MODULE 5

Module 5 (Embedded System Industry – Case Studies and Applications)

Design Case Studies – Battery Operated Smart Card Reader, Automated Meter Reading System, Smart Watch.

Automotive and Aerospace Systems – Networked Control Systems in Cars and Airplanes, Vehicular Networks – CAN bus, Time-triggered Architecture, FlexRay and LIN.

Internet of Things Systems – IoT System Architectures - Use Cases (Smart Appliance, Monitoring and Control Systems). Networks for IoT – Networking concepts, Bluetooth, Bluetooth Low Energy, 802.15.4, ZigBee and WiFi. Databases and Timewheels. Smart Home Example.

Q.1.: Illustrate and explain Embedded system application in a battery operated smart card reader.

BATTERY OPERATED SMART CARD READER

- Smartcard is a credit card sized plastic card containing a memory or a 'CPU and memory'.
- Smartcard follows a specific command sequence for data read/write operations.
- The data read write operation is controlled by a Smartcard Reader/Writer IC.
- Smartcards are classified as 'Contact type' and 'Contactless'.
    - Contact type smartcard requires physical contact between the reader and the smartcard and is exactly the same as phone's SIM card.
    - Contactless smartcard doesn't require a physical contact between the reader and the smartcard for data communication.
- The data communication for a contactless smartcard happens over air interface and it uses radio frequency waves(13.56 MHz) for data transmission.
- A rechargeable Li-Io battery is used as the power source for the handheld.
- The host processor can be an 8 or 16bit microcontroller(8051).
- The device power ON is controlled through a push button switch.
- A single chip contactless smartcard read/write IC is used for data read write operation with the smartcard.
- The smartcard reader IC is interfaced to the host processor and the data communication will be under the control of the host processor.
- The smartcard read/write IC contains CPU , read/write memory, analog circuits for data modulation and demodulation, transceiver unit for RF data transmission and reception, and antenna driver circuitry.
- For the handheld reader to communicate with a desktop machine, a communication channel using either USB or RS-232C is implemented in the reader.
- The I/O unit of the system includes a matrix keyboard for user inputs and a graphical/alpha-numeric LCD for visual indications.
- LEDs are used for various status indications like 'Charging', 'Battery Low', 'Busy/Error', etc.
- The Oscillator and Reset circuitry generates the necessary clock and reset signals for the proper operation of the host processor and smartcard read/write IC.
- The watchdog timer unit provides the necessary reset to the system in case of system misbehaviour and is connected to one of the interrupt lines of the processor.
- If the on-chip program and data memory are not sufficient for the application, external data memory and program memory chips can be used in the design.

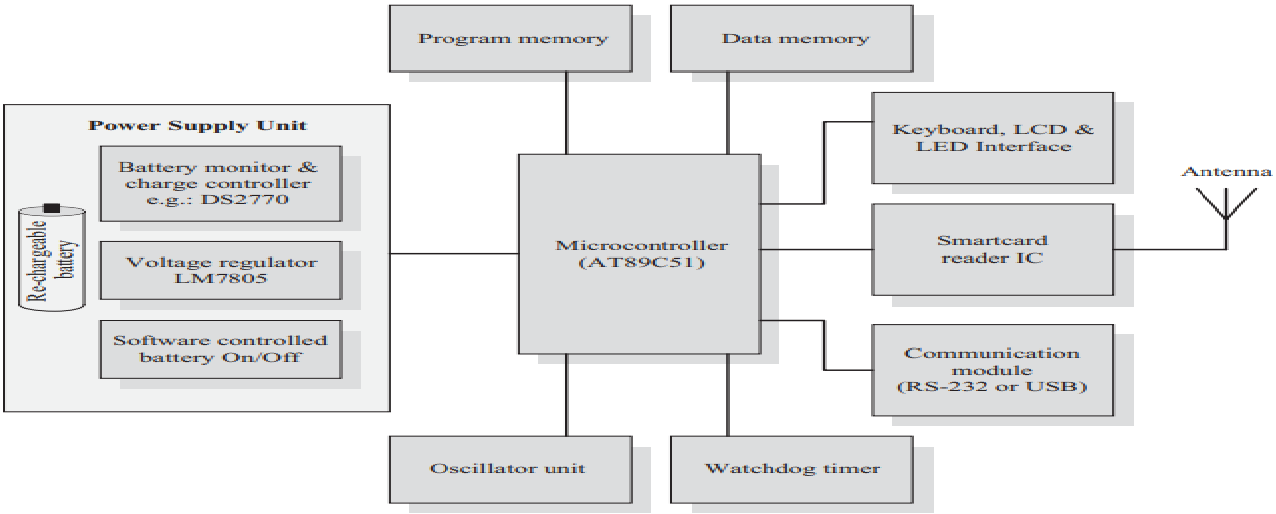


Fig. A2.12 Block Diagram of a Handheld Contactless Smart Card Reader

The firmware requirements for building the handheld smartcard reader can be divided into the following tasks.

1. Startup task
2. Battery monitoring and Charge controlling task
3. Card read/write operation task
4. Communication Task
5. Keyboard scanning task
6. LCD update task
7. Watchdog timer expire event

- **Startup task** implements the necessary startup operations like setting up the interrupts, configuring the ports of the host processor, initialising the LCD, initialising the battery monitor and charge control IC, initialising the smart card reader IC, etc.
- **Battery monitoring and charge controlling task** reads the various registers (Voltage, capacity registers, etc.) of the battery monitor IC, checks the presence of a charger and initiates a charge command, terminates the charging when the battery is full, produces warning signal when the battery voltage is below a threshold value and switch off the unit if the battery voltage falls below the critical threshold value.
- **Card read/write operation task** is responsible for implementing the communication sequence for data read/write operation with the card.
  The smartcard read/write operation follows a specific sequence of operation.
  A typical read write operation follows the sequence:

1. Reader initiates a 'Request' command for checking the presence of cards in the vicinity of the reader. If a card is present in the field it responds to the reader with Answer To Request (ATR).

2. Upon receiving the ATR, the reader sends a command to capture the serial number of all cards present in the field

3. Reader selects the serial number of a card from the list of serial numbers received and sends a command to select the specified card. Now the communication channel is established exclusively between the reader and a card.

4. The Reader authenticates the card with an encrypted key. If the key matches with the key stored in the card, the authentication succeeds.

- **Keyboard scanning task** scans the keyboard and identifies a key press and performs the operation corresponding to the key press.

- **LCD update task** updates the LCD with new data. This task can be invoked by other tasks like keyboard scanning task, battery monitoring task, card read/write task and communication task for displaying the various information.
- **Communication task** handles reader communication with the host PC. The communication interface can be either USB or RS-232.
- **Watchdog timer** expiration ISR handles the actions corresponding to a watchdog timer event.

Q.2.: Illustrate and explain embedded system application in automatic meter reading system.

AUTOMATED METER READING SYSTEM(AMR)

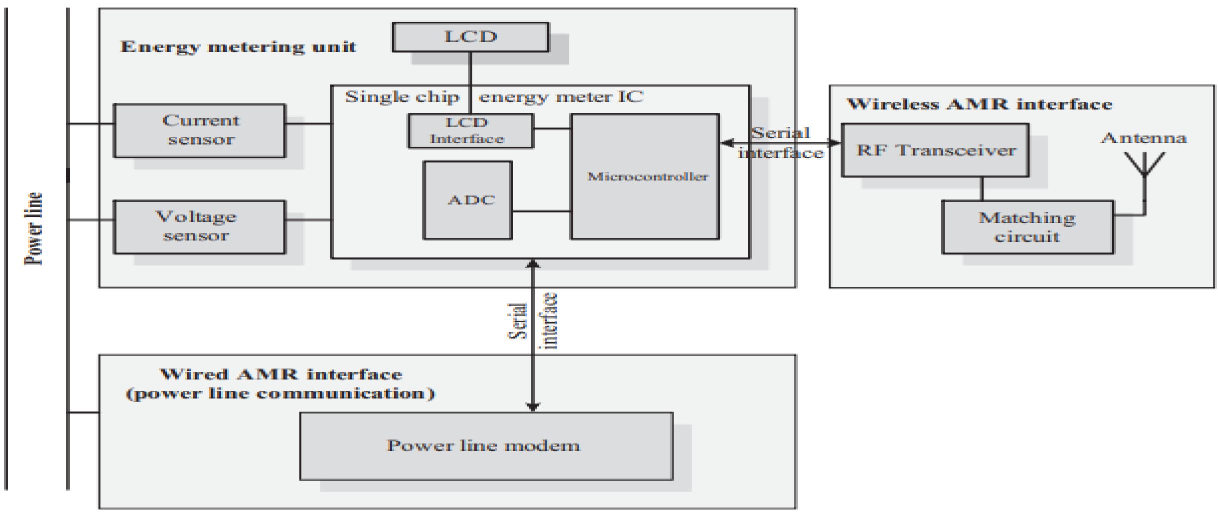


Fig. A2.13 Block Diagram of an AMR enabled Integrated Electronic Energy Meter

- AMR systems transfer the meter reading data automatically to a central station for billing and usage monitoring purposes over a wireless communication channel or a wired communication medium.
- The meter reading official carries a handheld for recording the energy meter reading through a Wireless AMR interface.
-
- Contains an AMR data transmission unit, which is interfaced with the utility meter and a remote AMR data receiver unit which collects the data for billing and usage monitoring purpose.
- The energy metering unit(single chip) records the electricity consumption.
- The electronic energy meter records the current consumption by integrating the instantaneous power, measured using a current sensor circuit.
- The signal conditioned current value is fed to the energy metering IC.
- The ADC present in the energy metering IC digitises the instantaneous current value.
- The voltage sensor circuit senses the instantaneous voltage and it is fed to the energy metering IC for digitisation.
- The microcontroller present in the energy metering IC computes the instantaneous power, the average power consumption and stores it in the EEPROM memory.
- The specific energy meter whose reading is to be recorded can be selected by sending the unique meter identification number (Meter ID) of the meter and then initiating an automated meter reading operation.
- The antenna is a metallic coil for transmitting and receiving RF modulated data.

