Subject: IOT and Wireless Sensor Networks (18EC741) valuation scheme

Semester: VII

Submitted by:

Prof. A. S. Joshi

Asst. Prof.

Dept of ECE,

KLS VDIT, Haliyal

Submitted on: 29/03/2022

29.03.2022

Head of the Department
Dept. of Electronic & Communication Engg.
KLS V.D.I.T., HALIYAL (U.K.)

CBCS SCHEME

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

18EC741

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022
IoT and Wireless Sensor Networks

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. What is IoT? Explain conceptual framework of IoT with necessary equations and explain the reference model suggested by CISCO. **(08 Marks)**

b. What are three architectural domain functionalities in m2M architecture? Compare IoT with M2M. **(08 Marks)**

c. Explain Constrained Application Protocol (CoAP) for IoT/M2M. **(04 Marks)**

OR

2 a. Explain modified OSI model for the IoT/M2M systems with appropriate figures. **(08 Marks)**

b. Explain Message Queuing Telemetry Transport (MQTT) protocol with Pub/Sub model with proper figures. **(08 Marks)**

c. Write and explain four layer architectural framework developed at CISCO for a smart city. **(04 Marks)**

Module-2

3 a. Explain about cloud service and cloud development models with examples. **(08 Marks)**

b. Explain Internet Protocol version 4 (IPv4) and IP addressing in IoT. **(06 Marks)**

c. Explain HTTPs protocol. **(06 Marks)**

OR

4 a. Explain IoT cloud based data collection, storage and computing services using Nimbits. **(06 Marks)**

b. What is Cloud Computing? Explain the cloud service models with necessary figures. **(08 Marks)**

c. Explain 6LoWPAN with necessary figures. **(06 Marks)**

Module-3

5 a. Explain the importance of security in IoT. Explain briefly the security models used in IoT. **(08 Marks)**

b. Write a short note on IoT Security Tomography and explain layered attacker model. **(08 Marks)**

c. Write a short note on Arduino programming for IoT. **(04 Marks)**

OR

6 a. Explain about the security and threat analysis in IoT/M2M using neat figure. **(08 Marks)**

b. Explain layered attacker model with possible attacks and suggest the steps for mitigating attacks. **(08 Marks)**

c. Explain how data is read from sensors and devices. **(04 Marks)**

Module-4

7 a. Write a short note on operational states of a sensor node with different power consumptions with figure. **(10 Marks)**

b. Write a detailed note on Optimization goals and figure of merit for wireless sensor networks. **(10 Marks)**

OR

8 a. Write a note on embedded operating system suitable for WSN and explain about different programming paradigms. **(10 Marks)**

b. Explain the single node architecture with necessary hardware components. **(10 Marks)**

Module-5

9 a. Explain the crucial points influencing the physical layer of WSN. **(08 Marks)**

b. Explain Mediation Device Protocol with advantages and disadvantages. **(06 Marks)**

c. Explain the CSMA protocol with proper flow diagram. **(06 Marks)**

OR

10 a. Explain the S-MAC protocol and explain how it handles the major sources of energy inefficiency in WSN. **(08 Marks)**

b. What is geographical routing and explain about Greedy Perimeter Stateless Routing for wireless networks with proper figure. **(08 Marks)**

c. Explain Leach protocol with necessary figure. **(04 Marks)**

* * * * *

Karnatak Law Society's Vishwanathrao Deshpande Institute of Technology, Haliyal - 581 329	
Doc. No.: VDIT/ACAD/AR/05b	Rev.No.:01
Page 1	Rev. Dt: 25/03/2021
Solution and Scheme for award of marks	

Department: E&C **AY: 2021-22**
Subject with Sub. Code: IOT & WSN- 18EC741 **Semester / Division: 7 /A&B**
Name of Faculty: Prof. A S Joshi

Q.No.	Solution and Scheme	Marks
Q1 a) Ans	What is IoT ? Explain conceptual framework of IoT with necessary equations and explain the reference model suggested by CISCO Definition of IOT : Internet of Things (IOT) means a n/w of physical things (objects) sending, receiving or communicating informations using the internet or other communication technologies and network just as the computers, tablets and mobiles do, and thus permits the monitoring, coordinating or controlling process across the internet or another data network IOT conceptual frame work given below ① The first conceptual framework describes a simple conceptual framework of IOT & is given by "Physical object + controller, sensor & actuators + Internet = Internet of Things" — eqn ① This eqn ① conceptually describes the internet of umbrellas as consisting of an umbrella, a controller, sensor & actuators, and the internet for the connectivity to a web service and a mobile service provider ② "Gather + enrich + stream + manage + acquire + organise and analyse = Internet of things with connectivity to data centre, enterprise or cloud servers" — eqn ② This is an IoT conceptual framework for the enterprise processes and services, based on a sysse - sted IOT architecture given by Oracle. This eqn ② also tells that IoT framework of is used in no. of applications as well as in enterprise & business processes is therefore, in general, more complex than one represented by eqn ① & is given by eqn ② ③ "Gather + consolidate + connect + collect + assemble + manage & analyse = Internet of Things with connectivity to cloud services" — eqn ③	Def 2M Three eqns with meaning 3M

Q.No.	Solution and Scheme	Marks

Eqn" ③ is an alternative conceptual framework for a complex system. It is based on IBM IOT conceptual framework. The equation ② shows the actions & communication of data at successive levels in IOT. The framework manages the IOT services using data from internetwork of devices & objects, internet & cloud services and represents the flow of data from the IOT devices for managing the IOT services using the Cloud Server.

IOT reference model suggested by CISCO

- Level 7 – Collaboration & processes (involving people & business processes)
- Level 6 – Application (Reporting, Analysis & control)
- Level 5 – Data Abstraction (Aggregation & Access)
- Level 4 – Data Accumulation (Storage)
- Level 3 – Edge computing (data element analysis & Transformation)
- Level 2 – connectivity (comm & processing units)
- Level 1 – Physical devices & controllers (things in IOT) [sensors, machines, devices, intelligent edge nodes of different types]

IOT ref. model 3M

A reference model can be used to depict building blocks, successive interactions & integration

(b) What are the three architectural domain functionalities in M2M architecture? Compare IOT with M2M.

Ans Three architectural domain functionalities in M2M architecture are

i) M2M device domain – This domain consists of three entities - physical devices, communication interface & gateway. Comm. interface is a port or subsys., which receives input from one end & sends data received to another.

ii) M2M Network domain – This domain consists of M2M servers, device identity management, data analytics and data & device management similar to IOT arch. level.

iii) M2M Application domain – This domain consists of application for services, monitoring, analysis & controlling of device networks.

4M

Compare IOT and M2M

IOT technology involves the integration of complex physical machinery M2M communication with networks of sensors and uses analytics, machine learning and knowledge discovery software.

Three pts 4x1M = 4M

Q.No.	Solution and Scheme	Marks

→ M2M closely relates to IoT when the smart devices or M/Cs collect data which is transmitted via the Internet to other devices or machines located remotely.

→ The close difference between M2M & IoT is that M2M must deploy device to device, and carry out the coordination, monitoring, controlling of the devices & communicate without the usage of Internet whereas IoT deploys the Internet, Server, Internet protocols & Server or cloud end applications, services or processes.

1(c) Explain constrained Application protocol (CoAP) for IoT/M2M

Ans

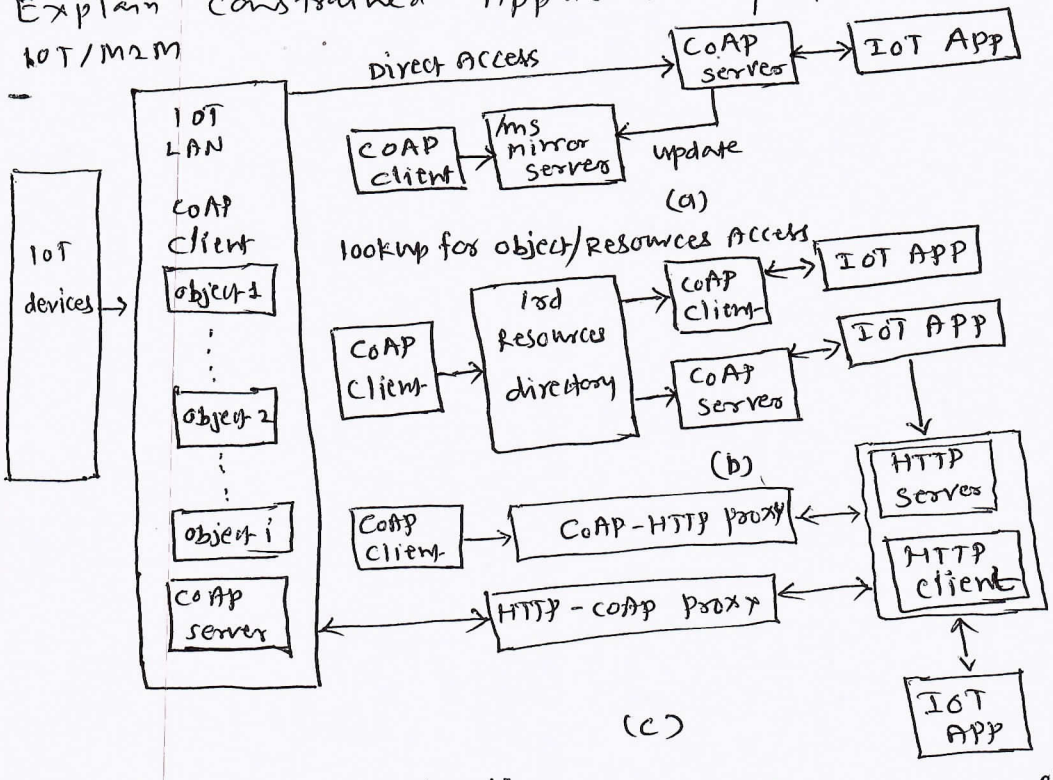


Fig (a) Direct Access / Indirect access of CoAP client objects to a CoAP Server

(b) CoAP Client access for lookup of object or resource using a resource directory (c) CoAP Client and server access using proxies

Def 1M

features 2M

fig 1M

Features: IETF recommends constrained Application protocol (CoAP) which is for CoRE using ROLL data network

(1) An IETF defined application - support layer protocol
(2) CoAP web-objects communicate using request / response interaction model.
(3) A specialised web - transfer protocol which is used for CoRE using ROLL network
(4) It uses object-model for the resources & each object can have single or multiple instances
(5) Each resource can have single or multiple instances

Q.No.	Solution and Scheme	Marks
2a) Ans	Explain modified OSI model for the IOT/M2M systems with appro-priate figures.	

