Unit-I

ADHOC NETWORKS - INTRODUCTION AND ROUTING PROTOCOLS

Wireless Networks:

→ Wireless Networks are computer Networks that are not connected by cables

→ It avoids the costly process of introducing cables into buildings

→ The information is transmitted through air without cable or wires, by using electromagnetic waves like IR, RF, satellite etc.

→ eg. IR wireless communication, broadcast radio, microwave, bluetooth zigbee.

Elements of ADHOC Wireless Networks

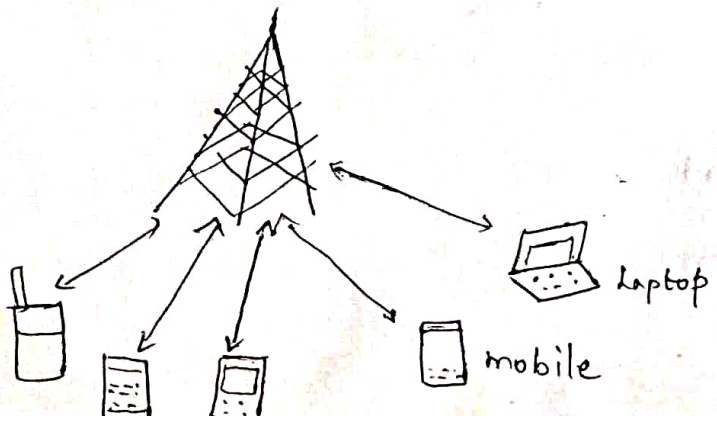
Wireless LAN is divided into

Infrastructure network (cellular)

Infrastructureless network (adhoc)

Infrastructure network:

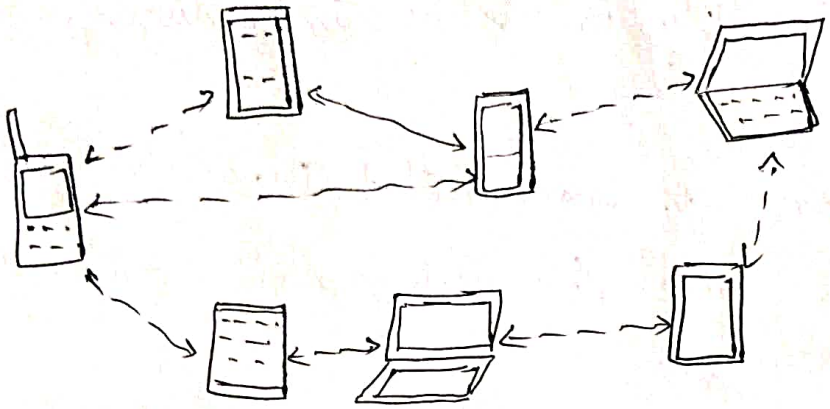
→ contains special nodes called Access Point (AP) which are connected via existing wired network AP and can interact with wired and wireless node



Infrastructureless network (adhoc)

→ Adhoc wireless network do not need any fixed infrastructure like Access Point and base station.

→ The nodes of this network can be mobile and They support multihop routing.



Wireless adhoc Network

→ Peer nodes does not require take part in transmitting packets

→ They are self organising and self configuring

→ It is useful to setup network fast at the time of emergency and relief operations

→ No access to network infrastructure

→ Not much planning is afforded to setup the network

Depending on topology and deployment, Adhoc network is classified into

i) Homogenous network

ii) Heterogenous network

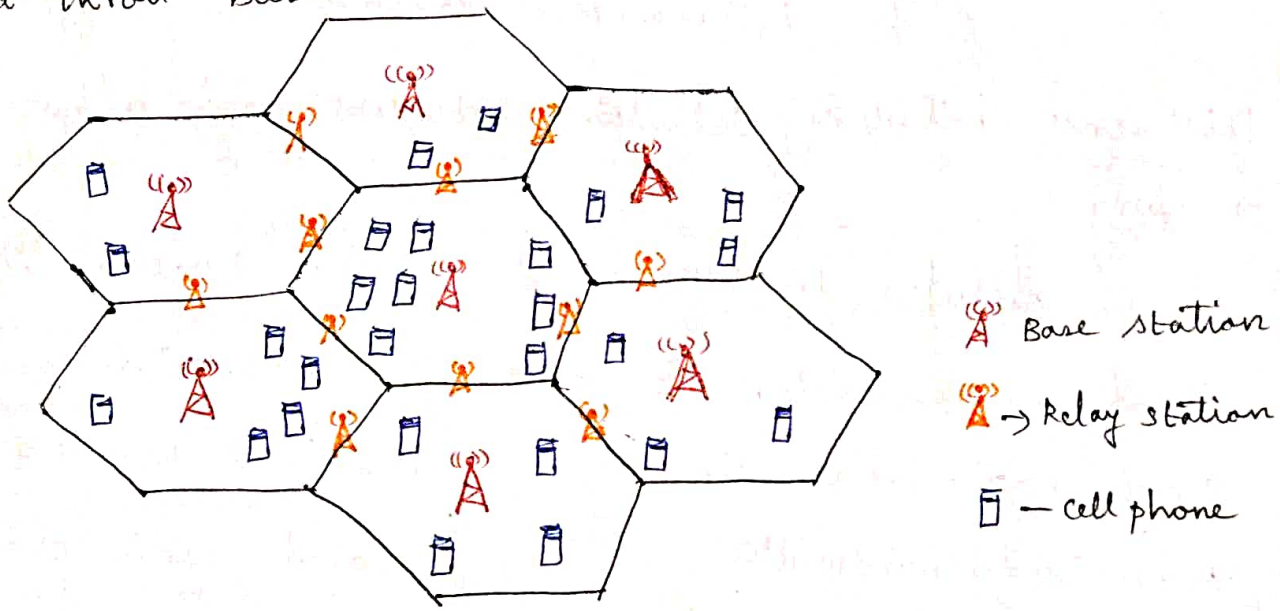
→ Neighbour nodes communicate with one another using single hop wireless technology like Bluetooth, Zigbee and IEEE 802.11

→ Node which are distant from each other communicate using a sequence of intermediate nodes

cellular and Adhoc wireless networks

→ The cellular network is infrastructure dependent networks.

→ The path set up for a call between two nodes is completed through base station

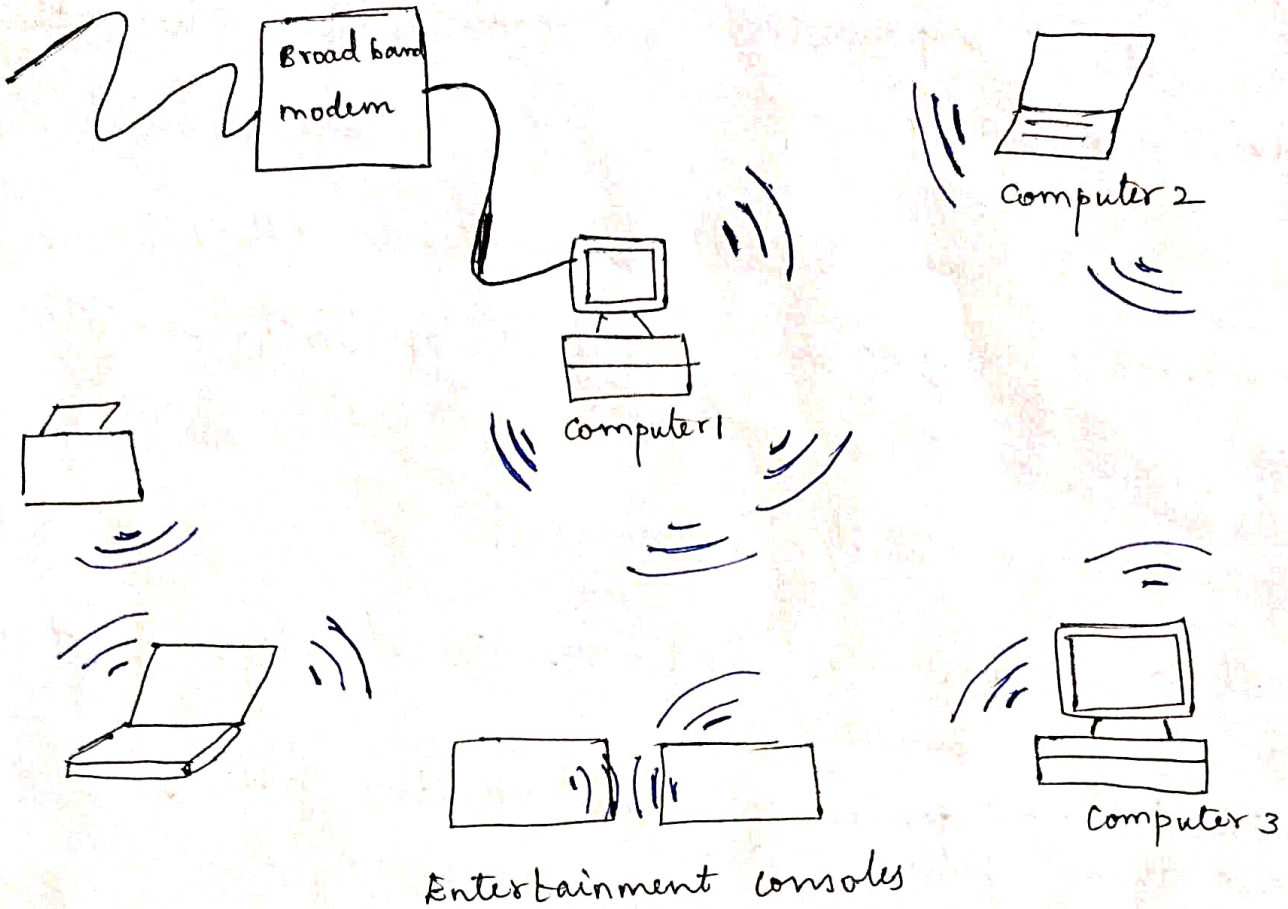


A cellular network

→ Adhoc wireless networks are defined as category of wireless networks that utilize multihop relay

→ The path setup between two nodes is completed through the intermediate mobile node

Adhoc Wireless Networks



Difference between Cellular Networks and adhoc wireless networks

Cellular Networks	Adhoc Wireless Networks
fixed infrastructure based	Infrastructureless
Single hop wireless links	Multihop wireless links
Guaranteed bandwidth	shared radio channel
centralized routing	Distributed routing
Circuit switched	Packet switched
Seamless connectivity	Frequent path breaks
High cost and time of deployment	Quick and cost effective deployment

Reuse of frequency spectrum through geographical channel use	Dynamic frequency reuse based on carrier sense mechanism
Easier to achieve time synchronisation	Time synchronisation is difficult and consumes Bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
High cost of network maintenance	self organizing and maintenance

Issues in Adhoc Wireless Network

The major issues in designing an Adhoc wireless system are

1.
a) Medium access scheme

The primary responsibility of medium access control (MAC) is distributed arbitration for shared channel for transmission of packets.

b) Distributed operation :

→ The adhoc wireless networks need to operate in environments where no centralized coordination is possible

c) Synchronisation :

→ Synchronisation is important for TDMA for management of transmission and reception slots

→ It involves usage of scarce resources such as bandwidth and battery power.

d) Hidden terminals:

→ Hidden terminals are nodes that are not reachable from sender of data but reachable to receiver.

→ It causes collision at receiver node.

e) Exposed terminals:

→ Exposed terminals are nodes in the transmission range of sender but prevented from making a transmission.

f) Throughput

→ MAC protocol should maximize the throughput by minimizing the occurrence of collision and maximizing channel utilization

g) Fairness:

→ The MAC protocol should provide an equal share of bandwidth to all competing nodes

→ real time traffic, resource reservation, capability of power control are other issues.

2. Routing:

→ It is the process of determining route based on hop count

→ The need of power and life time of the link in order to exchange information from one node to other node.

→ The major design issue of routing protocol are mobility, bandwidth constrained, error prone

and shared channel, location dependent contention and other resource constraints such as computing battery power, storage capacity

3. Multicasting

→ Transmission of same message to a group of mobile nodes in single transmission is called multicasting

→ The major design issues of multicasting are Robustness, efficiency, control overhead, QoS, efficient group management, scalability and security

4. Transport layer protocols.

→ Transport layer protocols are used to set up and maintain end to end connection

→ It provides reliable data delivery in wired network

→ TCP is one of the reliable connection oriented protocols widely used in wired networks.

5. Pricing Schemes:

→ In adhoc network, if any mobile node is not interested in relaying packet to its neighbors it can decide to power off

6. QoS provisioning:

→ It is the performance levels of services which is offered by a service provider

→ If there is better coordination and cooperation between service provider and user then high QoS is achieved.

→ QoS parameters differ from application to application

→ QoS aware routing protocol should possess QoS parameters for determining routing path

→ QoS framework is a complete system used to provide the assured services to concerned user or application

7. Self organization.

→ The mobile nodes in adhoc networks would self configure the network by itself.

8. Security:

→ It is a challenging one in Adhoc wireless networks

→ Two types of attack

i) Active attack → malicious node → do not disturb n/w

ii) Passive attack → disturb the network o/p. → By node from external n/w

by mobile nodes within n/w → internal attacks

external attacks

9. Addressing and Service discovery

→ Address of a mobile node is globally unique identifier used for communication

10. Energy management:

It is the process of managing the sources and

and consumes of energy in a node to boost up the lifetime of node in network.

It is divided into 4 categories

1. Transmission power management
2. Battery energy management
3. Processor power management
4. Device power management.

11. Deployment consideration

→ They are of low cost of deployment, incremental deployment, short deployment time, reconfigurability and non estimation of future traffic growth in network

Applications of Adhoc wireless Network.

1. Military applications

→ It establishes communication among a group of soldiers for tactical operations

→ Secure and reliable multimedia multicasting communication is more important.

→ For secure communication vehicle mounted nodes is assumed to be sophisticated and powerful.

2. Collaborative and Distributed computing

→ Adhoc network provides temporary communication infrastructure for quick communication with minimal configuration

→ For researchers to share their findings or presentation do not require security but reliable multicast routing, to share data to all users

→ For such application economical and portable devices are prefered.

3. Emergency Operations

→ Adhoc is very useful in emergency operation such as search and rescue, crowd control, and commando operations

→ During natural calamities such as earthquake, immediate deployment of adhoc wireless network is a good solution for rescue.

→ Self configuration, minimal overhead and support for scalability and voice communication are very important for emergency applications.

4. Commercial and civilian Environment

The emergence of Adhoc network E-commerce eg. electronic payments from anywhere is very efficient and fast.

5. Educational Applications:

It is used in universities and campus for setting up virtual class rooms

6. Entertainment

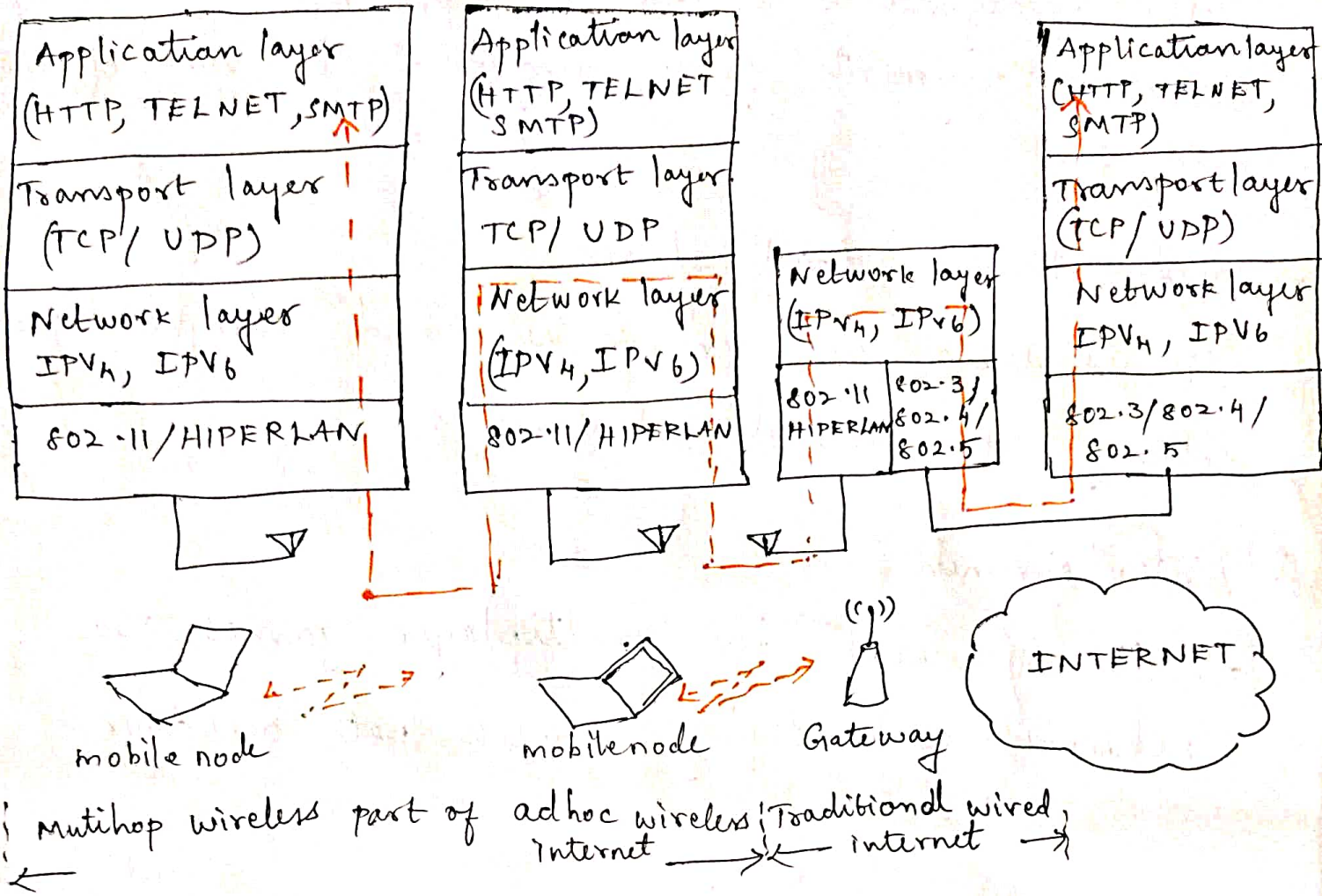
→ It is used in multiplayer games. The network can deploy robotics pets outdoor

Adhoc Wireless Internet

→ It extends the services of Internet to end user in an adhoc wireless network environment.

→ Important application are wireless mesh network provisioning of temporary internet services to meeting venues, sport venues, temporary military settlements, battlefields and broadband Internet services in rural regions.

Adhoc Wireless Internet



Issues in Designing a Routing Protocol for Adhoc Wireless Networks.

1. Gateways:

→ Gateway nodes in Adhoc wireless Internet are the entry points to wired Internet.

→ Gateways are owned and operated by service provider

→ They perform tasks like, keeping track of the end users, bandwidth management, load balancing, traffic shaping, packet filtering, bandwidth fairness, address discovery, and service discovery

2. Address Mobility:

→ Adhoc wireless Internet has address mobility

→ This problem is worse as the nodes operate over multiple wireless hops

→ Mobile IP provide temporary solution for this.

3. Routing

→ Routing is a problem due to dynamic topological changes

→ The solution is the use of separate routing protocol for wireless part

4. Transport layer protocol

→ The solution for transport layer protocol exists in favour of TCP extension proposed for Adhoc

→ A specialized transport layer protocol for Adhoc wireless network is considered when gateways acts as intermediate nodes

5. Load Balancing:

→ 100% Adhoc wireless Internet gateways experience heavy traffic.

→ Hence the gateways are saturated.

→ Load balancing distribute the load to avoid this situation

6 Usage Pricing / billing

→ As Internet bandwidth is expensive, it introduces pricing / billing strategies for Adhoc wireless Internet

→ Gate way is preferred choice for charging the traffic

→ It is very complex to calculate the pricing for local traffic, so have a dedicated, secure and lightweight pricing/billing infrastructure installed at every node

7. Security provision

→ As the end user can utilize the Adhoc wireless Internet to make e-commerce transactions it is vital to include security mechanism in Adhoc wireless Internet

8. QoS Support

→ Voice over IP (VoIP) is widely used all over and there is huge multimedia usage over Internet

→ So provisioning of QoS is very Important

9. Service, address, location discovery

→ Service discovery is activity of discovering the entity which provides a particular service or

→ resource

→ Address discovery refers to Address Resolution Protocol (ARP) operating within wireless domain

→ Location discovery is detecting the location of particular mobile node in a network

Classification of Routing Protocols

The routing protocols for adhoc wireless networks is classified into four categories

1) Routing information update mechanism
2) Use of temporal information for routing
3) Routing topology
4) Utilization of specific resources

Based on Routing Information Update mechanism

1. Proactive or table-driven routing protocols:

→ In table driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information

→ Routing information is generally flooded in the whole network

→ whenever a node requires a path to a destination it runs an appropriate path finding algorithm

on the topology information it maintains.

2. Reactive or on-demand routing protocols

→ On demand routing protocols do not maintain the network topology information

→ They obtain the necessary path when it is required, by using a connection establishment process

→ Hence these protocols do not exchange routing information periodically.

3. Hybrid routing Protocols:

→ They combine the features of above two routing protocols

→ Nodes within a certain distance from the node concerned, are said to be within the routing zone of the given node

→ For routing within the node zone, a table driven approach is used

→ For nodes beyond the zone, an on-demand approach is used

Table Driven Routing Protocol

→ These protocols are extension of wired network routing protocols

→ They maintain global topology information in the form of tables at every node

→ These tables are updated frequently in order to maintain consistent and accurate network state information

Destination Sequenced Distance Vector (DSDV)

→ The DSDV is the first protocol proposed for adhoc wireless networks

→ It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count to infinity problems and for faster convergence

→ Routes to all destination are readily available at every nodes at all times.

→ Tables are exchanged between neighbours at regular intervals to keep an up to date view of network topology

→ The table updates are of two types
1) incremental update
2) full dumps

Incremental update:

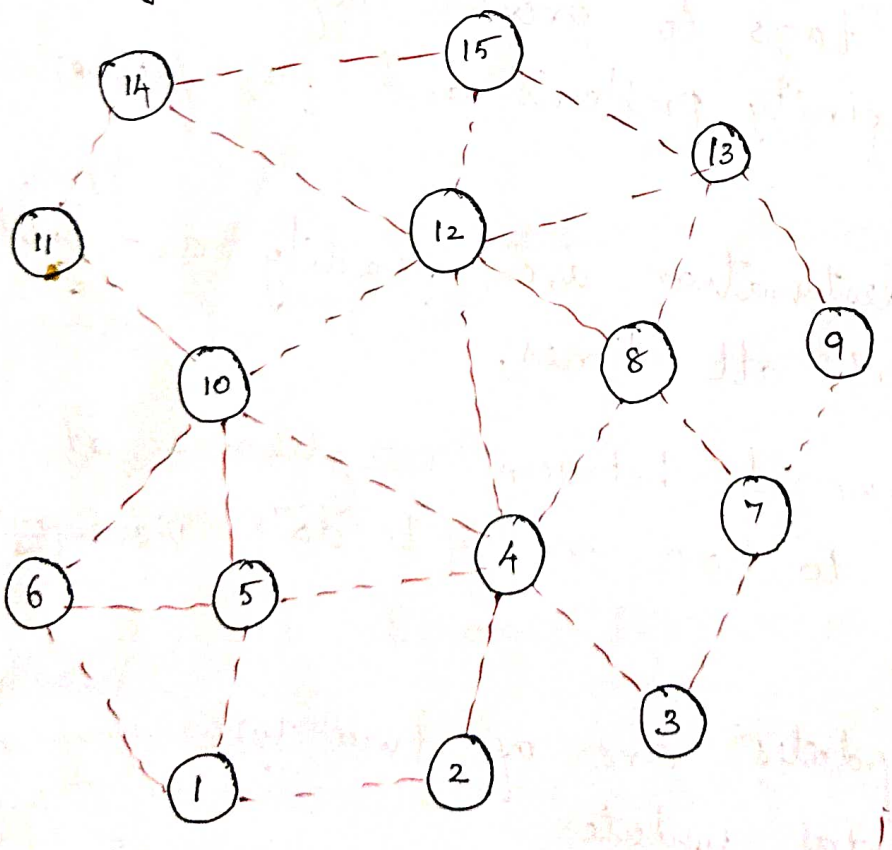
→ It takes a single network data packet unit. NDPU

→ Incremental updates are used when a node does not observe significant changes in local topology

full dump

→ It take multiple NDPU's.

