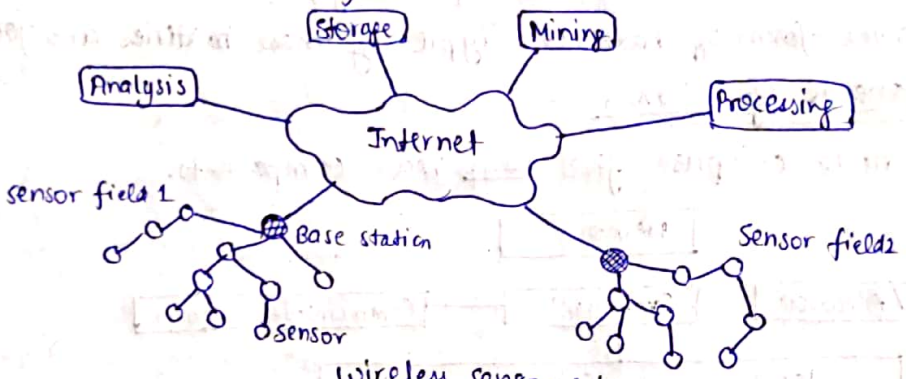
Ad Hoc and Sensor Networks

Unit - III

Wireless Sensor Networks

* A sensor n/w is composed of a large no. of sensor nodes, which are densely deployed either inside the phenomenon, they are observing, or very close to it. Sensor n/w may consist of different types of sensors such as seismic, low sampling rate magnetic, thermal, visual, infrared, acoustic and radar.



Wireless sensor N/w

* The failure of sensor nodes should not affect the overall task of the sensor n/w. This is the reliability or fault tolerance issue. Fault tolerance is the ability to sustain sensor n/w functionalities without any interruption due to sensor node failures.

* **Wireless Sensor N/w (WSN) & Components of WSN**

- A WSN consists of distributed radio nodes to monitor physical or environmental cond^{n}s, such as temp., sound, pressure, etc. & to transmit the data to main location.
- WSNs have been developed for machinery cond^n-based maintenance (CBM) as they offer cost savings & enable new-func^{n}alities. Inaccessible loc^{n}s, rotating machinery, hazardous or restricted areas, and mobile assets can ~~now~~ be reached with WSNs.
- A WSN consists of following components:
  - → Many different sensors : sensors capture measured variable in a data acquisition n/w quantitatively.
  - → Wireless Sensor Nodes or Radio Nodes: Sensor nodes serve to receive the sensor data from sensors and sends them to a wireless access point.
  - → WLAN Access Point (Wireless Access Point) : It receives the sensor data in a WSN, which are transferred to the evaluation S/W.
  - → Evaluation S/W: For data analysis the WLAN access point is connected to an evaluation unit which is usually a PC or laptop that can use a specific evaluation S/W, with which the sensor data is analyzed simultaneously.

* **Components of a Wireless Sensor Node**

- The central component of a WSN is the sensor node. These tiny devices consist of the following main components:
  - → Microcontroller : This is a computer-on-a-chip which is very tiny in size although capable of doing powerful tasks including controlling the func^{n}s of other devices connected to it. In general, it consists of microprocessor, a RAM memory &

→ For actual communication, both a transmitter and receiver are required in a sensor node. The essential task is to convert a bit stream coming from microcontroller and convert them to f from radio waves. For this, low-cost transceivers are commercially available.

(iv) Sensors and Actuators

→ The actual interface to the physical world; devices that can observe or ctrl physical parameters of the environment.

→ Sensors can be roughly categorized in three categories:

ⓐ Passive, omnidirectional sensors ⓑ Passive, narrow-beam sensors

ⓒ Active sensors

(v) Power Supply

→ Storing power is conventially done using batteries.

* Salient Features of Sensor N/ws

(i) Collaborative objective

- since a sensor n/w is deployed for achieving a certain system-wide goal, nodes collaborate instead of competing with each other. The nodes collaborate to optimise a system-wide objective.

(ii) Network Scale

- The basic premise being that because of redudancy, a n/w consisting of a large no. of sensor nodes is more robust to node failure than a n/w consisting of a fewer no. of nodes. High node density makes the system more robust to routing f node failures, since each node has several alternative paths to reach the sink.

(iii) Many-to-One Communication Paradigm

- Data flows in two directions in the n/w; upstream (many-to-one) in which sensor nodes send their measurements to the sink and downstream (one-to-many) in which sink send queries or code-updates to the sensor nodes. However, the majority of traffic flows in upstream, i.e., sensor nodes to sink.

(iv) Nodes with limited Capabilities

- A sensor node is limited in energy f usually cannot be replenished, slower computing speeds, small memory, low data rates f limited communication range.

(v) Clustering for Scalability

- Organize the n/w into smaller sub-n/ws called clusters. Each cluster can be then managed autonomously. Such a hierarchy results in lower routing overheads f could also be used for in-n/w aggregation of the measured data.

(vi) Node Deployment vs Placement

- Depending on the appln, sensor nodes could either be deployed randomly over the area of interest or the nodes could be placed, deterministically at specified locations.

(vii) Node Mobility & Dynamic Topology

- In many cases, sensor nodes have little or no mobility. When the nodes are mobile, topology of n/w changes, and it may be necessary to update the routing info. of the nodes. Sensor nodes often have a dynamic topology due to this mobility which has stronger impact than other factors.

* Applications

- Habitat Monitoring
- Environmental Monitoring
- Drinking water quality
- Soil Moisture Monitoring
- A Remote Ecological Micro-Sensor N/w
- Environmental Observation & Forecasting System
- Disaster Relief Management
- Health Care Monitoring
- Building, Bridge & Structural Monitoring

* Issues that makes WSN as a distinct category of Adhoc WSN

(i) Mobility of nodes

- Mobility of nodes is not a mandatory requirement in sensor n/ws. ~~In~~ general
- In general, sensor n/ws need not in all cases be designed to support mobility of sensor nodes.

(ii) Size of the n/w

- The no. of nodes in sensor n/w can be much larger than that in a typical adhoc wireless n/w.

(iii) Density of Deployment

- The density of nodes in a sensor n/w varies with the domain of appln.

(iv) Power Constraints

- The power constraints in sensor n/w as much more stringent than those in adhoc wireless n/w.

(v) Data / Information Fusion

- Data fusion refers to aggregation of multiple pkts into one before relaying it.
- Data fusion mainly aims at reducing bandwidth consumed by redundant headers of the pkts & reducing the media access delay involved in transmitting multiple pkts.

(vi) Traffic Distribution

- The communication traffic pattern varies with domain of appln in sensor n/ws.
- This kind of traffic requires low bandwidth
- Adhoc wireless n/ws generally carry user traffic such as digitized & pktized voice stream or data traffic, which demands high bandwidth.

* Issues & Challenges in Designing a Sensor N/w

(i) Energy

- Sensor nodes operate with limited ~~power supply~~ energy budgets. They are

powered through batteries, which must be either replaced or recharged when depleted. For some nodes, either option is appropriate.

(ii) Self-Management

- Sensor nodes must be self-managing in that they configure themselves, operate & collaborate with other nodes, and adapt to failures, changes in the environment, & changes in the environment stimuli without human intervention

(iii) Wireless networking

- The reliance on wireless n/ws & communications poses a number of challenges to a sensor n/w designer. An increasing distance b/w a sensor node & a base station rapidly increase the required transmission power. Multi-hop communication requires that nodes in a n/w cooperate with each other to identify efficient routes & to serve as relays. During downtimes, the server nodes can't receive msgs from its neighbours nor can it serve in a relay for other sensors.

