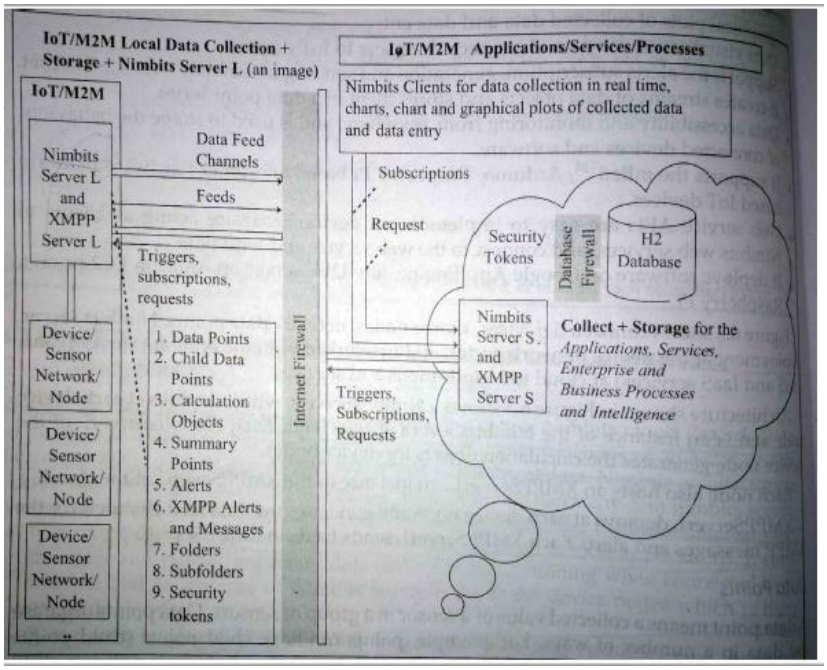
USN | | | | | | | | | | |

Internal Assessment Test 5 –Feb 2022

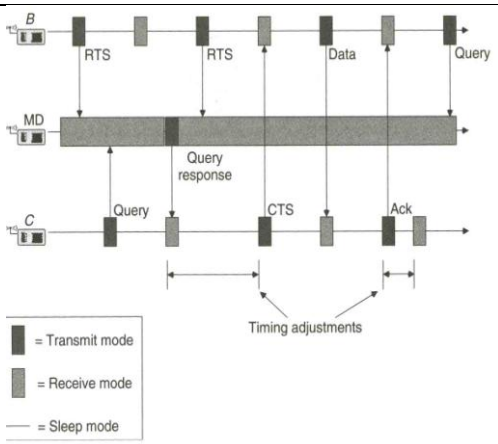
Sub:	IOT &WSN					Sub Code:	18EC742	Branch:	ECE
Date:	8/2/2022	Duration:	90 min's	Max Marks:	50	Sem / Sec:	7 A,B,C,D		OBE

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1	Explain IoT cloud based data collection, storage and computing services using Nimbits. IOT/M2M client applications communicates, subscribe and sets the triggers and receive the responses and feeds deploying (using) a cloud service. •Cloud service deploys an instance of cloud server at the sensor node which provisions for generation and communication of data points ,alerts and feeds on subscriptions ,triggers and requests. •Feed consists of time/geo-stamped data points, streams and alerts. •Depending on rules for filtering and calculations feeds for messages and alerts are generated. Nimbits is a Cloud PaaS service which deploys an instance of Nimbits server at Arduino ,Raspberry Pi or other IoT sensor nodes that enables real time data collection, storage at an H2 database ,Edge computing, Alerts, messages, application programmed to get alerts (twitter, email or other), data visualisation , Analytics, rule engine, calculations alerts, feeds on subscriptions ,triggers and requests. Nimbits is an open source process data historian for Google App Engine. It provides data logging, calculations and M2M communication for sensors and devices such as Arduino. It can be used to record and share data points on the cloud and lets users record their changing numeric, text based, GPS, json or xml values into them. The API lets users access the public server to push and pull their data from. The API also provides access to a chart image service, which can generate PNG format images of user data. The API uses HTTP calls and responses are formatted in JSON or TXT. The basic services offered by Nimbits • It provides edge computing locally on embedded systems, build up on local application •Nimbits enables Iot an open source distributed cloud. •It pushes important data to the cloud when connected to internet. •It supports multiprogramming languages, including Arduino, push functions from Arduino cloud, javascript, HTML. •It provides rule engine for connecting sensors, persons and software to cloud and to one another. Nimbits data points can relay data between the software systems or hardware devices like Arduino, using cloud as backend. •It provides data logging services and access, and stores historical data points and data objects. •Storage in any format that can be serialized into string such as json or xml. •It filters the noise and important changes sent to another larger central instance.	[10] [5+5] Explanation +Figure]	CO2	L1

