UNIT-I

Adhoc Networks - Introduction and Routing Protocols

Introduction

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, blue tooth zigbee.

Advantage of Wireless Networks

→ mobile users are provided with access to real time information even when they are away from their home or office.

→ Setting up a wireless system is easy and fast and it eliminates the need for pulling out the Cables through walls.

→ It offer more flexibility and adapt easily to change in the Configuration of the network.

Disadvantages

* Interference due to weather, other radio frequency devices, or obstructions like walls.
* The total Throughput is affected when multiple Connections exists.

Problems in Wireless Communication.

→ Some of the problems related to wireless Communication are multipath Probagation, Path loss, interference, and limited frequency Spectrum.

→ Multipath Probagation occurs when a Signal travel from its Source to destination, in between there are obstacles which make the Signal Propagate in paths beyond the direct line of sight due to reflections refraction and diffraction and Scattering.

→ Path loss is the attenuation of the transmitted Signal Strength as it Propagates away from the Sender. Path loss can be determined as the ratio between the powers of the transmitted Signal to the received Signal.

Wireless Adhoc Networks.

→ A mobile adhoc network is a Collection of mobile nodes forming an adhoc network without the assistance of any Centralized Structures.

→ Wireless adhoc Networks are a collection of two or more wireless Communications devices with wireless networking Capability. These wireless devices can Communicate with other nodes immediately within their radio range or one that is outside their radio range. for the latter, the nodes should deploy an intermediate node to be the router to route the Packet from the Source toward the destination

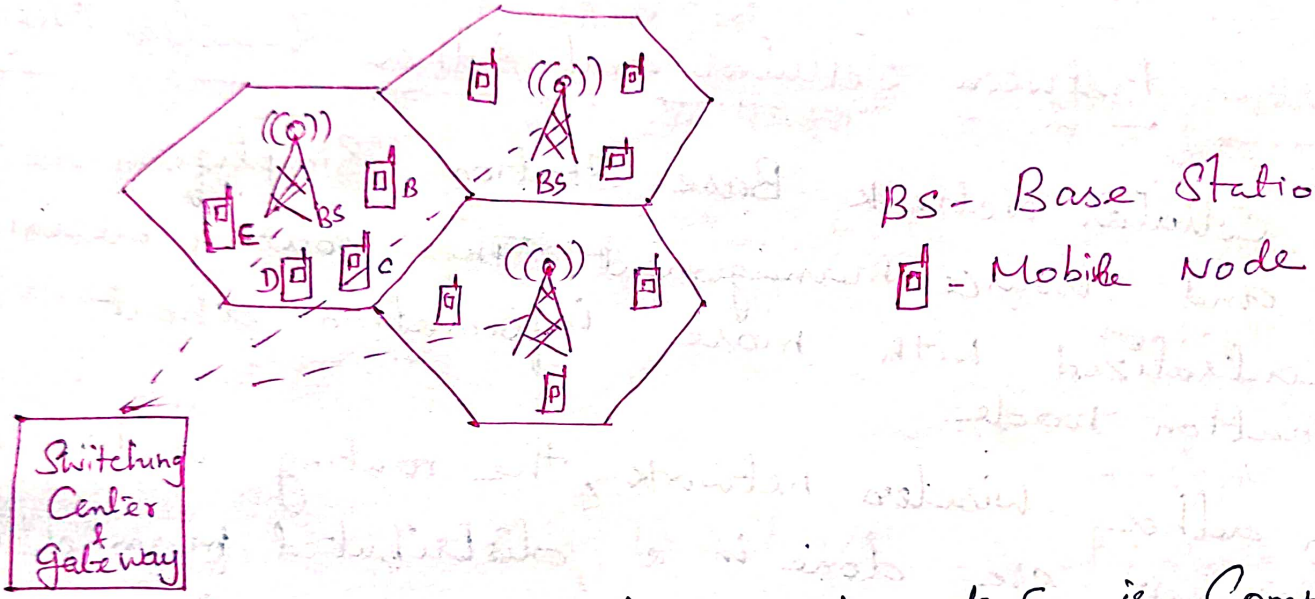
Elements of Adhoc Wireless Network.

Wireless networks are classified into

1. Cellular Networks.
2. Adhoc Wireless networks.

Cellular Wireless Networks

Cellular wireless networks are infrastructure dependent networks. The path setup for a call between two nodes is achieved through base station.



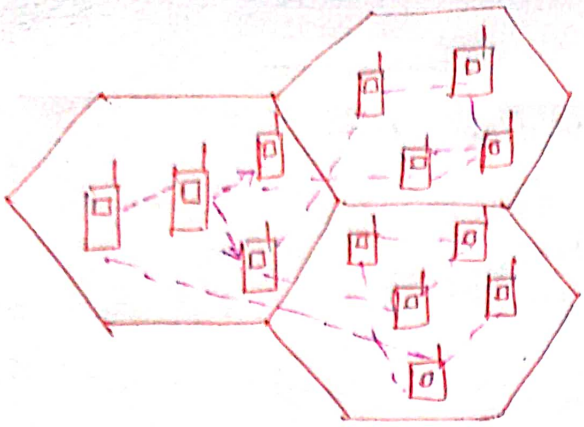
→ Path between node C and node E is completed via base station.

Adhoc Wireless Networks

→ Adhoc wireless networks are capable of operating without the support of any fixed infrastructure. So this is known as infrastructureless network.

→ Multihop radio relaying is used in adhoc wireless networks. Routing is complex due to the absence of central co-ordinator or Base Station

→ fig. shows the topology for adhoc wireless network for communication between node C and node E.



Adhoc Wireless network.

eg: Wireless mesh network, Wireless Sensor Network.

Comparison Between Cellular and Adhoc Wireless Network

→ In Cellular Network, Base Station Simplifies routing and resource management. The routing decisions are Centralized with more information about destination node.

→ In adhoc wireless network, the routing and resource management are done in a distributed manner in which all nodes Co-ordinate to enable Communication among themselves.

→ Each node performs 2 functions.

1. A network host for transmitting and receiving data
2. Network router for routing Packets from other nodes.

Difference between Cellular network and Adhoc Wireless Network

Characteristics	Cellular networks	Adhoc Wireless networks
Infrastructure	fixed infrastructure	Infrastructureless.
Hop	Single Hop	Multi Hop.
Bandwidth	Guaranteed Bandwidth	Shared radio channel
Routing	Centralized	Distributed.
Switching	Circuit Switching	Packet Switching
Connectivity	Seamless Connectivity.	Frequent Path breaks due to mobility.
Cost	High cost	Cost effective deployment.
Timereservation	Easy to achieve	difficult and Consumes Bandw
Bandwidth Reservation	Easy to employ	Require Complex medium access Control protocols.
Network Mainlenance	High cost	Self organized mainlenance.
Mobile host	low Complexity	require more intelligence.

Issues In Adhoc Wireless Networks.

The major issues that affect the design, deployment and Performance of an adhoc wireless Systems are.

1. Medium Access Scheme
2. Routing
3. MultiCasting
4. Transport layer Protocol.
5. Priang Scheme.
6. Qos Provisioning.
7. Self organization.
8. Security
9. Energy management.
10. Addressing and Service discovery.
11. SCalability.
12. Deployment Consideration.

1) Medium Access Scheme.

Medium access Control (MAC) Protocol in adhoc wireless networks is the distributed arbitration for the shared channel for Packet transmission.

1) Distributed Operation
   * NO Possibilty of Central Coordination.
   * Design Should be fully distributed involving minimum Control overhead.

2) Synchronization.
   * Mandatory for TDMA based System for managing transmission and reception slots.
   * Use Scarce resources such as Bandwidth and battery power

Hidden Terminals:

* Nodes that are hidden from Sender but reachable to the receiver of the transmission session is known as hidden terminals.
* Cause collision at the receiver node.
* Reduce throughput.

Exposed Terminals:

Nodes that are in the transmission range of the Sender but prevented to transmit are known as exposed terminals.

Throughput: Throughput should be maximised by

* Minimize collision.
* Maximize Channel utilization.
* Minimise control overhead.

Access Delay: The average delay experienced by a packet to get transmitted is known as access delay. The MAC protocol should minimize the delay.

Fairness: The ability of the MAC protocol to provide an equal or weighted share of the Bandwidth to all competing nodes is known as Fairness.

Real time traffic Support: The MAC protocol should support.

* Time Sensitive traffic such as voice, video, real time data,
* Limited Bandwidth, and location dependent contention in a Contention based channel access Environment.

Resource Reservation

A MAC protocol should support resource reservation Ex. Bandwidth, buffer space and processing power and Qos provisioning ex. Bandwidth, delay, and jitter.

Ability to Measure resource availability

At every node, MAC protocol should provide an estimation of resource availability such as Bandwidth to perform Call admission Control.

Capability for power Control

The transmission power Control is done to.

→ reduce the energy Consumption at the nodes.
→ reduce the Interference at neighbouring nodes.
→ increasing frequency reuse.

Use of Directional Antennas The directional antennas are used for. * increased Spectrum reuse.
* reduction in interference
* reduced power Consumption.

2 Routing: The main responsibilities of a routing Protocol are

* Exchange routing information.
* find feasible path to destination based on hop length, minimum power, lifetime of wireless link.
* gather information about path breaks.
* mend broken path.
* Minimum Bandwidth and Processing power

1) Mobility A good routing protocol should efficiently Solve frequent path breaks, packet Collisions, transient loops, resource reservation.

2) Bandwidth Constraint only a fraction of total Bandwid is available for every node because the channel is Shared by all nodes in the broadcast region.

Location dependent Contention

The Contention for the channel is high if the number of nodes are increased which results in high Collisions and Bandwidth wastage. Therefore the network load is distributed Uniformly across the network.

Other Resource Constraints.

The routing Protocol should also Consider the resource Constraints such as Computing Power, battery power and buffer Storage.

→ The major requirements of a routing Protocol are.

(i) Minimum route acquisition delay.
(ii) Quick Route Reconfiguration
(iii) Loop free Routing.
(iv) Distributed Routing approach.
(v) Minimum Control overhead

Scalability

The ability of the routing protocol to scale well in a network with large number of nodes is known as Scalability.

Multi Casting

Nodes forms groups to Carry out Certain tasks that require point to multipoint and multipoint to multipoint voice and dat Communication, multicasting is used.

→ major issues in designing multicast routing Protocols are

1. Robustness – Quick recovery and reconfiguration from link breaks.
2. Efficiency.
3. Control overhead.
4. Qos Support.
5. Scalability
6. Security.

Transport layer Protocols.

* The main objective of the transport layer Protocol are
  → Setup and maintain end to end connection
  → reliable end to end delivery of data packets.
  → flow control.
  → Congestion control.
* Connectionless transport layer Protocol is not used in adhoc network because.
  → data transfer is not reliable.
  → no flow control and Congestion control.
  → Increased collision.
* Connection-Oriented Protocol is reliable but cannot be used due to
  → frequent Path breaks
  → high channel error rate
  → frequent network partitions.

Pricing Scheme

An adhoc wireless network depends on the Presence of relay nodes and their willingness to relay other nodes traffic. If a neighbour node is not interested in relaying a call and needs to power down, then fully connected network cannot be established.

Qos Provisioning

Quality of Service (Qos) is the performance level of services offered by a service provider or a network to the user. Qos Provisioning requires.
  → negotiation between the host and the network.
  → resource reservation schemes.
  → Priority scheduling.

QoS - aware Routing.

→ QoS aware routing Protocol Use QoS parameters for finding a path during routing

→ The parameters for routing decisions may be network throughput, packet delivery ratio, reliability delay, Packet loss rate, bit error rate and path loss.

QoS framework A framework for QoS is a Complete System which Provide the Promised Services to each User or application.

QoS Service Model

→ The way in which User requirements are Served is known as QoS Service model.

→ The ~~Key~~ Components in design ~~are~~.

Self Organization Self organization refers to organizing and maintaining the network by itself.

The activities in Self Organization are

1. Neighbour discovery.
2. Topology Organization
3. Topology reorganization

Neighbour discovery: Every node in the network gathers information about its neighbours and maintains that information in appropriate data structures.

Topology organization Every node in the network gathers information about the entire network or part of the network

Topology reorganization The change in topology occurs due to mobility of nodes, feilures of nodes or complete depletion of power Sources of the nodes.

Security The security in adhoc wireless communication is very important especially in military applications.

→ These attacks are classified into two types.

(1) Passive attacks.
(2) Active attacks.

Addressing and Service discovery

Addressing An address of a node is globally Unique in the connected part of adhoc wireless network.

Service Discovery Service Discovery is important because nodes in the network should be able to locate the service provided by other nodes.

→ Topological changes force a change in location of the service provider.

Energy Management

Energy management is defined as the process of managing the sources and consumers of energy in a node or in the network to enhance the lifetime of the network.

Energy Management

- Transmission power management
- Battery Energy Management
- Processor power Management
- Device Power Management

Transmission Power Management Power consumption of mobile node is determined by state of operation; Transmit, receive and sleep modes of operation.

Battery Energy Management The battery life of a node is extended by using its chemical properties, discharge patterns, Selection of a battery from set of batteries available for redundancy

Processor power Management The Processor parameters which affect power consumption are the clock speed and the number of instructions executed per unit time

Device power Management Intelligent device management can be done by the Operating System (OS) by
→ selectively powering down interface device that are not used.
→ By putting devices into different power saving modes

Scalability Commercial deployment of adhoc wireless networks may require wide spread installation of adhoc wireless networks for mainstream wireless communication.

Deployment Considerations
→ The deployment in wireless networks require good planning and estimation. of future traffic growth over any link in the network.
→ Reconfiguration of any Partial deployment is difficult due to the cost and time for laying copper or fiber cables.

Example Commercial Applications of Adhoc Networking

Military Applications.
→ Establish Communication among a group of soldiers for tactical operations.
→ Co-ordinate military objects moving at high speed ex. fleets of airplanes or warships.
→ Quick reliable and Secure multimedia multi casting
→ Location Tracking (ex.) GPS may be used for efficient Communication and co-ordination

→ No resource Constraint such as battery life and transmitting power.

Collaborative and Distributive Computing

Collaborative Computing requires temporary Communication infrastructure infrastructure with minimal configuration among group of people.

Ex. 1. lecturer distributing notes to the class on the fly
2. Group of researchers share their research findings in a Conference.

Distributive Computing

→ Requires reliable multicast routing and less Security Compared to military applications.
1. Distribute a file to other nodes in the network.
2. Streaming multimedia among participating nodes.

→ Economical, Portable and battery powered Sources are preferred.

→ Devices such as laptops with add-on wireless interface Cards, enhanced personal digital assistant (PDAs) or mobile devices with high Processing power may be used.

Emergency operations

→ Ad hoc wireless networks are very useful in Emergency operations such as search and rescue, Crowd control, and Cammando operations.

→ The major factors that favor adhoc wireless networks for such tasks are self configuration of the system with minimal overhead, independent of fixed or Centralized infrastructure.

Wireless Mesh Networks

→ Wireless mesh networks are adhoc wireless networks that are formed to provide an alternate communication infrastructure for mobile or fixed nodes/users, without the spectrum reuse constraints.

→ The mesh topology of wireless mesh networks provide many alternate paths for a data transfer session between a source and destination, resulting in quick reconfiguration of the path when the existing path fails due to node failures.

Wireless Sensor Networks.

→ Sensor networks are a special category of adhoc wireless networks that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

→ A sensor network is a collection of a large number of sensor nodes that are deployed in a particular region.

Hybrid Wireless Network

→ One of the major application area of adhoc wireless network is in the hybrid wireless architecture such as multihop cellular networks (MCN) and integrated cellular adhoc relay (ICAR) network.

→ The primary concept behind cellular network is geographical channel reuse.

→ MCN's combine the reliability & support of fixed base station of cellular network with flexibility & multi hop relaying adhoc wireless networks.

Adhoc Wireless Internet

→ Adhoc wireless Internet extends the Service of the internet to the end users over an adhoc wireless networks.

Applications.

1. Wireless mesh networks.
2. Temporary internet Service to major Conference Venues, Sports Venues.
3. Temporary military Settlements.
4. Battlefields.
5. Broadband Internet Services in rural regions.

Issues in ADHOC Wireless Internet

The major issues to be considered for a successful adhoc wireless Internet. are.

1. Gate Way → Gateway nodes are the entry Point to the wired Internet.
   → Generally they are owned and operated by a Service Provider.
   → They performs the following tasks.
   * Keeping track of End Users.
   * Bandwidth Management
   * Load balancing
   * Traffic Shaping
   * Packet filtering.
   * Bandwidth fairness.

2. Address Mobility
   → This problem is worse here as the nodes operate over multiple wireless hops.
   → Solution such as Mobile IP Can Provide temporary alternative.

3. Routing Routing is a major problem due to
   * dynamic topological changes.
   * Presence of gate ways.
   * Multi hop relaying.
   * hybrid character of the network.

→ To overcome this a separate routing Protocol is used for the wireless part of the adhoc wireless internet.

4. Transport layer Protocol

Specialized transport layer protocol for adhoc wireless network part can be used.

* The intermediate node at which the connections are split act as gateways.
* The state maintenance overhead at the gateway nodes are considered.

5. Load Balancing: Load balancing distribute the load so as to avoid the bottleneck of gate way nodes.

6. Pricing / billing: Since internet bandwidth is expensive it becomes very important to introduce Pricing / billing Strategies for the adhoc wireless internet.

7. Provisioning of Security: The Security mechanisms should be included in the adhoc wireless internet.

1. To avoid snooping on important information by potential hackers.
2. To Provide Security for e-Commerce transaction.

8. QoS Support: QoS Support is very important in adhoc wireless internet to various applications Such as Voice over IP and Multimedia.

9. Service, Address, location Discovery:

Service discovery refers to the activity of discovering or identifying the party which provides a particular Service or resource.

Address discovery refers to the services such as those provided by address Resolution Protocol (ARP). or Domain Name Service (DNS) operating within the wireless domain.

Location discovery refers to detecting the location of a particular mobile node in the network. or detecting the geographical location of nodes.

Issues in Designing a Routing Protocol for Adhoc Wireless Networks

The various design challenges in adhoc wireless networks are

1. Mobility of nodes
2. Resource Constraints.
3. Error Prone channel
4. Hidden and exposed terminal Problem.

1. Mobility of Nodes

→ The movement of nodes leads to change in network topology and the communicating path breaks in the current session.

→ In wired networks all nodes are stationary. If any path break occurs, the protocols find the alternate routes and the convergence is very slow.

2 Resource Constraint:

In wired networks, Bandwidth is abundant whereas in wireless networks, the radio band is limited. So the data rate in wireless network is lesser than that in wired networks.

→ The routing protocols are designed such that the bandwidth is used optimally to minimize the overhead involved in maintaining topological information at all the nodes.

3. Error Prone Channel.

→ The wireless links have time varying characteristics in terms of link capacity and link-error probability.

→. The adhoc wireless network routing protocol should interact with the MAC layer to find the alternate routes via better quality links.

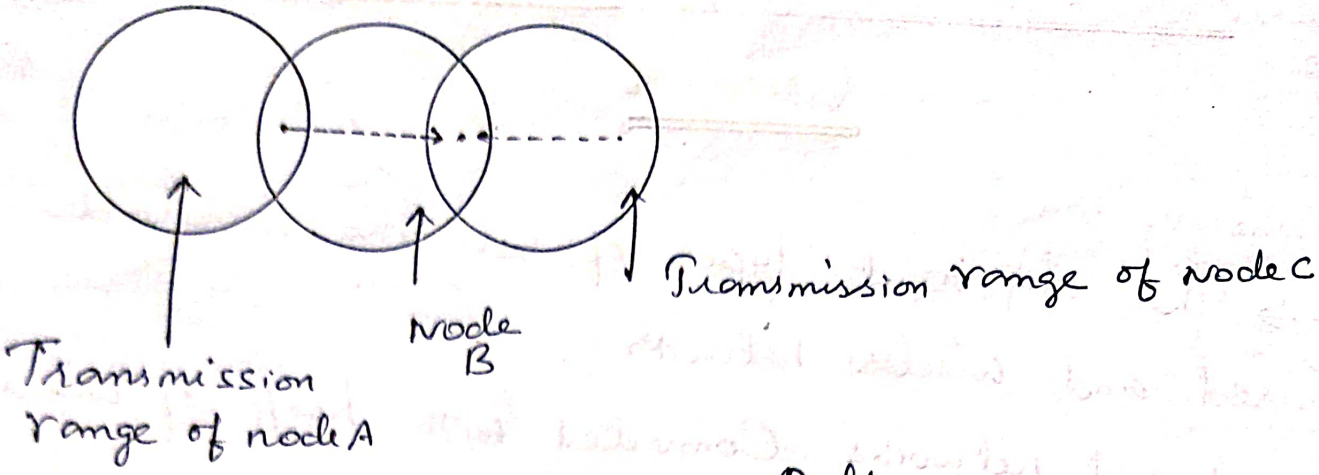
4. Hidden and Exposed Terminal Problem.

Hidden Terminal Problem: Collision of packets occurs at receiver due to simultaneous transmission by nodes outside the transmission range of sender but within the range of receiver

→ When both nodes transmit packets at the same time without knowing the transmission of each other collision occurs. This is known as hidden Terminal problem.

→ Consider fig. if node A and node C want to transmit to node B at the same time then packet collide at node B because both nodes A and C are hidden from each other (ie) A and C don't know the presence of each other.

→ To avoid this, Medium Acces collision Avoidance (MACA), MACA for wireless (MACAW), Floor Acquisition Multiple Access (FAMA) Protocols are used.



Hidden Terminal Problem.

Exposed Terminal problem. The node cannot Transmit information to other node due to blocking by nearby transmitting node. This is referred to as exposed Terminal problem.

Characteristics of ideal Routing Protocol.

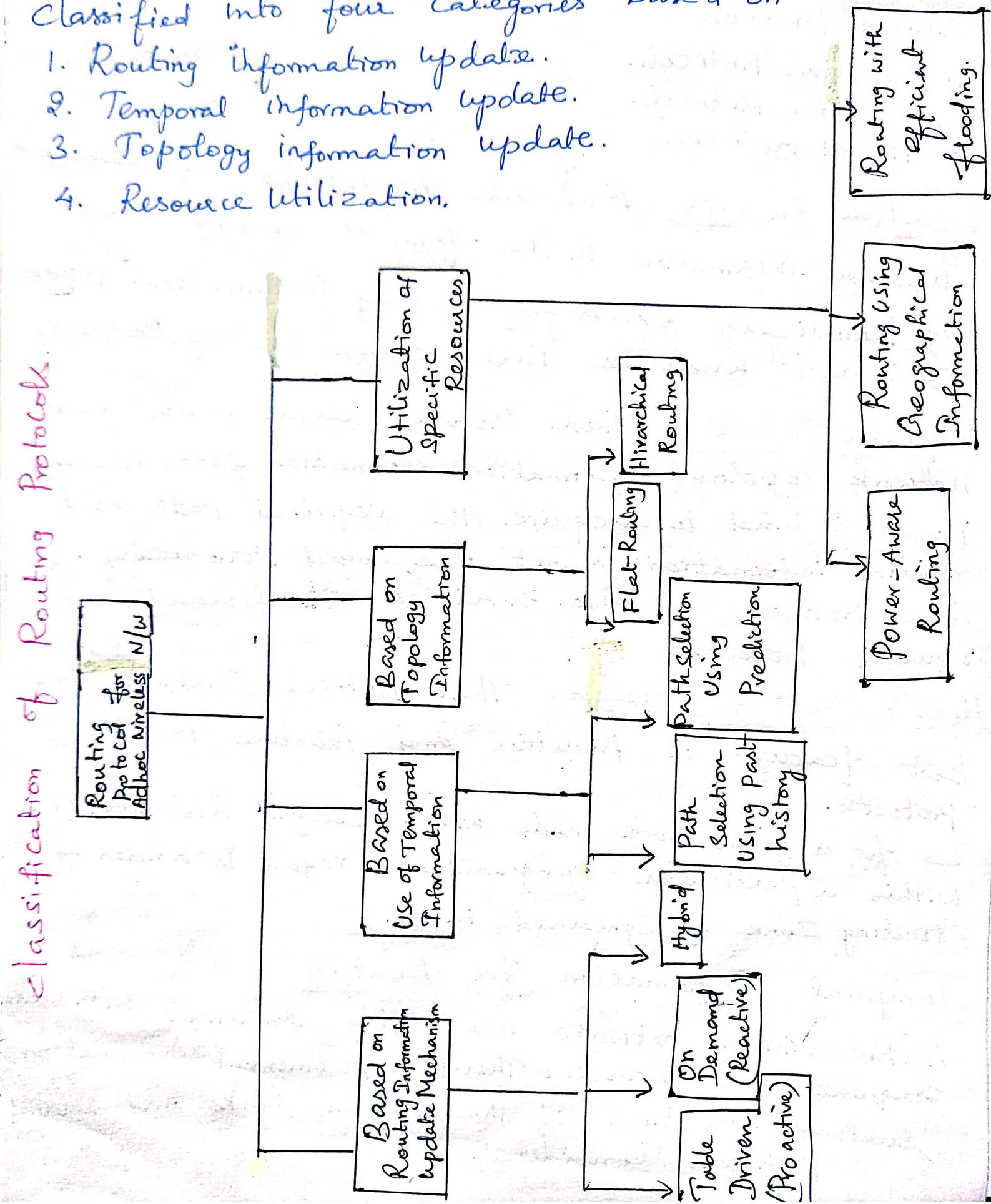
An ideal routing Protocol for adhoc wireless network should have the following characteristics.

1. Fully distributive.
2. Adaptive to frequent topology changes.
3. Minimum Connection Setup time is desired.
4. Must be loop free from Stale routes.
5. Minimum number of packet collisions to reduce message loss and to prevent Stale routes.
6. Coverage to optimal route quickly.
7. Quality of Service (QoS) Should be Provided.

Classification of Routing Protocols.

Routing Protocols for adhoc wireless networks can be classified into four categories based on

1. Routing information update.
2. Temporal information update.
3. Topology information update.
4. Resource utilization.



Routing Information update Mechanism.

Based on routing information update mechanism routing Protocols can be classified into three types.