(iv) Decentralized Management

- The large scale & energy constraints of many WSNs make it infeasible to rely on centralized algorithms to implement n/w management sol'ns. Nodes must collaborate with their neighbours to make localized decisions, i.e., without global knowledge. As a consequence, the results to these decentralized (or distributed) algorithms will not be optimal, but they may be more energy-efficient than centralized sol'ns.

(v) Design Constraints

- The need for small form factor and low energy consumption also prohibits the integration of many desirable components, such as GPS receivers. These constraints and requirements also impact the s/w design at various levels. The lack of advanced h/w features facilitates the design of small & efficient OS. Many s/w architectures and soln must be designed to operate efficiently on very resource-constrained h/w.

(vi) Security

- Many wireless sensor n/ws collect sensitive info. The remote and unattended operation of sensor nodes increase their exposure to malicious intrusion & attacks. While there are numerous techniques and solutions for distributed systems that prevent attacks or contain the extent and damage of such attacks, many of these incur significant computational, communication and storage requirements, which often cannot be satisfied by resource-constrained sensor nodes. As a consequence, sensor n/ws require new sol'ns for key establishment and distribution, node-authentication & secrecy.

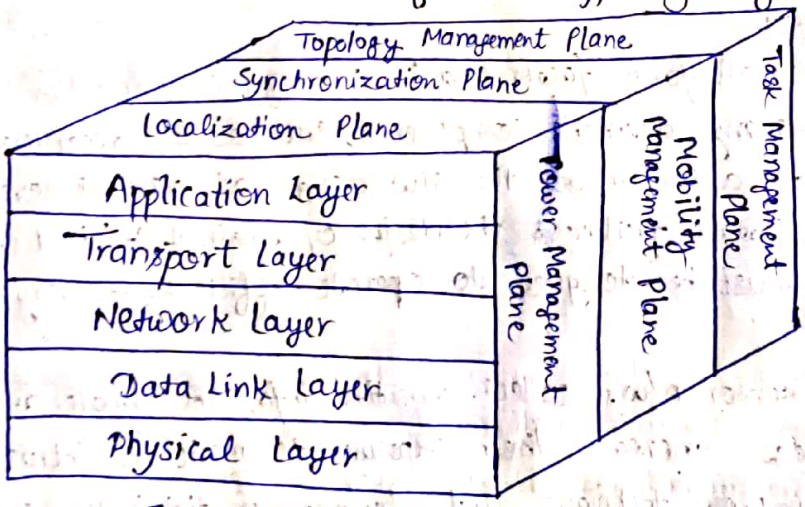
* Comparison with Adhoc wireless n/ws of WSN & Traditional N/Ws

Traditional N/Ws	WSNs
General-purpose design; serving many appl^{n}s	Single-purpose design; serving one specific appl^n
Typical primary design concerns are n/w performance & latencies; energy is not a primary concern	Energy is the main constraint in the design of all node & n/w components
N/Ws are designed & engineered acc^n to plans	Deployment, n/w structure, & resource use are often adhoc (without planning)
Devices & n/ws operate in a controlled & mild environment	Sensor n/ws often operate in environments with harsh cond^{n}s
Maintenance & repair are common & n/ws are typically easy to access	Physical access to sensor nodes is often difficult or even impossible
Component failure is addressed through maintenance & repair	Component failure is expected & addressed in the design of the n/w
Obtaining global n/w knowledge is typically feasible & centralized management is possible	Most decisions are made localized without the support of a central manager

* Sensor Network Architecture

– Layered N/w Architecture

→ WSN nodes are typically low-power modules, with limited CPU & memory, & the appln requirements & n/w architecture of WSNs differs greatly



Sensor N/w Protocol Stack

– Physical Layer

→ The main task of the physical layer is modulation & demodulation of data. Other roles include data encryption, frequency selection & signal detection among others.

→ The major design requirements of a WSN physical layer pertain to minimization of both the cost and power utilization of the sensor.

– Data Link Layer

→ The data link layer is responsible for the multiplexing of data streams, data-frame detection, and medium access & error ctrl. It ensures reliable

point-to-point and point-to-multipoint connections in a communication n/w.

→ The MAC protocol in a wireless multi-hop self-organizing sensor n/w must achieve two goals. The first goal is creation of the n/w infrastructure. The second objective is to fairly & efficiently share communication resources b/w sensor nodes.

→ MAC protocol must certainly support the operation of power saving modes for the sensor node. Another important func^n of data link layer is error ctrl of transmission.

→ Two important modes of error ctrl in communication n/ws are forward error correction (FEC) and automatic repeat request (ARQ), & hybrid ARQ.

- Network layer

→ The networking layer of sensor n/ws is usually designed acc^n to following principles:

Power efficiency is always an important consideration
Sensor n/ws are mostly data-centric
In addition to routing, relay nodes can aggregate the data from multiple neighbours through local processing
Due to large no. of nodes in WSN, unique IDs for each node may not be provided, the nodes may need to be addressed based on their data or location.

- Transport Layer

→ The transport layer is especially needed when the n/w is planned to be accessed through Internet or other external n/ws, TCP with its current transmission window mechanisms, does not address the unique challenges posed by WSN environments.

→ For communication inside a WSN, transport layer protocols are required for two main functionalities: reliability & congestion ctrl. Localized reliability mechanisms are necessary.

→ Transport layer aims to exploit the collaborative capabilities of the sensor nodes & shift the intelligence to the sink rather than sensor nodes.

- Application Layer

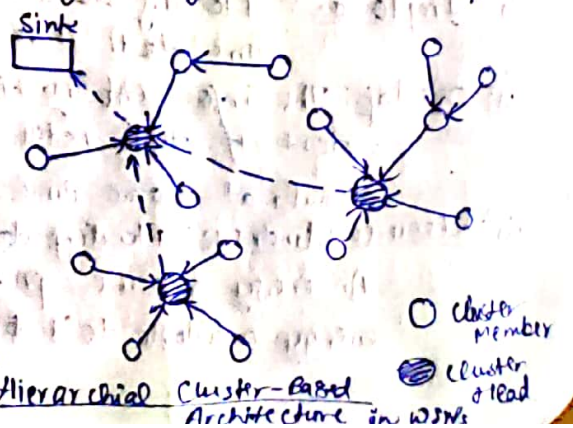
→ The appl^n layer includes the main appl^n as well as several management func^{n}alities. In addition to appl^n axle that is specific for each appl^n, query processing & n/w management func^{n}alities also reside at this layer.

→ By removing the boundaries b/w layers as well as the associated interfaces, increased efficiency in code space & operating overhead can be achieved.

→ A clustered architecture organizes the sensor nodes into clusters, each governed by cluster-head. The nodes in each cluster are involved in msg exchanges with their respective cluster-heads, and these heads send msgs to a BS, which is usually an access point connected to a wired n/w.

→ Clustered architecture is specially useful for sensor n/ws because of its inherent suitability for data fusion.

→ Sensor n/ws should be self-organizing, hence the cluster formation & election of cluster-heads



Hierarchical Cluster-Based Architecture in WSNs

must be an autonomous, distribute process. This is achieved through n/w layer protocols such as the low-energy adaptive clustering hierarchy (LEACH).

→ The LEACH protocol aims to minimize energy consumption in WSNs through a cluster-based operation. The goal of LEACH is to dynamically select sensor nodes as cluster heads & form clusters in the n/w. LEACH also changes the cluster head dynamically such that high-energy consumption in communicating with sink is spread to all sensor nodes in the n/w.

→ The operation of LEACH is ctalled through rounds, which consist of several phases. During each round, each cluster formation stays the same, and the cluster heads are selected at beginning of each round. A round is separated into two phases, the setup phase & steady state phase. During setup phase, cluster heads are selected, clusters are formed, & the cluster communication schedule is determined. During steady state phase, data communication b/w cluster members & cluster head is performed.