→ Full dump is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU



Dest	Next node	Dist	Seq-NO
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

→ Table updates are initiated by a destination with a new sequence number which is always greater than previous one.

→ upon receiving an updated table, a node either updates its table based on received information

Route establishment

→ node 1 is source node and node 15 is the destination

→ All nodes maintain global topology information

→ The routing table of node 1 indicates the shortest route to destination node (15), through node 5 with distance of 4 hops

Route maintenance

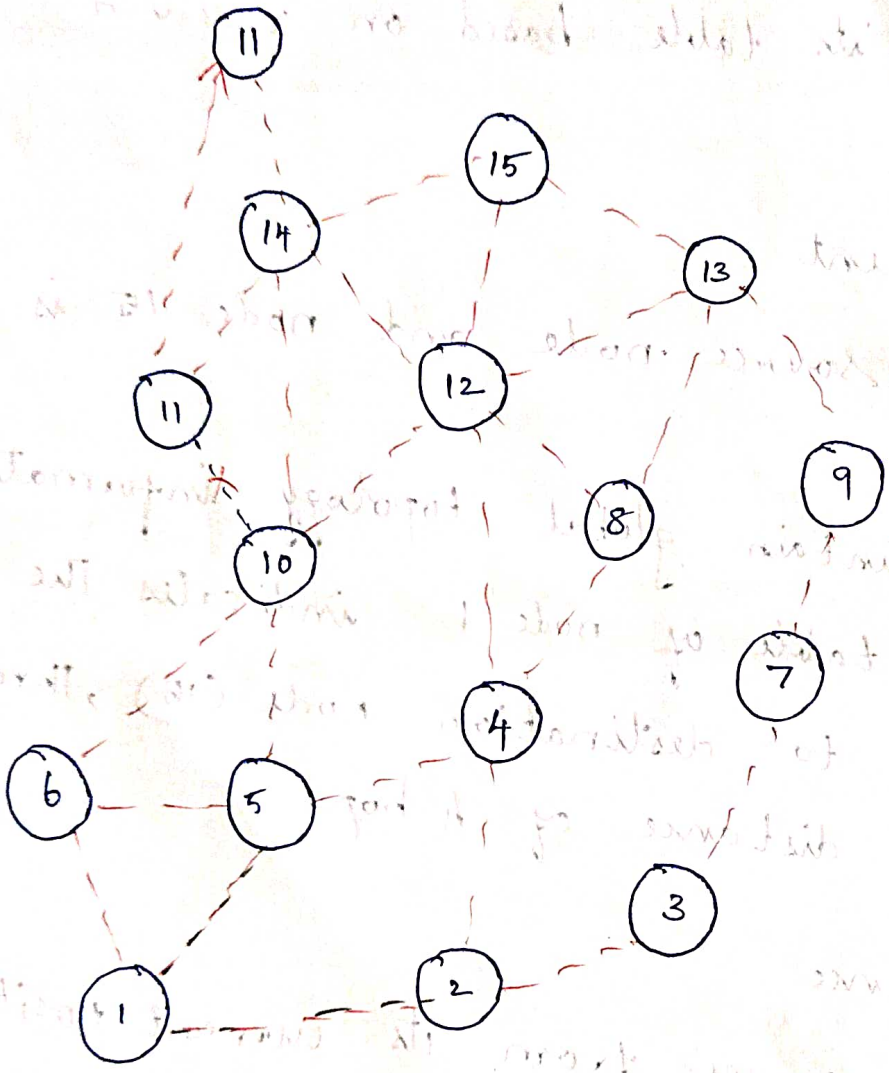
→ If node 11 moves from its current position

→ The neighbour node percives the link break and sets the broken link with distance as ∞.

→ node 1 sets the distance to node 11 as ∞

→ This information is also propagated throughout the network

→ In the updated table at node 1, the distance from node 1 to node 11 is increased from three to four hops



Route maintenance in DSDV

Routing Table for node 1

Dest	Next node	Dist	Seq. no
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

On Demand Routing Protocol

→ on demand routing protocols execute the path finding process and exchange routing information only when a path is required by a node to communicate

Adhoc on Demand Distance Vector Routing (AODV)

→ AODV uses an demand approach for finding routes

→ A route is established only when it is required by a source node for transmitting packets

→ It employs destination sequence numbers to identify the most recent path

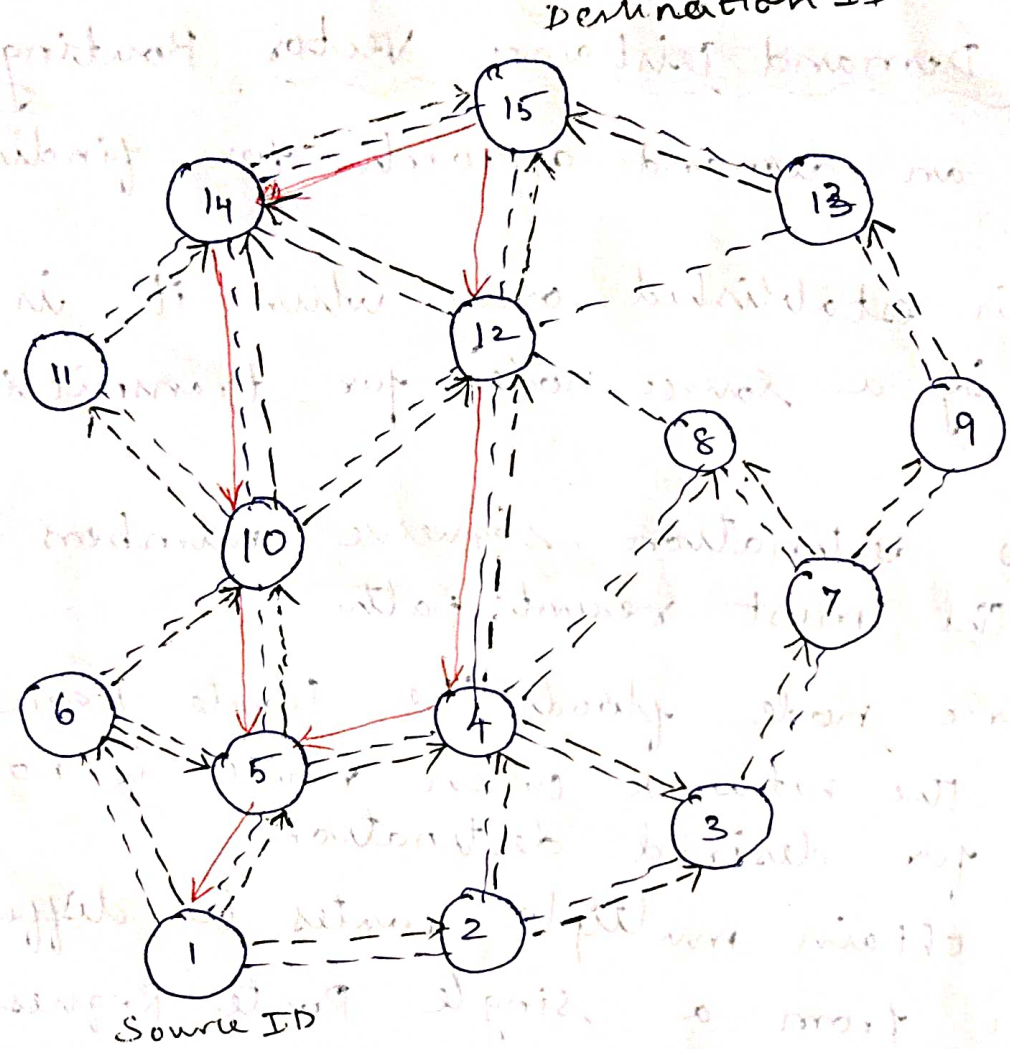
→ The source node floods the Route Request packet in the network when route is not available for desired destination

→ It may obtain multiple routes to different destination from a single Route Request

→ A Route Request carries the source identifier (Src ID), the destination identifier (Dest ID), Source sequence number (Src Seq Num) the destination sequence number (Dest seq Num) broadcast identifier (Broat ID), and time to live (TTL)

→ when an intermediate node receives a Route Request, it either forwards it or prepares a Route Reply if it has a valid route to the destination

Route establishment in AODV



Network link

Route Request

Route Reply

path 1 : 1 - 5 - 10 - 14 - 15

path 2 : 1 - 5 - 4 - 12 - 15

Route establishment

→ In the fig. source node 1 initiates a path finding process by originating a Route Request flooded in the network for destination node 15.

→ The Destination seq. no as 15 and source seq. no. as 1

→ when nodes 2, 5, 6 receives the Route Request packet, they check their routes to the destination

→ If route to the destination is not available they further forward to their neighbours

→ nodes 3, 4 and 10 are neighbours of 2, 5 and 6

→ This is with assumption that nodes 3 and 10 already have routes to destination node 15 through paths 10-14-15 and 3-7-9-13-15.

→ If destination sequence no. at intermediate node 10 is 4 and is 1 at intermediate node 3, then only node 10 is allowed to reply along cached route to source.

→ node 3 has older route to 15 with seq no. 1

→ while node 10 has recent route with destination sequence no. 4. to destination

→ If the Route Request reaches the destination

→ node 15 throw path 14-12-15, or any other the destination also sends Route Reply.

→ multiple Route Reply reach the source

→ All intermediate nodes receiving Route Reply update the route tables with the latest destination seq. no.

→ They update the ranting information if it leads to shorter path between source and destination

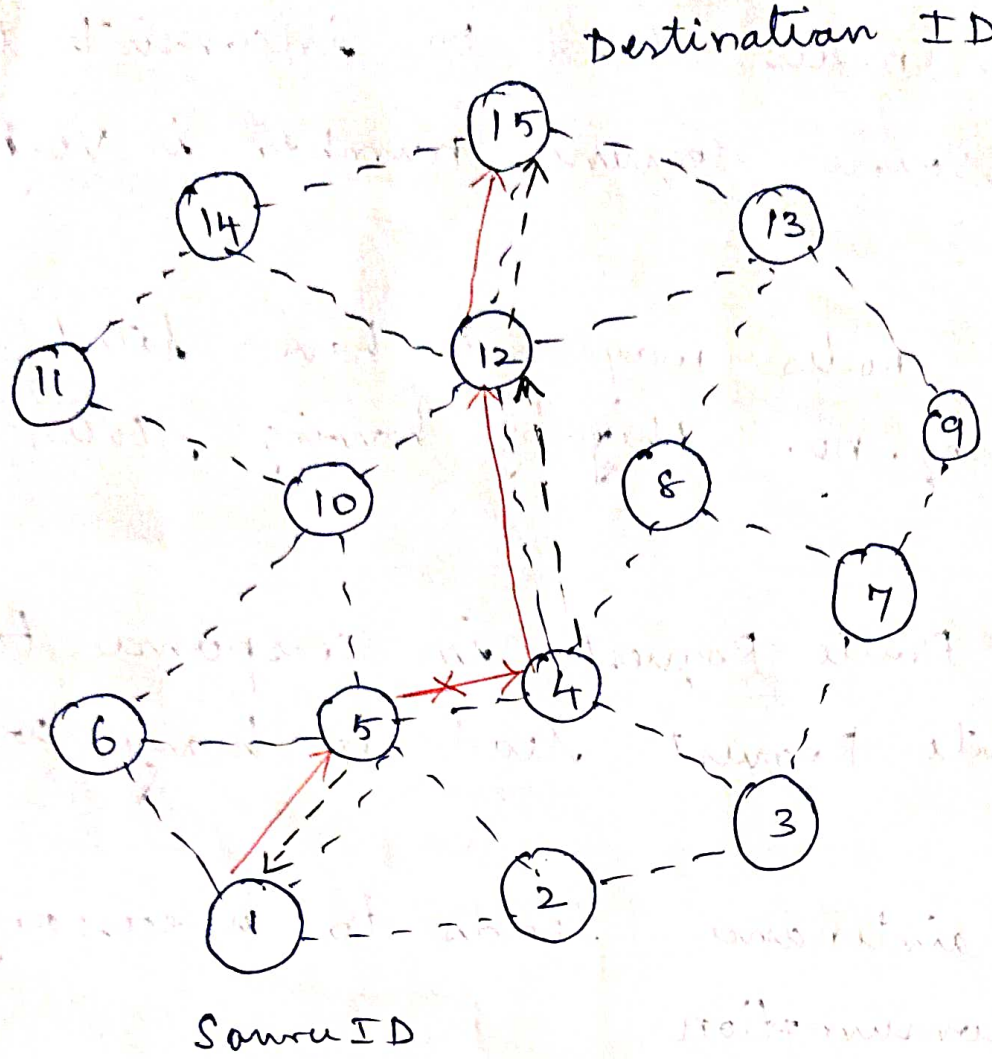
Route Maintenance

→ when a path breaks between 4 and 5 both node intiate Route Error messages to inform thir end nodes about link break

→ the end nodes delete the corresponding entries from thir tables

→ the sourse node intiates the path finding proces with new Broadcast ID and the previous destination sequence no.

Route maintenance in AODV



- - - - - Network link
——→ Route for 1→15
- - - -→ Route error
——✕——→ Broken link.

Advantages

→ Route are established on demand and destination sequence number are used to find latest routes

→ connection set up delay is less

Unit-II

Sensor Networks

WSN - Wireless Sensor Networks

→ The Network consists of individual nodes that are able to interact with each other with their environment

→ collaboratively work using wireless communication

Applications:

Disaster relief application

→ for wild fire detection : sensor nodes equipped with thermometers

→ Sensors are deployed over wildfire, from an aeroplane

→ They collectively produce temperature map

→ military application sensors should detect enemy troops ; sensors should be cheap enough

Environmental control and bio diversity mapping:

→ used to control the environment with respect to chemical pollutants - garbage dump sites

→ Surveillance of marine ground floor

→ understanding of erosion process

→ understanding the no. of plants and animals that live in a habitat

Intelligent Buildings :

* Buildings waste vast amount of energy by inefficient humidity, ventillation, Air conditioning
* A better real time high resolution monitoring of temperature, air flow, humidity & other physical

Parameters by WSN increase comfort level of inhabitants and reduce energy consumption

→ Sensor nodes used to monitor mechanical stress levels of buildings, and bending load of girders as for safe enter of given building after earth quake.

Facility Management:

→ Management of facilities larger than a single building

→ eg. keyless entry application where people wear badges & WSN checks which person to allow to which area of larger company

→ detection of intruders of vehicles that pass outside of normal business hours & tracks its position and alerts the security

Machine Surveillance and preventive maintenance:

→ Sensors are fixed i.e. in difficult to reach areas of machinery to detect vibration pattern & indicate the need for maintenance

eg. axles of trains, robotics

main adv: cable free operation, cheap installation

Types of application

Sources of data → actual node that sense data
Sinks → nodes where data should be

Event detection:

→ sensor nodes report to the sinks once they detect the occurrence of specific event
→ simplest event detected by single sensor node
→ Complicated events require collaboration of nearby remote sensors

Periodic measurement:

→ sensors are tasked for periodic reporting of measured values
→ reporting period is application dependent

Function approximation and edge detection

→ Physical value like temperature changes is regarded as function of location
→ WSN used to approximate unknown function using limited no. of samples
→ To find the isothermal points in forest fire - to detect the border of fire.
→ finding 'edges' in functions or to send messages along boundaries of patterns

Precision Agriculture :

→ WSN in agriculture allows precise irrigation and fertilizing by placing humidity sensors into fields

→ pest control of farmland

→ livestock breeding by attaching sensor to animals

Medicine & healthcare :

→ Sensors are directly attached to patients for drug administration

→ raising alarm when applied to wrong patient

Logistics :

→ equip goods with simple sensors and allow tracking of time objects during transportation

→ RFID tag support to locate items in warehouse

Telematics :

→ sensors embedded in street can gather information about traffic conditions

Challenges for WSN

Realizing the following characteristics is a major challenge of wireless sensor network

Characteristics requirements

Type of Service:

* WSN is expected to provide meaningful information for a task
* WSN moving bits only a means to an end
* scoping of interaction to specific geographic region or to time interval is important
* " People want answers not numbers'

Quality of Service:

* Type of networks service is quality of that service
* QoS comes from multimedia type application like bounded delay or minimum B.W
* In some cases occasional delivery of a packet is enough in other cases high reliability exist
* In some cases delay is important when actuators are to be controlled
* Adopted Quality concepts like reliable detection of events or approximation of quality is important

fault tolerance:

→ when nodes run out of energy it ~~might~~ is damaged or wireless communication between two nodes is interrupted.

→ WSN as whole should tolerate such faults

→ To tolerate, redundant deployment is necessary

Life time:

→ nodes will rely on limited supply of energy (using batteries)
→ Replacing these sources is not practicable
→ lifetime is an important figure of merit
→ A supplement to energy supplies, a limited power source (solar cell) is available on sensor node
→ These does not ensure continuous operation but provide recharging of batteries.
→ Investing more energy can increase quality but decrease lifetime

Scalability:

→ WSN include large no. of nodes, the employed architecture and protocols must be able to scale these numbers

Wide range of densities:

→ In WSN, the no. of nodes per unit area — density of network vary.
→ Different application have different node densities
→ The network should adapt to such variations

Programmability:

→ It is not only necessary for the nodes to process information but also to react flexibly on changes
→ so the nodes should be programmable and changeable during new operation and task

fixed way is insufficient

Maintainability:

→ As both WSN and its environment change, the system has to adopt

→ It has to monitor the status to change operational parameters to choose different trade offs (eg. provide lower quality when resource is scarce)

→ The network should maintain itself and interact with external mechanism to ensure its required quality

Required Mechanism:

→ To realize these requirements innovative mechanism for a communication network have to be found.

→ the mechanism has to generalize wide range of application

Some of the mechanism of WSN are

Multihop wireless communication:

→ In wireless, direct communication between a sender and a receiver is faced with limitation

→ For long distance high transmission power is required

→ The use of intermediate nodes reduce the total required power

→ So in WSN multihop communication is most necessary

Energy efficient operation

→ To support long lifetime, energy efficient operation is a key technique

→ non homogenous energy consumption forming hotspots is an issue.

Auto configuration :

→ WSN configure most of its operational parameters autonomously, independent of external configuration.

→ nodes determine their geographical position only using other nodes of n/w called 'self location'

→ the network should be able to tolerate failing node. (because of depleted battery) or integrate new nodes (because of incremental deployment after failure)

Collaboration and in-network processing :

→ single sensor is not able to decide, happening of an event

→ several nodes collaborate to detect an event, only joint data of many sensor, provides enough information

→ Information is processed in n/w in various forms to achieve collaboration instead of every node transmit data to external network

→ for eg. to determine the highest or average temp. within an area, readings from individual sensor is aggregated, reducing the amount of data to be transmitted, improving energy efficiency

Data centric:

→ In Traditional communication networks, data transfer between two devices is equipped with one n/w address

→ Hence they are address centric

→ In WSN, nodes are deployed redundantly to protect against node failure, the identification of node supplying data is irrelevant.

→ Hence switching from address centric, to data centric paradigm in designing architecture and communication protocols is promising.

Locality:

→ locality will ensure scalability

→ nodes which are very limited in resources, limit their states (processing only information of neighbours)

→ This will allow the network to scale large no. of nodes without relying on single node

→ The locality with efficient protocol is still an open research.

Exploit trade offs:

→ WSN rely to large inherent trade off

→ higher energy allows higher accuracy or longer life of node

→ Another trade off node density: depending on application deployment and node failures, at runtime

→ the density of n/w change considerably

→ The protocols have to handle very different situations at different places of a single nlw.

Enabling technologies for WSN

→ WSN has fundamental advances in enabling technologies

→ first is miniaturization of hardware

→ small feature size in chips drive down the power consumption

→ This is relevant to microcontrollers and memory chips and radio modems for wireless communication

→ Reduced chip size and improved energy efficiency is accompanied by reduced cost

→ In processing and communication the sensing element is the third relevant technology

→ The three basic parts of sensor node is accompanied by power supply which requires high capacity batteries

→ A sensor node has a device for energy scavenging, recharging battery with energy gathered from environment (solar cells or vibration based power generation).

→ It requires battery to be efficiently chargeable with small amounts of current

The counterpart of basic hardware technology is software.

→ The environment has to support simple restasking cross layer information exchange and modularity to allow simple maintenance

→ The software architecture on a single node has to be extended to network architecture

Single Node Architecture

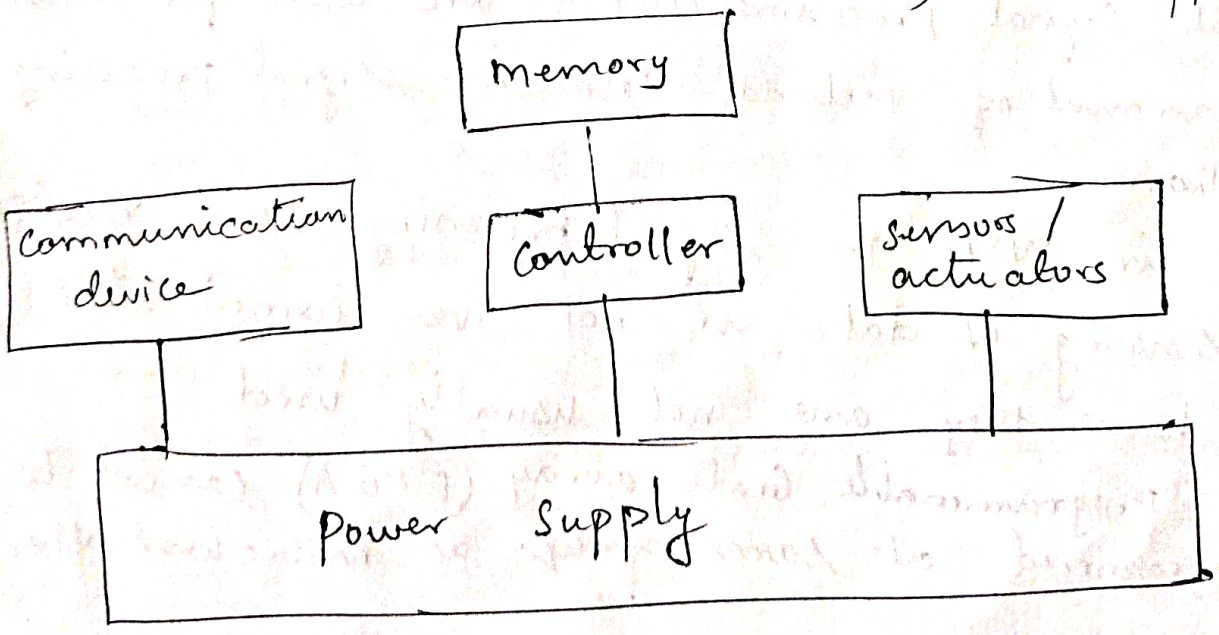
* The principle task of a node is computation, storage communication and sensing/actuation
* The energy consumption, energy gathering and saving is also an important task of a node

Hardware Components:

→ The application requirement plays an important factor in choosing hardware component.

The basic sensor node comprises of 5 main components

1) controller 2) Memory 3) sensors and actuators 4) Communication 5) powers supply



Controller

→ It is the core of wireless sensor node

→ It collects data from sensors, processes data and decides when and where to send it, receive data from other sensor nodes.

→ It has to execute various programs, it the central processing unit (CPU) of the node.

→ Variety of processing tasks are performed on various controller architectures, representing tradeoff between flexibility, performance, energy efficiency and costs

→ Simple processors like microcontrollers are best suited due to their flexibility in connecting with other devices like sensors

→ Their low power consumption, and their instruction set amenable to time critical signal processing and memory built in make them more flexible

→ Microcontrollers are suitable for WSN as they enter the 'sleep mode' only when only parts of controllers are active.

→ Digital Signal Processors (DSPs) are used for processing large amount of vectorial data in signal processing applications

→ Since in WSN the signal processing task related to sensing of data is not over complicated and hence they are not usually used

→ Field Programmable Gate array (FPGA) cannot be reprogrammed at same freq. as microcontroller

ASIC provide the same function in ~~more~~ potentially more costly hardware

→ In WSN, bigger flexibility and simpler usage make microcontroller the superior solution

eg: for microcontrollers

i) ~~Atmel processors~~ or Texas instruments. MSP 430 (16 bit) at 4MHz Clk freq

ii) Intel strong ARM [379]
SA-1100 model → 32 bit RISC at 206 MHz

iii) Atmel ATmega 128L — 8 bit processor used in embedded applications

Memory

→ RAM is used to store intermediate sensor readings packets from other nodes

→ RAM is fast, but loses its content if power supply is interrupted

→ program is stored in Read Only Memory (ROM) or Electrically Erasable Programmable Read Only Memory (EEPROM)

→ Flash memory also serve as intermediate storage of data if RAM is insufficient or when power supply is shut down for RAM for some time.