- The interface between the energy metering unit and the RF module is implemented through serial interfaces like SPI, I2C, etc.
- The firmware running in the microcontroller of the single chip energy meter IC controls the communication with the RF module.
- The Power Line Carrier Communication (PLCC) based AMR interface makes use of a power line modem for interfacing the power lines with the energy metering unit for data communication.
- The PLC modem provides bi-directional half-duplex data communication over the mains.
- The PLC modem can be interfaced to the microcontroller of the energy metering unit through serial interfaces like UART, SPI, etc.
- ZigBee, Wi-Fi, etc. are other wireless interface options for AMR interface.
- The firmware requirements for building the AMR enabled energy meter can be divided into the following tasks:
    - ✓ *Startup task*
    - ✓ *Energy consumption recording task*
    - ✓ *Automatic meter data transfer task*
    - ✓ *LCD update task*

- **Startup task** deals with the initialisation of various port pins, interrupt confi guration, stack pointer setting, etc. for the microcontroller, initialisation of the RF interface for the communication parameter, and initialisation of the LCD.
- **Energy consumption task** records the energy consumption. The energy metering SoC may contain dedicated hardware units for calculating the energy consumption based on the instantaneous voltage and current and the meter reading will be available in some dedicated registers of the SoC.
- **Automatic meter data** transfer task can be implemented as a periodic task or a command driven operation in which the meter reading is sent upon receiving a command from the host system.
- **LCD update task** updates the LCD when a change in display parameter (like instantaneous current and voltage, energy consumption, etc.) occurs.

Q.3.: Illustrate and explain embedded system application in a battery operated smart watch.

SMART WATCH

- Smartwatches are wearable computing devices with many features such as fitness tracking, mobile notifications, and voice commands.
- The embedded system in a smartwatch is responsible for running the device's software, processing user input, and controlling the various sensors and peripherals that the watch comes equipped with. These systems are usually designed to be low-power and compact, as space and battery life are important considerations for a wearable device.

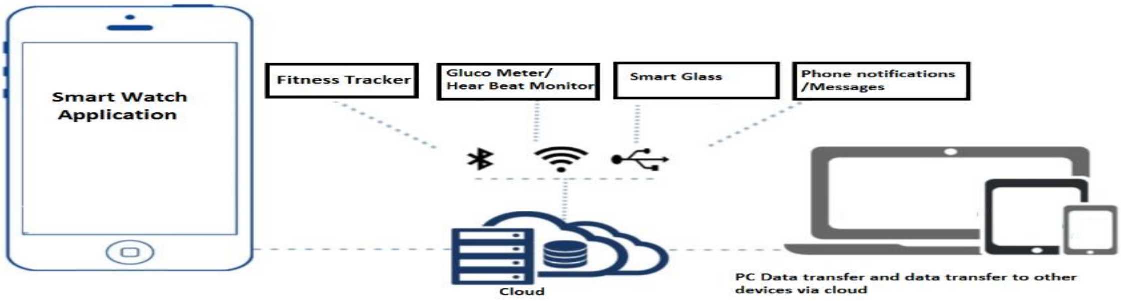


Figure 4: Concept of smartwatch design

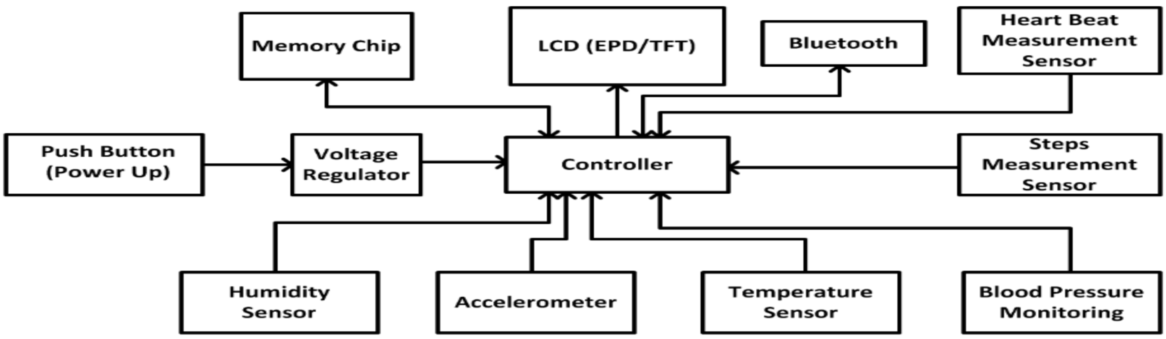


Figure 1: Wearable block diagram

KEY COMPONENTS

- **Processor**: The processor is the central component of the embedded system, responsible for running the device's software and processing user input. The processor is the heart of the smartwatch's embedded system, responsible for executing all of the device's instructions. Smartwatches typically use low-power processors, such as ARM Cortex-M, which are optimized for battery life .
- **Memory:** Smartwatches have limited memory, as the device needs to be compact and lightweight. The embedded system typically uses flash memory for storing the device's firmware and application code, as well as RAM for storing temporary data during the device's operation. Flash memory can be used for storing firmware and SRAM can be used for storing
- **Sensors:** Smartwatches come equipped with a range of sensors, including accelerometers, gyroscopes, heart rate monitors, and GPS sensors. The embedded system must be able to read data from these sensors and use it to provide the user with useful information
- **Communication**: Smartwatches are designed to communicate with other devices, such as smartphones, via Bluetooth or Wi-Fi. The embedded system must be able to manage these connections and transfer data between devices efficiently.
- **User Interface**: The embedded system provides the user interface for the smartwatch, including the display, touch screen, and buttons. The system must be able to process user input and display information on the device's screen.
  OLED display or Touch screen can be used
  - OLED displays are made up of organic materials that emit light when an electric current is applied, making them self-emitting.
  - OLED displays offer several advantages over other display technologies such as LCDs (Liquid Crystal Displays):
    - Better Image Quality: OLED displays produce deeper blacks, higher contrast ratios, and better color accuracy than LCDs. OLED displays also have wider viewing angles than LCDs.

- Thin and Flexible: OLED displays are very thin and flexible, making them suitable for curved screens, wearable devices, and other applications where space is limited.
- Energy Efficient: OLED displays consume less power than LCDs because they only light up the pixels that are needed, whereas LCDs require a backlight to illuminate the entire screen.
- Faster Refresh Rates: OLED displays can achieve faster refresh rates than LCDs, resulting in smoother animations and better video playback.

- **Power Management**:. The system must be optimized to minimize power usage. The battery is typically a lithium-ion polymer (LiPo) battery, which is small and lightweight. A charging circuit is used to recharge the battery when it runs low on power.
- **Operating system** is an embedded OS, such as a real-time operating system (RTOS), designed to handle the watch's various tasks and ensure that it operates efficiently and reliably.

Q.4.: Explain networked control systems in cars
OR
Explain networked control system in automotives

- Networked control systems are computer networks with processors and I/O devices that perform control functions for real time responsiveness.
- Complex machines require network-based control for fast reaction.
- First, a network allows more computing power to be applied to the system than with a single CPU.
- Second, many control applications require the controller to be physically near the controlled device.

CAR SUBSYSTEM INTERACTIONS
- The term electronic control unit (ECU) is widely used in automotive design.
- Modern automobiles may contain over 100 processors that execute 100 million lines of code.

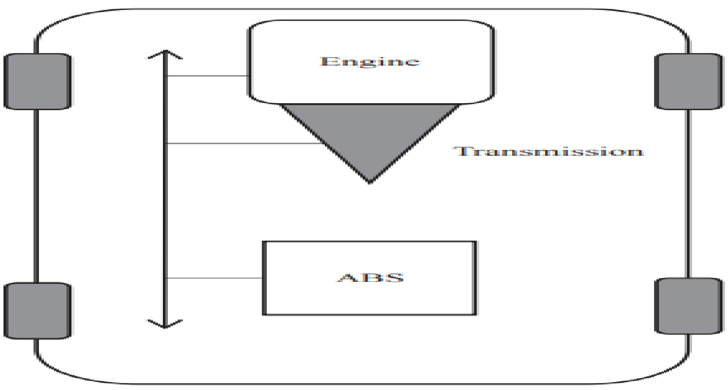


FIGURE 9.1
Major elements of an automobile network.

- There are three major subsystems in the car: the **engine**, the **transmission**, and **the antilock braking system (ABS)**.
- Each of these is a mechanical system that is controlled by a processor.
- Roles of the mechanical systems
  The **engine** provides power to drive the wheels.
  The **transmission** mechanically transforms the engine's rotational energy for wheel.

The **ABS** controls how the brakes are applied to each of the four wheels.

- Roles of the associated processors:

  The **engine controller** accepts commands from the driver via the gas pedal and , it determines the spark and fuel timing on every engine cycle.

  The **transmission controller** determines when to change gears.

  The ABS takes braking commands from the driver via the brake pedal. It also takes measurements from the wheels about their rotating speed.

Q.5.: Explain networked control system in AVIONICS

OR

Explain networked control system in aviation.

