

UNIT-IV

i) Dissemination protocols for large Sensor networks:

Dissemination protocols in a large sensor network typically take a data-centric paradigm in which the communication primitives are organised around the sensing data instead of the network nodes.

i) Declarative Routing protocol

DRP achieves energy efficiency through in-network aggregation. It uses reverse path forwarding to establish a routing tree for each sink to receive data reports from all other nodes. It also exploits the application-specific property of sensor networks to build a cross-layer declarative service for better efficiency.

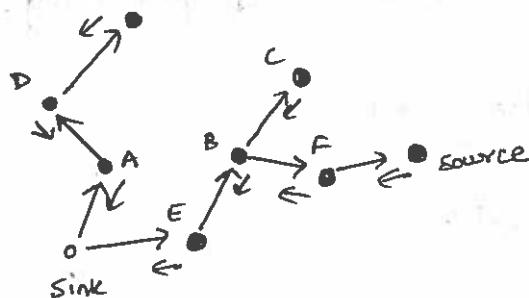


fig. Reverse path forwarding approach.

ii) Receiver-decided protocols

GRad uses hop Count as the cost. A sink builds its cost-field by flooding a REQUEST message. A source broadcasts a report; all neighbors with smaller costs forward the report. This process is repeated, and multiple-copies of the report travel within a forwarding mesh of intermediate nodes towards the sink.

iii) Sender-appointed protocol

EAR achieves load balancing among multiple paths to extend the system lifetime. A node makes forwarding decision probabilistically among neighbors. A node N_a keeps one energy cost $C_{a,i}$ for each of the neighbors N_i from which an ADV is received. It assigns a probability p_i inverse proportional to each of these neighbors. When sending a report it selects one of probability.

iv) Routing with virtual hierarchy

Two-tier data dissemination

Sink mobility brings new challenges to large-scale sensor network. Both reverse-path and cost-field based approaches requires mobile sinks.

2)

Data dissemination

A data dissemination is a process by which data and queries for data are routed in the sensor n/w. In a scope of data dissemination, a source is the node that generates the data and an event is the information to be reported. A node that is interested in data is called sink and the interest is a descriptor for some event.

Methods

1. Flooding
2. Gossiping
3. SPIN
4. cost - field Approach.

1. Flooding :-

In flooding method each sensor node that receives a packet broadcasts it to its neighbors assuming that node itself is not the destination of the packet and the maximum hop count is not reached. This ensures that the data and queries for data are sent all over the network.

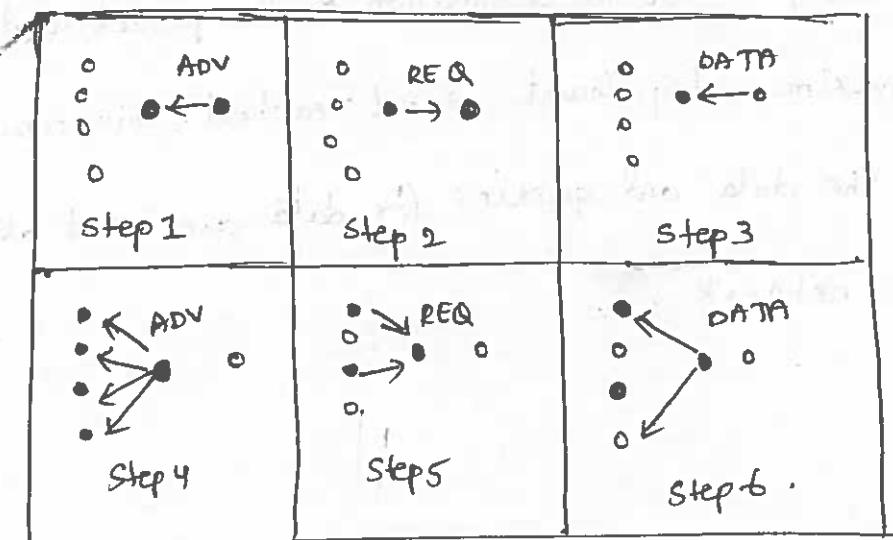
2. Gossiping :

Gossiping method is based on flooding, but node that receives the packet forwards it only to a single randomly selected neighbor instead of sending it to all neighbors.

The advantage of gossiping is that it avoids the problem of implosion and it does not waste as much network resources as flooding. The biggest disadvantage of gossiping is that since neighbor is selected randomly some nodes may not receive the message at all.