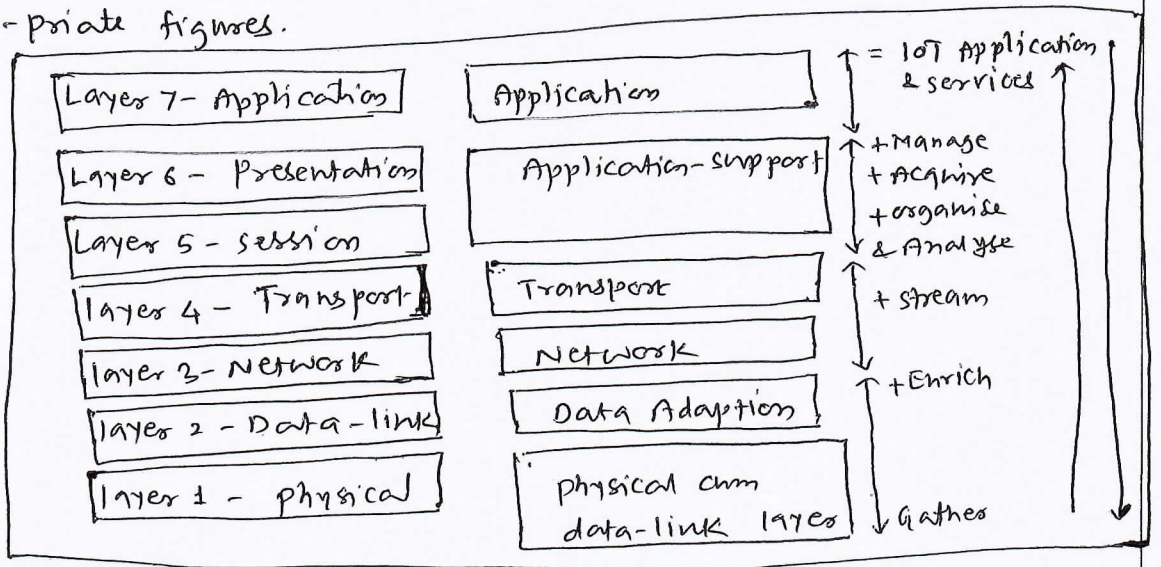


Fig shows a classical 7-layer OSI model on left and modification in that proposed by IETF in the middle. — fig 2M

→ Data communicates from device end to application end.
→ Each layer processes the received data & creates a new data stack which transfers it to the next layer.
→ New applications & services are present at the application layer 6
→ A modification to this is that the application-support layer 5 uses protocols, such as CoAP. IOT application and services commonly use them for n/w comm.
→ The CoAP protocol at the layer is used for the request/response interactions between the client & server on the n/w. — 6M
→ Similarly, the application-support layer may include processes for data managing, acquiring, organising & analysing which are mostly used by applications & services.
→ Modifications are also at data-link layer 2 (L2) & physical layer 1 (L1).
→ The new layers are data-adaptation (new L2) and physical cum data-link (new L1). The data-adaptation layer includes a gateway. The gateway permits communication between the devices n/w and web.
→ A physical IOT/M2M device h/d may integrate a wireless transceiver using a communication protocol as well as a data-link protocol for linking the data stacks of L1 & L2.

2b) Ans	Explain MQTT protocol with Pub/sub model with proper figures.	

Message Queuing Telemetry Transport- is an open-source protocol for machine-to-machine connectivity.

Q.No.	Solution and Scheme	Marks

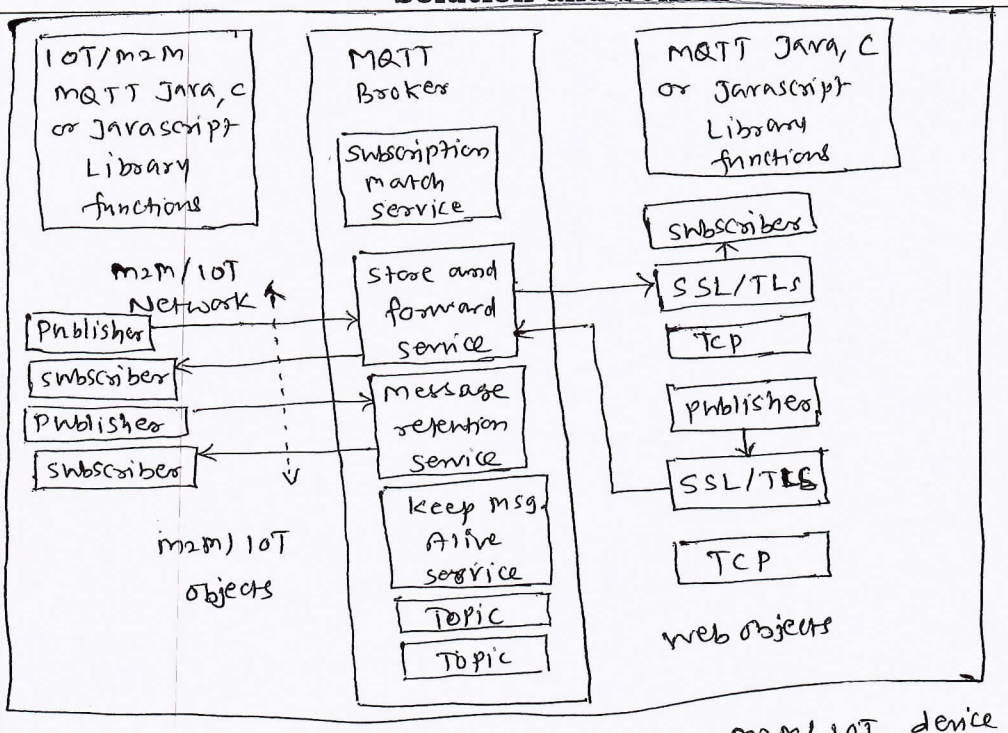


Fig 4M

Exp 4M

Fig: messages interChange between m2m/IOT device objects (publisher/subscribers) and web objects (pub/sub) using an MQTT Broker

→ IBM first created & donated it to m2m 'paho' Project object of Eclipse. A version is MQTT v3.1.1.

→ MQTT has been accepted as organization for the Advanced mem. of Structured Information Standards (OASIS) & MQTT protocol is used for Connectivity in m2m/IOT communication.

→ A version is MQTT-SN v1.2. Sensor networks & non-TCP/IP networks, such as ZigBee can use the MQTT-SN. MQTT-SN is also a pub/sub messaging protocol. It allows extension of the MQTT protocol for WSNs, the sensor & actuator devices & their nfws.

→ Fig shows MQTT-broker subscription, subscription match, store & forward, last good message retention and keep message alive services.

→ Fig also shows that device objects use MQTT Java, C or Javascript library functions.

→ The objects communicates using the connected devices nfw protocols such as ZigBee, web objects also use MQTT library functions & communicate using IP network and SSL & TSL security protocols for subscribing and publishing web APIs.

Q.No.	Solution and Scheme	Marks
2c)	Write and explain four layer architectural framework developed by at cisco for a smart city	
Ans	Layer 1 consists of sensors, sensor networks and devices network in parking spaces, hospitals and streets, vehicles banks, water supply, roads, bridges and rail roads. Bluetooth, ZigBee, NFC, WiFi are the protocols used at this layer. Layer 2 captures data at distributed computing points where data is processed, stored and analysed. Layer 3 is meant for central collection services, connected data centres, cloud & enterprise servers for data analytics applications Layer 4 consists of new innovative applications such as waste containers monitoring, WSNs for power loss monitoring, bike sharing management & smart parking.	1M/layer (4M)
3a)	Explain about cloud service & cloud deployment models with examples	08M
Ans	Cloud service/platform offers infrastructure for large data storage of devices, RFIDs, industrial plant machines, automobiles & device networks. Cloud service also offers computing capabilities, such as analytics, integrated development environment (IDE), collaborative computing & data store sharing	
	Cloud deployment models are :	Cloud deployment models 4M
	i) Public cloud — This model is provisioned by educational institutions, industries, govt. institutions or business or enterprises & is open for public use	Cloud service models 4M
	ii) Private cloud — This model is exclusive for use by institutions, industries, businesses or enterprises & is meant for private use in organisation by the employees & associated users only	
	iii) Community Cloud — This model is exclusive for use by a community formed by institutions, industries, businesses or enterprises, & for use within the community	

Q.No.	Solution and Scheme	Marks

organisation, employees & associated users. The community specifies security & compliance considerations

ID Hybrid cloud – A set of two or more distinct clouds with distinct data stores and applications that bind between them to deploy the proprietary or standard technology.

3b) Explain IPv4 & Ip addressing in IOT. — 06 M

Internet layer receives & forwards data to the next layer using IP version 4 or IPv6.

IP refers to the process when a packet transmits data. The transmission is acknowledged data flow. IP packet segment consists of the data which the Internet layer receives on transfer from the transport layer to the receiver end, when using the IP protocol.