1. Proactive Protocols.
2. Reactive Protocols.
3. Hybrid Protocols.

Proactive Protocols: Each node maintains the network topology information in the form of routing tables by Periodically exchanging routing information. Hence it is also known as Table driven routing Protocol.

Reactive Protocols: These Protocols donot maintain the network topology information. Connection establishment Process is used to acquire the required Path and routing information is not exchanged Periodically. These Protocols are also known as On demand routing. Protocols.

Hybrid Routing Protocols: These Protocols Combines the best features of Proactive and reactive routing protocols.

→ for a given node, nodes within Certain distance or within a particular geographical region is known as routing zone of Concerned node.

Temporal Information for Routing

Adhoc Wireless networks are highly dynamic with more frequent path breaks. Therefore, temporal information such as life time of the wireless links and selected path are Considered.

→ It is classified into 2 types.
1. Routing Protocols using past temporal information
2. Routing Protocols using future temporal "

Routing Protocols using Past temporal Information.

→ These Protocols use information about past status of the links or status of links at the time of routing to make routing decisions.

2. Routing Protocols using future Temporal Information.

The information about the expected future status of the wireless link is used to make routing decisions.
→ future status information may includes lifetime of the nodes (Based on battery charge and discharge rate), location Prediction.

Based on the Routing Topology.

→ Ad hoc networks do not have central infrastructure which introduces the lack of fixed topologies. So that routing Protocols should be designed in a very flexible fashion to work in a dynamically changing topology.

1. Flat Topology 2. Hierarchical Topology.

Flat Topology Routing Protocol.

→ Flat addressing scheme is used.
→ A globally unique addressing mechanism for nodes is assumed in adhoc wireless network

Hierarchical Routing Protocol.

→ A logical hierarchy and an associated addressing scheme is used in these Protocols.
→ The hierarchy is based on geographical information

Based on Utilization of Specific Resources.

It is classified into 2 types based on resource utilization.

1. Power aware routing
2. Geographical Information assisted routing.

1. **Power aware routing.** The Consumption of battery Power is minimized in these protocols. The routing decisions are based on minimizing power Consumption either locally or globally in the network.

2. **Geographical Information Assisted Routing**

The available geographical information is utilized effectively to improve the routing performance and reduce control overhead.

Routing Protocols based on routing inform update

- Proactive (Table driven)
  1. Destination Sequenced Distance Vector Routing Protocol (DSDV)
  2. Wireless Routing Protocol (WRP)
  3. Cluster Head Gateway Switch Routing Protocol (CGSR)
  4. Source-free Adaptive Routing Protocol (STAR)
- Reactive (On-demand)
  1. Dynamic Source Routing Protocol (DSR)
  2. Adhoc on-demand distance Vector Routing Protocol (AODV)
  3. Temporally ordered Routing Algorithm (TORA).
  4. Location Aided Routing (LAR)
  5. ABR
  6. SSA
  7. FORP (Flow oriented Routing Protocol)
- Hybrid
  1. CEDAR
  2. ZRP (Zone Routing Protocol)
  3. ZHLS.

Table-Driven Routing Protocols (or) Proactive protocols

→ These Protocols are also called as Proactive Protocols. they maintain the routing information even before it is needed.

→ Each node maintains the network topology information in form of routing tables. & routing information is exchanged periodically.

→ Some examples of Proactive Protocols are given below

1. Destination Sequenced Distance-Vector Routing Protocol (DSDV)
2. Wireless Routing Protocol (WRP).
3. Source Tree Adaptive Routing Protocol (STAR).
4. cluster head Gateway Switch Routing Protocol (CGSR).

Destination Sequenced Distance Vector Routing Protocol (DSDV)

→. The DSDV is one of the first Protocols Proposed for adhoc Wireless networks. It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and first node on the shortest path to every other node in the network.

→ It incorporates table updates with increasing sequence number tags to prevent loops, to counter the Count to infinity Problem,

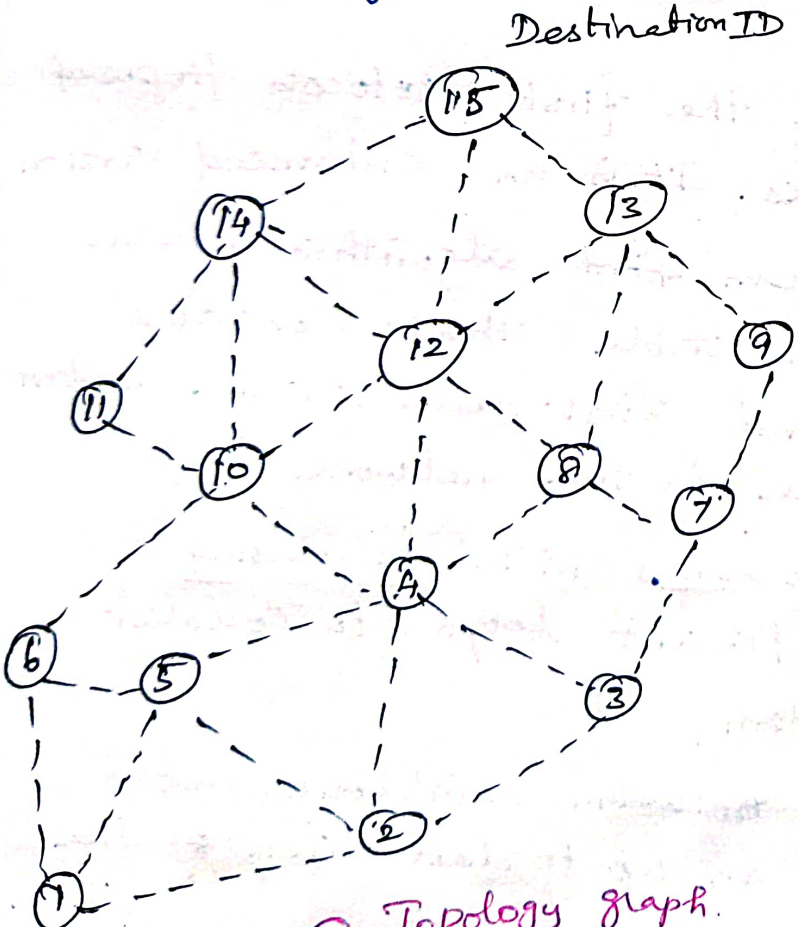
→ The tables are exchanged between neighbours at regular intervals to keep an up to date view of the network topology.

→ Table updates are two types:

① Increamental updates: Takes a single network data packet Unit (NDPU). These are used when a node does not observe significant changes in the local topology.

② Full dumps: Takes multiple NDPU's. It is done either when the local topology changes significantly or when an increamental update requires more than a single NDPU.

→ Consider the example as shown in figure (a) here node 1 is the Souce node and node 15 is the destination. As all the nodes maintain Global Technology information, the route is already available as shown in fig (b).



(a) Topology graph.

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

(b) Routing Table for Node 1.

Advantage
1. Routes are established on demand
2. Minimum Connection Setup delay.

Disadvantage
1. Intermediate nodes may lead to in Consistent routes if these nodes donot have latest destination Sequence number.
2. Heavy Control overhead due to multiple Route Reply packets.
3. Unnecessary bandwidth Consumption due to periodic beaconing.

ON-Demand Routing Protocols.

→ Unlike the table driven routing Protocols, on demand routing Protocols execute the path-finding Process and exchange routing information only when a Path is required by a node to Communicate with a destination.

→ Various On demand routing Protocols are.

① Dynamic Source Routing Protocol (DSR).
② Adhoc On demand Distance Vector Routing Protocol (AODV).
③ Temporally ordered Routing Algorithm. (TORA).
④ Location Aided Routing (LAR).
⑤ flow-oriented Routing Protocol (FORP).

Adhoc ON Demand Distance Vector Routing Protocol.

→ Adhoc on demand distance Vector (AODV) routing Protocol Uses an on-demand approach for finding routes, that is route is established only when it is required by a Source node for transmitting data packets. it employs destination sequence numbers to identify the most recent path.

→ In AODV, the Source node and the intermediate nodes Store the next hop information Corresponding to each flow for data packet transmission. The Source node floods the Route Request packet in the network when a route is not available for the desired destination. it may obtain multiple routes to different destinations from a single Route Request.

→ The major difference between AODV and other On demand routing Protocols is that it uses a destination sequence number (DestSeqNum). to determine an up to date path to the destination.

→ A node updates its path information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum at the node.

→ A Route Request Carries.
  * The Source identifier (SrcID)
  * The destination identifier (DestID)
  * The Source Sequence number (SrcSeqNum)
  * The destination Sequence number (DestSeqNum).
  * The broadcast identifier (BCastID)
  * The Time to live (TTL) field.

→ DestSeqNum - indicates the freshness of the route that is accepted by the Source.

→ when an intermediate node receives a Route Request it either forwards it or Send a Route Reply if it has Valid route to the destination.

→ The Sequence number of the intermediate node is Compared with the destination Sequence number in the Route Request packet and the Validity of a route is identified.

→ BCastID - SrcID Pair indicates the node receiving multiple Route Request, and discards the duplicate Copies.

→ All intermediate nodes having valid routes to the destination or the destination node itself, are allowed to Send Route Reply packets to the Source.

UNIT-II

Sensor Networks - Introduction & Architectures.

Introduction.

→ Wireless Sensor Network is a wireless network. that contains distributed independent sensor devices that are meant to monitor physical or environmental conditions.

→ A WSN consists of a set of connected tiny sensor nodes, which communicate with each other and exchange information and data. These nodes obtain information on the environment such as temperature pressure, humidity or pollutant and send this information to a base station.

→ The latter sends the information to a wired network or activates an alarm or an action, depending on the type and magnitude of data monitored.

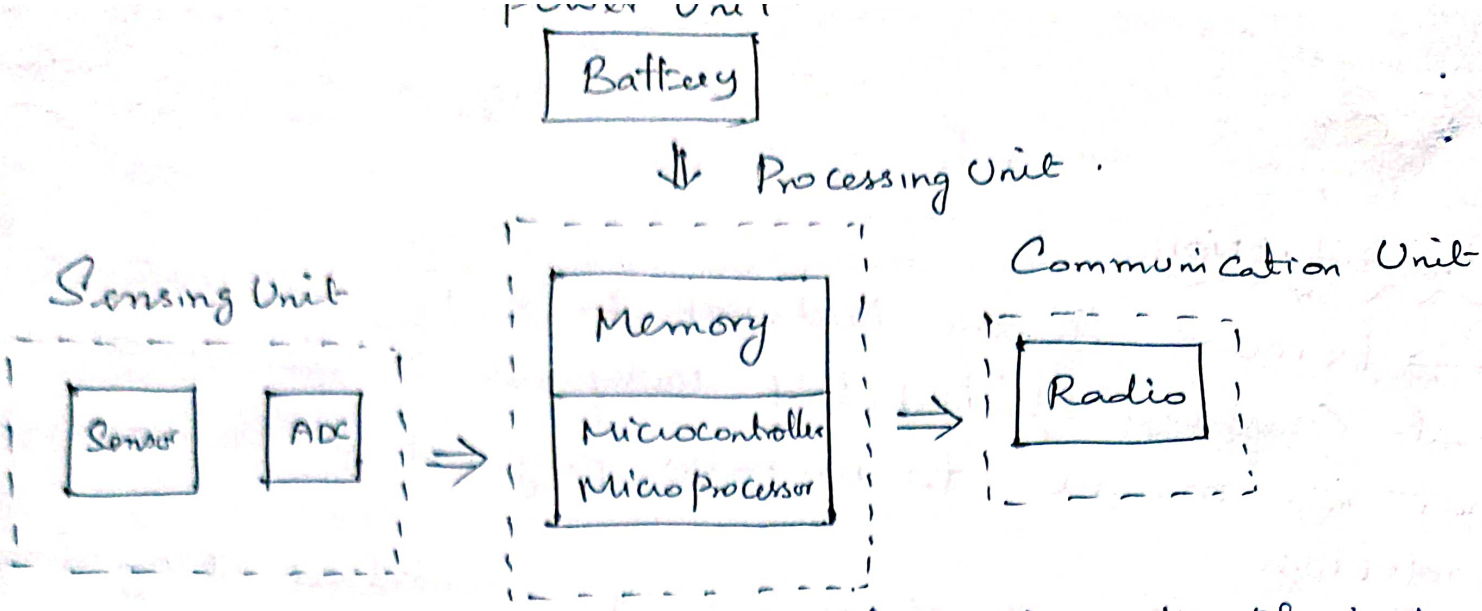
Elements of WSN.

→ A typical wireless sensor network can be divided into two elements. They are

① Sensor Node. ② Network Architecture.

Sensor Node: A sensor node in a WSN consists of four basic components. They are

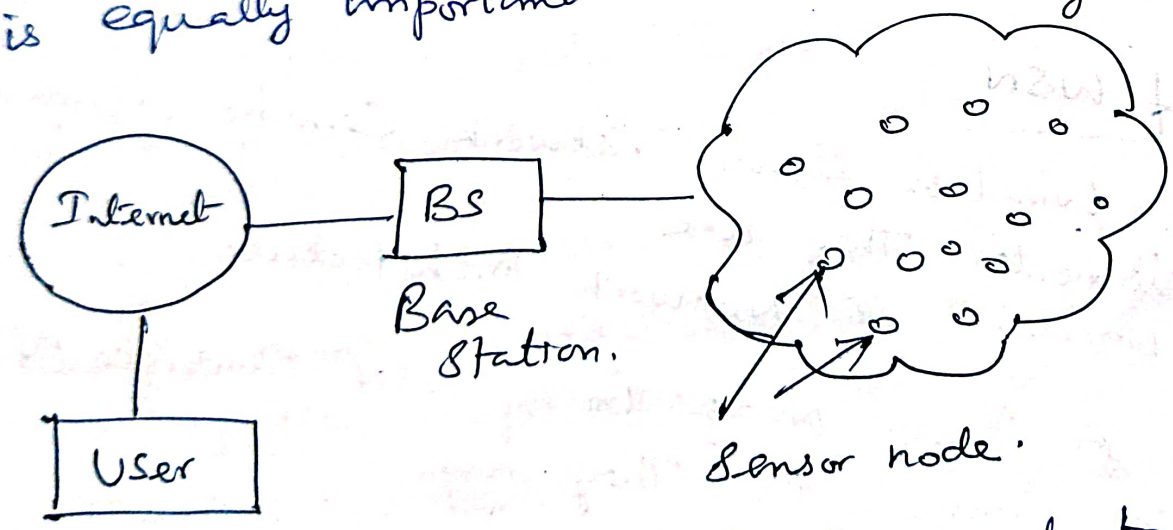
① Power Supply
② Sensor
③ Processing Unit.
④ Communication System.



→ Sensor collects the analog data from the Physical world and an ADC Converts this data to digital data. The main Processing Unit, which is usually a micro processor or a micro Controller, Performs an intelligent data Processing and manipulation.

Network architecture.

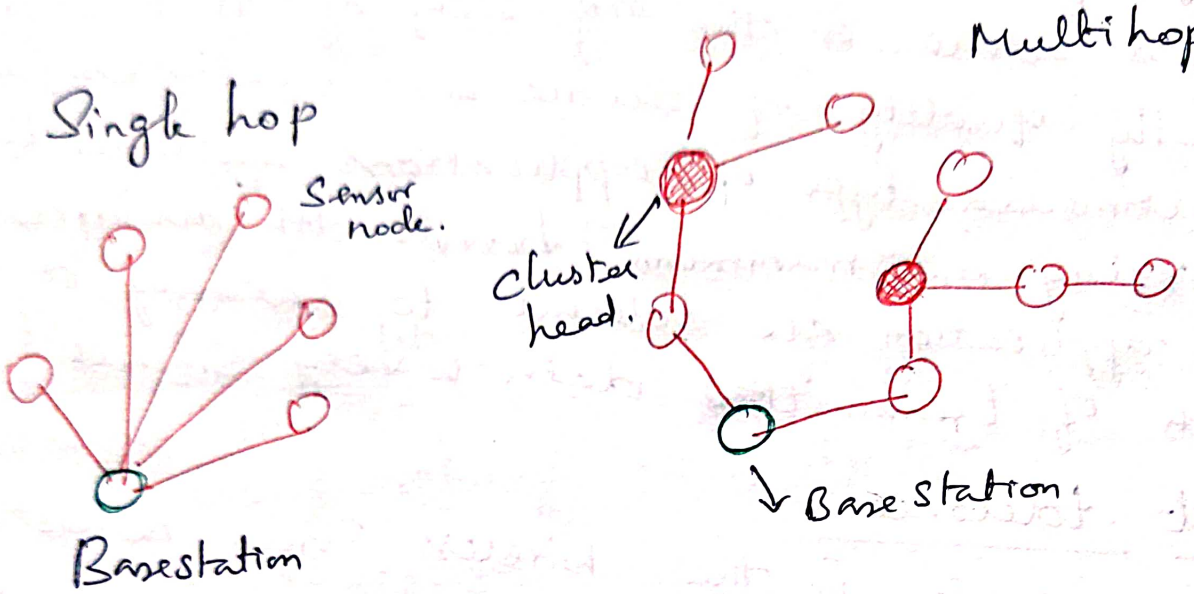
→ When a large number of Sensor nodes are deployed in large area to Co-operatively monitor a physical environment, the networking of these Sensornodes is equally important.



→ The base Station Sends Commands to the Sensor nodes and Sensor node Perform the task by Collaborating with Each other. After Collecting the necessary data, the Sensor nodes Send the data back to the base Station.

→ If each Sensor node is Connected to the base Station it is Known as Single hop network. (2)

→ Multihop network architecture is Usually Used. here the data is transmitted through one or more Intermediate node.



challenges for Wireless Sensor Networks.

The design challenges in Sensor networks are listed as follows.

(i) Characteristic requirement.

(ii) Required mechanism.

Characteristic Requirement

The following characteristics are shared among most of the applications. They are.

(i) Type of Service. The Service type is rendered by a Conventional Communication network is evident

(ii) it moves bits from one place to another.

→ In Wireless Sensor network, moving bits is only a means to the end node, but not the actual node. Hence this the first challenge to the Wireless Sensor network to provide meaningful information to the respective node.

(ii) Quality of Service closely related to the type of a network's Service is the quality of that Service. Traditionally quality of Service is usually coming from multimedia type of applications such as like a bounded relay or minimum bandwidth are irrelevant when the application are tolerant to latency or bandwidth of transmitted data is very small

(iii) Fault tolerance

Since nodes in the Wireless Sensor network may run out of energy or might be damaged or since the wireless communication between two nodes can be permanently interrupted. So it is important that the wireless sensor is able to tolerate such faults

(iv) Life time

→ In many scenarios, nodes will have to rely on a limited supply of energy. Replacing these energy sources in the field is usually not practicable and simultaneously a wireless Sensor network must operate at least for a given mission time. hence life time of a Sensor network becomes a very important.

v) Scalability Since a wireless Sensor network might include a large number of nodes, the employed architecture and protocols must be able to scale to these numbers.

Wide range of densities.

According to the number of nodes per unit area, the density of the network can vary considerably for different applications will have very different node densities.

(vii) Programmability. Programming the wireless sensor network is also a challenge. It is not only necessary for nodes to process information but also they will have to react flexibility on changes in their tasks.

(viii) Maintainability

According to the environment, the wireless sensor networks itself change the system has to adapt.

Required Mechanisms:

→ To realize these requirements, innovative mechanism for a communication network have to be found, as well as new architectures and protocol concepts.

(i) Multihop wireless Communication.

→ wireless communication is a direct communication between a sender and receiver is faced with limitations. In particular communication over long distances is only possible using prohibition of high transmission power.

→ The use of intermediate nodes as relays can reduce the total required power.

(ii) Energy efficient operation

Energy efficient operation is a key technique to support long lifetimes. It also includes in the process of data transport between two nodes or more importantly.

(iii) Auto Configuration.

→ A wireless Sensor network will have to Configure most of its operational parameters autonomously independent of external Configuration and number of nodes.

→ Also the network should be able to tolerate failing nodes because of depleted battery and to integrate new nodes because of incremental deployment after failure.

(iv) Collaboration and in network Processing

→ In many applications 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 network in various forms to achieve collaboration instead of every node transmit data to external network.

(v) Data Centric

→ In Traditional Communication networks, data transfer between two devices is equipped with one network address, hence they are address Centric.

→ In a 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 Para Paradigm in designing architecture and Communication Protocols is promising.

Locality:

→ Locality will ensure scalability.
→ nodes which are very limited in resources, limit their status (Processing only information of neighbours).
→ This will allow the network to scale large no. of nodes without relying on single node.

Exploit trade off

→ WSN rely to large inherent trade off
→ higher energy allows higher accuracy or longer life of node.
→ Another tradeoff node density depending on application deployment and node failures at run time the density of network change considerably.
→ The Protocol will have to handle very different situations at different places of a single n/w.

Enabling Technologies for Wireless Sensor Networks.

→ Building such a wireless sensor networks has only become possible with some fundamental advanced in enabling technologies,
→ Some of the enabling Technologies are.
(1) Hardware miniaturization.
(2) Processing and Communication
(3) Sensing equipment
(4) Software architecture.

1. Hardware Miniaturization.

→ Smaller feature size in chips reduces the power consumption of the basic components of a Sensor node

→ Construction of WSNs can be the microcontrollers memory chips and radio modems which are responsible for wireless communication have become much more energy efficient.

→ Reduced chip size and improved energy efficiency leads to reduced cost and deployment of nodes.

② Processing and Communication

→ It is difficult to generalize sensors because they come in various forms and huge range depending upon their functionality. But it is the fact that their nature and design has made the sensor networks possible.

③ Sensing equipment.

→. Sensing equipment is the third relevant Technology

→. However it is difficult to generalize because of the vast range of possible sensors.

→ The Sensor node should be accompanied by power supply.

→ Depending on application high capacity batteries with negligible self discharge rate and small amount of current can be used.

→ Ideally, a Sensor node has a device for Energy Scavenging. ie) the battery is recharged with Energy gathered from the environment such as Solar cells or Vibration-based power generation.

→ Battery should be efficiently chargeable with small amount of current.

⇒ Energy Scavenging is used to remove Unwanted Component from the energy Consumption.

4. Software Architecture.

→ The division of tasks and functions in a single node the architecture of the operating system or run time Environment.

→ This environment should support simple retasking, Cross layer information exchange and modularity.

→ The Software architecture on a single node is extended to a network architecture where the division of tasks is important between nodes. Then appropriate Communication Protocol is selected

1. Division of tasks in a single node
2. Node architecture extended to network architecture
3. Select Communication Protocol

WSN Applications Examples.

→ Sensor nodes are used in various applications which require constant monitoring and detection of specific events.

① **Area monitoring** → It is a common application of WSN In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored.

→ A military example is the use of sensors detects Enemy intrusion, a civilian example is the geo-fencing of gas or oil pipelines.

② **Disaster relief application.**

→ It is one of most important application of Wireless Sensor networks. It is a typical scenario is wild fire detection.

→ Sensor nodes are equipped with thermometers and can determine their own location.

③ **Environmental Applications.**

→ To monitor weather conditions.
→ Detection of forest fire.
→ Flood detection
→ Habitat exploration of animals.
→ Monitor environmental changes in plants, oceans and other disaster areas.

④ **Intelligent buildings.**

Building waste vast amount of energy by inefficient humidity, Ventilation, air conditioning usage

A better real time high resolution monitoring (b) of temperature, airflow humidity and other physical parameters in a building by means of wireless Sensor networks.

Medical applications

→ Monitor medical devices.
→ Patient diagnosis.
→ Monitoring patient ~~Patient~~ physiological data such as heart rate or blood Pressure.
→ Data collected from patient can be sent to automated monitoring systems.
→ Prevent wrong diagnonsis.

Machine Surveillance

→ In Industries the wireless Sensor network is used to surveillance the machine by fix sensor nodes is difficult to reach areas of machinery where they can detect vibration pattern that indicate the need for maintenance.

Examples: → Robotics or the Axles of Trains.

Precision Agriculture.

→ Bring out fertilizer / Pesticides / irregation only when and where needed.
→ Pest Control can Profit from a high resolution Surveillance of farm land.

Military Applications

→ Battlefield Surveillance and monitoring.
→ Remote Sensing.
→ Monitoring the movements of enemies.
→ Guidance Systems of Intelligent missiles.
→ Gather more information about movement of Enemy vehicle and explosions.
→ Biological and Chemical attack detection investigation.

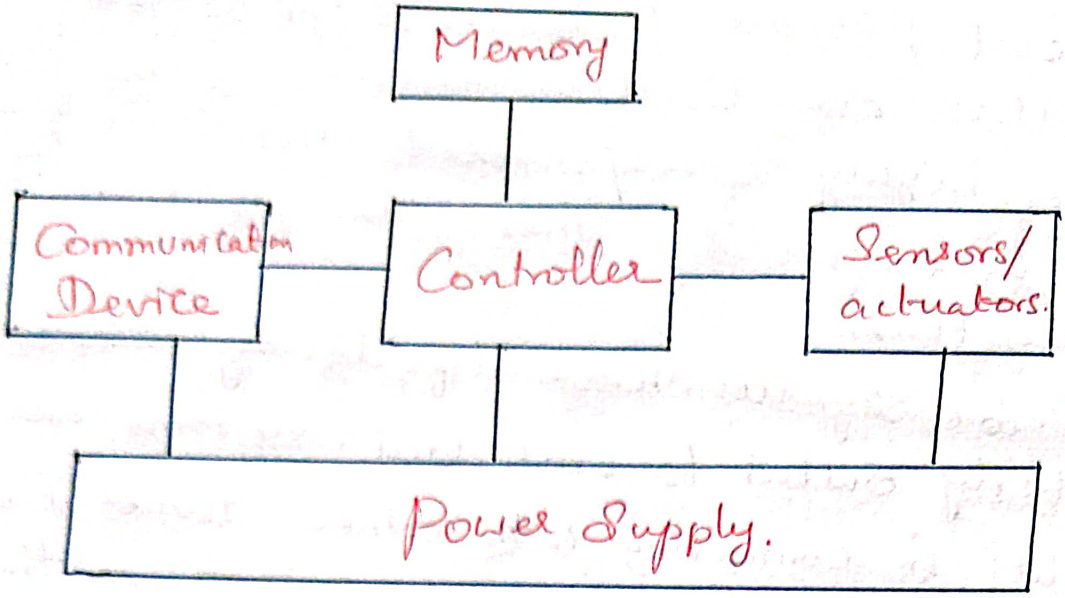
Single Node Architecture.