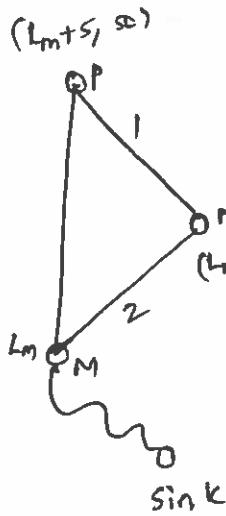
3. SPIN :

Sensor protocols for Information via Navigation use negotiation and resource adaption to address the disadvantages of basic flooding. SPIN uses data-centric routing, nodes are advertising their data and they will send the data after receiving a reply from interested nodes. SPIN uses three types of messages : ADV, REQ and DATA .

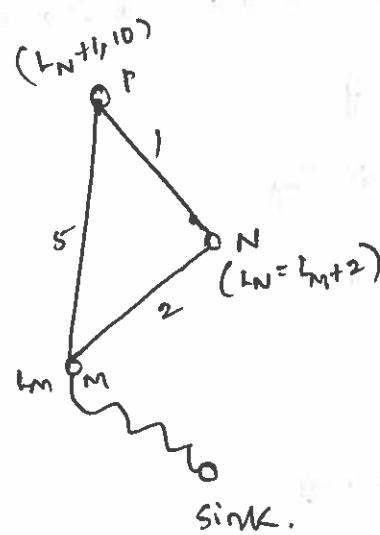


4. Cost-field Approach :-

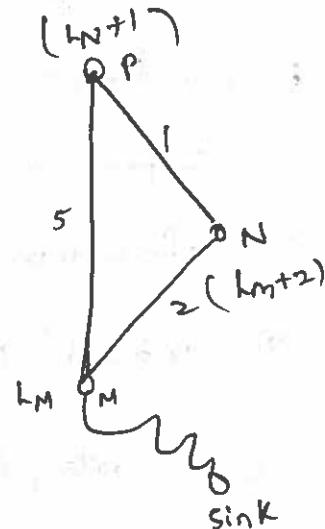
The aim of the cost-field approach is to solve problem of setting paths to the sink. The cost-field approach is a two-phase process, first the cost-field is set-up in all sensor nodes, based on the some metric like a delay. In the second phase, data is disseminated using the costs. The cost at each node is the minimum cost from the node to the sink, which occurs on the optimal path.



a) Time T , after M 's ADV



b) Time $T+20$
after N 's ADV



c) Time $T+30$,
after P 's ADV.

3)

Data Gathering

Data gathering is one of the primary operations carried out in WSNs. It involves data collection with aggregation and data collection without aggregation, referred to as data aggregation and data collection respectively.

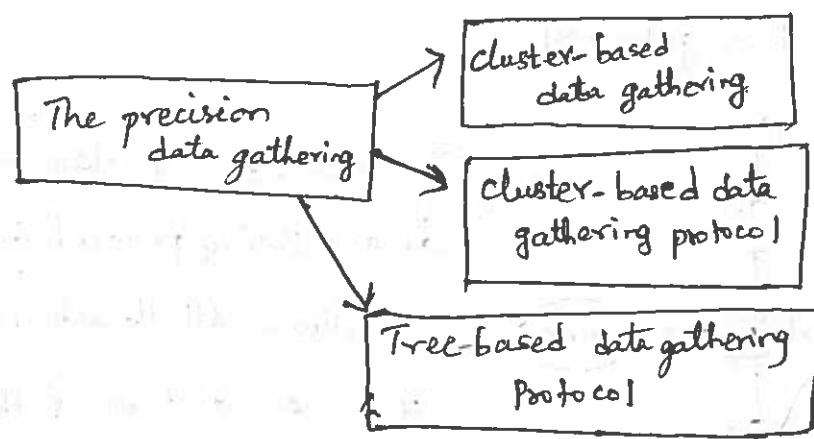
The main aim of data gathering is to reduce energy consumptions in WSNs by exploiting correlations among sensory data. The techniques are:-

- i) signal processing
- ii) compressive sensing
- iii) information theory
- iv) networking.

