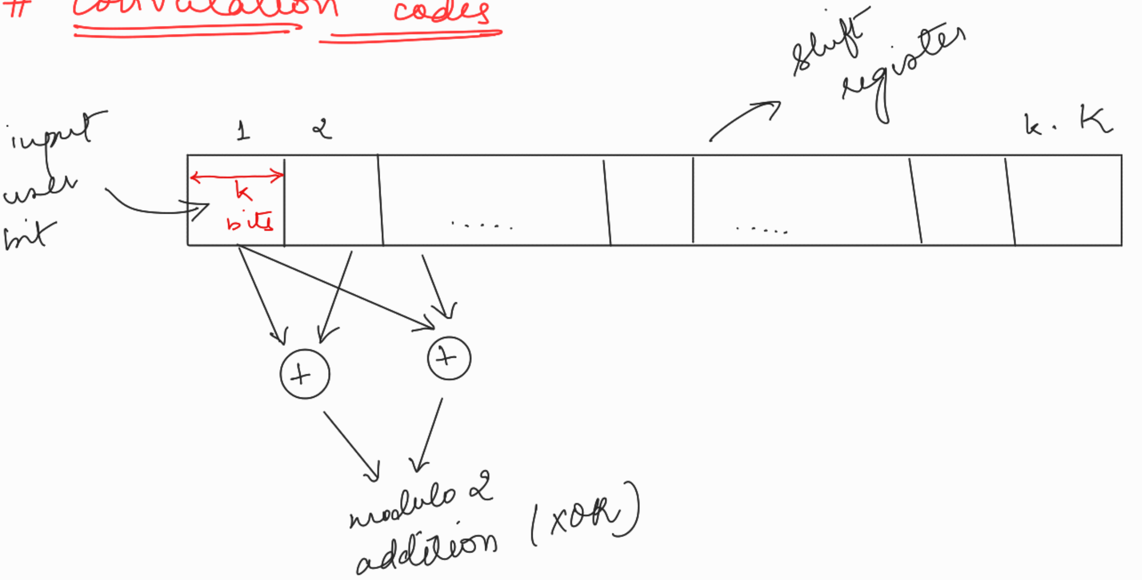
Convulation codes



Each block consist of k bits. Total no of block : K

∴ length of shift register = k.K

Evaluation at k.K depends on that at k.(K−1)

Block codes are more energy efficient than convulation codes.

Convulation codes have better error correction ability.

framing

To deal with time variation of channel (slow & fast fadding) that results in variation in packet size. Thus framing a packet is essential. It is of 2 types —

(i) Adaptive Scheme ↓ packet fragmentation and re assembly is required

(ii) Intermediate checksum scheme (ICS) ↓ packet fragmentation and re assembly isnt required

channel is BSC : ok → ack is true

Binary symmetric code.

if not → ack is −ve (channel has error) → resolved by

Random

MLE

Reforwarded packet

• user data :

header	data	Tailor

address of Tx & Rx, framelength, control mech

checksum of data

depends on header & tailor

probability of error (P) due to user data (U) and overhead (O) considering the channel as random variable where M pcks are transmitted & reception rate is T. Then expectation : $\frac{T}{M}$.
Knowing the expectation and prob. of correctly transmission pckt.
∴ probability of error is a func of user data (U) and overhead (O). P(O, U, P) is used to determine packet size required for adaptive scheme –

• Disadv of adaptive scheme –
– will retransmit the entire frame if there is error in packet

• In ICS, only packets with error are transmitted again rather that retransmission of entire frame.

• considering a sender with S bits and overhead with O bits (consisting of h header & t tailor). During retransmission, total bits required are S + h + t. But in case of ICS, we have L chunk with C bits in each. These L chunks take care of reducing the no of bits transmitted. If S' is no of bits of data with L chunks and c bits, it will lead to correct those chunks which are in error. Thus the header & tailor of error chunks are asked for retransmission

Here $S' + \underbrace{L}_{\text{no. of chunks with error}}(\underbrace{h' + t'}_{\text{header \& tailor of error chunks}}) < S + h + t$