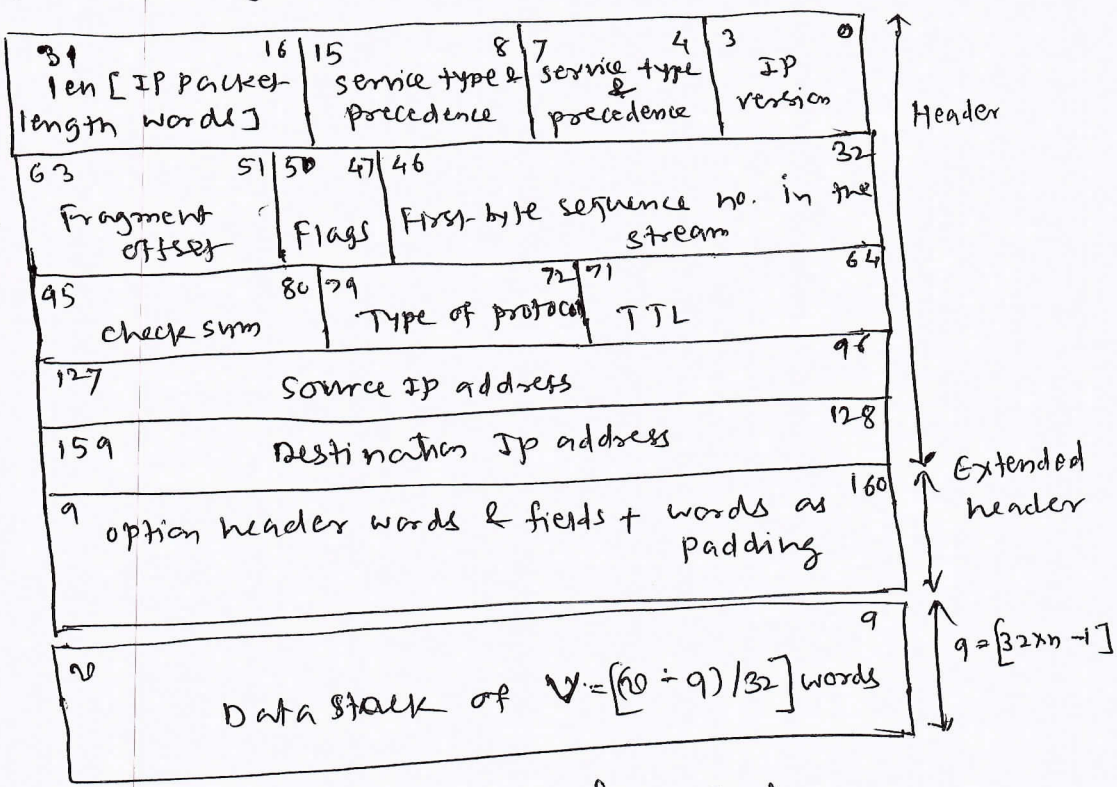


fig 2M

Data packet (stack) from or to transport layer = 2^{16} B

Exp 2M

fig: Data stack received or transmitted at or to n/w layer & Ip packet consisting of IP header field 160 bits & extended header upto bit q

Q.No.	Solution and Scheme	Marks
3b)	IP addressing in the IOT An IP header consists of source & destination addresses called IP addresses. The IPv4 addresses is used for Internet & IPv6 addresses are used by IOT/M2M. i) IP address – IPv4 consists of 32 bits. However it can be considered as four decimal nos. separated by dot for eg. 198.136.56.2 Each IP address can be between 0.0.00 to 255.255.255.255, total 2^{32} addresses due to 32-bit address ii) Static IP address – is the one assigned by the Internet service provider (ISP). ISP may provide an individual just one address or may provide class C network address consisting of a group of 254 IP addresses iii) Dynamic IP address – once a device connects to the Internet, it needs to be allotted an individual IP address. When device connects to a router, the router & device use the DHCP which assigns an IP address at an instance to the device. iv) DNS: It is Domain Names system is an application which provids an IP address for a corresponding service from the named domain service. eg of domain name .com, .org v) DHCP – Dynamic Host configuration protocol is a protocol to dynamically provide new IP addresses and set subnet masks for the connected node so that it can use the subnet server & subnet router at the Comm. framework vi) IPv6 – Devices (nodes) for IOT need large no. of addresses. IPv6 uses 128 bits address. eg 40a0:0acb:8a00:b372:0000:0000:0000:0000 IANA manages allocation process for IPv6 addresses	2d addressing 2M
3c)	Explain HTTPs protocol	06M
Ans	Hyper text transfer protocol (HTTP) is an application layer protocol. A pair uses a protocol for sending	

Q.No.	Solution and Scheme	Marks
	class hierarchy com.nimbits.server.system.serverInfo of java.lang.object.	
	Nimbits paas services offer the following features	
	I) Edge computing locally on embedded systems, built up of local applications. It runs the rules & pushes important data up to the cloud running when connected over the internet & an instance of a Nimbits server hosts at the device nodes which is then applied.	
	II) It supports multiple programming languages, including Arduino, new Arduino library, push functions from Arduino Cloud, Javascript, HTML or the Nimbits.io Java library.	
	III) Nimbits ~~function~~ server functions as a backend platform.	
	IV) It provides rule ~~engine~~ engine for connecting sensors, persons & software to the cloud one another	Nimbits features 1M x 6 = 6M
	V) It provides data logging service & access, & stores the historical data pts. & data objects.	
	VI) It filters the noise & important changes sent to another largers central instance	
	VII) It processes a specific type of data & can store it to	
	VIII) Time- or geo-stamping of the data	
	IX) data visualisation for data of connected sensors to IoT devices.	
	X) It deploys software on Google App Engine, any J2EE server on Amazon EC2 or on a Raspberry Pi.	
4b)	What is Cloud Computing? Explain Cloud service models with necessary figures.	08M
Ans	Cloud computing means a collection of services available over the internet. Cloud delivers computational functionality. Cloud computing deploys infrastructure of a cloud-service providers. The infrastructure deploys on a utility or grid computing or web services environment that includes n/w, sys., grid of computers or servers or data centres.	Defn 2M
	Cloud service models are:	
	(1) SaaS = software as a service	

Q.No.	Solution and Scheme	Marks
	& receiving messages. HTTP port number is 80. A web HTTP server listens to port 80 only & responds to port 80 only. An HTTP port sends application data stack at the output to the lower layer using the HTTP protocol. → An HTTP port uses a URL like http://www.mheducation.com/ → The default port is taken as 80. The port no. can be specified after Top Level Domain (TLD). → HTTPS (HTTP over secure socket Layer or TLS) port number is 443. An HTTPS port sends a URL. For eg. https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. → The port receives the data stack at the input at the receiver end. Each port at the application layer uses a distinct protocol. A port is assigned a no. according to protocol used for transmission & reception. Features of HTTP are :- 1) HTTP is the standard protocol for requesting a URL defined web-page resource, & for sending a response to the web server. An HTTP client requests an HTTP server on the internet & server responds by sending a response. The response may be with or without applying a process. 2) HTTP is a stateless protocol. This is because for an HTTP request, the protocol assumes a fresh request.	HTTP Exp 4M HTTPS & Ports 4M
4a)	Explain IOT cloud based data collection, storage and computing services using Nimbits.	06M
Ans	Nimbits enables IOT on an open source distributed cloud. Nimbits cloud Paas deploys an instance of Nimbits server at the device nodes. Nimbits functions as an m2m sys. data store, data collector & logger with access to historical data. Nimbits architecture is a cloud-based Google App Engine. Nimbits server is a	

Q.No.	Solution and Scheme	Marks
	The s/w is made available to an application or service on demand. SaaS is a service model where the applications or services deploy & host at the Cloud, and are made available through the internet on demand by the service user. The s/w control, maintenance, updation to new version & infrastructure, platform & resource requirements are the responsibilities of the cloud service provider iii) PaaS = platform as a service. The platform is made available to a developer of an application on demand. PaaS is a service model where the applications & services develop & execute using the platform which is made available through the internet on demand for the developer of the applications. The platform, network, resources, maintenance, updation & security as per the develop-ers requirements are the responsibilities of the cloud service provider. iii) IaaS = infrastructure as a service. The infra-structure (data stores, servers, data centres & n/w) is made available to a user or developer of application on demand. Developer installs the os image, data store & application & controls them at the infrastructure. IaaS is a service model where the applications develop. IaaS computing systems, network & security are the responsibilities of the cloud service provider. iv) DaaS = Data as a service. Data or a data centre is made available to a user or developer of applications on demand. DaaS is a service model where the data store or data warehouse is made available through the internet on demand on rent to an enterprise.	cloud service models 8M
4a) Ans	Explain 6LoWPAN with necessary figures. 6LoWPAN protocol is used as adaptation layer before a data stalk transmits to IPv6 internet	06M

Q.No.	Solution and Scheme	Marks

Ans layer.

→ The stack uses 6LoWPAN (IPv6 over Low power wireless personal Area Network) protocol at adaptation layer before the data stack transmits to IPv6 Internet layer.

→ An IEEE 802.15.4 WPAN device has a 6LoWPAN Interface serial port for connectivity.

→ 6LoWPAN is an adaptation-layer protocol for the IEEE 802.15.4 network devices. The device are the nodes having low speed & low power.

→ They are WPAN nodes of a multiple device mesh network.

