Routing Challenges and Design Issues in WSNs

Overview

- The design of routing protocols in WSNs is influenced by many challenging factors. These factors must be overcome before efficient communication can be achieved in WSNs.
  - **Node deployment**
  - **Energy considerations**
  - **Data delivery model**
  - **Node/link heterogeneity**
  - **Fault tolerance**
  - **Scalability**
  - **Network dynamics**
  - **Transmission media**
  - **Connectivity**
  - **Coverage**
  - **Data aggregation**
  - **Quality of service**

Node Deployment

- Node deployment in WSNs is application dependent and affects the performance of the routing protocol.
- The deployment can be either deterministic or randomized.
- In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths.
- In random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

Energy Considerations

- Sensor nodes can use up their limited supply of energy performing computations and transmitting information in a wireless environment. Energy conserving forms of communication and computation are essential.
- In a multi-hop WSN, each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and might require rerouting of packets and reorganization of the network.

Data Delivery Model

- Time-driven (continuous)
  - Suitable for applications that require periodic data monitoring
- Event-driven
  - React immediately to sudden and drastic changes
- Query-driven
  - Respond to a query generated by the BS or another node in the network
- Hybrid
- The routing protocol is highly influenced by the data reporting method

Node/Link Heterogeneity

- Depending on the application, a sensor node can have a different role or capability.
- The existence of a heterogeneous set of sensors raises many technical issues related to data routing.
- Even data reading and reporting can be generated from these sensors at different rates, subject to diverse QoS constraints, and can follow multiple data reporting models.

Fault Tolerance

- Some sensor nodes may fail or be blocked due to lack of power, physical damage, or environmental interferences
- It may require actively adjusting transmission powers and signaling rates on the existing links to reduce energy consumption, or rerouting packets through regions of the network where more energy is available

Scalability

- The number of sensor nodes deployed in the sensing area may be on the order of hundreds or thousands, or more.
- Any routing scheme must be able to work with this huge number of sensor nodes.
- In addition, sensor network routing protocols should be scalable enough to respond to events in the environment.

Network Dynamics

- Routing messages from or to moving nodes is more challenging since route and topology stability become important issues
- Moreover, the phenomenon can be mobile (e.g., a target detection/ tracking application).

Transmission Media

- In general, the required bandwidth of sensor data will be low, on the order of 1-100 kb/s. Related to the transmission media is the design of MAC.
  - TDMA (time-division multiple access)
  - CSMA (carrier sense multiple access)

Connectivity

- High node density in sensor networks precludes them from being completely isolated from each other.
- However, may not prevent the network topology from being variable and the network size from shrinking due to sensor node failures.
- In addition, connectivity depends on the possibly random distribution of nodes.

Coverage

- In WSNs, each sensor node obtains a certain view of the environment.
- A given sensor's view of the environment is limited in both range and accuracy.
- It can only cover a limited physical area of the environment.

Data Aggregation

- Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated to reduce the number of transmissions.
- Data aggregation is the combination of data from different sources according to a certain aggregation function.

Quality of Service

- In many applications, conservation of energy, which is directly related to network lifetime.
- As energy is depleted, the network may be required to reduce the quality of results in order to reduce energy dissipation in the nodes and hence lengthen the total network lifetime.

Routing Protocols in WSNs: A taxonomy

Routing protocols in WSNs

Network Structure

Flat routing
- SPIN
- Directed Diffusion (DD)