Tradition framing —

DLL-MAC header	User Data	FCS

FCS → forward correction

ICS ————

DLL-MAC header		fcs		fcs		fcs

↓

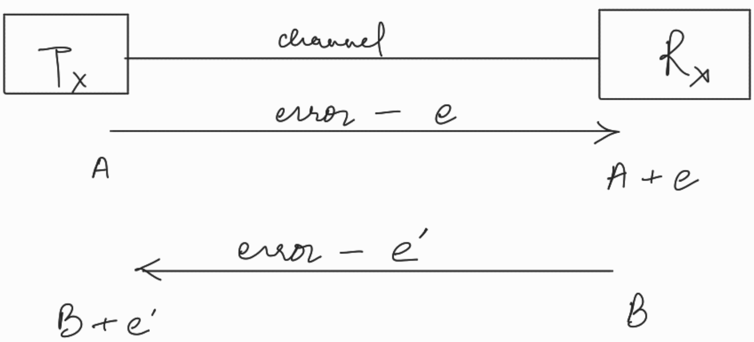
Merit : bit to be retransmitted ↓

Demerit : computationally extensive due to CRC checksum.

link Management

- The data from link layer is transmitted to upper layer without error but if error is more, it is transmitted to upper layer. Thus efficiency of application layer decreases.

- The link management deals with proper management of link with transceiver. Some properties of link —
  - (i) link can be good or bad ← determines the link quality
  - (ii) for a particular transmittor power, link quality is independent of distance (d).
  - (iii) Region around node with packet loss scenario isn't a circle but a random scenario
  - (iv) link can be assymmetric —



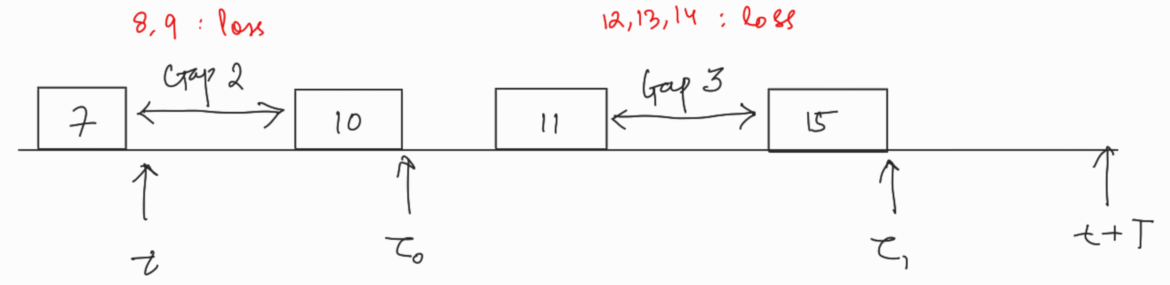
$e \neq e'$ → coz link is assymmetric.

(v) packet loss is time variable (varies with time)

link Quality Estimation

- It's imp as data transⁿ with faulty link is irrelevant. So properties/matrix can be used to estimate — precision, agility, stability, efficiency
- Types < passive estimation (deals with neighbours packet & status to estimate) — status → sequence
  active " (nodes send info to neighbours & collect info from them, periodically)

⇒ Passive Estimation



estimate Gap & repair those pckts and resend.

from this diagram, 2 packets loss b/w t to τ_0 & from t to τ_1 only 3 packet received. So we need to estimate the gap from τ_1 to $t+T$.

Some estimation tech are — exponentially weighted moving avg, time moving avg

for estimation parameters are — T, $\alpha \in (0,1)$ → waiting factor, μ → learning factor

if the update for instance t_n is r_n which indicate the no. of received packet b/w interval t_{n-1} to t_n and f_n is no of packets lost during that interval, then $\mu_n = \dfrac{r_n}{r_n + f_n}$

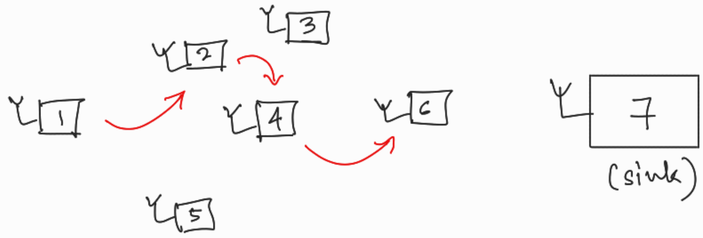
$$\hat{P}_n = \alpha \hat{P}_{n-1} + (1-\alpha)\, \mu_n$$

$\hat{P}_n$ → possible estimation time

Routing Protocol

- we use technique named multi hop.

In diagram since 1 & 6 aren't neighbours → no direct hopping but indirect " can be done.