→ The setup phase of LEACH consists of three phases: advertisement, cluster setup & schedule operation. Once cluster formation is completed in setup phase, LEACH switches to steady state phase during which the sensor nodes can begin sensing & transmitting data to cluster heads.

Data Dissemination

- It is the process by which queries or data are routed in the sensor n/w. The data collected by sensor nodes has to be communicated to the BS or to any other node interested in the data. The node that generates data is called a source & the info. to be reported is called event. A node which is interested in an event & seeks info. about it is called sink.
- In data collection model, the source sends the data it collects to a collection entity such as the BS. This could be periodic or on-demand. The data is processed in the central collection entity.

- Flooding

→ The simplest design is flooding. Each node repeats the received data by broadcasting it to neighbour unless dest. reached or max hop ~~count~~ lifetime reached.

→ The major support for flooding is simplicity, it requires no costly topology maintenance or complex route discovery.

→ The shortcomings are substantial:

(i) Implosion: Flooding doesn't restrict multiple nodes from broadcasting same pkt to same dest. Thus, duplicated msg are received.

(ii) Overlap: The info. sent by the sensor nodes is closely related to their sensing regions if two nodes have overlapping regions, then both may sense same stimuli at same time. As a result, neighbour nodes receive duplicate msgs.

(iii) Resource Blindness: Flooding does not take into account the available energy resources. An energy resource protocol must take into account the amount of energy available to it at all times.

- Gossiping

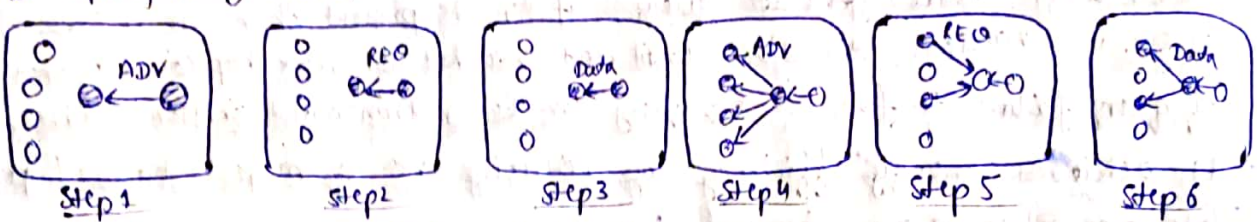
→ It is an enhancement to flooding. When a node receives data, it randomly chooses a neighbour & sends data to it. It avoids problem of implosion but does not address other two concerns & contributes to latency of n/w.

→ A setup from flooding & gossiping is ideal dissemination. In this algo., data is sent along a shortest-path route from originating node. Such approach guarantees that every node will receive every piece of info. exactly once. Ideal dissemination does not take into account that some node may not need a particular piece of info.; nor does it allow for resource awareness.

- Sensor Protocols for Information via Negotiation (SPIN)

→ SPIN disseminates all info at each SN to every other SN in the n/w. An implicit assumption in SPIN is that all SNs in the n/w are potential BS.

→ SPIN assigns a high level name to appropriately describe their collected data called meta data & perform meta data negotiations before any data is transmitted. This ensures that no redundant data is transmitted throughout n/w. The format of meta-data is appln-specific & is not specified by SPIN.



SPIN Protocol

→ SPIN is a 3-stage protocol as sensor nodes use three types of msgs: ADV, REQ & Data to communicate.

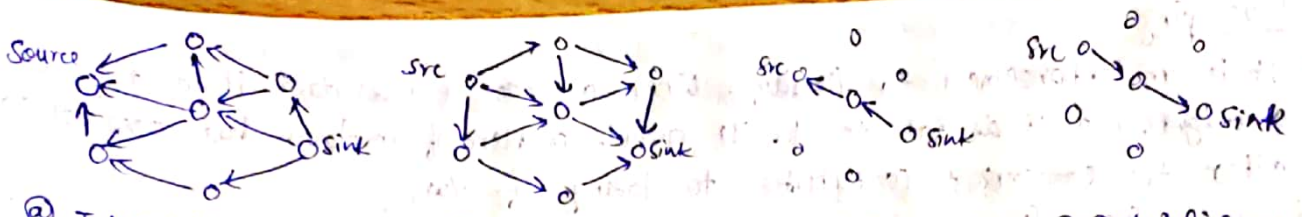
- Direct Diffusion.

→ Traffic flow in SPIN is initiated from sensors & usually ends up at sink. This type of traffic may not always be preferable when user requests specific info from sensors. The direct diffusion data dissemination paradigm has been developed to address this requirement.

→ It consists of 4 stages to construct routes b/w sink & sensors of sink's req. request: (a) Interest Propagation (b) Gradient Setup (c) Reinforcement (d) Data Delivery

→ It is initiated when sink sends out interest msgs to all sensors. This phase is called interest propagation. Upon receiving interest msg, each node stores it in an interest cache which has several fields including timestamp, gradient, interval, & duration. The gradient indicates node from which interest is received. This gradient field is used to form reverse paths towards sink. The sink can reinforce a particular path by resending the interest through specified node in that path. This path can be selected acc^n to several rules such as best link quality, no. of pkts received from a neighbour; or lowest delay. Finally, a route b/w source & sink can be established

→ Using reinforcement, the data routes can be dynamically changed acc^n to changes in the WSN.



ⓐ Interest Propagation ⓑ Gradient Setup ⓒ Reinforcement ⓓ Data Delivery

→ For appln's where data need to be initiated from sensors, an extension of direct diffusion, i.e., push diffusion, has been developed which omits the interest propagation phase & sensors advertise data to sink. Upon receiving advertisements, sink sends reinforcement pkts to establish routes blw sources & sink.

– Rumor Routing

→ It is a probabilistic data-centric routing protocol for large-scale WSNs containing several thousands of nodes. In this, each node maintains a neighbour table as well as an event table. When a nodes notices an event, it probabilistically generates an agent (a long lived pkt that propagate info about sensed events to distant nodes through the n/w). When a node receives agent, it updates event table. When node generate query, if route present then use it else forward query in random direction until dest. reached or max hop count reached. In case of query failure to find event, query can be retransmitted or flooded through n/w.

→ It achieves energy efficiency by reducing no. of msgs exchanges & performing data aggregation along the path.

– Sequential Assignment Routing (SAR)

→ It provides a table-driven multi-path approach & considers QOS requirements

→ Main goal is to create multiple trees originating from root node which is a one of the single hop neighbours of the sink. Each tree grows outward from sink while avoiding nodes with very low QOS & energy resources.

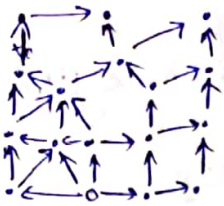
→ Each node specifies two parameters for each path to sink:
Energy Resources # Additive QOS metric: High value means low QOS

→ Whenever a node sends a pkt, it calculates weighted QOS before sending. Weighted QOS is product of QOS metric & priority level of pkt. As a result paths with higher QOS are used for higher priority pkts.

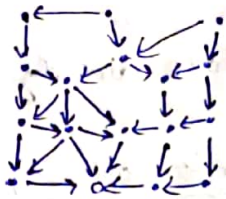
– Cost-Field Approach

→ A cost-field routing assigns each node a cost value that is determined based on the distance blw node & sink. The actual may be chosen calculated from an arbitrary chosen metric. The only requirement is that the cost of is increased on each hop, otherwise a loop could occur.

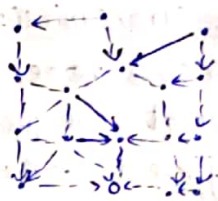
→ When a node receives an Advertisement msg, it compares cost included in msg against own cost. If decreased, accept new cost, increase cost in msg & resend it to neighbours. Thus, farther nodes from sink have higher cost & data can be sent to a neighbour that has a lower cost.