→ Wireless Sensor node having two kinds of architecture.
1. Single node architecture
2. Multiple node architecture

→ Single node architecture means only one Sensor will be placed on the architecture Multiple node architecture Contains more than one Sensor on architecture

→ A basic Sensor node Comprises five main Components.

① Controller module
② Memory module
③ Sensing modules.
④ Communication module.
⑤ Power Supply module.



Overview of main Sensor node hardware Components.

Controller.

→ A Controller to Process all the relevant data, Capable of executing arbitrary node.

→ A Controller is the Core of a Wireless Sensor node It collects data from the Sensors, Processes this data, decides when and where to send it; receive data from other Sensor node,

→ It has to execute various Programs, ranging from time Critical Signal Processing and Communication Protocols to application Programs.

→ It is the Central Processing Unit of the node.

→ Main options:

① MicroController ② DSP (Digital Signal Processing)

③ FPGA (Field Programmable Gate Arrays).

④ ASIC. (Application Specific Integrated Circuit)

→ For General Purpose Processors applications. micro Controllers are used.

→ These are highly overpowered and their energy Consumption is excessive. These are used in Embedded systems.

→ Some of the key characteristics of micro Controllers are particularly suited to embedded systems are their flexibility in Connecting with other devices like Sensors and they are also Convenient in that they often have memory built in.

→ Examples of micro controllers

① Texas Instruments MSP 430 → 16 bit RISC Core.

② Atmel ATMega. → 8 bit Controller larger memory than MSP430.

A Specialized Case of Programmable Processors are

→ Digital Signal Processors.

→ In a wireless sensor node, such a DSP could be used to Process data Comming from a simple analog wireless Communi Cation devices to extract a digital data stream.

→ In broad band wireless Communi Catin DSPs are appropriate and successfully used platform.

→ An FPGA Com be reprogrammed (or rather reconfigured) "in the field" to adapt to a changing set of requirements. however this Com take time and energy.

→ An ASIC is a Specialized Processor, Custom designed for a given application such as, for example, high Speed routers and Switches. (8)

→ Micro controller requires Software development, ASICs provide the same functionality in hardware resulting in Potentially more costly hardware development.

Memory → Some memory to store Programs and intermediate data, Usually different types of memory are used for Programs and data.

→ The memory module of a Sensor node has two major tasks.

* To store intermediate Sensor readings, Packets from other nodes and so on.

* To store Program Code.

→ While RAM is fast, its main disadvantage is that it loses its Content if Power Supply is interrupted

→ Program Code can be stored in Read only Memory (ROM) or more typically in Electrically Erasable Programmable Read only Memory (EEPROM) or flash memory.

→ Flash memory Can also Serve as intermediate Storage of data in case RAM is insufficient or When the power supply of RAM Should be shut down for Some time.

Communication

→ The Communication Unit has both a Transmitter and receiver for establishing Wireless Communication between Sensor nodes.

→ The Communication module of a Sensor node is Called "Radio Transceiver".

→ The essentially tasks of transceiver is to "Transmit" and "Receive" data between a pair of nodes

→ Transceiver should have following characteristics for Sensor node.

* Capabilities.
* Energy characteristics.
* Radio Performance.

→ Transmit, Receive, Idle and Sleep are the operational states of transceiver.

→ (i) Transmit mode → Transmitting data
(ii) Receive mode → Receiving data
(iii) Idle mode → Ready to receive but not doing so. Some function in hardware can be switched off
(iv) Sleep mode → * Significant parts of the transceiver are switched off.
* Not able to immediately receive something

→ Some of the standard radio transceiver used in various Sensor nodes. include.

(i) RFM TR1000 family from RF Monolithics.
(ii) chipcon (TI) CC1000
(iii) chipcon (TI) CC2400
(iv) TDA 525x family from Infineon.

→ IEEE 802.15.4

→ LMX3162 from National Semiconductor

→ Transceiver structure has two parts as Radio frequency RF front end and baseband part.

* RF Front end → Performs analog Signal Processing in the actual radio frequency Band.

* RF Base Band → Performs all Signal Processing in the digital domain

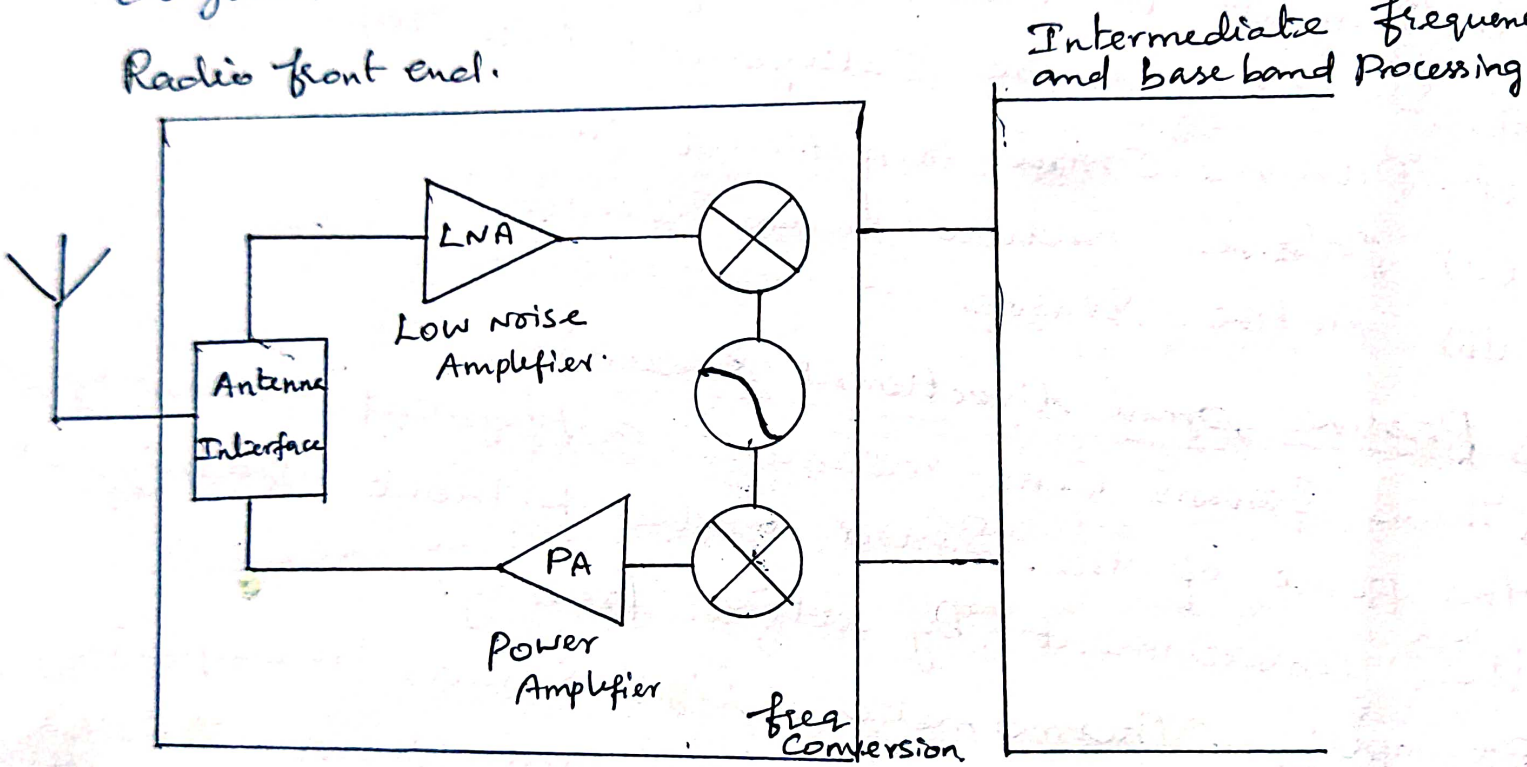


fig. RF front end.

→ The Power Amplifier (PA) accepts un-Converted signals from the IF or Base band Part and amplifies them for transmission over the antenna.

→ The Low Noise Amplifier (LNA) amplifies incomming signals up to levels. Suitable for further Processing without significantly reducing the SNR

Sensors and actuators.

→ Sensors and actuators are more Important Component in a WSN.

→ Sensornode: The actual interface to the physical world that can observe or control physical parameters of the environment

→ Sensors converts physical quantities into a electrical signal which can be used by a human or by an instrument to take necessary decisions.

→ Sensors can be categorized into Three types.

(i) Passive omni directional Sensors.

(ii) Passive narrow beam Sensors.

(iii) Active Sensors.

(i) **Passive, omni directional Sensors:**

→ These Sensors can measure a physical quantity at the point of the Sensor node without manipulating the environment by active Probing.

Examples Thermometer, light Sensor, microphones, humidity Sensor, vibration Sensor, Smoke detector

(ii) **Passive narrow beam Sensors.**

→ These Sensors are passive and Precise in direction while the Sensor nodes Sense the environment.

→ An example for such Sensor is camera which can "take measurement" in a given direction, but we can rotate based on our needs.

(iii) **Active Sensors**

→ It actively probe the environment

→ The sonar, radar or some types of Seismic Sensors are example of active Sensors.

Actuators An actuators is a device to Convert an electrical Control signal to a physical action.

Power Supply module.

* It Provides as much energy as Possible.
* No tethered Power Supply is available, Some form of batteries are necessary to Provide energy.
* Some form of recharging by obtaining energy from the Environment is available as well (eg. Solar Cells).
* There are essentially two aspects: Storing energy and Energy Scavenging.

Storing energy * options of Power Supply module
* Primary batteries. → not rechargeable.
* Secondary batteries → rechargeable, In WSN, recharging may or may not be an option

Energy Scavenging
→ Depending on application, high Capacity batteries that last for long times, that is have only a negligible self discharge rate, and that Can efficiently Provide Small amounts of Current.

Storing Energy Batteries.

Traditional Batteries.

The power Source of a Sensor node is a battery.
Battery Can have two types.
(1) non rechargeable (or) Primary batteries.
(2) Rechargeable (or) Secondary batteries.

Energy Consumption of Sensor Nodes.

→ The energy Consumption of a Sensor node should be Controlled because
* Batteries have Small Capacity.
* Recharge by energy Scavenging is Complicated and volatile.

→ The main Consumers of energy are the Controller, Radio front end and Memory.

→ To reduce Power Consumption of these Components Comes from chip level and lower technologies.

→ Designing low power chips is the best starting Point for an energy efficient Sensor node.

→ Also multiple States of operation Consume more energy. for this introducing the multiple States of operation with reduced energy efficient wireless Sensor nodes, it also reduced in functionality.

→ Advanced Configuration and Power interface (ACPI) introduces one state representing fully operational machine and four sleep states of graded functionality / Power Consumption / wakeup time. This is used for all Components of a Sensor node.

→ These modes Can be introduced to the Controller radio front end, memory and Sensors.

→ According to different for Controller, the typical states are active idle and sleep and for radio front end modem has transmitter, receiver or both on or off and Sensor and memory was on or off.

→ finally the sleep state called deeper, it is used to speak off if less power is consumed.

→ In fig at time t power consumption is reduced by putting into sleep mode from P_{active} to P_{sleep}. If it remains active, the next event occurs at time t_{even} then a total energy is

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

Time T_{down} is the time to put the Component into sleep mode.

→ The average Power Consumption during this phase is $\left(\frac{P_{active} + P_{sleep}}{2}\right)$

P_{sleep} – Power Consumed until t_{event}.

→ The energy required in sleep mode is

$T_{down}(P_{active} + P_{sleep})/2 + (t_{event} - t_1 - T_{down}) P_{sleep}$.

The energy in active mode is $(t_{event} - t_1) P_{active}$

The energy Saving is

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

The additional overhead due to event is

$$E_{overhead} = T_{up}(P_{active} + P_{sleep})/2$$

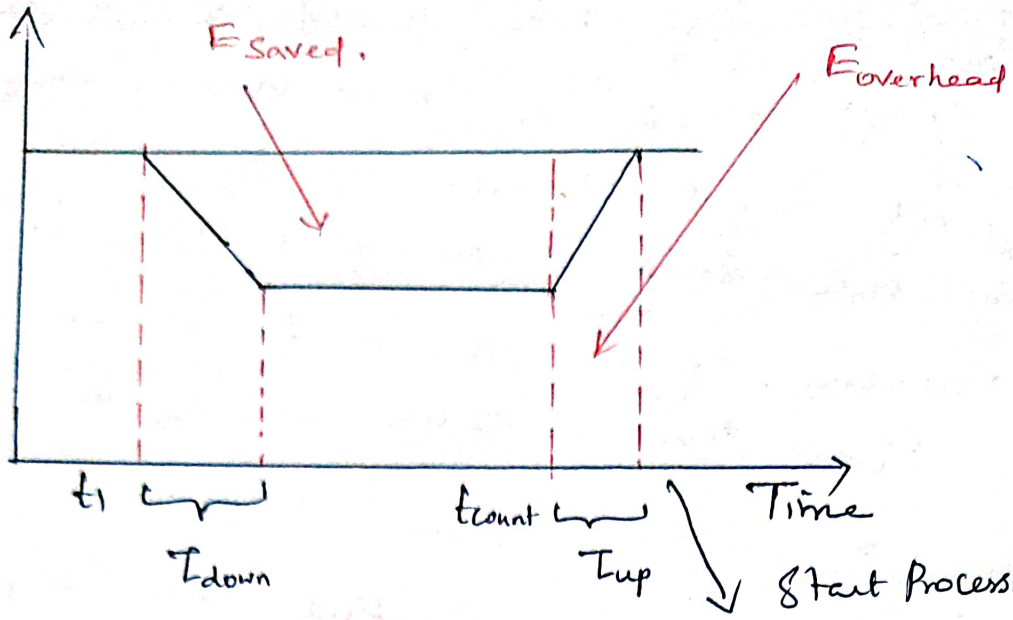


fig: Energy Saving for Sleep modes.

Micro controller Energy Consumption.

→ Embedded Controllers are fairly ease to control the power Consumption even though it commonly implement the multiple operational states.

→ Some Embedded Processors are listed below

Intel Strong ARM.

* Provide Three sleep states.

(i) In normal mode → all parts of the Processor fully powered.

(ii) In idle mode → clk to cpu are stopped, Clk that pertain to peripherals are active.

(iii) In Sleep mode → Only real time clock is active.

Texas Instrument

(i) Wide range of operating modes.

(ii) There are 4 sleep modes in total

ATMEL - ATMega.

→ It has Six different modes of power Consumption.

Memory Energy Consumption.

→ The memory device Consumes the more energy It also has a three sleep states, they are writing, reading and erase.

→ To reduce the energy, the designers use only the onchip memory of a micro controller and flash memory

Radio Transceivers Energy Consumptions.

→ It has two tasks, transmitting and Receiving data

→ It Operates in different modes.

→ For low total energy Consumption, the transceiver 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

(i) 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,

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

Where.

T_{start}, P_{start} are time and Power at starting Point

R → normal bit rate, R_{code} - Coding rate.

$P_{tx\,elec}$ → Power due to other circuitry

Modelling Energy Consumption during reception

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

→ Energy Consumption depends on number of hardware and system parameter.

→ The energy or power required to receive a packet is (E_{revd}) given by.

$$E_{revd} = T_{start} P_{start} + \frac{n}{R R_{code}} (P_{rx\,Elec} + \eta E_{dec\,Bit})$$

$P_{rx\,Elec}$ → receiver other circuitry energy.

$E_{dec\,Bit}$ → decoding energy.

Network Architecture

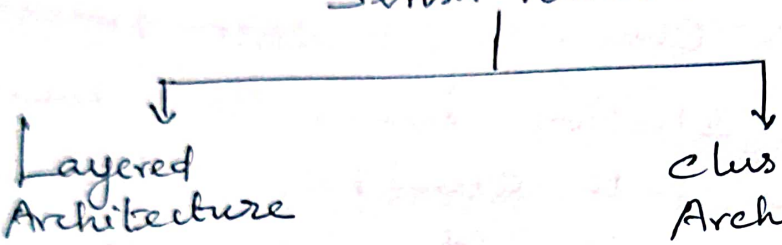
Sensor Network Architecture.

→ A Sensor node can gather information from other Sensor node.

→ The factors to be considered while designing the Sensor network are.

1. Scalability 2. Fault tolerance. 3. Power Consumption

→ Sensor networks are classified as.



Layered Architecture

→ It Consists of Single, Powerful base station and the layers of Sensor nodes around it

→ It uses military Sensor based infrastructure such as Multi Hop Infrastructure Network Architecture (MINA)

In Building Back bones.

→ The BS acts as an access point to wired network and Small nodes form a wireless backbone to Provide wireless Connectivity.

Military Application

→ B.S act as data gathering and Processing Entity with a Communication link to a larger network

→ The main functions of Protocols used for implementing layered architecture are.

1. Network initialization and maintenance
2. MAC Protocol
3. Routing Protocol.

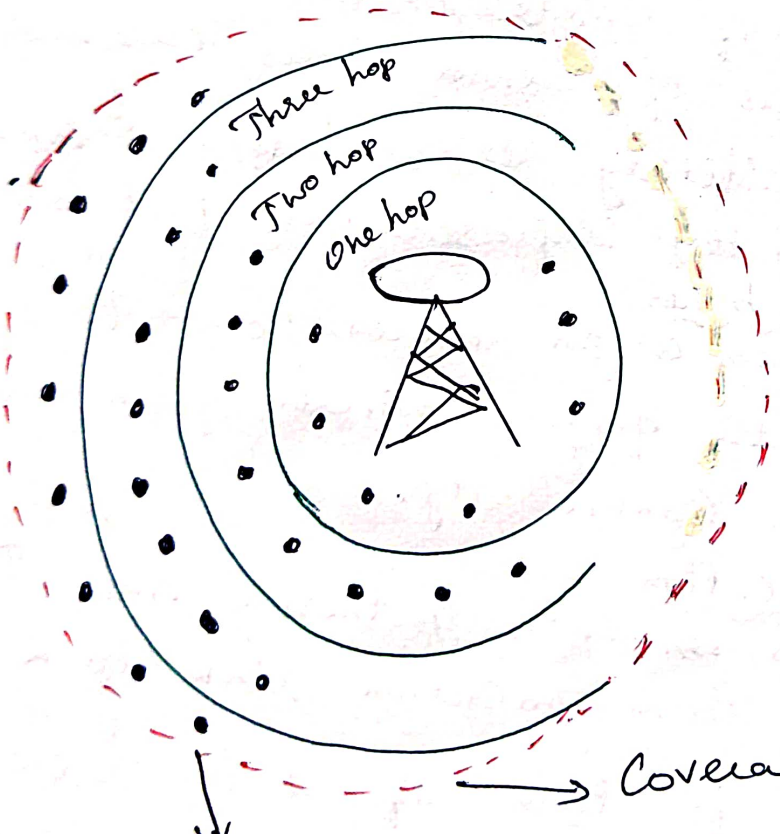
1. Network Initialization and Maintenance Protocol

→ Sensor nodes are organized into different layers using broadcast capability of base station.

→ The Base station broadcasts its identifier (ID) on the common control channel using a known CDMA code.

→ All nodes record the ID of base station on hearing this broadcast and they send a beacon signal with their own ID at low power levels.

→ When the base station hears the message from nodes, these nodes with one hop distance form a layer. The base station then broadcast a control packet with all layer one node ID's.



Layered Architecture.

→ The layer one nodes inform the BS about layer two nodes and then it is broadcasted to the Entire network in the next round of beacons.

MAC Protocol

→ Network initialization is done on a Common Control channel. The distributed TDMA receiver Oriented channel assignment MAC Protocol (DTROC) is used for data transmission.

→ Base station assigns a reception channel to each node and channels are reused to avoid collisions

→ The node schedules transmission slots for all its neighbours and broadcasts the schedule so that collision free transmission is possible.

→ The main function of DTROC
1. Channel allocation.
2. channel Scheduling.

Routing Protocol

→ Data transfer from the Sensor nodes are transmitted to base station by multihop data forwarding.

→ UNPF-R is the modified form of UNPF Protocol. The Sensor nodes can adapt to their transmission range to optimize the n/w performance.

→ If the transmission range is small, it leads to new partitioning, while the large transmission range reduces the frequency reuse.

Advantage of Layered architecture.

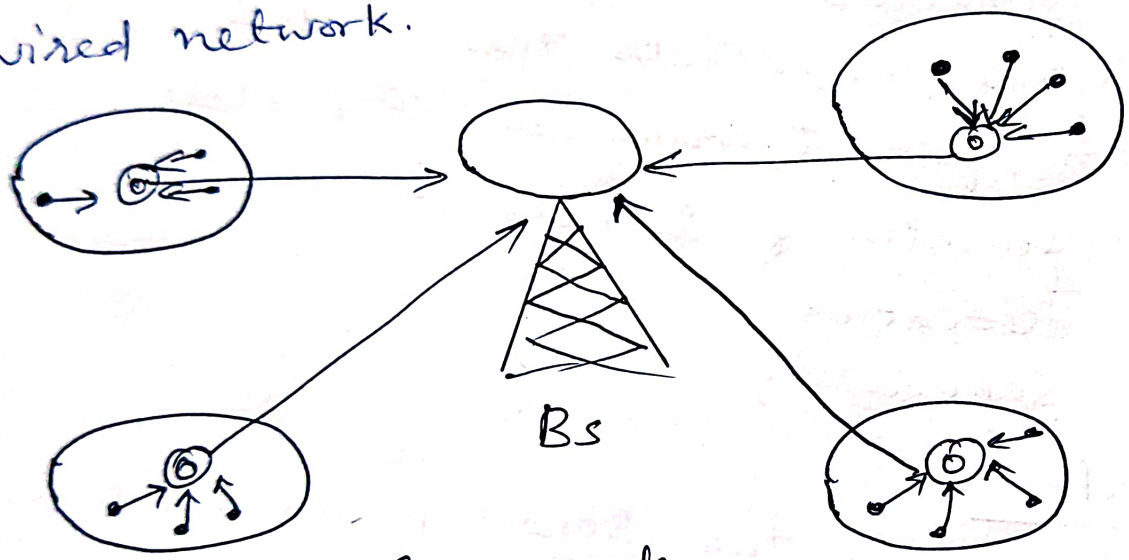
① Each node is involved in minimum distance.

② Low power transmission.

Clustered Architecture.

→ Sensor nodes are organized into clusters with each cluster having cluster head.

→ The nodes in each cluster exchange message with their respective cluster heads, which inturn send message to a base station connected to a wired network.



• → Sensor nodes

⊙ → cluster head.

clustered Architecture.

→ The self organizing Sensor networks are used such that cluster formation and selection of cluster heads are automated and distributed. This Process is achieved through network layer Protocol Such as low Energy adaptive clustering Hierarchy (LEACH).

Sensor Network Scenarios.

→ A Source is any entity in the network that can provide information [Example] Sensor node (or) actuator.

→ A Sink is the entity where information is required

The Sink may be 3 types. They are.

1. Belong to the Sensor network.
2. Another Sensor / actuator node. eg. hand held, PDA, Gateway
3. Entity Outside the network.

Single hop Vs Multihop networks

→ The direct Communication between Source and Sink is not feasible due to limited distance in WSNs.

→ Relay Stations are used with the data Packets taking multiple hops from the Source to Sink. The Sensor node acts as relay nodes.

→ Multihop n/w where direct Communication is not possible due to distance or obstacle.

→ The intermediate Sensor nodes may be used depending upon the application.

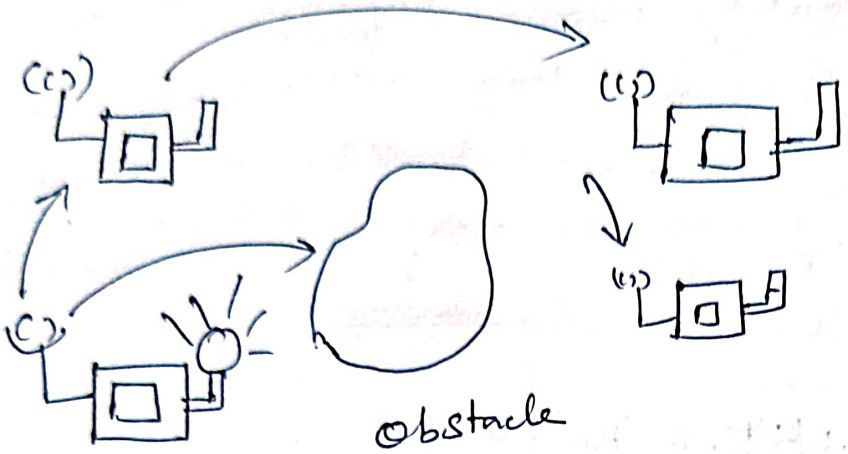
→ The attenuation of radio signals is atleast quadratic in most environment. So it consumes less energy to use relays instead of direct Communication.

→ for Constant SNR, the radiated energy required over a distance d is $C\, d^{\alpha}$.

C → Constant α → path loss Co-efficient $\alpha \geq 2$.

for relay at distance $d/2$, energy $= 2c\left(\frac{d}{2}\right)^{\alpha}$.

→ If intermediate relays are used for short distances d then energy will be wasted.

