function. In this hierarchy, there is usually a Human Machine Interface (HMI) at the top, where an operator monitors or operates the system.
- This top-level system is typically linked to a middle layer of one or more programmable logic controllers (PLC), historically via a non-time-critical communications system (e.g., Ethernet), i.e., a serial network.
- At the bottom of the control chain is the Fieldbus that links the PLCs to the components that do the actual work, such as sensors, actuators, electric motors, console lights, switches, valves, and contactors.

3. Data Distribution Service (DDS)

- Data Distribution Service is a middleware protocol and API standard for data-centric connectivity from the object management group. It integrates the components of a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture that business and mission-critical IoT applications need.
- The underlying technology of DDS is the Real-Time Publish-Subscribe (RTPS) wire protocol. This protocol serves as a standardized API for Ethernet based communication and follows the communication behavior of Data-Centric Publish-Subscribe (DCPS) mechanisms.
- DDS provides applications with explicit control over a wide set of non-functional properties, such as data availability, data delivery, data timeliness and resource usage through a rich set of QoS policies.
- DDS subscriptions are matched against the topic type and name, as well as against the QoS being offered/requested by data writers and readers.

4. OPC Unified Architecture

- The OPC Unified Architecture (UA), released in 2008, is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC classic specifications into one extensible framework.
- Automation systems have emerged from closed control loops on the shop floor that are merely connected through a field bus protocol. In traditional automation systems, vertical interoperability is not present, and if, then only operating from top-level systems down to the shop floor.

- Fig. 5.5.1 shows the hierarchical organization of automation systems.

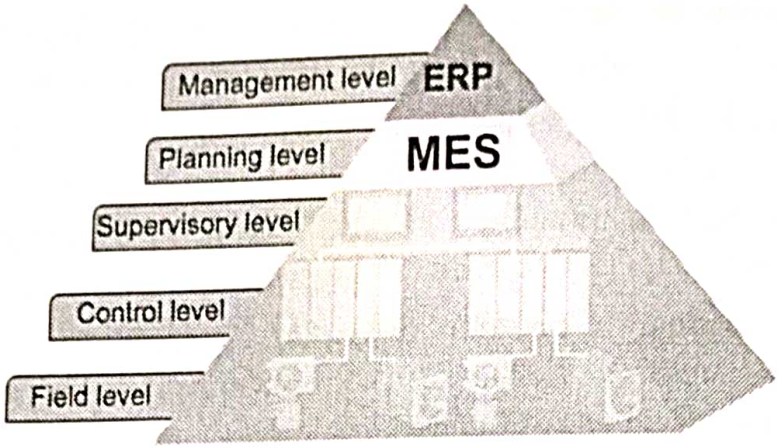


Fig. 5.5.1 : Hierarchical organization of automation systems

- Information for the planning and execution of production processes are usually predefined in ERP and MES systems based on historical data or special domain knowledge in a rather manual way.
- Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems use information from the field level, to guarantee the functionality of production in a determined way.
- The basic communication functionalities of OLE for Process Control (OPC) Data Access (DA) are based on the traditional server-client principles. OPC is a software interface standard that allows Windows programs to communicate with industrial hardware devices.
- Fig. 5.5.2 shows OPC.