(a) Set-up phase



(b) Established Gradients



(c) Traffic to sink

→ Advantage is that knowledge of forwarding path states is not required.

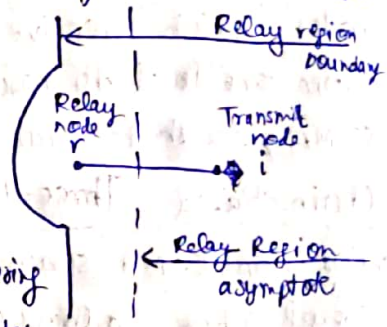
- Geographic Hash Table (GHT)

→ In GHT, whole sensor n/w is considered to be an autonomous database which collects, stores, & manages data. An advantage of this independence is that sampled data can reside where it originates & does not need to be routed to a central sink in the first place. If nodes don't store info., data constantly flows from sources to one sink. On way to central root node, info. will accumulate more & more, and eventually it has to pass bottleneck of root node itself which can mitigated by introducing large no. of sinks.

- ~~Small~~ Minimum Energy Communication N/w (MECN)

→ It maintains a minimum energy n/w for wireless n/ws by utilising low power GPS. The idea is to calculate a min-power topology for stationary nodes, including a master node. It assumes ~~no~~ that the master node is info. sink or base station.

→ ~~Global minima~~ It identifies a relay region for every node which consists of nodes in a surrounding area where transmitting through those nodes is more energy efficient than direct transmission.



Relay Region

→ Global minimum power paths are found without considering all nodes in the n/w. This path discovery is implemented using a two-steps localised search algo for each nodes considering its relay region.

→ Firstly, node take position of its neighbourhood in a 2-D plane & constructs an enclosure graph which contains global optimal links in terms of energy consumption. This table is maintained periodically in order to keep routing table up-to-date.

→ After that, optimal links on enclosure graph use a Belmann-Food shortest path algo. with power consumption as the cost metric. In case of mobility, the position coordinates are updated using GPS.

* Data Gathering

- The objective of data gathering problem is to transmit the sensed data from each sensor node to a BS. The goal of algo.s which implement data gathering is to maximize no. of rounds of communication before nodes die & n/w becomes inoperable. The 'energy × delay' metric is used to compare algorithms, since this metric measures speedy and energy-efficient data gathering.

- Direct Transmission
→ All sensors nodes transmit their data directly to the BS. This scheme performs poorly wrt energy × delay metric.

- Power-Efficient Gathering for Sensor Information Systems (PEGASIS)
→ It is a near optimal chain based protocol. The basic idea of this protocol is that, in order to extend n/w lifetime, nodes need only communication with their closest neighbours & take turns in communicating with base station. When the rounds of all nodes communicating with BS ends, a new round will start & so on.
→ It has two main objectives:
(i) to increase lifetime of each node by using collaborative techniques & thus increase n/w lifetime; and
(ii) to allow only local coordination blw nodes that are close together so that the bandwidth consumed in communication is reduced.
→ The chain in PEGASIS will consist of nodes closest to each other that forms a path to Base Station.
→ It uses assumptions that may not always be realistic.

- Binary Scheme
→ This is also a chain based scheme which classifies nodes into different levels. All nodes which receive msgs at one level rise to next. No. of nodes ~~will be~~ is halved from one level to next. This scheme is possible when nodes communicate using CDMA, so that transmissions of each level can take place simultaneously.

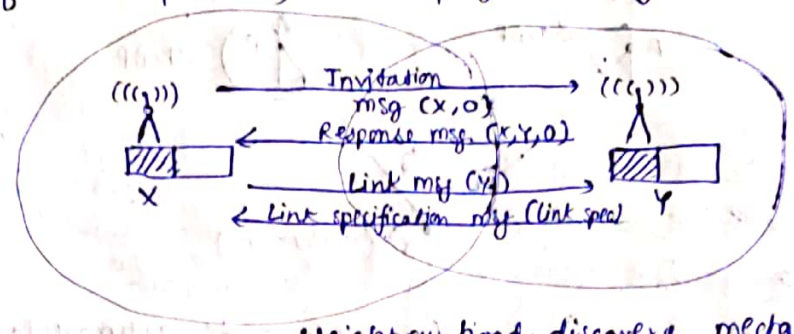
- Chain-Based Three-Level Scheme
→ For non-CDMA sensor nodes, binary scheme is not applicable. The chain-based three-level scheme addresses this situation, where again a chain is constructed ~~like~~ as in PEGASIS. The chain is divided into no. of groups to space out simultaneous transmissions in order to minimize interference. Within a group, nodes transmit one at a time. One node out of each group aggregates data from all group members & rises to next level. The index of this leader node is decided a priori. In second level, all nodes divided into two groups, & the third level consists of msg exchange blw one node from each group of second level. Finally, leader transmits a single msg to the BS.

* MAC Protocols for sensor N/ws
- MAC protocol in sensor n/ws must create a n/w infrastructure to establish communication links among thousands of randomly scattered sensors. It must also ensure fair & efficient sharing of communication resources among nodes so that overall lifetime of n/w. can be maximized.

- Self-Organizing MAC for Sensor N/ws & Eavesdrop & Register
→ Sensor medium access ctrl (SMAC) assume that the available spectrum is divided into several channels & each node can tune its transceiver

to anyone of them as well as nodes have several CDMA codes at their disposal. Each node has fixed time-slots & these are divided into superframes.

→ In start of SMACS protocol, nodes perform neighbour-hood discovery.



Neighbour-hood discovery mechanism in SMAC

→ The major drawback of this protocol is length of super-frame. If superframe is too short, then all neighbour nodes will not be visible to node. Another drawback is that if n/w load is low but no. of nodes in neighbourhood is high, the node will be awake on every set schedule just to find no data transfer.

– Hybrid TDMA/FDMA

→ To find optimum no. of channels which gives min. system power consumption.

→ The optimum no. of channels is found to depend on ratio of power consumption of transmitter to that of receiver. If transmitter consumes more power, TDMA scheme is favoured, while scheme leans towards FDMA when receiver consumes greater power.

– CDMA-Based MAC Protocols

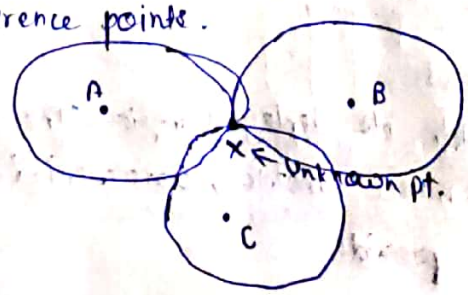
→ MAC protocol for sensor n/ws must be able to support variable, but highly correlated & dominantly periodic traffic. Any CSMA-based medium access scheme has two important components, the listening mechanism & backoff scheme. A CDMA-based MAC scheme for sensor n/ws is presented.

* Location Discovery

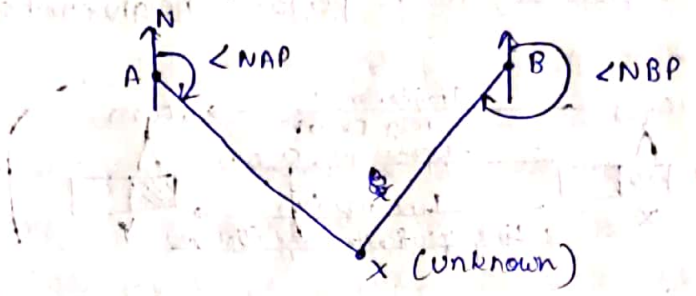
– Loc^n Discovery Concepts

→ Existing localization schemes, mostly on principle of triangulation. For 3-D space, an additional reference point is needed.

