SNS College of Technology, Coimbatore-35.
(Autonomous)
B.E/B.Tech- Internal Assessment -I
Academic Year 2023-2024 (ODD)
Fifth Semester
Department of Information Technology
19ITT302 & INTERNET OF THINGS
Answer Key for SET A

PART - A (5 x 2 = 10 Marks)

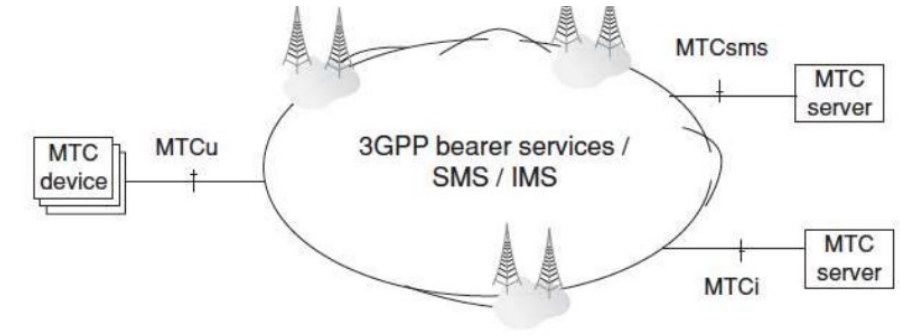
1. **What are the key factors that must be considered in selecting the most suitable battery for a particular IoT application?**
   Smart sensors, smartwatches, and door locks all have one thing in common: their small size necessitates the use of a smaller and lighter battery. Choose a battery that does not take up too much space or add too much weight to the device for these types of products.
   The most common option is to use rechargeable lithium button batteries or other coin-type batteries. However, some IoT devices require replaceable batteries, which can be either lithium-ion or nickel metal hydride.

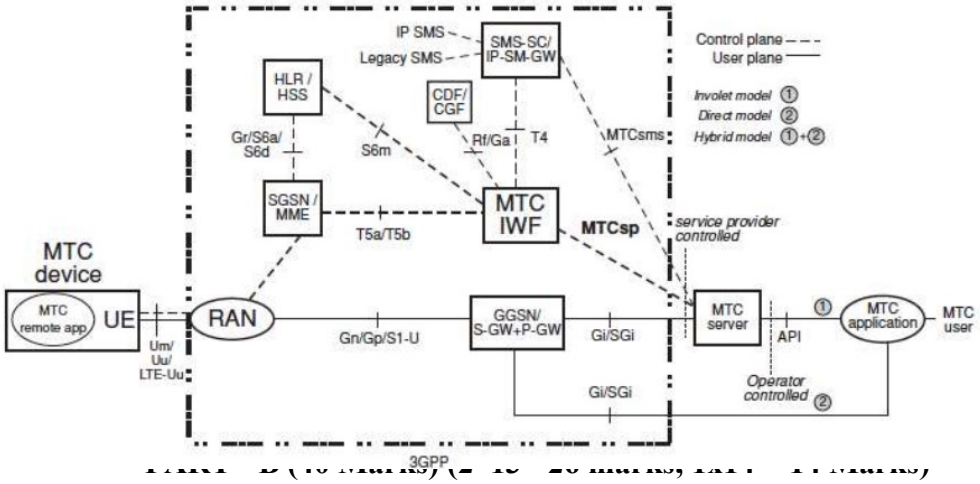
2. Difference between Contactless smart card and RFID.

RFID	Vs	Contact less Smart Cards
• Chip, antenna, package • Active and Passive • Contact less • Security issues in terms of information leakage and traceability		• Chip embedded in card, antenna • Not powered • Contact or contactless • Memory or Microprocessor • High emphasis on security
Information storage only (product identification numbers)		On-card functions possible (authentication & encryption)

3. Examine the use of RPL RoLL.

   The RPL supports various communication paradigms, Point-to-MultiPoint (P2MP), Point-to-Point (P2P), and MultiPoint-to-Point (MP2P). In addition, the RPL supports two modes of operation. First, the storing mode, where each node maintains a downward routing table for its sub-DODAG and uses it to transmit P2P traffic
4. What are the metrics to be considered for IoT applications?
   - Routing state memory space—limited memory resources of low power nodes;
   - Loss response—what happens in response to link failures;
   - Control cost—constraints on control traffic;
   - Link and node cost—link and node properties are considered when choosing routes
5. Drive the usecase for MTC devices communicating with one or more MTC servers.

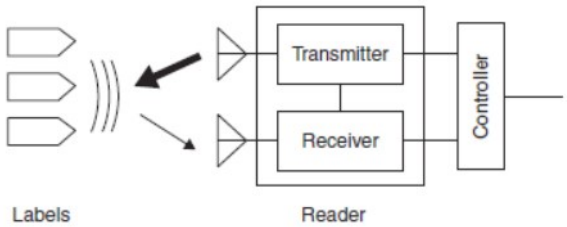




6.a Illustrate the Concept of RFID and Satellite Technology

RFIDs are electronic devices associated with objects ("things") that transmit their identity (usually a serial number) via radio links. RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. RFID tags have broad applications, including the rapid collection of data in commercial environments.