Hierarchical routing
- LEACH
- PEGASIS
- TTDD

Location based routing
- GEAR
- GPSR

Protocol Operation

Negotiation based routing
- SPIN

Multi-path network routing
- DD

Query based routing
- DD, Data centric routing

QoS based routing
- TBP, SPEED

Coherent based routing
- DD

Aggregation
- Data Mules, CTCCAP

Flat Routing

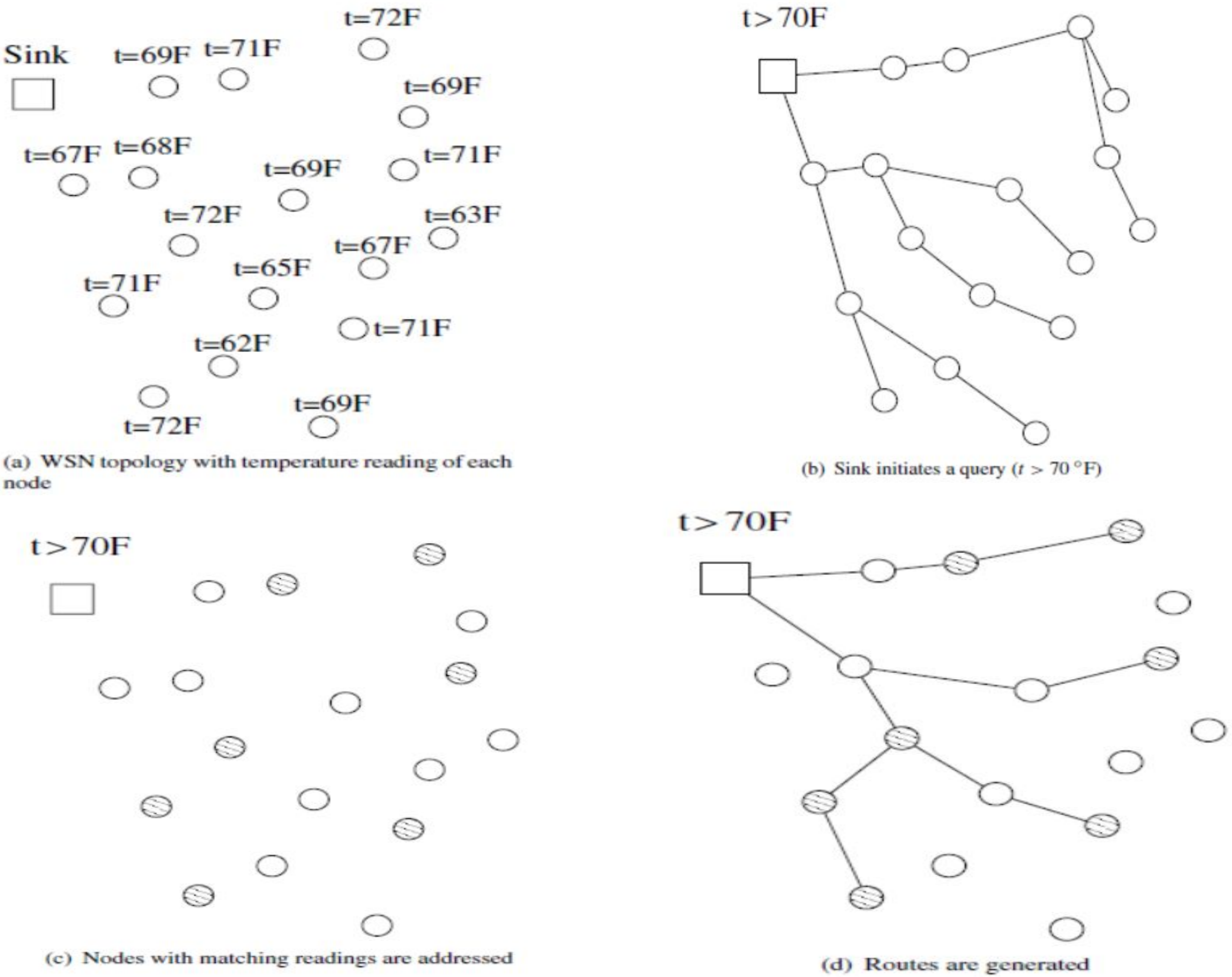
Overview

- In flat network, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task.
- Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data.
- Prior works on data centric routing, e.g., SPIN and Directed Diffusion, were shown to save energy through data negotiation and elimination of redundant.

- It is hard to assign specific IDs to each of the sensor in WSN because of their large numbers.

- Hence, address-based routing protocols are not preferred for WSNs. Thus, datacentric routing is preferred .

- As an example, “the areas where the temperature is over 70 ◦F (21 ◦C)” is a more common query than “the temperature read by a certain node.” Attribute-based naming is used to carry out queries by using the attributes of the phenomenon.



(a) WSN topology with temperature reading of each node

(b) Sink initiates a query ($t > 70\,^{\circ}$F)

(c) Nodes with matching readings are addressed

(d) Routes are generated

Flooding

- Flooding is the classic approach for dissemination without the need for any routing algorithms and topology maintenance.
- Source node sends data to all neighbors Receiving node stores and sends data to all its neighbors Disseminate data quickly.

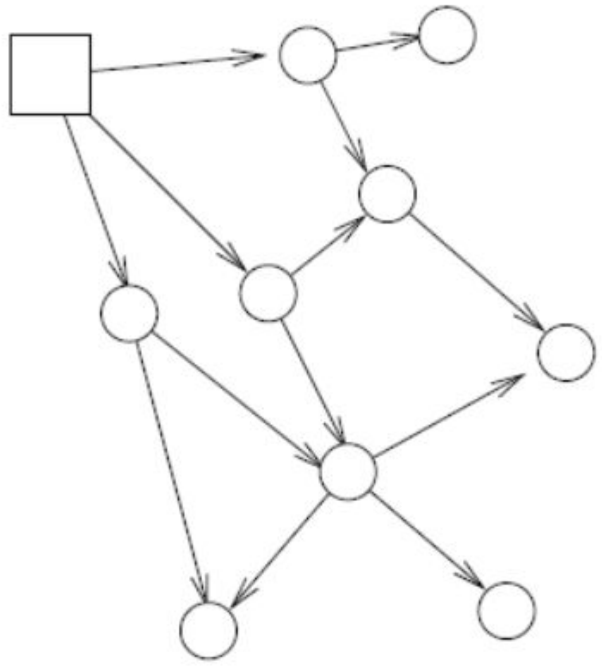
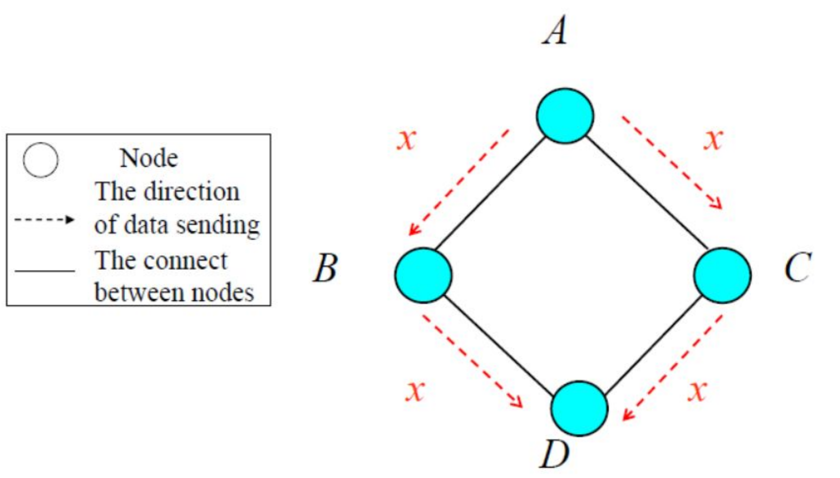


Figure 7.3 Flooding.