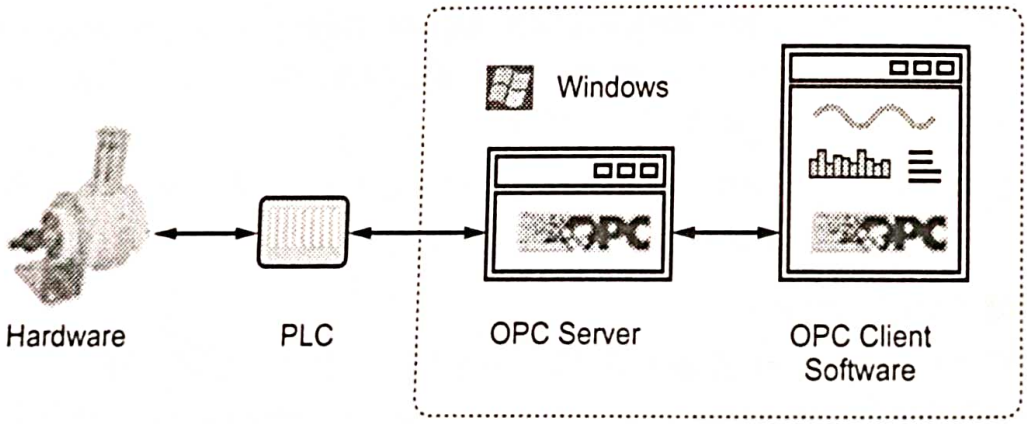


Fig. 5.5.2 : OPC

- The OPC server is a software program that converts the hardware communication protocol used by a PLC into the OPC protocol. The OPC client software is any program that needs to connect to the hardware, such as an HMI. The OPC client uses the OPC server to get data from or send commands to the hardware.

- OPC Servers are able to store information and to provide services to the data, whereas OPC Clients read and redistribute this information.
- OPC specification describes the interface between clients and servers, servers and servers, including access to real-time data, monitoring of alarms and events, access to historical data and other applications.
- Benefits of using OPC standard are :
  a) Reduced load on the hardware device.
  b) Increased scalability of the system.
  c) Because of OPC server, client applications need not know anything about hardware protocol details.
  d) Though device need not serve multiple clients, So Increased life for the device.
  e) Interoperability (Unix/Linux and Windows - both platforms are supported by OPC)
  f) Standardization

5.6 IoT Protocols

- Fig. 5.6.1 shows IoT protocols.

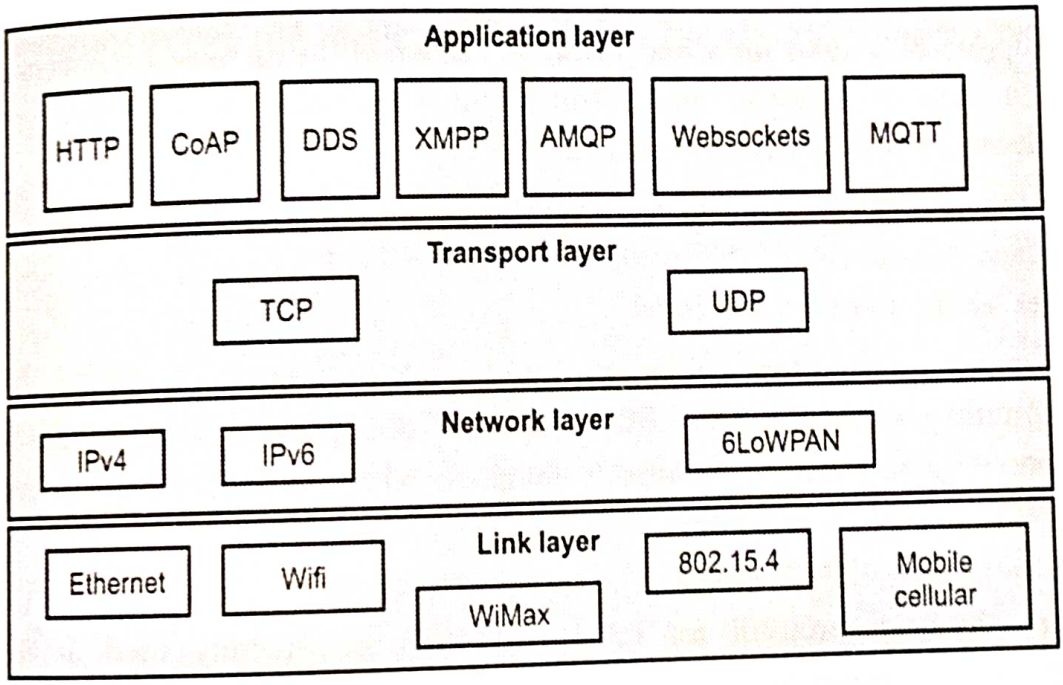


Fig. 5.6.1 IoT protocol

- IoT protocols are an integral part of the IoT technology stack. IoT protocols and standards are broadly classified into two separate categories. These are :
  a) IoT data protocols (Presentation / Application layers)
  b) Network protocols for IoT (Datalink / Physical layers)

- IoT data protocols are used to connect low-power IoT devices. They provide communication with hardware on the user side, without the need for any Internet connection. The connectivity in IoT data protocols and standards is through a wired or cellular network.
- A protocol is a standard set of regulations and requirements that allow two electronic items to connect to and exchange information with one another. Protocols regulate data transmission among devices as well as within a network of linked devices, through both error control and specifying which data compression method to use.