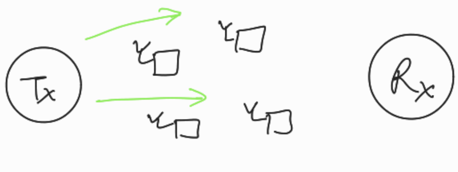


- during multi hop, there are intermediate nodes which decide to which node, data packet to be routed, if the neighbourhood node isn't the instanded node.
- Routing possibility is done via routing table which takes care of the construction & maintainance

forwarding & Routing

- passing info can be done — flooding, Gossip, Routing → complex due to computation extensive

(1) flooding

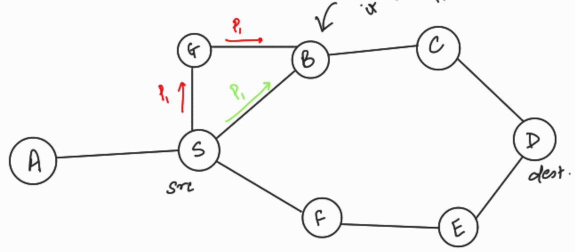


packet delivery ratio is higher. (Adv)

Disadv — packet circulation (one packet received at R_x multiple time) → resolve : (i) use packet identifier at a node
(ii) a threshold of packet hop (restrict no of hop)
(iii) restrict the packet time

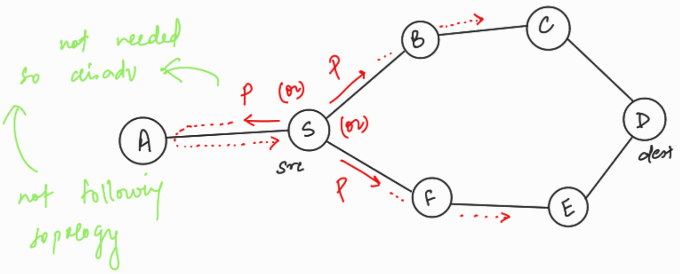
methods to restrict flooding

if B gets P_1 from S before G then it will never accept P_1 from G.



(2) Gossiping

- its the mech. where the packet is arbitarily sent in the network and it randomly searches the destination.
- pckt moves randomly in the network
- simple than flooding (Adv)
- Disadv — it doesnt following network topology & cause delay



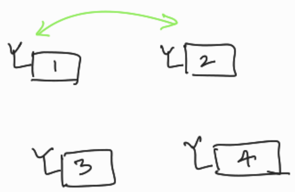
(3) Routing

- Routing table is a type of forwarding tech where a suitable neighbour is chosen on behalf of the cost. Cost is found from the no of hops and min energy of a link.

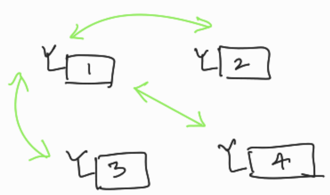
Types of Routing

- Types of Routing
  - Unicast — data sent to 1 identified sensor
  - Multicast — " specific grp of " nodes
  - Broad cast — " all "

on basis of geographical regions



unicast



Broad cast

Tech. for unicast

- There are diff tech like Gossiping & Agent Based Unicast Routing

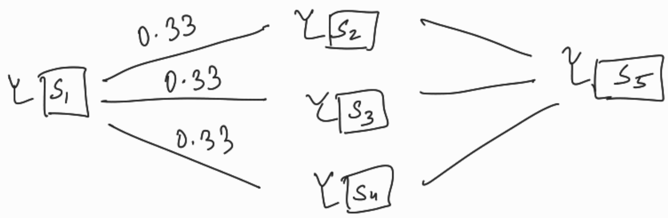
Gossiping → Randomized forwarding

Agent Based → Random work — with known destinations / without knowledge of dest.