For example, RFID and bar coding are nearly ubiquitous in the inventory process, providing both accuracy and speed of data collection. These technologies facilitate the global supply chain and impact all subsystems within that overall process, including material requirement planning (MRP), just in time (JIT), electronic data interchange (EDI), and electronic commerce (EC). RFIDs are also used in industrial environments, such as but not limited to dirty, wet, or harsh environments. The technology can also be used for identification of people or assets



Contactless smart cards (SCs) are more sophisticated than RFID tags, being that they contain a microprocessor that enables

- on-board computing,
- two-way communication including encryption, and
- storage of predefined and newly acquired information.

RFID Layers

An RFID system is logically comprising several layers, as follows:

▪ the tag layer,

▪ the air interface (also called media interface) layer, and

▪ the reader layer;

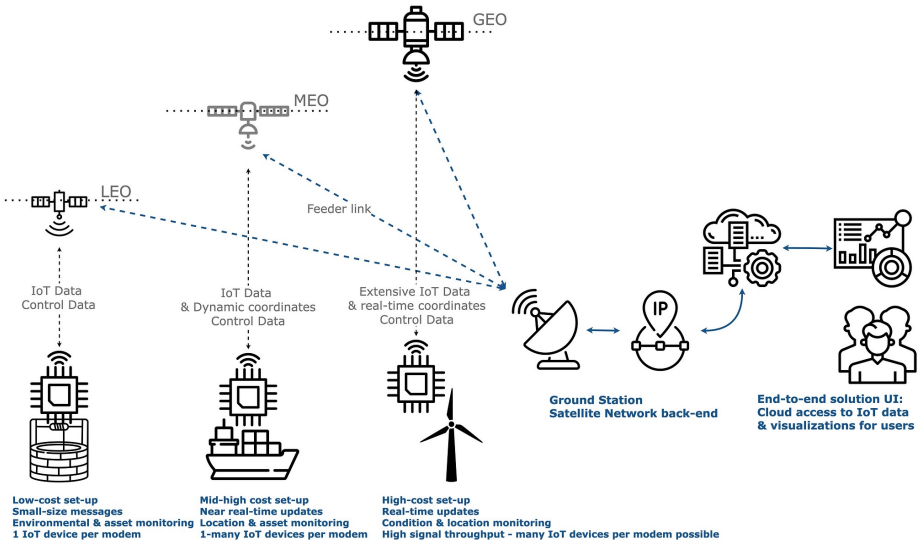
additionally, there are network, middleware, and application aspects. Some of the key aspects of the basic layers are as follows:

▪ Tag (device) layer: Architecture and EPCglobal Gen2 tag finite state machine

▪ Media interface layer: Frequency bands, antennas, read range, modulation, encoding, data rates

▪ Reader layer: Architecture, antenna configurations, Gen2 sessions, Gen2

Satellite Technology



b Demonstrate the IoT Enabling Technologies with real world example

- Wireless Sensor Network (WSN)
- Cloud Computing
- Bigdata Analytics
- communication protocols
- embedded systems

7.a Analyse in detail the IoT Application protocol and their characteristics with suitable illustration

Constrained Application Protocol.

- Organizations use CoAP with limited hardware that has a low transmission rate because it's lightweight. The protocol is HTTP-friendly, using two basic message types: request and response. Messages can be confirmable or non-confirmable. Data packets are small, so message losses are few. The disadvantage is the protocol lacks security, which engineers normally can remedy with datagram transport layer security, but DTLS is of limited use in IoT.

Message Queue Telemetry Transport.

- MQTT is a publish/subscribe protocol, which is effective for lightweight machine-to-machine (M2M) connectivity over TCP and minimizes data loss. Publish/subscribe for IoT means clients don't have to call for updates, which lessens network traffic and processing load. The protocol

also accommodates a range of quality enforcement levels, from single handshake delivery to acknowledgment requirement.

Representational State Transfer.

- REST is the most ubiquitous protocol and gives IoT synchronous request-response via HTTP. HTTP makes it feature-rich, as well as capable of authentication and caching, both of which are useful in complex environments, although difficult to implement in IoT. The protocol is both XML- and JSON-compatible, which is useful for M2M and communication with tablets and smartphones, a boon for IoT.

7.b i) Illustrate the concept of 3GPP service requirements for MTC

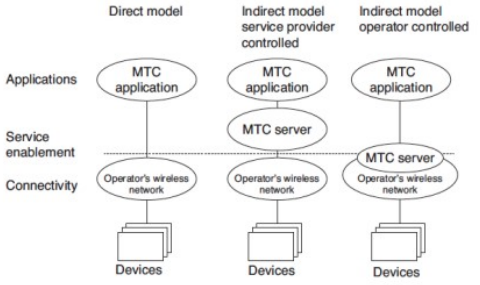
Current mobile networks are optimized for human-to-human (H2H) traffic and not for M2M/MTC interactions; hence, optimizations for MTC are advantageous. 3GPP has started work on M2Mspecification in 2010 for interoperable solutions, particularly in the 3G/4G/LTE context.