5.6.1 Link Layer

- Link layer protocols determines how the data is physically sent over the network's physical layer. Link layer determines how the packets are coded and signalled by the hardware device over the medium to which the host is attached.
- Link layer protocols are Ethernet, 802.11, 802.16, 802.15.4, mobile communication, etc.
- Link layer protocols decide how data is sent on physical medium. Link layer works within the local area network. Protocol of link layer is explained below :

a. 802.3 Ethernet

- This protocol is used for wired medium. Ethernet, in its most basic version runs at 10 Mbit/s. Ethernet has traditionally been used to network enterprise workstations and to transfer non-real-time data.
- The Ethernet standard allows for several different implementations such as twisted pair and coaxial cable. The maximum length of an Ethernet is determined by the nodes' ability to detect collisions.
- The worst case occurs when two nodes at opposite ends of the bus are transmitting simultaneously. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.
- Carrier sense multiple access with collision detection (CSMA/CD) is the most commonly used protocol for LANs. 10BASE5 is generally used as low cost alternative for fiber optic media for use as a backbone segment with in a single building.
- 10BASET is 10 MHz Ethernet running over UTP cable. It also uses passive star topology. The maximum cable segment allowed is 100 - 150 meters. There is no minimum distance requirements between devices, such devices cannot be connected serially but in star wired

b. 802.11 Wifi

- Commonly referred to as Wi?Fi the 802.11 standards define a through?the?air interface between a wireless client and a base station access point or between two or more wireless clients.
- **802.11a :** The 802.11a standard uses the 5 GHz spectrum and has a maximum theoretical 54 Mbps data rate. The 5 GHz spectrum has higher attenuation than lower frequencies, such as 2.4 GHz used in 802.11b/g standards. Products with 802.11a are typically found in larger corporate networks or with wireless Internet service providers in outdoor backbone networks.
- **802.11b :** The 802.11 standard provides a maximum theoretical 11 Mbps data rate in the 2.4 GHz Industrial, Scientific and Medical (ISM) band.
- 802.11b uses Complementary Code Keying (CCK) instead of Differential Quadrature Phase Shift Keying (DQPSK) used at lower rates.
- **802.11g :** It provides 20 Mbps and more in the 2.4 GHz band.

c. 802.16 WiMax

- WiMAX refers to broadband wireless networks that are based on the IEEE 802.16 standard, which ensures compatibility and interoperability between broadband wireless access equipment.
- The802.16astandard will support OFDM in the 2-to-11 GHz frequency range. The 802.16b standard will operate in the 5 GHz ISM band. A single WiMAX tower can provide coverage to a very large area as big as 3000 square miles
- WiMAX receiver : The receiver and antenna could be a small box or Personal Computer Memory card or they could be built into a laptop the way WiFi access is today.

d. 802.15.4 Zigbee

- In 2002, seeing that neither Wi-Fi nor Bluetooth could not fit some of their needs for embedded systems, a number of industrial companies formed the consortium called ZigBee Alliance, aimed at providing standards for low cost / low consumption wireless communications. Then, with the birth of IEEE 802.15.4 group.
- ZigBee communications can reach up to 500 m, with a data rate of up to 250 kbs, for a typical power consumption of 125 to 400 µW.
- As ZigBee is based on IEEE 802.15.4, there is no wake-up signal, but slots for sleep or activity, or in asynchronous mode, devices sleeping anytime they have nothing to say, with an ever-vigilant coordinator.

- To use a ZigBee module with a microcontroller, you need to connect it to a UART. There are other, optional pins to use, including a number of analog inputs / digital IOs and a PWM output indicating the strength of the signal which you can directly connect to a LED pin for observation purposes.
- There are two modes of data transfer namely Beacon mode and Non Beacon mode.
- In Beacon mode, when the devices are not sending the data they may enter a low power state and reduces the power consumption.
- In Non-beacon mode, the end devices need to be wake up only while sending the data while the routers and coordinators need to be active most of the time.

e. Mobile Communication (2G/3G/4G)

- GSM frequencies originally designed on 900 MHz range, now also available on 800 MHz, 1800 MHz and 1900 MHz ranges. The backbone of a GSM network is a telephone network with additional cellular network capabilities
- 4G is also called as Long-Term Evolution. It's promises data transfer rates of 100 Mbps.