Flooding Drawbacks

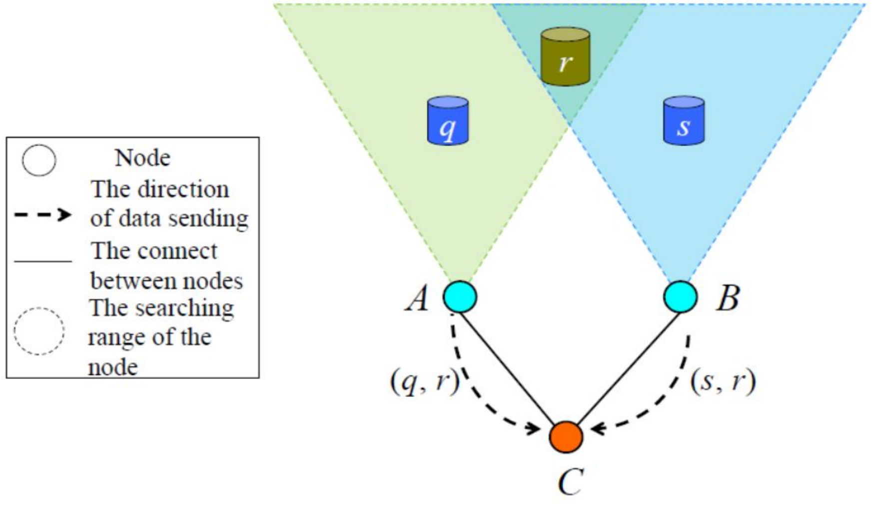
- Implosion

Duplicated messages are usually sent to the same node or multiple copies of the same packet traverse the network



- Overlap

Two nodes have overlapping sensing regions, then both of them may sense the same stimuli at the same time.



- Resource Blindness: Consumes much energy and bandwidth.

Gossiping

- Gossiping avoids implosion by selecting a single node for packet relaying.
- As a result, whenever a node receives a packet it does not broadcast the packet but selects a random node among its neighbors and forwards the packet to that particular node.
- Once the neighbor node receives the packet, it randomly selects another sensor node.
- It avoids the implosion problem by just having one copy of a message at any node, it increases the latency in propagating the message to all sensor nodes.
- Flooding and/or gossiping techniques can still be used by recent
- routing protocols for specific functions.
- As an example, during the deployment phase, the sink can use flooding or gossiping protocols to determine the active nodes. Similarly, during sensor network initialization, limited flooding can be used to gather information from neighbors in close proximity.

SPIN

Sensor Protocols for Information via Negotiation

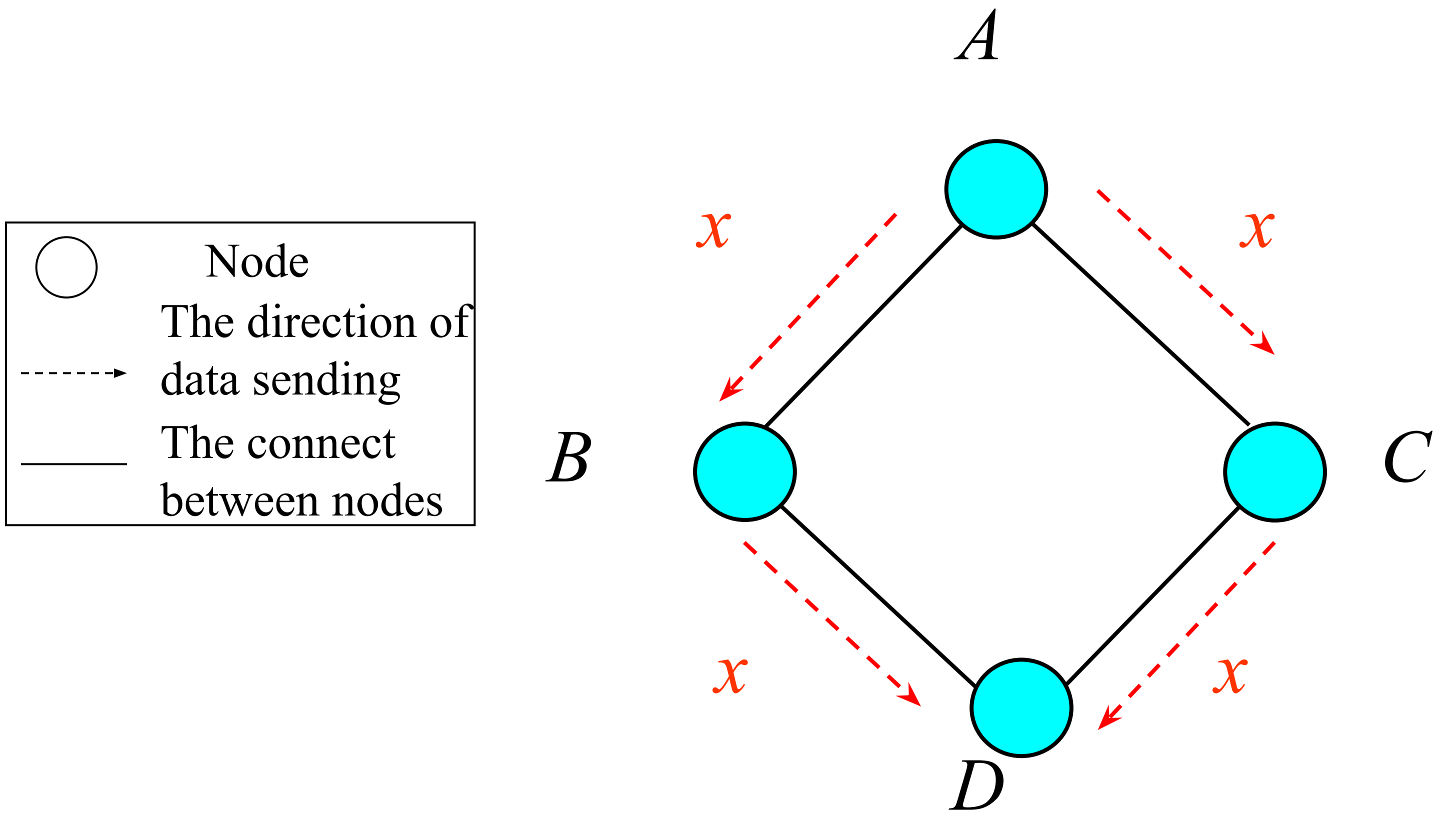
SPIN -Motivation

- Sensor Protocols for Information via Negotiation, SPIN
  - A Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks.
- Dissemination is the process of distributing individual sensor observations to the whole network, treating all sensors as sink nodes
  - Replicate complete view of the environment
  - Enhance fault tolerance
  - Broadcast critical piece of information