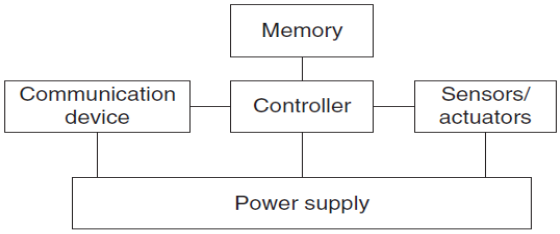


2	Explain Mediation Device Protocol with advantages and disadvantages. Mediation Device avoid useless listening on the channel for messages. It uses a mediation device (MD) which is available all the time and allows each node to go to sleep mode periodically and to wake up only for short times to receive packets .No global time reference , node does not take care of neighbour schedule. Working of the Protocol ❑ Sender B sends RTS to MD ❑ MD stores this information ❑ Receiver C sends query to MD ❑ MD tells reciever C when to wake up ❑ C sends CTS to B (now in sync) ❑ B sends data ❑ C acknowledges ❑ C returns to old timing	[10] [4+4+2] [explaination+Diagram +Advantages and Disavantages]	CO3	L1



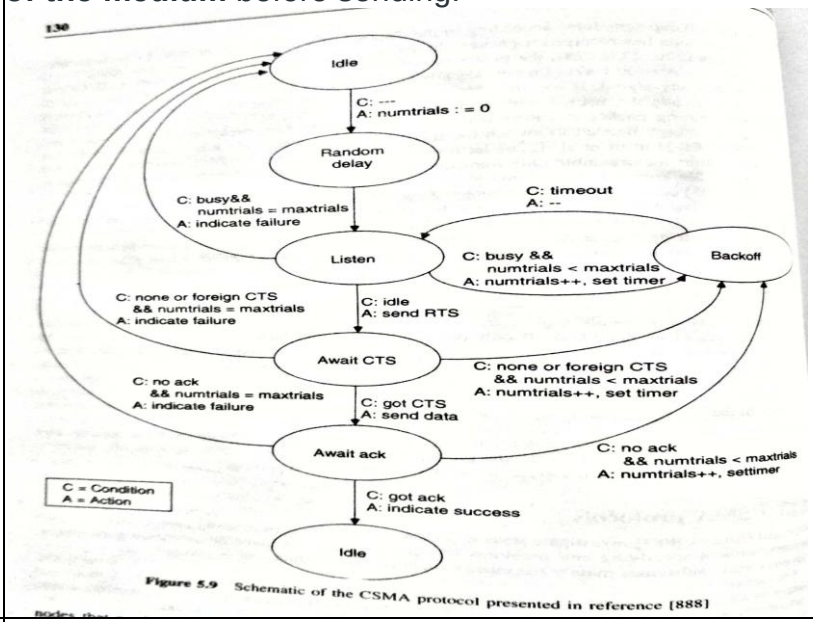
- Advantages-
  - Does not require time synchronisation between the nodes only the MD has to learn the periods of the nodes
  - Most of the power burdon is shifted to MD,other devices can be in sleep mode most of the time and have to spend energy only for periodic becons.
  - Synchronisation work is done by MD,very low duty cycles can be supported.
- Disadvantages:
  - The becons of different nodes may collide repeatedly when nodes have overlaping wakeup periods.
  - MD has to be energy independent or unconstrained.