5.6.2 Network Layer

- The network layer is responsible for the delivery of packets from the source to destination.
- Network layer uses IP address to choose one host among millions of hosts. In network layer, datagram needs a destination IP address for delivery and a source IP address for a destination reply.

a. IPv4

- IP is used for communicating all Internet enabled devices. The transport layer is responsible for delivery of message from one process to another.
- The network does the host to destination delivery of individual packets considering it as independent packet. But transport layer ensures that the whole message arrives intact and in order with error control and process control.
- An IP address is a numeric identifier assigned to each machine on an IP network. IP address is a software address, not a hardware address, which is hard-coded in the machine or NIC.
- An IP address is made up of 32 bits of information. These bits are divided into four parts containing 8 bit each.
- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- Packets in the IPv4 layer are called datagrams. A datagram is a variable length.

b. IPv6

- IPv6 addresses are 128 bits in length. Addresses are assigned to individual interface on nodes, not to the node themselves.
- A single interface may have multiple unique unicast addresses. The first field of any IPv6 address is the variable length format prefix, which identifies various categories of addresses.

c. 6LoWPAN

- IPv6 over Low power Wireless Personal Area Network enables IPv6 in low-power and lossy wireless networks such as WSNs.
- 6LoWPAN defines header compression mechanisms.

5.6.3 Transport Layer

- A transport layer protocol provides for logical communication between application processes running on different hosts.
- The transport layer is responsible for delivery of message from one process to another. The network does the host to destination delivery of individual packets considering it as independent packet.
- But transport layer ensures that the whole message arrives intact and in order with error control and process control.
- A transport protocol can offer reliable data transfer service to an application even when the underlying network protocol is unreliable, even when the network protocol loses, garbles and duplicate packets.

a. TCP (Transmission Control Protocol)

- TCP is the connection-oriented protocol whereas UDP is connectionless protocol. Both are internet protocols used in the transport layer.
- TCP provides a connection-oriented, reliable, byte stream service. The term connection oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.
- TCP does not support multicasting and broadcasting. The application data is broken into what TCP considers the best sized chunks to send. The unit of information passed by TCP to IP is called a segment.
- When TCP sends a segment it maintains a timer, waiting for the other end to acknowledge reception of segment. If an acknowledgement isn't received in time, the segment is retransmitted.

b. (UDP) User Datagram Protocol

- UDP is a simple, datagram-oriented, transport layer protocol. This protocol is used in place of TCP.
- UDP is connectionless protocol provides no reliability or flow control mechanisms. It also has no error recovery procedures.
- UDP makes use of the port concept to direct the datagrams to the proper upper-layer applications. UDP serves as a simple application interface to the IP.
- UDP uses port numbers as the addressing mechanism in the transport layer.

5.6.4 Application Layer

- Application layer is responsible for accessing the network by user. It provides user interfaces and other supporting services such as e-mail, remote file access, file transfer, sharing database, message handling (X.400), directory services (X.500).

a. HTTP (HyperText Transport Protocol)

- HTTP is an application protocol. HTTP is used to retrieve Web pages from remote servers.
- HTTP uses the services of TCP. HTTP is a stateless protocol. The client initializes the transaction by sending a request message. The server replies by sending a response.
- HTTP includes commands such as GET, PUT, POST, HEAD, DELETE, MOVE, LINK and UNLINK.
- HTTP messages are two types: Request and Response
- URL is a standard for specifying any kind of information on the internet. HTTP uses URL.

b. CoAP - Constrained Application Protocol

- CoAP is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks.
- CoAP is designed for simplicity, low overhead and multicast support in resource-constrained environments.
- CoAP is a web protocol that runs over the UDP for IoT. Datagram Transport Layer Security (DTLS) is used to protect CoAP transmission.
- The protocol is designed for M2M applications such as smart energy and building automation.

- CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types.
- CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments.
- The key features of CoAP are :
  1. CoAP is a RESTful protocol.
  2. Four methods similar to HTTP : Get, Put, Post and Delete.
  3. Four different message types : Confirmable, Non-Confirmable, Acknowledgment and Reset (Nack).
  4. It support synchronous message exchange.
  5. Easy to proxy to and from HTTP.
  6. Constrained web protocol fulfilling M2M requirements.
  7. UDP binding with optional reliability supporting unicast and multicast requests. Confirmable and Acknowledgment / Reset messages to provide optional reliability when required. Low header overhead and reduced parsing complexity.
  8. Simple proxy and caching capabilities.
- Fig. 5.6.2 shows CoAP protocol stack.
- CoAP is based on the exchange of compact messages that, by default, are transmitted over UDP. Message of CoAP uses simple binary format.
- Message Layer supports 4 types message : CON (confirmable), NON (Non-confirmable), ACK (Acknowledgment), RST (Reset).
- Reliable message transport : Keep retransmission until get ACK with the same message ID. Using default time out and decreasing counting time exponentially when transmitting CON. If recipient fail to process message, it responses by replacing ACK with RST.

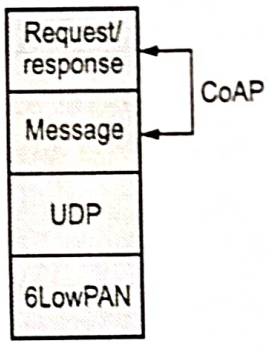


Fig. 5.6.2 CoAP protocol stack

- Unreliable message transport : Transporting with NON types message. It doesn't need to be ACKed, but has to contain message ID for supervising in case of retransmission. If recipient fail to process message, server replies RST.

- Piggy-backed : Client sends request using CON type or NON type message and receives response ACK with confirmable message immediately. For successful response, ACT contain response message (identify by using token), for failure response, ACT contain failure response code.
- Separate response : If server receive a CON type message but not able to response this request, it will send a new CON to client and client reply a confirmable message with acknowledgment. ACT is just to confirm CON message, no matter CON message carry request or response.

Advantages :

- It runs over UDP and avoids overhead of TCP.
- It is easy to do HTTP - CoAP translation.
- It is a lightweight application layer protocol designed for constrained devices and constrained networks.

Disadvantages :

- Constraints associated with DTLS.
- No standardized framework for authorization and access control for CoAP exists as of now.
- No explicit support for real-time IoT application at present.

c. Websocket

- WebSocket is a communications protocol, providing full-duplex communication channels over a single TCP connection. The WebSockets protocol does not run over HTTP, instead it is a separate implementation on top of TCP.
- The WebSocket protocol starts by a handshake in order to start the communication and exchange messages formatted as frames.
- After connection is established, messages can be transmitted, either client or server initiated. This means that you can make a dynamic web page where changes occur in real time.
- In that way Websockest communication presents a suitable protocol for IoT world where changes are usually asynchronously occurring and number of clients can be very large.

d. MQTT (Message Queue Telemetry Transport)

- MQTT is Open Connectivity for Mobile, M2M and IoT. MQTT is designed for high latency, low-bandwidth or unreliable networks. The design principle minimizes the network bandwidth and device resource requirements .

- MQTT is a lightweight broker-based publish/subscribe messaging protocol designed to be open, simple, lightweight and easy to implement.
- The MQTT protocol works by exchanging a series of MQTT control packets in a defined way. Each control packet has a specific purpose and every bit in the packet is carefully crafted to reduce the data transmitted over the network.
- A MQTT topology has a MQTT server and a MQTT client. MQTT control packet headers are kept as small as possible.
- Having a small header overhead makes this protocol appropriate for IoT by lowering the amount of data transmitted over constrained networks.
- MQTT is the protocol built for M2M and IoT which is used to provide new and revolutionary performance.

MQIT characteristics :

1. Lightweight message queueing and transport protocol.
2. Asynchronous communication model with message (events).
3. Low overhead (2 bytes header) for low network bandwidth applications.
4. Publish / Subscribe (PubSub) model.
5. Decoupling of data producer (publisher) and data consumer (subscriber) through topics (message queues).
6. Simple protocol, aimed at low complexity, low power and low footprint implementations.
7. Runs on connection-oriented transport (TCP).
8. MQIT caters for (wireless) network disruptions.