→ Lateration: If distance from an unknown location to three reference pts. are known, the loc^n of unknown pt. can be obtained using geometrical calculations known as multilateration. Here, unknown pt. loc^n is obtained as pt. of intersection of three circles centered at reference pts having radii equal to distance from these reference points.



→ Angulation: Alternatively, angles from two known reference pts. may be used to determine loc^n of an unknown. This mechanism is called as angulation.



- Indoor Localization

→ These techniques uses a fixed infrastructure to estimate loc^n of sensor nodes. The randomly distributed sensors receive beacon signals from the beacon nodes & measure signal strength, angle of arrival, & time difference b/w arrival of different beacon signals. Using the measurements from ~~three~~ multiple beacons, the nodes estimate their loc^n.

- Sensor N/w Localization

→ In situations where there is no fixed infrastructure available & prior measurements are not possible, some of the sensor nodes themselves act as beacons. They have their loc^n info, using GPS, & these send periodic beacons to other nodes.

→ In case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate distance. Alternatively, time difference b/w beacons arrivals from different nodes can be used to estimate distance, if RF or ultrasound signals are used for communication.

→ Localization algo(s) require techniques for loc^n estimation depending on the beacon nodes' loc^n. These are called multi-lateration (ML) techniques.

→ The atomic multilateration localization of a single node which has at least three neighbouring nodes.

→ There may be cases in which network ~~where~~ have a node that does not have any neighbours with enough nodes as neighbours. In this case, collaborative multilateration technique is used where one of the node solves a joint set of loc^n estimate func^{n}s using multi-hop info. from an unknown neighbour node to find loc^n of both nodes simultaneously.

* Quality of a Sensor N/w

- ~~to~~ Main parameters which define how well the n/w observes a given are are "coverage" and "exposure".

- Coverage

→ A WSN is typically used to monitor its deployed region. The coverage of the n/w is a very important performance metric, characterizing the quality of surveillance that the WSN can provide.

→ A good coverage provides necessary basis for high-level func^ns such as intrusion detection, target localization, classification, and tracking. Coverage requirements vary with different appln scenarios. Coverage holes can be created in the region of interest due to lack of appropriate no. of sensor nodes, limited sensing range of individual nodes, & the random deployment of nodes.

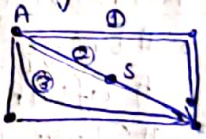
→ There exists a threshold value for node density. Complete coverage is possible if the node density is greater than the threshold value.

→ Voronoi diagram provides proximity info about a set of geometric nodes or pts. The Eucledian diagram of two pts p, q is denoted by ed(p,q). A Voronoi-diagram based node-deployment protocol is to optimize n/w coverage. Each sensor node calculates its Voronoi polygon from received neighbourhood info. The sensor nodes check whether coverage hole exists or not in their polygon. If so, estimate their next locn to reduce or omit hole.

→ Virtual force-based approaches, proposed are used to optimize coverage area. Here nodes are assumed as virtual particles or electrostatic particles. Movement of a node is influenced by virtual forces. The basic principle is that, after initial deployment, nodes spread from densely populated area to all over the monitored area. Each node repels its neighbour nodes & is repelled by local obstacles. The n/w reaches a static equilibrium state when all nodes stop due to viscous-force.

— Exposure

→ The notion of exposure can represent such a measurement ~~that~~/described as the expected average ability of observing a target moving in a sensor field.



→ A Voronoi approach based on notion of exposure to evaluate coverage of WSN has been proposed. To solve worst-case coverage problem, the maximal breach path is used. It is a path through a sensing field b/w two pts such that distance from any pt. on the path to the closest sensor is maximized. Maximal breach path must lie on line segments of Voronoi diagram corresponding to sensor nodes. The best-case is solved through maximal ~~maximal~~ support path which is the path through a sensing field b/w two pts for which distance from any point on it to the closest sensor is minimized ~~minimized~~.

→ The Delaunay triangulation produces triangles that have minimal edge lengths among all possible triangulations. Thus, maximal support path must lie along lines of Delaunay triangulation of sensors.

* Evolving Standards

- The IEEE 1451 family of standards define a set of common cmds & func^ns to access sensors in a wireless sensor n/w.
- On July 11, 2001, the first wireless sensing workshop was held at the Sensors Expo in Chicago, IL, to determine the interest & requirements for wireless interfaces for sensor-based n/ws. In this workshop, the various wireless

technologies, such as IEEE 802.11x & Bluetooth, were presented & discussed. In order to greatly reduce time to develop IEEE 1451 wireless standard, IEEE 1451 wireless standard adopted parts of these wireless standards.

- The second workshop was held on Oct, 4, 2001, in Philadelphia, PA, & examined alternative wireless communication technologies for sensors. An IEEE 1451.5 study group was formed to further explore this idea, along with wireless sensor interface requirements at 2002 Sensor Expo/Conference held on Sept. 23-26 in Boston, MA. Later an IEEE 1451.5 working group was formed to develop a wireless sensor standard.
- IEEE 1451.5 WSN standards should cover wireless n/ws PANs, LANs, WANs & even larger n/ws. IEEE 802.15 supports a WPAN with range of 10m to 100m. IEEE 802.11 supports WLAN with range 20m to 5km. IEEE 802.16 supports WWAN with range of 5km to 15km. IEEE 1451.5 has adopted WPAN & WLAN.
- The first draft of IEEE 1451.5 standard was proposed at 2004 Sensors Expo/Conference. IEEE 1451.5 standard was finally developed & published in 2007. This standard was developed to be compatible with IEEE 1451.0 standard. It also adopts multiple wireless communication protocols, including IEEE 802.11 (WiFi), Bluetooth, ZigBee, & 6LOWPAN. An implementation of IEEE 1451.0 & 1451.5 based on IEEE 802.11 is provided.

* Other Issues

(i) **Synchronization**: Various issues in synchronization are:
- # Energy utilization of synchronization schemes
- # Lifetime & degree of failures of sensor nodes
- # Data fusion & Data estimation
- # Degree of accuracy
- # Jitter

(ii) **Data Aggregation & Data Dissemination**: Some design issues in these are:
- # Up-to date info. of adjacent nodes
- # Data Transmission
- # Redudancy elimination
- # Clustering techniques improvements
- # In n/w data aggregation improvements

(iii) **Architecture**: Some issues that must be addressed are:
Channel Monitoring # Data encoding & transfer # Scalability # Flexibility # Precision of CSI

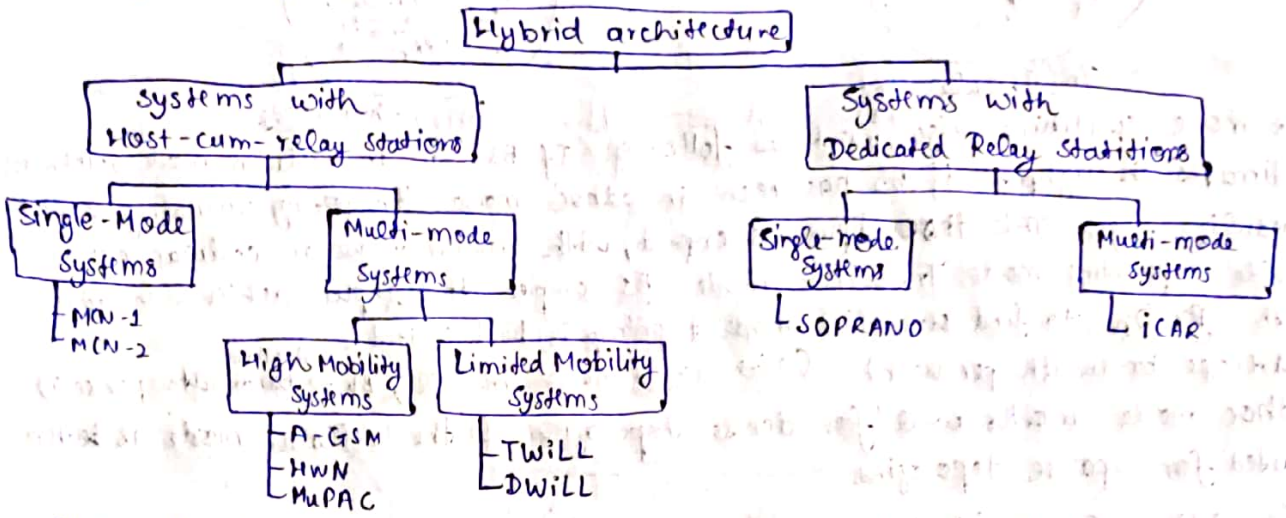
(iv) **QOS**: Various QOS issues are:
Topology Management # Bandwidth utilization # Traffic management # Scalability