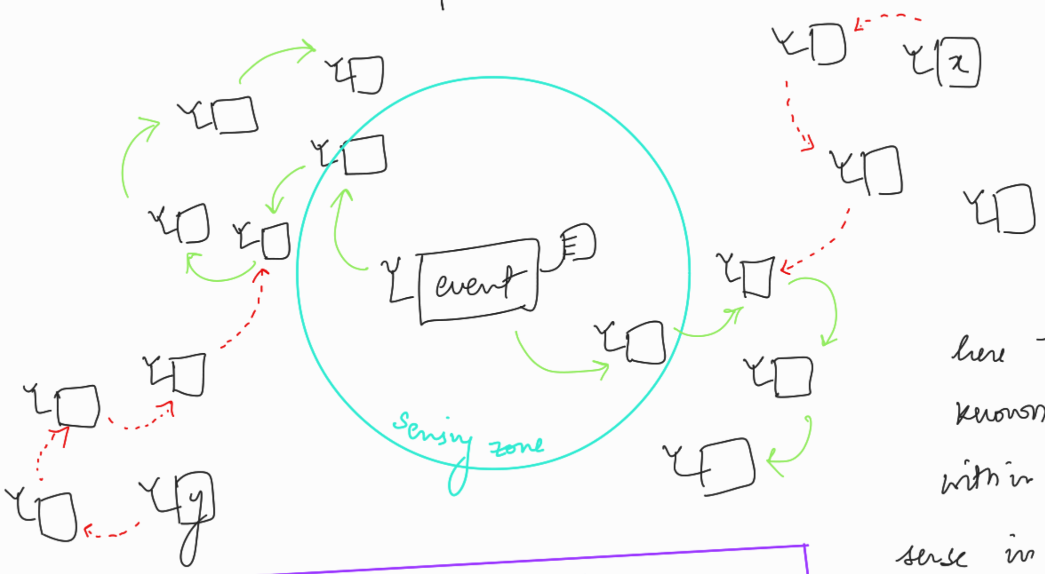
- if node retransmit data with probability higher than critical prob., then gossiping mech works. If condⁿ is violated gossiping isnt successful.

⟹ Random Work

Case 1: All nodes take the forwarding burden and dist is known



Case 2: rumour routing (Nodes have diff forwarding burden and dest is unknown)

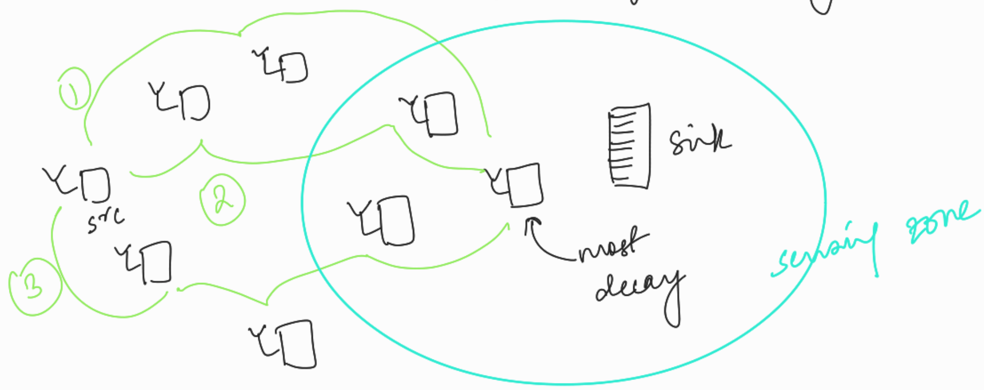


here the event / dest isnt known. When it happens, sensors within the range (i.e. neighbour) sense it. And sensor like x & y regularly query to nearby sensors for event detection

⟹ Multipath unicast routing

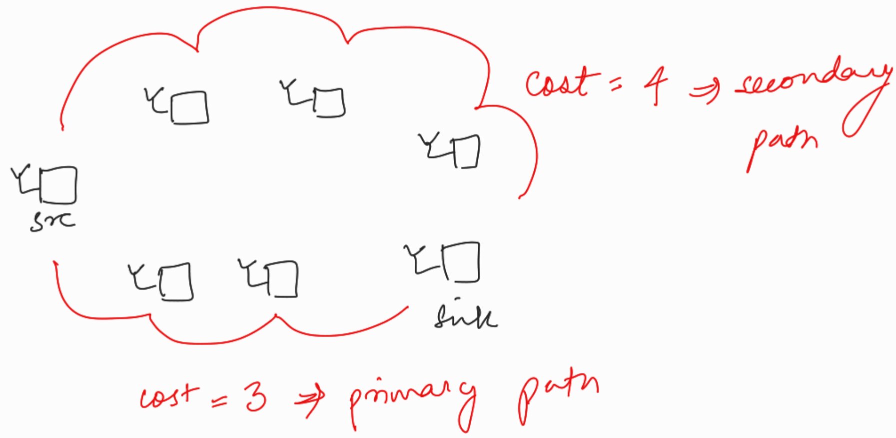
Single link → ensures trade off b/w comm. energy and device battery

- The multipath link follows a algo called sequential assignment routing. The multipath link acts as a stand by.
- As the node closest to sink node decays max energy. To avoid this, neighbours of sink nodes are used & a tree is formed considering the nodes of each neighbourhood of sink node. The trees cover all the nodes & best possible packet path is found on the basis of delay & battery resource.