- Networked control systems are computer networks with processors and I/O devices that perform control functions for real time responsiveness.
- Complex machines require network-based control for fast reaction.
- Aircraft electronics are known as avionics.
- The most fundamental difference between avionics and automotive electronics is **certification.**
- Anything that is permanently attached to the aircraft must be certified.
- The certification process is a prime reason why avionics architectures are more conservative than automotive electronics systems.
- A more sophisticated system is bus based.
- The Boeing 777 avionics , for example, is built from a series of racks.
- Each rack is a set of **core processor modules (CPMs**), I/O modules, and power supplies.
- The CPMs may implement one or more functions.
- A bus known as SAFE bus connects the modules.
- Cabinets are connected together using serial bus known as ARINC 629.
- A more distributed approach to avionics is the **federated network.**
- In this architecture, a function or several functions have their own network. The networks share data as necessary for the interaction of these functions.
- A federated architecture is designed so that a failure in one network will not interfere with the operation of the other networks.

Q.6.: Explain in detail about various vehicular networks

- Vehicular networks often have relatively low bandwidth .
- However, the computations are organized so that each processor has to send only a relatively small amount of data to other processors to do the system's work.
- CAN bus, which is widely used in cars and aeroplanes

1.	**CAN bus**	**Refer Q:7**
2.	**Time-triggered Architecture**	**Refer Q:8**
3.	**FlexRay**	**Refer Q:9**
4.	**LIN**	**Refer Q:10**

Q.7. : Explain any 1 vehicular network

OR

Explain CAN bus

- CAN bus, which is widely used in cars and aeroplanes.

- A CAN network consists of a set of electronic control units (ECU)connected by the CAN bus
- ECUs pass messages to each other using the CAN protocol.
- CAN bus is used for safety-critical operations such as antilock braking.
- CAN is well suited to the strict requirements of automotive electronics: reliability, low power consumption, low weight, and low cost.
- CAN uses bit-serial communication and runs at rates of 1 Mb/s over a twisted pair connection of 40 m.
- Broadcast type
- Serial half duplex asynchronous communication
- Use twisted pair shielded cable to avoid data loss
- The bus protocol supports multiple masters on the bus.
- Each node in the CAN bus has its own electrical drivers and receivers that connect the node to the bus in wired-AND fashion.

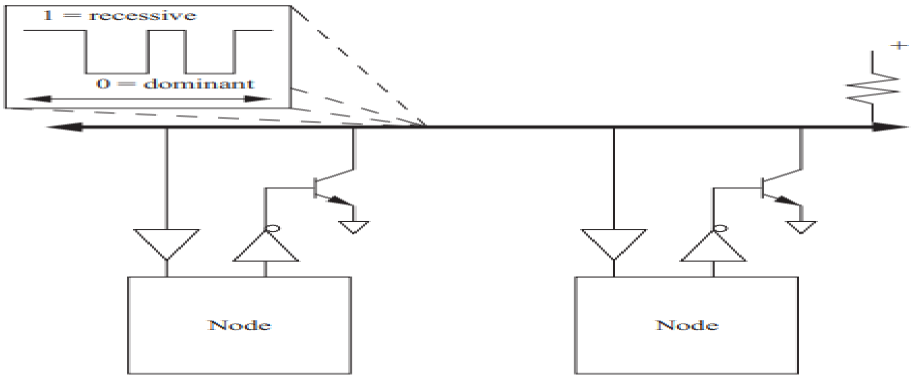


FIGURE 9.2
Physical and electrical organization of a CAN bus.

- In CAN terminology, a **logical 1** on the bus is called **recessive** and a ***logical 0*** is ***dominant.***
- Logical high and low is achieved by applying differential voltage across the lines.
- When all nodes are transmitting 1s, the bus is said to be in the recessive state; when a node transmits a 0, the bus is in the dominant state.
- Data are sent on the network in packets known as data frames.
- CAN is a synchronous bus-all transmitters must send at the same time for bus arbitration to work.
- Nodes synchronize themselves to the bus by listening to the bit transitions on the bus.

Data frame

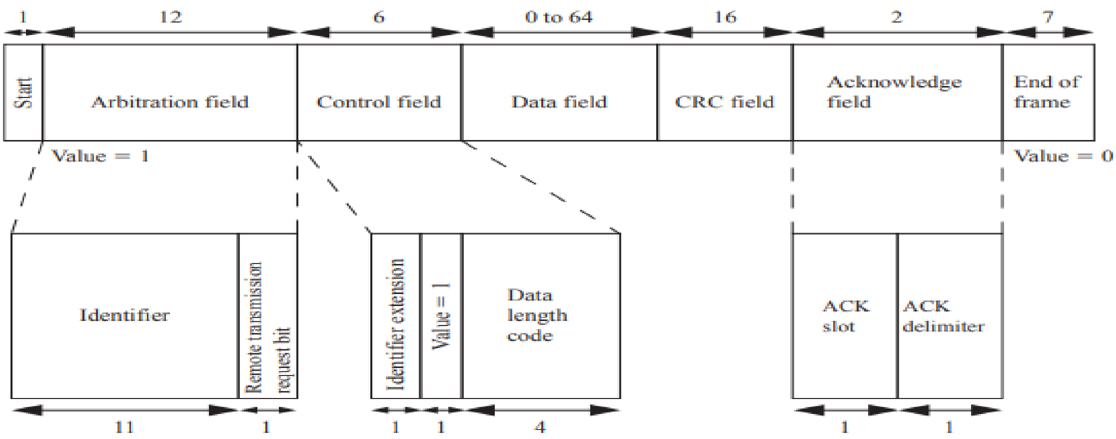


FIGURE 9.3

The CAN data frame format.

- A data frame starts with a 1 and ends with a string of seven zeroes.
- The first field in the packet contains the packet's destination address and is known as the arbitration field.
- The destination identifier is 11 bits long.
- The trailing remote transmission request (RTR) bit is set to 0 if the data frame is used to request data from the device specified by the identifier.
- When RTR is 1, the packet is used to write data to the destination identifier.
- The control field provides an identifier extension and a 4-bit length for the data field with a 1 in between.
- The data field is from 0 to 64 bytes, depending on the value given in the control field.
- A cyclic redundancy check (CRC) is sent after the data field for error detection.
- The acknowledge field is used to let the identifier signal whether the frame was correctly received:
- If the receiver detected an error, it forces the value to a dominant (0) value.
- If the sender sees a 0 on the bus in the ACK slot, it knows that it must retransmit.
- Control of the CAN bus is arbitrated using a technique known as Carrier Sense Multiple Access with Arbitration on Message Priority (CSMA/AMP)

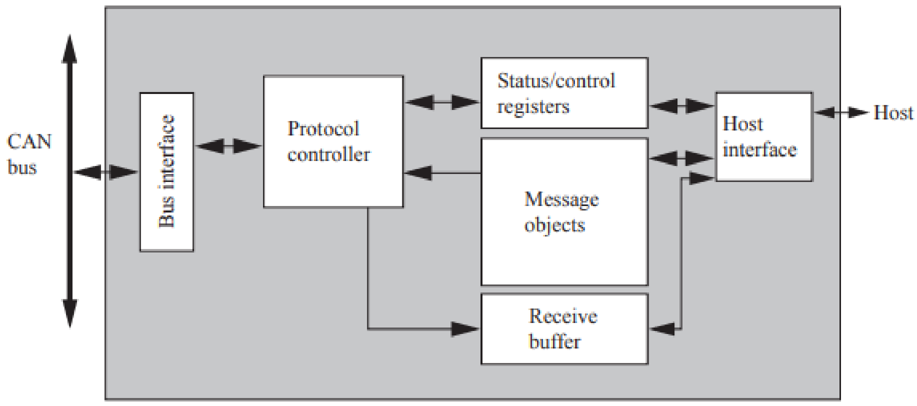


FIGURE 9.4

Architecture of a CAN controller.

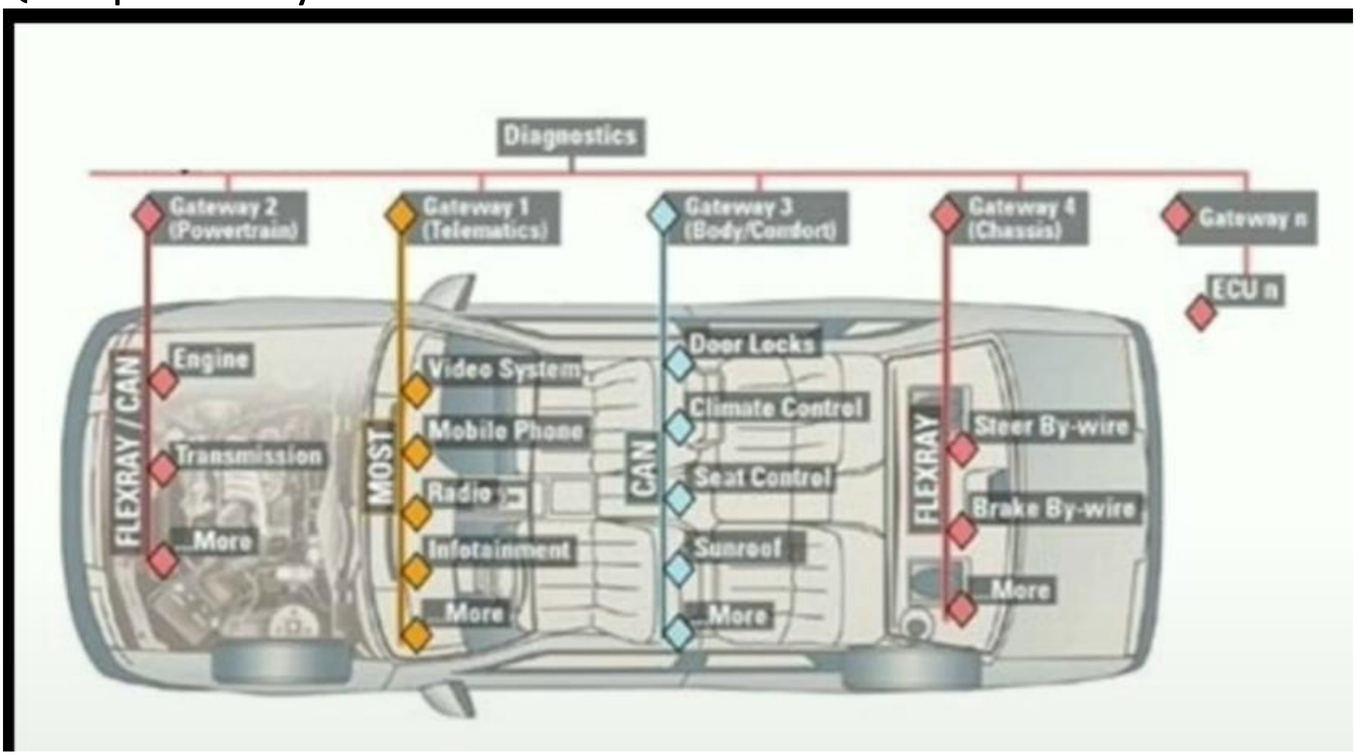
- CAN encourages a data-push programming style.
- Network nodes transmit synchronously, so they all start sending their identifier fields at the same time.