(v) **Security**: The security requirement to WSN appl^n^s are:
Confidentiality # Authentication # Integrity # key Distribution methods # Msg exchange methods

Hybrid Wireless N/Ws

* Next-Generation Hybrid Wireless Architectures

- Classification of Hybrid architectures

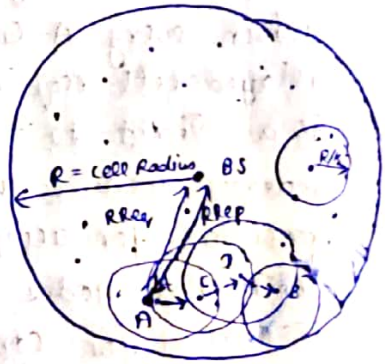


- MCN Architecture

→ A cellular architecture where a conn. b/w source & dest. is established over a multihop path. The design philosophy of MCN is that the transmission power of the MHs & the base station (BS) over the data channel is reduced to a fraction 1/k (where k is referred to as reuse factor) of the cell radius.

→ All MHs in a cell take part in topology discovery, wherein each MH regularly sends to the BS, info. about its neighbours. While the transmission range on data channel is kept half of cell radius, that on ctrl channel is equal to cell radius.

→ A base-associated-on-demand approach is used for routing for MCN. The routing protocol has a route discovery phase & a route maintenance phase. Route is computed by Dijkstra's shortest path algorithm



→ On reception of this info., the sender, the intermediate nodes, & the dest. become aware of call setup. If call can't be established, sender informed by unicast pkt over ctrl channel.

→ For each hop, the channels are checked in a predetermined order & first channel that satisfies constraints is selected for use.

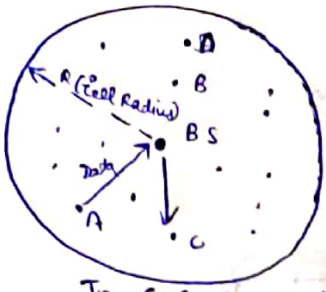
→ To reduce chance of call dropping, some channels are reserved for rerouting calls.

→ MCN-2 uses a new routing protocol called Base Associated Adhoc Routing (BAAR) protocol.

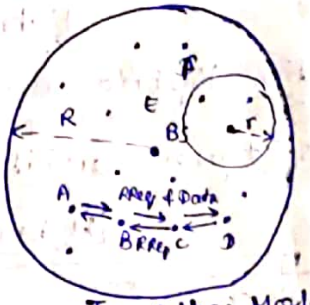
- Hybrid Wireless N/W (HWN) Architecture

→ It is a novel multihop architecture having the capability of switching b/w multihop mode & single-hop mode of operation based on throughput achieved. HWN has two modes of operation: the cellular mode & adhoc mode.

→ In cellular mode, nodes sends pkts to BS, which forwards them to dest. In adhoc mode, nodes use the Dynamic Source Routing (DSR) protocol to discover routes.



In Cellular Mode



In Adhoc Mode

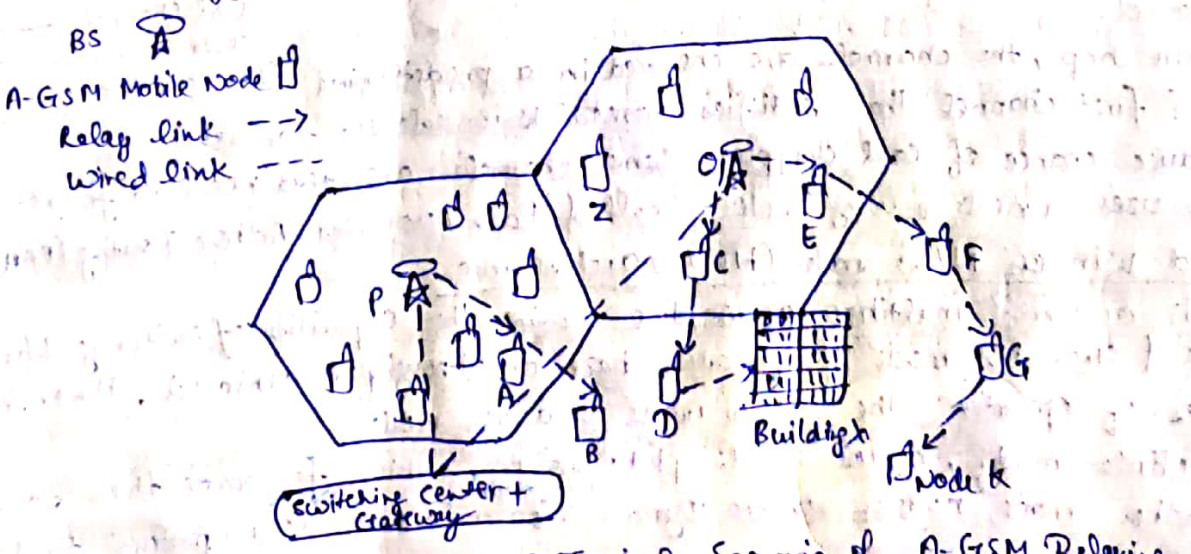
→ The mode switching algo at BS work as follows. If BS is in cellular mode, then BS estimates throughput if BS has been in adhoc mode ~~through~~ by simulating a pkt scheduling algo. This throughput is cmped, with actual value in cellular mode to decide operating mode. In adhoc mode, BS cmpes throughput achieved in adhoc with $BW/2n$ to find out which mode topology is best suited.
(Average bandwidth per user) ($n \rightarrow$ no. of nodes in cell, $BW \rightarrow$ Available Bandwidth per cell)

→ Adhoc mode works well for dense topologies & the cellular mode is better suited for sparse topologies.

— The Adhoc-GSM (A-GSM) architecture

→ It was proposed as an extension to GSM cellular architecture for providing extended service coverage to dead spots. This is a multihop-relaying-enabled extension to GSM architecture in which service coverage can be provided to regions that are not covered otherwise. It aims to use the existing GSM system modules & entities with minimal changes for providing compatibility with existing GSM systems.

→ The GSM link layer protocol is modified to handle a beaconing scheme by which every A-GSM-enabled node originates beacons periodically. Every relayed cell requires bandwidth, buffer space, and processing time. Hence, there is a limit to total no. of calls that an A-GSM node can relay. A resource manager module running in an A-GSM node executes a call admission ctrl procedure for accepting or rejecting a call through the node. All the intermediate nodes relaying the call request and acknowledgement reserve resources for completion of the call.