→ Correct dimensioning of RAM is crucial with respect to cost and power consumption

Communication device

→ It is used to exchange data between individuals

→ Wired communication is frequently applied in many sensor network like settings

→ The communication devices for these networks are custom off-the shelf components → something available now (or) in stock

→ In wireless communication, choice is made on transmission medium.

→ The medium are radio frequencies, optical communication and ultrasound.

→ Radio frequency (RF) based communication best fits WSN

→ It provides long range, high data rates and acceptable error rates, and does not require the line of sight between sender and receiver.

Transceivers: Design Considerations

→ Both transmitter and receiver are required in sensor node

→ The main task is to convert a bit stream coming from microcontroller and convert them to ~~rdi~~ radio waves.

→ The combined devices to perform the two tasks in single entity is called transceivers

→ Half duplex operation is performed.

→ Low cost transceivers is commercially available for transmitting and receiving

Transceiver tasks and characteristics

Service to upper layer:

→ A receiver has to offer certain services to upper layer (ie) MAC (medium Access control layer)

→ The transceiver must provide an interface to allow MAC layer to initiate frame transmission

Power consumption and energy efficiency

→ Transceivers must be switchable between different states eg. active and sleeping

Carrier frequency and Multiple channels

→ Transceivers are available at different carrier frequencies

→ It must match application requirements and regularity restriction

State change times and energy

→ A transceiver can operate in different modes: sending or receiving, use different channels, or be in different power-safe states

Data rates:

→ Different data rates can be achieved by using different modulation or changing the symbol rate

Modulation:

The transceiver support one or several of on/off keying, ASK, FSK or similar modulation

Coding : Transceivers allow various coding schemes

Transmission power control :

→ Transceivers directly provide control over transmission power

Noise figure :

It is defined as the ratio of signal to noise Ratio (SNR_i), at the input of the element to SNR ratio (SNR_o) at the elements output

$$NF = \frac{SNR_i}{SNR_o}$$

It describes the degradation of SNR due to elements operation, and given in dB as

$$NF\ dB = SNR_i\ dB - SNR_o\ dB$$

Gain : It is the ratio of o/p signal power to input signal power

Power efficiency : It is defined as the ratio of radiated power to overall power consumed by front end

Receiver Sensitivity : It specifies the minimum signal power at the receiver to achieve the prescribed error bit rate.

Range : Range depends on maximum transmission power on antenna characteristics, on attenuation caused by environment, which depends on carrier frequency It ranges from few metres and several hundred metres

socking performance:

It the achieved bit error rate of receiver in presence of interferer

Out of band emission:

To limit the disturbance of other system, the transmitter should produce, the transmission power a little outside the prescribed Band Width.

Carrier sense and RSSI

The receiver must able to provide information whether channel, or carrier, is busy (another node is transmitting).

IEEE 802.15.4 has following modes

* The received energy is above threshold.
* A carrier has been detected.
* carrier detected and energy is present.

Frequency stability:

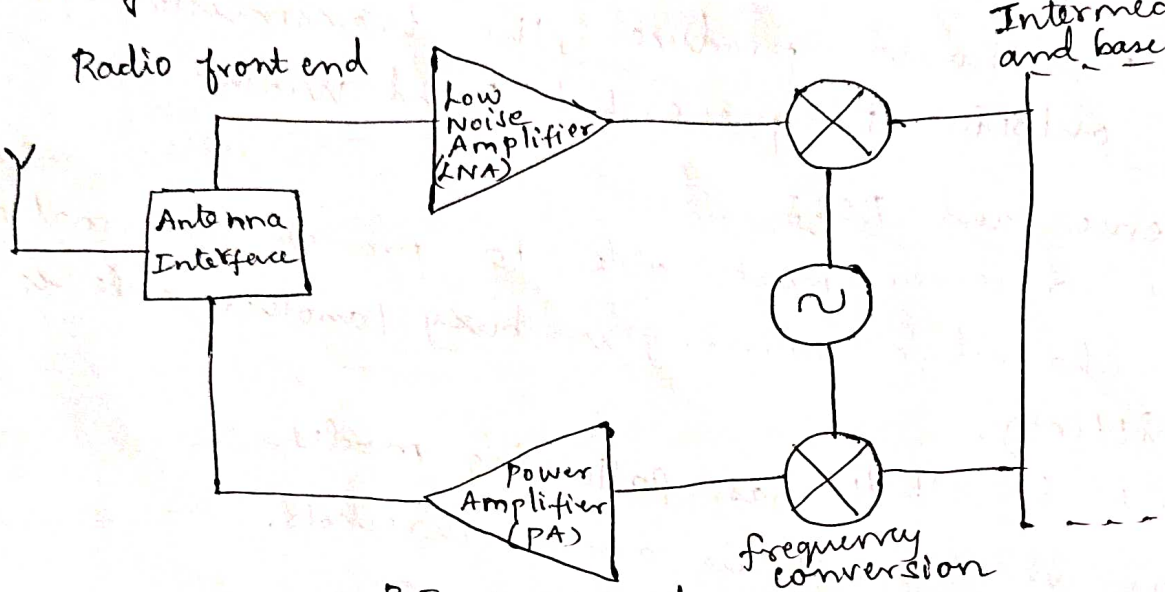
It denotes the degree of variation from nominal centre frequencies when environmental condition of oscillator, like temperature or pressure change

Voltage range:

The Transceivers should operate over a range of supply voltage.

Transceiver structure

* The radio frequency front end performs analog signal processing
* The baseband procesor performs all signal processing in digital and communicatis with sensor nodes



RF front end

The element of RF front end

Power Amplifier (PA) :

It accepts the upconverted signals from IF or base band part and amplifies them for transmission over antenna

Low Noise amplifier (LNA):

It amplifies the incoming signals suitable for further procesing without reducing (SNR)

Local oscillator or Voltage controlled Oscillators (VCO) and Mixers:

They are used for frequency conversion from RF spectrum to intermediate frequencies to base band.

transceiver operational states:

Transmit: The transmit part of transceiver is active and the antenna radiates power

Receive: The receiver parts is active

Idle: A transceiver is ready to receive but not currently receiving to be in idle state.
→ many parts are ~~idle~~ active and others are switched off.

Sleep: In sleep state, significant parts of transceiver are switched off.
→ In complete power down includes complete initialisation & configuration of radio
→ In lighter sleep modes, the clock driven parts is throttle down and operational state is remembered.

Sensors and Actuators

Sensors:
→ The sensor open or close a switch or relay to set a value
→ It is categorized into three categories

Passive, omnidirectional sensors
→ It can measure a physical quantity
→ Sensors are self powered, obtain energy they need from environment
→ energy is only needed to amplify their analog signal
eg: thermometer, light sensor, chemical sensor, smoke detectors

Passive narrow beam sensors:
→ They are passive but have well defined notion of direction of measurement.
eg. camera

Active sensors:

→ It actively probes the environment
eg. sonar, radar or seismic sensors

→ seismic sensors generate shock waves by small explosion

Actuators:

→ It controls a motor, a bulb or physical objects

Power supply of sensor nodes

→ power supply is a crucial system component.

There are two aspects.

1) Storing energy & providing energy in required form

2) to replenish consumed energy by scavenging

Storing energy: Batteries

→ Battery is the power source of sensor node

→ Non chargeable batteries are called primary batteries

→ If an energy scavenging device is present and rechargeable it is called secondary batteries

→ Batteries are electro chemical — the chemical is the determining factor of battery technology

The requirements of battery are

Capacity:

→ They should have high capacity at small weight, small volume and low price. The main metric is energy per volume: $1/cm^3$

city under load:

They should withstand various levels of power over time and a sensor draw high current in certain operation modes.

Self discharge:

→ The self discharge should be low, and last for long time

Efficient recharging:

Recharging must be efficient even at low recharge powe

Relaxation:

This relaxation effect is the self recharging of an empty battery when no power is drawn

Unconventional energy stores:

→ fuel cells is a electro-chemical storage of energy

→ It directly produces electrical energy by oxidising hydrogen or hydrocarbon fuels

→ They have excellent energy densities

→ Energy stored in hydrocarbon is to use miniature version of heat engines

→ 'Gold caps' are high quality and high capacity capacitors can store large amount of energy

DC- DC conversion:

→ Batteries alone are not sufficient as a direct source for a sensor node

→ On reduction of battery voltage, less power is delivered to sensor node which reduces oscillator frequency

and transmission power

→ A DC-DC converter is used to overcome the problem by regulating the voltage delivered

Energy Scavenging:

- For long lasting nodes, a limited energy is unacceptable

→ The energy from nodes environment must be tapped into and made available to the node energy scavenging should take place

Photo voltaics:

→ The solar cells can be used to power sensor nodes

→ The amount of power depends on nodes at outdoors or indoors

→ The resulting power is 10 μW/cm² for indoors and 1.5 mW/cm² for outdoors

→ Single cells achieve o/p voltage of 0.6V.

Temperature gradients:

→ Differences in temperature is directly converted to electrical energy

→ Small difference, 5k can produce considerable power

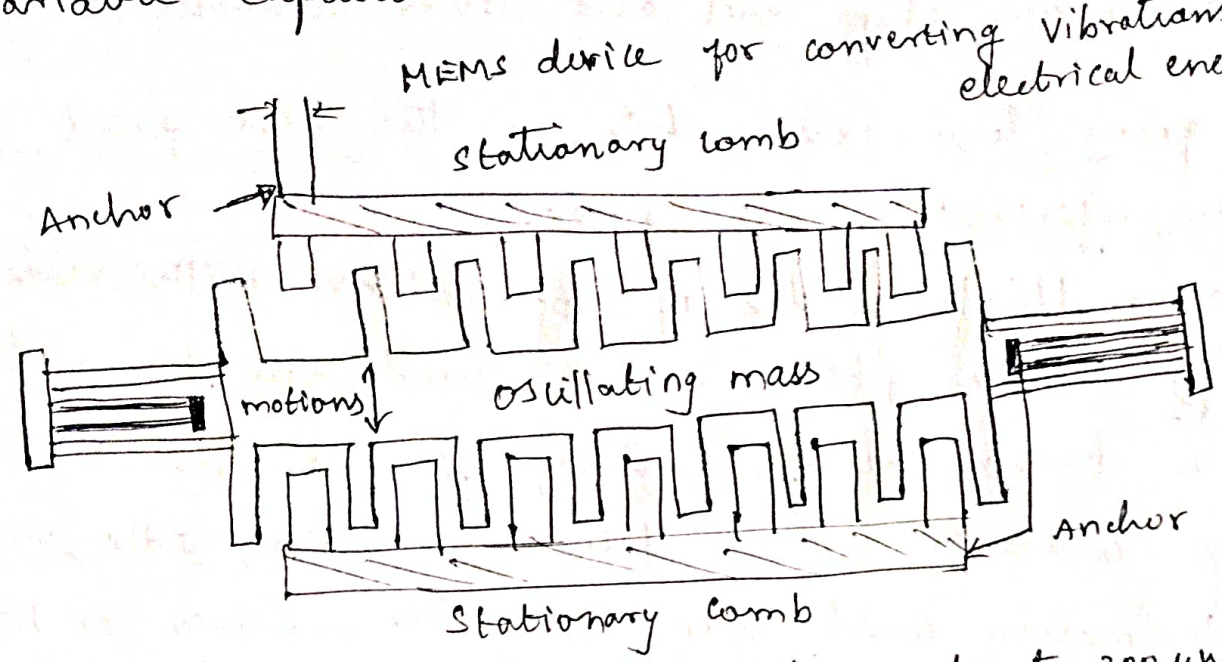
→ seebeck effect base thermoelectric generator are used to achieve about 60μW/cm² about 1V from 5 kelvin temperature difference

Vibrations:

→ The pervasive form of mechanical energy is Vibration

→ the available energy depends on both amplitude and frequency of vibration ranges from 0.1μW/cm² to 10,000 μW/cm²

The fig. shows eg. for generator based on variable capacitor



→ practical devices of $1cm^3$ produce about $200\mu W/cm^3$ from $2.25 m/s^2$, 120Hz vibration sources, sufficient for wireless transmitter

Pressure Vibrations

→ Vibration of pressure is used as power source
eg: piezoelectric generators

Flow of air/liquid:

→ Another power source is flow of air or liquid in windmills or turbines

Energy consumption of sensor nodes:

operation states with different power consumption

→ As battery have small capacity and recharging by energy scavenging is complicated, the energy consumption of a sensor node must be tightly controlled

→ The main consumers of energy are the controller the radio front end and memory

→ To reduce power consumption of these comps comes from chip level and lower technologies

→ Designing low power chip is the best point for energy efficient sensor node

→ Using multiple states of operation with reduced energy consumption for reduced functionality is a technique for energy efficient sensor.

→ For a controller typical states are 'active', 'Idle' and 'sleep'

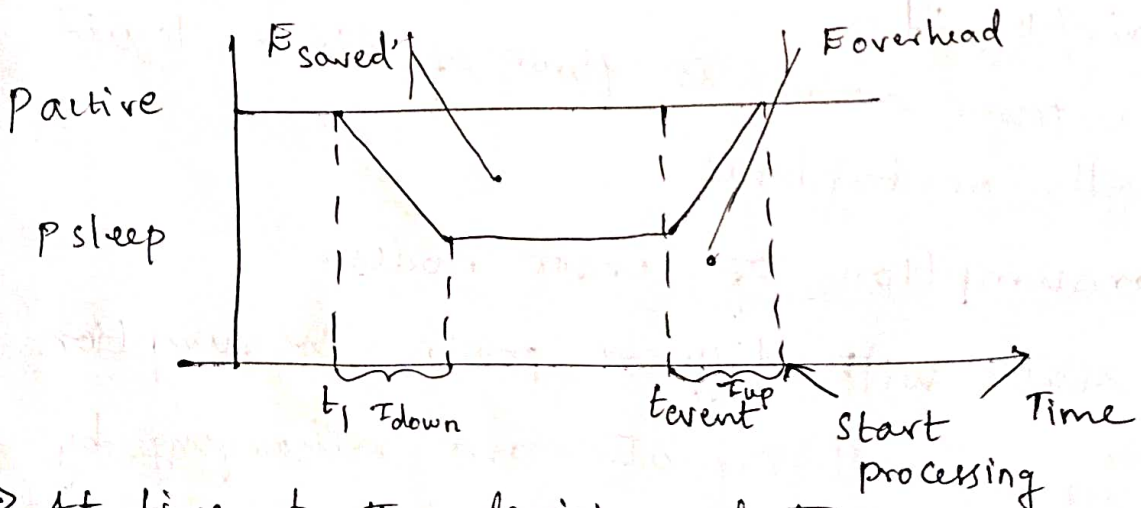
→ A radio modem could turn transmitter, receiver or both on or off.

→ sensors and memory could also be turned on or off.

→ In 'deeper sleep' state less power is consumed

→ more time and energy is taken to wake up from deeper sleep state

→ The fig. illustrates the commonly used model



→ At time t_1, the decision whether or not a component put into sleep mode, is taken for reduce power consumption from P_{active} to P_{sleep}

If it remains active and the next event occurs at time t_{event}, then a total energy of

$$E_{active} = P_{active}(t_{event} - t_1)$$

has been spent useless

→ Putting the component to sleep mode requires a time τ_{down} until sleep mode is reached.

→ The average power consumption during this phase is

$$(P_{active} + P_{sleep})/2$$

P_{sleep} is consumed until t_{event}

→ In total

$$= \tau_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down}) P_{sleep}$$

energy is required in sleep mode as oppose to

$(t_{event} - t_1) P_{active}$ → when remaining active

The energy saving is

$$E_{saved} = (t_{event} - t_1) P_{active} - (\tau_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - \tau_{down}) P_{sleep}$$

→ Once the event processed occurs, an additional overhead of

$$E_{overhead} = \tau_{up}(P_{active} + P_{sleep})/2$$ is incurred to come back to operational state

→ No useful activity is done in this time

→ so switching to sleep mode is only beneficial if

$E_{overhead} < E_{event}$, or if the time to next operation

event is sufficiently large

$$(t_{event} - t_1) > \frac{1}{2}\left(\tau_{down} + \left(\frac{P_{active} + P_{sleep}}{P_{active} - P_{sleep}}\right)\tau_{up}\right)$$

Microcontroller energy consumption.

Basic power consumption in discrete operational stat
Embedded controllers implement the concept of multiple
operational state. Some examples are

Intel StrongARM :

→ provides three sleep states

1) In normal mode → all parts are fully powered

2) In Idle mode → clk to CPU are stopped, clk that pertain to pheripherals are active

3) In sleep mode → only real time clk is active

Texas Instruments

→ wide range of operating modes

→ 4 sleep modes in total

Atmel ATmega:

→ 6 different modes for power consumption

Dynamic Voltage Scaling:

→ The idea is to choose best possible speed to compute a task in a given dead line

- The solution is to switch the controller in fully operative mode, compute the task at high speed and go back to sleep mode as quickly as possible

→ next approach is to compute the task only at the speed required to finish before deadline

⇒ the fact that a controller running at lower speed at lower clock rates, consumes less power than at full speed

→ the supply voltage is reduced at lower clock rates. This technique is called Dynamic Voltage Scaling (DVS)

→ Power consumption depends on frequency $P_d \propto V_{DD}^2$

Memory:

→ From energy perspective, the most relevant kinds of memory are on chip memory and FLASH memory

→ The power needed to drive an chip is included in power consumption

→ The use of FLASH memory heavily influence node lifetime

→ Read times and read energy consumption is similar in different types of FLASH memory

Radio transceivers

→ It has two tasks, transmitting and receiving data

→ It operates in different modes

→ For low total energy consumption, the transceivers should be turned off.

Modelling energy consumption during transmission

→ The energy consumed by a transmitter is due to two sources

→ one part is due to RF signal generation depends on chosen modulation and target distance (ie) transmission power P_{tx}, the power radiated by antenna

→ second part is due to electronic components for frequency synthesis, frequency conversion, filters and so on.

→ The transmitted power is generated by amplifier of transmitter

$$P_{amp} = \alpha_{amp} + \beta_{amp} P_{tx}$$

α_{amp}, β_{amp} are constants depending on process technology

* The efficiency of power amplifier is

$$\eta_{PA} = \frac{P_{tx}}{P_{amp}}$$

→ The energy to transmit a packet 'n' bits long depends on how long it takes to send the packet; by nominal bit rate R and coding rate R_{code}.

$$E_{tx}(n, R_{code}, P_{amp}) = T_{start} P_{start} + \frac{n}{R R_{code}} (P_{txElec} + P_{amp})$$

$P_{tx\,Elec}$ → power due to other circuitry.

Modelling energy consumption during reception.

Like transmitter, the receiver can be either turned off or on.

E_{rcvd} – energy required to receive a packet has a start up component $T_{start} P_{start}$

$$E_{rcvd} \approx T_{start} P_{start} + \frac{n}{R \cdot R_{code}} P_{relec} + n E_{dec\,Bit}$$

$P_{dec\,Bit}$ → decoding energy

Dynamic Scaling of radio power consumption

→ Scaling down supply voltage or frequency to obtain lower power consumption

→ For radio communication it includes the choice of modulation

Dynamic Modulation Scaling (DMS), Dynamic code Scaling (DCS), Dynamic Modulation code Scaling (DMCS).

Relation between computation and communication

→ Communication is more expensive than computation

→ still energy required for compution cannot be ignored

Power consumption of sensors and actuators

→ For passive light or temperature sensors → power consumption is ignored

→ For active devices like sonar, power consumption is considered in dimensioning of power sensors

Optimization Goals and Figure of Merit

i) Quality of Service

→ QoS is regarded as low level, networking device observable attribute

→ QoS depends on application like

1) Event detection
2) Event classification error
3) Event detection delay
4) Missing reports
5) Approximation accuracy
6) Tracking accuracy

ii) Energy Efficiency

→ Energy is precious resource in WSN

The most commonly considered aspects are

1) Energy per bit
2) Energy per reported event
3) Delay energy
4) Network life time
5) Time to first node
6) Time to partition
7) Time to failure of first notification

Network Architecture

→ A sensor node can gather information from other sensor node

Two Types
- i) layered Architecture
- 2) clustered Architecture

Layered Architecture

→ It consists of single powerful base station

→ It uses military sensor based infrastructure

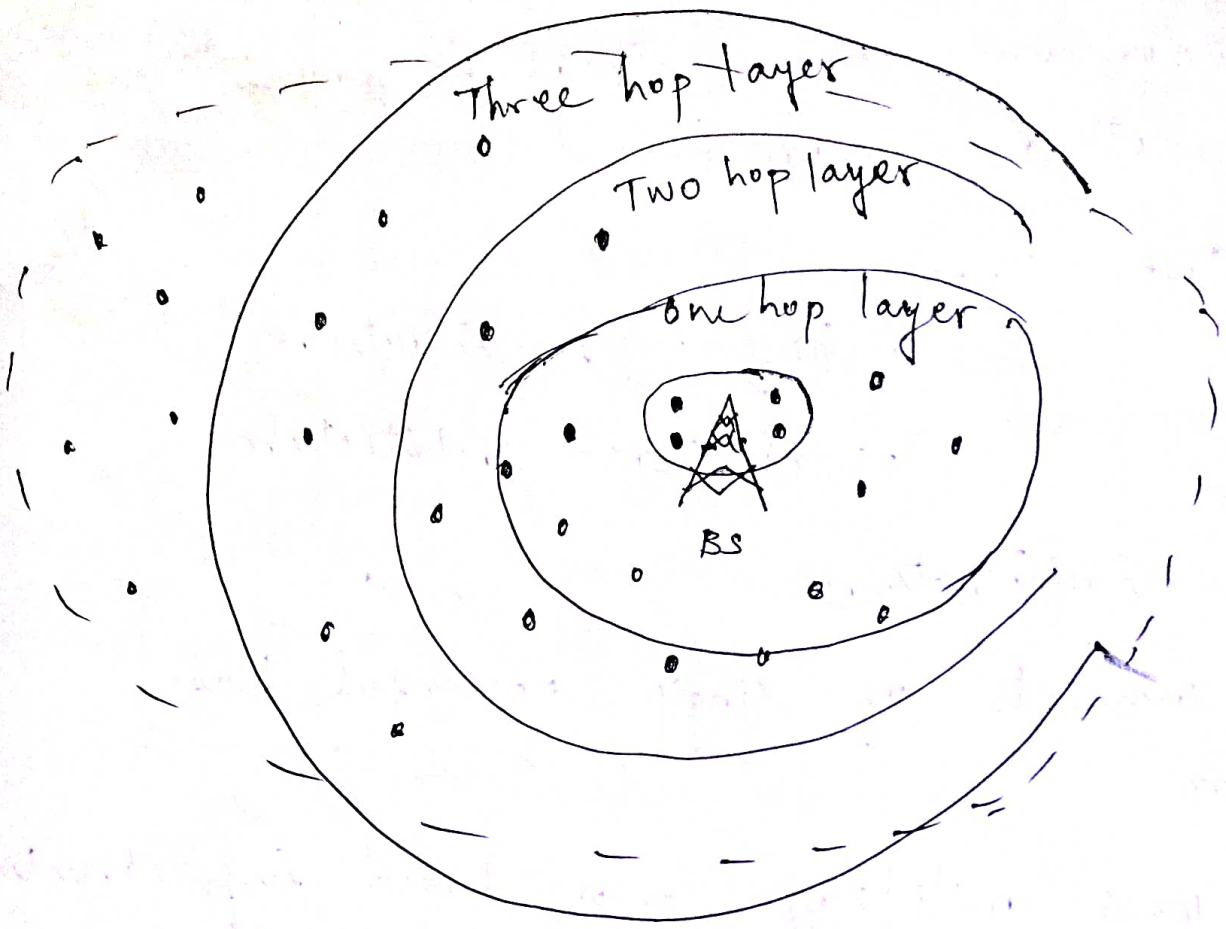
→ Base station acts as fixed point to a wired network.