Precision data gathering mode:-

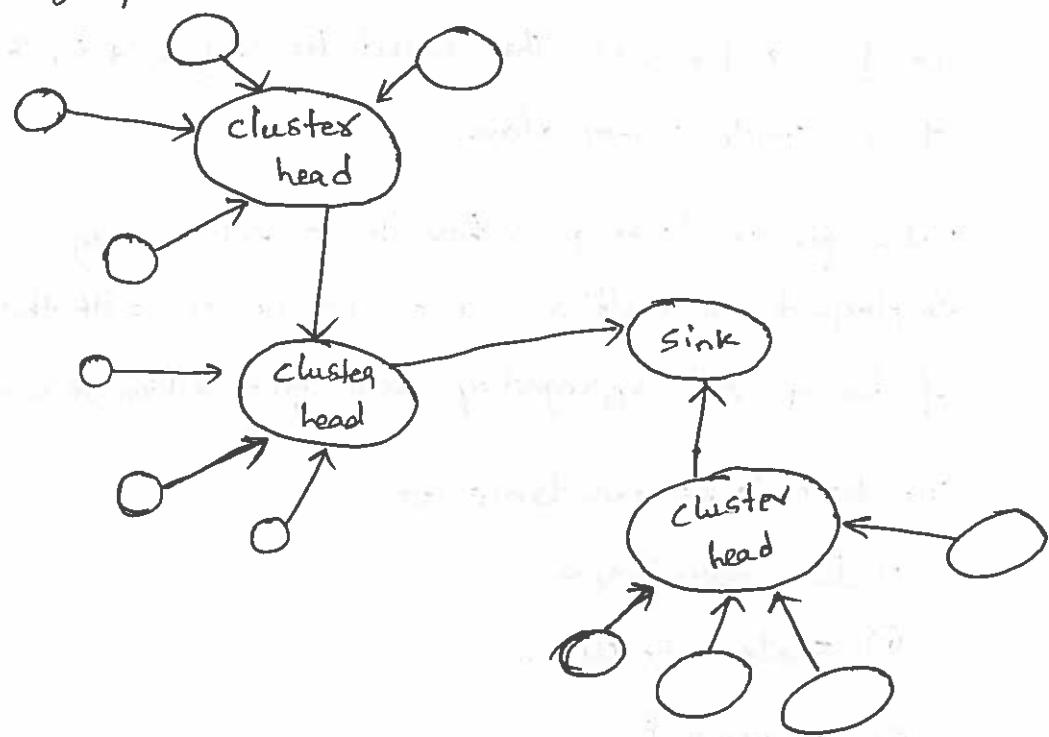
As the nodes in WSNs constantly sensing data all the time. The easiest way is to transfer all the sensor data to the sink node directly. However, they will accelerate the dissipation of energy of each node.

Correlated data gathering mode:-

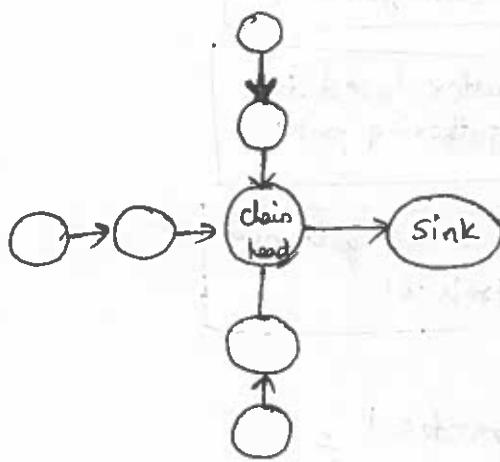


cluster-based data gathering protocol :

In order to reduce the communication cost caused by all the nodes frequently interact with sink, cluster-based, chain-based and tree-based data gathering protocol. While, the last protocol can be subdivided into centralized and distributed data gathering protocol.



chain-based data gathering



- The main idea of chain-based data gathering protocol is as follows. All the nodes consist of a chain and one of the nodes is selected and treated as the head node.

4)

Data Fusion:

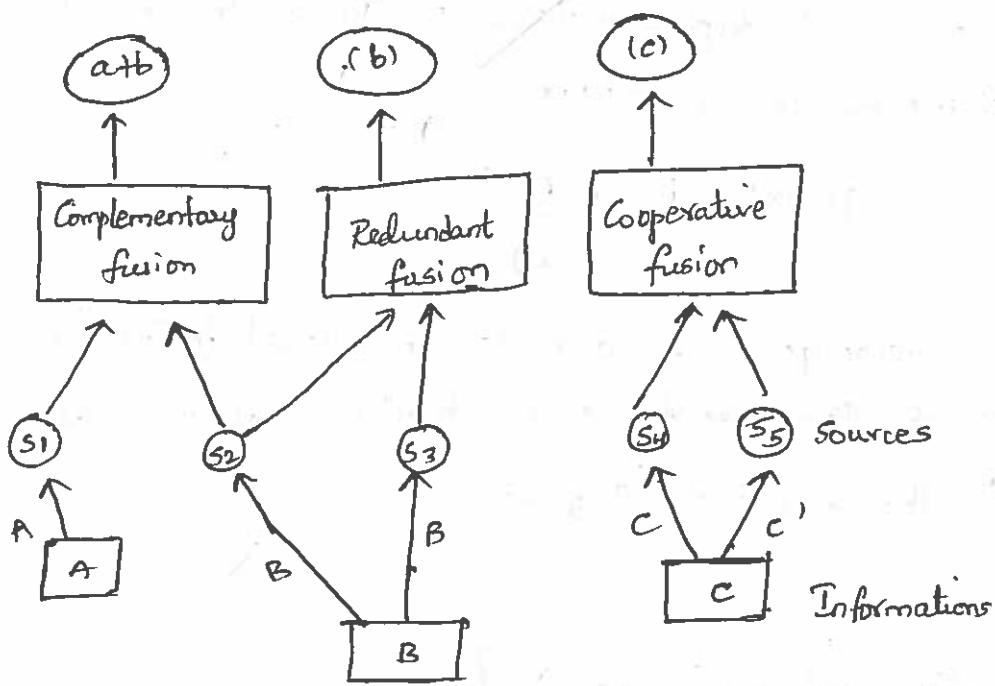
Data fusion techniques combine data from multiple sensors and related information from associated databases to achieve improved accuracy and more specific inferences than could be achieved by the use of a single sensor alone."