- When a node hears a dominant bit in the identifier when it tries to send a recessive bit, it stops transmitting.
- Each possible data request must have its own identifier.
- An error frame can be generated by any node that detects an error on the bus.
- Upon detecting an error, a node interrupts the current transmission with an error frame, which consists of an error flag field followed by an error delimiter field of 8 recessive bits.
- The error delimiter field allows the bus to return to the quiescent state so that data frame transmission can resume.
- The bus also supports an overload frame, which is a special error frame sent during the interframe quiescent period.
- An overload frame signals that a node is overloaded and will not be able to handle the next message.
- The CRC field can be used to check a message's data field for correctness.
- If a transmitting node does not receive an acknowledgment for a data frame, it should retransmit the data frame until the data are acknowledged. This action corresponds to the data link layer in the OSI model.
- The controller implements the physical and data link layers; because CAN is a bus, it does not need network layer services to establish end-to-end connections.

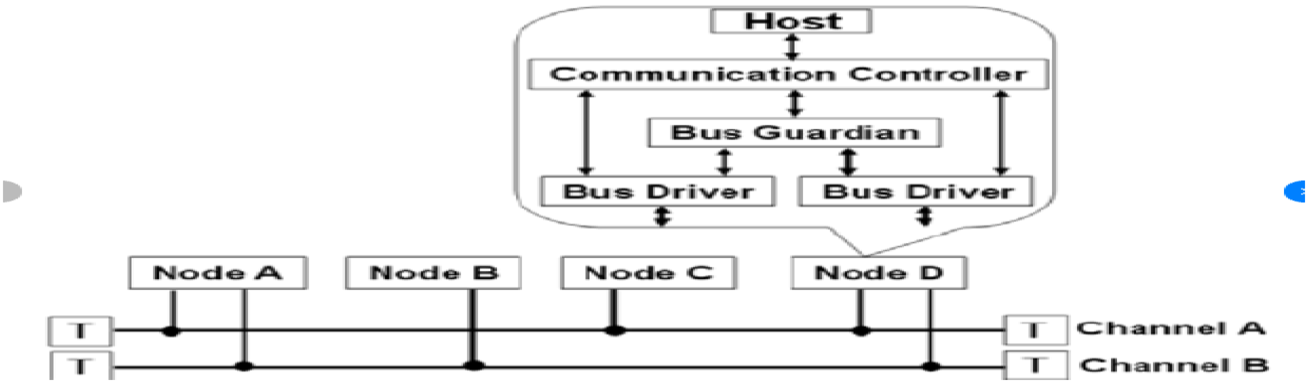
Q.8.:Explain time triggered architecture

- Events on the timetriggered architecture are organized around real time.
- Since devices in the network need time to respond to communication events, time is modeled as a sparse system.
- Intervals of active communication are interspersed with idle periods.
- This model ensures that even if the clock's value varies somewhat from device to device, all the devices on the network will be able to maintain the order of events in the system.

Q.9.: Explain Flex Ray



- Flex Ray is a communication protocol used in automotive networks for high-speed data exchange between electronic control units (ECUs) in a vehicle.
- Flex Ray is designed to handle real-time data communication and is known for its high data transfer rates, low latency, and deterministic communication.
- Flex Ray provides high data ratesdup to 10 Mbits/sdwith deterministic communication.
- FlexRay uses a bus topology, where all ECUs are connected to a single communication bus.
- It supports both time-triggered and event-triggered communication, allowing for efficient and predictable data exchange between ECUs.
- It is also designed to be fault tolerant.
- Flex Ray also includes error detection and correction mechanisms to ensure data integrity and reliability.
- It has become a standard in the development of safety-critical systems in vehicles
- Communications on the bus are designed around a communication cycle.
- The timing of communication for each of these events determined by a schedule set up by the designer.
- Some devices may need only sporadic communication and they can make use of dynamic segment for these events.



FlexRay node architecture and dual bus topology configuration

- Each Flex Ray node consists of a host, communication controller (CC), bus guardian (BG) and bus driver (BD) .
- Host is the user software which controls the communication process.
- CC is an electronic component in a node that is responsible for implementing the protocol aspects of the Flex Ray communications system.
- BG is an electronic component which protects slots against faulty media access.
- BD is consisted of a transmitter and a receiver that connects a communication controller to one communication channel.
- A node can be connected to both channels (e.g., Node A or Node D) or only to a single channel (e.g., Node B or Node C).
- Flex Ray supports simple multi-drop passive connections as well as active star connections for more complex networks.

  Multi-drop Bus
- Flex Ray is commonly used in a simple multi-drop bus topology that features a single network cable run that connects multiple ECUs together.

- ***Star Network***

The FlexRay standard supports "Star" configurations which consist of individual links that connect to a central active node. This node is functionally similar to a hub. The active star configuration makes it possible to run Flex Ray networks over longer distances. If one of the branches of the star is cut or shorted, the other legs continuing functioning.

- There are four main parts to a communication cycle:

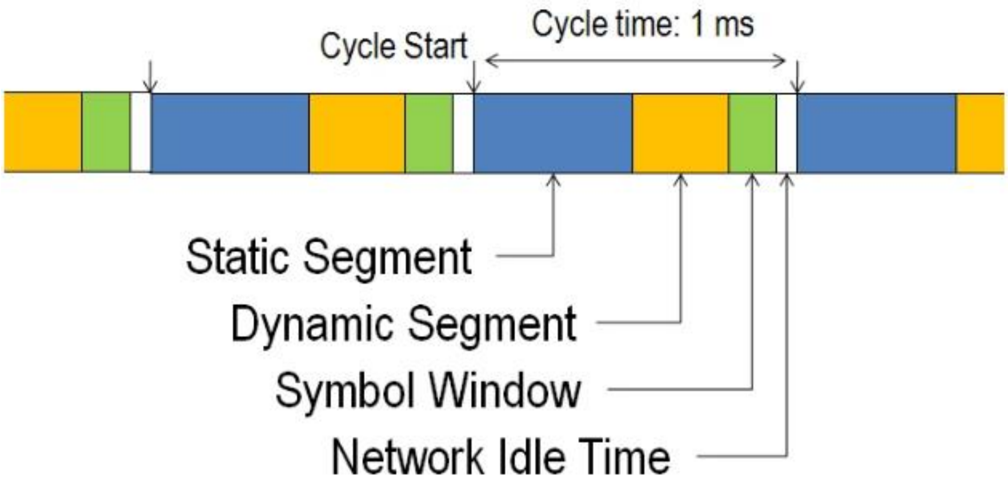
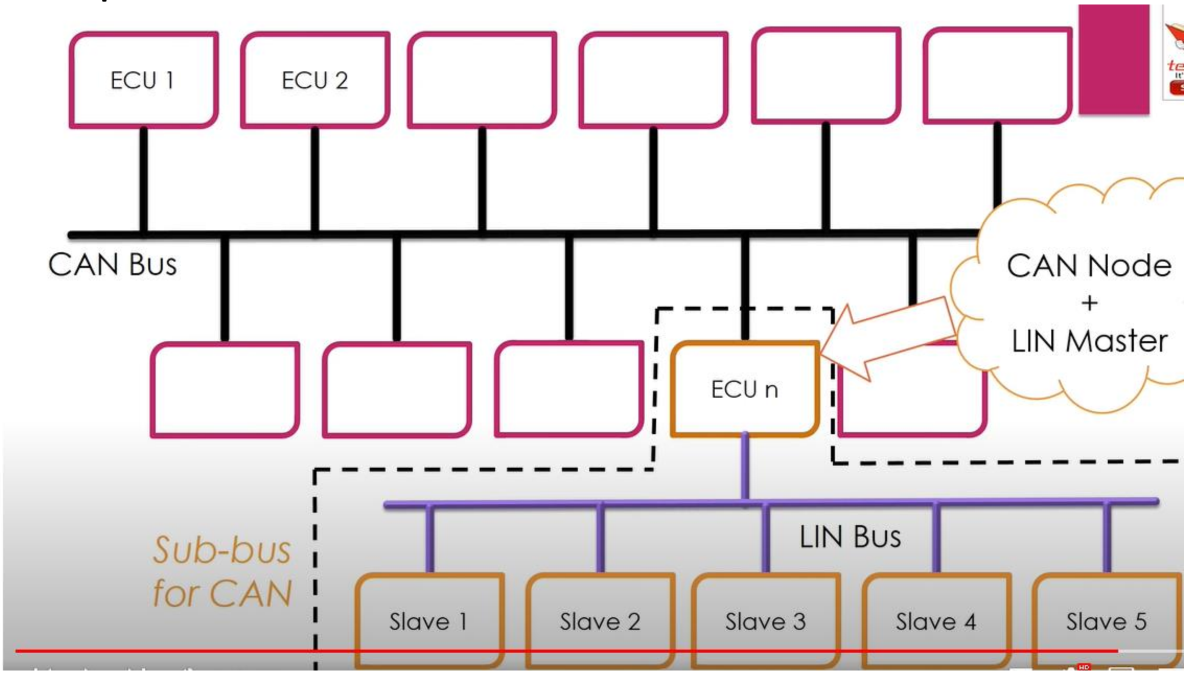