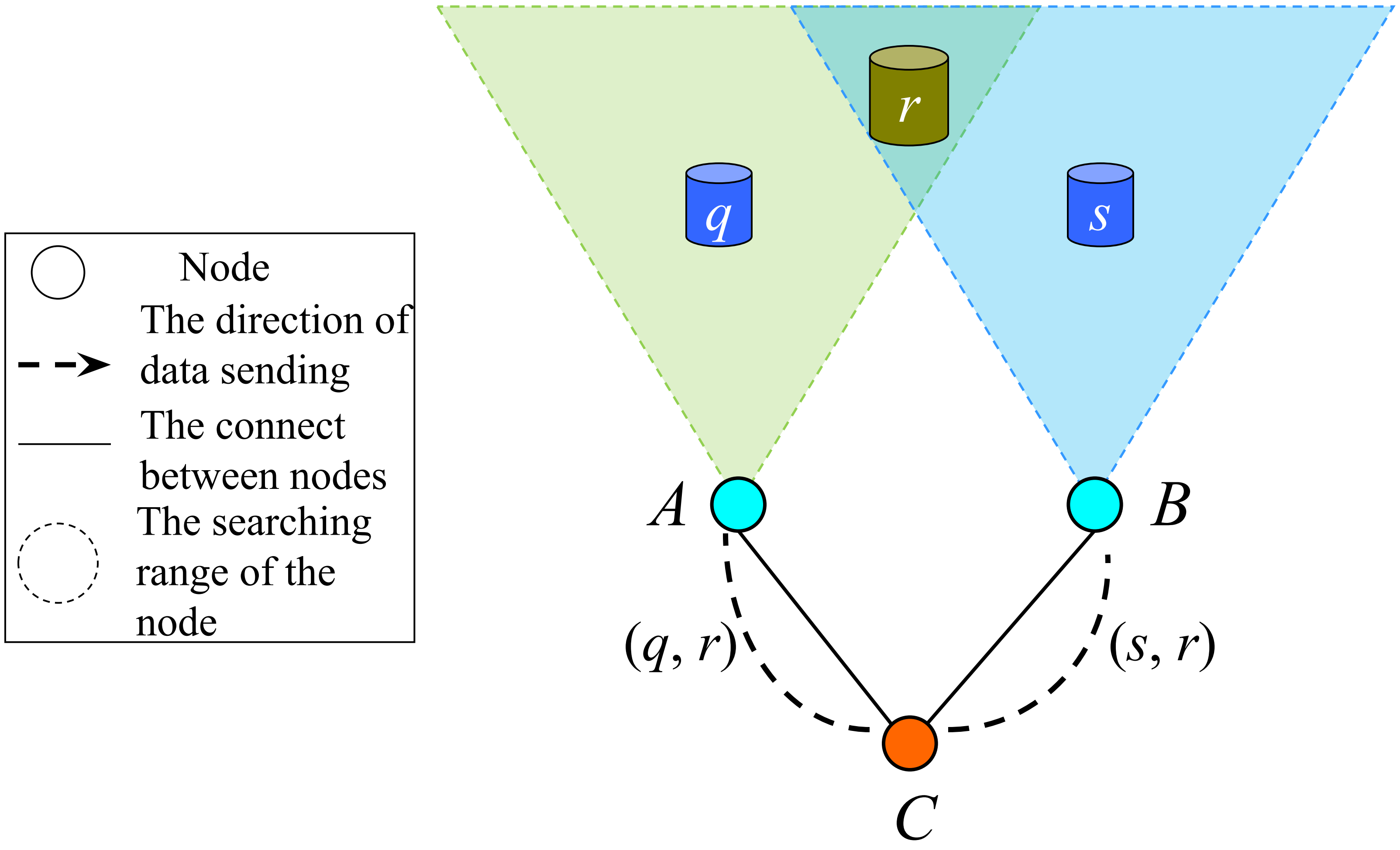
SPIN (cont.)- Motivation

- Flooding is the classic approach for dissemination
- Source node sends data to all neighbors
- Receiving node stores and sends data to all its neighbors
- Disseminate data quickly
- Deficiencies
  - Implosion
  - Overlap
  - Resource blindness

SPIN (cont.)-Implosion



SPIN (cont.)- Overlap



SPIN (cont.)- Resource blindness

- In flooding, nodes do not modify their activities based on the amount of energy available to them.

- A network of embedded sensors can be resource-aware and adapt its communication and computation to the state of its energy resource.

SPIN (cont.)