3	Explain the single node architecture with necessary hardware components.	[10] [5+5] [figure+exla nation]	CO3	L1



A basic sensor node contains five main components such as Controller, Memory, Sensors and Actuators, Communication devices and Power supply Unit.

- **<u>Controller:</u> The controller is the core of a wireless sensor node, it process all the relevant data, capable of executing arbitrary code.**
  It collects data from the sensors, processes this data, decides when and where to send it, similarly receives data from other sensor nodes and decides on the actuator's behavior.
  It has to execute various programs, hence it is the Central Processing Unit (CPU) of the node.
  For General-purpose processing applications microprocessors are used. These are highly overpowered, and their energy consumption is excessive. These are used in embedded systems.
  Examples: Intel Strong ARM, Texas Instruments MSP 430, Atmel ATmega.
- **<u>Memory:</u>**
  Memory is required to store programs and intermediate data; usually, different types of memory are used for programs and data.
  In WSN there is a need for Random Access Memory (RAM) to store intermediate sensor readings, packets from other nodes, and so on.
  RAM is fast, its main disadvantage is that it loses its content if power supply is interrupted.
  Program code can be stored in Read-Only Memory (ROM) or in Electrically Erasable Programmable Read-Only Memory (EEPROM) or flash memory.
  Flash memory is similar to EEPROM but allowing data to be erased or written in blocks instead of only a byte at a time.
  It can also serve as intermediate storage of data in case RAM is insufficient or the power supply of

	RAM should be shut down. ➢ **Sensors and actuators:** The actual interface to the physical world: The devices that can observe or control physical parameters of the environment. **Actuators:** Actuators are just about as diverse as sensors, yet for the purposes of designing a WSN that converts electrical signals into physical phenomenon. ➢ **Communication Device:** To turn nodes into a network a device is required for sending and receiving information over a wireless channel. *Transmission medium selection:* The communication device is used to exchange data between individual nodes. In some cases, wired communication can actually be the method of choice and is frequently applied in many sensor networks. The case of wireless communication is considerably more interesting because it include radio frequencies. Radio Frequency (RF)-based communication is by far the most relevant one as it best fits the requirements of most WSN applications.			
4	Explain the CSMA protocol with proper flow diagram. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.  Figure 5.9 Schematic of the CSMA protocol presented in reference [888]	[10]	CO3	L1
5	Write short note on 1) XMPP 2)COAP 3)MQTT 4)HTTP **XMPP** is a short form for Extensible Messaging Presence Protocol. It's protocol for streaming XML elements over a network in order to exchange messages and presence information in close to real time. This protocol is mostly used by instant messaging applications like WhatsApp. • X in XMPP It means eXtensible. XMPP is a open source project which can be changed or extended according to the need. • **M :** XMPP is designed for sending messages in real time. It has very efficient push mechanism compared to other protocols. • **P :** It determines whether you are online/offline/busy. It indicates the state. • **P :** XMPP is a protocol, that is, a set of standards that allow systems to communicate with each other. **COAP** The CoAP protocol is specified in RFC 7252. It is a web transfer protocol which is used in constrained nodes or networks such as WSN, IoT, M2M etc. Hence the name Constrained Application Protocol. The protocol is targetted for Internet of Things (IoT) devices having less memory and less power specifications. As it is designed for web applications it is also known as "The Web of Things Protocol". It can be used to transport data from few bytes to 1000s of bytes over web applications. It exists between UDP layer and Application layer. Following are the features of CoAP Protocol: • It is very efficient RESTful protocol. • Easy to proxy to/from HTTP. • It is open IETF standard • It is Embedded web transfer protocol (coap://) • It uses asynchronous transaction model. • UDP is binding with reliability and multicast support. • GET, POST, PUT and DELETE methods are used. • URI is supported.	[4*2.5]	CO2	L2

• It uses small and simple 4 byte header.
• Supports binding to UDP, SMS and TCP.
• DTLS based PSK, RPK and certificate security is used.
• uses subset of MIME types and HTTP response codes.
• Uses built in discovery mechanism.