Figure 1: Communication Cycle

1. Static Segment
Reserved slots for deterministic data that arrives at a fixed period.
2. Dynamic Segment
The dynamic segment behaves in a fashion similar to CAN and is used for a wider variety of event-based data that does not require determinism.
3. Symbol Window
Typically used for network maintenance and signaling for starting the network.
4. Network Idle Time
A known "quiet" time used to maintain synchronization between node clocks.

Q.10.:Explain LIN architecture



- The Local Interconnect Network (LIN) bus was created to connect components in a small area, such as a single door.
- LIN (Local Interconnect Network) is a communication protocol used in automotive networks for low-speed data exchange between electronic control units (ECUs) in a vehicle.
- Uses serial communication using single wire.
- Consist of 1 master and more than one slaves
- Slave just respond to master.
- It is typically used for applications that do not require high data transfer rates, such as body control modules, interior lighting, and seat controls.
- The physical medium is a single wire that provides data rates of up to 20 kbits/s for up to 16 bus subscribers.
- All transactions are initiated by the master and responded to by a frame.
- The master node controls the communication on the network and initiates communication with the slave nodes. The slave nodes respond to commands from the master node and may also send status information or data to the master node.
- The software for the network is often generated from a LIN description file that describes the network subscribers, the signals to be generated, and the frames.
- Bluetooth is becoming the standard mechanism for cars to interact with consumer electronics devices such as audio players or phones.
- The network is organized as a ring.
- Data transmission is divided into channels.
- A control channel transfers control and system management data.
- Synchronous channels are used to transmit multimedia data;
- An asynchronous channel provides high data rates but without the quality-of-service guarantees of the synchronous channels
- The data exchange in LIN is typically asynchronous, meaning that the communication does not occur at fixed time intervals.
- It also includes error detection and correction mechanisms to ensure data integrity and reliability.

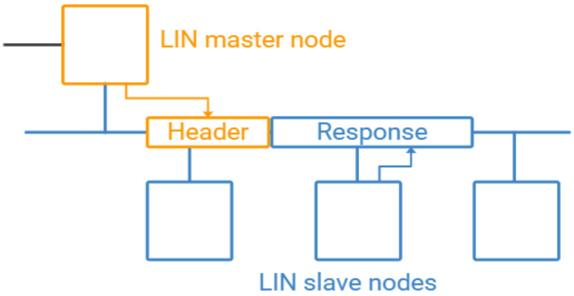
How does LIN bus work?

LIN communication at its core is relatively simple:

A master node loops through each of the slave nodes, sending a request for information - and each slave responds with data when polled. The data bytes contain LIN bus signals (in raw form).

However, with each specification update, new features have been added to the LIN specification - making it more complex.

Below we cover the basics: The LIN frame & six frame types.



Q.11.:Differences between CAN and LIN architecture

	CAN	LIN
Communication Type	Broadcast type	Master-Slave
Communication Network	Multi-master	Single Master, Multi Slave
No. of Lines required	2 wire	1 wire
Max Communication speed	1Mbps	20Kbps
Applications	Safety Critical - Airbag, ABS, Engine Management System	Non-Safety Critical – Entertainment System, Wip Control, Mirror Control
Implementation Complexity	Higher	Comparatively Lower
Implementation Cost	Higher	Comparatively Lower
Bus Conflicts	Uses Arbitration process to resolve bus conflict	No bus conflict
Message transmission Latency	Depends on the Message priority	Guaranteed Latency
Triggered Technique	Event-triggered	Time-triggered

Q.12.: Explain IoT(Internet of things)

IoT= Sensors + Wireless Networks + Database

- An Internet-of-Things system is a soft real-time networked embedded computing system.
- An IoT system always includes input devices: tags, sensors, etc.
- It may also include output devices: motor controllers, electronic controllers, displays, etc.
- The devices can be a combination of data processing devices (displays, buttons) and cyber-physical devices (temperature sensors, cameras).
- A computer-readable identification code for a physical object can allow a computer system to keep track of an inventory of items.
- A complex device or an appliance, for example can be controlled via a user interface on a cell phone or computer.
- A set of sensors can monitor activity, with data analysis algorithms extracting useful information from the sensor data.
- Sports sensor systems, for example, can monitor and analyze the activity of an athlete or team of athletes.

- Smart building systems can monitor and adjust the temperature and air quality of a building.

Q.13.: Draw the use case of IoT smart appliance

The simplest design formula is the smart appliance:

IoT smart appliance = connected appliance + network + UI

- Here, a user interface runs on a device such as a smart phone.
- The UI can interact with the smart appliance by sending and receiving messages via the hub.
- The UI can check the status of the smart appliance or give it commands.

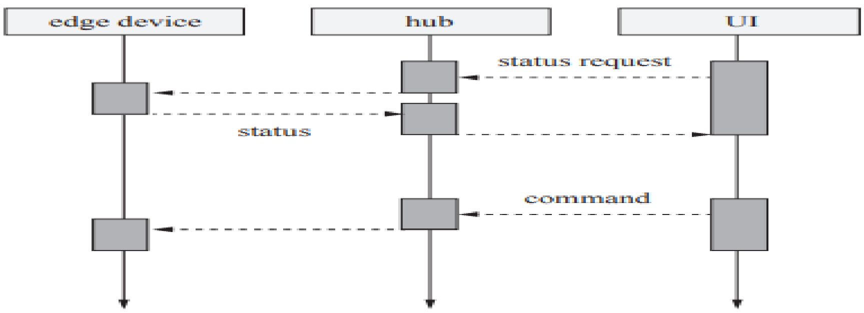


FIGURE 8.1
Use case for an IoT smart appliance.

Q.14.: Draw the use case of IoT monitoring system

The simplest design formula for IoT monitoring system:

IoT monitoring system = sensors + network + database + dashboard

- IoT monitoring systems include smart homes and buildings or connected cities.
- The sensors feed data into a database via their hubs.
- A data analysis program runs in the cloud to extract useful information from the sensor data
- Results are then given to the user on a dashboard that provides a summary of systems status, important events, etc.

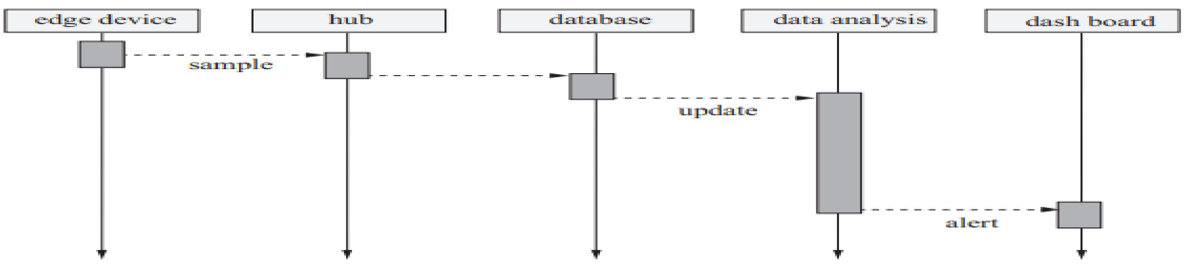


FIGURE 8.2
Use case for an IoT monitoring system.

Q.15.: Draw the use case of IoT control system

The simplest design formula for IoT control system:

IoT control system = sensors + network + database + controller + actuator

- A wireless sensor network can make sensor measurements that are sent to a cloud based controller which then sends a command to an actuator in the network.

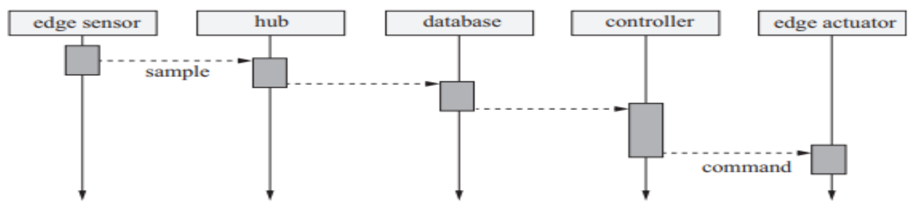


FIGURE 8.3

Use case for an IoT control system.