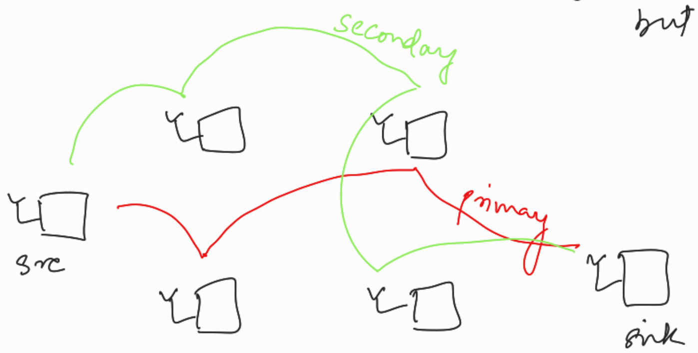


⟹ constructing energy efficient secondary path

(a) Disjoint path



(b) Braided path (chance of path in node failure is ↓ but not nullified)



⇒ Simultaneous transmission through multiple path.

No of path ↑ ⇒ delivery ratio ↑ & packet error ↓ (adv) but overhead ↑ (dis adv)

⇒ Randomly choosing one of several path

Here a particular node v has neighbours $v_1, \dots v_n$ with cost $c_1 \dots c_n$. Then random sending is done via the probability obtained from sensors neighbours. $C = \frac{n}{\sum_{i=1}^{n} c_i}$ then finally pkt is forwarded to neighbours but then neighbours will decide the future

$$P = \frac{1}{c_i} \cdot \frac{1}{\sum_{i=1}^{n} c_i}$$

multipath ensures broadcast.

Routing strategies

Routing strategies

- Unicast (one node to one intermediate node)
- Broadcast (one node to all nodes)
- Multicast (one node to a grp of nodes)
  - Source based tree
    - Stiener tree
    - Shortest path tree
  - Shared core tree
    - single core
    - multicore
  - Mesh

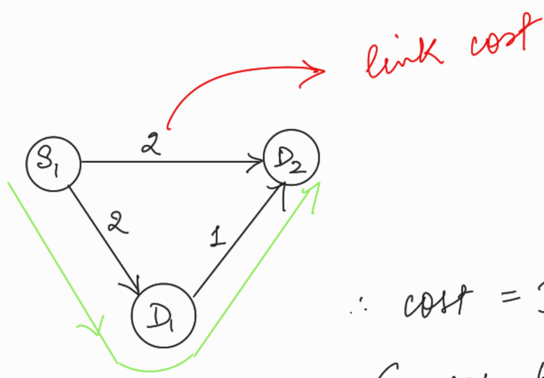
(1) Source based tree

- consist of a rootnode & childnode. Both are connected via a link at a time
- $G(V,E)$: $V \rightarrow$ vertex $E \rightarrow$ edges
- $S_1, \dots S_n$: source and $D_1, \dots D_n$: destination

⇒ Stiener Tree

- min. total cost of tree

optimisation goal: optimise cost of tree

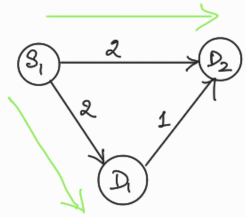


∴ cost = 3
(covers both dest)

⇒ Shortest path tree

here min the max cost to each destination.

$\therefore$ cost = 2



(2) Shared core tree

- for this, rather than considering one tree for each src - dest pair, a single tree can be considered with all diff dest. This is acheived through the concept of representative node (nodes excluding src & dest node)

- if a single represented node / core is present, it can be lost due to decay of battery & then the tree structure is invalid. To avoid this multi core share tree is used.

- The path here may not be the shortest path & failure of link is also possible here, making the tree not redundant. This can cause improper routing. Hence providing multiple no of links in tree to over come this is done. This is mesh.