- Fig. 5.6.3 shows MQIT publish / subscribe framework. (See Fig. 5.6.3 on next page.)
- The MQIT protocol works by exchanging a series of MQIT controls packets in a defined way. Each control packet has a specific purpose and every bit in the packet is carefully crafted to reduce the data transmitted over the network.
- A producer publishes a message (publication) on a topic (subject). A consumer subscribes (makes a subscription) for messages on a topic (subject).
- A message server (called BROKER) matches publications to subscriptions.
- If none of them match the message is discarded after modifying the topic. If one or more matches the message is delivered to each matching consumer after modifying the topic.

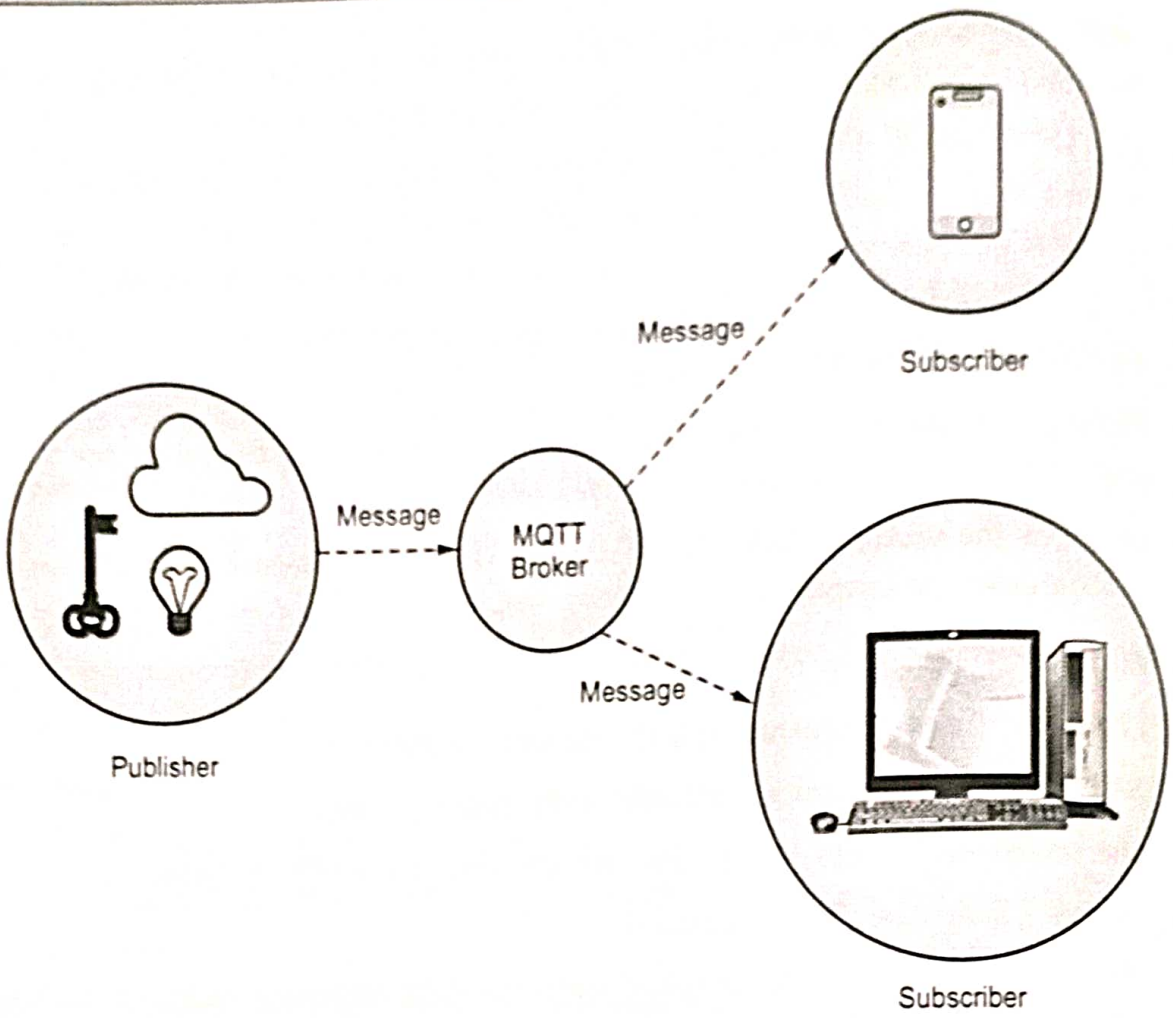


Fig. 5.6.3 MQTT publish/subscribe framework

- Publish / Subscribe has three important characteristics :
  1. It decouples message senders and receivers, allowing for more flexible applications.
  2. It can take a single message and distribute it to many consumers.
  3. This collection of consumers can change over time and very based on the nature of the message.
- The MQIT messages are delivered asynchronously ("push") through publish subscribe architecture.
- The MQIT protocol works by exchanging a series of MQIT control packets in a defined way.
- Each control packet has a specific purpose and every bit in the packet is carefully crafted to reduce the data transmitted over the network.
- A MQIT topology has a MQIT server and a MQIT client. MQIT client and server communicate through different control packets.

- MQIT control packet headers are kept as small as possible. Each MQIT control packet consist of three parts, a fixed header, variable header and payload.
- Each MQIT control packet has a 2 byte fixed header. Not all the control packet have the variable headers and payload.
- A variable header contains the packet identifier if used by the control packet. A payload up to 256 MB could be attached in the packets.
- Having a small header overhead makes this protocol appropriate for IoT by lowering the amount of data transmitted over constrained network.

e. XMPP (Extensible Messaging Presence Protocol) :

- The XMPP is targeted at delivering instant messages and presence information. It is an open and XML -based protocol.
- Instant messaging (IM) is a service, where communicating parties typically end users send messages in one- to-one or one -to -many fashion in near real - time.