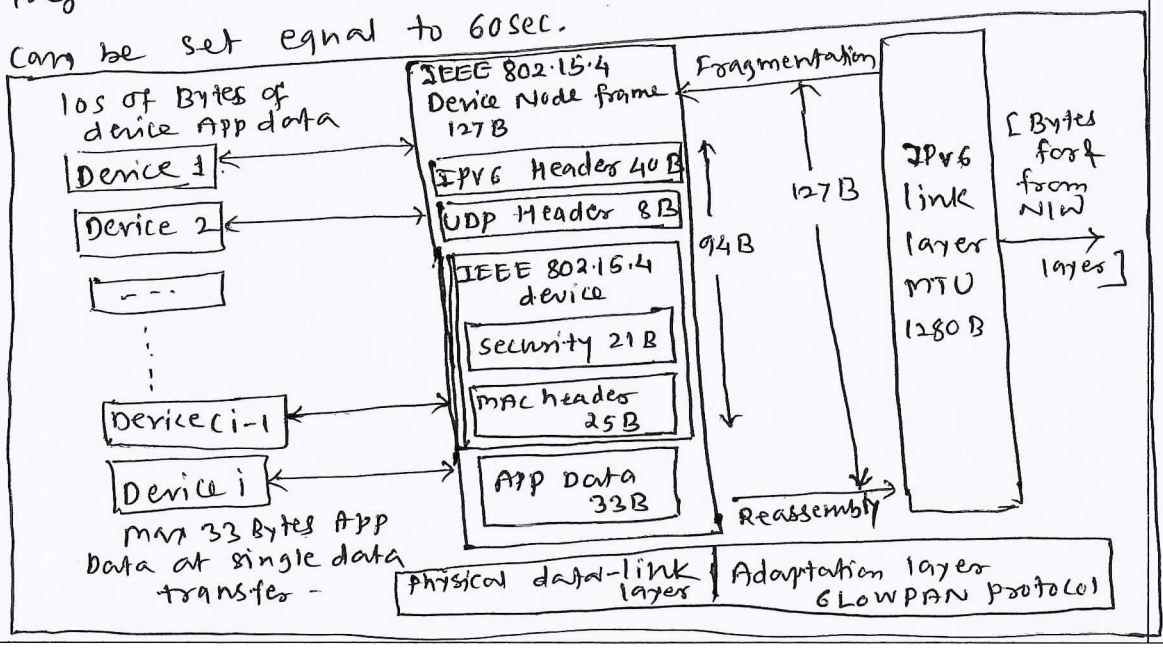
→ Low-power devices need to limit data size per instance. Data compression reduces data size. Fragmentation of data also reduces data size per instance.

6xp 2m

Features of 6LOWPAN :- (i) supports mesh routing (ii) header compression, fragmentation & reassembly. when data is fragmented before communication, the first fragment header has 27 bit which includes the datagram size (11 bits) & a datagram tag (16 bits). subsequent fragments have header 8 bit which include the datagram size, datagram tag and the offset. Fragments reassembly time limit can be set equal to 60sec.

features 2m

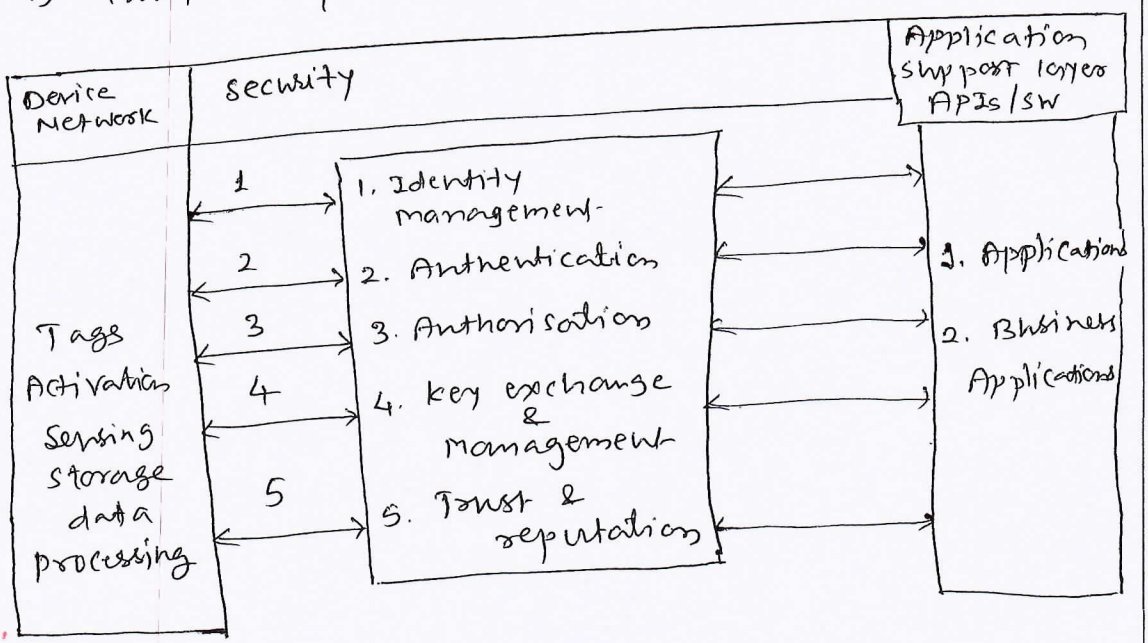
fig 2m



105 of Bytes of device App data

max 33 Bytes App Data at single data transfer -

Q.No.	Solution and Scheme	Marks
5a)	Explain importance of security in IOT. Explain briefly the security models used in IOT.	08M
Ans	A Security functional group contains five sets of functions which are reqd. for ensuring security & privacy. Five functional components of security are i) Identity management ii) Authentications iii) Authorisation iv) key exchange & management v) Trust & reputation	with explaination 4M

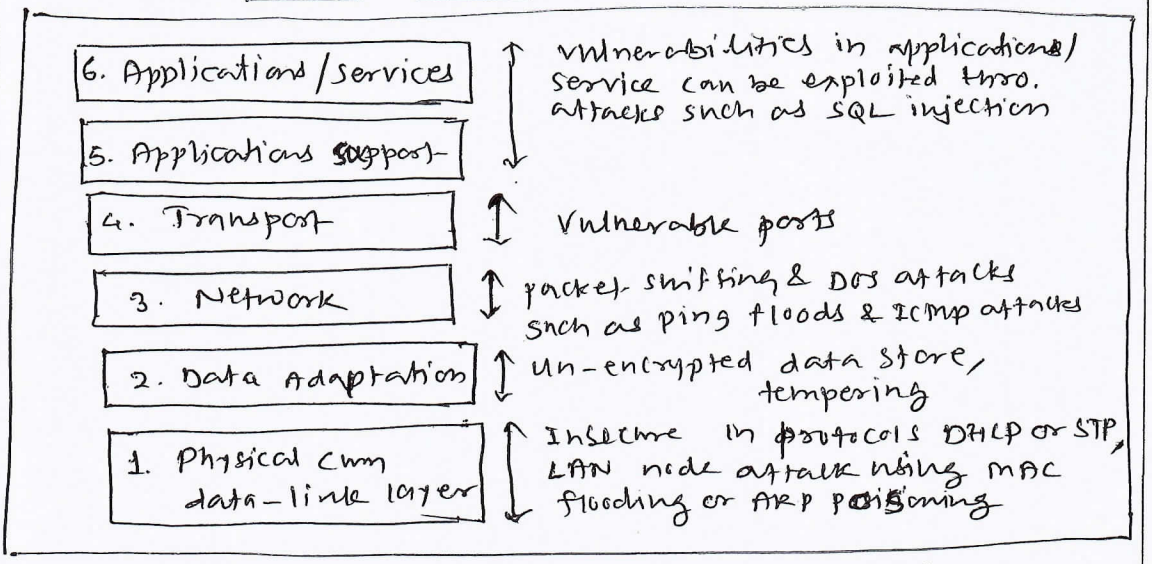


4M

5b)	Write a short note on IOT security Tomography and explain layered attacker model.	08M
Ans	Computational tomography means a computing method of producing a 3D picture of the internal structures of an object by observation & recording of the differences in effects on passage of ~~en~~ energy waves impinging on those structures. Computational security in complex set of n/w's utilises the n/w tomography procedures of identifying the n/w vulnerabilities. This permits design of efficient attack strategies.	Tomography Defn & explaination 4M

Q.No.	Solution and Scheme	Marks

layered Attacker model



Attacker model 4M

5c Ans → Arduino programming for IOT - short note — 04M

→ Arduino board can be programmed using avr-gcc tools. — 1M

→ The Arduino board has a pre-installed bootloader embedded into the firmware

→ Arduino programmes develops the codes using a graphical cal cross-platform IDE. Arduino provides simplicity, → The board connects to a computer which runs the IDE

→ Bootloader pgm hands overs the control & allows running of the loaded, which loads the required os functions & s/w into the sys. h/w & networking capabilities into the board. — 1M

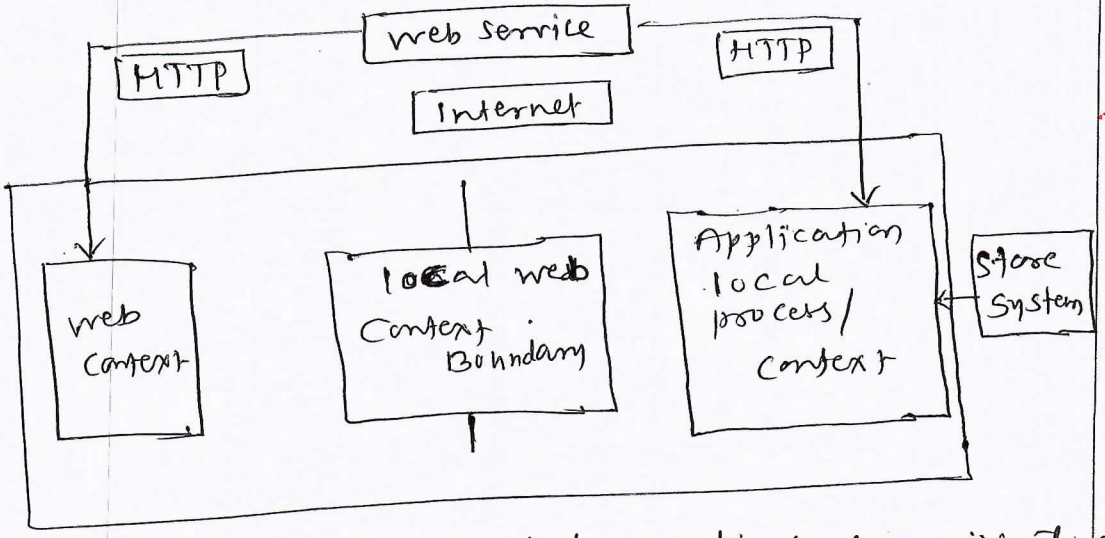
→ The Arduino bootloader provisions for multitasking. by the usage of interrupt handling functions for each task