Geographic Routing

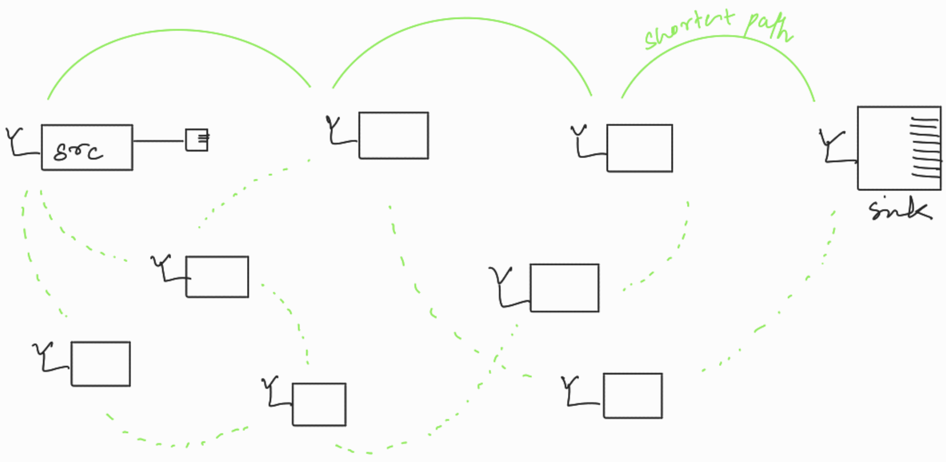
- it is a type of multicast routing. Types - geocasting, position based routing

sending data to any arbitrary node in a geographic region

here -ve position of sensor node & neighbours is used

(1) Position based Routing

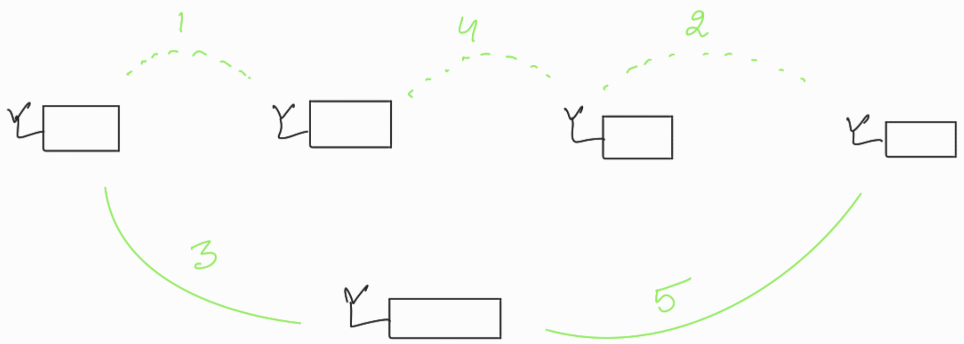
⇒ Most forwarded with 'r'



We use the greedy approach. It takes the min distance path

- Here each sensor & neighbourhood position is known, thus it can find the direct / min distance path for data routing.

- The less no of hops doesnt mean that the cost is also less



- formula for finding next hop –

$$\text{next hop}(v) = \arg(\min\{ud\})$$

distance b/w src and destination

- Also there is a chance of collision & noise here. To avoid this, nearest with forward progress used to max the hops. & it min. collision.

here we first jump to nearest node & then apply the greedy approach

⇒ Directional Routing

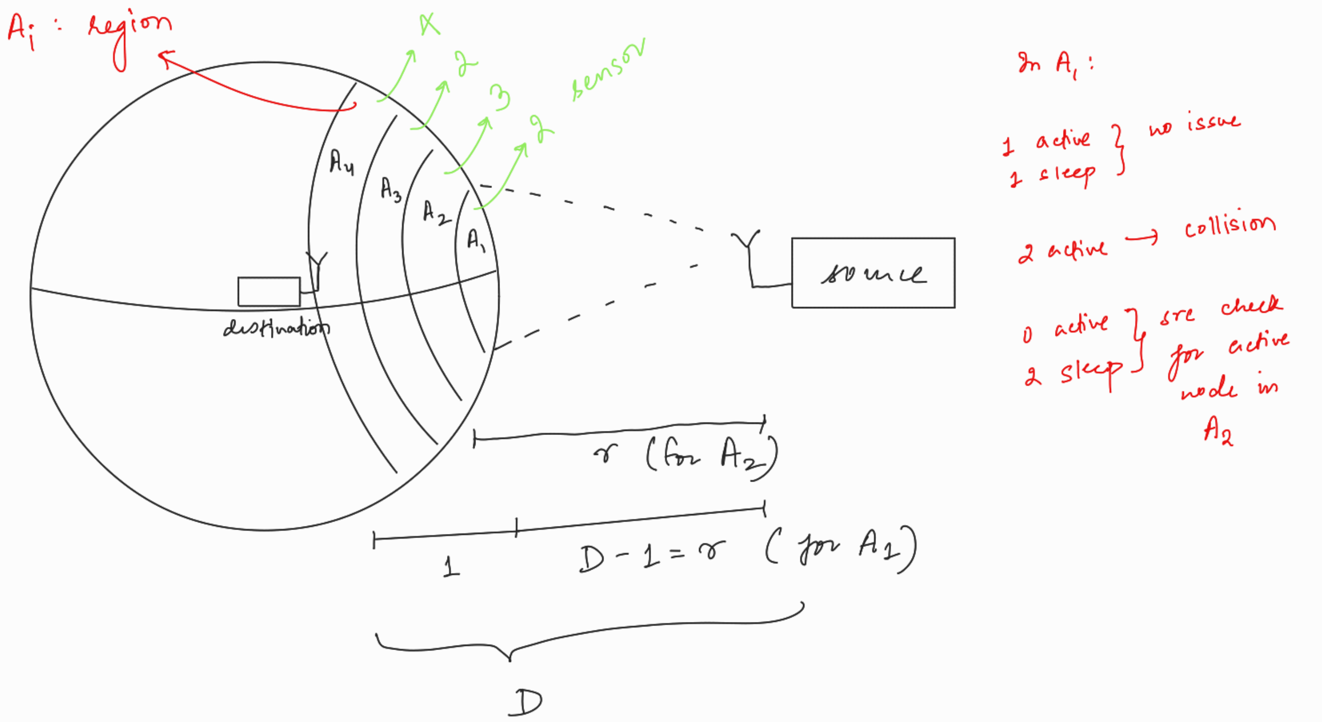
- it is another possibility to forward data to nodes that are close in dir^n rather than cost.