→ the small sensor nodes form a wireless backbone

→ It uses Unified Network Protocol Framework (UNPF)

operation :- Network intialisation and maintenan

→ The protocol organizes the sensor node into different layer



• — Sensor node

(_ _) — Coverage area

→ Base station communicate with all nodes using one hop

→ BS broadcasts its identifier to sensor nodes using CDMA

→ Each node sends its ID at lowest powerlevel

→ The layer one node form layer two with nodes which are one hop away from layer one node

eration 2 MAC

→ The Distributed TDMA Receiver oriented channel assignment MAC protocol is used

The two operation are

1) channel allocation
2) channel scheduling

Clustered Architecture

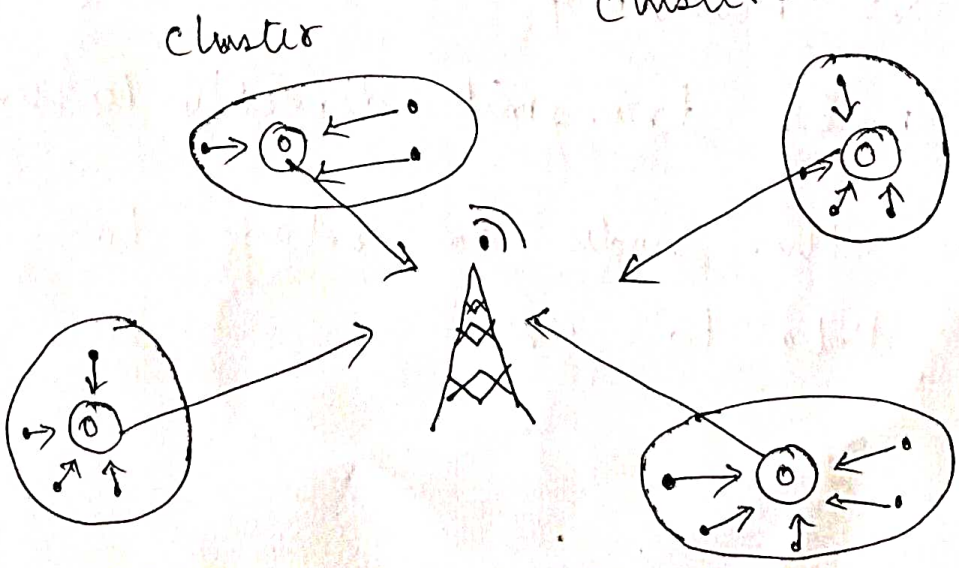
→ It organizes the nodes in sensor network into clusters

→ Each cluster has cluster head

→ The nodes in each cluster exchange message within the cluster

→ Each cluster head also communicate with BS which is an access point

Clustered Architecture

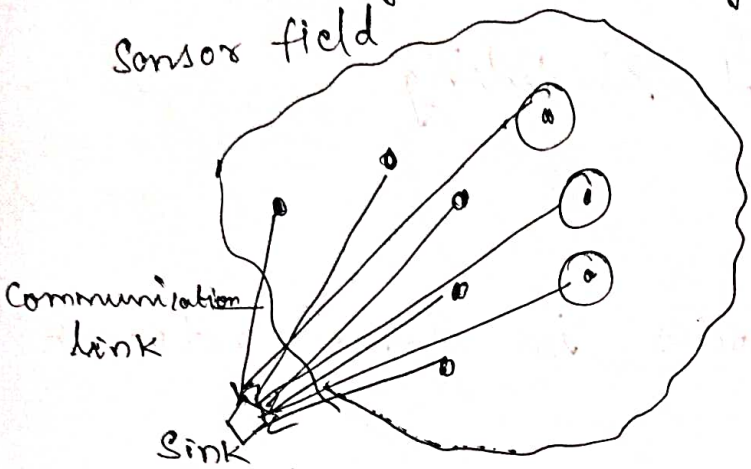


Sensor Network Scenarios

1. Homogenous Vs Hetrogenous networks

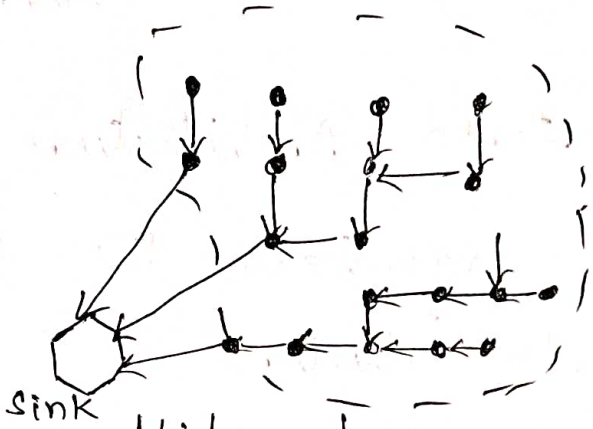
→ In homogenous, all sensor nodes have same sensing, processing, communication

→ In heterogenous, they have different capabilities



Single hop, heterogenous

a → normal sensor node



multi hop homogenous

① → Advanced sensor node

2) Stationary Vs Mobile

→ In stationary all mobile nodes are fixed

→ Mobile sensor node is equipped with locomotive unit

3) Single hop Vs Multihop

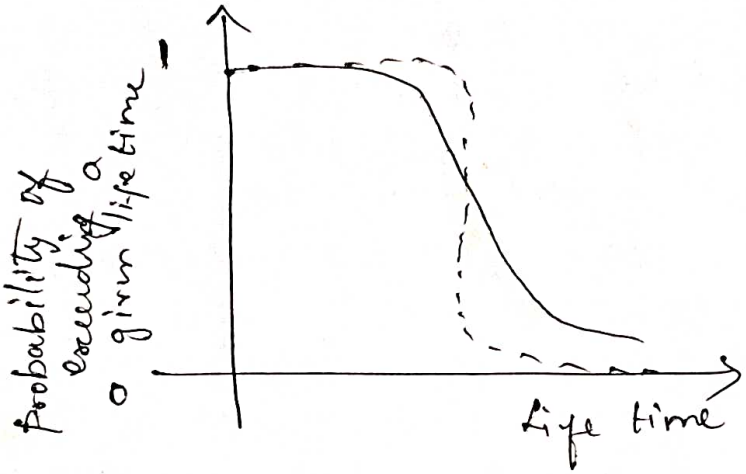
→ Single hop all nodes transmit directly to sink

→ Multihop has other nodes as relays to deliver their data to sink.

Scalability:

→ It is ability to maintain performance irrespective of size

→ Architectures & protocols should implement appropriate scalability



Two probability curve of a node exceeding the given lifetime - the dotted curve tracks off better

Robustness

→ WSN expected to exhibit appropriate robustness

→ they should not fail just because a limited no. of nodes run out of energy,

→ the failure must be compensated for finding other routes

UNIT - III

WSN NETWORKING CONCEPTS & PROTOCOLS

MAC protocols for Wireless Sensor Networks, Low Duty cycle protocols and Wakeup Concepts - S-MAC, The Mediation Device protocol, Contention based protocols - PAMAS, Schedule based protocols - LEACH, IEEE 802.15.4 MAC protocol, Routing protocols - Energy Efficient Routing, Challenges and Issues in Transport Layer protocol.

Wireless MAC Protocols :

Medium Access Control (MAC) protocols is the first protocol layer above the physical Layer (PHY) and consequently MAC protocols are heavily influenced by its properties. The fundamental task of any MAC protocol is to regulate the access of a number of nodes to a shared medium in such a way that certain application-dependent performance requirements are satisfied. Some of the traditional performance criteria are delay, throughput, and fairness,

Whereas in WSNs, the issue of energy conservation becomes important

The MAC protocol determines for a node the points in time when it accesses the medium to try to transmit a data, control, or management packet to another node (unicast) or to a set of nodes (multicast, broadcast).

Requirements and design constraints for wireless MAC protocols.

Traditionally, the most important performance requirements for MAC protocols are throughput efficiency, stability, fairness, low access delay and low transmission delay, as well as a low overhead. The overhead in MAC protocols can result from per-packet overhead, collisions, or from exchange of extra control packets. Collisions can happen if the MAC protocol allows two or more needs to send packets at the same time. Collisions can result in the inability of the receiver to decode a packet correctly, causing the upper layers to perform a retransmission.

The operation and performance of MAC protocol is heavily influenced by the properties of the underlying physical layer. since WSNs use a wireless medium, they inherit all the well-known problems of wireless transmission. One problem is time-variable, and sometimes quite high, error rates, which is caused by physical phenomena like slow and fast fading, path loss, attenuation, and man-made or thermal noise.

The hidden-terminal problem occurs specifically for the class of carrier Sense Multiple Access (CSMA) protocols, where a node senses the medium before starting to transmit a packet. If the medium is found to be busy the node defers its packet to avoid a collision and a subsequent retransmission Consider the example in figure Here, we have three nodes A, B and C that are arranged such that A and B are in mutual range, B and C are in mutual range, but A and C cannot hear each other. Assume that A starts to transmit a packet to B and Some time later node C also decides to starts a packet transmission. A carrier-sensing operation by C shows an idle medium since C cannot hear A's signals. When C starts its packets, the signals collide at B and both packets are useless. Using Simple

CSMA in a hidden-terminal scenario thus leads to needless collisions.

In the exposed-terminal scenario, B transmits a packet to A, and some moment later, C wants to transmit a packet to D. Although this would be theoretically possible since both A and D would receive their packets without distortions, the carrier-sense operation performed by C suppresses C's transmission and bandwidth is wasted. Using Simple CSMA in an exposed terminal scenario thus leads to needless waiting.

Two Solutions to the hidden-terminal and exposed-terminal problems are busy-tone solutions and the RTS/CTS handshake used in the IEEE 802.11 WLAN standard.

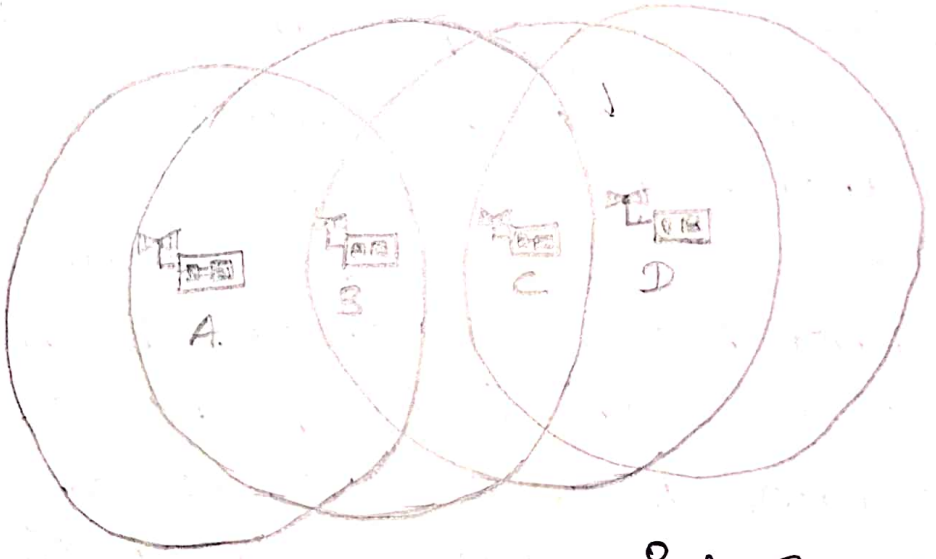


Fig: Hidden-terminal Scenario

On wired media, it is often possible for the transmitter to detect a collision at the receiver immediately and to abort packet transmission. This feature is called collision

detection (CD) and is used in Ethernet's CSMA/CD protocol to increase throughput efficiency. Such a collision detection works because of the low attenuation in a wired medium, resulting in similar SNRs at transmitter and receiver. Consequently, when the transmitter reads back the channel signal during transmission and observes a collision, it can infer that there must have been a collision at the receiver too. More importantly, the absence of a collision at the transmitter allows to conclude that there was been no collision at the receiver during the packet transmission.

Important classes of MAC protocols

- → Fixed assignment protocols
- → Demand assignment protocols
- → Random assignment protocols

→ Fixed assignment protocols

In this class of protocols, the available resources are divided between the nodes such that the resource assignment is long term and each node can use its resources exclusively without the risk of collisions. Long term means that the assignment is for durations of minutes, hours, or even longer, as opposed to the short-term case where assignments have a scope of a data burst, corresponding to a time horizon of perhaps milliseconds.

Typical protocols of this class are TDMA, FDMA, CDMA and SDMA.

→ Demand assignment protocols

In demand assignment protocols, the exclusive allocation of resources to nodes is made on a short-term basis, typically the duration of a data burst. This class of protocols can be broadly subdivided into centralized and distributed protocols.

In central control protocols the nodes send out requests for bandwidth allocation to a central node that either accepts or rejects the requests. In case of successful allocations, a confirmation is transmitted back to the requesting node along with a description of the allocated resource, for example, the number and positions of assigned time slots in a TDMA system and the duration of allocation.

→ Random access protocols:

The nodes are uncoordinated, and the protocols operate in a fully distributed manner. Random access protocols often incorporate a random element, for example, by exploiting random packet arrival times, setting timers to random values, and so on. One of the first and still very important random access protocols is the ALOHA or slotted ALOHA protocol, developed at the University of Hawaii.

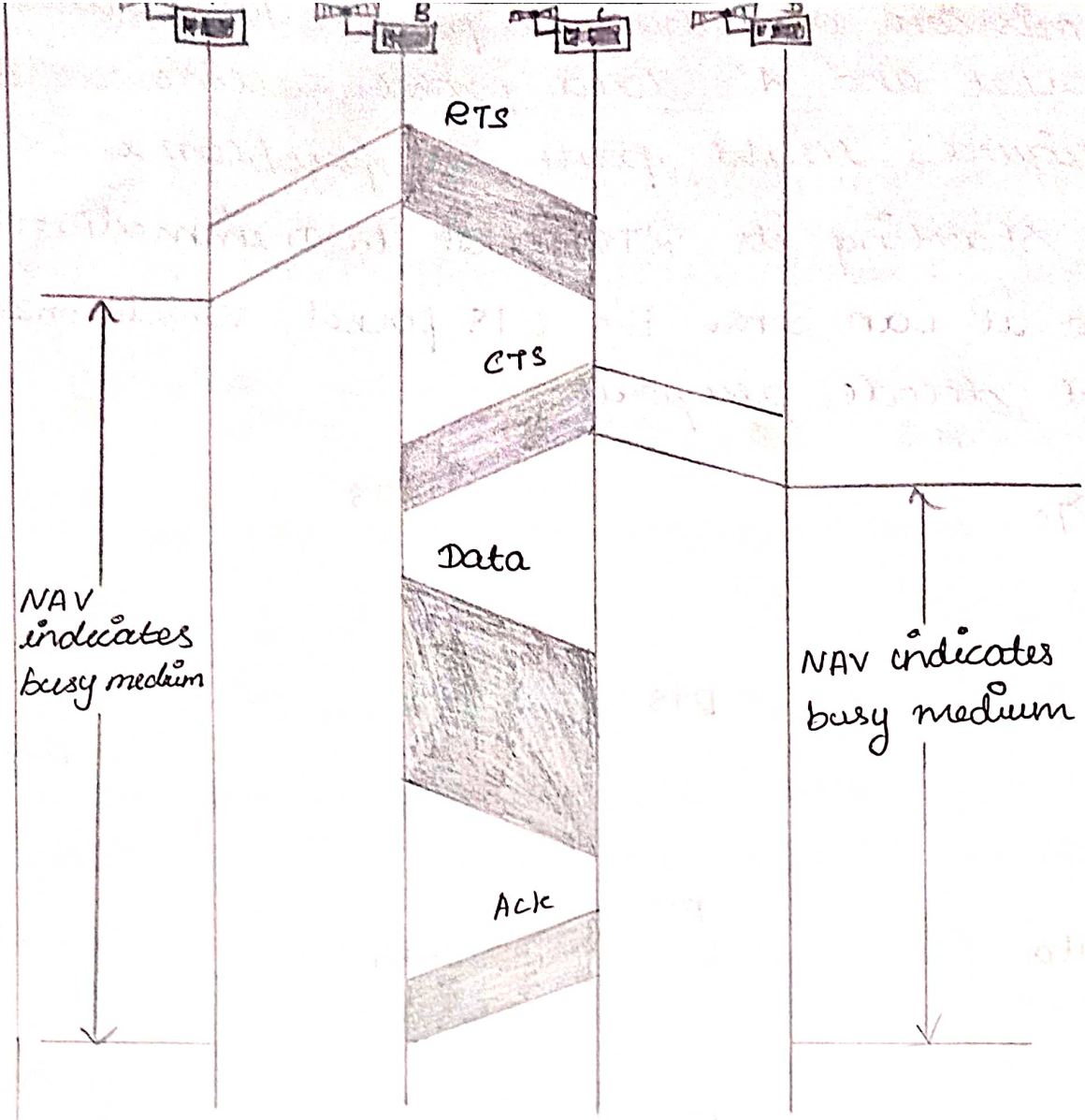


Fig: RTS/CTS handshake in IEEE 802.11

In the left part of the figure, nodes A and B run the RTS - CTS - Data - Ack sequence, and B's CTS packet also reaches node C. However, at almost the same time, node D sends an RTS packet to C, which collides at node C with B's CTS packet. This way, C has no chance to decode the duration field of the CTS packet and to set its NAV variable accordingly. After its failed RTS packet, D sends the RTS packet again to C and C answers with a CTS packet. Node C is doing so because it cannot hear A's ongoing

transmission and has no proper NAV entry. C's CTS packet and A's data packet collide at B. In the figure's right part, the problem is created by C starting its RTS packet to D immediately before it can sense B's CTS packet, which consequently cannot decode properly.

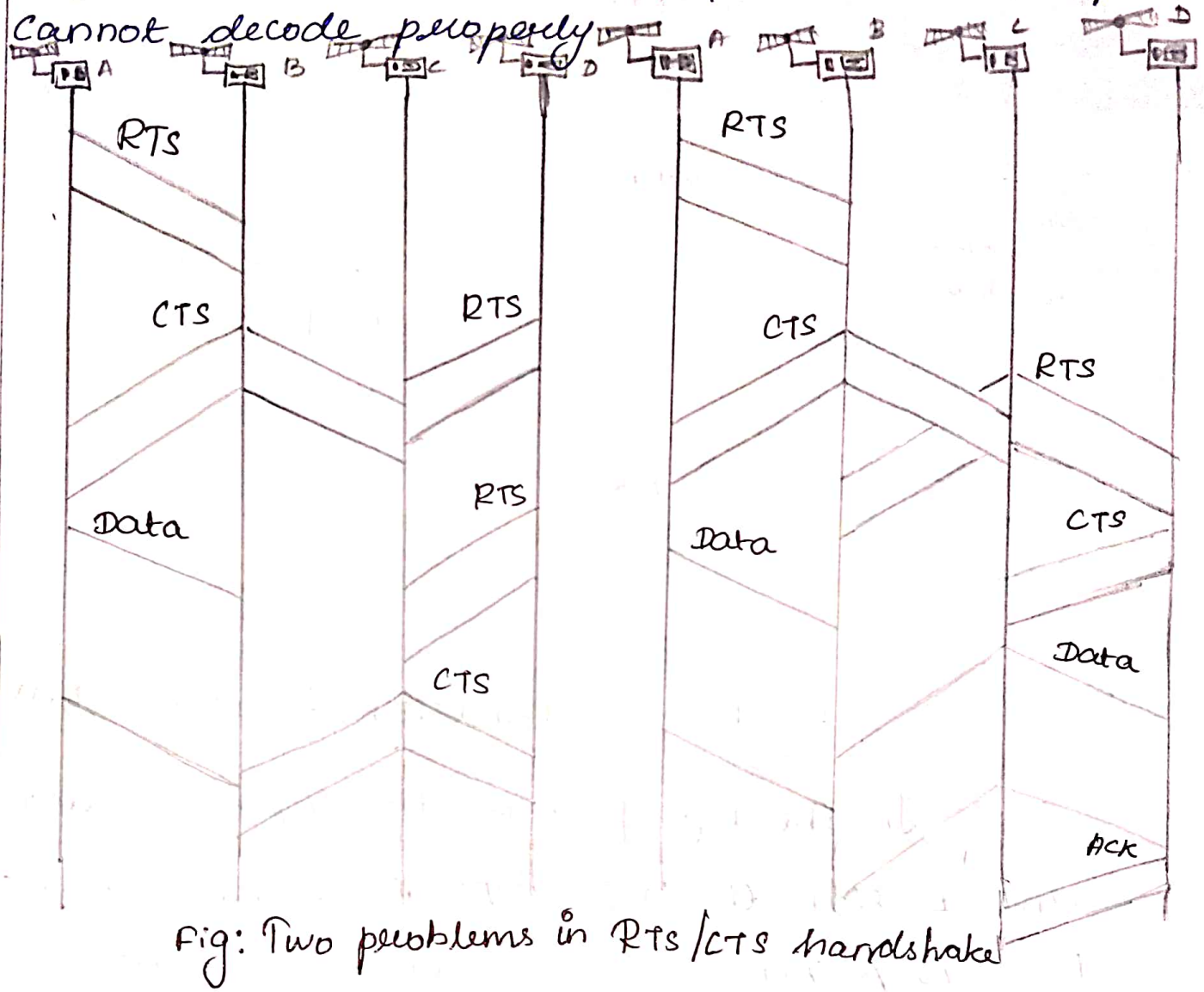


Fig: Two problems in RTS/CTS handshake

In this section, we narrow down the specific requirements and design considerations for MAC protocols in wireless sensor networks.

Balance of requirements

For the case of WSNs, the balance of requirements is different from traditional networks. Additional requirements come up, first and foremost, the need to conserve energy

The importance of energy efficiency for the design of MAC protocols is relatively new and many of the "classical" protocols like ALOHA and CSMA contain no provisions toward this goal.

Energy problems on the MAC layer

A nodes transceiver consumes a significant share of energy. A transceiver can be in one of the four main states: transmitting, receiving, idling or sleeping. In short: Transmitting is costly, receive costs often have the same order of magnitude as transmit costs, idling can be significantly cheaper but also about as expensive as receiving and sleeping costs almost nothing. Based on these facts, we can derive the following energy problems.

Collisions:

Collisions incur useless receive costs at the destination node, useless transmit costs at the source node, and the prospect to expend further energy upon packet retransmissions.

Overhearing:

Unicast frames have one source and one destination node. However, the wireless medium is a broadcast medium, and all the source's neighbours that are in receive state hear a packet and drop it when it is not destined to them;

protocol overhead:

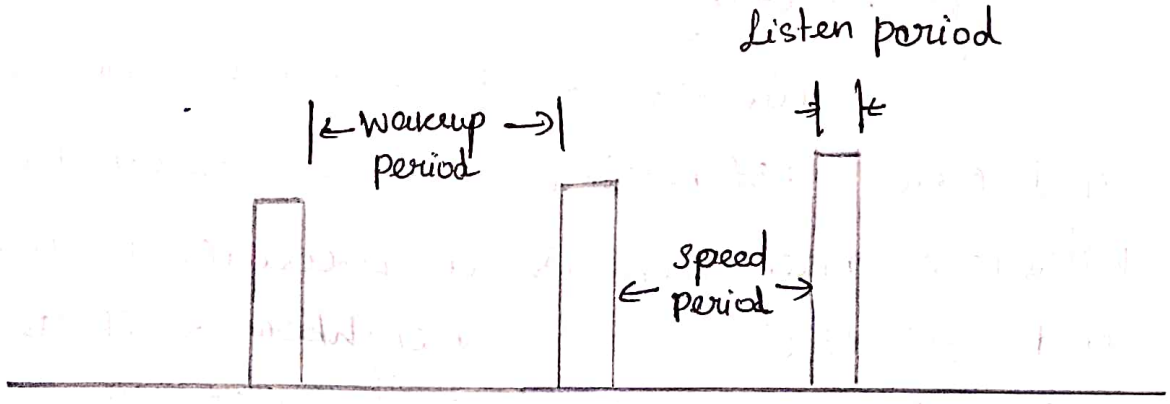
protocol overhead is induced by MAC-related control frames like, for example, RTS and CTS packets or request packets in demand assignment protocols, and furthermore by per-packet overhead like packet headers and trailers.

Idle listening:

A node being in idle state is ready to receive a packet but is not currently receiving anything. This readiness is costly and useless in case of low network loads; for many radio modems, the idle state still consumes significant energy.

LOW DUTY CYCLE PROTOCOLS AND WAKEUP CONCEPTS

Low duty cycle protocols try to avoid spending (much) time in the idle state and to reduce the communication activities of a sensor node to a minimum.



From this discussion, we already can make some important observations:

1. By choosing a small duty cycle, the transceiver is in sleep mode most of the time, avoiding idle listening and conserving energy.