→ IDE consists of set of s/w modules which provide s/w & H/w environment for developing & prototyping the s/w for a specific device platform. — 1M

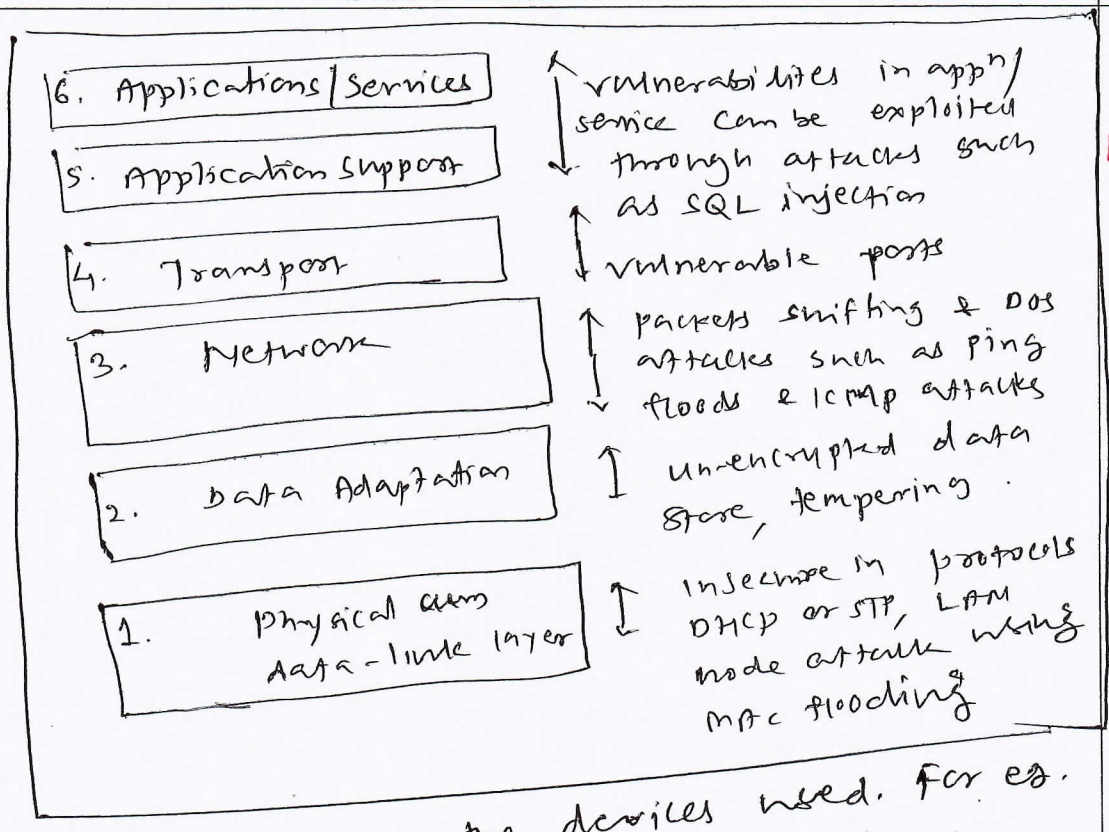
→ Bootloader allows the computer to push the developed codes into a board using the Arduino IDE through a USB cable or labelled serial port.

→ Arduino IDE is available from the website of Arduino. A programmer downloads the required IDE version. IDE runs on the computer & permits the development of the codes, their simulation & upload on to the device platform

→ Arduino IDE includes a C/C++ library. — 1M

Q.No.	Solution and Scheme	Marks
6a) Ans	Explain about the security & threat analysis in IOT/M2M using neat figure Security requirements – IOT reference architecture means a guide for one or more concrete architects. IOT ref. arch. is a set of 3 architectural views – functional, information & deployment & operational. Security FG (functional groups) contains five sets of functions which are reqd. for ensuring security & privacy. Five functional components are – i) Identity management ii) Authentication iii) Authorisation iv) Key exchange & management v) Trust & reputation	4M
	Threat analysis – → A threat analysis tool first generates the threats & analyses the system for threat(s). → Threat analysis means uncovering the security design flaws after specifying the stride category, data flow diagram, elements between that the interactions occuring during the stride & processes which are activated for analysis. Fig below shows the case of a threat-analysis tool for analysis during a stride.	Threat model & Threat analysis 4M
		
6b)	Following are the suggested solutions for mitigating the attacks on the layers Layer 1 Attacks solution	

Q.No.	Solution and Scheme	Marks



Layered attacker model 2M

Solution depends on the devices used. For eg. link-level provisioning of security uses — BT-LE link level AES-CCM 128 authenticated encryption algorithm for confidentiality & authentication, and ZigBee at link-level security using AES-CCM-128.

Layer 2 Attacks solution

programming the n/w switches to prevent internal node attacks during use of DHCP or STP. Additional controls may include ARP inspection, disabling unused ports & enforcing effective security an virtual LAN to prevent VLAN hopping.

LWM2M OMA specification for device gateway to the Internet has provisions for MAS for security, root key, data store, and devices & data authentication

Attack solutions for 6 layers 6M

Layer 3 Attacks solution : use of tamper resistant router, use of packet filtering & controlling routing messages & packets data between layers 3 & 4 through a firewall reduces the risks.

Q.No.	Solution and Scheme	Marks
	Layer 4 Attacks solution port scanning method is a solution which identifies the vulnerable port. A solution is the opening of new ports and configuring effectively the firewall, and locking down ports only to those required. A solution is DTLS between layers 5 and 4. Layers 5 & 6 Attacks solution Above layer 4, we are looking primarily at application-level attacks which are results of poor coding practices.	04M
6 c)	Explain how data is read from sensors & devices	
Ans	1) Using ADC Analog input 2) Using the software serial libraries & their usage for data communication using serial bus protocols UART, I2C, USB & CAN 3) Using s/w serial library 4) Using I2C serial protocol 5) Using cloud library at xively 6) Using an OS 7) Using threads 8) Using Real-time Thread scheduling library 9) Using GNU C-library version	Any four 1M×4 =4M
7 a)	write a short note on operational states of a sensor node with different power consumptions with figure	10 M
Ans	Typical operational states of a sensor node are → active → idle → sleep WRT energy supply for a sensor node is at a premium: batteries have small capacity & recharging by energy scavenging is complicated & volatile.	1M

Q.No.	Solution and Scheme	Marks
⇒	many components of energy consumption are controller, radio front ends, to some degree the memory and depending on the type of the sensors.	1m
→	As per observation most of the time wireless sensor node has nothing to do. Hence it is best to turn off. Naturally it should be able to wake up again, on the basis of external stimuli or on the basis of time. Therefore, completely turning off a node is not possible but rather its operational state can be adapted to the tasks at hand.	1m
⇒	Introducing and using multiple states of operation with reduced energy consumption in return for reduced functionality is the core technique for energy-efficient wireless sensor node	1m
→	Different models usually support different nos. of such sleep states with different characteristics	3m
→	For microcontroller, typical states are active, idle and sleep. a radio modem could turn transmitter receiver or both on or off. sensors and memory could also be turned on or off	

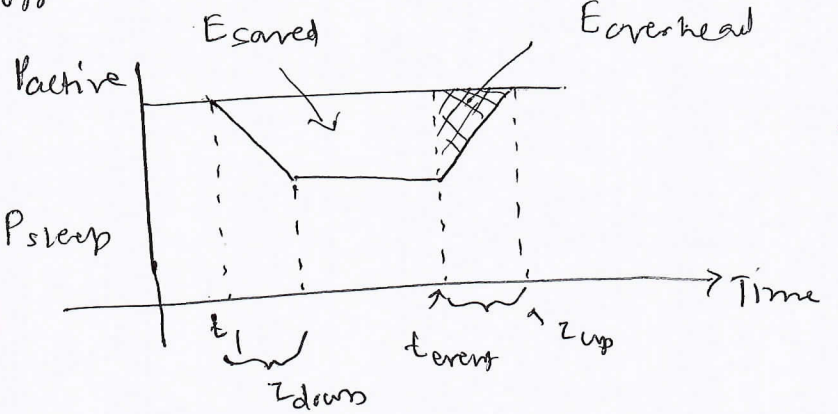


fig 2m

fig: Energy saving & overheads for sleep modes

→	At time t_1 the decision whether or not a component is to be put into sleep state/mode should be taken to reduce power consumption from P_{active} to P_{sleep}.	1m

Q.No.	Solution and Scheme	Marks
	If it remains active & next event occurs at time t_{event}, then total energy of P_{active} = $P_{active}(t_{event} - t_1)$ has be spent uselessly idling.	
→	putting the component into sleep mode, on the other hand, requires a time τ_{down} until sleep mode has been reached.	
	Avg power consumption during this phase $= (P_{active} + P_{sleep})/2$	1M
	Then P_{sleep} is ~~consump~~ consumed until t_{event}.	
	In total $\tau_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down})$	
	$\times P_{sleep}$ energy is required in sleep mode as opposed to $(t_{event} - t_1) P_{active}$ when remaining active.	
	The energy saving is thus	
	$E_{saved} = (t_{event} - t_1) P_{active} - (\tau_{down}(P_{active} + P_{sleep})/2$	
	$+ (t_{event} - t_1 - \tau_{down}) P_{sleep})$	1M
	once the event to be processed occurs, an additional overhead of	
	$E_{overhead} = \tau_{up}(P_{active} + P_{sleep})/2$	
7(b)	Write a detailed note on optimization goals & figure of merit for WSNs	10m
Ans	1> Quality of service –	
	WSNs differ from other conventional comm. networks mainly in the type of service they offer. These nws essentially only move bits from one place to another.	