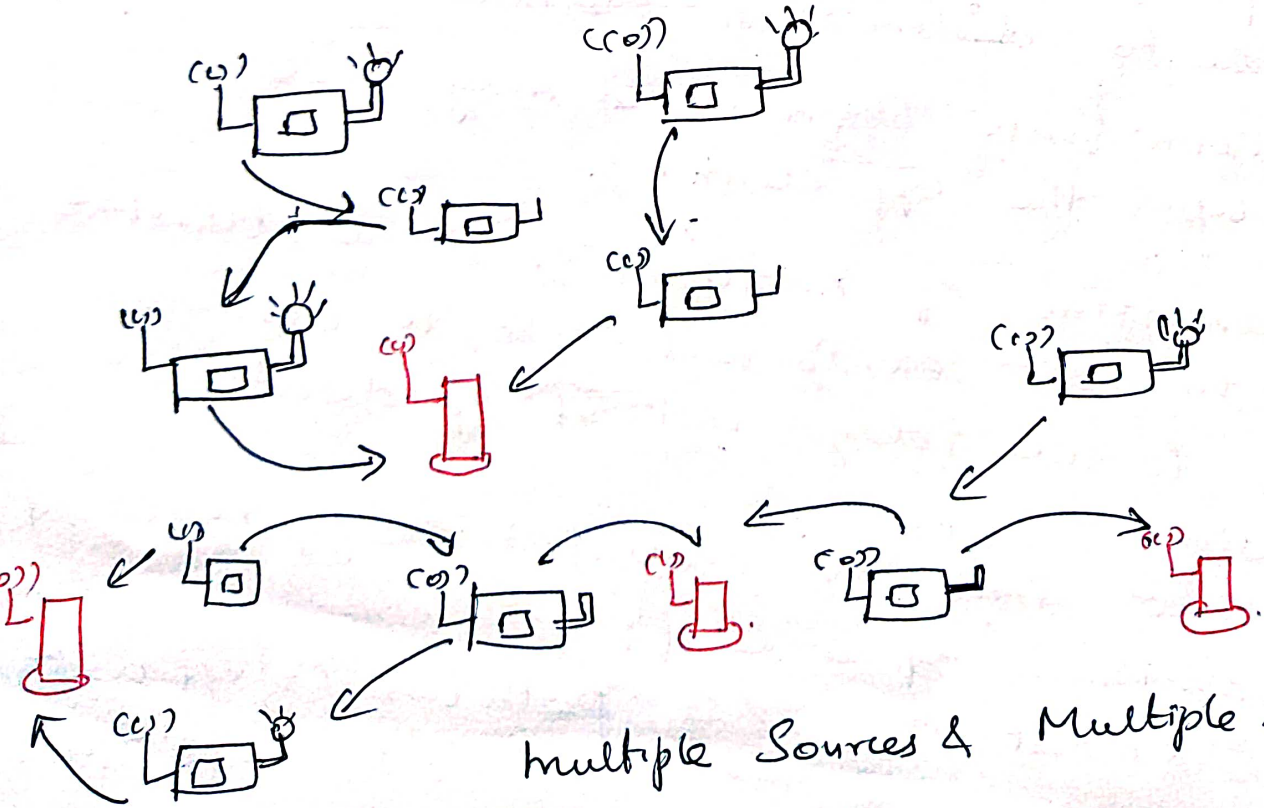


Multihop network.

Multiple Sinks and Sources.

→ There are multiple sources and multiple sinks present in some applications.

→ Multiple sources may send information to multiple sinks if all or some of the information has to reach all or some sinks.



Multiple Sources & Multiple Sinks.

Mobility

All users are assumed to be Stationary. But Wireless Sensor networks Should Support mobile Participants. The mobility are classified into 3 types.

1. Node mobility
2. Sink mobility
3. Event mobility.

Node mobility

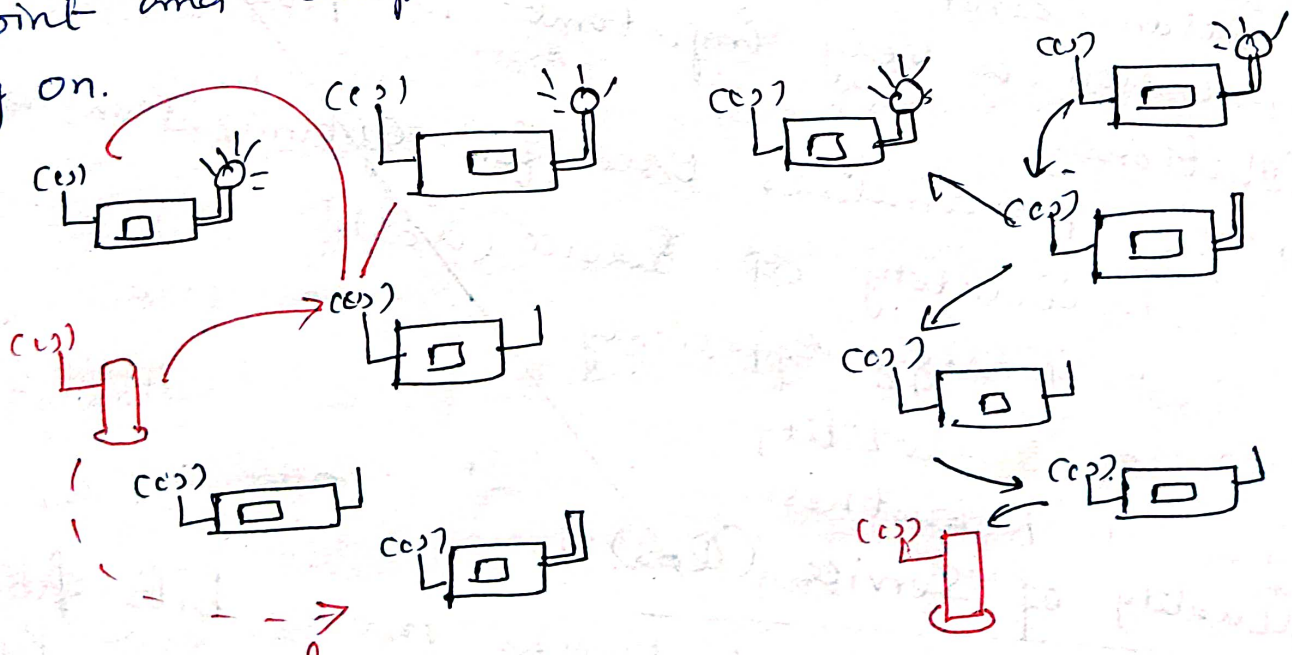
→ The wireless Sensor nodes can be mobile depending on the application.

Example In Environmental Control, node mobility will not occur. In livestock Surveillance ex: Sensor node attached to Cattle.

Sink mobility

The information Sinks can be mobile.

→A human user walking with PDA request Information A requesting user can interact with the WSN at One point and complete its interactions before moving on.



Sink mobility.

→ The requester may be allowed to interact with any node or only with specific nodes.

→ If the requested data is not locally available but available in remote part of the network the network should assist the mobile requester to get the requested data.

Event mobility

→ The events or objects to be tracked may be mobile.

Example: event detection or tracking application.

→ The observed event is covered by a sufficient number of sensors all the time. As the event source moves through the network, it is accompanied by an area of activity within the network. This is known as frisbee model.

Optimization Goals and figure of Merit

→ The optimization of network, comparing the solution and deciding better solution for a given application is very important in providing network solutions.

→ The parameters used for optimization are.

1. Quality of Service (QoS).
2. Energy efficiency.
3. Scalability.
4. Robustness.

1. Quality of Service (QoS)

→ Wireless Sensor Networks move bits from one place to another. for multimedia applications QoS can be regarded as

Optimization Goals and figure of merit

→ Optimizing a network is the challenging task and it is used to find out the better solutions or supports for a given application.

→ It can be achieved by following series of tasks.

Quality of Service (QoS)

→ Wireless Sensor networks differ from other Conventional networks mainly in the type of service they offer. These networks move bits from one place to other.

→ Quality of Service is mainly important in multimedia application. Quality of service has types.

* low level quality of Service.
* High level quality of Service.

→ In low level QoS the networking device have many attribute to observe such as bandwidth, delay, Jitter, Packet loss rate.

→ In high level QoS User observe the perceived quality of a voice communication or video communication. High level quality of Service attributes in wireless Sensor networks highly depends on the application.

Event Detection → Any event occur means it must be detected on node. But some events not yet detected and not reported to an information Sink. for this kind of situations actual task will not take place.

Event classification error:

Events are not only to be detected but it also be classified. The error in classification must be small

Transceiver Design Consideration.

→ Low Power Consumption
→ As one Consequence, Small transmit power and thus small transmission range
→ low degree of mobility
→

Energy Usage Profile

→ The choice of a Small transmit power leads to an Energy consumption Profile different from other wireless devices like cell phones.
first the radiated Energy is Small, typically on the order of 0 dBm.

Choice of Modulation Scheme

A Crucial Point is the choice of modulation Scheme. Several factors have to be balanced here: the required and desirable data rate and symbol rate, the implementation Complexity, the relationship b/w radiated power

UNIT-III

WSN Networking Concepts and Protocols.

Introduction.

* In adhoc wireless network nodes share a common broadcast radio channel. The Bandwidth available is limited due to limited radio spectrum. Therefore all nodes should have equal share of the available bandwidth for effective bandwidth utilization.
* The protocols required for controlling access to the shared medium is different from that of wired network

The various medium access control (MAC) protocols used for adhoc wireless networks.

MAC Protocols.

→ Medium Access Control (MAC) protocol is the first protocol layer above the physical layer 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. is

→ MAC protocols coordinate the times between multiple number of nodes access a shared communication medium.

→ The MAC protocol determines point time of a node when it accesses the medium to try to transmit a data, control or management packet to another node or to a set of nodes.

Fundamentals of MAC Protocols.

→ MAC protocol is the wireless protocol used in wireless Sensor networks.

→ Main task of MAC protocol try to reduce overall energy Consumption

Requirements and Design Constraints for Wireless MAC Protocols.

→ The most important performance requirements for MAC protocols are throughput, efficiency, Stability fairness, low access delay, low transmission Delay. and low overhead.

→ The overhead in MAC Protocol is caused by three things
1. Per Packet overhead
2. Collisions.
3. Exchange of extra Control Packet

MAC Protocols for Wireless Sensor Networks.

* The Single most important requirement is energy efficiency.
* One important approach is to Switch the wireless transceiver into a Sleep mode.
* Specific requirement and design Considerations for MAC Protocols in wireless Sensor networks.

Balance of Requirement-

→ Balancing between many kinds of requirement is more important tasks, because one requirement of system will depend on many other requirements.

→ The important requirements of MAC protocols are ② Scalability, robustness, throughput and fairness.

→ In the MAC layer we have some energy problems such as follows.

* Collisions.
* Overhearing
* Protocol overhead
* Idle listening.

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

→ Important requirements for MAC Protocols are Scalability and robustness against frequency topology changes.

Energy Problems on the MAC layer

* A nodes transceiver consumes a significant share of energy to perform operation.
* Transceiver can be in one of the four main state Transmitting, receiving, idle and sleeping.
* Sleeping can be significantly cheaper than Idle stat
* MAC protocols objective is to reduce energy Consumptio

Major Sources of Energy Waste.

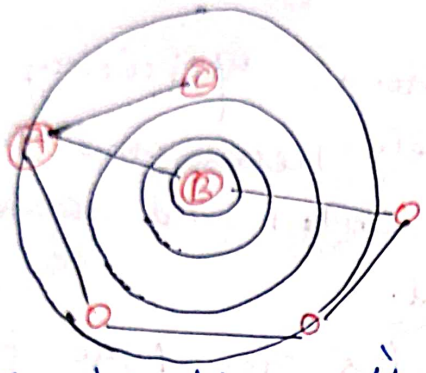
1. Collisions. 2. Overhearing 3. Overhead. 4. Idle listening.

Collisions. → Collisions occur in the MAC protocol if more than one node sends a packet at the same time
→ Collision happen in the node means it request retransmission of packet which increase energy

→ To avoid collisions in the Sensor node following methods can be useful.

- ✓ Fixed Assignment / TDMA
- ✓ Demand Assignment Protocols.
- ✓ Appropriate collisions Avoidance.
- ✓ Hidden terminal Procedures in CSMA protocols.

Over hearing



→ The wireless medium is a broadcast medium and all the Source's neighbours receive a packet. In receive state hear a packet and drop it when it is not destined to them this is called nodes overhear the packet.

→ Node hear packet intended from other nodes.

Idle listening

* Nodes listen to channel for possible traffic. If nothing is Sensed then most of the time nodes is ideal.
* Ideal listening Consume 50-100% energy required to receive packets.
* Idle state node is ready to receive a packet but is not currently receiving anything.

Protocol overhead

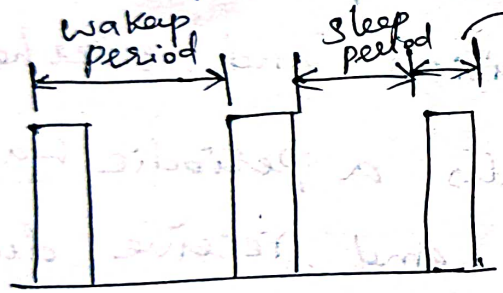
* Protocol overhead is included by MAC-related control frames like RTS and CTS packets or request packets in demand assignment protocols.

Low Duty cycle Protocols and Wakeup Concepts. (3)

* Need for low duty cycle Protocols.
  1. To avoid Spending more time in idle State.
  2. To reduce activities of a Sensor node.

* In an idle Case the node turn into next State when it perform transmit or receive packet. To transmit a node from idle State into active State we need wakeup period.

* cycled Receiver.
  It is one of the periodic wakeup node spend most of their time in sleep mode and wakeup periodically to receive packets from other node.



→ Node A listen the channel during its listen Period and goes back into sleep mode. A transmitter node B should know the listen periods of node A to Send packets at right time. This can be done by
  1. Node A Can transmit a Short beacon at the beginning of its listen period.
  2. Node B Send frequent request packets until A receives it during its listen Period.

Wakeup Period.
A whole cycle of sleep period and listen Period is also called wakeup period.

Duty cycle :

The Ratio of the listen period length to the wakeup period length is known as duty cycle

1. Duty cycle is selected minimum.
   - To avoid idle listening and Conserve Energy of transceiver.
   - The traffic from neighbouring nodes are Concentrated on small time period (or) listen period.
2. Long sleep period increases perhop latency.

S-MAC (Sensor MAC)

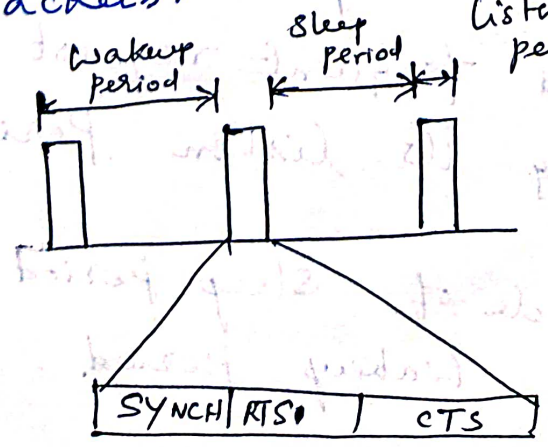
The S-MAC (Sensor MAC) protocol provides mechanism to circulate idle listening, collisions and overhearing

→ S-MAC protocol also provides a periodic wakeup but nodes can both transmit and receive during their wakeup phases.

→ It uses a periodic wakeup scheme.

Each node alternates between a fixed length period and fixed length sleep period according to its schedule.

The listen period of S-MAC is used to receive and transmit packets.



SMAC - operation

→ SMAC protocol co-ordinates the schedules of neighbouring nodes such that their listen periods start at the same time.

→ A node x's listen period has 3 phases.

1. SYNC phase 2. RTS phase 3. CTS phase.

1. SYNCH phase:

A node x accepts SYNCH packets from its neighbours. x stores the schedule of their neighbours in the schedule table.

→ Node x's SYNCH phase is subdivided into time slots and x's neighbours contend according to a CSMA scheme with additional back off.

* Neighbour y select one of the time slots randomly and start to transmit otherwise y goes to sleep mode and waits for x's next wakeup.

* As x knows y's schedule x can wakeup at appropriate times and send its own SYNCH packets to y.

* x send the SYNCH packets periodically for time synchronization and to allow new nodes to learn their new network topology. This period is known as Synchronization Period.

2. RTS phase.

x listen for RTS packets from neighbouring nodes. RTS-CTS handshaking reduce collision of data packets due to hidden terminals.

3. CTS phase.

* Node x transmits a CTS packet if an RTS packet was received in the previous phase. This packet exchange continues extending into x's normal sleep state.
* When nodes compare for the medium, they use the RTS, CTS, handshake and virtual carrier sense mechanism with NAV variable.
* To avoid overhearing, NAV mechanism switch off the node during on going transmission.

Virtual cluster

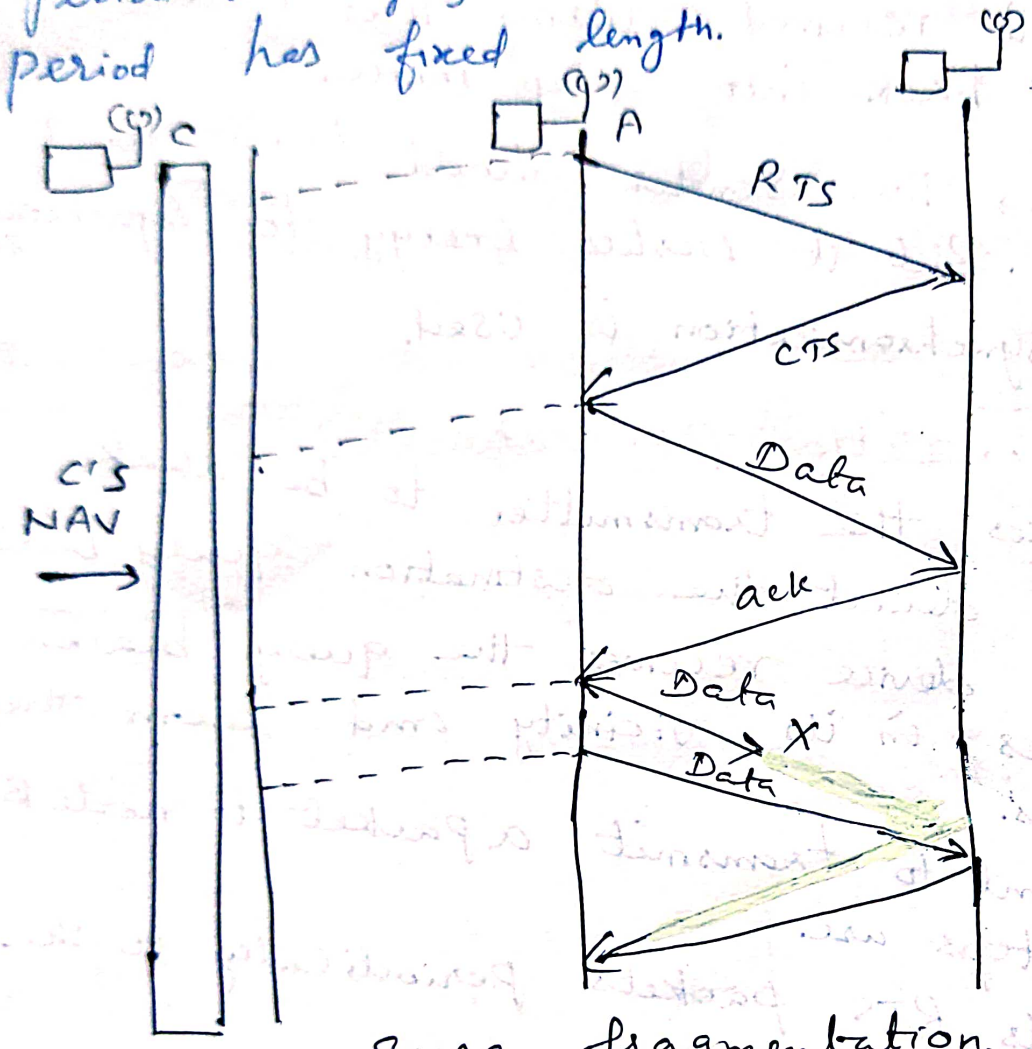
→ The Schedules of node-x and its neighbours are synchronized. x and its neighbours wakeup at the same time and x send a single SYNCH packet to all its neighbours.

Message Passing. → Message is a larger data item useful to the application. In wireless media the longer packet is divided into smaller ones known as fragments.

* Series of fragment is transmitted with only one RTS/CTS exchange between the transmitting node A and receiving node B.
* After each fragment B answer with an acknowledgement packet.
* All the packets such as data, ack, RTS, CTS have a duration field and a neighbouring node C sets its NAV field accordingly.
* The duration field has the remaining length of whole transaction. So the entire message is passed at once.

Advantage Reduced latency.

Disadvantage.
1. Single node can block the medium for long time.
2. Difficult to adopt the length of wakeup period to varying load situations as the listen period has fixed length.



SMAC- fragmentation.

Mediation Device Protocol

→ It is Compatible with the Peer to Peer Communication of IEEE 802.15.4 low rate WPAN Standard.

→ Each node in a WSN goes to sleep mode periodically and wakeup only for short time to receive packet from neighbour nodes.

→ Each node has its own Sleeping Schedule and does not care of its neighbours sleep Schedules.

Query Beacon.

→ A node transmits a short query beacon during periodic wakeup. It indicates the node address and it can accept packets from other nodes.

→ The node is awake for some short time and if no packet is received during this window. the node goes back into sleep mode.

Disadvantages. → The Sender Should wait for the query beacon. But it wastes energy for Synchroni zatio so dynamic Synchronization is used.

Dynamic Synchronization Approach.

→ It eliminates the transmitter to be awake permanently to detect the destination query beacon The mediation device receives the query beacon from all nodes in its vicinity and learn their wakeup periods.

→ node A want to transmit a packet to node B. The required steps are.

1. Node A Sends RTS packets periodically to the mediation device MD.
2. A listen for answer Using the short answer window after the RTS packet.
3. Then MD wait for B's next query beacon and answer this with a query response packet with A's address and timing offset.
4. B Send the CTS packets in the short answer window of A's next RTS packet. Thus B has learned A's period.

5. After receiving CTS packet, A Send its data packet and wait for B's acknowledgement.

6. After transmission A restores its periodic wakeup cycle and Send the query beacons again. B also restores its own periodic cycle.

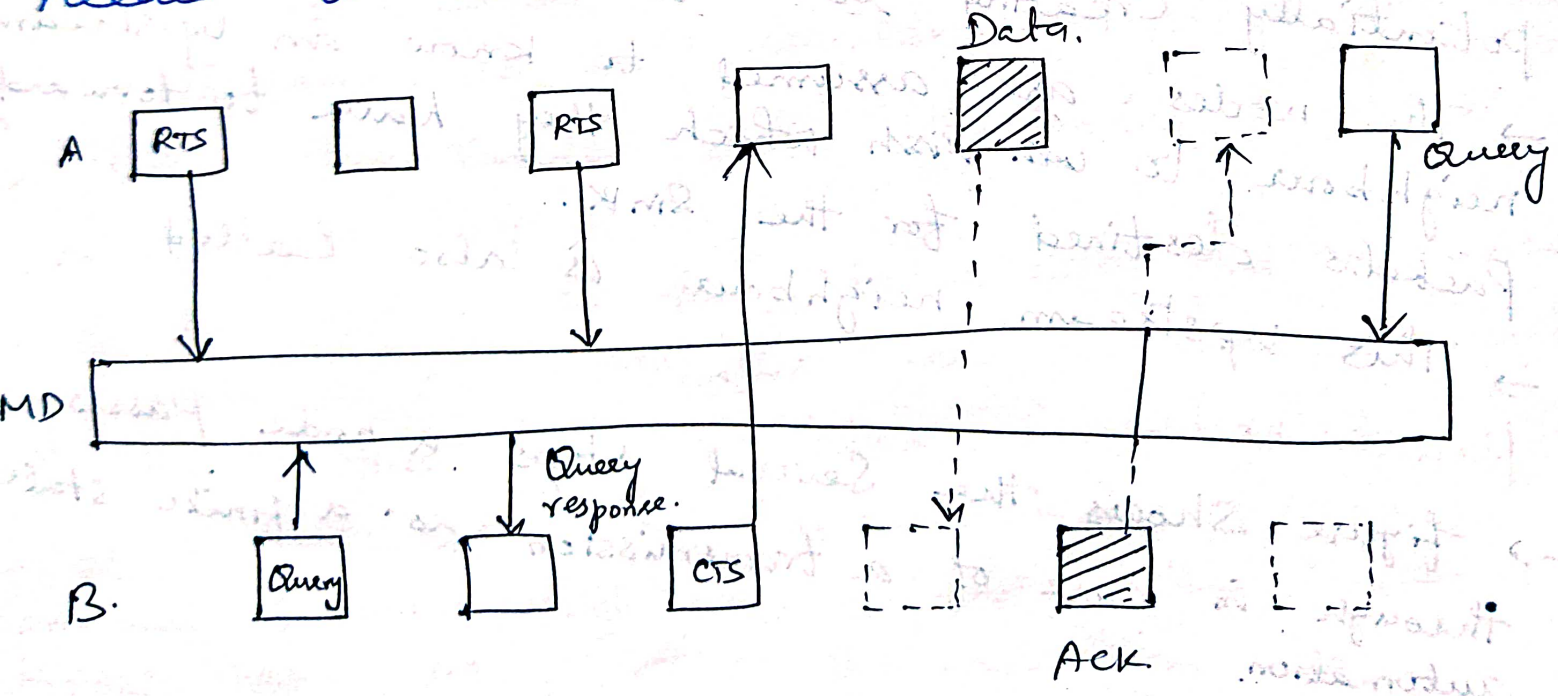
Advantages: * It does not require any time Synchronization between the nodes Only the mediation device has to learn the periods of the nodes.

* The Protocol is asymmetric.

Drawbacks * The nodes transmit their query beacons without checking for ongoing transmission.

* The mediation device is energy unconstrained which does not conform to the idea of a "Simply thrown out" Wireless Sensor networks.

* There is Sufficient mediation devices are needed to cover all nodes.



Mediation device Protocol.

Contention Based Protocol - PAMAS Protocol

→ In Contention based protocols a given transmit opportunity toward a receiver node can in principle be taken by any of its neighbours.

→ If only one neighbour tries its luck, the packet goes through the channel. If two or more neighbours try their luck, these have to compete 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.

CSMA Protocols:

→ A network that is idle for long times and starts to become active when triggered by an important external event.