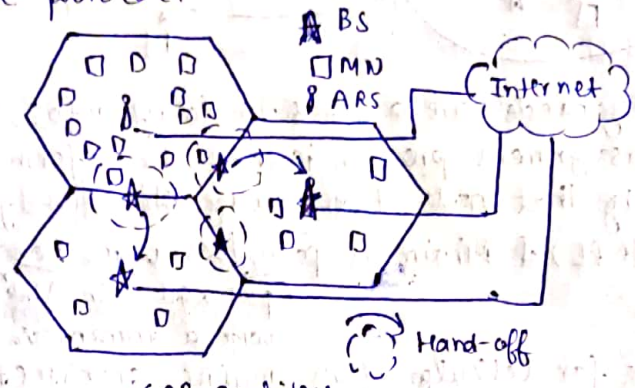


A Typical Scenario of A-GSM Relaying

- iCAR (Integrated Cellular & Adhoc Relaying) Architecture

→ An iCAR system enables a cellular n/w a achieve a throughput closer to its ~~throughput~~ theoritical capacity. This approach is based on dynamically balancing the load among different cells. A no. of Adhoc Relaying stations (ARS) are deployed at appropriate loc^n s.

→ The ARSs serve to relay excess traffic from a heavily loaded cell to a lightly loaded cell in the same vicinity. The coordination b/w BSs, ARSs & MNs is handled by a ctrl protocol.



iCAR architecture

→ A similar approach, relaying access traffic is shown in MADF (Mobile Associated data-forwarding) architecture. Main difference ~~btw~~ is that MADF doesn't use dedicated nodes to relay excess traffic as iCAR does, but rather MADF uses MNs.

→ iCAR system proposes three modes of relaying:

(i) Primary Relaying: In a SCN, if a MH x in a congested cell A makes a call request & also no data channel is free at BS A, the call will be blocked through primary relaying.

(ii) Secondary Relaying: It capitalizes on the feet that not all MHs with ongoing calls in ARS coverage region would be using primary relay. The idea is to free up a DCH from BS A for use by MH X.

(iii) Cascaded Relaying: It is possible that a relay path can be set up b/w MH X in cell A & a neighbouring BS B, which is unfortunately congested. Here, secondary relay can be deployed to free a DCH in a cell B by establishing a relay path b/w MH Z in cell B & neighbouring cell C. The freed DCH can be used to connect MH X to BS B through a relay path.

- ~~The~~ Self-Organizing Pkt Radio Adhoc N/w with Overlay (SOPRANO) architecture

→ It advocates six steps of self-organization for the physical data link and n/w layers to optimize n/w capacity: neighbour discovery, connection setup, channel assignment, planning transmit/receive mode, mobility management and topology updating, exchange of ctrl & routing info.

→ In MAC layer, if transmissions are directed to a node with several intermediate nodes by multi-hop, clever frequency channel assignments for each node can significantly reduce the interference & could result in better performance.

→ In N/w layer, the system capacity can be enhanced by taking multi-hop routing, the interference & the energy consumption into account.

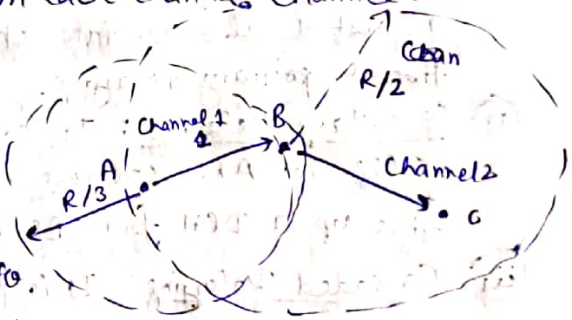
→ The goal is to provide high data rate Internet access by using inexpensive dedicated relay stations. The n/w capacity can be maximized by choosing a suitable routing strategy, which is a funcn of all techniques used in physical layer. This approach can assure load balancing & potential throughput enhancement.

→ Two separate frequency bands are assumed to carry info., one each for up & down streams. A channel assignment process is used to inform every node about channel to be used by that node. Two routing strategies for this architecture (Minimum Path loss (MPL) & Minimum path loss with Forward progress (MPFP)) (pkt with min link propagation along with a transmission direction towards BS))

– Multi-Power Architecture for Cellular N/ws (MuPAC) architecture

→ In an n-channel MuPAC architecture, there are n+1 channels, each operating at a different transmission range. The total bandwidth is divided into a ctrl channel using a transmission range equal to cell radius (R) & n data channels each operating at different transmission ranges. The decision to use a particular channel at an intermediate node in a path is a local decision taken by the intermediate node based on current load on each ~~channel~~ channel.

→ The path selection at the BS is done by assigning appropriate edge weights that are directly proportional to the approx distances blw nodes. This approx distance is measured using GPS (Global Positioning System) info. Dijkstra's shortest path algo is used to obtain a min. weight path. MuPAC solves the n/w partition problem at low node density using single-hop ctrl channel for data transmission.



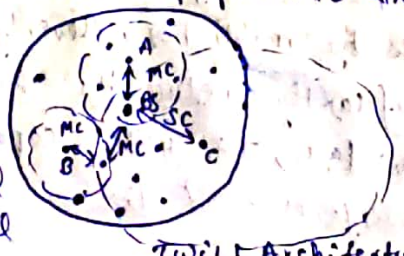
Pkt Transmission in 2-channel MuPAC n/w

– Throughput-enhanced Wireless in local Loop (TWiLL) architecture

→ It is a multihop architecture for limited mobility systems such as WLL. MH will also be used to refer to as a WLL or TWiLL subscriber, be it a stationary fixed subscriber unit (FSU) or an FSU with limited mobility.

→ The bandwidth available is split into one ctrl channel & several data channels. TWiLL solves the problem of n/w partitions by allotting a channel ch in single-hop mode when there is no multi-hop path to the BS.

→ The stationary nature of subscribers enables use of directional antennas at MHs, thus reducing interference incurred at nodes in TWiLL.



MC - Multihop channel
SC - Single hop channel

TWiLL Architecture

- The DWiLL (Directional throughput-enhanced Wireless in Local Loop) Architecture

→ DWiLL uses dual throughput enhancement strategies of multi-hop relaying and directional antennas. The major advantages include reduction in energy expenditure at FSUs & ability to provide enhanced throughput when no. of subscribers becomes large.

→ The spectrum is divided into no. of channels, similar to TWiLL. The key difference b/w TWiLL & DWiLL is use of directional relaying by FSUs in DWiLL. DWiLL assumes that directional antennas at FSU is oriented in the direction of the BS.

→ The FSUs use directional antenna to transmit ctrl info., beacon signals, and the data msgs. The system works by building the topology info at BS, as in BAAR protocol.

→ DWiLL also designates data channels into two categories : Multihop channels (MCs) & single-hop channels (SCs). SCs are further divided into uplink channels (ULCs) & downlink channels (DLCs). ULCs are assigned to those nodes that do not find immediate relaying stations to use MCs for setting up data paths to BS. The DLCs are used by BS for downlink transmissions to FSUs.

→ The BS chooses appropriate transmission mode (multi-hop/single-hop) to FSU by means of channel selection.

* Routing in Hybrid Wireless N/Ws

(i) Base Assisted Adhoc Routing (BAAR)

→ Node A is source node & node B is dest. node

(a) If BS(A) = BS(B),
- # Run shortest path algo. over the wireless links in common cell
- # Return path obtained

(b) Else if BS(A) & BS(B) are BSs for adjacent cells,
- # Get state of links in adjacent cell B belongs to
- # Run shortest path algo over all the wireless links in two adjacent cells, including the link (BS(A), BS(B)) with w(BS(A), BS(B)) = 0
- # Return path obtained

(c) Else,
- # Run shortest path algo over all the links in A's cell & get shortest path p1 from A to BS(A).
- # Similarly, get shortest path p2 from BS(B) to B. Note that because all this happens at the BS, it has access to the loc^n database of nodes. All the info. required to find BS(B) & path from BS(B) to B is available from BS(B).
- # Return p1.(BS(A), BS(B)).p2.