- Negotiation
  - Before transmitting data, nodes negotiate with each other to overcome implosion and overlap
  - Only useful information will be transferred
  - Observed data must be described by meta-data
- Resource adaptation
  - Each sensor node has resource manager
  - Applications probe manager before transmitting or processing data
  - Sensors may reduce certain activities when energy is low

SPIN (cont.)- Meta-Data

- Completely describe the data
  - Must be smaller than the actual data for SPIN to be beneficial
  - If you need to distinguish pieces of data, their meta-data should differ
- Meta-Data is application specific
  - Sensors may use their geographic location or unique node ID
  - Camera sensor may use coordinate and orientation

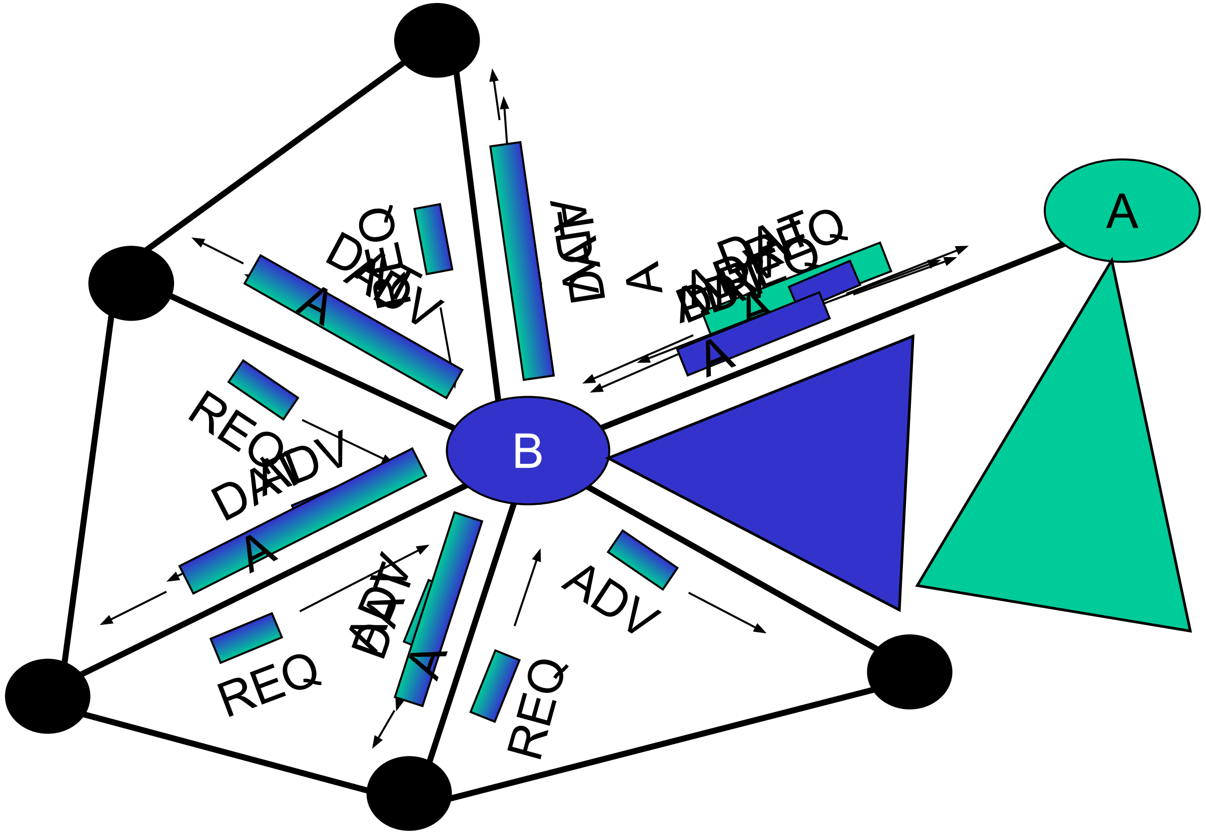
SPIN (cont.)- SPIN family

- Protocols of the SPIN family
  - SPIN-PP
    - It is designed for a point to point communication, i.e., hop-by-hop routing
  - SPIN-EC
    - It works similar to SPIN-PP, but, with an energy heuristic added to it
  - SPIN-BC
    - It is designed for broadcast channels
  - SPIN-RL
    - When a channel is lossy, a protocol called SPIN-RL is used where adjustments are added to the SPIN-PP protocol to account for the lossy channel.

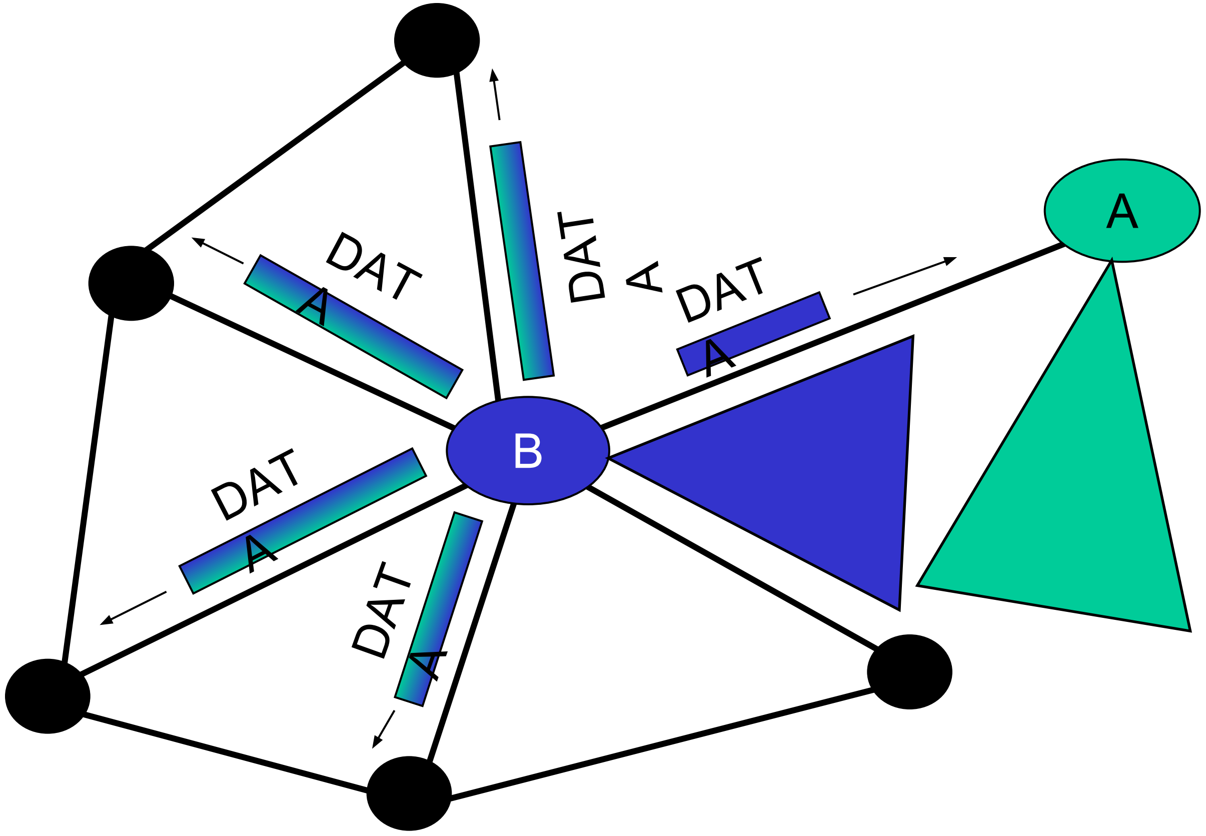
SPIN (cont.)- Three-stage handshake protocol