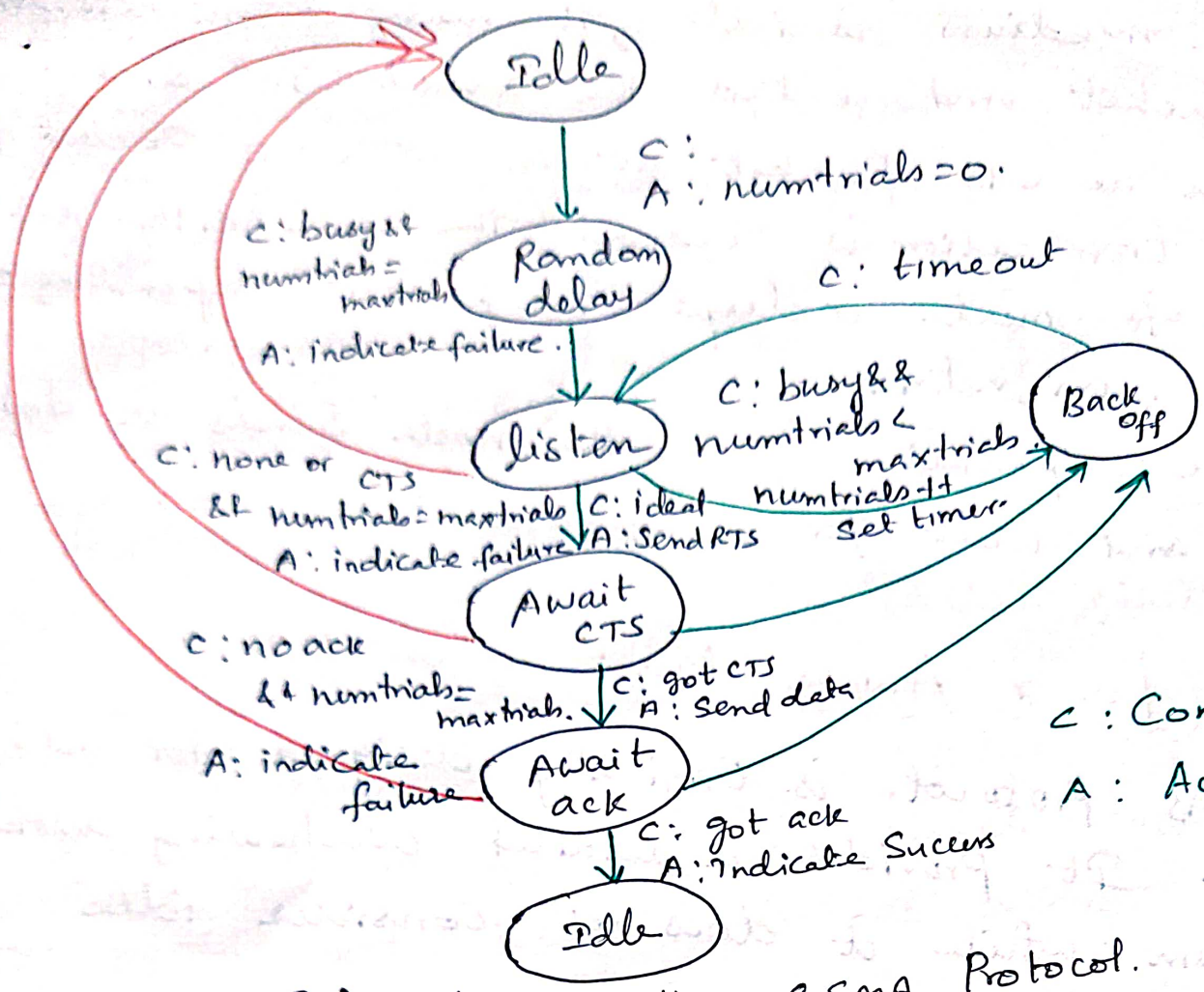
→ all nodes wish to transmit simultaneously potentially creating lots of collisions.

→ The nodes are assumed to know an upstream neighbour to which they have to forward packets destined for the sink.

→ This upstream neighbour is also called

→ Parent node

→ figure shows the several steps a node passes through in case of a transmission as a finite state automation.



Schematic of the CSMA Protocol.

→ After a node gets a new packet for transmission from its upper layers it starts with a random delay and initializes its trial counter num retries with zero

→ During this random delay the node's transceiver can put into sleep mode.

→ If the medium is found to be busy and the number of trials so far is smaller than the maximum number the node goes into the back off mode.

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

→ If the medium is busy and node has exhausted its maximum number of trials, the packet is dropped.

→ If the medium is idle, the node transmits an RTS packet and enters the "await CTS" state.

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

→ If CTS packet arrives, the node Sends its data packet and wait for an acknowledgement.

PAMAS (Power Aware Multi access with Signaling)

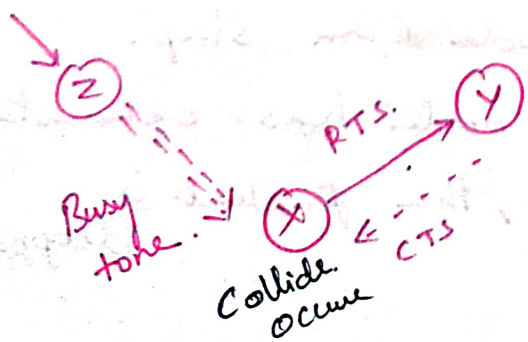
→ PAMAS Protocol is Originally designed for adhoc networks. It provides a detailed overhearing avoidance mechanism while it does not consider idle listening problem.

→ The protocol Combines the busy tone solution and RTS/CTS handshake. Similar to the MACA protocol.

→ Feature of PAMAS is that it Uses two channel
- A - data channel
- A Control channel.

→ All the signalling packets (RTS, CTS, busy tones) are transmitted on the Control channel.

→ Data channel is reserved for data packet.



→ First X sends an RTS packet on the Control channel without doing any Carrier Sensing.

→ 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 start 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 it enters the backoff mode.

→ If z is currently receiving a packet it reacts by sending a busy tone packets which overlaps with y's CTS at node x. and destroys the CTS.

→ Therefore x cannot start transmission and z's packet reception is not disturbed. Since busy tone packet is longer than CTS so CTS is really destroyed

Schedule Based Protocols.

→ Schedule based protocols are based on TDMA technique. It can avoid collisions over hearing and Idle listening problems by time sharing the medium and resource access of the participants.

Scheduled based MAC Protocol challenges.

→ Schedule based MAC Protocols can avoid collisions over hearing and idle listening Problems. there have some drawback. also.

* During network setup and topology changes the maintenance of Scheduling involves traffic Signalling which causes protocol overhead.
* A strict time Synchronization between the neighbouring node is required.
* Schedule adaption becomes difficult with the change of network traffic load.
* The nodes require significant amount of memory to keep its and its neighbour Schedule.

LEACH [Low Energy Adaptive clustering Hierarchy]

→ LEACH assumes a dense Sensor network of homogeneous, energy contrained nodes, which shall report their data to a Sink node.
→ In LEACH, a TDMA based MAC protocol is integrated with clustering and Simple routing protocol.
→ LEACH partitions the nodes into clusters and in each cluster a dedicated node, the cluster head is responsible for creating and maintaining a TDMA schedule; all the other nodes of a cluster are member nodes.
→ To all member nodes, TDMA slots are assigned which can be used to exchange data between the member and cluster head.

→ The cluster head aggregates the data of its members and transmits it to the sink node or to other nodes for further relaying.

→ Since the sink is often far away the cluster head must spend significant energy for this transmission.

→ All nodes make their decisions to become a cluster head.

→ The non cluster head nodes have to associate to a cluster head subsequently

→ The non cluster heads choose their cluster head based on received signal strengths.

→ After the clusters have been formed each cluster head picks a random CDMA code for its cluster, which it broadcasts and which its member nodes have to use subsequently.

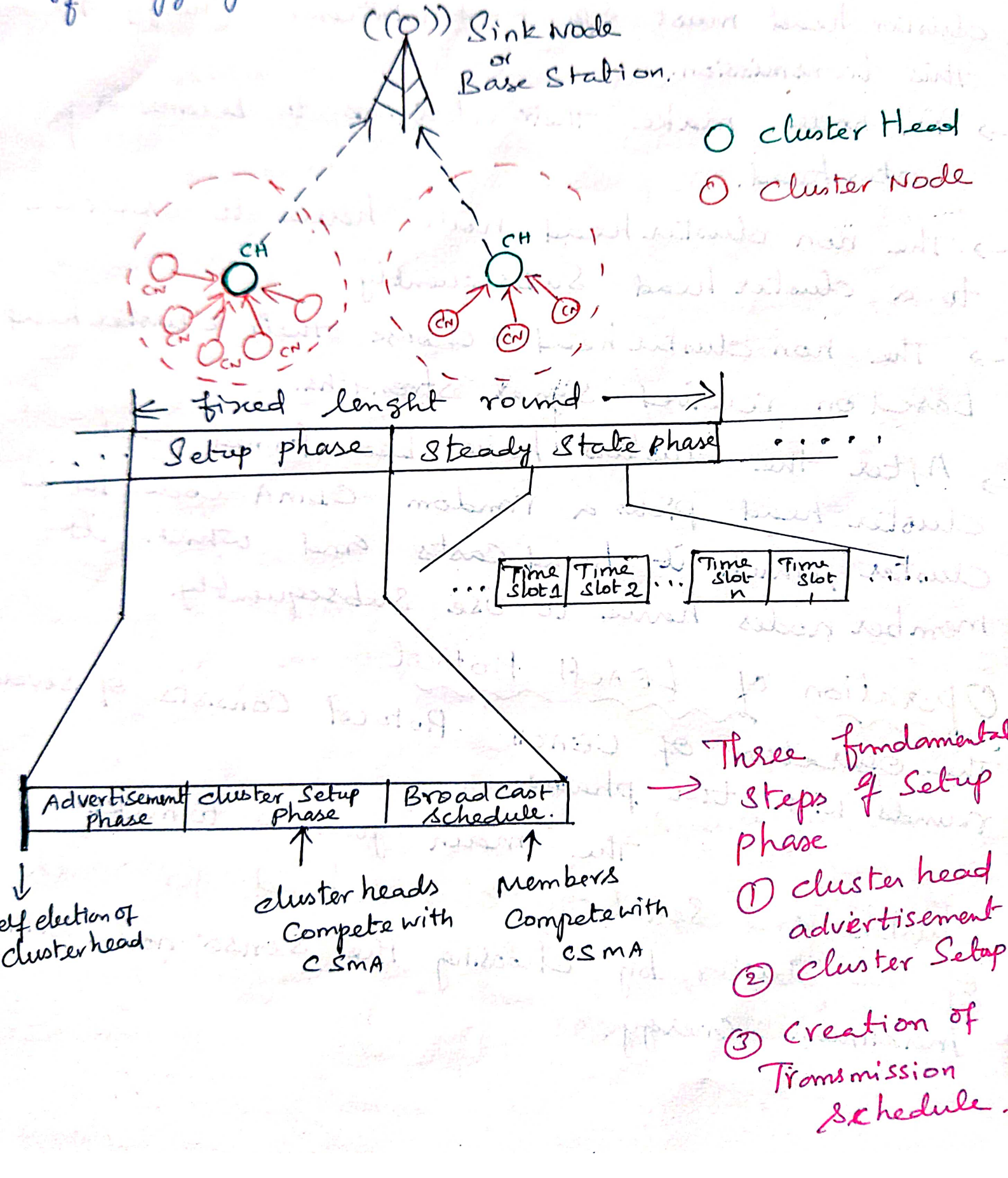
Operation of LEACH Protocol

The operation of LEACH Protocol consists of several rounds with two phases.

① Set up phase: The main goal is to make cluster and select the cluster head for each of the cluster. by choosing the sensor node with maximum energy.

2. Steady Phase:

Which is Comparatively longer in duration than the Set up deals mainly with the aggregation of data at the cluster heads and transmission of aggregated data to the Base Station.



→ Three fundamental steps of Setup phase

1. cluster head advertisement
2. cluster Setup
3. Creation of Transmission schedule.

① Cluster Head advertisement.

→ During the first step cluster head Sends the advertisement packet to inform the cluster nodes that they have become a cluster head.

→ The node becomes cluster head for current round based on energy availability.

→ Once the node is elected as a cluster head it cannot become cluster head again until all the nodes of the cluster have become Cluster head once This helps in balancing the energy Consumption.

② cluster Setup:

→ The non cluster head nodes receive the cluster head advertisement and then Send join request to the cluster head informing that they are the membe of the cluster under that cluster head

→ These non cluster head nodes Saves a lot of energy by turning off their transmitter all the time and turn it ON only when they have Something to transmit to the cluster head.

③ Creation of Transmission Schedule.

→ In the third step each of the chosen cluster head creates a transmission schedule for the member nodes of their cluster.

→ TDMA Schedule is created according to the number of nodes in the cluster. Each node then transmits its data in the allocated time Schedule.

② Steady phase:

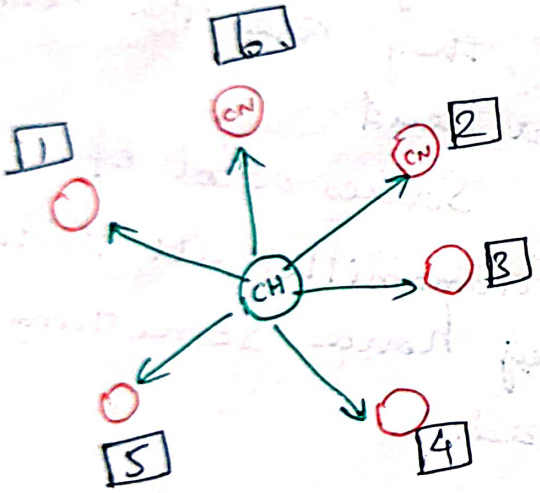
→ The second phase of LEACH is the steady phase during which the cluster nodes send their data to the cluster head.

→ The member sensors in each cluster communicate only with the cluster head via single Hop transmission.

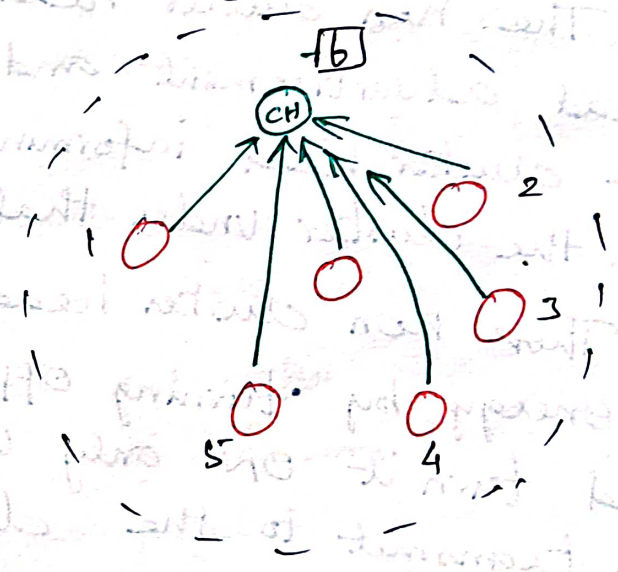
→ The cluster head then aggregates all the collected data and forwards this data to the base station, either directly or via other cluster head.

→ After the certain predefined time, the network again goes back to the setup phase.

① cluster Head advertisement



② cluster setup.



Advantages:

① Schedule based protocols LEACH that do explicitly address idle listening avoidance by employing TDMA schedules.

② which explicitly assign transmission and reception opportunities to nodes and let them sleep at all other times.

③ Transmission schedules can be computed such that no collision occur at receivers.

④ Hence no Special mechanisms are needed to avoid hidden terminal Situations.

Disadvantages:

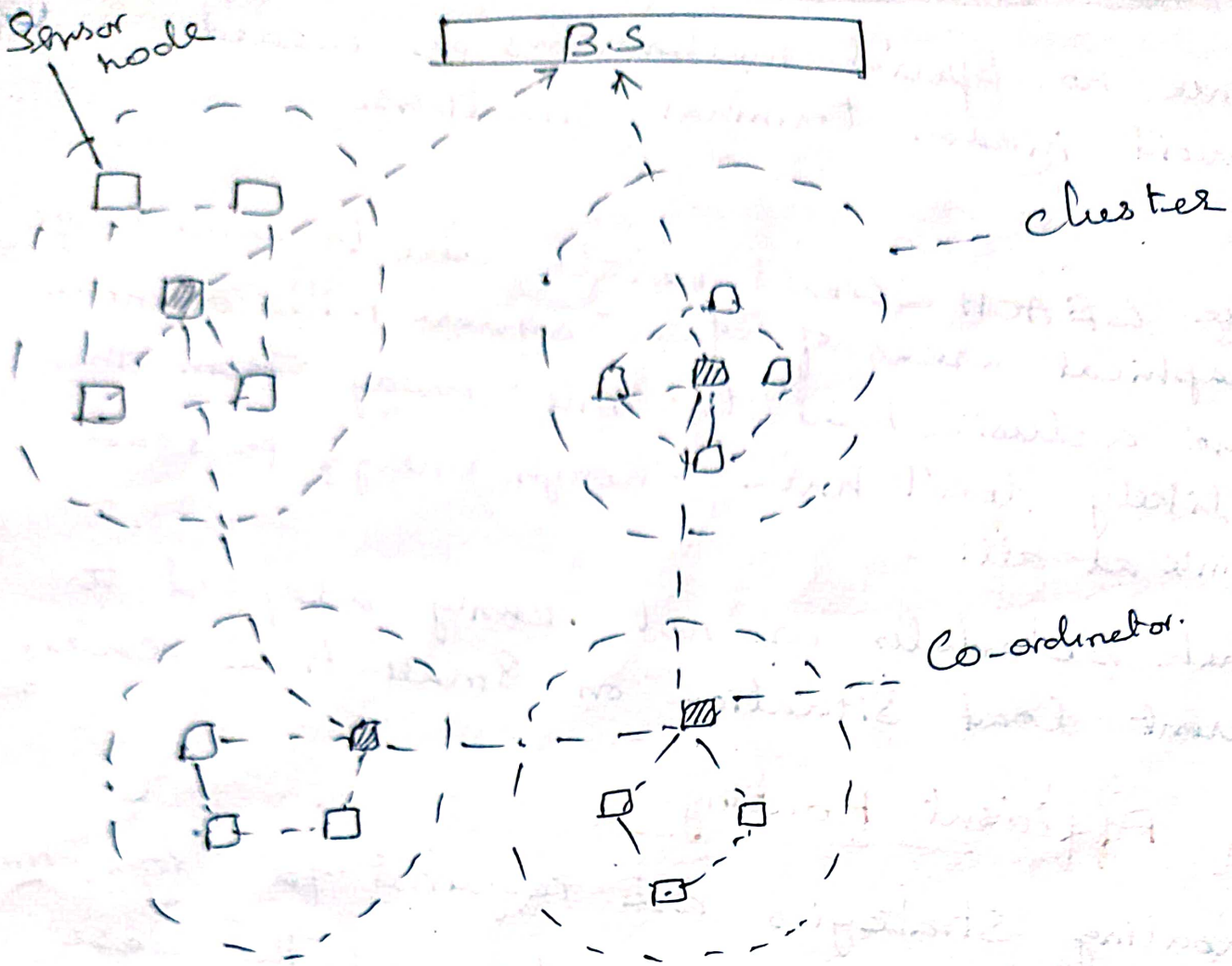
① The LEACH would not be able to cover large geographical areas of some square miles or more because a cluster head two miles away from the sink likely doesn't have enough energy to reach the sink at all.

② Such schedules are not easily adapted to different load Situation on small time scales.

Energy Efficient Routing.

* Routing Strategies are required for transferring data between the Sensor nodes and the base Station.

* Energy efficiency of a network is a significant Concern in WSN. These days networks are becoming large, So information gathered is becoming even larger, which all Consume a great amount of energy resulting in an early death of a node. Therefore many energy efficient protocols are developed to lesson the power used in data Sampling and collection to extend the life time of a network.



Energy efficient Unicast Routing

* 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.

1). Minimize energy Per Packet (or per bit)

2) Maximize network life time

3) Routing Considering available battery energy.

(i) Maximum Total Available battery Capacity

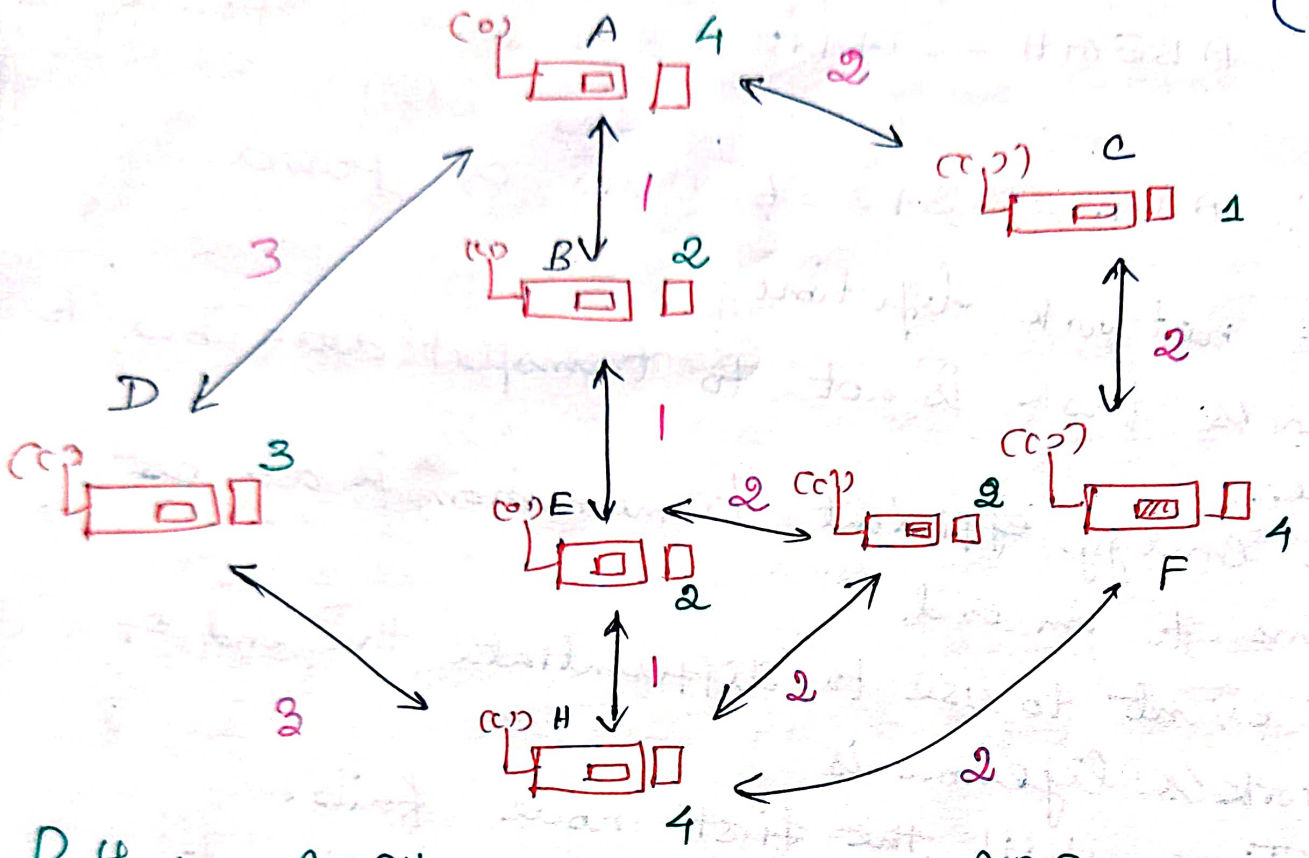
(ii) Minimum Battery cost Routing (MBCR)

(iii) Min-Max Battery Cost Routing (MMBCR)

(iv) Conditional Max-Min Battery Capacity Routing (CMMBCR)

(v) Minimize Variance in Power level.

(vi) Minimum Total Transmission Power Routing (MTPR).



Path 1 = ACFH

Path 2 = ABEGH

Path 3 = ABEH

Path 4 = ADH.

Send data from node A to node H.

Minimize Energy Per Packet (or Per bit)

* The most straight forward formulation is to look at the total energy required to transport a packet over a multihop path from source to destination.

* The goal is then to minimize for each packet by selecting a good route.

However this cost metric can be easily included in standard routing algorithm.

→ Based on cost of the link per path.

Path 1: ACFH = 2+2+2 = 6. Units of Power

Path 2: ABEGH = 1+1+2+2 = 6 Units of Power

Path 3: ABEH = 1+1+1 = 3 Units of Power

Path 4: ADH = 3+3 = 6 Units of power.

Maximize network lifetime:

* A WSN's task is not to transport data but to observe.
* Hence energy efficient transmission is at best a means to an end.
* Which event to use to differentiate the end of a network's lifetime is
  1. Time until the first node fails.
  2. Time until there is a spot that is not covered by the network.
  3. Time until network partition (when there are two nodes that can no longer communicate with each other).

Maximum Total Available Battery Capacity.

* Choose that route where the sum of the available battery capacity is maximized.
* Based on available battery units per path

Path 1 = ACFH = 1+4 = 5 Units of power - Selected

path 2: ABEGH = 2+2+2 = 6 Units of power - not Selected.

Path 3: ABEH = 2+2 = 4 Units of Power

Path 4: ADH = 3 = 3 Units of power.

* Looking only at the intermediate nodes route A-B-E-G-H has a total available capacity of 6 units. but that is only because of the extra node G that is not really needed.