Data fusion techniques have been extensively employed on multisensor environments with the aim of fusing and aggregating data from different sensors

The techniques available are:-

- i) data association
- ii) state estimation.
- iii) decision fusion.

Data fusion classification by Whyte's



i) Data Association :

The data association problem must determine the set of measurements that correspond to each target.

- i) each sensor's observation is received in the fusion node at discrete time intervals.
- ii) the sensor might not provide observations at a specific interval.
- iii) some observations are noise, .

ii) state-estimation methods :

This method aims to determine the state of the target under movement. given the observation or measurements state estimation techniques are also known as tracking techniques.

iii) Decision fusion :-

A decision is typically taken based on the knowledge of the perceived situation.

$$P(Y/x) = \frac{P(x|y) P(y)}{P(x)}$$

These techniques aim to make a high-level inference about the events and activities that are produced from the detected targets.

5)

Quality of a Sensor Network

- The purpose of a sensor network is to monitor and report events take place in a particular area.
- Hence, the main parameters which defines how well the network observes a given area "Coverage" and "exposure".

Coverage :

- Coverage is a measure of how well the network can observe or cover an event.
- The worst-case coverage defines area of breach where coverage is the poorest. This can used to improve the deployment of the network.
- The best-case coverage defines the areas of best coverage.

Worst-case :-

- The problem is to identify PB , the maximal breach path from I to F .
- PB is defined as the locus of points p in the region A , where p is in PB if the distance from p to the closest sensor is maximized.

Best-Case :-

- The problem is to identify PS , the maximum support path I to F .
- Delaunay triangulation, which obtain from voronoi diagram by connecting the sites.

Exposure :-

- Exposure is defined as the expected ability of observing a target in the sensor n/w.
- The sensing power of a node s at point p is modeled as.

$$S(s_{IP}) = \frac{A}{[d(s_{IP})]^k}$$

- All-sensor field Intensity: $I_A(F, p) = \sum_{i=1}^n S(s_i, p)$
- Conversion from Cartesian Coordinates

$$\frac{dp(t)}{dt} = \sqrt{\left(\frac{dx(t)}{dt}\right)^2 + \left(\frac{dy(t)}{dt}\right)^2}$$

6)

Security Protocols

.....

Security protocols and encryption prevents an attacker from tapping into the air and reading data as it passes by. Some of the security protocols are

- i) WPA
- ii) WPA 2
- iii) PEAP
- iv) PEAP-MS-CHAP v2
- v) EAP-TLS

i) WPA

Considered older technology and the least secure of the wireless security protocols. Originally designed with a 40-bit key but now also supports a 104-bit key.

Created due to the vulnerabilities found in WEP.

ii) WPA 2:

The newest of the standards, launched in 2004, WPA 2, is the most secure standard. It supports 802.1x/EAP authentication but also includes support.

for AES encryption. WPA2 require implementers to purchase new hardware.

iii) PEAP :-

Open standard for transmitting encrypting authentication information across wireless networks. Uses only server-side public keys to authenticate wireless clients.

iv) PEAP-MS-CHAP v2 :-

Wireless authentication protocol where wireless clients can use Active Directory accounts and passwords to authenticate to a wireless n/w.

v) EAP-TLS :-

wireless authentication protocol where clients can authenticate to the wireless network using certificates or even smart cards.

to work with you & my wife now? No - if

you can't get me a job, I'll go elsewhere

and you can't get me a job, I'll go elsewhere

what's the difference between us & the rest?

What's the difference between us & the rest?