Q.16.: Explain networks for IoT

OR

Explain Networking Concepts used in IoT(Bluetooth, Bluetooth Low Energy, 802.15.4, ZigBee and WiFi)

- Networking is a critical component of an IoT system,wireless networking allows a much wider range of sensor applications.
- Three widely used wireless networks:
  - Bluetooth
  - Bluetooth Low Energy
  - IEEE 802.15.4/Zigbee
  - Wi-Fi

OSI model

- International Standards Organization(ISO) has developed a 7-layer model for networks known as Open System Interconnection (OSI) models.

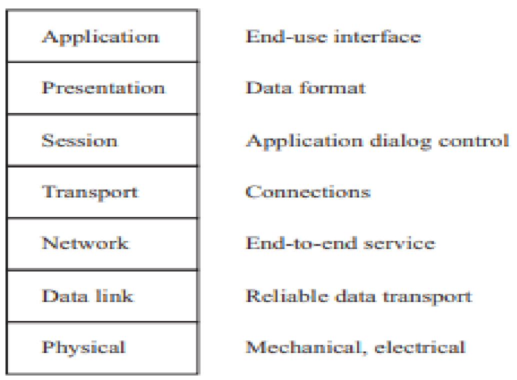


FIGURE 8.4

The OSI model layers.

- The OSI model includes 7 levels of abstraction known as layers:

  Physical: The physical layer defines the basic properties of the interface between systems, including the physical connections (plugs and wires), electrical properties etc

  Data link: The primary purpose of this layer is error detection and control across a single link.

  Network: This layer defines the basic end-to-end data transmission service.

  Transport: The transport layer defines connection-oriented services that ensure that data are delivered in the proper order and without errors across multiple links.

  Session: A session provides mechanisms for controlling the interaction of end-user services across a network, such as data grouping and check pointing

  Presentation: This layer defines data exchange formats and provides transformation utilities to application programs.

  Application: The application layer provides the application interface between the network and end-user programs.

IP

- The Internet Protocol (IP) is the fundamental protocol on the Internet.
- It provides connectionless, packet-based communication.
- Internet packet will travel over several different networks from source to destination.
- The relationship between IP an individual networks is:

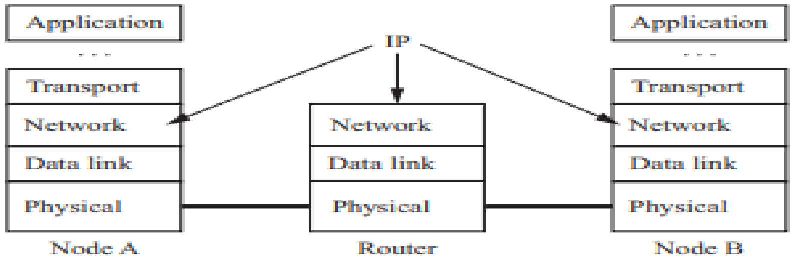


FIGURE 8.5

Protocol utilization in Internet communication.

- IP works at the network layer.
- When node A wants to send data to node B, the application's data pass through several layers of the protocol stack to get to the Internet Protocol.
- IP creates packets for routing to the destination, which are then sent to the data link and physical layers.
- A node that transmits data among different types of networks is known as a router.
- A packet may go through several routers to get to its destination.
- At the destination, the IP layer provides data to the transport layer and ultimately the receiving application.
- As the data pass through several layers of the protocol stack, the IP packet data are encapsulated in packet formats appropriate to each layer.
- The basic format of an IP packet is

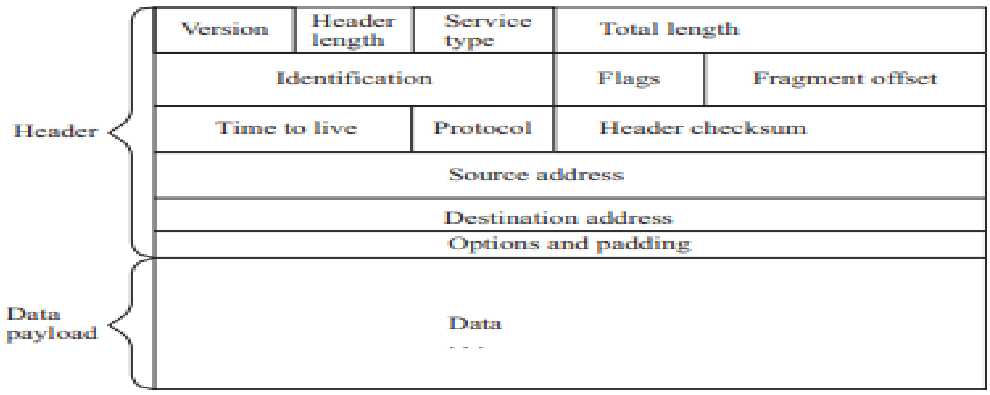


FIGURE 8.6

IP packet structure.

- The header and data payload are both of variable length.
- An Internet address is a number (32 bits in early versions of IP, 128 bits in IPv6).
- The IP address is typically written in the form xxx.xx.xx.xx.
- The fact that IP works at the network layer tells us that it does not guarantee that a packet is delivered to its destination.
- Because routes for data may change quickly with subsequent packets being routed along very different paths with different delays, real-time performance of IP can be hard to predict.
- The Transmission Control Protocol (TCP) is one such example.

- It provides a connection-oriented service that ensures that data arrive in the appropriate order, and it uses an acknowledgment protocol to ensure that packets arrive.

Iot networking concepts

- The topology of a network describes the structure of communication within the network.
- In the OSI model, a link is a direct connection between two nodes.
- The topology of a wireless IoT network is influenced by several factors, including the range of the radios and the complexity of the management of the topology. shows several example IoT network topologies.

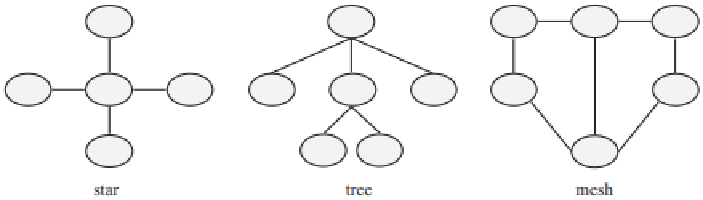


FIGURE 8.9

Example IoT network topologies.

4

- The star network uses a central hub through which all other nodes communicate.
- A tree network provides a more complex structure but still only provides one path between a pair of nodes.
- A mesh network is a general structure.
- Once the network authenticates a node, it must perform some housekeeping functions to incorporate the new node into the network.
- Routing discovery determines the routes that will be used by packets that travel to and from other nodes to the new node.
- Routing discovery starts by searching the network for paths to the destination node.
- A node will broadcast a message requesting routing discovery services and record the response it receives.
- The recipient nodes will then broadcast their own routing discovery request with the process continuing until the destination node is reached.
- Once a set of routes have been identified, the network evaluates the cost of the paths to choose onepath.
- The cost computation for a path can include the number of hops, the transmission energy required, and the signal quality on each link.

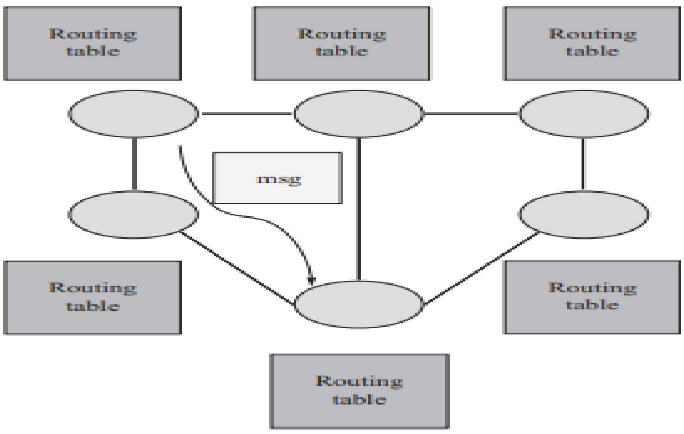


FIGURE 8.10

Routing packets through a network.

-

- To provide synchronous data with its quality of service characteristics, the network needs to reserve bandwidth for that communication.
- Many networks perform admission control to process a request for synchronous transmission and to determine whether the network has the bandwidth available to support the request.
- One challenge in synchronous communication over wireless networks is synchronizing the nodes.
- Many wireless networks provide synchronous communication using beacons.
- Beacon is a transmission from a node that marks the beginning of a communication interval.
- The time between beacons is usually divided into two segments, one for synchronous and the other for asynchronous packets.
- A synchronous communication can be assigned its own time slot in the synchronous segment

FIGURE 8.11
Beacon transmissions.

a) Bluetooth

- Bluetooth is now used to connect a wide range of devices to host systems.
- Bluetooth is designed to operate in a radio band known as the instrumentation, scientific, and medical (ISM) band.
- Bluetooth networks are often called piconets, thanks to their small physical size. A piconet consists of a master and several slaves. A slave can be active or parked. A device can be a slave on more than one piconet.
- The Bluetooth stack is divided into three groups:
  - Transport protocol
  - Middleware protocol
  - Application

✓ The transport protocol group itself has several constituents:
• The radio provides the physical data transport.
• The baseband layer defines the Bluetooth air interface.
• The link manager performs device pairing, encryption, and negotiation of link properties.
• The logical link control breaks large packets into Bluetooth packets. It negotiates the quality of service required and performs admission control.

✓ The middleware group has several members:
• The service discovery protocol (SDP) provides a directory for network services.
• The Internet Protocol and IP-oriented services such as TCP and UDP.
• A variety of other protocols, such as IrDA for infrared and telephony control.

✓ The application group includes the various applications that use Bluetooth.