Q.No.	Solution and Scheme	Marks

But just like in tradional hlns, high-level QoS attributes in WSNs highly depend on the application. Some generic possibilities are:

→ Event detection/reporting probability
→ Event classification error
→ Event detection delay
→ missing reports
→ Approximation accuracy
→ tracking accuracy

3M

2) Energy efficiency

The term energy efficiency is, in fact, rather an umbrella term for many different aspects of a system, which should be carefully distinguished to form at actual, measurable figures of merit. The most commonly considered aspects are:

→ Energy/correctly received bit
→ Energy/reported event
→ Delay/energy trade-offs
→ Network lifetime
  i) Time to first node death
  ii) Network half-life
  iii) Time to partition
  iv) Time to loss of coverage
  v) Time to failure of first event notification

3M

3) Scalability - The ability to maintain the performance characteristics irrespective of the size of the network is referred to as scalability. With WSN potentially consisting of thousands of nodes, scalability is an evidently indispensable requirement.

The need for extreme scalability has direct consequences for the protocol design.

2M

Q.No.	Solution and Scheme	Marks
	4) Robustness - Related to QoS & somewhat also to scalability requirements, WSNs should also exhibit an appropriate robustness. They should not fail just because a limited number of nodes run out of energy, or because their environment changes & severs existing radio links between two nodes - if possible, these failures have to be compensated for for example by finding other routes	2M
8a)	write a note on embedded OS suitable for WSN & explain about different programming paradigms.	
Ans	The traditional tasks of OS are controlling & protecting the access to the resources (including support for i/p/o/p) and managing their allocation to different users as well as the support for concurrent exe. of several processes & communication between these processes. These tasks are only partially required in an embedded system as the executing code is much more restricted & usually much better harmonized than in a general-purpose sys.	embedded OS 4M
	An OS or an execution environment for WSNs should support the specific needs of these systems In particular, the need for energy-efficient execution requires support for energy management, Also the external components (sensors, timers etc) should be handled easily & efficiently.	
	programming paradigms	
	① Concurrent programming One of the first questions for a programming paradigm is how to support concurrency. Such support for concurrent execution is crucial for WSN nodes as they have to handle data continuously from	

Q.No.	Solution and Scheme	Marks

arbitrary sources — for eg. multiple sensors or radio transceiver - at arbitrary point in time.
For eg. a sys could poll a sensor to decide whether data is available and process the data right away, then poll the transceiver to check whether a packet is available and then immediately process the packet & so on
Such a sequential model would run the risk of missing data while a packet is processed or missing a packet when a sensor information is processed,

Correctly event-based 2M

Concurrent prog 2M

process-based concurrency —
most modern, general-purpose operating systems support concurrent execution (MPE) of multiple proce -sses on a single CPU. Hence such a process-based approach would be a first candidate to support concurrency in a sensor node as well

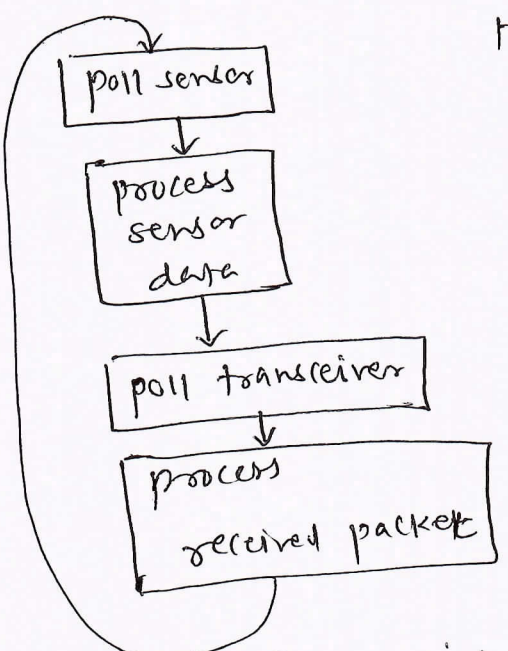


fig (a) Sequential programming model

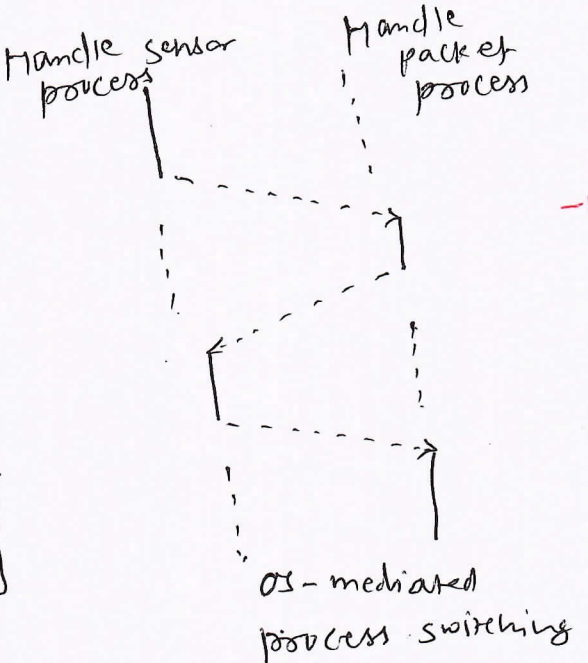


fig (b) process-based programming model

process -based 2M

Fig (b) shows this approach works in principle, mapping such an execution model of concurrent processes to a sensor node shows, however, that there are some granularity mismatches.

Q.No.	Solution and Scheme	Marks

Event-based programming -

To overcome the problem of process-based programming somewhat different programming model seems preferable. The idea is to embrace the reactive nature of a new node & integrate it into the design of OS. The sys. essentially waits for any event to occur/happen, where an event typically can be the availability of data from a sensor, the arrival of packet, or expiration of a timer. such an event is then handled by a short sequence of instructions that only stores the fact that this event has occured & stores necessary information. This

event-based 2M

The actual processing of information is not done in these event handler routines, but separately, decoupled from the actual appearance of events.

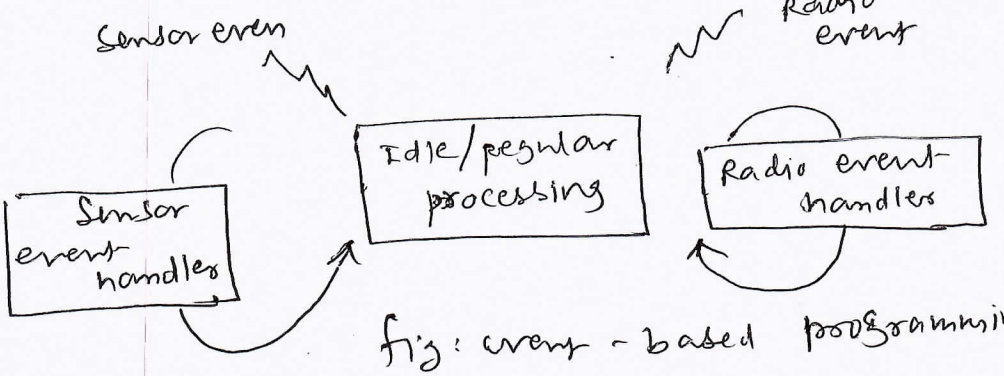


fig: event-based programming model

8b) Explain single node architecture with necessary hardware components

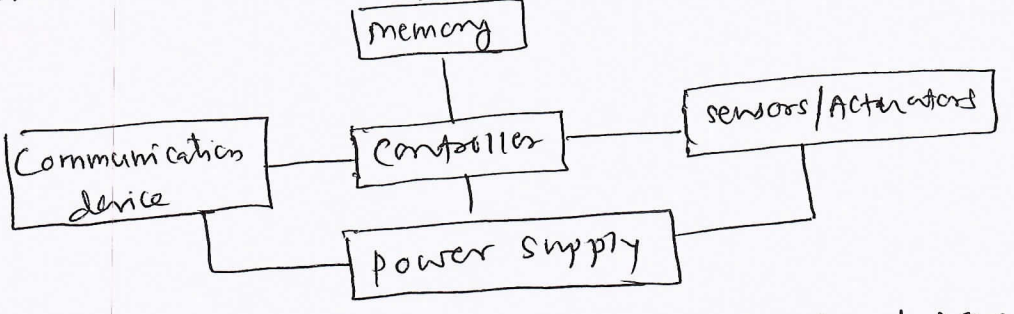


fig: overview of main sensor node hardware components/architecture

Q.No.	Solution and Scheme	Marks

Controller – A controller to process all the event data, capable of executing arbitrary code
eg. microcontrollers, FPGAs, ASICs, msp 430, Intel strongARM, Texas Instruments msp 430, Atmel ATmega

Memory – Some memory to store programs & intermediate data, usually different types of memory (ROM, EEPROM, RAM) are used for programs & data

Sensors and Actuators – The actual interface to the physical world: devices that can observe or control physical parameters of the environment
passive, omnidirectional sensors, passive, narrow-beam sensors, Active sensors

Communication – Turning nodes into a network requires a device for sending & receiving information over a wireless channel
choice of transmission medium
Transceivers

power supply – To provide energy some form of batteries are necessary. sometimes some form of recharging by obtaining energy from the environment is available as well.