- SPIN-PP: A three-stage handshake protocol for point-to-point media
  - ADV – data advertisement
    - Node that has data to share can advertise this by transmitting an ADV with meta-data attached
  - REQ – request for data
    - Node sends a request when it wishes to receive some actual data
  - DATA – data message
    - Contain actual sensor data with a meta-data header
    - Usually much bigger than ADV or REQ messages

SPIN (3-Step Protocol)

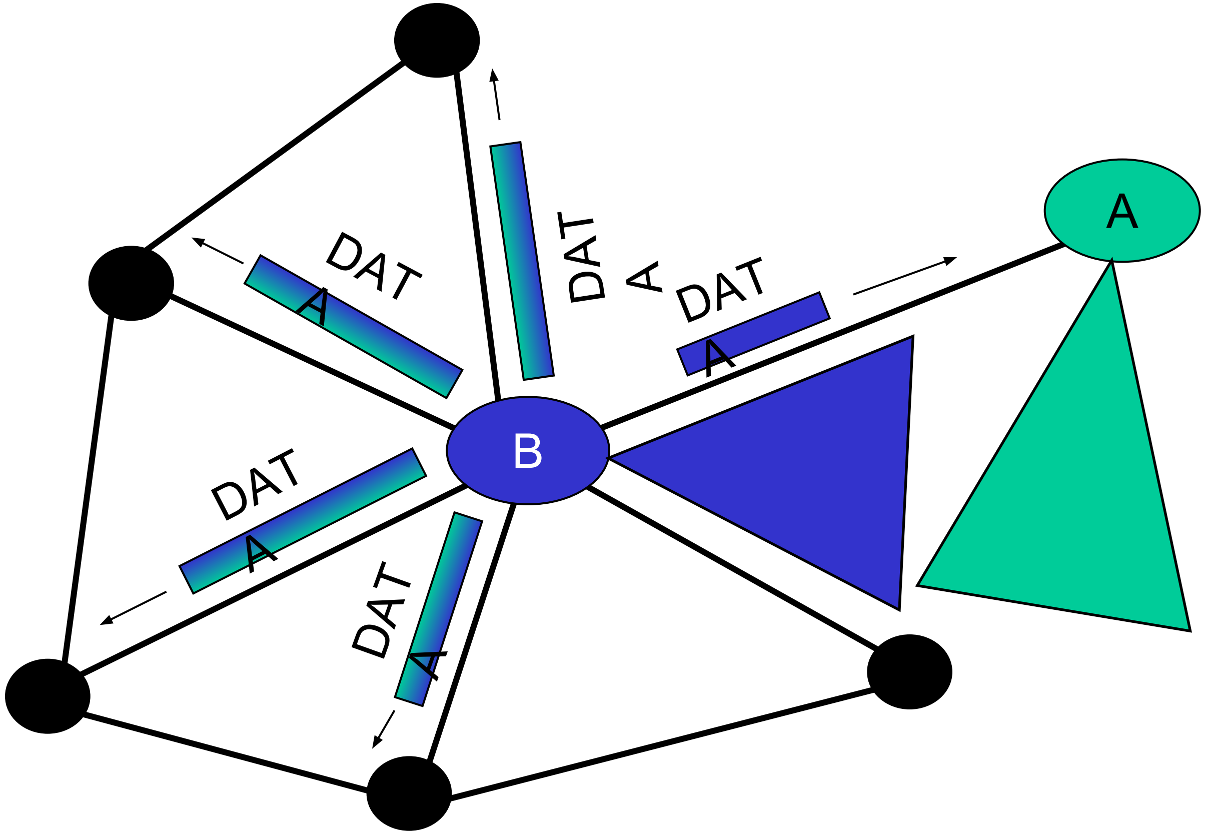


SPIN (3-Step Protocol)



Notice the color of the data packets sent by node B

SPIN (3-Step Protocol)



SPIN effective when DATA sizes are large :
REQ, ADV overhead gets amortized

SPIN (cont.)- SPIN-EC (Energy-Conserve)

- Add simple energy-conservation heuristic to SPIN-PP
  - SPIN-EC: SPIN-PP with a low-energy threshold
- Incorporate low-energy-threshold
- Works as SPIN-PP when energy level is high
- Reduce participation of nodes when approaching low-energy-threshold
  - When node receives data, it only initiates protocol if it can participate in all three stages with all neighbor nodes
  - When node receives advertisement, it does not request the data
- Node still exhausts energy below threshold by receiving ADV or REQ messages