2. By Choosing a small duty cycle, the traffic directed from neighboring nodes to a given node concentrates on a small time window and in heavy load situations significant competition can occur.

3. Choosing a long sleep period induces a significant per-hop latency, since a perospective trans-mitter node has to wait an advantages average of half a sleep period before the receiver can accept packets.

4. In the multihop case, the per-hop latencies add up and create significant end-to-end latencies. Sleep phases should not be too short lest the start-up costs outweigh the benefits.

Mediation device protocol:-

The mediation device protocol is compatible with the peer-to-peer communication mode of the IEEE 802.15.4 low-rate WPAN standard. It allows 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.

There is no global time reference, each node has its own sleeping, schedule and does not take care of its neighbors sleep schedules.

Upon each periodic wakeup, a node transmits a short query beacon indicating its node address and its willingness to accept packets from other nodes. The node stays awake for some ~~packets~~ time following the query beacon to open up a 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 neighbor, it has to synchronize with it. One option would be to have the sender actively waiting for query beacon, but this

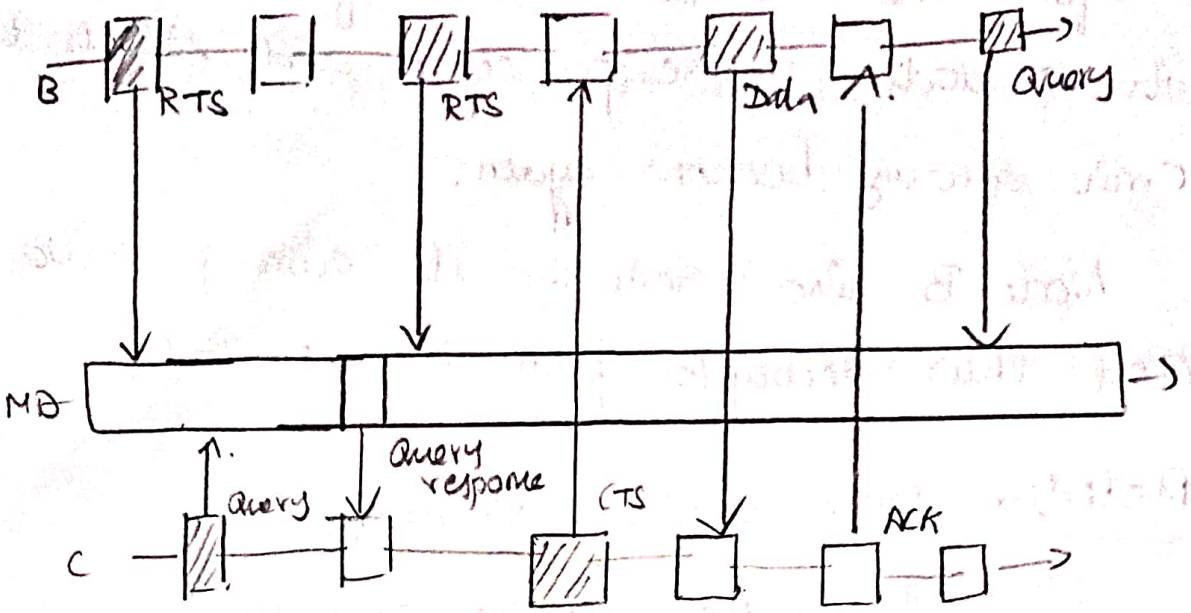
wastes considerable energy for synchronization purpose only.

The dynamic synchronization approach achieves this synchronization without requiring the transmitter to be awake permanently to detect the destinations query beacon. To achieve this a Mediation Device is used. The case where the mediation device is not energy constrained is discussed and can be active all the time, this scenario is illustrated in below figure.

Because of its full duty cycle, the mediation device can receive query beacons from all nodes in its vicinity and learn their wakeup periods.

Suppose that node A wants to transmit a packet to node B. A announces this to the mediation device by sending periodically Request to send (RTS) packets, which the MD captures.

Node A send its RTS packets instead of its query beacons and thus they have the same period. Again there is a short answer window after the RTS packets, where A listen for answers.



▨ -> Transmit mode

□ -> Receive mode

After the MD has received A's RTS packet, it waits for B's next query beacon. The MD answers this with a query response packet, indicating A's address and a timing offset, which lets B know when to send the answering clear to send (CTS) to A such that the CTS packet hits the short answer window after A's next RTS packet.

Therefore, B has learned A's period. After A has received the CTS packet, it can send its data packet and wait for B's immediate acknowledgment.

After the transaction has finished, A restores its periodic wakeup cycle and starts to emit query beacons again.

Node B also restores its own periodic cycle and thus decouples from A's period.

Mediation device protocol advantages:

First it does not require any time synchronization between the nodes. only the mediation device has to learn the periods of nodes.

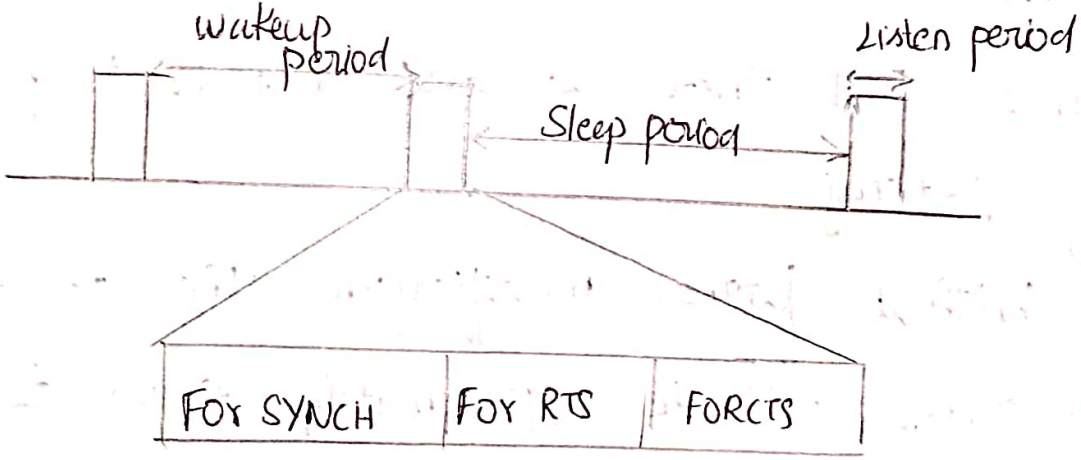
Second the protocol is asymmetric in the sense that the most of the energy burden is shifted to the mediation device, which so far is assumed to be power unconstrained.

Mediation device protocol drawbacks: The node 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 and their wakeup periods overlap.

S-MAC

The S-MAC (Sensor-MAC) protocol provides mechanisms to circumvent idle listening, collisions and overhearing. It does not require 2 different channels.

S-MAC adopts a periodic wakeup scheme, that is each node alternates between a fixed-length listen period and a fixed-length sleep period according to its schedule. 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



SYNCH phase:-

In the first phase node x accepts SYNCH packets from its neighbours. In these packets, the neighbours describe their own schedule and x stores their schedule in a table

RTS phase:-

In this second phase x listens for RTS packets from neighbouring nodes. In S-MAC the RTS/CTS handshake is used to reduce collisions of data packets due to hidden-terminal situations.

CTS phase:-

In the third phase node x transmits a CTS packet if an RTS packet was received in the previous phase. After this the packet exchange continues, extending into x's nominal sleep time.

Wakeup scheme:-

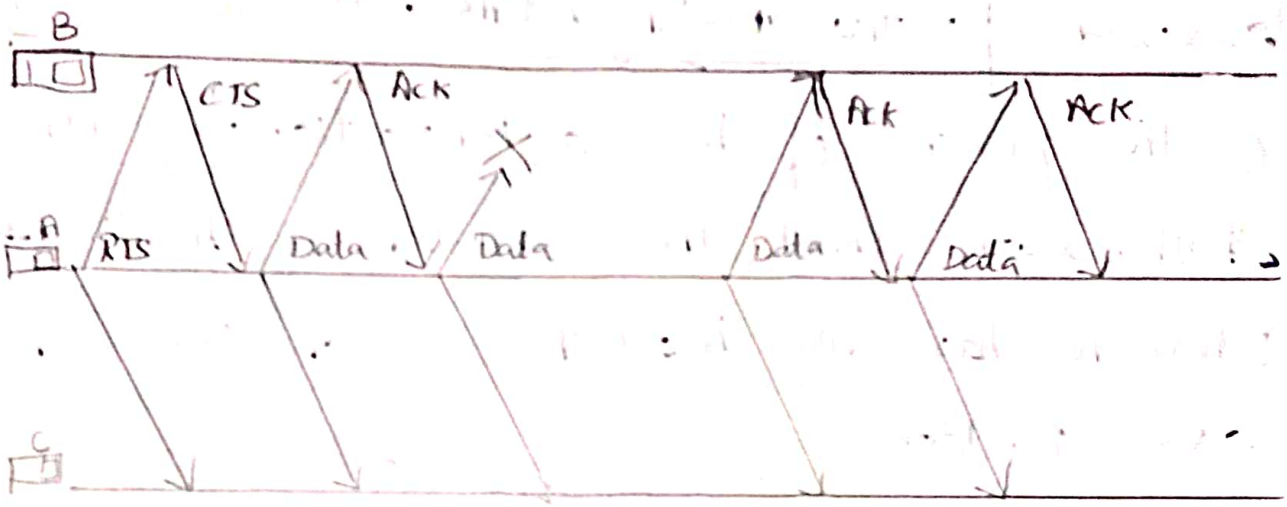
The periodic wakeup scheme adopted by S-MAC allows nodes to spend much time in the sleep mode but there is also a price to pay interms of latency.

Without further modifications, the per-hop latency of S-MAC will be approximately equal to sleep period on average when all nodes follow the same schedule.

The adaptive-listening scheme roughly halves the pre-hop latency.

Message - passing approach:

S-MAC also adopts a message - passing approach. where a message is a larger data item meaningful to the application. In-network processing usually requires the aggregating node to receive a message completely. On the other hand, on wireless media, it is advisable to break a longer packet into several shorter one.



S-MAC includes a fragmentation scheme working as follows:

A series of fragments is transmitted with only one RTS/CTS exchange between the transmitting node A and receiving node B.

After each fragment, B has to answer with an acknowledgment packet.

All the packets have a duration field and a neighboring node C is required to set its NAV field accordingly.

In S-MAC the duration field of all packets carries the remaining length of the whole transaction, including all fragments and their acknowledgments. Therefore the whole message shall be passed at once.

If one fragment needs to be retransmitted, the remaining duration is incremented by the length of data plus ack packet and the medium is reserved for this prolonged time. However, there is the problem of how a nonparticipating node shall learn about the elongation of the transaction when he has only heard the initial RTS or CTS packets.

SMAC has one major draw back: It is hard to adapt the length of the wakeup period to changing load situations, since the length is essentially fixed as is the length of the listen period.

Contention Based Protocols

In contention based protocols, a given transmit opportunity toward a receiver node can in principle be taken by any of its neighbors. If only one neighbor tries its luck, the packet goes through the channel. If two or more neighbors try their luck, these have to complete with each other and in unlucky cases, for example, due to hidden-terminal situations, a collision might occur, wasting energy for both transmitter and receiver.

PAMAS

The PAMAS protocol is originally designed for ad hoc networks. It provides a detailed overhearing avoidance combines while it does not consider the idle listening problem. The protocol combines the busy-tone solution and RTS/CTS handshake similar to the MACA protocol. The distintive feature of PAMAS protocol is that it uses two channels. a data channel and control channel. All the signalling packets are transmitted on the control channel while the data channel is reversed for data packets.

Let us consider an idle node x to which a new packet destined to a neighboring node Y arrives. First x sends an RTS packet on the control channel without doing any carrier sensing. This packet carries both Xs and Y's MAC addresses. If Y receives this packet, it answers with a CTS packet if Y does not know of any ongoing transmission in its vicinity. Upon receiving the CTS, x starts to transmit the packet to Y on the data channel. When Y starts to receive the data, it sends out a busy-tone packet on the control channel. If x fails to receive a CTS packet within some time window, it enters the

backoff mode, where a binary exponential backoff scheme is used

Now let us look at the nodes receiving x's RTS packet on the control channel. There is intended receiver y and there are other nodes; let z be one of them. If z is currently receiving a packet, it reacts by sending a busy-tone packet, which overlaps with y's CTS at node x and effectively destroys the CTS. Therefore x cannot strat transmission and z's packet reception is not disturbed. Since the busy tone packet is longer than the CTS, we can be sure that the CTS is really destroyed. Next, we consider the intended receiver. If y knows about an ongoing transmission in its vicinity, it suppresses its CTS, causing x to back off. Node y can obtain knowledge by either sensing the data channel or by checking whether there was some noise on the control channel immediately after receiving the RTS. This noise can be an RTS or CTS of another node colliding at y. In the other case, y answers with a CTS packet and starts to send out a busy-tone packet as soon as x's transmission has started. Furthermore, y sends out a busy-tone packet as soon as x's transmission has started

Furthermore, Y sends out busy-tone packets each time it receives some noise or a valid packet on the control channel, to prevent its neighborhood from any activities.

A node that receives an RTS packet while being in the backoff state starts its packet reception procedure, that is, it checks the conditions for sending a CTS.

When can a node put its transceivers into sleep mode? Roughly speaking, any time a node knows that it cannot transmit or receive packets because some other node in its vicinity is already doing so. However the decision to go into sleep mode raises an important question: When to wake up again? This decision is easy if a node X knows about the length of an ongoing transmission, for example from overhearing the RTS or CTS packets or the header of the data packet on the data channel.

Suppose that X wakes up and finds the data channel busy. There are two cases to distinguish: either X has no own packet to send or X wants to transmit. In the first case, X desires to go back into sleep mode

Schedule based MAC protocol - Challenges

Although schedule-based MAC protocols can avoid collision, overhearing and idle listening problems.

During network setup and topology changes, the maintenance of Scheduling involves traffic signalling which causes protocol overhead.

A strict time synchronization between the neighboring nodes is required which involves some extra traffic signalling and due to clock drift of oscillators and mobility of nodes, resynchronization is required.

Schedule adaptation becomes difficult with the change of network traffic load.

The node require significant amount of memory to keep its and its neighbors schedule.

Distributed assignment of conflict free TDMA schedules is difficult.

Schedule-bare MAC protocol Challenges.

Although schedule based MAC protocols can avoid collisions, overhearing and Idle listening problems.

During network setup and topology changes the maintenance of scheduling involves traffic

signalling which causes protocol overhead.

A strict time synchronization between the neighboring nodes is required which involves some extra traffic signaling and due to clock drift of oscillators and mobility of nodes, resynchronization is required.

Schedule adaptation becomes difficult with the change of network traffic load.

The nodes require significant of memory to keep its and its neighbors Schedule.

Distributed assignment of conflict free TDMA schedules is difficult.

Schedule based MAC protocol.

In this class of MAC protocols, message delay and bandwidth are readily guaranteed because of the requirement of accurate time synchronization among neighborhood nodes.

A dedicated time slot is allocated to each node for message transmission and the node that owns the slot has the sole access rights on the medium during this time interval.

A scheduler is elected which collects all time slot allocation requests and distributes the final schedule back to the transmitters and receivers

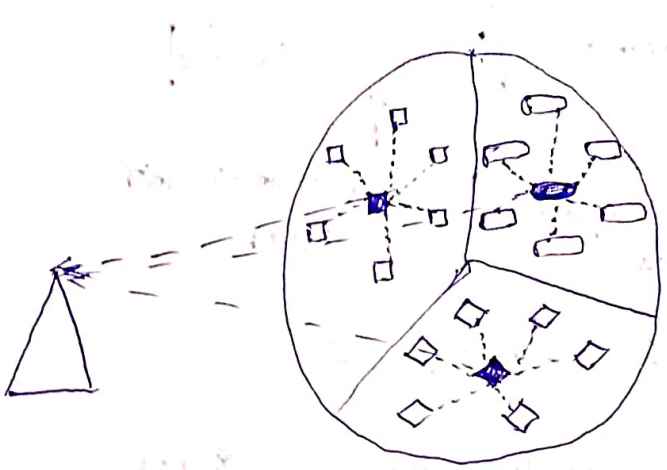
For large wireless networks such as WSNs, clustering may be utilized simpler and less hopping request collection procedure purpose.

Cluster heads are the schedulers and nodes within a cluster send their request to the cluster head. The cluster head schedules the transmissions on the basis of the requests and distributes the time slot assignment to the cluster member.

packets that are destined for the sink must either hop through the cluster heads that form the second tier of nodes

LEACH :- (Low Energy Adaptive Clustering Hierarchy)

It is a TDMA (Time Division Multiple Access) based protocol designed for dense sensor. LEACH partitions the sensor nodes into cluster head in each cluster.



The role of cluster head is to create a TDMA schedule, distribute & maintain this schedule with its cluster members. The cluster head aggregates data of its members & transmits data to the sink.

The cluster head selection is done by each node independently based on the last time the node served as a cluster head.

The non-cluster head choose their cluster head based on the received signal strength. Since the cluster head node is switched on all the time, so it burns its energy quickly and goes to die

In LEACH, each round consists of a setup phase & a steady-state phase. During the setup phase, first node elect themselves as a cluster head based on last serving. After that, in advertisement phase, cluster head nodes inform their neighbours with an advertisement packet. The non-cluster head nodes picks the packet with strongest received signal & inform the cluster head node to join in the cluster during

the cluster setup phase. Now, the cluster head node knows all its member nodes & creates

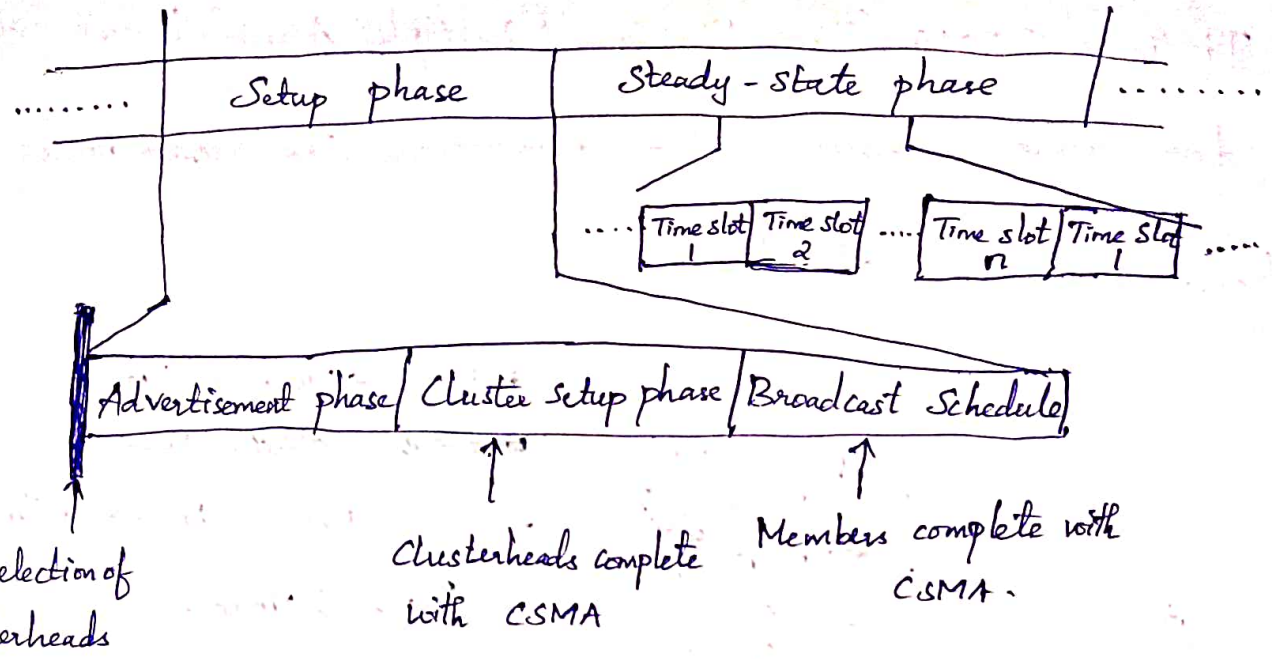


Fig: Organization of LEACH rounds

TDMA schedules with a randomly choosen CSMA code (Avoid interclust interference) for its members and then broadcast the schedule. Now the member nodes know their owned timeslot during which it has to be switched on.

At a time the optimum percentage of clusterhead among all the node of the network is about 5%.

IEEE 802.15.4 MAC PROTOCOL:

In October 2003, The Institude of Electrical & Electronics Engineers (IEEE) finalized the IEEE 802.15.4 standard. The standard covers the physical layer and the MAC layer of a Low-rate WPAN (Wireless Personal Area Network). The targeted applications for IEEE 802.15.4 are in the area of wireless sensor networks, home automation, home networking, connecting devices to a PC, home security, and so on.

The protocol is asymmetric in that different types of nodes with

different roles are used as follows:

(i) Network architecture and types/roles of nodes.

(ii) Super frame structure.

(iii) GTS management

(iv) Data transfer procedures.

(v) Slotted CSMA-CA protocol.

(vi) Non beaconed mode.

(i) Network Architecture and types/roles Of Nodes:-

The standard distinguishes on the MAC layer two types of nodes.

(i) A Full Function Device (FFD):- It can operates in three roles as PAN (Personal Area Network) Co-ordinator, a simple Co-ordinator or a device.

(ii) A Reduced Function Device (RFD): It can operate only as a device.

Co-ordinators can operate in peer-to-peer fashion and multiple Co-ordinators can form a PAN. A co-ordinator has following tasks;

(i) Manage a list of associated devices.

(ii) Allocates short address to its device.

(ii) Super frame Structure:-

The Co-ordinator of a star Network operating in the "beaconed mode" organizes channel accers and transmission with the help of a super frame structure. All super frames have the same length. The co-ordinator starts each super frame by sending a frame beacon packet. The super frame is subdivided into two types. They are,

(i) Active Period:- It is subdivided into 16 time slots. The first time slot

is occupied by the beacon frame & the remaining time slots are partitioned into a CAP (Contention Access Period) followed by a number (maximal seven) of GTSs (Contiguous Guaranteed Time Slots).

(iii) GTS

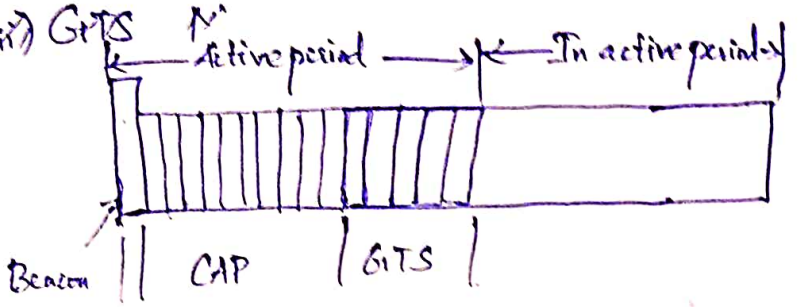


Fig :- Super frame Structure.

(iii) GTS Management :-

The co-ordinator allocates GTS to device only when the latter send appropriate request packets during the CAP. After receiving the acknowledgm packet, the device is required to track the co-ordinator's beacons for some specified time is called a GTS Desc Persistence Time.

A device can use its allocated slots each time they are announced by the co-ordinator in the GTS descriptor. If the co-ordinator has insufficie resources, it generates a GTS descriptor for (invalid) time slot zero, indicati the available resources in the descriptors length fied. Upon receiving such a descriptor, the device may consider renegotiation. A GTS is allocated to a device on a regular basic until it is explicity deallocated. The deallocation can be requested by the devices by means of a special control frame.

(vi) Non Beconed mode :-

(i) In the non beaconed mode, the co-ordinator does not send beacon frames nor is there any GTS mechanism.

(ii) All packets from devices are transmitted using an unslotted CSMA-CA protocol.

(iii) Co-ordinator must be switched on constantly but devices can follow their own sleep schedule.

Devices wakeup for two reasons:

(i) To send a data/control packet to the co-ordinators,

(ii) To fetch a packet destined to itself from the co-ordinator by using the data request/acknowledgement/data/acknowledgement handshake.