Fig 1M + Explain each component with example 5×2M =10M

9a) Explain the crucial points influencing the physical layer of WSN

Ans crucial points:

→ Low power consumption
→ Low degree of mobility
→ Comparably low data rates
→ Low implementation complexity & costs
→ A small form factor for the overall node
→ As one consequence: small transmit power & thus a small transmission range

Crucial points 1M×4 =4M

Q.No.	Solution and Scheme	Marks
	→ As a further consequence : low duty cycle. most h/d should be switched off or operated in a low-power standby mode most of the time.	
	Influencing factors :	Influencing factor 1M×4 =4M
	→ Energy usage profile	
	→ Choice of modulation scheme	
	→ Dynamic modulation scaling	
	→ Antenna considerations	
(b)	Explain mediation device protocol with advantages & disadvantages	
Ans	mediation device protocol is compatible with the peer-to-peer communication mode of the IEEE 802.15.4 low-rate WPAN standard.	
	→ it permits each node in a WSN to go into sleep mode periodically and to wake up only for short times to receive packets from neighbor nodes.	Explaination 3M
	→ There is no global time reference, each node has its own sleeping schedule, and does not take of its neighbors sleep schedules	
	→ upon each periodic wakeup, a node transmits a short query beacon, indicating its node address & its willingness to accept packets from other nodes. The node stays awake for some short time following the query beacon, to open up window for incoming packets. If no packet is received during this window, the node goes back into sleep mode.	
	→ when a node wants to transmit a packet to a neighbor, it has to synchronize with it. The dynamic synchronization approach solves this problem without requiring the TX to be awake permanently to detect the destinations query-beacons.	

Q.No.	Solution and Scheme	Marks
	To achieve this mediation device (MD) is used. Advantages i) It does not require any synchronization between the nodes, only the MD has to learn the periods of the nodes. ii) The protocol is asymmetric in the sense that most of the energy burden is shifted to the MD, which so far is assumed to be power unconstrained. Drawbacks (i) The nodes transmit their query beacons without checking for ongoing transmissions and, thus, the beacons of different nodes may collide repeatedly when nodes have the same period & their wakeup periods overlap. If the wakeup periods are properly randomized & the node density is sufficiently low, this collision probability can be low too. However, in case of higher node densities, the no. of collisions can be significant. OR Fig 2M + Exp 2M + Adv 1M + Disadv 1M = 6M	2M 1M

Q.No.	Solution and Scheme	Marks
9c) Ans	Explain CSMA protocol with proper flow diagram In contention-based protocols, a given transmit opportunity toward a receiver node can in principle be taken by any of its neighbors. If any one neighbor tries its luck, the packet goes through the channel. If two or more neighbors try their luck, these have to compete with each other and in unlucky cases; eg. due to hidden-terminal situations, a collision might occur, wasting energy for both TX & RX.	

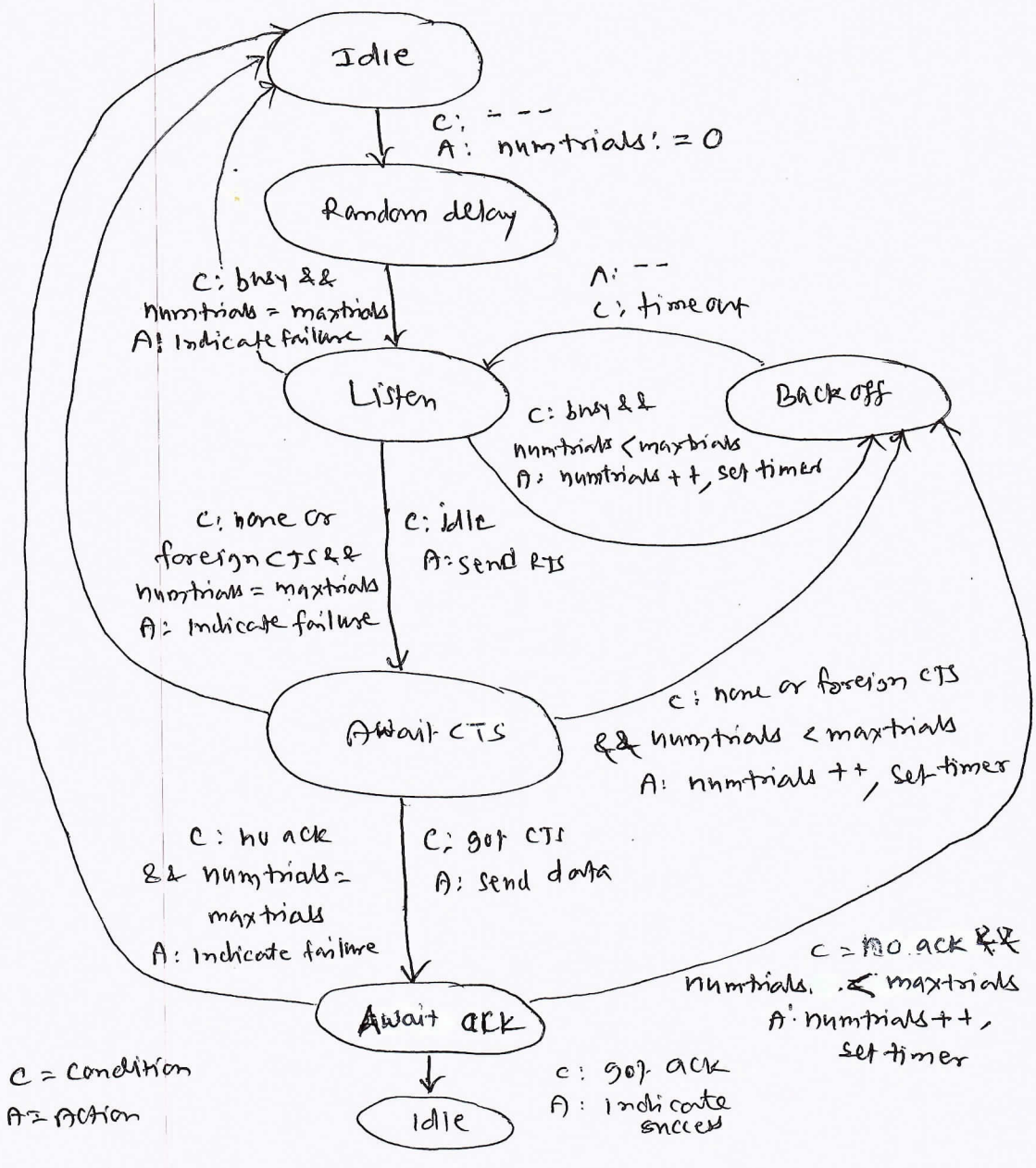


Fig 4M

fig: schematic of the CSMA protocol

Q.No.	Solution and Scheme	Marks

The above fig shows the several steps a node passes through in case of a Tx^n as a finite state automaton.

→ After a node gets a new packet for Tx^n from its upper layers, it starts with random delay & initializes its trials counter num_retries with zero. ~~a node get a new packet for~~ The purpose of the random delay is to desynchronize nodes that are initially synchronized by the external event.

→ During this random delay, nodes transceiver can be put into sleep mode.

→ During the following listen period, the node performs carrier sensing. If the medium is found to be busy & the no. of trials so far is smaller than the max. number, the node goes into the back-off mode.

Explanation 4M

→ In the back-off mode, the node waits a random amount of time, which can depend on the number of trials and during which the node can sleep.

→ Back-off mode can also be used by the application layer to initialize a phase change for its locally generated periodic traffic

→ After the back off finishes, the node listens again.

→ If the medium is busy & node has exhausted its max. no. of trials, the packet is dropped.

→ If the medium is idle, the node transmits an RTS packet & enters the "Await CTS" state, where it waits for the corresponding CTS packet.

→ In case no CTS packet arrives or a CTS packet for another transaction is received, the node either enters the back off mode or drops the packet, depending on the value of num_retries.

→ If the CTS packet arrives, the node sends its data

Q.No.	Solution and Scheme	Marks

packet and waits for an acknowledgement. This acknowledgement can be either an explicit acknowledgement packet, or the parent node piggybacks the acknowledgement on a packet that it forwards to the node's grandparent

10(a) Explain the S-MAC protocol & explain how it handles major sources of energy inefficiency in WSN

Ans S-MAC protocol provides mechanisms to circumvent idle listening, collisions and overhearing. As opposed to STEM (Sparse Topology & Energy management) Sensor-MAC (S-MAC) it does not require two different channels.

→ S-MAC adopts a periodic wakeup scheme, that is, each node alternates between a fixed-length listen period & fixed-length sleep period according to its schedule, compare fig (a) shown below

S-MAC (Def^n + explanation with + fig) 4 M

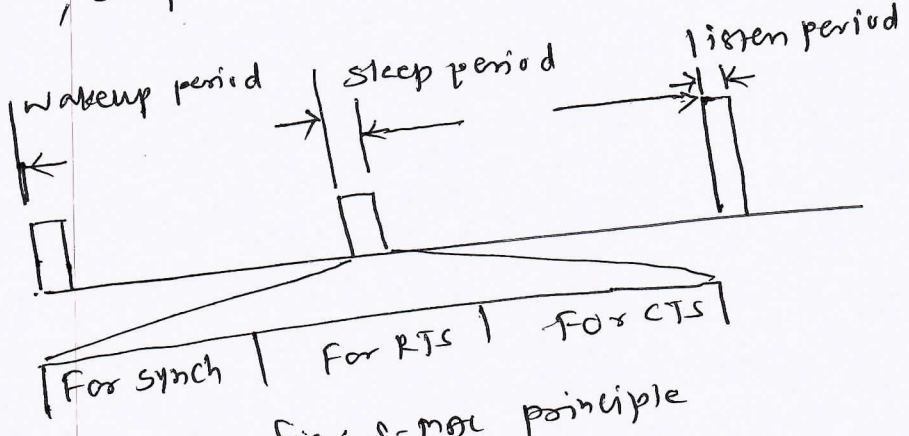


fig: S-MAC principle

→ However as opposed to STEM, the listen period of S-MAC can be used to receive and transmit packets.