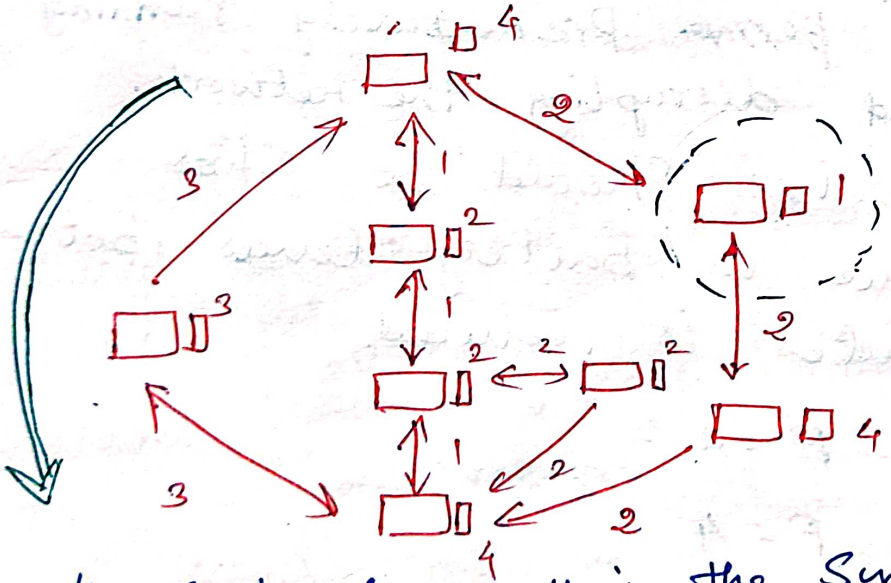
* Hence A-B-E-G-H should be discarded as it contains A-B-E-H as a proper subset.

Minimum Battery Cost Routing (MBCR):

→ Instead of looking directly at the sum of available battery capacities along a given path.

→ MBCR looks at the "reluctance" of a node to route traffic

→. This reluctance increase as its battery is drained for example routing cost can be measured as the reciprocal of the battery capacity.



→ Then the cost of a path is the sum of this reciprocals and the rule is to pick that path with the smallest cost.

Path 1 = ACFH = $1/1 + 1/4 = 1.25$

Path 2 = ABEGH = $1/2 + 1/2 + 1/2 = 1.5$

Path 3 = ABEH = $1/2 + 1/2 = 1$

Path 4 = ADH = $1/3 = 0.33$ Selected

Conditional Max-Min Battery Capacity Routing (CMMBCR).

→ Minimize Energy Per Packet.

→ Minimum Battery Cost Routing (MBCR).

→ Another option is to conditionalize upon the actual battery power levels available. 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.

→ If there is no such route, then pick that route which maximize the minimum battery level (Minimum Battery Cost Routing).

Minimize Variance in Power levels:

→ To ensure a long network lifetime one strategy is to use up all the batteries uniformly to avoid some nodes prematurely running out of energy and disrupting the network.

→ Hence routes should be chosen such that the variance in battery levels between different routes is reduced.

A = 4 E = 2

B = 2 F = 4

C = 1 G = 2

D = 3 H = 4

Minimum Total Transmission Power Routing (MTPR)

→ Without actually considering routing a such looked at the situation of several nodes transmitting directly to their destination mutually causing interference with each other.

→ A given transmission is successful if its SINR (Signal to Interference plus noise ratio) exceeds a given threshold.

→ The goal is to find an assignment of transmission power values for each transmitter such that all transmissions are successful and that the sum of all power value is minimized.

→ MTPR is of course also applicable to multihop networks

Challenges and Issues in Transport layer Protocol

Induced Traffic:

* Unlike wired networks, adhoc wireless networks utilize multi hop radio relaying.
* A link level transmission affects the neighbor node of both the sender and receiver of the link.
* In a path having multiple links, transmission at a particular link affect one upstream link and one downstream link.
* This traffic at any given link (or path) due to the traffic through neighbouring links (or paths) is referred to as induced traffic.

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.

→ for example an ad hoc wireless network that uses IEEE 802.11 DCF as the MAC protocol may experience throughput unfairness at the transport layer as well.

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 activities, where as Congestion can at times be a local activity

→ The Transport layer flow can experience Congestion with just one intermediate link under Congestion.

Power and Bandwidth Constraints:

→ Nodes in ad hoc wireless networks face resource Constraint including the two most important resources. (i) power source (ii) bandwidth.

→ The performance of a transport layer protocol is significantly affected by these Constraints.

Misinterpretation of Congestion:

→ Traditional mechanism of detecting Congestion in networks such as packet loss and retransmission timeout, are not suitable for detecting the network Congestion in adhoc wireless networks.

Completely decoupled transport layer:

→ Another challenge faced by a transport layer protocol is the interaction with the lower layers.

→ 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, partioning and remerging of networks. and high delay in re establishment of paths.

→ Hence the performance of a transport layer protocol is significantly affected by the rapid changes in the network topology.

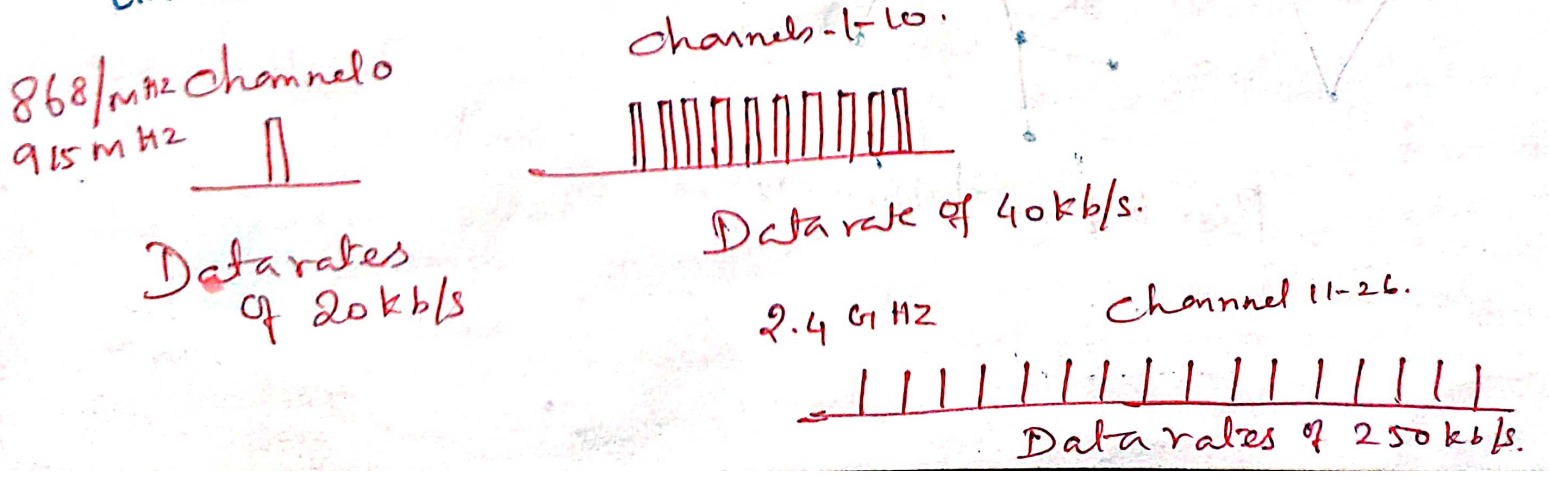
The IEEE 802.15.4 MAC Protocol.

→ The Standard Covers the physical layer and the MAC layer of a low rate wireless personal Area Network (WPAN).
→ star or peer to peer operation.
→ Support for low latency devices.
→ Fully hand shake Protocol for transfer reliability
→ Low power Consumption
→ Combines both Schedule-based as well as Contention based Schemes.

Applications: → Home automation, home networking, Connecting devices to a PC, home security.

Physical layer overview:

→ physical layer offers bitrates of 20 kbps (single channel in the frequency range 868-868.6 MHz)
→ 40 kbps (ten channels in the range between 905 and 928 MHz)
→ 250 kbps there are a total 27 channels
→ MAC Protocol Uses only one of these channels at a time. it is not a multi channel Protocol.



Network architecture and Types/Roles of nodes.

Two types of nodes:

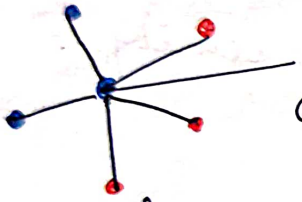
Full Function Device (FFD) can Operate in three different roles:

1. PAN Co-ordinator (PAN = Personal Area Network)
2. A Simple Co-ordinator.
3. A device.

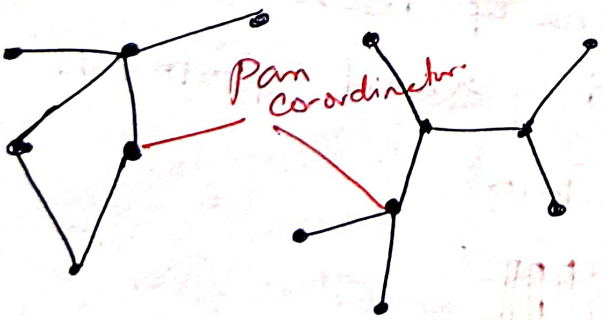
Reduced Function Device (RFD)

* It operate only as a device.

- Full function Device
- Reduced function Device.



* A device node must be associated to a Coordinator node and communicates directly to the Co-ordinator. (forming a star network).
* Co-ordinators can Operate in a Peer to Peer fashio
* Multiple Co-ordinators can form a Personal Area Network. (PAN).



Peer to peer technology.

A Co-ordinator handles among other tasks.

→ It manages a list of associated devices.

→ Devices are required to explicitly associate and disassociate with a Co-ordinator Using Certain Signaling packets.

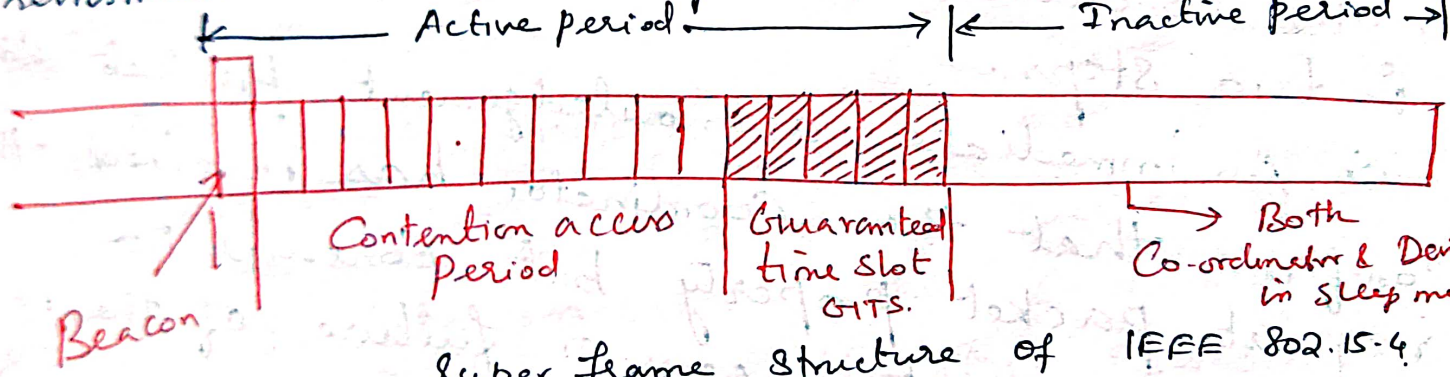
→ It allocates short address to its devices.

→ All IEEE 802.15.4 nodes have a 64 bit device address

→ It exchanges data packets with devices and with Peer Coordinators.

Super frame Structure:

The Coordinator of a Star network operating in the beaconed mode organizes channel access and data transmission with the help of a Superframe Structure.



Super frame Structure of IEEE 802.15.4

→ Superframe is subdivided into an active period and an inactive period. During the inactive period, all nodes including the Co-ordinator can switch off their transceiver and go into sleep state.

→ The nodes have to wakeup immediately before the inactive period ends to receive the next beacon.

→ The co-ordinator is active during the entire active period

→ The associated devices are active in GTS phase only in time slot allocated to them. in all other GTS slots they can enter sleep mode.

GTS Management (Guaranteed Time Slots)

→ The Coordinator allocates GTS to devices only by Sending appropriate request packets during the CAP.

→ Flag in the request indicates whether the requested time slot is a transmit slot or receive slot.

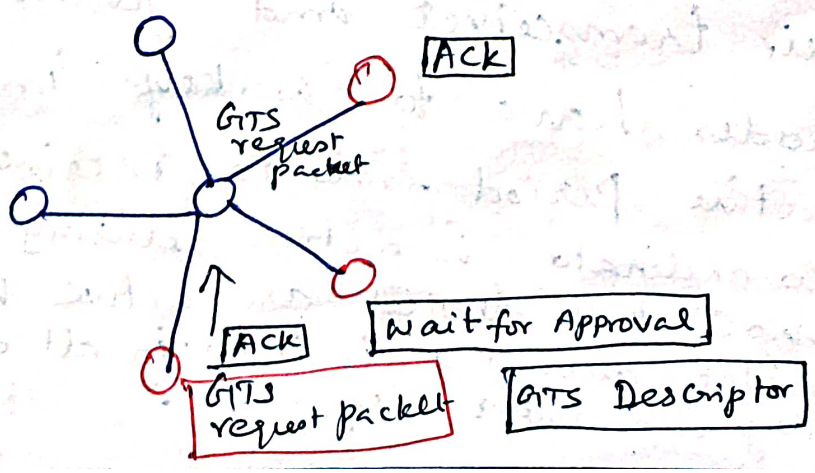
→ In a transmit slot the device transmits Packets to the coordinator and in a receive slot the data flow in the reverse direction.

→ Another field in the request Specifies the desired number of time slots in GTS phase.

→ The Co-ordinator answers the request packet in two steps.

(i) An immediate acknowledgement packet Confirms that the Coordinator has received the request packet properly but Contains no information about Success or failure of the request

(ii) After receiving the acknowledgement packet the device is required to track Coordinator's beacons for some Specified time.



→ If the Co-ordinator has insufficient resources it generates a GTS descriptor for (invalid) time slot zero.

→ The device may Consider renegotiation. it Concludes that allocation request has failed.

→ A GTS is allocated to a device on a regular basis Until it is explicitly deallocated.

→ The deallocation Com be requested by the device by means of a Special Control frame.

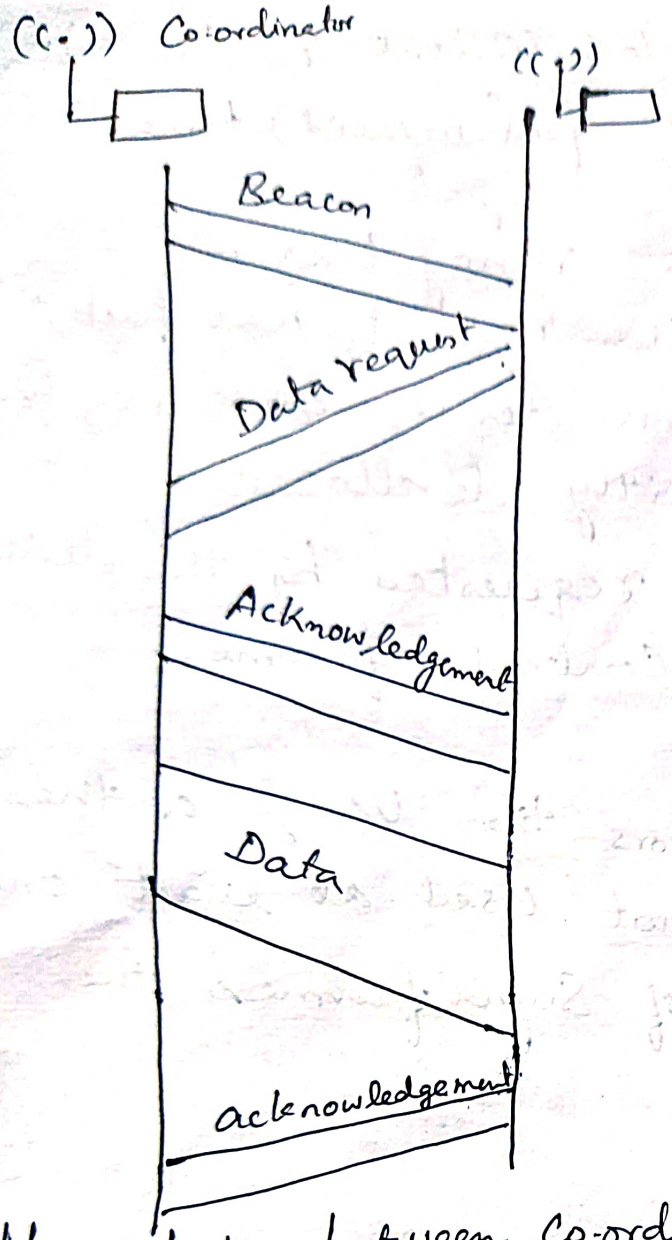
→ After Sending

→ The Co-ordinator monitors the Usage of the time slot If the slot not used at least once within a Certain number of Superframes the slot is deallocated.

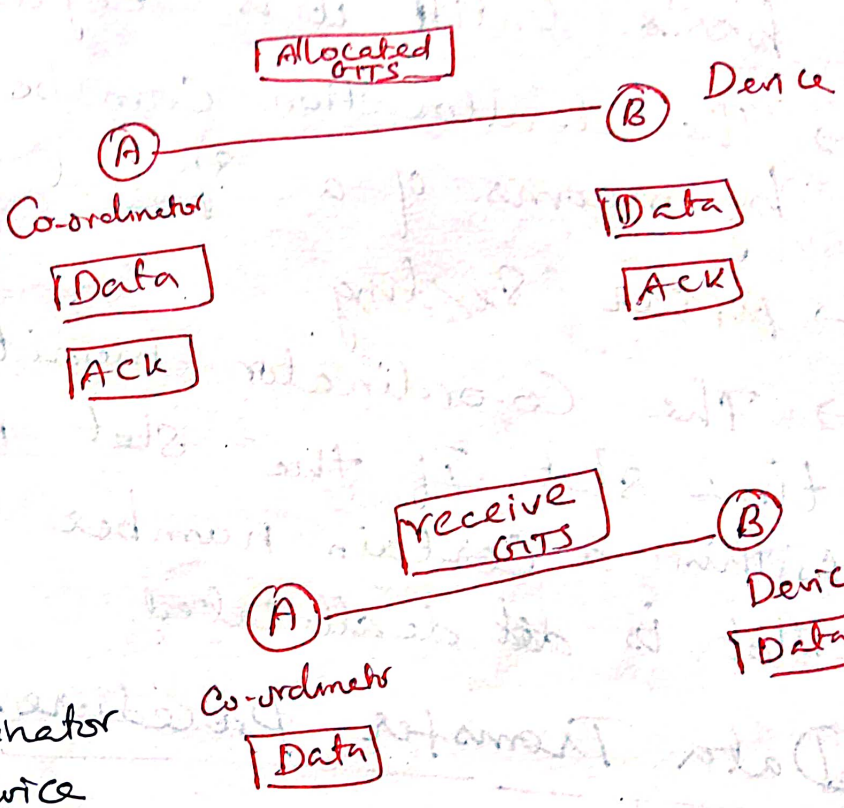
Data Transfer Procedure.

→ First assume that a device wants to transmit a data packet to the Coordinator. If the device has an allocated transmit GTS, it wakes up just before the time slot starts and Sends its packet immediately without running any Carrier Sense or other Collision avoiding Operations.

→ However, the device Can do so only when the full transaction Consisting of the data packet and an immediate acknowledgement Sent by the Co-ordinator as well as appropriate Inter frame spaces (IFSs) fit into the allocated time slots



Handshake between co-ordinator and device when the device retrieves a packet.



UNIT-IV

Sensor Network Security

Network Security Requirements

A Security Protocol for adhoc wireless networks should satisfy the following requirements.

Confidentiality

→ The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node).

→ Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data.

→ One of the popular techniques used for ensuring Confidentiality is data encryption.

Integrity

The data sent by the source node reach the destination node as it was sent, unaltered.

* It should not possible for any malicious node in the network to tamper with the data during Transmission.

Availability:

→ The network should remain operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it.

Non repudiation:

Non repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient

Cannot deny having received the message.

Issues and Challenges in Security Provisioning

→ The design of Security Protocol for adhoc wireless network is very challenging due to their Unique characteristics such as

1) Shared broad cast radio channel
2) Insecure operating environment
3) Lack of Cntral authority
4) Lack of association among nodes.
5) Limited availability of resources.
6) physical Vulnerability.

Shared broadcast radio channel:

→ In wired network a Separate dedicated transmission line exist between a pair of end users.

→ But in adhoc network the radio channel is broadcast nature and shared by all nodes in the network ie) data transmitted by a node and received by all nodes in the network.

→ Hence malicious node Can easily access the data transmitted in the network.

→ Directional antenna Can minimize this problem.

InSecure Operating environment:

→ The operating environment may not always be secure Ex. In battle field the nodes may move in and out of insecure enemy territory and they are highly Vulnerable to Security attacks.

Lack of Central authority

→ In wired network the traffic is monitored and Security mechanisms are implemented at Central points.
→ Ex. Routers, base stations, access points. But adhoc wireless networks do not have any such Central points.

Lack of association.

→ Due to dynamic nature a node can join or leave at any point of the time.
→ If no proper authentication mechanism is used for associating nodes with a networks, an intruder would be able to join into the network, quite easily and carry out his/her attacks.

Limited Resource availability

→ Resources such as bandwidth, battery power and Computational power are scarce in adhoc wireless networks.
→ Therefore Complex Cryptography based security mechanism are difficult to implement.

Physical Vulnerability

→ In adhoc networks nodes are usually Compact and hand held in nature. They are damaged easily and vulnerable to theft.
→ "Node Capture": The Sensor nodes are physically accessed by attackers. This is known as node capture. The attackers may achieve full Control over the Captured node. (ie) read its memory, change its Operation etc.

Network Security Attacks.

Attacks on adhoc wireless networks can be classified into two broad categories. 1. active 2. passive attack.

Passive attack

→ A passive attack doesnot disrupt the operation of the network, the adversary snoops the data exchanged in the network without altering it.

→ The requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping.

Active attack

→ An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

→ Active attacks can be classified further into two categories external and internal attacks.

→ External attacks are carried out by nodes that do not belong to the network.

→ These attacks can be prevented by using standard security mechanism such as encryption techniques and firewalls.

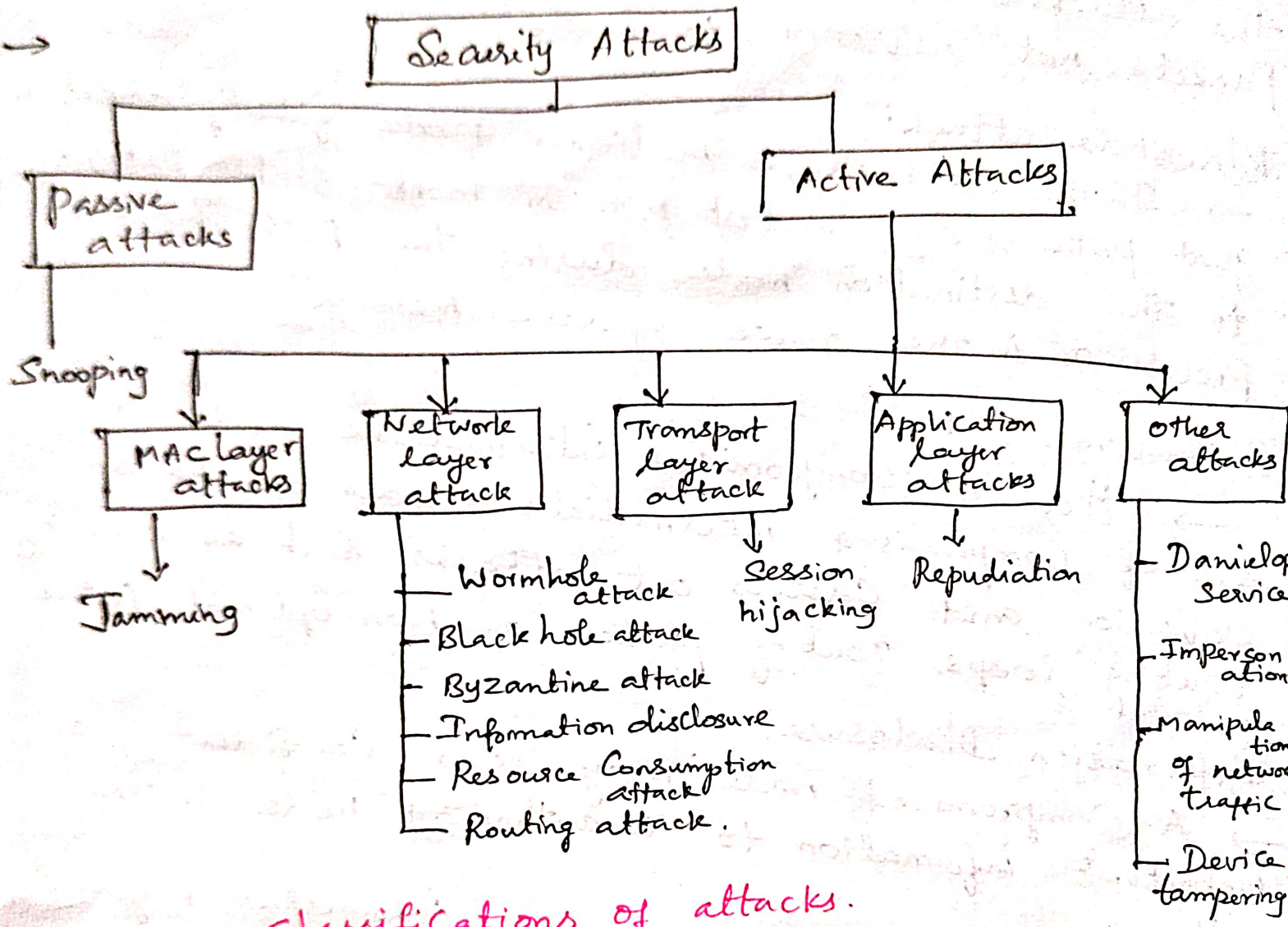
→ Internal attacks are from compromised nodes that are actually part of the network.

Firewalls:

→ A Firewall is used to separate a local network from the outside world.

→ It is a software which works closely with a router program and filters all packets entering the network to determine whether or not to forward those packets towards their intended destinations. (3)

→



Classifications of attacks.

Network layer attacks:

This Section lists and gives brief description of the attack pertaining to the network layer in the network.

Wormhole attack.