SPIN (cont.)- Conclusion

- SPIN protocols hold the promise of achieving high performance at a low cost in terms of complexity, energy, computation, and communication
- Pros
  - Each node only needs to know its one-hop neighbors
  - Significantly reduce energy consumption compared to flooding
- Cons
  - Data advertisement cannot guarantee the delivery of data
    - If the node interested in the data are far from the source, data will not be delivered
    - Not good for applications requiring reliable data delivery, e.g., intrusion detection

SPIN (cont.)- Reference

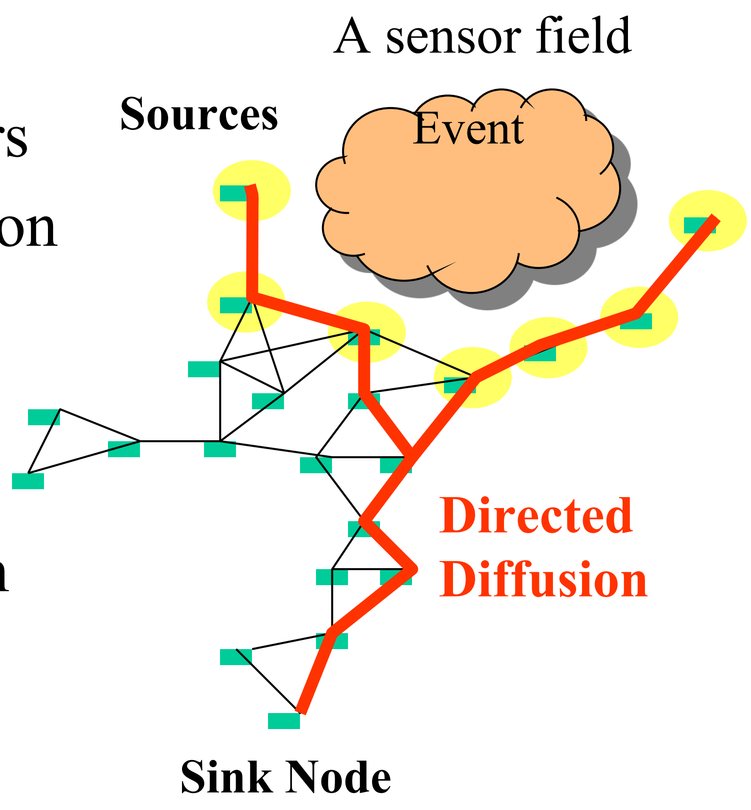
- J. Kulik, W.R. Heinzelman, and H. Balakrishnan, “Negotiation-based protocols for disseminating information in wireless sensor networks,” *Wireless Networks*, Vol. 8, pp. 169-185, 2002.

Directed Diffusion

A Scalable and Robust Communication Paradigm for Sensor Networks

Overview

- Data-centric communication
  - Data is named by attribute-value pairs
  - Different form IP-style communication
    - End-to-end delivery service
  - e.g.
    - How many pedestrians do you observe in the geographical region X?



Overview (cont.)

- Data-centric communication (cont.)
  - Human operator's query (task) is *diffused*
  - Sensors begin collecting information about query
  - Information returns along the reverse path
  - Intermediate nodes *aggregate* the data
    - Combing reports from sensors
- Directed Diffusion is an important milestone in the data centric routing research of sensor networks

Directed Diffusion

- Typical IP based networks
  - Requires unique host ID addressing
  - Application is end-to-end

- Directed diffusion – use publish/subscribe
  - Inquirer expresses an interest, *I*, using attribute values
  - Sensor sources that can service *I*, reply with data

Directed Diffusion (cont.)

- Directed diffusion consists of
  - Interest - Query which specifies what a user wants
  - Data - Collected information
  - Gradient
    - Direction and data-rate
    - Events start flowing towards the originators of interests
  - Reinforcement
    - After the sink starts receiving events, it reinforces at least one neighbor to draw down higher quality events

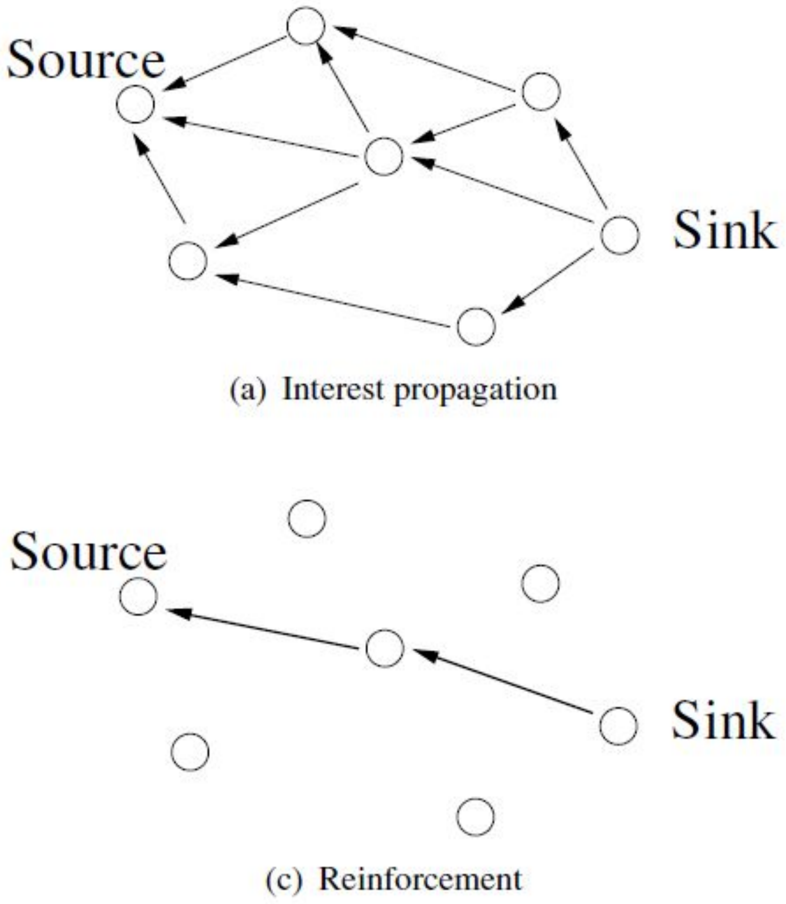


Figure 7.6 Operation of the directed diffusion protocol [14].