(v) Slotted CSMA-CA Protocol:

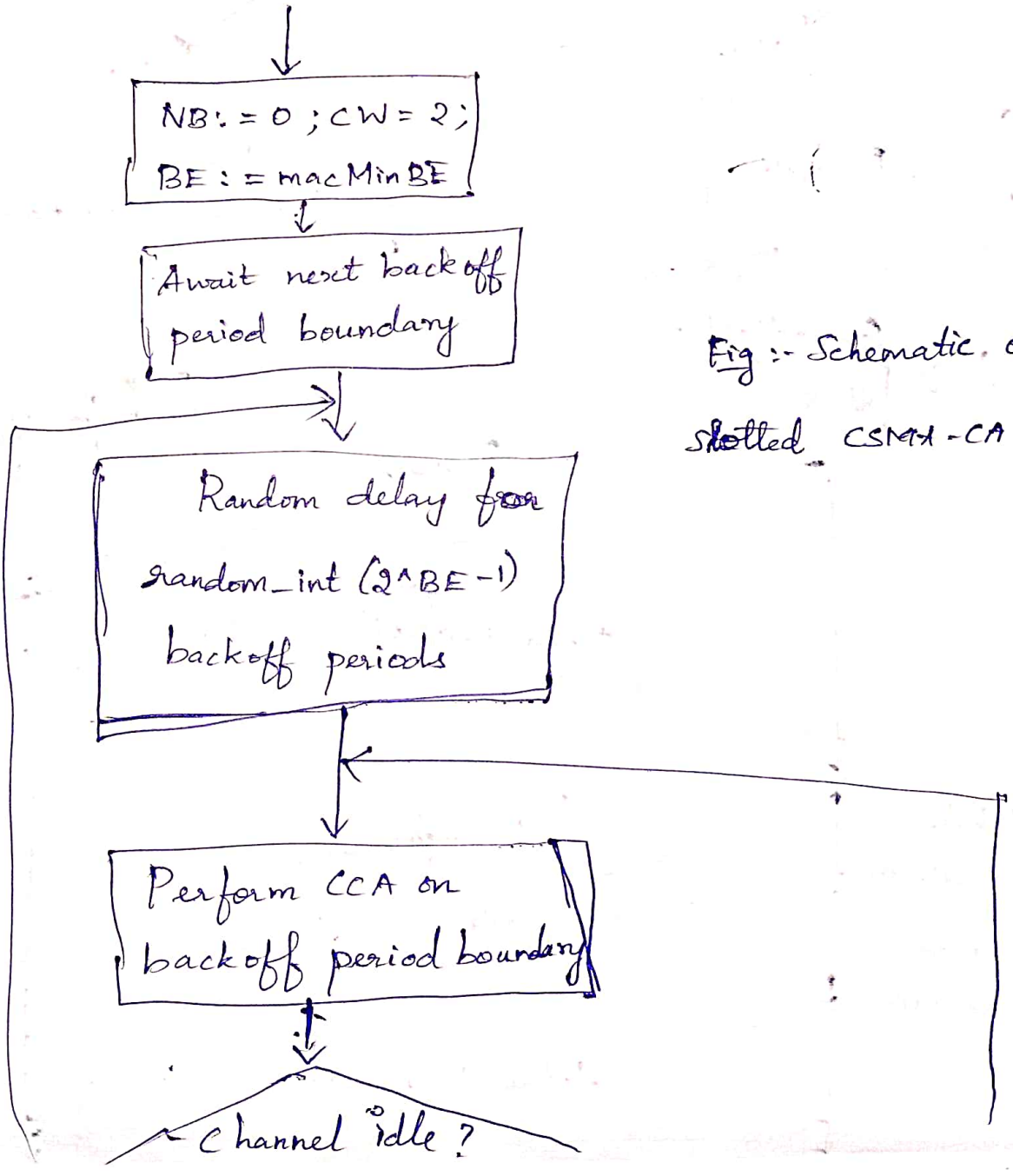
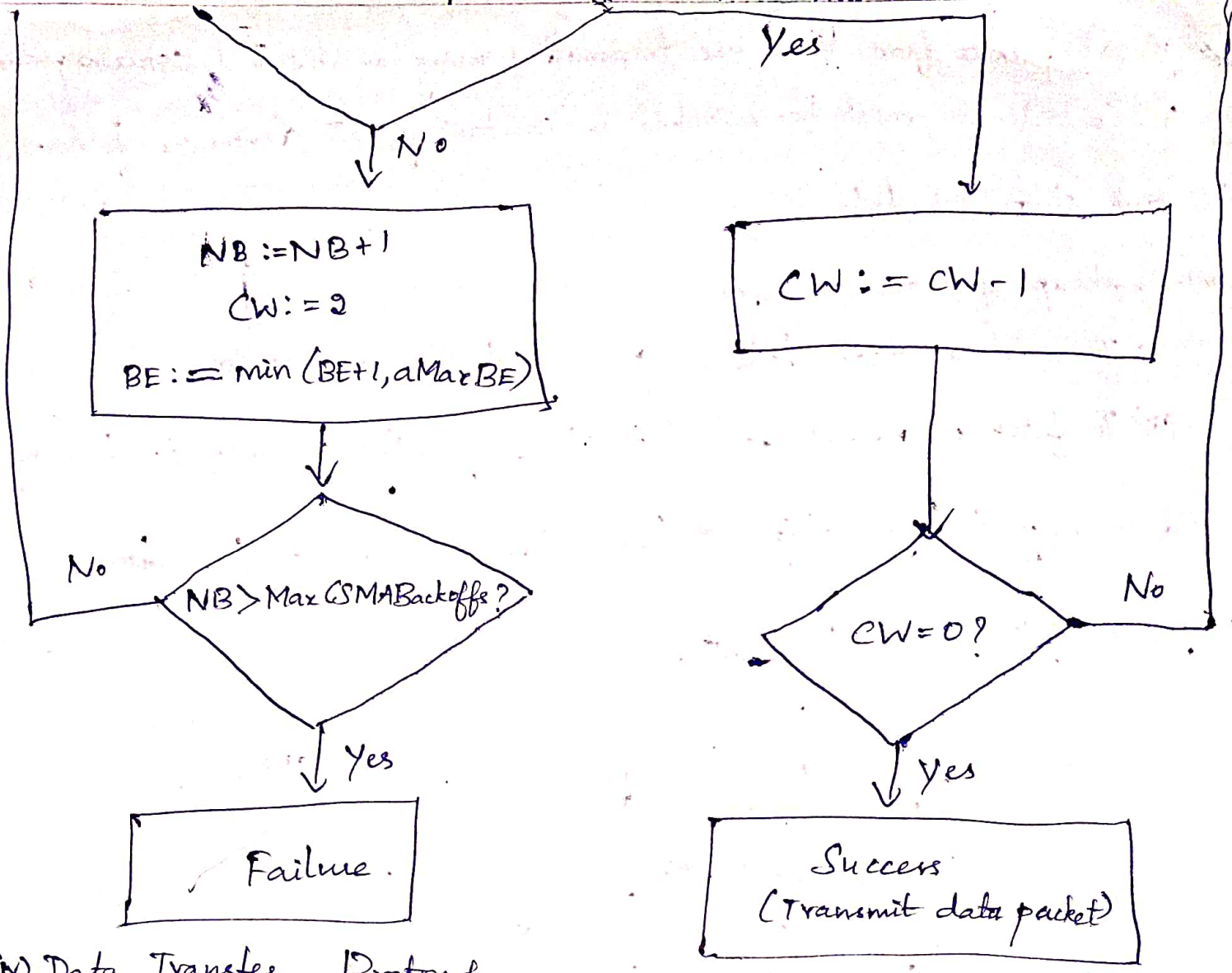


Fig :- Schematic of the slotted CSMA-CA algorithm



(iv) Data Transfer Protocol:-

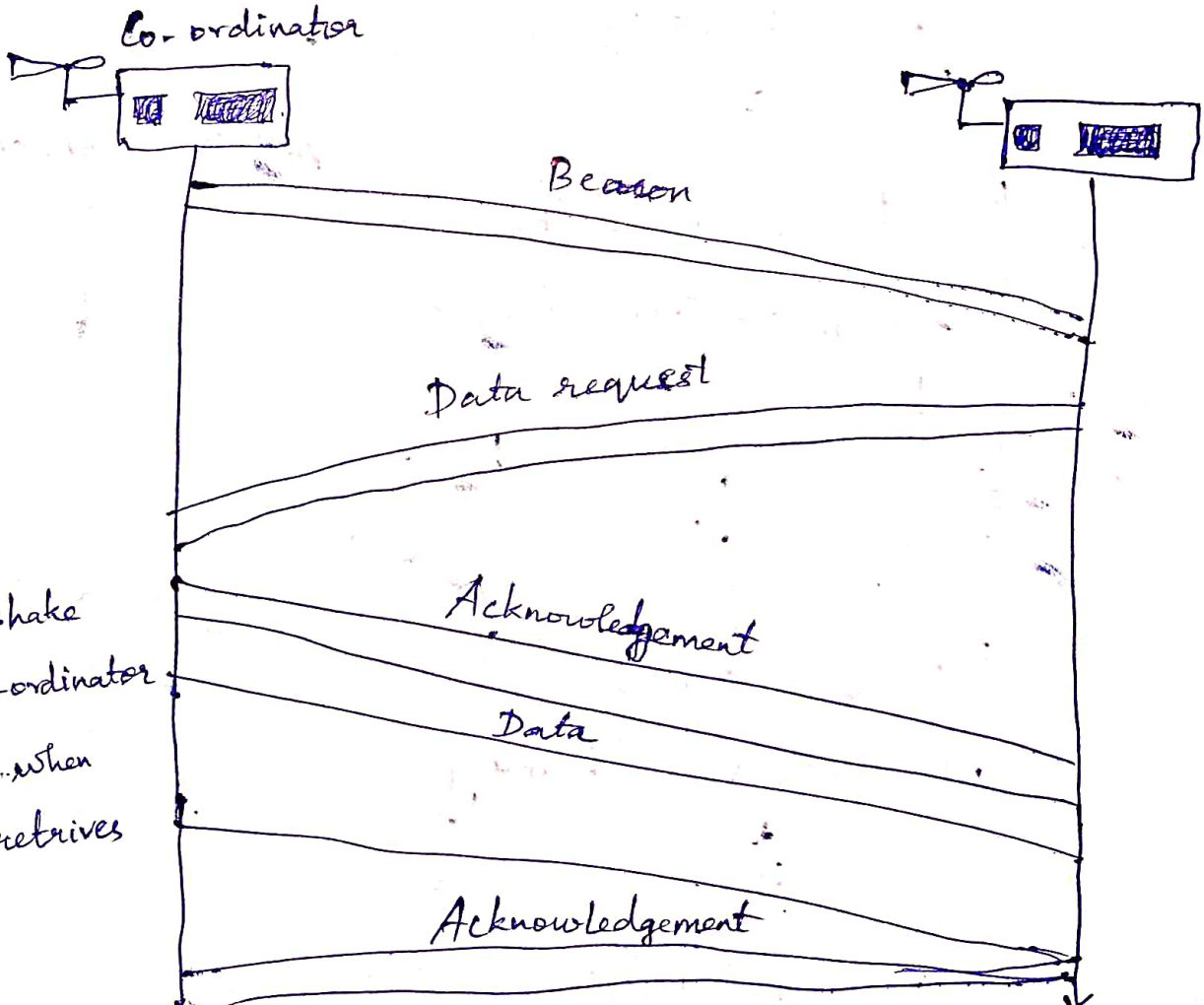
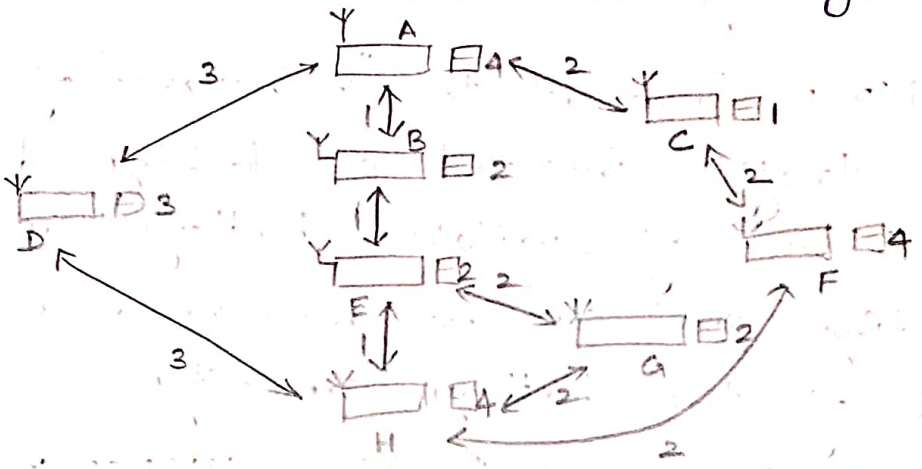


Fig:- Handshake between co-ordinator and device when the device retrives a packets

Routing Protocols:

Energy- Efficient unicast Routing Protocols:-

Energy - efficient unicast routing appears to be a simple problem: take the network graph, assign to each link a cost value that reflects the energy consumption across this link, and pick any algorithm that computes least - cost paths in a graph.



Minimize energy per packet (or per bit):-

The total energy required to transport a packet over a multihop path from source to destination.

Maximize network lifetime:

The network should be capable to fulfill its duty for as long as possible.

Routing Considering available battery energy:-

As the finite energy supply in nodes batteries is the limiting factor to network lifetime,

it stands to reason to use information about battery status in routing decisions. Some of the possibilities are:

* Maximum Total Available Battery Capacity:-

Choose the route where the sum of the available battery capacity is maximized, without taking maximum available power.

*Minimum Battery Cost Routing (MBCR):-

MBCR looks at the "reluctance" of a node to route traffic instead of looking directly into the sum of available battery capacities. The routing cost can be measured as the reciprocal of the battery capacity.

* Min- Max Battery Cost Routing (MMBCR):-

The main idea behind this routing is to protect nodes with low energy battery resources.

*Conditional Max-Min Battery Capacity Routing :- (CMMBCR)

If there are routes along which all nodes have a battery level exceeding a given threshold, then select the route that requires the lowest energy per bit.

*Minimum Total Transmission Power Routing :- (MTPR)

A given transmission is successful it its SINR exceeds a given threshold.

Attracting routes by redirecting:-

Nodes can overhear packet exchanges between other nodes. If in these packets, information about the energy required to communicate between two adjacent nodes x and z is included, a third node y can decide whether it can offer a more energy-efficient route by breaking the direct communication xz into a two-hop communication x-y-z.

Distance vector routing on top of topology control:-

Bellmann-Ford-type algorithm is used to find paths with minimal power consumption in the enclosure graph.

Maximizing time to first node outage:-

It attempt to maximize the time until the first node runs out to energy. To do so, a centralized, flow-based modeling approach is used.

The Zone routing approximation:-

The disadvantage of max min zPmin is that knowledge of battery power levels is required. The "Zone routing" heuristic removes this need.

Challenges and Issues in Transport Layer protocol:

Induced traffic:-

Unlike wired networks, adhoc wireless network utilize multi-hop radio relaying. A link-level transmission affects the neighbour nodes of both the sender and receiver of the link.

Induced throughput unfairness:-

This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the network and MAC layers.

Separation of Congestion control, reliability and flow control:-

A transport layer protocol can provide better performance if end-to-end reliability, flow control and congestion control are handled separately. Reliability and flow control are end-to-end activites, whereas congestion can at times be a local activity.

Power and bandwidth:-

The performance of a transport layer protocol is significantly affected by the constraints such as i, power ii, bandwidth.

Misinterpretation of Congestion:-

Traditional mechanisms of detecting congestion in networks such as packet loss and retransmi-ssion timeout are not suitable for detecting the network congestion in adhoc wireless networks This is because the high error rates of wireless channel, location-dependent contentionetc.

Completely decoupled transport layer:-

Wired network transport layer protocols are almost completely decoupled from the lower layers.

Dynamic topology:-

Some of the deployment scenarios of adhoc wireless networks experience rapidly changing network topology due to the mobility of nodes. This can lead to frequent path breaks, partitioning and remerging of networks and high delay in re-establishment of paths.

Design Goals of a transport layer protocol for Adhoc wireless Networks:-

* The protocol should maximize the throughput per connect.

* It should provide throughput fairness across per connection.

* The transport layer protocol should have mechanisms for congestion control and flow control in the network.

* It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.

* One of the important resources, the available bandwidth, must be used efficiently.

* The protocol should maintain end-to-end semantics.

UNIT-IV

Syllabus Sensor Network Security

Network Security Requirements, Issuses and challanges in security provisioning, Network Security Attacks, layer wise attacks in wireless sensor Networks, possible solutions for jamming, tampering, black hole attack, flooding attack. key Distribution and Management, Secure Rounting - SPINS, reliability requirements in sensor networks.

Wireless Sensor Network - Security Requirements.

According the characteristics, the wireless sensor networks differ from the traditional wireless networks, facing more demands especially in terms of security. In order to resist different kinds of security attacks and threats and to ensure the confidentiality of the tasks performed, the reliability of data generated, the correctness of data fusion, and the security of data transmission, the security requirements are mainly in the following areas.

(1) Data Confidentiality - Data Confidentiality is an important network security need requiring that all sensitive information in the storage and transmission process must ensure its confidentiality. Divulging the content of the information to any unauthorized is not allowed.

(2) Data integrity - With the assurance of confidentiality, an attacker could not get the real content of information, but the recipient does not guarantee that the data it receives is correct, because malicious intermediate nodes can intercept, tamper or disturb the information during the transmission. Through data integrity identification, one can ensure that the data won't change anymore during its transference process.

(3) Data Freshness - Data Freshness view is to emphasize that each of the received data is the latest from the Sender, which makes it stop receiving repeated information. The main purpose to ensure the freshness of the data is to prevent replay attacks.

(4) Availability :- Availability requires the sensor networks that can always provide information access service to the legitimate users according to the preset. But the attacker can make some or all of the sensor network paralyzed by jorging and interfacing signal or other methods to destroy availability of the system. Such as Dos (Denial of service) attacks.

(5) Robustness :- Wireless sensor networks are highly dynamic and uncertain including changes in the network topology and the nodes disappering or joining. Therefore the wireless sensor networks under a variety of security attacks should have strong adaptability, and even in a particular attack succeeds, the performance can make the impact minimized

(6) Access control :- Access control requires the ability to identify the users who access wireless sensor networks to ensure the legitimacy. Access control determines who can access the system, what system resources can be accessed and how to use these resources.

Issues, Challenges and various security Constraints of sensor Networks.

(1) Wireless sensor networks have distinctive as compared to traditional networks making the implementation of existing security measures not practicable.

(2) These constraints construct it impossible to employ the existing strong but complex security solutions to the WSNs. In order to design competent and useful security mechanisms for WSNs, it is essential to understand the constraints in WSN.

(3) Node constraints :- Security solutions need high computation, memory storage and energy resources which create an extra challenge when working with tiny sensor nodes. The resources in this perspective include energy, processing, storage and the communication bandwidth.

(a) Limited memory :- Typical sensor nodes are tiny devices which come with very limited memory and storage capacity. This means any security solution designed for sensor networks should be lesser in code.

(b) Limited energy:- energy is another vital factor to consider when designing security procedures for sensor nodes. Given the sensor network topology which makes accessing them after deployment unbearible, it is very important to restrict the energy consumption and thereby widen the battery life.

(c) Limited processing capability :- Sensor nodes processors are exceptionally slow and they do not support some arthmetic and logic operations.

(d) Limited storage capability :- The memory offered for security is very low. This requires that any security method designed for sensor networks should consume as less memory as possible

(4) Network constraints :- Sensor networks having all the constraints of mobile adhoc networks such as untrust worthy network communication, collison related problems and their lack of physical infra -structure.

(a) unreliable communication
(b) collisions and latency
(c) Limited bandwidth.

(5) physical limitations - Sensor networks are often installed in public and potentially hostile environments, which make some of their components extremely vulnerable to obtain and destruction. To physically secure sensor nodes with tamper proof objects increases the cost.

(a) unattended after deployment
(b) Remotely managed.
(c) Unattended operations
(d) Nature of deployment.

(b) Energy consumption.

The factors which consume energy for their operations,

(a) Sensing energy consumption depends on the hard ware and the application.
(b) An A/D converter for sensor consumes only 3.1 μW, in 31 PJ/8-bit of energy at 1 volt supply

The computing unit related with a wireless sensor is a microcontroller/ processor with memory which can control and function the sensing, computing and communi -cation unit.

The energy consumption of this unit has principally two parts.

* switching energy
* leakage energy.

The dynamically changing workload without degarding performance thus saving energy. Leakage energy is the energy consumed when no computation work is made.

Sleeping - To conserve the energy, sensors can be put into sleep - wake up cycles. when a sensor is in sleep ~~state~~ state, it off some units to conserve energy. There are different types of sleep modes.

Security goals & Services of sensor networks.

The goal of security services in WSN's is to protect information (confidentiality, integrity, authentication; access control & freshness) and resources (availability) from attacks.

1. Authentication.

→ It enables every message sender in the sensor networks, including the base station, sensor nodes and outer users to verify that the data received was actually send by the trusted sender

→ If false data are supplied into the network, then the behaviour of the network could not be predicted.

2. Message integrity.

→ There is the danger that information could be altered when exchanged over insecure network.

→ Integrity controls must be implemented to ensure that information will not be altered in any unexpected way.

→ There is a need to make sure that information is travelling from one end to other end without being intercepted & modified in the process.

3. Verification.

* It empowers every sensor node in the network to confirm the legitimacy of the received message.

* A legitimate message sender might send an authenticated message to the sensor nodes.

* The sensor nodes may not have access to authendication information of the message sender or may not able of performing efficiently the computation that is required to verify authentication information.

4. Freshness

* It ensures that the received message is new and recent one.

* Freshness can be both data freshness and key freshness.

* To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

5. Confidentiality.

Confidentiality is required to ensure that sensitive information is well protected and not revealed to unauthorized third parties

* It helps to protect information traveling between the sensor nodes of the network or between the sensors and the base station from

disclosure.

* A confidential message should not disclose its contents to an eavesdropper.

6. Access control.

→ It ensures that only the authorized sensor is involved in providing information to network services.

→ An authorized user obtains a certain type of data according to his access privileges.

→ Access control is required in those applications of WSN's, which collect variety of data.

7. Availability

It ensures the survivability of sensor network to authorized parties, when needed. in spite of the presence of internal or external attacks.

8. Key distribution

→ It ensures the secure communication should be encrypted and authenticated from distributing the keys among sensors.

→ It is used to provide security for WSN.

Layerwise attacks in WSN & solutions to Attacks.

WSN are vulnerable to various types of attacks. These attacks can be broadly categorized as follows:

1. Attacks on network availability attacks

→ Availability attacks are often referred to as denial of service.

→ DOS attacks may target any layer of a sensor network.

2. Attacks on secrecy & authentication

Standard cryptographic techniques can protect the secrecy & authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

3. Stealthy attack against service integrity.

→ In a stealthy attack, the goal of the attacker is to make the network accept the false data

for eg: An attacker compromises a sensor node and injects a false data throughout the sensor node. In these attacks, keeping the sensor network available for its intended use is essential.

→ DOS attacks against WSN is may permit real-world damage to the health and safety of people.

→ DOS attack can diminishes or eliminates a network's capacity to perform its expected functions.

Black hole attack

* occurs on demand routing protocol.

* when ever node have some information.

ex:- The node has detect some information.

like forest fire, animal moments ~~detect~~

* information share the correspond sink node. with a help of intermediate node only information passed or reached to the corrosponding sink node.

* To create a path the source node can generate to route request packet depends ~~on~~ AOD and forward (or) flooding broadcasting. to the immediate node to the its neighbour hood node.

* It will be passing another intermediate node then again it will be flooding and passed to the corrosponding sink node. ~~and the~~ (or) destination node.

* The destination will stop generated route packet again it will be broadcasting flooding.

* once source node has received this route reply packet which was generated by the corrosponding destination node. assume the path has sucessfully

the of data through the destination node.

*due to this, another important cocept,

* reduce the power supply consumption

* can increase the consme more power and increase delay.

* using this cocept catch route. Intermediate node has enough information about how to reach the corrosponding node,

b) black hole attacks

malicious -> does not have enough information.

* In this atlack, a malicious node fasely advertises good paths to the destination node during the path finding process or in the route update messages.

* The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets beig sent to the distination node concerced.