→ In this attack, an attacker receives packets at one location in the network and tunnels them to other location in the network where the packets are resent into the network.

→ This tunnel between two colluding attackers is referred to as a wormhole.

→ Due to the broadcast nature of the radio channel the attackers can create a wormhole even for packets not addressed to itself.

Blackhole attack:

→ In this attack, a malicious node falsely advertises good paths (e.g shortest path or most stable path) to the destination node during the path finding process or in the route update message.

Byzantine Attack

→ Here a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, routing packet on non-optimal paths.

Information Disclosure:

→ A compromised node may leak confidential or important information to unauthorized nodes in the network.

→ Such information may include information regarding the network topology, geographic locations of nodes.

Resource Consumption attack

→ In this attack, a malicious node tries to consume/waste away resources of other nodes present in the network.

→ The resources that are targeted are battery power, bandwidth, and computational power.

Routing attacks

→ There are several types attacks mounted on the routing protocol which are aimed at disrupting the operation of the network.

Routing table overflow:

→ In this type of attack an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.

→ The main objective of such an attack is to cause an overflow of the routing tables.

Routing table poisoning:

→ Here the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.

Packet Replication:

→ In this attacks an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes.

Route cache poisoning:

→ In this case of on-demand routing protocols, each node maintains a route cache which holds information regarding routes

→ Similar to routing table poisoning, an adversary can also poison the route cache.

Rushing attack:

→ On demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.

→ An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react.

→ Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets.

Transport layer attack.

→ This section discusses an attack which is specific to the transport layer in the network protocol stack.

Session Hijacking.

→ Here an adversary takes control over a session between two nodes.

→ Once the session between two nodes gets established the adversary node masquerades as one of the end nodes of the session and hijacks the session.

Application Layer attacks.

→ This section briefly describes a security flaw associated with the application layer in the network protocol stack.

Repudiation.

→ In simple terms, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

Other Attacks

This Section discusses Security attacks that Cannot Strictly be associated with any Specific layer in the network protocol stack.

Multi-layer attacks.

→ Multi layer attacks are those that could in any layer of the network protocol stack.

Denial of Service:

→ In this type of attack, an adversary attempt to prevent legitimate and authorized Users of Services offered by the network from accessing those Services.

→ A denial of Service (DOS) attack Can be carried out in many ways. The classic way is to flood packets to any Centralized resource. Ceg. an access Point). Used in the network so that the resource is no longer available to nodes in the network, resulting in the network no longer operate in the manner it was designed to operate.

→ On the physical and MAC layer an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel.

→ On the network layer, an adversary could take part in the routing process. and exploit the routing protocol to disrupt the normal functioning of the network.

Jamming:

→ In this form of attack, the adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender.

→ Frequency hopping Spread Spectrum (FHSS) and direct Sequence Spread Spectrum (DSSS) are two commonly used techniques that overcome jamming attacks.

SYN flooding:

→ Here an adversary sends a large number of SYN packets to a victim node, spoofing the return addresses of SYN packets.

→ On receiving the SYN packets, the victim node sends back acknowledgement (SYN-ACK) packets to nodes whose addresses have been specified in the received SYN packets.

Possible Solutions for Jamming

→ Jamming can be described as any disruption or interference with the physical transmission and reception of wireless signals.

→ This can be either intentional in the form of radio frequency interference, Unintentional in cases of collision and noise interference at the receiver.

→ During jamming attack, the jammer aim is to disrupt communication between the transmitter and receiver using minimal power.

→ It disrupt the communication by reducing the SNR.

→ Main aim of the jamming device is to occupy the channel and ensure that network is not available for legitimate nodes.

→ Two types of jamming attack namely physical and Virtual jamming.

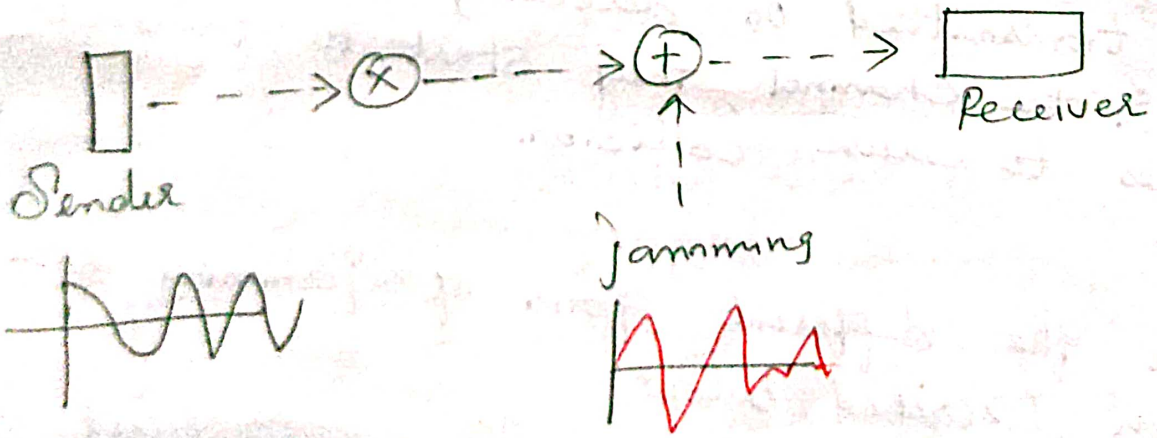
→ physical jamming attacks are radio jamming and Collision attack.

→ Virtual jamming attack Consists of RTS/CTS attack.

Constant Attack

→ In a constant jammer attack the jamming device donot follow laid down Protocol before Continually transmitting Series of radio signals, electromagnetic waves or radio Sequence of bits to interfere with legitimate transmitted Signals in the network

→ Furthermore Constant jammer attacks can Cause interference at the transmitting nodes to corrupt the Signals received by the receiving nodes.



Deceptive jammer:

→ The deceptive jammer Continuously transmits regular packets of data, instead of emitting random bits of data

→ When Compared to a Constant jammer it is more difficult to detect a ~~dope~~ deceptive jammer because

it tend to be more effective and look like a legitimate transmission.

Random jammer

→ Random jammer attacks differ from both Constant and deceptive attacks as they Conserve their energy by alternating between jamming and Sleep mode.

→ During the jamming Process the attacking node jams for a Predefined time before turning off its radio and Switching to Sleep mode.

→ After a while it reactivates the jamming Process from Sleep mode and Continually follows that sequence.

Reactive jammer

→ All three previous jamming strategies discussed are active jammers as they attempt to block the Communication Channel, regardless of the traffic Pattern.

→ Reactive jammers function by Continually Sensing the Communication channel to detect when signals are being transmitted on detecting a signal transmission in the Channel, they start to transmit radio signals to cause collision.

Detection metrics for jamming attack.

→ To detect the different form of jamming attack that has been described below

→ These metrics closely monitored and Captured during a normal traffic flow to detect the malicious ~~bio~~ node during a jamming attack.

→ Common these metrics are packet delivery ratio (PDR), packet Sending ratio (PSR), Bad Packet ratio, (BPR), BER, Energy Consumption amount ECA, SNR.

Packet Delivery Ratio (PDR)

→ PDR is the ratio of the number of packets that has been Successfully delivered and acknowledged by the destination node to the number of packets Sent by the transmitting node.

→ Transmitting node only Confirms the Successful delivery of packets upon receiving an ack packet from the destination node.

→ This process involves 4 way handshaking (RTS, CTS, Data, Ack) where PDR is determined by Comparing the RTS/Data packets transmitted with CTS/Ack packet received.

Packet Sending ratio (PSR)

→ PSR is the ratio of the number of packets that has been Sent during a given time to the number of packets intended to be Sent by the transmitting node during that given Period.

→ PSR Can be Used to determine how effective the jamming attack is on a transmitter using Carrier Sensing as its medium access policy.

Bad Packet Ratio (BPR)

→ BPR is the ratio of the number of damaged packets received by a node to the total number of packets received in a given Period.

→ Sensor nodes often determine this by using cyclic redundancy check (CRC) for damaged packets

→ BPR is very effective method to detect different forms of jamming due to ease to calculate.

Bit Error Rate (BER)

→ BER in WSN can be determined by computing the ratio of the number of corrupt bits to the entire bits received during a transmission session by a node.

→ BER can be effective in detecting reactive jamming attacks.

Energy Consumption Amount (ECA)

→ ECA is the measure of the approximate amount of energy consumed by a sensor node over a period of time.

SNR - Signal to Noise ratio.

* SNR can be calculated by finding the ratio of received signal power to received noise power at the node

* It is very effective method to detect jamming attack in the physical layer.

Packet interval arrival time (IAT)

→ Packet IAT is the time that elapse between the receipt of a packet and subsequent packets in WSN

→ The distribution of the packet IAT can be used to determine the probability of occurrence of DoS jamming attacks during transmission signals.

Tampering

→ Tampering another Dos attack in physical layer.
→ By physical access an attacker can extract the information such as cryptographic keys or other data on the node.
→ A compromised node creates which attacker controls by altering or replacing node.
→ Tampering means changing or deleting a resource without authorization.
→ eg. data tampering in web application

Types 1. Parameter tampering 2. Data tampering.

Data tampering

* It is the act of deliberately modifying (destroying manipulating, or editing) data through unauthorized channels.
* Data exist in two states : in Transit or at rest
* In both instances data could be intercepted and tampered.
* Ex, data packets are transmitted unprotected a hacker can intercept the data packet, modify its contents and change its destination address.
* Data at rest a system application can suffer a security breach and unauthorized intruder could deploy malicious node that corrupts the data.

Prevention of data tampering

* Encryption
* Copy on write file systems
* Data integrity using HMACs
* File integrity monitoring (FIM).
* (WORM) Systems Write Once read Many

Encryption for Data at rest and Data in transit.

→ One of the most effective ways to protect data at rest and in transit is encryption.

→ Data encryption is the process of translating data from one form into another that unauthorized users cannot decrypt.

→ Ex. To Protect data at rest, you can encrypt sensitive data prior to storing it.

→ For encrypting data in transit you can use encrypted connections such as SSL, HTTPS, FTPS, etc.

Copy On Write file System:

→ Copy on write often referred to as CoW is a concept used to maintain instant Snapshots are taken. Security teams can detect data tampering by monitoring Snapshots and checking for

→ Copy On Write often referred to as CoW is a Concept used to maintain instant Snapshots on database Servers. It can also helps with data tampering Prevention.

→ Each time database is modified, Snapshots, are taken. Security teams can detect data tampering by monitoring Snapshots and checking for unexpected file system Snapshots

→ Many data base applications and operating systems (such as linux, Unix) come with a built in Snapshot features.

Data Integrity Using HMACs.

→ Hash-based message authentication code is a type of message authentication code (MAC) that consists of a cryptographic hash function and secret cryptographic key.

→ When two or more parties exchange data through Secure file transfer protocol the data is accompanied by HMAC instead of just plain hashes.

→ This technology consists of shared secret key and hash function.

→ A hash is taken of the message and that is then signed by the shared key.

File Integrity monitoring (FIM)

→ File integrity monitoring is a powerful Security technique to Secure business data and IT infrastructure against both known and unknown. threats.

→ FIM is the process of monitoring files to check if any changes have been made.

→ It assesses system files and generates a cryptographic Checksum as a baseline, then the FIM repeatedly recalculates the checksum of the same resources Compare it to the baseline and if it detect changes it also generates a Security alert.

WORM Systems (Write Once read many).

→ Write once read many (WORM) Systems refers to a storage technology where data, Once written, cannot be overwritten or modified.

→ This technology used for archival purpose of large enterprises and government agencies.

Black Hole Attack

→ The black hole attack is one of the well known security threats in wireless mobile adhoc network.

→. Black hole attack occurs Under Dos attack in the network layer of OSI model.

→ In this kind of attack the malicious node forgery other nodes by announcing a shortest false route to the destination.

→. During the data transmission the source node sends the Route Request RREQ message to all the nodes including malicious node.

→. Malicious node may become active by receiving RREQ message and replies using RREP (Route Reply)

→ Normal nodes trust any reply for the requests that they broadcast and black hole node takes the advantage of this and keeps the replying to any request claiming that it has the shortest path to the desired node.

→ Source node believe that reply, because there is no mechanism to verify that request from normal node or from black hole node.

→ This can be classified as Single and Co-operative black hole attacks.

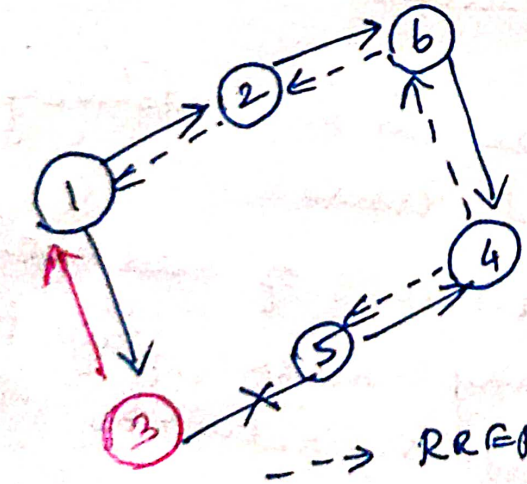
Single black hole attack.

→ In this type of attack the malicious node individually attacks as a black hole node which hysterics into the routes between the Source and the destination.

Co-operative black hole attack.

→ In this type of attack the malicious nodes act in a group.

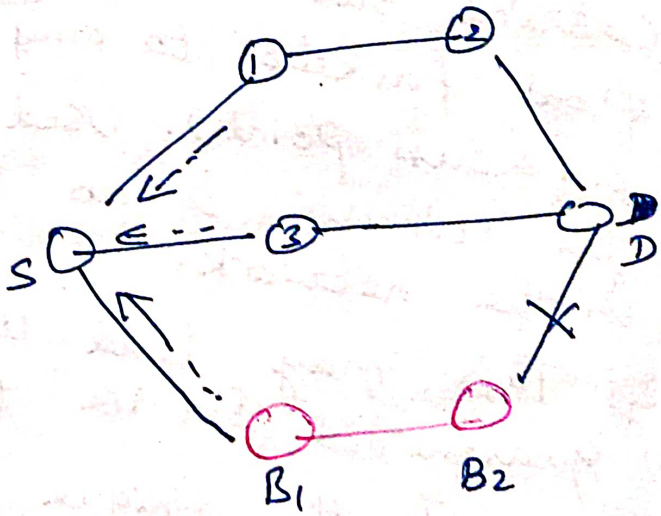
→ Unlike Single black hole attack here the multiple nodes absorb the packets sent for the destination node.



→ RREQ

--> RREP

Single black hole attack



→ Malicious RREP.

--> RREP.

Co-operative black hole attack.

Flooding Attack.

Flood attacks are also known as Denial of Service (DoS) attack. In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic.

→ Denial of Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

Denial of Service.

→ A "denial of Service" or DoS attack is used to tie up a website's resources so that users who need to access the site cannot do so.

→ A denial of Service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource (e.g. an access point). Used in the network so that the resource is no longer available to nodes in the network.

→ This may lead to a failure in the delivery of guaranteed Service to the end users.

→ Due to the unique characteristics of adhoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks.

Key Distribution and Management

Key Management:

Cryptography: It is one of the most common & reliable means to ensure Security & Can be applied to any Communication network.

* In the Parlance of cryptography, the original information to be Smt from One person to another is called plain text.
* The plain text is Converted into Ciphertext by the process of encryption.
* An authentic receiver Can decrypt / decode the Ciphertext back into plain text by the process of decryption.
* The process of encryption and decryption are governed by keys, which are Small amounts of information used by the cryptographic algorithms. When the keys is to be kept Secret to ensure the Security of the System it Es called Secret key.

→ The secure administration of cryptographic keys is Called Key management.

→ The 4 main goals of cryptography are Confidentiality, integrity, authentication & Non-repudiation

→ There are 2 major kinds of Cryptographic algorithm.

1 Symmetric key algorithms, which use the same key for encryption & decryption.

2. Asymmetric Key algorithms, which use two different keys for encryption & decryption.

→ The asymmetric key algorithms are based on some mathematical Principles which make it feasible or impossible to obtain one key from another. therefore one of the keys can be made Public while the others is kept Secret (Private). This is called Public key Cryptography.

Symmetric key algorithm:

* Symmetric key algorithms rely on the Presence of Shared key at the both the Sender & Receiver, which has been exchanged by some Previous arrangement.
* There are 2 kinds of Symmetric key algorithm
  → One Involving block ciphers
  → The Stream ciphers.

* A block cipher is an encryption scheme in which plaintext is broken into fixed length Segments called blocks & blocks are encrypted one at a time.

* The Simplest examples includes Substitution & Transportation.

* In Substitution. each alphabet of plain text is substituted by another in the cipher text & this table mapping of the Original & the Substituted alphabet is available at both the Sender & Receiver.

* A Transposition cipher. permutes the alphabet in the plaintext to produce the cipher text.

Original Alphabet

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Substitution.

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D.

plaintext EVERYDAY CREATES A HISTORY

EVERY DAYCR EATES ATHIST ORY.

Ciphertext IZIVC HECGV IEXIW ELMWX SVC.

(a). illustrates the encyption using Substitution.

Transposition. 1 2 3 4 5

↓

3 5 1 4 2.

plaintext : EVERYDAY CREATES A HISTORY

EVERY DAYCR EATES ATHIST ORY.

Ciphertext : EYERV YRDCA TSEEA ITASH YOR.

Shows a transposition cipher.

→ The block length used 5. A Stream cipher is in effect a block cipher of block length one.

→ One of the simplest stream ciphers is Vernam cipher. which uses a key of same length as plaintext for encryption.

→ for example If the plaintext is the binary string 10010100 & key is 01011001 then the encrypted string is given by the XOR of the plaintext & key to be 11001101.

→ The plain text is again recovered by XORing the cipher text with the same key.

Asymmetric Algorithm:

→ Asymmetric key (or public key) algorithms use different keys at the sender end & receiver ends for encryption & decryption,

→ Let the encryption process be represented by a function E, & decryption by D.

→ Then plaintext 'm' is transformed into the cipher text 'c' as $c = E(m)$ The receiver then decodes C by applying D. Hence D is such that $m = D(C) = D(E(m))$.

→ When this asymmetric key concept is used in public key algorithms, the key E is made public, while D is made private, known only to the intended receiver.

→ RSA algorithm is the best example of public key Cryptography.

Key Management Approches

→ The primary goal of key management is to share a secret (some information) among a specified set of participants.

→ The main approaches to key management are Key Predistribution, Key transport, Key arbitration and Key agreement.

Key Predistribution:

→ Key Predistribution, as the name suggests, involves distributing key to all interested parties before the start of communication.

→ This method involves much less communication & computation, but all participants must be known a priori, during the initial configuration.

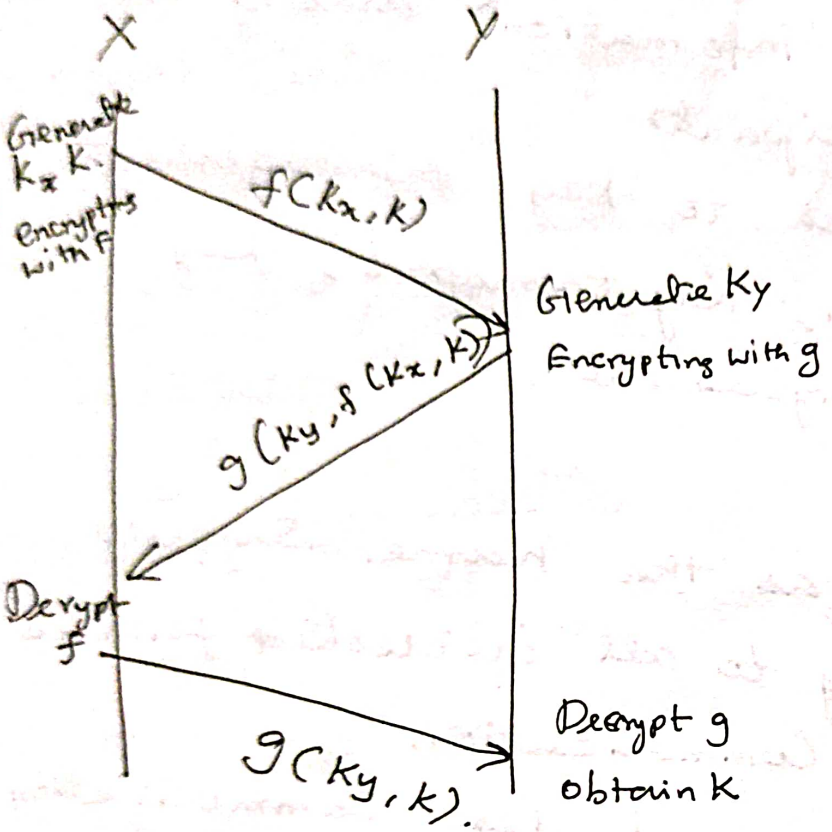
→ Once deployed there is no mechanism to include new members in the group or to change the key.

Key Transport

* In key transport systems, one of the communicating entities generates keys & transports them to the other members.

* The simplest scheme assumes that a shared key already exists among the participating members. This shared key is used to encrypt a new key and transmitted to all corresponding nodes

* Only those nodes which have the Priori Shared key can decrypt it.
* This is called the key Encrypting key (KEK) method.



Key Arbitration.

* Key arbitration Schemes Use a Central arbitrator to Create & distribute keys among all participants. hence they are a class of key transport Schemes.
* In adhoc wireless networks, the Problem with implementation of arbitrated Protocol is that the arbitrator has to be powered on at all times to be accessible to all nodes.
* This leads to a Power drain on that particular node.

* Key arbitration schemes use a Central arbitrator to Create & distribute Keys among all participan

Key agreement

* Key agreement Protocols are used to establish a secure Content over which a Session Can be run starting with many parties who wish to Communicate & an insecure Channel.
* In group key agreement schemes, each participant Contributes a part to the secret key.

Secure Routing.

Requirement of Secure routing Protocol for adhoc wireless networks.

Detection of malicious node:

* A secure routing Protocol Should be able to detect the presence of malicious nodes in the network and Should avoid participation of such node.
* Routing Protocol Should choose paths that do not include such node.

Guarantee of Correct route discovery.

* If a route between the source and destination nodes exist the routing Protocol Should be able to find the route and Should also ensure the Correctness of the Selected route.

Confidentiality of network topology:

→ An information disclosure attack may lead to the discovery of the network topology by the malicious nodes. Once the network topology is known the attacker may try to study the traffic pattern in the network.

Stability against attacks:

→ The routing Protocol must be self stable.

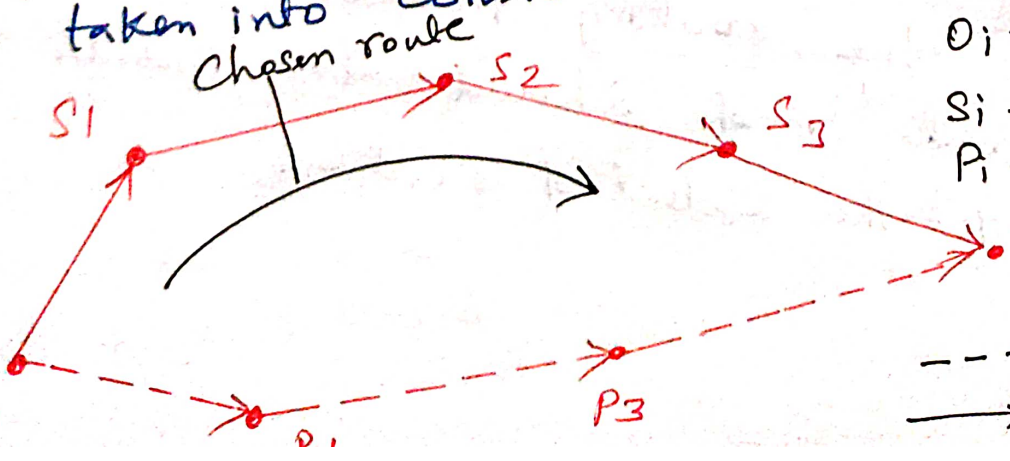
→ It must be able to revert to its normal operating state within a finite amount of time after a passive or an active attack.

Security Aware Adhoc Routing Protocol.

* This routing protocol uses security as one of the key metrics in path finding.

* In adhoc wireless networks, communication between end nodes through possibly multiple intermediate nodes is based on the fact that the two end nodes trust the intermediate nodes.

* SAR defines level of trust as a metric for routing & as one of the attributes for security to be taken into consideration while routing.



* Two path exist between the two officers O_1 and O_2 who want to communicate with each other. One of these paths is a shorter path which runs through Private nodes whose trust levels are very low.
* Hence the Protocol choose a longer but Secure path which passes through other secure nodes.
* SAR Protocol can be explained using any one of the traditional routing Protocols.
* In the AODV Protocol, the source node broadcaste a Route Request packet to its neighbours

* Two path exist between the two officers O_1 and O_2 who want to communicate with each other. One of these path is a shorter path which runs through Private nodes whose trust levels are very low.
* Hence the Protocol choose a longer but secure path which passes through other

* Each packet is associated with a security level which is determined by a number calculation method.
* Each intermediate node is also associated with certain level of security.
* If the node's security level is less than that of packet the Route request is simply discarded.
* If it is greater than node is considered to be secure node and is permitted to forward the packet in addition to being able to view the packet.

→ If the security levels of intermediate node and received packets are equal the intermediate node will not be able to view the packet it just forward the packet further.

Sensor Protocols for Information Via Negotiation. (SPINS)

* SPINS Consists of a Suite of Security Protocols that are optimized for highly resource Constrained Sensor networks.
* SPINS Consists of Two main modules.
  1. Sensor Network Encryption Protocol (SNEP).
  2. Micro Version of timed, efficient, streaming loss tolerant authentication Protocol (μTESLA).
* SNEP Provides data authentication, Protection from attacks and Semantic Security.
* Semantic Security means that an adversary Cannot get any idea about the plain text even by seeing multiple encrypted versions of the same plaintext.
* plain text means that Original information to be Sent from one Person to another.
* Encryption of plaintext Uses a shared Counter (shared between Sender and receiver) hence the Same message is encrypted differently at different instance in time.