- An open technology for real-time communication, which powers a wide range of applications including instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data.
- XMPP support server-to-server communication and client-to-server communication.
- XMPP is based on a decentralized client-server architecture. In this architecture, clients don't communicate directly with each other; instead, there's a decentralized server acting as the intermediary between them.
- XMPP allocates an XMPP address to every client on the XMPP network. This address works just like a standard email address with an IP address/domain name, an optional node and a username for the resident server.
- Fig. 5.6.4 shows simple architecture of XMPP.

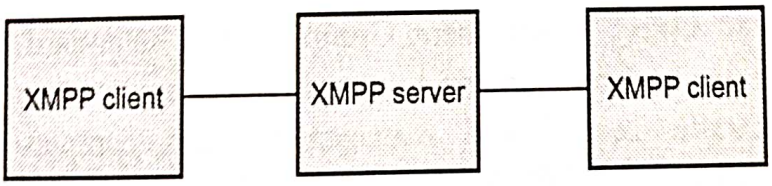


Fig. 5.6.4 XMPP simple architecture

- In a simple XMPP architecture consisting of a server and two clients, a client with a unique name communicates through an associated XMPP server with another client using a unique name.

- Each client on the XMPP network implements the client form of the protocol with the XMPP server providing routing capability. The architecture may include XMPP gateways which are often used to translate between foreign messaging domains and IM protocols.
- The XMPP gateways permit the termination of a given client-to-server session as well as the initiation of a new client-to-server session to the target endpoint protocol, along with the necessary protocol translation.
- XMPP uses the Transmission Control Protocols as its original and "native" transport protocol for web applications and firewalls.
- Advantages of XMPP protocol
  1. Supports HTTP transport protocol.
  2. It offers persistent connection.
  3. It is decentralized in nature as no central XMPP servers are needed.
  4. It allows servers with different architectures to communicate.
  5. Utilize a decentralized client-server architecture.
  6. It users TLS and SASL to provide secured end to end connection.
- Disadvantages of XMPP protocol
  1. It does not have QoS mechanism as used by MQTT protocol.
  2. Streaming XML has overhead due to text-based communication compare to binary based communication.
  3. XML content transports asynchronously.
  4. Server may overload with presence and instant messaging.

f. DDS (Data Distribution Service)