MQTT

MQTT stands for **Message Queuing Telemetry Transport**. MQTT is a machine to machine internet of things connectivity protocol. It is an extremely lightweight and publish-subscribe messaging transport protocol. This protocol is useful for the connection with the remote location where the bandwidth is a premium. These characteristics make it useful in various situations, including constant environment such as for communication machine to machine and internet of things contexts. It is a publish and subscribe system where we can publish and receive the messages as a client. It makes it easy for communication between multiple devices. It is a simple messaging protocol designed for the constrained devices and with low bandwidth, so it's a perfect solution for the internet of things applications.

Characteristics of MQTT

The MQTT has some unique features which are hardly found in other protocols. Some of the features of an MQTT are given below:

- It is a machine to machine protocol, i.e., it provides communication between the devices.
- It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.
- It does not require that both the client and the server establish a connection at the same time.
- It provides faster data transmission, like how WhatsApp/messenger provides a faster delivery. It's a real-time messaging protocol.
- It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.

HTTP

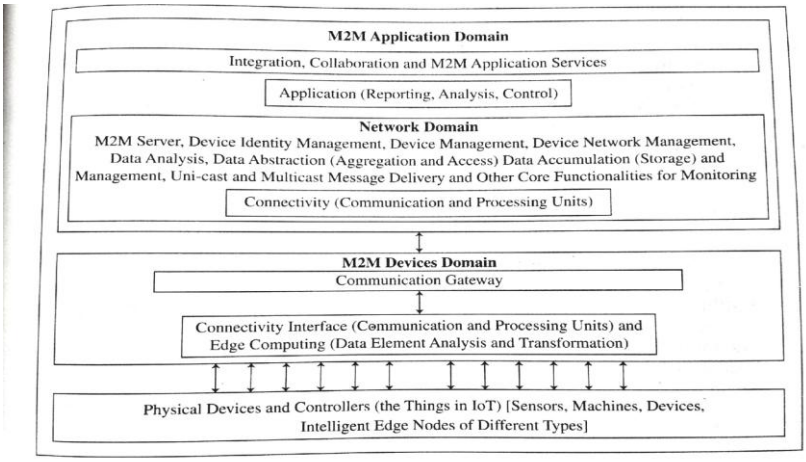
The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (i.e. internet) since 1990. HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) on the World Wide Web. The default port is TCP 80, but other ports can be used as well. It provides a standardized way for computers to communicate with each other. HTTP specification specifies how clients' request data will be constructed and sent to the server, and how the servers respond to these requests.

Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client waits for the response. The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only. Further requests are made on new connection like client and server are new to each other.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither

	the client nor the browser can retain information between different requests across the web pages.			
6	Explain three domains of M2M Architecture. What are the differences between IoT and M2M? Consists of three domains: • M2M Device Domain: Three entities physical devices, communication interface and gateway • M2M Network Domain consists of M2M server, device identity management, data analytics and data and device management • M2M Application Domain consists of applications for services , monitoring, analysis and controlling of devices networks  **Figure 1.9** Three domains of M2M architecture **M2M versus the IoT** 	M2M	IoT
---	---
M2M is about direct communication between machines.	The IoT is about sensors automation and Internet platform.
It supports point-to-point communication.	It supports cloud communication.
Devices do not necessarily rely on an Internet connection.	Devices rely on an Internet connection.
M2M is mostly hardware-based technology.	The IoT is both hardware- and software-based technology.
Machines normally communicate with a single machine at a time.	Many users can access at one time over the Internet.
A device can be connected through mobile or other network.	Data delivery depends on the Internet protocol (IP) network.			
7	Give five applications of IOT.	[10] [2*5]	CO1	L1

1. Smart Homes

One of the best and the most practical applications of IoT, smart homes really take both, convenience and home security, to the next level. Though there are different levels at which IoT is applied for smart homes, the best is the one that blends intelligent utility systems and entertainment together. For instance, your electricity meter with an IoT device giving you insights into your everyday water usage, your set-top box that allows you to record shows from remote, Automatic Illumination Systems, Advanced Locking Systems, Connected Surveillance Systems all fit into this concept of smart homes. As IoT evolves, we can be sure that most of the devices will become smarter, enabling enhanced home security.