- in all above problem, the issue is "problem of dead end".

'if there is a huge obstacle in direct path b/w src & dest. Even if src & dest are connected, there is loss of data.

⇒ Randomized forwarding & adaptive node activity

- Adaptiveness is needed coz of varying topology of WSN.

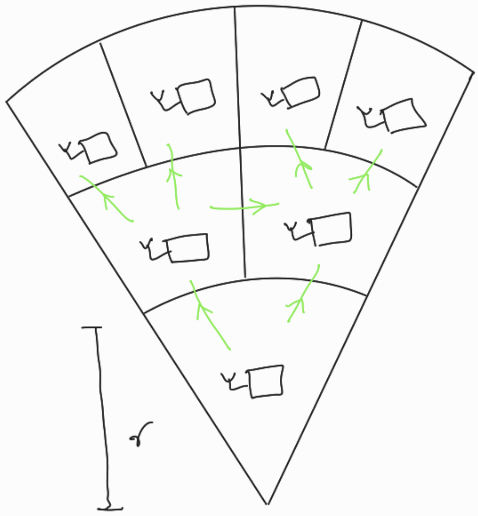


The problem of varying topology can be taken care of via this random strategy. Since neighbourhood node has no idea of other node, thus it will check for active nodes. If intersecting region is A_i b/w src & dest. then first S_1 broadcast to A_1. If one node is active in A_1, that node will forward to A_2. If both are active, then there is collision which is taken care of & then forwarded to A_2. Again A_2 forward to A_3 & so on.

The annual radius (r) = $D - 1 + \frac{(i-1)}{N}$ where $i \in [1, N]$

⇒ Geographic Routing with positions

- here virtual location is found rather than actual location of sensor & neighbourhood, to facilitate routing



virtual location is found via polar coordinate system. → radius & angle

if hop ↑ ⇒ radius ↑

- The radius calculation is easy & is found that no of hops dist from sender to R_x. Denoted as 'r'.

- Angle is calculated in range $[\alpha, \beta]$ for a node. Thus if the subtrees (associated with v) are $S_1 \ldots S_n$, then range of angle is —

$$\left[\alpha + (\beta - \alpha) \cdot \frac{S_1 + S_2 + \ldots S_{i-1}}{S_1 + S_2 + \ldots S_N},\ \alpha + (\beta - \alpha) \cdot \frac{S_1 + S_2 + \ldots S_i}{S_1 + S_2 + \ldots S_N}\right]$$

(2) Geocasting

- sending data from a node to any arbitrary intermediate node in a geographic region.
- it is also multicasting.

⟹ LMB protocol

- has forwarding & restricting zone where node will transmit pckts that are received.
  - → Static zone : smallest zone b/w src - dest.
  - → Adaptive " : zone adapted by neighbourhood of sender.
  - → " distance
- This scheme recomputes in each step on the basis of destination region info and coordinates of prev. hop.

Note - technique for geocasting :

(i) Voronoi diagram
(ii) Tesellating the plane
(iii) Mesh based geocasting
(iv) Geocasting using unicast protocol
(v) projecting based forwarding

Ch- Transport Layer and Quality of Services

• Users of internet are worried about application whereas users of WSN are concerned about the sensor event. ∴ Accuracy of event detection is imp.