- The first open international middleware standard directly addressing publish-subscribe communications for real-time and embedded systems.
- The DDS is an Object Management Group (OMG) standard for Pub/Sub that addresses the needs of mission and business critical applications, such as, financial trading, air traffic control and management, and complex supervisory and telemetry systems.
- DDS provides a shared "global data space" where any application can publish the data it has and subscribe to the data it needs.
- DDS is highly configurable by means of QoS settings. Heterogeneous systems can be easily accommodated.

g. AMQP (Advanced Message Queuing Protocol)

- A protocol to communicate between clients and messaging middleware servers (brokers). The Broker is the AMQP Server.
- AMQP supports both publish-subscribe model and point-to-point communication, routing and queuing.
- AMQP divides the brokering task between exchanges and message queues, where the first is a router that accepts incoming messages and decides which queues to route the messages to, and the message queue stores messages and sends them to message consumers.
- AMPQP supports username and password authentication as well as SASL authorization. It also supports TLS encryption. Fig. 5.6.5 shows AMQP architecture.

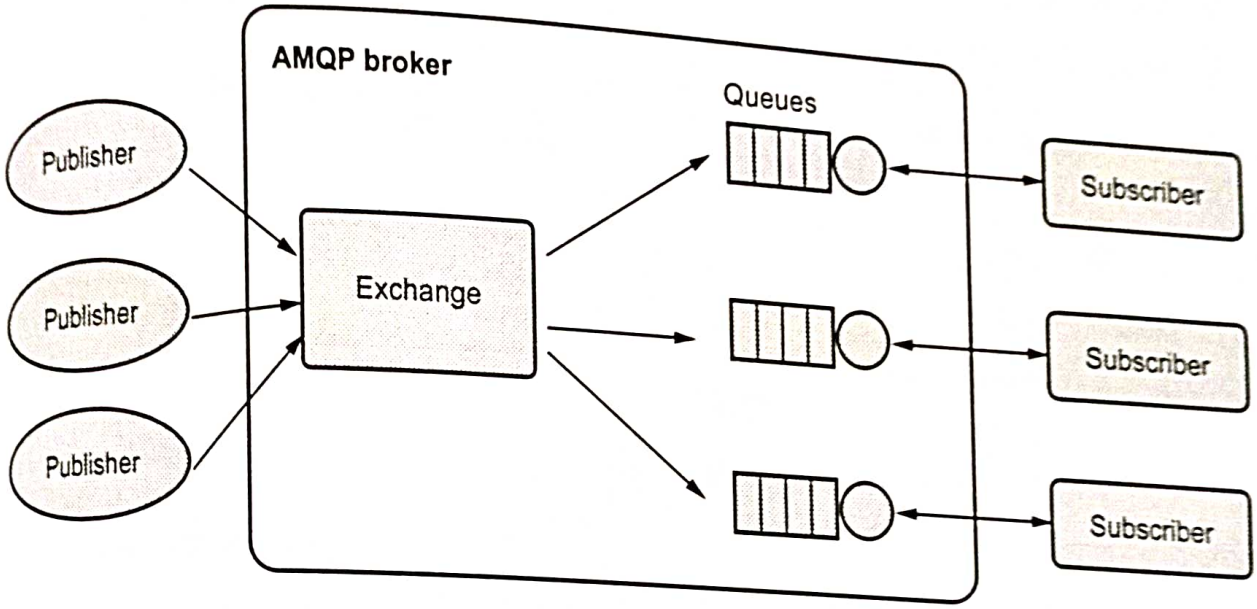


Fig. 5.6.5 AMQP architecture

- Exchange : Receives messages from publisher primarily based programs and routes them to message queues.
- Message queue : Stores messages until they may thoroughly process via the eating client software.
- Binding : States the connection between the message queue and the change.

5.6.5 Difference Between CoAP and MQTT

CoAP	MQTT
CoAP uses UDP protocol.	MQTT uses TCP protocol.
It uses Request/Response messaging.	It uses publish/subscribe messaging.
Communication model is one-to-one.	Communication model is many-to-many.
Advantages : • Lightweight and fast • Low overhead • Support for multicasting	Advantages : • Simple management • Scalability • Robust communication
Weakness : Not as reliable as TCP based MQTT	Weakness : Higher overhead, no multicasting support
Security type is DTLS.	Security type is SSL/TLS.
Effectiveness in LLN is excellent.	Effectiveness in LLN is low.