* Message integrity and Confidentiality are maintained Using a message authentication Code (MAC).
* This is similar to checksum derived by applying an authentication scheme with a Secret shared key to the message.
* The message can be decrypted only if the same shared key is present. The message also carries the Counter Value at the instance of transmission, to & Protect against replay attacks.
* μTESLA ensures an authenticated broadcast, that is nodes which receive a packet can be assured of its 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.
* All nodes have an initial key K_0, which is some key in the key chain. The relationship between Keys Proceeds as $K_0 = F(K_1)$, $K_1 = F(K_2)$ and in general $K_i = F(K_{i+1})$. Given $K_0, K_1, \ldots K_i$ it is not possible to Compute K_{i+1}.
* The key to be used changes periodically, and Since 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 time instant

Reliability Requirements in Sensor Network.

Single Packet Versus Block Versus Stream Delivery:

* The cases of delivering only a single packet on the one hand and of delivering a number or even an infinite stream of packet on the other hand differ substantially in the protocol usable in either case.
* In the single packet delivery problem, a single packet must be reliably transported between two nodes
* It may be argued that such a requirement will not occur in dense wireless sensor networks where many nodes observe the same phenomenon and report highly correlated data.
* However there are arguements against this claim. The first one is that not all sensor networks will be dense

Sink to Sensors Versus Sensors to Sink Versus Local Sensor to Sensor.

* It can be assumed that most communications in sensor networks are not between arbitrary peer nodes but information flows either from sensor nodes toward a single or a few sink/ gateway nodes or in the opposite direction, from sinks to sensors.

UNIT-V

Sensor Network Platforms and Tools.

Sensor Node hardware:

→ A Sensor node is also called as Mote (Called in North America). It is a node in a wireless Sensor network that is capable of performing some Processing, gathering Sensors information and Communication with other Connected nodes in network

→ So one of the major challenges in a wireless Sensor network is to ~~be~~ Produce how lost and tiny Sensor nodes.

→ Sensor node hardware can be granted into 3 Categories.

(i) Augmented general purposed Computers.

(ii) Dedicated Embedded Sensor nodes.

(iii) System On chip (SOC).

(i) Augmented general purposed Computers:

* These are the node which is in the general purpose Computers which moderately deals with the real time constraints.

* The Most Common examples are custom designed PCs and various personal digital assistant (PDA).

* These nodes typically run off the Self Operating Systems such as WinCE, Linux, or real time operating systems.

(ii) Dedicated Embedded Sensor nodes:

* There are the Sensors which are used in the Embedded and real time systems. It mainly depends with the system operating in a real time Constraint.

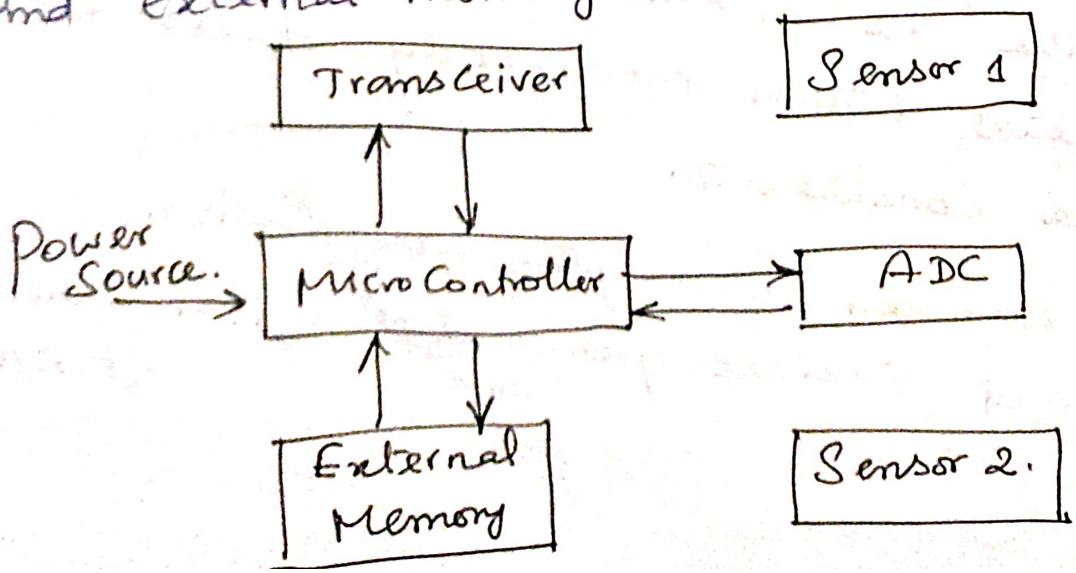
* Examples include the Berkeley, Mote family Ember nodes and MITμAMP.

(iii) System On chip (SoC) nodes:

* These are the Sensors which are very tiny and very flexible to use. It is also used in a real time constraints. Examples of SoC hardware includes Smart dust, the BMRC Picoradio node and the PASTA node.

Examples of Sensor node hardware.

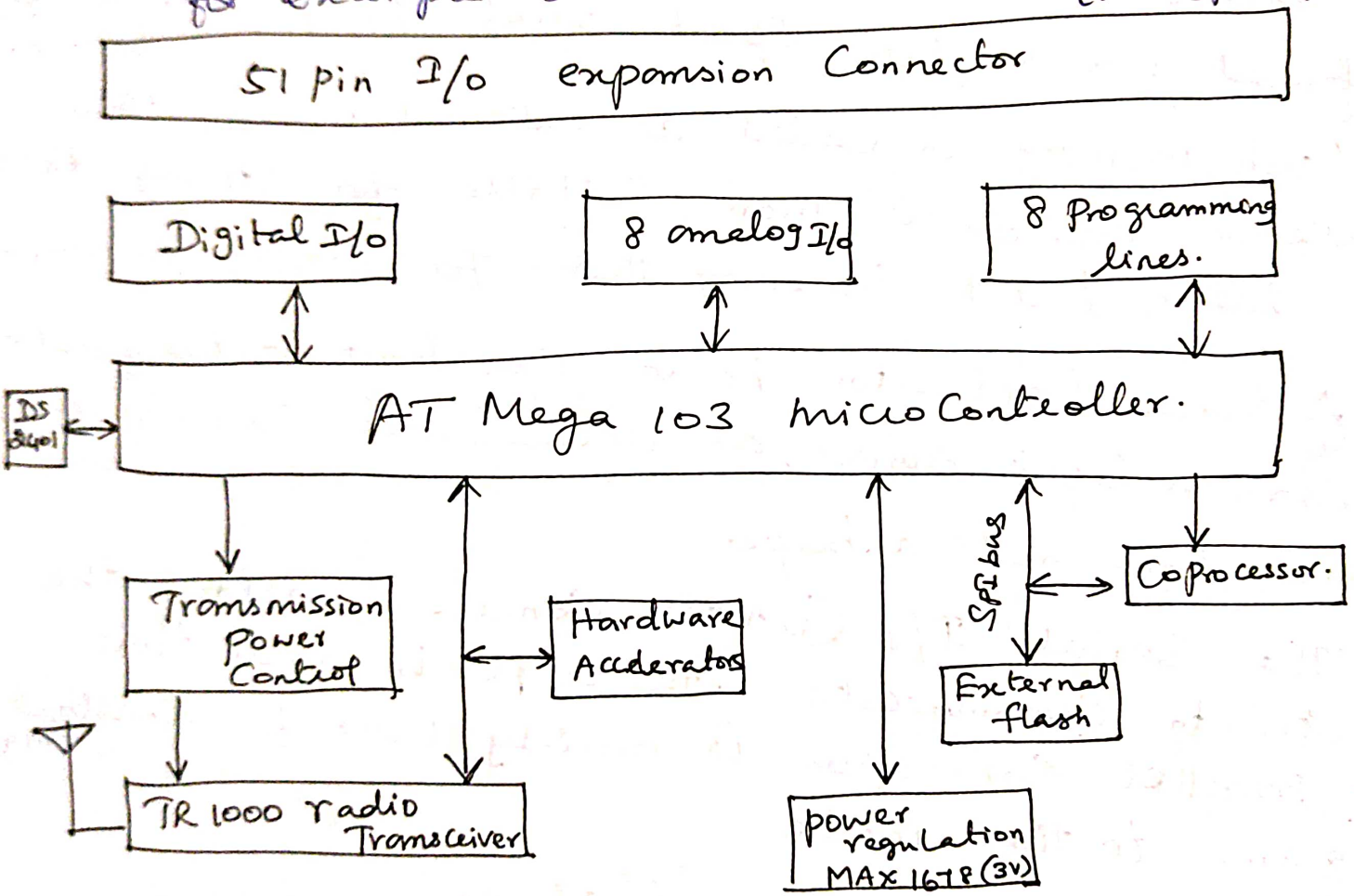
A typically Sensing device with micro Controller, transceiver and external memory.



Berkeley Motes.

* A Berkeley mote is a wireless sensor module manufactured by Berkeley, Typically a sensor node Composed of Sensing Capabilities, Communication radi Computation Unit and a power source.

* The Berkeley motes are a family of embedded Sensor nodes sharing roughly the same architecture that it have for example consider MICA mote a two CPU Design.



MICA mote architecture.

→ The main microcontroller (MCU) Atmel AT mega 103L takes care of regular Processing. A Separate and much less Capable Coprocessor is active when the MCU is being reprogrammed.

→ The AT Mega 103L micro Controller has integrated the 512 KB flash memory with the 4 KB of data Memory.

→ Using these small memory sizes, writing software for nodes is challenging. Due to small memory size, the programmers should be relieved from optimizing code at assembly level to keep code foot print in small amount.

→ In MICA mote have a separate 512 KB flash memory unit it can hold data. The connection between the microcontroller and this flash memory is performed via a low speed serial peripheral interface protocol

→ Flash memory is called as external memory. The external memory is more suitable for storing data for later batch processing than for storing programs.

→ A sensor/actuator board can host a temperature sensor, a light sensor, an accelerometer, a magneto meter a microphone and a beeper.

→ The serial I/O (UART) connection allows the mote to communicate with a PC in real time. The parallel connection is mainly used for downloading programs to the mote.

Node level Software platforms:

Most design methodologies for sensor network software are node centric, it means programmers think in terms of how a node should behave in the environment.

* A node level platform also a node centric Operating system it provides hardware and networking abstraction of a sensor node to Programmers.
* A Typical Operating System abstract the hardware platform by Poviding a set of Services for application The Services are as follows.
  * File management
  * Memory allocation
  * Task Scheduling
  * Peripheral device drivers.
  * Networking.

Examples of Node - Level Programming:

→ Tiny os and Tiny GIALs are two examples of node level Programming tools. In addition two those two operating System mate is used in Berkeley mote It is a act virtual machine for Berkeley mote.

→ polling Sensors and accessing internal states are common operations in all Sensor network application

Operating Systems TINY OS:

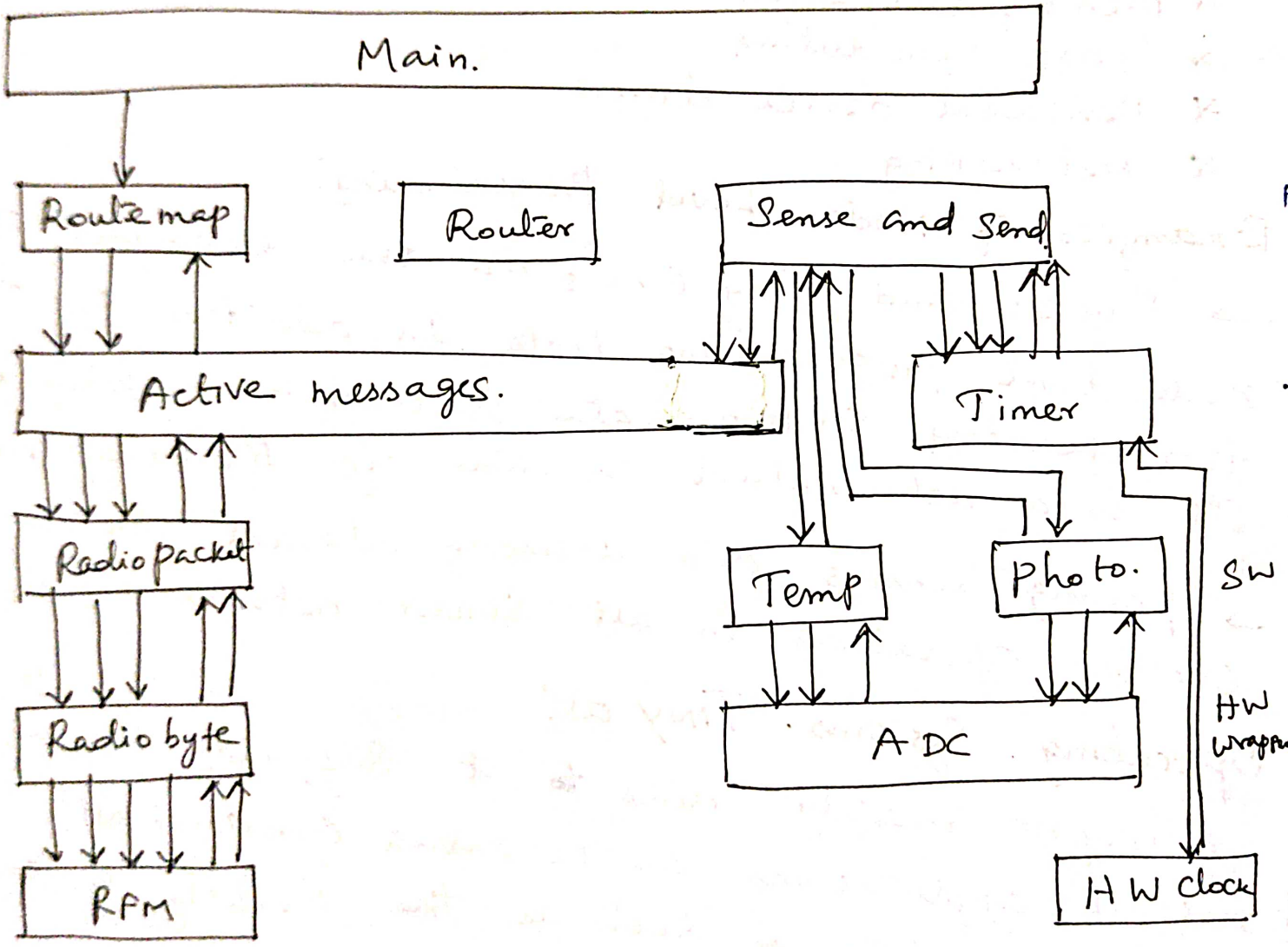
→ Tiny os mainly aims at Supporting Sensor network applications on resources constrained hardware platforms such as the Berkeley motes.

→ To make ensure that an application code has an extremely small foot print, the Tiny os choose to have no file System.

→ Tiny os supports only static memory allocation and its implements a simple task mode.

→ Tiny os organizes components into layers. The lower layer is closer to the hardware and higher layer is closer to the application.

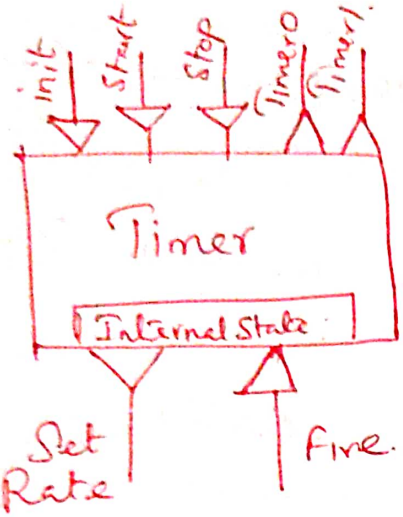
Tiny os Application Example:



Field monitor application for Sensing and Sending measurements.

Timer Component.

→ Timer Component is designed to work with a clock it is a software wrapper around a hardware clock that generates periodic interrupts.



→ An arrow head pointing into the Component is a method of how one Component can call another Component

→. An arrow head pointing outward it means that Components require another layer Components. to provide services or information.

→ A Program execution in Tiny os can be performed in two Contexts Such as
1. Tasks 2. Events.

Imperative Language : nesC.

* The nesc is an extension of C to Support and reflect the design of Tiny OS. V1.0 and above Version.
* It provides a Set of language Constructs and restrictions to implement Tiny os Components and applications.

Component Interface.

In nesc Component having two things first is the Component interface Specification. and Second is the Component implement Specification.

→ Component interface of a nesC are classified into types.

1. Provides interface 2. Uses interfaces.

Provides interface is a set of method calls exposed
→ to the upper layers.

→ A uses interfaces is a set of method calls hiding the lower layer components.

→ The nesC having the two different method call mechanism for interface

* Event calls * Command calls.

Component Implementation:

There are two types of components. in nesC depending on how they are implemented

1. Modules 2. Configuration.

Types of Code in nesC

In nesC code can be classified into two types.

1. Asynchronous code (AC): Code that is reachable from atleast one interrupt handler.

2. Synchronous code SC: code that is only reachable from tasks.

→

Programming challenges:

→ Sensor network can be Programmed in many ways Programming Sensor network is not a easy task.

→ Traditional Programming technologies rely on Operating Systems and it will Provide abstraction for Processing, networking I/O and User interaction hardware.

→ If we apply traditional Programming to Sensor network, the application Programmers need to explicitly ideal with many things

(i) Message Passing (ii) Event Synchronization.
(iii) Interrupt handling (iv) Sensor reading.

→ As a result of dealing the above things an application is typically implemented as a finite state machine (FSM).

→ Finite State machine covers all extreme cases such as unreliable Communication Channels, long delays, irregular arrival of messages simultaneous events and so on.

→ Micro kernel technologies modularize the operating system so that only the necessary parts are deployed with the application.

→ Schkduling algorithms Optimize Code at the assembly level technique will work for small stand alone embedded systems but it is not suitable for the Programming of Sensor network.

(i) Sensor networks are large scale distributed systems.
(ii) Distributed Algorithms are hard to implement.
(iii) Infrastructure Support only limited power constraints. memory Bandwidth resources.
(iv) Sensor nodes deeply embedded into the physical world.
(v) Sensor network must be able to respond to multiple Concurrent system.
(vi) In distributed nodes the global Properties are derivable from Program execution to all nodes.

→ A design methodology of Sensor networks implies a Conceptual model for Programmers, with associated techniques for Problem decomposition for the Software designers.

→ If the network is used for monitoring a Small Set of phenomena and the Sensor nodes are organized in a Simple Star topology.
Tree structure is suitable for following reasons.
(i) If the network is used for monitoring a large area from a single access point.
(ii) If User queries can be decoupled into aggregation of Sensor reading from a subset of Sensor nodes.

Node level Simulators:

→ Node level design methodologies are usually associated with Simulators that Simulate the behaviour of a Sensor network on a Peer-node basis.

→ Simulation helps the designers to quickly study the Performance of Potential algorithm without implementing it on actual hardware.

Components of Node level Simulator:

Node level Simulator is having the following set of components.

1. Sensor node model
2. Communication model
3. physical environment model
4. Statistic and visualization.

Sensor Node Model

* A node in a Simulator act as a three format such as Software execution platform, a Sensor host, communication terminal.
* To focus on the application level Code, a node model provides or Simulates a Communication Protocol Stack, Sensor behaviors and Operating System Services.
* If the nodes are mobile, then the Positions and motion Properties of the nodes need to be modeled.

Communication Model.

→ Depending on the details of modeling, Communication may be captured at different layers. The Communication media at the physical layer is Simulating the RF Probagation delay and collision of Simultaneous transmission.

physical Environment Model:

The environment Can be also be Simulated at Various levels of detail. for example, a moving object in the physical world may be abstracted into a Point Signal Source.

→ If the Sensor network is passive, it does not impact the behaviour of the environment. Then the enviroment Can be Simulated Separately.

Statistics and visualization:

The Simulation result will be used to Perform analy The goal of a Simulation is typically to derive global Propertise from the execution of individual nods.

→ An ideal visualization tool should allow Users to easily observe the following things

1. The Spatial distribution.
2. Mobility of the nodes.
3. Connectivity among nodes.
4. Link qualities.
5. End to End Communication routes and delays.
6. Sensor node states.

→. A Sensor network Simulator Simulates the behavior of a Subset of the Sensor nodes with respect to time.

Types of Execution Models:

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.

Cycle driven Simulation:

→ A cycle driven Simulation discretizes the continuous notion of real time into ticks and Simulates the System behavior at these ticks.

→ At each tick, the physical phenomena are first Simulated and all nodes are checked to see if they have anything to Sense, Process or Communicate.

Discrete event Simulation:

→ In a discrete event, Simulator assumes the time is continuous and an event may occur at any time An event is having two things one is a value and another is a time stamp.

→ The time stamp of an event indicates that When the event is supposed to be handled.

Types of Components

There are two types of Components available.

1. Causal Component
2. Non Causal Component.

→ Causal Component means the output event is computed from an input event, then the time stamp of the output event should not be earlier of the input event.

→ Non Causal Component means it require the Simulators to be able to roll back in time and worse it may not define a deterministic behaviour of a system.

The NS-2 Simulator.

The Simulator ns-2 is an Open Souce network Simulator that was designed for wired, IP network, wireless / mobile networks and Sensor networks.

→ Originally this simulator is designed for wired, IP networks but now a days it will be used in some other areas

→ The original ns-2 only supports logical address for each node, the wireless / mobile extension of it introduces the notion of node locations and a simple wireless channel model.

→ This also supports hybrid Simulation, it means some real sensor nodes running in real application can be executed together with a simulation.

→ The NRL Sensor network extension provides a flexible way of modeling physical phenomena in a discrete event simulator.

Advantages:

1. The ns-2 has rich libraries of Protocols for all network layers and has many routing mechanisms.
2. These Protocols are modeled in fair and resemble the actual Protocol implementations.

Examples:
1. TCP : reno, tahoe, Vegas and SACK implementation.
2. MAC : 802.3, 802.11 and TDMA.

The Simulator TOSSIM (Tiny Os Simulator).

→ TOSSIM is a dedicated Simulator for Tiny OS applications running on one or more Berkeley motes.

→ The main aim of designing Tossim is to make Scalable to a network of potentially thousands of nodes and able to use the actual Software code in the Simulation.

→ To achieve these goals, Tossim takes a Cross Compilation approach that compiles the nesC Source code into Components in the Simulation. The event driven Execution model of Tiny OS greatly Simplifies the design of Tossim.

→ Tossim has a visualization package Called Tiny Viz, which is a Java application that can Connect to TOSSIM Simulations.

→ TinyViz also provides mechanism to Control a running Simulation. Tiny Viz is designed as a Communication Service that interacts with the Tossim event queue.

Programming Beyond Individual Nodes:

State Centric Programming

→ In all the Sensor network application the system consists of many states of different process.

→ To Programming these states is not an easy thing because some of these states may be represented with a small number of nodes. and evolve over time, as in the target tracking problem and distinct in motion of the object etc.

→ To control these process the programming of all the states should be combined and form a large and spatially distributed number of nodes.

→ A distinctive Property of physical states, such as location, shape and motion of object is their continuity in space and time.

→ This gives the basis for most signal and information processing algorithm provide abstractions for state update such as the state update and status is

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

$$y_k = g(x_k, u_k).$$

x - is the state of a system.

u - are the inputs. , y - are the outputs.

k - is the integer update index over space and time.

→ The above formula gives the broad enough to capture a wide variety of algorithm. in Sensor fusion., Signal Processing and control. Some of algorithms also explain such functions are.

(i) Kalman filtering
(ii) Bayesian Estimation
(iii) System identification.
(iv) Feedback Control laws.
(v) Finite State automate.

Collaboration Groups:

→ A Collaboration group is a Set of Entities that Contributes to a State update..

→ These Entities Can be physical Sensor nodes, or they Can be more abstract System Component such as Virtual Sensors. They are reffered to as agents.

→ A Collaboration group provides two abstraction
(i) its scope to encapsulate network topologies
(ii) its structure to encapsulate Communicatio protocols.

Scope: The scope of a group defines the membership of the nodes with respect to the group. The group also includes both physical Sensor nodes and Virtual Sensor if that may not be attached to any physical Sensor.

Structure:

→ The structure of a group defines the 'roles' each member plays in the group. and thus the flow of data.

→ Also structure ensure (i) are all members in the group equal peers (ii) Is there a leader member in the group that Consumer data (iii) Do members in the group form a tree with parent and children relation.

(i) Geographically Constrained group:

→ A geographically Constrained group (GCG) consis members within a pre specified geographical extent. of It may propagate only to a limited extent in a Environment.

→ There are many ways to specify the geographic shape such as (i) circles (ii) polygons, (iii) End their Unions.

N-Hop Neighborhood group:

This is more important that the geographical Constrained group and it hop counts are useful to Constrain group membership. It has an anchor node which defines all nodes within n Communication hops are members of the group.

(iii) Publish / Subscribe Group:

A group may also be defined more dynamically by all entities that can provide certain data or Service or that can satisfy certain predicates over their Observation or internal states.

COOJA - WSN Simulators

→ Due to the ability to increase the real WSN Prototyping, the cross level Simulators like COOJA have become an important class of Simulators

→ This kind of Simulators operates at three abstraction levels.

① The network level
② Operating System level
③ Machine code instruction set level

→ Although these Simulators are open source, flexible and extensible, at all levels, The test interface, the external connection at a physical level and the direct interaction with the Process Control via the WSN are very poor.

→ Cooja Simulator is specifically designed to Simulate Wireless Sensor network. It is most widely used to Simulate IoT Network applications

→ COOJA Simulator is a cross layer java-based Wireless Sensor network Simulator distributed with Contiki.

→ It allows the Simulation of different levels from physical to application layer and also allows the emulation of the hardware of a set of Sensor nodes.

→ Contiki is an Operating System with a focus on low power IoT devices.

→ COOJA is the Contiki network Simulator. COOJA allows the large and small networks of Contiki motes to be Simulated.

Characteristics of COOJA Simulator

→ Contiki offers a java based Simulator called as COOJA which is used to Simulate Wireless Sensors.

→ It is more flexible so that many parts of the Simulator is replaceable and extendable.

→ The parts of the Simulator like Simulated mode hardware, plug ins and radio medium can be replaceable.