→ S-MAC attempts to coordinate the schedules of neighboring nodes such that their listen periods start at the same time.

→ A node x's listen period is subdivided into three

Q.No.	Solution and Scheme	Marks
	different phases: i) SYNCH phase – In which node x accepts SYNCH packets from its neighbors. ii) In RTS phase – x listens for RTS packets from neighboring nodes iii) In CTS phase – node x transmits a CTS packet if an RTS packet was received in the previous phase	Three phases 2M
	Major sources of energy inefficiencies are i) Collisions – collisions incur useless receive costs at the destination node, useless transmit costs at the source code, & the prospect to expend further energy upon packet transmission. ii) overhearing iii) protocol overhead iv) Idle listening –	four sources of energy inefficiencies 2 M
10 b)	what is geographical routing & explain about Greedy perimeter stateless Routing for wireless networks with proper figure	08 M
Ans	Geographic routing The idea behind the relatively large class of geographic routing protocols is twofold: (i) For many applications, it is necessary to address physical locations, for example, as "any node in a given region" or "the node at/closet to a given point", when such requirement exists, they have to be supported by a proper routing scheme (ii) When the position of source & destination is known as are the positions of intermediate nodes, this information can be used to assist in the routing process. To do so the destination node has to be specified either geographically	GPSR with fig 4M

Q.No.	Solution and Scheme	Marks

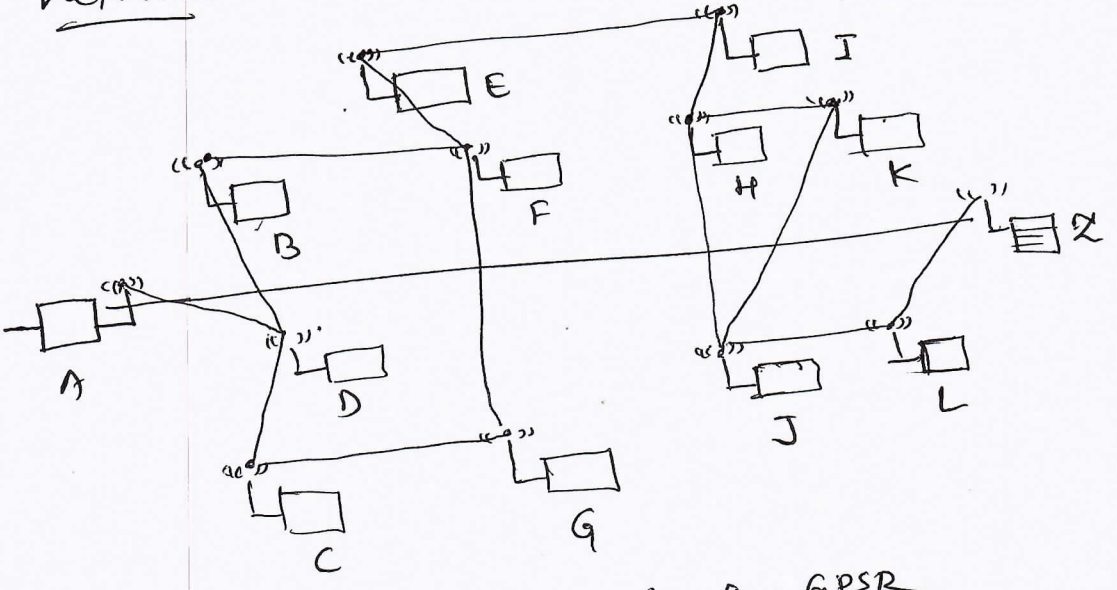
or as some form of mapping - a location service - between an otherwise specified destination & its current position is necessary.

The first aspect - sending data to arbitrary nodes in a given region - is usually referred to as geocasting.

The second aspect is called position-based routing

→ In wireless sensor networks, usually the geocasting aspect of geographic routing is considerably more important. Since nodes are considered as interchangeable and are only distinguished by external aspects, in particular their position, a location service is usually not necessary.

Greedy perimeter stateless Routing for wireless networks



1M

fig @ example for GPSR

Pure.

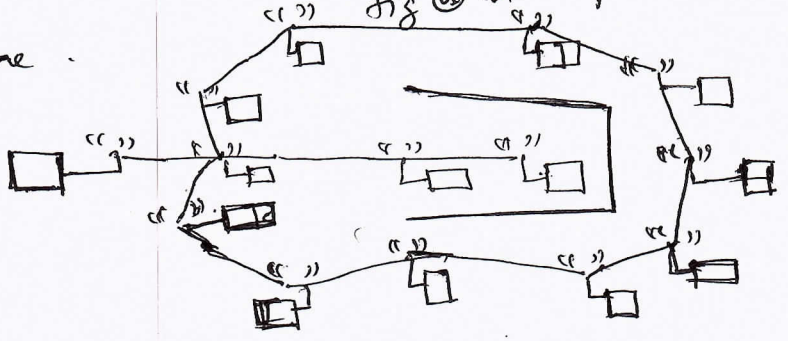


fig (b)

1M

Q.No.	Solution and Scheme	Marks
	Fig (b) Simple greedy geographic forwarding fails in presence of obstacles The fig (b) shows, this heuristic can lead to packets looping back and forth between the nodes near the obstacle The obstacle problem is not solved by randomly choosing a node that is closer to the destination than the transmitter. Right-hand rule to recover greedy routing – GPSR fig (a) not only illustrates the problem of greedy forwarding in dead ends but also gives an intuition about a possible solution. Fig (a) illustrates how a packet should be routed from node A to node 2. While at node A, packet can greedily forwarded to node D. At node D greedy forwarding fails, so the packet has to be routed around the perimeter of the interior face defined by BFGCD. That is, it is forwarded to 3 & from there to F. there, edge FG intersects line D2 & routing can proceed to the next face. The packet proceeds around the perimeter of the exterior face via E & I to H. from there via K to J & then to L & 2.	Expl + fig 4 m
10(c)	Explain Leach protocol with necessary figures.	

Q.No.	Solution and Scheme	Marks

Low-energy Adaptive clustering Hierarchy (LEACH)

LEACH partitions the nodes into clusters & in each cluster a dedicated node, the clusterhead, is responsible for creating & maintaining a TDMA schedule, all other nodes of a cluster are member nodes.

To all member nodes, TDMA slots are assigned, which can be used to exchange data between the member and the clusterhead, there is no peer-to-peer communication with the exception of their time slots, the members can spend their time in sleep state. The clusterhead aggregates the data of its members and transmits it to the sink node or to other nodes for further relaying.

The protocol is organized in rounds & each round is subdivided into a setup phase and a steady-state phase

The state phase starts with the self-election of nodes to clusterheads.

In the following advertisement mode/phase, the clusterheads inform their neighborhood with an advertisement packet.

4M

34

Q.No.	Solution and Scheme	Marks

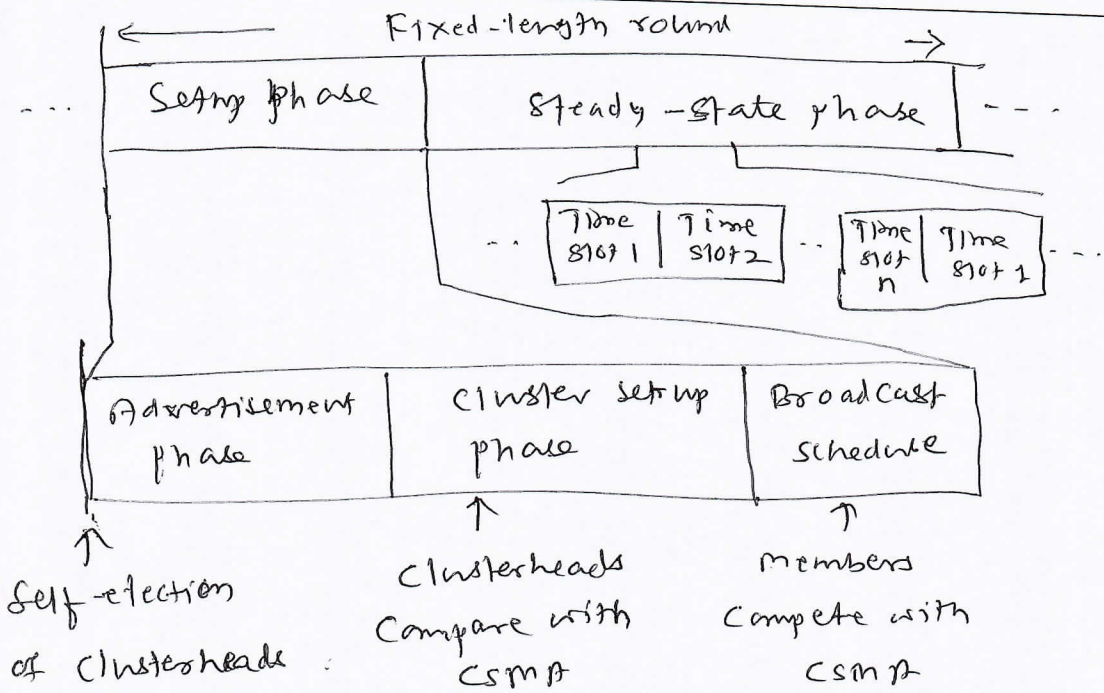


Fig 2M

fig: organization of LEACH rounds — 2m