- Every Bluetooth device is assigned a 48-bit long Bluetooth Device Address.
- Every Bluetooth device also has its own Bluetooth clock that is used to synchronize the radios on a piconet.
- When a Bluetooth device becomes part of a piconet, it adjusts its operation to the clock of the master.
- Transmissions on the network alternate between master and slave directions.

b) Bluetooth Low Energy

- Bluetooth Low Energy is designed to support very low energy radio operation.
- Eg: A radio operated by a button-sized battery for an extended period
- BLE uses a different modulation scheme in the physical layer than does Classic Bluetooth.
- Minimizing the amount of time the radio is on is critical to low energy operation.
- BLE is designed to minimize radio on-time in several ways.
- At the link level, packets are designed to be relatively small.
- BLE is also designed to support communications that do not require long-lived connections.
- Advertising is one form of communication that is designed to support low energy operation.
- A device can transmit advertising packets; devices can also listen for advertising packets.
- Advertising can be used to discover devices or to broadcast information.
- If longer communications are required between devices, BLE also supports the establishments of connections

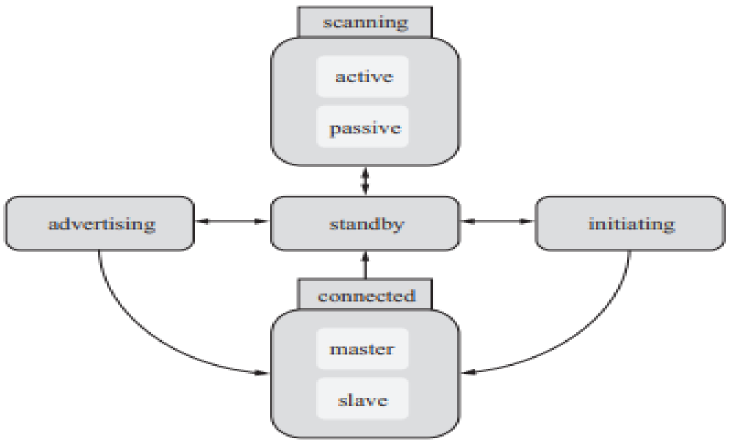


FIGURE 8.13

Bluetooth Low Energy link level state machine.

- The scanning state allows the device to listen to advertising packets from other devices: passive scanning only listens while active scanning may also send requests for additional information.
- The advertising state corresponds to a device transmitting advertising packets.
  The BLE Host Controller Interface (HCI) provides several interfaces to the host:
- UART for link establishment and acknowledgment; USB provides high-speed communication; and Secure Digital Input Output (SDIO) is designed for mediumspeed communication.
- The Attribute Protocol Layer provides a mechanism to allow devices to create application-specific protocols for their particular data communication and management needs.
- An attribute has three components: its handle, which functions as the name of the attribute; its type, which is chosen from the set of Universally Unique Identifiers (UUIDs); and its value.

- Most UUIDs used in BLE devices are part of a restricted set built around the Bluetooth Base UUID and come in several types: service UUIDs,units, attribute types, characteristic descriptors, and characteristic types
- Attributes are collected in an attribute database that is maintained in an attribute server.
- An attribute client can use the Attribute Protocol to query a database.
- Each device has only one attribute database. An attribute has permissions: readable,writable, or both.
- Attributes can also be protected with authentication and authorization.
- A set of attributes can be used to define a state machine for a protocol.
- The states and transitions in the state machine can be stored as attributes; the current state, inputs, and outputs can also be represented by attributes.
- The Generic Attribute Profile Layer (GATT) defines a basic set of attributes for all BLE devices.
- The main purpose of the Generic Attribute Profile is to define procedures for discovery and for the interactions of clients and servers.
- BLE provides mechanisms for security.
- Two devices communicating for the first time is known as pairing.
- This process uses a short-term key to send a long-term key to the device.
- The long-term key is stored in the database, a process known as bonding.
- Data sent as part of a connection may be encrypted using the AES standard.

c) 802.15.4 and ZigBee

- ZigBee is a widely used personal area network based on the IEEE 802.15.4 standard.
- The standard is designed for systems with either no battery or those that allow only very little current draw from the battery.
- 802.15.4 supports two types of devices: full-function device (FFD) and reduced function device (RFD).
- A full-function device can serve as either a device, a coordinator, or a personal area network coordinator.
- A reduced-function device can only be a device.
- Devices can form networks using either a star topology or a peer-to-peer topology.
- In a star topology network, a PAN coordinator serves as a hub; peer-to-peer networks also have a PAN coordinator but communications do not have to go through the PAN coordinator.
- The basic unit of communication in an 802.15.4 network is the frame, which includes addressing information, error correction, and other information as well as a data payload.
- A network can also make use of optional superframes.
- A superframe, which is divided into 16 slots, has an active portion followed by an inactive portion.
- The first slot of a superframe is known as the beacon.
- It synchronizes the nodes in the network and carries network identification information.
- To support QoS guarantees and low-latency operation, the PAN coordinator may dedicate parts of a superframe to those high-QoS or low-latency operations.
- Those slots do not have contention.

- The PHY layer activates the radio, manages the radio link, sends and receives packets, and other functions.
- It has two major components: the PHY data service and the PHY management service.
- The interface to the physical layer is known as the physical layer management entity service access point (PLME-SAP).
- The standard uses carrier sense multiple access with collision avoidance (CSMA-CA)
- The MAC layer processes frames and other functions.
- It also provides encryption and other mechanisms that can be used by applications to provide security functions.
- The MAC layer consists of the MAC data service and MAC management service; its interface is known as the MLME-SAP.
- ZigBee defines two layers above the 802.15.4 PHY and MAC layers: the NWK layer provides network services and the APL layer provides application-level services.
- The ZigBee NWK layer forms networks, manages the entry and exit of devices to and from the network, and manages routing.
- The NWK layer has two major components.
- The NWK Layer Data Entity (NLDE) provides data transfer services; the
- NWK Layer Management Entity (NLME) provides management services.
- A Network Information Base (NIB) holds a set of constants and attributes.
- The NWK layer also defines a network address for the device.
- The NWK layer provides three types of communication: broadcast, multicast, and unicast.
- A broadcast message is received by every device on the broadcast channel.
- Multicast messages are sent to a set of devices.
- A unicast message, the default type of communication, is sent to a single device.
- The devices in a network may be organized in many different topologies.
- A network topology may be determined in part by which nodes can physically communicate with each other but the topology may be dictated by other factors.
- A message may, in general, travel through multiple hops in the network to its destination.
- A ZigBee coordinator or router performs a routing process to determine the route through a network used to communicate with a device.
- The choice of a route can be guided by several factors: number of hops or link quality.
- The NWK layer limits the number of hops that a given frame is allowed to travel.
- The ZigBee APL layer includes an application framework, an application support sublayer (APS), and a ZigBee Device Object (ZDO).
- Several application objects may be managed by the application framework, each for a different application.
- The APS provides services interface from the NWK layer to the application objects.
- The ZigBee Device Object provides additional interfaces between APS and the application framework.
- ZigBee defines a number of application profiles that define a particular application.
- The application identifier is issued by the ZigBee Alliance.
- The application profile includes a set of device descriptions that give the characteristics and state of the device.
- One element of the device description also points to a cluster which consists of a set of attributes and commands

d) WiFI

- The 802.11 standard, known as Wi-Fi [IEE97], was designed originally for portable and mobile applications such as laptops.
- The original standard has been extended several times to include higher performance links in several different bands.
- It was designed before ultra low energy networking became an important goal.
- But a new generation of Wi-Fi designs are designed for efficient power management and operate at significantly lower power levels
- Wi-Fi supports ad hoc networking.
- A basic service set (BSS) is two or more
- 802.11 nodes that communicate with each other.
- A distribution system (DS) interconnects basic service sets.
- More expansive links are provided by an extended service set (ESS) network.
- BSS related by an ESS can overlap or be physically separate.
- A portal connects the wireless network to other networks.
- A network provides a set of services.
- The most basic service is distribution of messages from source to destination.
- Integration delivers a message to a portal for distribution by another network.
- Association refers to the relationship of a station to an access point; reassociation allows an association to be moved to a different access point; disassociation allows an association to be terminated.
- Every station must provide authentication, deauthentication, privacy, and MAC service data unit (MSDU) delivery.
- A DSS must provide association, disassociation, distribution, integration, and reassociation.
- The reference model for 802.11 breaks the physical layer into two sublayers: physical layer convergence protocol (PLCP) and physical medium dependent (PMD). They communicate with a PHY sublayer management entity.
- The MAC sublayer communicates with a MAC sublayer management entity.
- Both management entities communicate with the station management entity.
- The MAC provides several services:
  • Asynchronous data service. This service is connectionless and best-effort.
  • Security. Security services include confidentiality, authentication, and access control.
  • StrictlyOrdered service. A variety of effects can cause packets to arrive out of order. This service ensures that higher levels see the packets in the strict order in which they were transmitted.

Q.17.: What are databases in IoT

- Databases are used in many applications to store collections of information.
- IoT networks use databases to manage and analyze data from the IoT devices.
- IoT databases are often kept in the cloud;
- The traditional database model is the relational database management system
- Data in a relational database is organized into tables.
- The rows of the table represent records (sometimes called tuples).
- The columns of the table are known as fields or attributes.
- One column of the table (or sometimes a set of column) is used as a primary key and each record has a unique value for its primary key field and each key value uniquely identifies the values of the other columns.
- The device_data table records time-stamped data from the devices.