Users of internet & WSN have issues like jitter, Quality of service, delay, packet error, etc.

• Transport layer is used to design and manage protocols to transport data.

• Basic criteria –

(i) coverage area (area ↑ ⇒ event detection ↑ ⇒ QoS ↑)
(ii) deployment ↑ ⇒ detection ↑

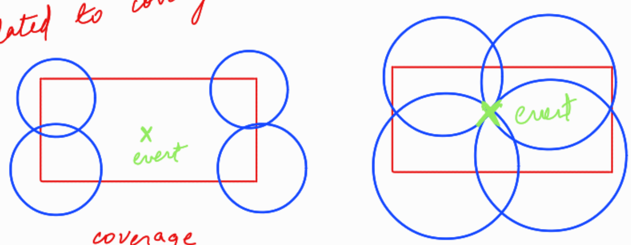
QoS is broadly defined wrt coverage area.

QoS / Reliability

• Reliability in WSN has many dirⁿ –

(i) detection ability (high)

related to coverage area



coverage low

coverage high

(ii) Information correctness (high)

the data generated from sensor should be noise free & free from outliers.

(iii) Reliable data transport (high)

sensor to sink

sink to sensor

(application code sent from sink to sensor)

Tasks of transport protocol

(1) Reliable data transport — pckt need to be error free

(2) flow control — controlling the speed of data transmission from Tx, so that Rx has free buffer space to gather the data.

(3) congestion control — if more pckt are sent than the network can carry. Thus network drops few pkts

congestion problem

(4) Network abstraction — generally transport layer has programming interface of application layer which reduces the complexity in application

• Challenges for Transport protocol are due to homo ereons multihop operation of WSN with energy & computational constraints along with topology variations

Sensing Model

• Sensing model
  - deterministic
    - boolean
    - general
  - random (pratical)

• The sensing models are defined on basis of Quality, directionality, variability in o/p of sensor

eg. today temp at 10 am is 21°C. tomorrow at 10 am temp is 25°C

∴ variability

dist ↑ ⇒ Quality of data ↓

practical sensing ability of sensor

(1) Boolean Sensing Model

Boolean → 2 value : high or low

- $S(p,q) = \begin{cases} \underbrace{\alpha}_{\text{constant}} ; & \| \underbrace{p}_{\text{sensor point}} - \underbrace{q}_{\text{event point}} \|_2 < r \\ 0 ; & \text{otherwise} \end{cases}$

$\|p-q\|_2$ → distance b/w 2 pts, p and q

α is the value of data provided by the sensor

(2) General Sensing Model

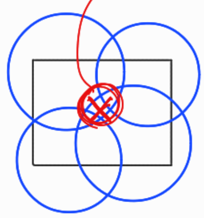
- $$S = \begin{cases} \dfrac{\alpha}{\|p-q\|_2^{\beta}} ; & r_0 \leqslant \|p-q\|_2 \leqslant r \\ 0 ; & \text{otherwise} \end{cases}$$

β : depends on sensor parameter & sensing technology

Coverage measures

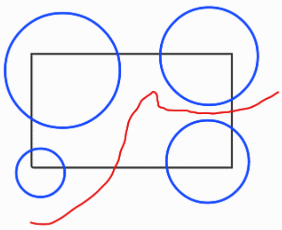
coverage measures

- k coverage : coverage becomes $k \cdot \alpha$ ← best case coverage



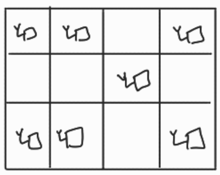
event

- worst case coverage : min coverage region which allow intrusion mech to take a path in sensor network.



intrusion path

- coverage of grid deployment :



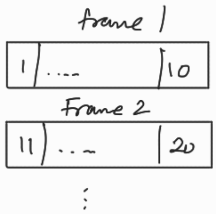
each sensor in middle of grid has the coverage of that grid.

Reliable Data transport

- Transmission Error : handled by error reduction techniques
  congestion : handled by congestion control technique
  flow control : " flow "

Reliability Requirement

- Data needs to be correctly transmitted
  - packet : transmission b/w 2 sensor nodes
  - frame : " single or multiple nodes
    code block : "
  - stream (pkt are continuously arriving)



Guaranteed vs Stoicastic delivery

- We have 'm' packets —
  - ↳ guaranteed : — more overhead
    — all pkt to be delivered successfully
  - ↳ stocastic : — n pkt (for each k block) min to deliver successfully
    $(n < m)$