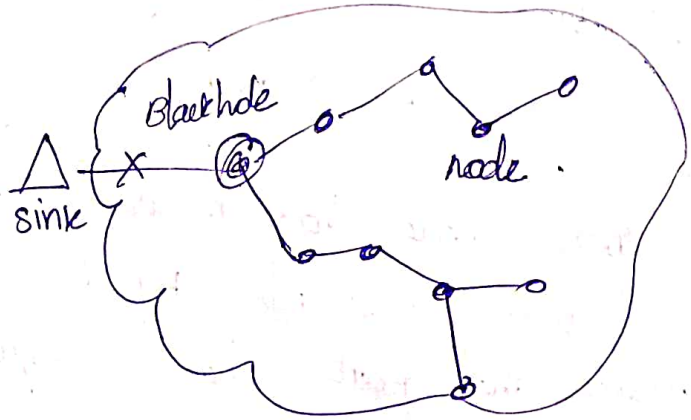
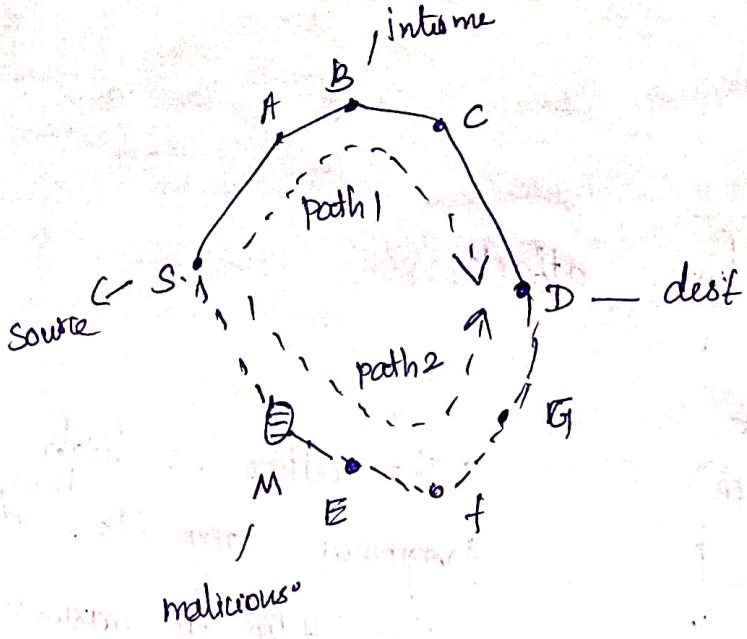


Illustration of black hole problem:



Malicious node that enters the network. it advertises that it has the path to the destiond node D when it receives the route request packet send by node S.

* the attacker may not able to sucess if node A, which also receives the Route request packet from node S replies earlier than node m.

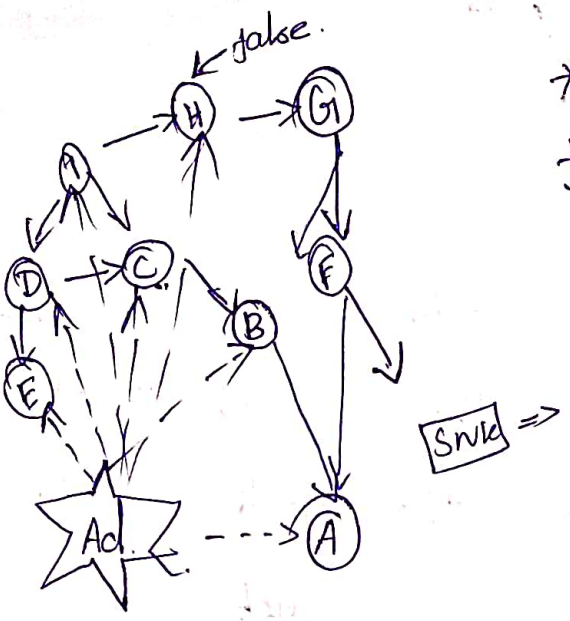
Solutions

* first method:
  * To restrict the intermediate nodes from originating Route reply packets. only the destion node would be permitted to initiate route repty packets

* second method:
  * as soon as the Route reply packets receive from one of the intermediate nodes, another Routes request packet is sent from the source not to the

neighbor node of the intermediate node in the path.

Flooding attack



* The adhoc has high frequency range its send the Hello in maximum distance, so its send neighbor packet

* The high signal strength.

*Many protocoles require nodes to broadcast Hello packets to announce themselves to their neighbours, and a node receiveig such a packet may assume that it is within radio range of the sender.

*This assumption may be fals a lapto-clas attacker broadcastion routing or other information with large enough transmission power could convice every node in the network the the adversary is its neighbour.

Counter meters

* using secret keys method.

*In multipath, multi base station data forwarding technigh. each sensor nodes maintains number of different secrets in a multiple tree.

* sensor node can forward its sensed data to multiple routes by using these secrets. These more multiple base stations in the network that have control over specific number of nodes and also, there are common means of communication among base stations.

*Each base station has all the secrets that are shared by all the sensor nodes, covered by it, according to the key assignment protocol.

* using threshold method:

* A threshold based solution is used to defined against flooting attling in wsn.

*The mobile use a threshold value to check whether its neighbours are intruders or not.

*when the number of route request packets broadcast by a node exceeds the threshold value, it is treated as an intruder and the node stop providing its services to the intruder.

Key distribution and management.

* The main aim of key managent. is to generate a secret key between two parties and store it to prove the authenciby between commuedting users.

* cryptography methods used
  * Symmetric cryptography.
  * Asymmetric cryptography

symmetic cryptograph -> both users
  * enen'ption deefrion.

Asymmetric g key cryptography ->
  * public key * private key.

* Key management is the techniques which support key generation, storage and maintanance of the key between authorized users.

* key management plays an important role in cryptography as the basis for seuring cryptographic goals like,

confidentially.

* during transmission sender

*measured should be known sender and receiver.

authentication

*The receiver was must be known the orginal sender. and receiver.

data authenti integrity.

message should not be altert.

digital signature:

both case uses.

* It is not the case where communicating parities are using same key for encryption and decryption or whether two different keys are used for encryption and decryption.

Basic purpose.

* key generation
* key distribution.
*controlling the use of keys
* updating, destruction of keys and key backup/recovery

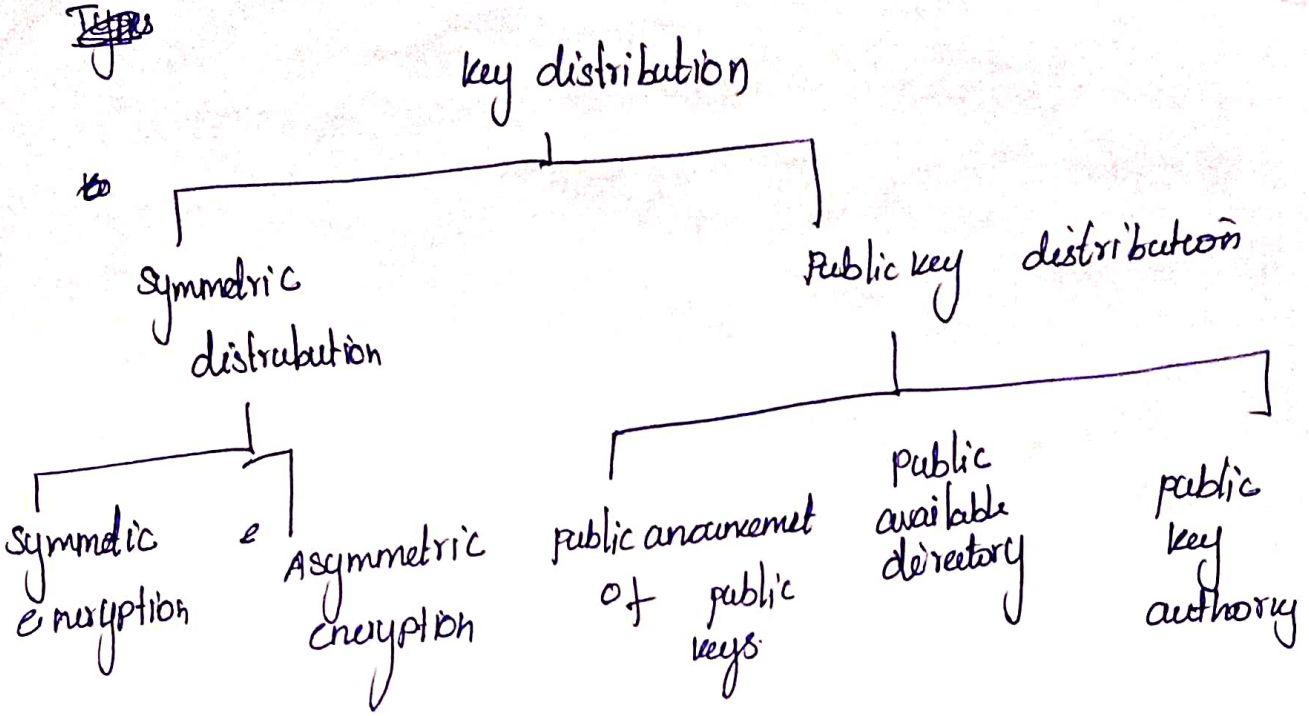
following point to be executed in key management;

* using registration
    * centralized
    * decentralized. -> key must be registered.

* initialization:

* key generation.
* key installation.
* key registration:
* normal use
    encrypted - decrypted.
* key backup
    -> generated by user so must be backup.
* key update.
    some capture the key.
* key de-registration and revocation.
    session is .
* key recovery:
    * key will recover from the backup.

key distribution



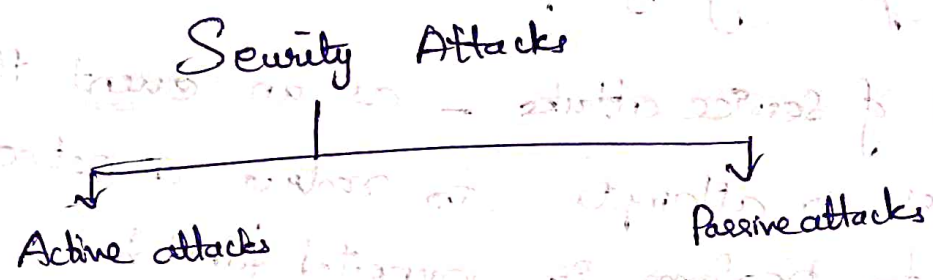
(4) public key - certifi

Possible soultion for Jamming - tampering.

Layer wise Attacks in wireless sensor networks & solutions to Attacks.

Denial of Service Attacks

Physical layer attacks (Jamming, Tampering) & Solutions.



Characteristics:

* Access & modify the information
* System is harmed
* Easy to detect than prevent
* Threat to Integrity, availability

Sender sends the information to the receiver, but the active attacker receives the message that have been sent by the sender & the attacker modifies the message that has been sent by the sender & now the attacker sends the modified message to the receiver. - Active attack.

Characteristics of Passive attack.

* Access information
* No harm to system

Sender is sending the message to the receiver & the passive attacker observes the

message that is being sent by the sender. The passive attacker does not change the information that has to be sent to the receiver. The receiver receives the message exactly it is been send by the sender

Layer wise attacks in WSN:

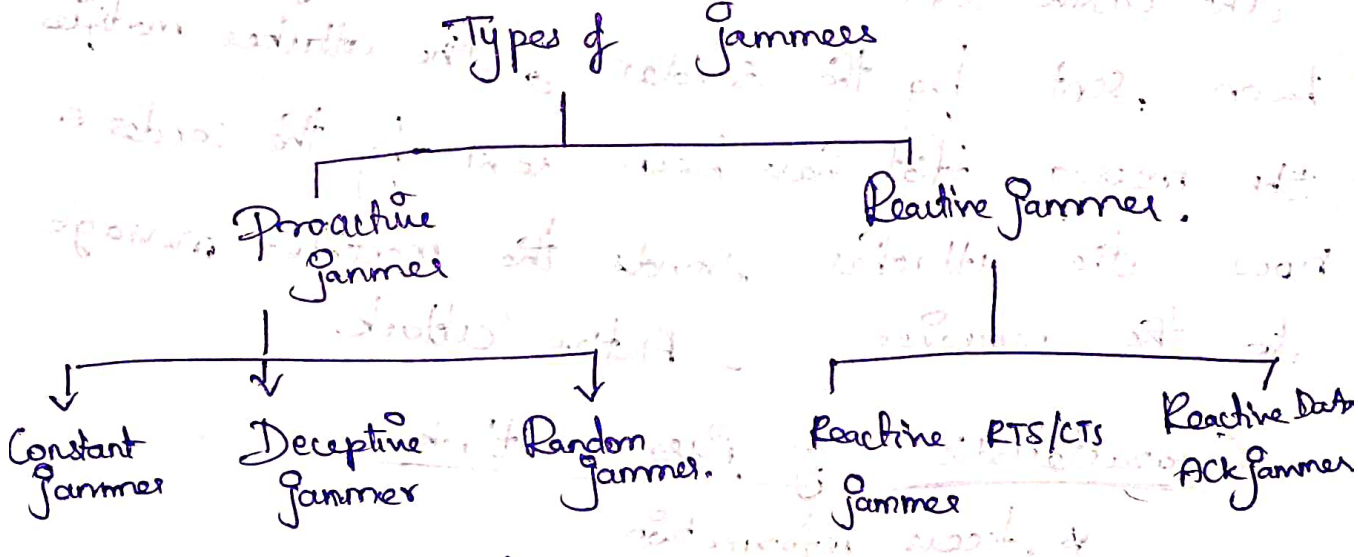
1) Attacks on network availability attacks (DOS) →

it may target any layer of the sensor network.

Denial of service attacks – as an event that diminishes or attempts to reduce a networks capacity to perform its expected function.

Jamming :-

Jamming is one of the Denial of service attacks in which the adversary attempts to disrupt the operation of the network by broadcasting a high energy signal



Jammer are wireless nodes planted by an attacker to cause International Interference in a wireless networ

Constant → Corrupt packet as they are transmitted

Deceptive → sends a constant stream of bytes into the network to make it look like legitimate traffic

Random → Randomly alternates between sleep & jam to save energy

Reactive – transmits a jam signal when it senses traffic

To defense against this attack we spec. spectrum techniques for radio communication

Handling jamming over the madayer requires admission control mechanism

Jamming → disrupt communications – by decreasing signal to noise ratio at recieves sides through the transmission of interfering wireless signal

It keeps the medium busy by. comminicating causing a transmitter to back off whenever it senses busy wireless medium or corrupted signal recieved at reciever

Proactive Jammer:-

It transmits the jamming or interfering signal whether or not there is a data communication in a network.

It sends packets on random bits on channel it is operating on putting all the other nodes on that channel in non-operate modes

It does not switch channels & operates on only one channel until its energy is exhausted

Constant Jammer:-

It emits continuous random bits without following the CSMA protocol

It prevents the communication by causing the medium to be constantly busy

Deceptive Jammer.

Random Jammer:

It transmit random bits or regular packets into network.

It continuously switches between two states — sleep phase & jamming phase

It sleeps for a certain time of period & then becomes active for jamming before returning back to the sleep.

Reactive Jammer.

It starts jamming only when it observes the network activity occurs on certain channel

It can disrupt both small & large sized packet

Reactive RTS/CTS Jammer.

It jams the network when it send is a request to send message is being transmitted from a sender.

It starts jamming the channel as soon as rts is send in this way the receiver will not send back CTS reply becoz at the packet sent from the sender is distorted

Then the sender will not send data becoz it believes the receiver is busy with another ongoing transmission.

Reactive DATA/ACK Jammer.

It jams the network by corrupting the transmission of the data or ack packets or it wait until the packets reach the

receives & then corrupts the ack packet. It, lead to retransmission at the sender end.

Countermeasures for proactive jammer.

In proative jamming, the jammer chokes the bandwidth so that a transmitter is unable to transmit.

Therefore carrier-sensing thresholds can be used to detect such type of jammers.

When jamming is detected, nodes in a network can map the jammed area, re-route traffic, switch channel or perform spatial retreat to counteract this jamming act.

Reactive jammer Countermeasures

Reative jamming detection using Bit error rate that keep the received signal strength low while introducing disruption in a packet.

By looking at the loss of each bit during the reception, it identifies the cause of bit errors of individual packet using error correction code

Tampering Attack or Destruction

An attacker can damage or replace sensor & computational hardware & the program codes or remove sensitive materials.

Given physical access to a node an attacker can extract sensitive information such as cryptographic keys or other data on the node

One defense to this attack involves tampering, tamper proofing node's physical package

Self destructive ~~+~~; whenever somebody access the sensor nodes physically the nodes vaporize their memory contents & this prevents any leakage of information

Countermeasures:

Techniques that prevents attacker from accessing the wireless medium in use include sleeping, hibernating, & spread spectrum communication. These techniques use either analog or digital scheme. By this way attacker cannot easily locate the communication channel

Bidirectional antenna — technique for access restriction

Encrypt

Cryptograph

key

Device Tampering:

Unlike nodes in a wired network, nodes in adhoc wireless networks are usually compact, soft & hand held in nature. They could get damaged or stolen easily.

Data tampering is the act of deliberately modifying (destroying, manipulating or editing) data through unauthorized channels.

Data exist in 2 states: in transit or at rest.

Jamming: It initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender.

It then transmits signals on that frequency so that error free reception at the receiver is hindered. Overcome Frequency hopping spread spectrum → direct sequence spread spectrum.

⊛ Secure Routing Protocol - SPINS

* Unlike the traditional wired Internet, where dedicated routers controlled by the internet service providers (ISP's) exist, in ad-hoc wireless networks, nodes act both as regular terminals (source & destination) and also as regular routers for other nodes.
* In absence of dedicated routers, providing security becomes a challenging task.
* Other factors which make the task of ensuring secure communication in ad hoc network difficult include limited processing power, limited available resource of battery power, bandwidth and memory.

* Requirements of a Secure Routing Protocol:

The fundamental requirement of a secure routing protocol for ad hoc network is:

(i) Detection of a malicious node: A secure routing protocol should be able to detect the presence of malicious nodes in the network and should avoid the participation of such nodes in the routing process.

(ii) Guarantee of correct route discovery: If a route between the source & destination node exists, the routing protocol should be able to find the route and also ensure the correctness of that route.

(iii) Confedentiality of network topology: A malicious node mounts information disclosure attack may lead to discovery of network topology. By this the attacker may try to study the traffic pattern in the network. If some node found to be active compared to others, the attacker may try to mount Dos attack. Therefore confidentiality is a very important requirement.

(iv) Stability against attacks: The routing protocol must be self-stable that is it must be able to revert to its original operating state within a finite amount of time after a active or passive attack.

*The protocol must also ensure Byzantine robustness, that is, the protocol should work properly even if some of the nodes, which were earlier participating in the routing process, turn out to become malicious at a later point of time or intentionally damaged.

(*) Security protocol for sensor networks (SPINS)

*Security protocol for sensor networks (SPINS) consist of a suite protocols that are optimized highly for resource-constrained sensor networks.

* SPINS consists of two main modules:

(i) SNEP (Sensor network encryption protocol)

(ii) TESLA is micro version protocol.

(Timed, Efficient, Streaming, Loss-tolerant, Authentication.)

* SNEP provides :
  (i) Data authentication
  (ii) Protection from replay attacks.
  (iii) Semantic Security.
  ↳ all with low communication overhead of 8 bytes/message

* Semantic Security means that an adversary cannot get any idea about the plain text even by seeing multiple encrypted version of the same plaintext.
* Encryption of the plain texts uses a shared counter, Hence the same message is encrypted differently at different instances in time.
* Message integrity and confidentiality are maintained using a message authentication code (MAC).
* The message also carries the counter value at the instance of transmission like a time stamp, to protect against replay attacks.

* µTESLA ensures an authenticated broadcast, that is, nodes which receive a packet can be assured of it's sender's identity.
* It requires a loose time synchronization between BS and nodes, with an upper bound on maximum synchronization error.
* The MAC keys are derived from a chain of keys, obtained by applying a one-way function F (a function whose inverse is not easily computable)

All nodes have initial key, $K_0 = F(K_1)$, $K_1 = F(K_2)$ &
in general, $K_i = F(K_{i+1})$.

* The key to be used changes periodically, and since all nodes are synchronized to a common time within a bounded error, they can detect which key is to be used to encrypt / decrypt a packet at any instant of time.

* The BS (Base Station) periodically discloses the next verification key to all the nodes and this period is known to all nodes.

* There is also a specific lags of certain intervals between the usage of a key for a ~~key~~ for encryption and its disclosure to all receivers.

* The node which receives the packets buffers it until the appropriate verification key is disclosed.

* The packets are decrypted once the key-disclosure packet is received from the BS.

* If one of the key disclosure packet is missed, the data packets are buffered till the next time interval and then authenticated. ~~For~~ instance, suppose the disclosure packet of K_j doesnot reach a node; it waits till it receives K_{j+1}, then computes $K_j = F(K_{j+1})$ and decrypts the packets received in the previous time interval.

Reliability Requirements in Sensor Networks:

In traditional network like the internet, the transport protocol (TCP, UDP) and the underlying network layer protocols have essentially no clue. what kind of data they transport.

* Key requirement of these protocol is data transparency.
* Sensor networks are data-centric, they know the data they carry.

(*) General data transport tasks for wireless sensor networks can be roughly classified into the following division:

(i) Single packet versus block versus stream delivery:

* In a single packet delivery, a single packet must be reliably transported between two nodes.
* This requirement of reliable transpod is will not occur in dense wireless sensor networks.
* But all sensor network are not dense.
* Secondly data aggregation in wireless sensor networks to condense many redundant or correlated measurement into a small piece of data. Aggregation drastically reduces the size of data.
* In block delivery problem, a data block comprising multiple packets must be delivered to a sensor or a set of sensors. some application example is the

retasking of a sensor network or the injection of user queries.

* In stream delivery problem, a theoretically unbounded number of packets has to be transported between two nodes. An example is the periodic measurement reports.

(ii) Sink to sensors Vs Sensor to Sink Vs Sensor to Sensor

* Information flows either from sensor ~~source~~ nodes to single or few sinks node or in the opposite direction
* A group of sensor ~~of~~ sensors can be geographically specified or by attributes ("all temprature ~~two~~ sensors with less than 50% battery capacity")

Eg: Target tracking requires reliable handover of target state b/w neighbouring nodes close to target.

(iii) Guarenteed versus Stochastic delivery

* In case of guranteed delivery, it expected that all transmitted packets reach the destination, anything else is considered a failure.
* Losing any packet renders the code block useless.
* The concepts of stochastic delivery allow minimum number of losses. For example out of ~~every~~ total packet 'k' atleast 'm' number of packets must reach the destination. Transport protocol that are lightweight (enough to run on) constrained sensor node seem not to have appeared yet.

Unit - V

Sensor Network Platforms and tools.

Sensor Node Hardware - Berkeley Motes, Programming Challenges, Node-level software Platforms - TinyOS, nesC, CONTIKIOS, Node level Simulators - NS2 and its extension to Sensor networks, COOJA, TOSSIM, Programming beyond individual nodes - State centric Programming.

Introduction

When Choosing the hardware components for a wireless sensor node, evidently the application's requirements play a decisive factor with regard mostly to size, costs, and energy consumption of the nodes.

A basic sensor node comprises five main components.

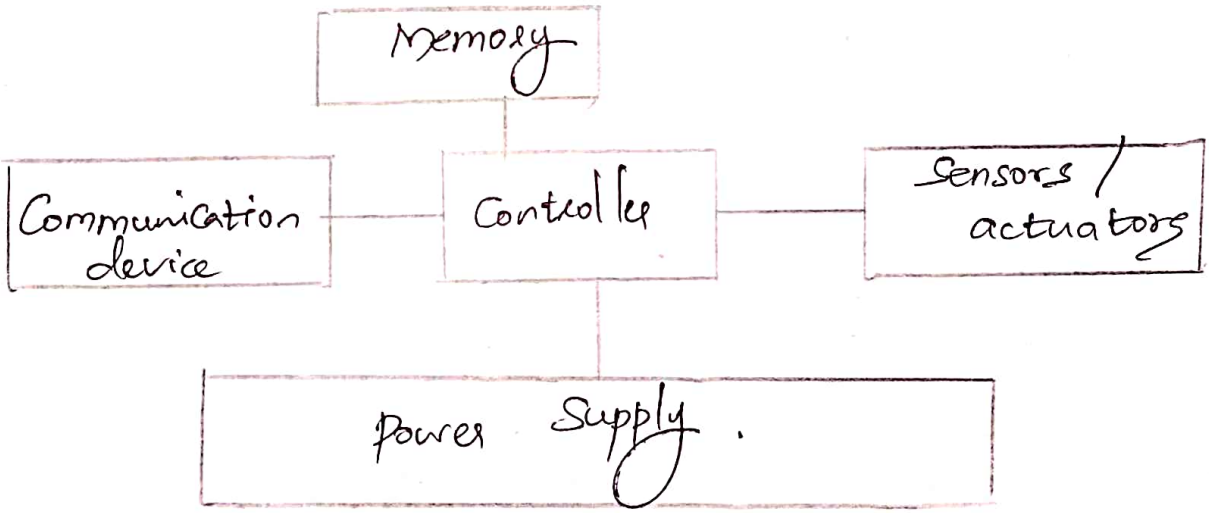


fig: Block diagram of sensor node

controller:

A controller to process all the relevant data capable of executing the Process.