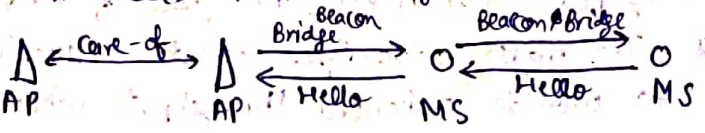
→ The BS runs the BAAR protocol upon request from any mobile node.

(ii) Base-Driven Multi-Hop Bridging Rowing Protocol (BMBP)

→ It is implemented in both MSs & APs to enable multihop routing and roaming. It works by building bridging tables at each node, either a MS or an AP. In the bridge table the dest. seq. no. is used to prevent loops in routing. The MS additionally timestamps the entry to avoid stale entries. For each dest. in the bridge the node records the next hop & hop count.

msgs used in BMBP:

Beacon # Hello # Bridge # Care-of



→ Protocol Procedures:

Beacon msgs, originated from APs, are used to help MSs decide their associated APs.

Each MS will consider a Hello msg for propagation only if the Associated AP field in the Hello msg corresponds to its associated AP, otherwise ignores Hello.

At the AP when a Hello is received, it does a sanity check if Hello is indeed intended for it, & then proceeds to process Hello msg. The path taken by Hello msg gives AP a partial bridge table.

When a MS receives Bridge msg, it checks if it is intended dest. of msg. If it is the dest. it just replaces its bridging table entries with those given in msg. Otherwise ~~it look~~ it looks up is local bridge table to find next hop to dest, & forwards the Bridge if an entry exists. The AP on receiving ~~an~~ a Care-of msg just records the address of the remote MS & its associated AP.

(iii) SMCN Routing Protocol

→ The main types of protocol msgs are:

Registration Request (RegReq) # Registration Acknowledgement (RegAck)

Route Request (RouteReq) # Route Reply (RDute Rep)

Neighbour Update (NeighUpdt)

→ Each node, both BSs & MSs will periodically generate Neighbour or Beacon msgs.

→ When a Beacon reaches a MS it has to process the msg & suitably find the BS nearest to it on basis of hop count metric.

→ When Beacon arrives, if Beacon has come from MSs current next hop to its registered BS, it simply update contents of its local data with new data. Then the MS proceeds to compute the new BS to register by finding BS with smallest hop count.

→ In order to reduce vulnerability of the case path, nodes will not register if the hop count exceeds a particular threshold. The MS then sends a RegReq to the nearest BS computed, by forwarding the request to its current next hop to that BS.

→ As the request is propagated toward the BS each node will append its address into the Path field of the request pkt to facilitate routing of RegAck pkts. When RegReq has reached the intended BS, it will then generate a RegAck to be sent to the MS that originated the request through path specified in request pkt.

→ If the difference b/w newly received power & previously recorded power exceeds a particular threshold the MS will have to send a NeighUpdt. msg to BS informing it of the new power.

* Pricing in Multi-Hop Wireless N/Ws

- Pricing in Multi-Hop wireless WANs

→ The multi-hop wireless mesh n/w for local communication are intended for commercial deployment, the pricing should be as realistic as possible, with the charging units having a realistic correspondance to actual monetary units.

- Pricing in Adhoc Wireless N/Ws

→ Pricing framework should be decentralized, due to absence of any perceivable supporting infrastructure. Several pricing models have been presented as part of the tremendous project to enforce service availability in adhoc wireless n/ws.

- Pricing for voice traffic

→ In End-to-End Successful Transmission Reimbursement Scheme (EESR), the intermediate nodes are reimbursed only when pkts that they forwarded reach the dest. successfully. The pricing info. that is sent to BS consists of a list of paths along with the no. of bytes transferred along that path within that pricing period. The pricing info. can be sent along with periodic neighbour updates that the dest. generates & forwards to the BS.

→ Hop-to-Hop Successful Delivery Reimbursement (HHSR) scheme reimburses the intermediate nodes for all successful link-level transmissions. If an intermediate node has successfully forwarded a pkt on behalf of a src to next-hop node supplied in IP src route, then it has performed its duty, and it needs to be reimbursed for the service that it has provided to src irrespective of whether pkt actually reaches dest.

→ In Hop-by-Hop & Retransmit Attempts Scheme for Reimbursement (HRSR), the pricing info. has to be aggregated to all nodes in n/w, each keeping track of no. of bytes it has successfully forwarded to the next hop, & the total no. of attempts it has made for each src for which it func's as an intermediary.

* Power Ctrl Schemes in Hybrid Wireless N/Ws

- Power ctrl schemes are designed to serve large no. of power-constrained mobile nodes. The HWN architecture utilizes power ctrl in adhoc mode to maximize the achievable system throughput.
- In power optimization scheme, the available bandwidth is considered to be divided into n channels, each of which can operate at different transmission ranges similar to MuPAC architecture. Using periodic Hello pkts used in MCN & MuPAC architectures & received power at every node, an approx distance to sender is calculated. The transmission power is estimated from sum of estimated distance & the mobility margin value.
- In scheme proposed by Bhaya et al. in the transmission power of RTS/CTS is kept constant & at same time, transmission power for Data & Ack is reduced to the sufficient value required for communication. The effect of this scheme is as follows. The no. of nodes affected by transmission are same as that in non-power optimized system.

* Load Balancing in Hybrid Wireless N/Ws

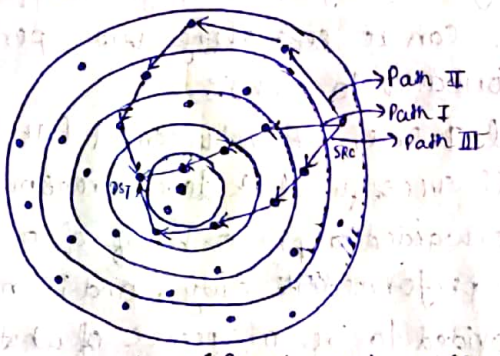
- Load Balancing refers to distribution of relay traffic load uniformly throughout the n/w so that no region in the n/w is particularly overloaded.

- Preferred Ring-Based Routing Schemes

→ The existing ring-based schemes for load distribution & throughput improvement in WMNs are following:

- # Preferred Outer Ring Routing Scheme (PORS)
- # Preferred Inner Ring Routing Scheme (PIRS)
- # Preferred Dest. Ring Routing scheme (PDRS)
- # Preferred Src. Ring Routing scheme (PSRS)

→ The primary idea behind all these schemes is that any traffic generated by a node in ring 'i' for a node in ring 'j' must not be forwarded through nodes which are in rings beyond the one enclosed by rings i & j. Dijkstra's shortest path algorithm when applied to n/w to determine path from a src to dest., with all edges of weight one, yields the shortest path blw the src & the dest. in terms of hop count.



Src - Source
DST - Destination
Path I : Shortest Routing Path
Path II : PORS / PSRS
Path III : PIRS / PDRS

Example of Routing Using Different Schemes

- Preferred Outer Ring Routing Scheme (PORS):

→ In this case path blw src & dest. pair is chosen in such a way that the path predominantly lies on outer ring. Every pkt remains the max time in outer ring of src & dest.

- Preferred Inner Ring Routing Scheme (PIRS)

→ The pkt must be preferably routed through in the inner of the sender's or receiver's rings.

- Preferred Dest. Ring Routing Scheme (PDRS)

→ The angular transmission takes place in the ring of dest. node. This scheme is hybrid of PIRS & PORS. The hybrid character is due to due use of PORS in half the cases & PIRS for other half. Also, avg path length lies in blw that of PIRS & PORS.

- Preferred Src. Ring Routing Scheme (PSRS)

→ Cmpred to PDRS, in PSRS, the angular transmission takes place in the ring of src. node. Similar to PDRS, this is also a hybrid of PIRS & PORS. Also, the avg length in PSRS lies in blw that of PIRS & PORS.