2. Smart City

Not just internet access to people in a city but to the devices in it as well – that's what smart cities are supposed to be made of. And we can proudly say that we're going towards realizing this dream. Efforts are being made to incorporate connected technology into infrastructural requirements and some vital concerns like Traffic Management, Waste Management, Water Distribution, Electricity Management, and more. All these work towards eliminating some day-to-day challenges faced by people and bring in added convenience.

3. Self-driven Cars

We've seen a lot about self-driven cars. Google tried it out, Tesla tested it, and even Uber came up with a version of self-driven cars that it later shelved. Since it's human lives on the roads that we're dealing with, we need to ensure the technology has all that it takes to ensure better safety for the passenger and those on the roads.

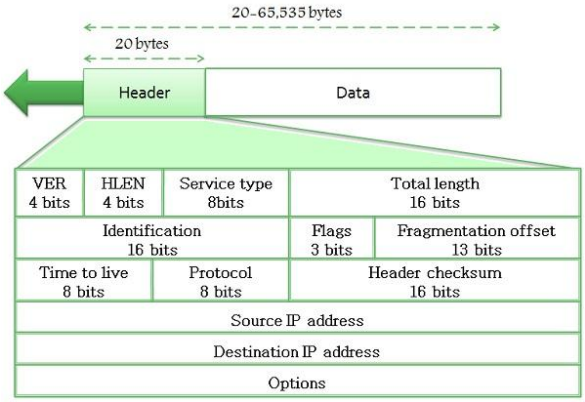
The cars use several sensors and embedded systems connected to the Cloud and the internet to keep generating data and sending them to the Cloud for informed decision-making through Machine Learning. Though it will take a few more years for the technology to evolve completely and for countries to amend laws and policies, what we're witnessing right now is one of the best applications of IoT.

4. IoT Retail Shops

If you haven't already seen the video of Amazon Go – the concept store from the eCommerce giant, you should check it out right away. Perhaps this is the best use of the technology in bridging the gap between an online store and a retail store. The retail store allows you to go cashless by deducting money from your Amazon wallet. It also adds items to your cart in real-time when you pick products from the shelves.

If you change your mind and pick up another article, the previous one gets deleted and replaces your cart with the new item. The best part of the concept store is that there is no cashier to bill your products. You don't have to stand in line but just step out after you pick up your products from shelves. If this technology is effective enough to fetch more patronage, this is sure to become a norm in the coming years.

5. Farming

	Farming is one sector that will benefit the most from the Internet of Things. With so many developments happening on tools farmers can use for agriculture, the future is sure promising. Tools are being developed for Drip Irrigation, understanding crop patterns, Water Distribution, drones for Farm Surveillance, and more. These will allow farmers to come up with a more productive yield and take care of the concerns better.			
8	Explain IPV4 and IPV6 with necessary figures An IP stands for internet protocol. An IP address is assigned to each device connected to a network. Each device uses an IP address for communication. It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets. Mainly, both the networks, i.e., IP and TCP, are combined together, so together, they are referred to as a TCP/IP. It creates a virtual connection between the source and the destination. We can also define an IP address as a numeric address assigned to each device on a network. An IP address is assigned to each device so that the device on a network can be identified uniquely. To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4). An IP address consists of two parts, i.e., the first one is a network address, and the other one is a host address. There are two types of IP addresses: ○ IPv4 ○ IPv6 What is IPv4? IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device. For example, **66.94.29.13**  Drawback of IPv4 Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses,	[10] [5+5]	CO2	L1

which are not enough for each device connected to the internet on a planet.

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.