Memory:

Some memory to store Programs and intermediate data; usually, different types of memory are used for Programs and data.

Sensors and actuators:

The actual interface to the physical world: devices that can observe or control Physical Parameters of the environment.

Communication:

Turning nodes into a network requires a device for sending and receiving information over a wireless channel.

Power supply:

As usually no tattered power supply is available, Some form of batteries are necessary to Provide energy. Sometimes, Some form of recharging by obtaining energy from the environment is available as well. The blocks of basic Sensor is given that above figure.

Each of these components has to operate balancing the trade off between as small an energy comsumption as possible on the one hand and the need to fulfill their tasks on the other hand.

Sensor Node Hardware

⇒ Sensor node hardware can be grouped into three categories, each of which entails a different set of trade offs in the design choices.

Augmented general purpose Computers:

Examples include the low power PCs, embedded PCs (e.g., PC104), custom designed PCs and various personal digital assistants (PDA). These nodes typically run off the-shelf operating systems such as Win CE, Linux, or real time operating systems and use standard wireless communication protocols such as Bluetooth or IEEE 802.11. Because of their relatively highes processing capability, they can accommodate a wide variety of sensors, ranging from simple microphones to more shopisticated video cameras. Compared with dedicated sensor

nodes, PC like platforms are more power hungry. However, when power is not an issue, these platforms have the advantage that they can leverage the fully supported networking protocols, popular programming languages, middleware and other off-the-shelf software.

Dedicated embedded sensor nodes:

Examples include the Berkeley mote family, the UCLA Medusa family, Ember nodes and MIT μAmp. These platforms use commercial off-the-shelf (COTS) chip sets with emphasis on small form factor, low power processing and communication, and simple sensor interfaces. Because of their COTS CPU, these platforms typically support at least one programming language, such as C. However, in order to keep the program foot print small to accomodate their small memory size, programmers of these platforms are given full access to hardware but barely any operating system support. A classical example is the TinyOS platform and its companion programming language, nesC.

System-on-chip (SOC) nodes :

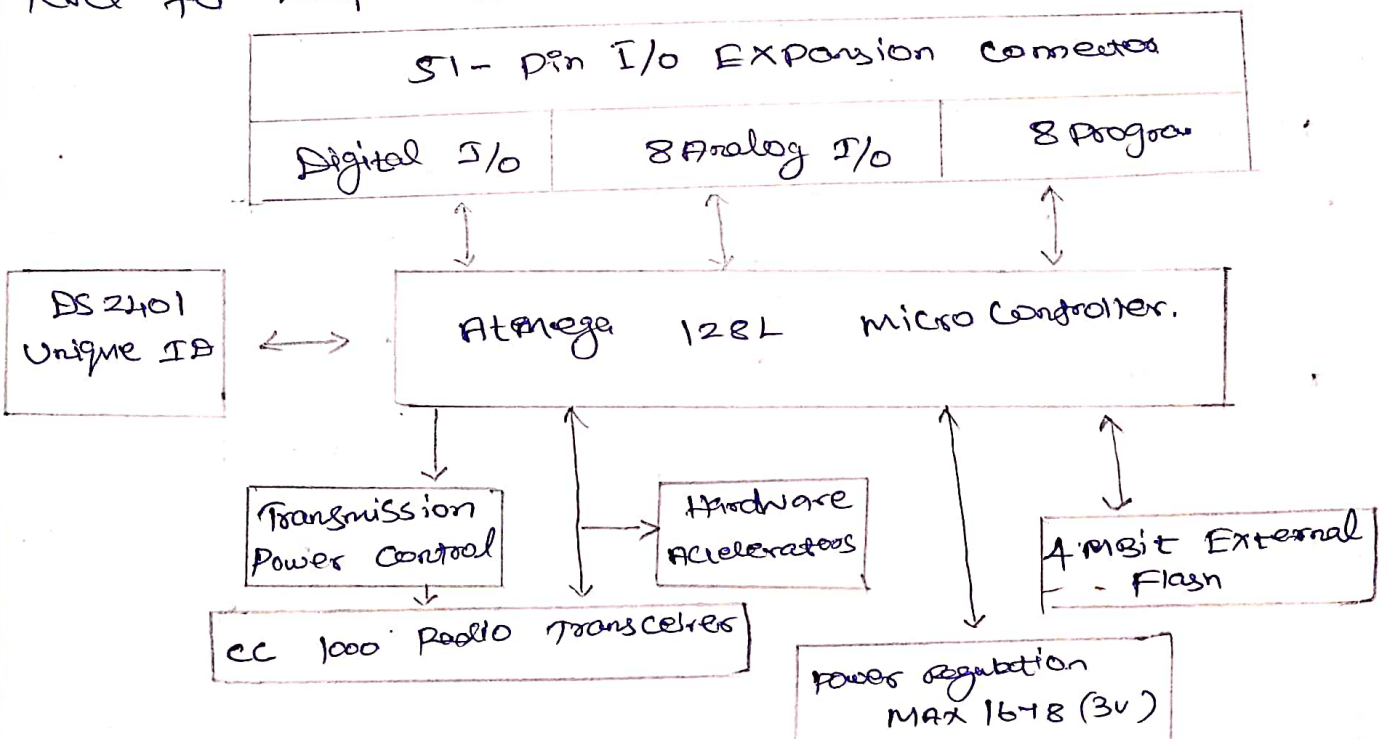
Examples of SOC hardware include Smart dust, the BWRC picoradio node, and the PASTA node. Designers of these platforms try to push the hardware limits by fundamentally rethinking the hardware architecture trade-offs for a sensor node at the chip design level. The goal is to find new ways of integrating CMOS, MEMS, and RF technologies to build extremely low power and small footprint sensor nodes that still provide certain sensing, computation, and communication capabilities. Most of these platforms are currently in the research pipeline with no predefined instruction set, there is no software platform support available.

Berkeley motes:-

The Berkeley motes are the family of embedded sensor nodes sharing roughly the same architecture. It shows a comparision of a subset of mote types.

Example - MICA MOTES:-

The MICA motes have a two-CPU design The main microcontroller an Atenl ATmega 103L, takes care of regular processing. A seperate and much less capable coprocessor is only active when the MCU is being reprogrammed. The ATmega 103L MCU has Integrated 512KB flash memory and 4KB of data memory. Given these small memory size. writing software for motes is challenging. Ideally Programme should be relived from optimizing code at assemb level to keep code foodPrint small.



* In addition to the memory inside the MCU, a MICA mote also has a seperate 512 KB flash memory Unit that can hold data. Since the connection Between the MCU and this external memory is a Low-Speed serial peripheral Interface (SPI) protocol the External memory is more Suited for storing data for later Batch processing than for Storing programs.

* The transmission power can be digitally adjusted By Software through a potentiometer. The maximum transmission range is about 300 feet in open source. Like other types of motes in the family, MICA motes Support a 51 pin I/O extension connector Sensors, actuators, Serial I/O Boards or parallel I/O ports. Can be connected via the Connector. A Sensor Board can host a temperature Sensor, a light Sensor, an accelerator, a magnetometer, a microphone, and a Beeper. The Serial I/O connection allows the mote to Communicate with a PC in real time.

	MICAZ	MICA2	MICA2dot
Flash memory	128k Bytes	128k Bytes	128k Bytes
Measurement memory	512 k Bytes	512 k Bytes	512 k Bytes
EEPROM	4k Bytes	4k Bytes	4k Bytes
A/D (Channels)	10 Bits(8)	10 Bits(8)	10 Bits(8)
Data rate	250k bps	19.2k bps	19.2k bps.
Outdoor range	100m	300m	300m
Size	6x3x1 cm	6x3x1 cm	2.5x0.6m

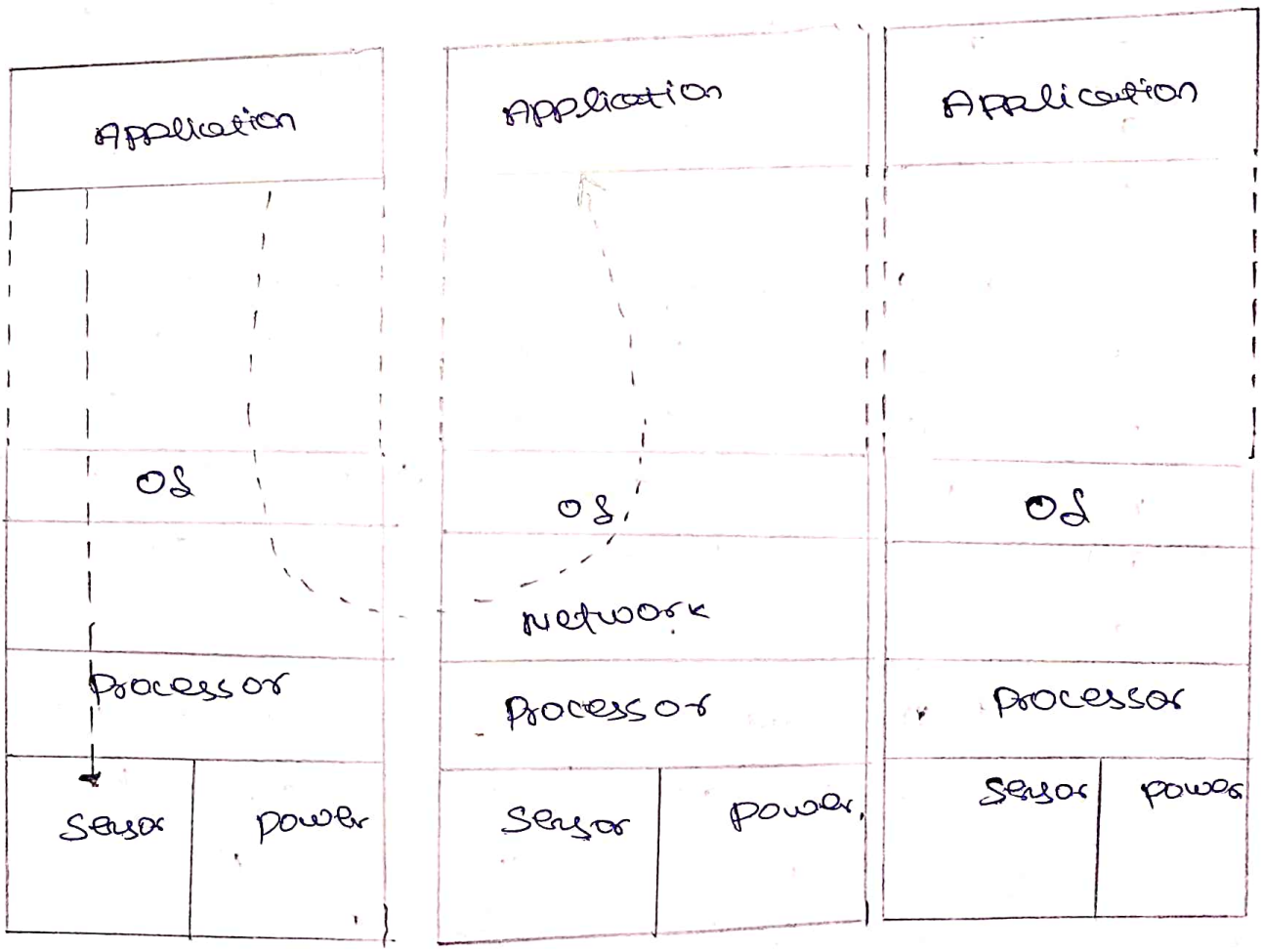
* Traditional programming technologies rely on operating system to provide abstraction for processing, I/O networking, and user interaction hardware. When applying such a model to programming networked embedded systems such as sensor networks, the application programmers need to explicitly deal with message passing, event synchronization, interrupt handling, and server reading.

* For resource-constrained embedded systems with real-time requirements several mechanism are used in embedded operating systems to reduce code size, improve response time and reduce energy conception. microkernel technologies modularize the operating system so that only the necessary parts are deployed with the application. Real time scheduling allocates resources to more urgent tasks so that they can be finished early.

* Sensor networks are large-scale distributed systems, where global properties are derivable from program execution in a massive number of distributed node. Distributed algorithm themselves are hard to implement, especially when infrastructure support is limited due to the adhoc.

* As sensor nodes deeply embed into the physical world, a sensor network should be able to respond to multiple concurrent stimulate the speed of change of the physical phenomina of interest.

* There no single universal design methodology for all application, depending on the specific tasks of a sensor network and the way the sensor nodes are organized, certain methodologies and platforms may be better choices than others. For example if the network is used for monitoring a small set of phenoming and the sensor nodes are organized in a simple star topology then a client-server software model would be sufficient. If the network is used for monitoring a large area from a single access point and if users queries can be decoupled into aggregation of sensor reading from a subset of nodes, then a tree structure that is rooted at the Base Station is a better choice.



* A Node-level platform can be a node centric operating system, which provides hardware and networking abstractions of a sensor node to programmes, or it can be a Language platform, which provides a library of components to programmers. A typical operating system abstract the Hardware Platform By Providing a set of service for application including file mangement memory allocation task scheduling, Peripheral device drivers, and networking. For embedded system due to their highly specified application and limited resources thier operating system have different trade offs when these service.

* TinyOS and tiny GALS are two representative examples of node-level programming tools.

TinyOs:

TinyOs aims at supporting sensor network applications on resource constrained hardware platforms, such as the Berkeley motes. Like many operating systems, TinyOs organizes components into layers. A component specification is independent of the component implementation.

A diagram of the FieldMonitor application, where blocks represent TinyOs components and arrow represent function calls among them. The directions of the arrows are from callers to callees.

The absolute directions of the arrows, up or down, illustrate this components relationship with other layers. A program executed in TinyOs has two contexts, tasks and events, which provide two source of concurrency. Tasks are created by components to a task scheduler. The processing of events also runs to completion, but it preempts tasks and can be preempted by other events.

In TinyOS, resource contention is typically handled through explicit rejection of concurrent requests. Using a component architecture that contains all variables inside the components and disallowing dynamic memory usage statically analyzable.

Imperative Language : nesC

* nesC is an extension of C to support and reflect the design of TinyOS. It provides a set of language constructs and restrictions to implement TinyOS components and applications. A component in nesC has an interface specification and an implementation.

* A component can provide and use the same interface type, so that it can act as a filter interposed between a client and a service. A component may even use or provide the same interface multiple times.

* There are two types of nesC, depending on how they are implemented : modules and configurations. modules are implemented by application code. Configurations are implemented by connecting interface of existing components.

* In nesC, code can be classified into two types.

(i) Asynchronous code (AC) : code that is reachable from at least one interrupt handler.

(ii) Synchronous code (SC). code that is only reachable from tasks.

Contiki OS:

Contiki OS is open source operating system for resource constraint hardware device with low power and less memory. Contiki OS support the resource constraint hardware with following features.

* Lower power
* Limited memory
* Slow CPU
* Size (small)
* Limited hardware parallelisms
* Low bandwidth

Contiki provides serialized access to all resources due to events run to completion and Contiki does not allow interrupt handlers to post new events.

The uIP implementation is written in C and it has the minimum set of features needed for a full TCP/IP stack, uIP can only support one network interface, and it supports TCP, UDP, ICMP and IP protocols.

Node Level Simulator

Node - level design methodologies are usually associated with simulators that simulate the behavior of a sensor network on a per-node basis.

Sensor node model:

A node in a simulator acts as a software execution platforms, a sensor host; as well as communication terminal. In order for designers to focus on the application level code, a node model typically provides or simulates a communication protocol stack, sensor behaviour and operating system services.

Communication node:

Depending on the details of modeling communication may be captured at different layers. The most elaborate simulators model that communication medium at the Physical layer, simulating the RF propagation delay and collision of simultaneous transmissions.

Physical Environmental Model:

A key element of the environment with in a sensor network operates is the physical phenomenon of interest. The moving object in the physical world may be abstracted into a point signal source.

Statistics and visualization:

* The simulation results need to be collected for analysis. Since the goal of a simulation is typically to derive global properties from the execution of individuals nodes, visualizing global behaviours is extremely important.

* A sensor network simulator simulates the behaviour of a subset of the sensor nodes with respect to time. Depending on how the time is advanced in the simulation, there are two types of execution models.

1. Cycle-driven simulation
2. Discrete-event simulation.

* A cycle-driven (CD) simulation discretes the continuous notion of real time into ticks and simulates the system behaviour at these ticks. At each tick, the physical phenomena are first simulated and then all node are checked to see if they have anything to sense, process or communicate.

* Unlike cycle-driven simulator a discrete-event simulator assumes that the time is continuous and an event may occur at any time. An event is 2-tuple with a value and a time stamp indicating when the event is supposed to be handled.

* In terms of timing behavior, a DE simulator is more accurate than CD simulator, and as a consequence, DE simulator run slower. The overhead of order all events and computations, in addition to the values and time stamps of events, usually dominates the computation time.

* DE simulations are sometimes considered as good as actual implementations because of their continuous notion of time and discrete notion of events. There are several open-source or commerical simulators available.

* One class of these simulator comprises extensions of classical network simulators, such as ns-2, J-Sim (Previously known as Javasim), and GLOMOSIM.

* The focus of these simulators is on network modeling, Protocol stacks and simulation Performance. Another class of simulators, sometimes called software in the loop simulators, incorporate in actual node software into the simulation.

NS& and its extension to sensor Networks:-

The stimulator ns-2 is an open source Network stimulator that was orginally designed for Wired IP networks, Extensions have been made to stimulate wireless/mobile Networks (e.g: 802.11 MAC and TDMA MAC) and more recently sensor Networks. While the original ns-2 only supports logical addresses for each node. the wireless channal model for a large Network, this significantly slows down the simulation speed.

There are two widly known efforts to extend ns-2 for stimulating sensor network sensor sim from UCLA and the NRL sensor Network extension from the Navy Research Laboratory.

The main functinality of ns2 is Implemented in C++ while the dyanamics of the Simulations (e.g time dependent application characteristics) is Controlled by Tcl scripts Events are Communication packets that are passed between Consective layers within one node or between the same layers across node

The key advantage of ns.2 is implemented in C++ and its ns2 is rich. libraies of protocols for nearly all network. layers and for many routing machanisms. These Protocols are modeled in fair detail so that they closely resemble the actual protocol implementations

Examples:-

TCP : reno, tahoe and SACK Implementations, Vagas

MAC; 802.3, 802.11, and TDMA

Ad hoc routing: Destination Sequenced distance vector (DSDV) dynamic routing, Source Routing (DSR,) ad hoc On demand distance vector Routing and temporally ordered routing algorithm

Sensor Network Routing: Directed diffusion, geographical routing (GEAR) and Geographical adaptive fidelity (GAF) Routing.

Tossim:-

Tossim is a dedicated stimulator for TinyOs applications running on one or more Berkeley motes. The key design decisions on building Tossim were to make it scalable to a network of potentially thousands of nodes and to be able to use the actual software and stimulations.

Tossim uses a simple but powerful abstraction to model a wireless networks. A network is directed graph, where each vertex is a sensor node and each directed edge has a bit error-rate

Tossim has a visulaization Package called Tinyviz, which is a java application that can connect to Tossim stimulations Tinyviz also provides mechanisms to control a running stimulation by, for example. modifying also provids ADC readings, changing Channal properties and injecting packets. Beside the default visual interfaces users can add applications ~~specific~~ ones easily.

Cooja stimulator is a cross layer Java based wireless sensor Network stimulator distributed with contiki, it allows the stimulation of diffrent Levels from physical to applications layer. and also allows the emulators of diffrent levels of the haedware of a set of sensor nodes, Cooja stimulater is a network stimulator specifically designed for wireless sensor Networks

Cooja is a Network stimulator which Permits the emulation of real hardware platforms. COOJA is the application of Contiki os Concentracting on network behavior. COOJA is Capable of stimulating Wireless sensor Network without any particular mote. Cooja supported followed set of Standards

There are four propagation models in the COOJA which must be selected before starting a new stimulation. The first model a Constant loss unit Disk Graph medium (UDGM) and it take the ideal transmission range disk in which motes inside the transmission disk receive data packets and motes outside the transmission disk do not get any packet.

MRM is also Capable if Computing the diffractions, reflections and refractions along the radio links

Cooja simulation Interface:-

Cooja Network Simulator Interface.

Comprises of five Windows. The Network window displays the physical arrangment of the motes. In order to build a topology.

One Could Change the physical position of the motes. In Network window all the different have different Colors according to their functionaliy. i.e sink mote has a green Color and the sender mote has the yellow Color. mote attributes, radio environment of each mote, mote type and radio traffic between the motes Could also seen vissually in the Network window, Simulations Control. Window helps us to Control the Speed of the Simulations and to pause start and reload the Current running Simulations.

Node window is used to write the theory and key points of the stimulations and save them in the node window. Cooja Network Stimulator shows a timeline for each mote in the running stimulation. We could use timeline for visualizing the both the power Consumption and network traffic in the Wireless sensor Networks. In row three for mote1, color of the mote shows the power state of the transceiver. if the mote is off then it is white, on then it is gray as shown for mote1. White and gray color is either hardware is off or On but the red color line in the second row shows that whenever the node hardware goes on its radio transceiver is also goes on. In first row in timeline of mote1, Radio transmission are shown by blue color: reception by green and radio interference is show by red. the Cooja simulation is very essential to Implement.

PROGRAMMING BEYOND INDUVIDUAL NODES:

* Sensor - actutor network system offer some unique advantages. Dense network of distributed sensors can improve percieved signal to noise ratio by reducing distances from sensor to physical phenomena

* In network proussing and actuation shorten the fied back chain and improve the timelines of observation and response

* A decentralized system is inherently more robust against individual node or line failure because of redundancy. Because of decentralized system spatial coverage and multiplicity in sensing aspect and modality, the detection, classification and tracking of moving, nonlocal or low observable events require cross node collaboration among sensors

* As a vechile moves through a sensor field nearby sensors detect it. An elected leader node aggregates data from the sensor and migrates the information from one node to other node as the vechiles move

* the sensor nodes collaborate primarily to improve sensing accuracy and acceptable estimation quality might be achieved using only a sensors

* one node, the leader, plays a key role in fusing others' sensor measurement If no leader is present all sensors the form the contour are equally important.

- maintain sensor connectivities in a neighbourhood
- discover the best node for handoff
- Invite neighbour nodes into the group
- Handle communication delays and failures

STATIC CENTER PROGRAMMING;

* A distinctive property of physical state, such as location, shape and motion of objects is their continuity in space and time

$$x_{k+1} = f(x_k, u_k)$$
$$y_k = g(x_k, u_k)$$

Where x is the state of the system, u is the system input, y is the output and k is the index update index over space and time

* This formulation is broad through to capture a wire variety of algorithm in sensor fusion, signal processing and control

* However in distributed real time embedded system such as sensor networks, the formulation is not as clean as represented in above equations

* The following issues must be properly addressed during the design to ensure the correctness and efficiency of the system

(i) Where are the state variables stored?

(ii) Where do the inputs come from?

(iii) Where do the outputs go?

(iv) Where are the functions f and g evaluated?

(v) How long does the acquisition of input take?

(vi) Are the inputs in uk collected synchronously?

(vii) Do the inputs arrive in the correct order through communication?

(viii) What is the time duration between indices k and $k+1$? Is it a constant?

* These issues addressing where and when rather than how to perform sensing computation and communication, play a control role in the overall system performance

* However the "non functional" aspects of computation related to concurrency responsiveness, networking and resource management.

* State center programming aims } at providing design methodologies and frameworks that give meaningful abstractions for these issues

* A Collaborative group is such an abstraction

A collaboration group is set of entities that contribute to a state update

* A software agent that hops among the sensor nodes to track a target in virtual node,

While a real node is physical sensor. Limiting the scope of a group to entire space of all agents improves scalability.

* Grouping nodes according to some physical attributes rather than node address is an important and distinguishing characteristic of sensor networks. The structure of a group defines the 'roles' each member plays in the group and thus the flow of data.

(i) All members in the group all equal peers?

(ii) Is there a "leader" member in a group that consumes data

(iii) Do members in the group form a tree with parent and children relations?

* Furthermore having multiple members with the same role provides some degree of redundancy and improves robustness of the application in the node and link failure.