- Each of those records has its own primary key, given the name signature.
- The set of table definitions in a database is known as its schema.
- Eliminating redundancy is key to maintaining the data in the database.
- If a piece of data is stored in two different tables (or two different columns in one table), then any change to the data must be recorded in all its copies.
- If some copies of the data are changed and some are not, then the value returned wil depend on which copy was accessed.
- The database designer's description of the tables does not necessarily reflect how the data are organized in memory or on disk.
- The database management system may perform a number of optimizations to reduce storage requirements or improve access speed.
- Database normal forms are rules that help us create databases without redundancies .
- **The first normal form** is a schema in which every cell contains only a single value
- The **second normal form** obeys the first normal form and, in addition, the values of all the other cells in a record are unique to the key.
- If a database does not obey the second normal form, then we have duplicated information in the database.
- The **third normal form** satisfies the second normal form and also requires that the non key columns are independent.
- A request for information is known as a query.
- Users do not deal directly with the tables.
- Instead, they formulate a request in a query language known as a structured query language (SQL).
- The result is the set of records that satisfy the query.
- A common type of query combines information from more than one table. This operation is known as a join.
- A join can be described mathematically as a Cartesian product of rows.
- DBMS may optimize the internal representation for that type of query; these sorts of optimizations do not change the schema, merely represent the data in a particular format that is hidden from the user.

Q.18: Explain timewheels in IoT

- The timewheel allows the IoT system to process events in the order in which they actually happen.
- This is particularly important when controlling devices like turning lights on and off at specified times, for example.
- Timewheels are used in event-driven simulators to control the order in which simulated events are processed.
- We can also use timewheels to manage the temporal behavior of devices in an IoT system.
- Timewheel is a sorted list of input and output events.
- As input events arrive, they are put in sorted order into the queue.
- Similarly, when output events are scheduled, they are placed at the proper time order in the queue.

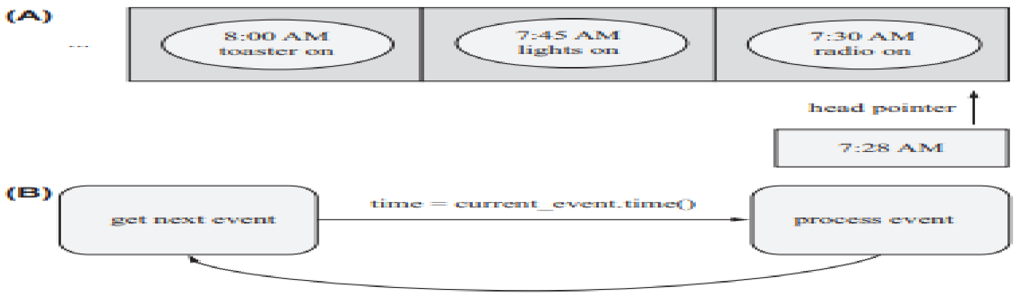


FIGURE 8.15
Timewheel organization. (a) Timewheel queue (b) UML state diagram.

- UML state diagram for the operation of the timewheel.
- It pulls the head event from its queue.
- When the time specified in the event is reached, that event is processed.
- A system may have one or more timewheels.
- A central timewheel can be use to manage activity over the entire IoT system.
- In larger networks, several timewheels can be distributed around the network, each of which keeps track of local activity

Q.19.: Show the case study of Smart Home using IoT

- A smart home is a house equipped with sensors that monitor activity and help run the house. A smart home may provide several types of services:
  remote or automatic operation of lights and appliances;
  energy and water management for efficient use of natural resources;
  monitoring activities of residents.
- Performing these tasks requires not only operating sensors but also analyzing the sensor data to extract events and patterns.
- The smart home system can provide three types of outputs:
  - reports on the activities of residents;
  - alerts for out-of-the-ordinary activity;
  - recommendations to the residents and caregivers as to what actions may be taken

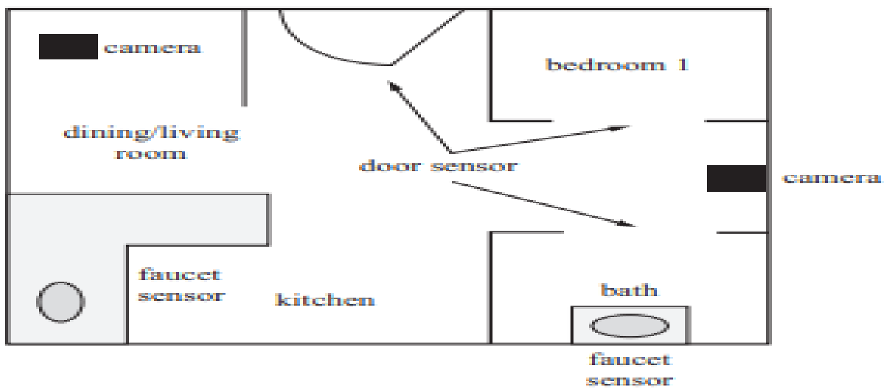


FIGURE 8.16
IoT network in a smart home.

- The home includes several cameras to monitor common areas.
- Other types of sensors can also help to keep track of activity: door sensors tell when someone has passed through a door, but does not give the person's identity or even whether they are entering or leaving;sensors on water faucets can tell when someone is using a bathroom or kitchen sink; electrical outlet sensors can tell when someone is using an electrical appliance.

- Appliances and devices can also be controlled: lights can be turned on and off, heaters and air conditioners can be managed, sprinklers can be turned on and off, etc.

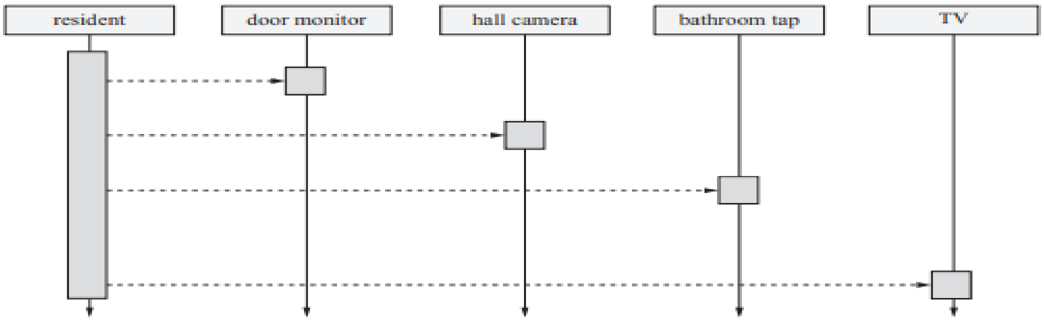


FIGURE 8.17

Analyzing a resident's activity in a smart home.

- The above UML shows how sensors can be used to monitor a resident's activity.
- The resident leaves her bedroom, walks through the hallway to the bathroom, uses the sink, then moves to the living room, and turns on the TV.
- Sensors can be used to monitor these actions.
- In the case of the hall camera, computer vision algorithms can identify the person in the hallway and track their movement from one room to another.
- Analysis algorithms can use statistical methods to infer that the same person was likely to have caused all these events. for example, a person in another part of the house may not be able to change locations quickly enough to cause some of the events.

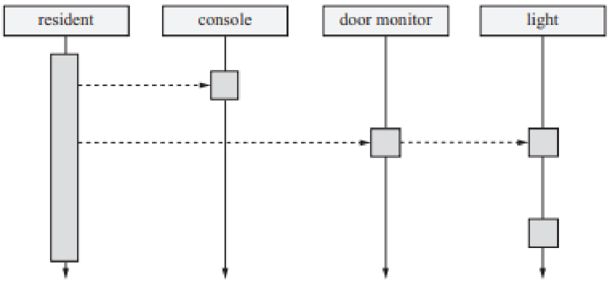


FIGURE 8.18

Light activation in the smart home.

- The above object diagram shows how smart home can control as well as monitor activities.
- The resident uses the console to set up two conditions in which the light should be turned on: whenever anyone goes through the resident's doorway, or at a specified time.
- In this use case, the resident later goes through the doorway, causing the light to turn on for a specified interval.
- The light also goes off automatically at the appointed time.

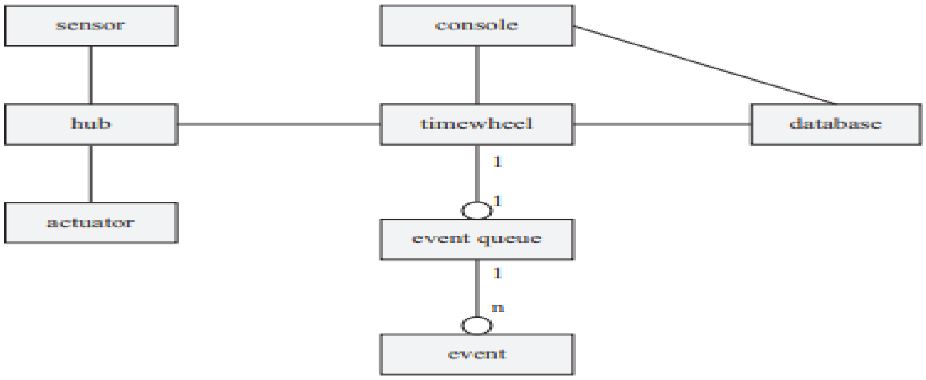


FIGURE 8.19

UML object diagram for smart home.

- The above shows an object diagram for the smart home. Sensors and hubs form the network.
- The console is the main user interface.
- Data are processed in two stages.
- Sensor readings and events are initially processed by a timewheel that manages the timely operation of devices in the house.
- Not all sensor readings are of long-term interest.
- Sensor events for long-term analysis are passed to a database.
- The database can reside in the cloud and allow access to a variety of analysis algorithms.

-----------------------------*****************-----------------------