In M2M architecture, the interfaces are as follows:

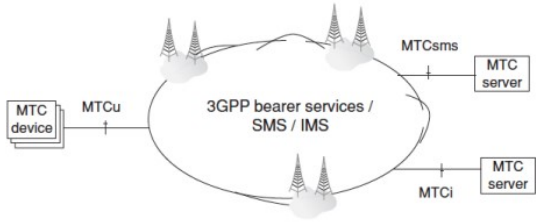
• MTCu: provides MTC devices access to the 3GPP network for the transport of user traffic;
• MTCi: the reference point for MTC server to connect the 3GPP network via 3GPP bearer service; and
• MTCsms: the reference point for MTC server to connect the 3GPP network via 3GPP SMS.

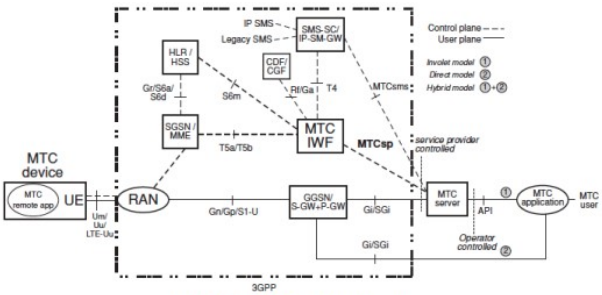
For MTC communication, the following communication scenarios are identified and described

- MTC devices communicating with one or more MTC server;
- MTC devices communicating with each other. For MTC devices communicating with one or more MTC servers, the following use cases exist:
- MTC server controlled by the network operator; namely the MTC server is located in the operator domain. Here – The network operator offers API (e.g., Open Systems Architecture [OSA]) on its MTC server(s) – MTC user accesses MTC server(s) of the network operator via AP



M2M in 3GPP—service models

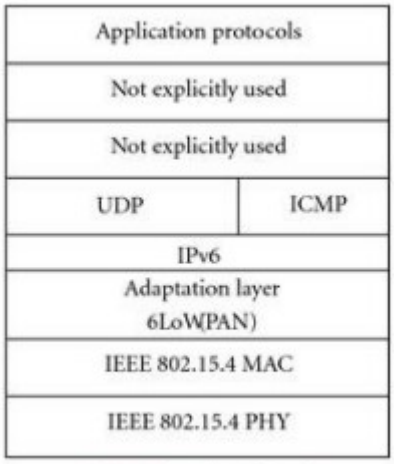




M2M in 3GPP—Architecture

7.b.ii) Define and explain in briefly about 6LoWPAN with example

- 6LoWPAN is an IPv6 adaption layer for low power wireless PAN (LoWPAN).
- A link in a LoWPAN is characterized as lossy, low power, low bit-rate, short range, with many nodes saving energy with long sleep periods.
- 6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks.
- A LoWPAN is potentially composed of a large number of overlapping radio ranges works on 2.4 GHz It uses AES-128 link layer security for authentication and encryption and TLS 6LoWPAN is a low power wireless mesh network where every node has its own IPv6 address.
- This allows the node to connect directly with the Internet using open standards. It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web sockets.
- It offers end-to-end IP addressable nodes.
- There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP. In a 6LowPAN network, leaf nodes can sleep for a long duration of time



6LoWPAN protocol stack

8.a Explain briefly about various communication protocol with block diagram

- Zigbee/IEEE 802.15.4
- RF4CE
- Bluetooth
- WiFi

b Demonstrate Routing over Low Power and Lossy Networks with suitable explanation

- Low power and lossy networks (LLNs) are1 a class of networks in which both the routers and their interconnect are constrained.
- LLN routers typically operate with constraints on processing power, memory, and energy (battery power); their interconnects are characterized by high loss rates, low data rates, and instability.
- The IPv6 Routing Protocol for LLNs (RPL) is a mechanism proposed by the IETF to support multipoint-to-point traffic from devices inside the LLN toward a central control point, as well as point to- multipoint traffic from the central control point to the devices inside the LLN.

- Challenges in LLNs are low processing power, memory and energy constrained operation and it must also support point to point, point to multipoint and multipoint to point traffic.
- To address these issues, the IETF ROLL Working Group has defined application-specific routing requirements for an LLN routing protocol; it has also specified the RPL.

RPL defines a new ICMPv6 message with three possible types:

- DAG information object (DIO)—carries information that allows a node to discover an RPL instance, learn its configuration parameters, and select DODAG parents;
- DAG information solicitation (DIS)—solicit a DODAG information object from an RPL node;\
- Destination advertisement object (DAO)—used to propagate destination information upward along the DODAG.