Data Naming

- Expressing an Interest
  - Using attribute-value pairs
  - e.g.,

```
Type = Wheeled vehicle      // detect vehicle location
Interval = 20 ms            // send events every 20ms
Duration = 10 s             // Send for next 10 s
Rect = [-100,100, 200,400]  // from sensors in this area
```

Interests and Gradients

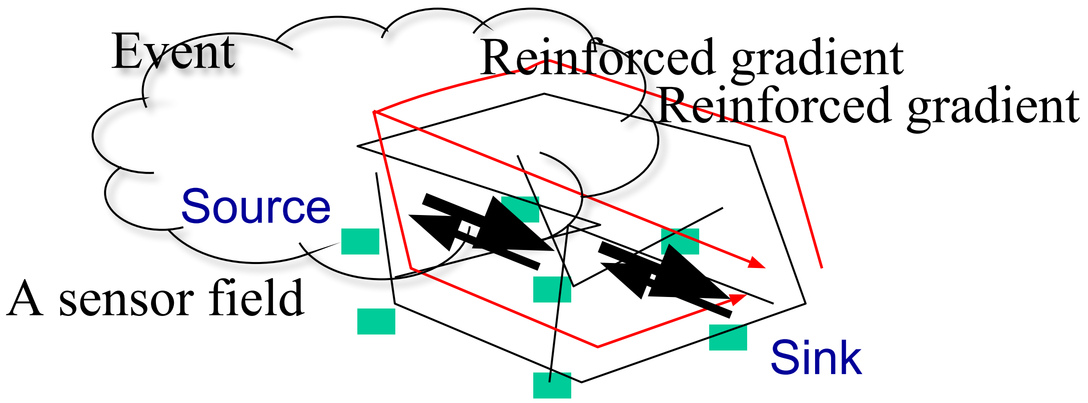
- Interest propagation
  - The sink broadcasts an interest
  - Neighbors update interest-cache and forwards it
    - Flooding
    - Geographic routing
    - Use cached data to direct interests
- Gradient establishment
  - Gradient set up to upstream neighbor
  - Low data-rate gradient
    - Few packets per unit time needed

Data Propagation

- A sensor node that detects a target
  - Search its interest cache
  - Compute the highest requested data-rate among all its outgoing gradients
  - Data message is unicast individually
- A node that receives a data message
  - Find a matching interest entry in its cache
  - Check the data cache for loop prevention
  - Re-send the data to neighbors

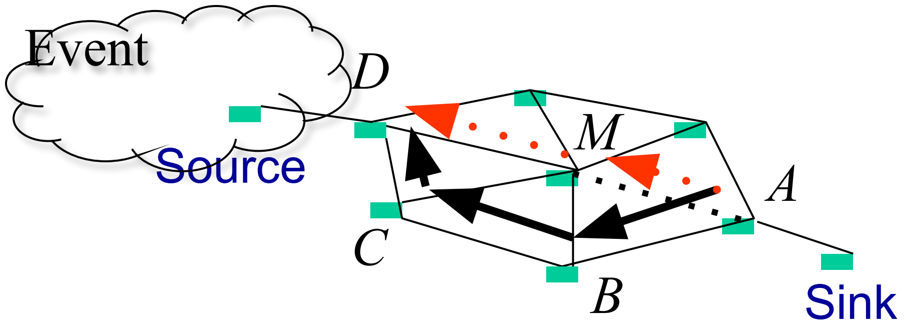
Reinforcement (1/4)

- Positive reinforcement
  - Sink selects the neighboring node
  - Original interest message but with high data-rate
  - Neighboring node must also reinforce at least one neighbor
  - Low-delay path is selected
  - Exploratory gradients still exist: useful for faults



Reinforcement (2/4)

- Path failure and recovery
  - Link failure detected by reduced rate, data loss
    - Choose next best link (i.e., compare links based on infrequent exploratory downloads)
- The sink sends reinforcement messages through a new path other than the current path. Negative reinforcement messages are sent through the current path to suppress data transfer through that path



Link *A*-*M* lossy
A reinforces *B*
B reinforces *C*
C reinforces *D*
or
A negative reinforces *M*
M negative reinforces *D*

Directed Diffusion: Pros & Cons

- Different from SPIN in terms of on-demand data querying mechanism
  - Sink floods interests only if necessary (lots of energy savings)
  - In SPIN, sensors advertise the availability of data
- Pros
  - Data centric: All communications are neighbor to neighbor with no need for a node addressing mechanism
  - Each node can do aggregation & caching
- Cons
  - On-demand, query-driven: Inappropriate for applications requiring continuous data delivery, e.g., environmental monitoring
  - Attribute-based naming scheme is application dependent
    - For each application it should be defined a priori
    - Extra processing overhead at sensor nodes

References

- C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks,” *in the Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks* (*MobiCom’00*), August 2000.
- C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, “Directed Diffusion for Wireless Sensor Networking,” IEEE/ACM Transactions on Networking, Vol. 11, No. 1, Feb. 2003.

Chapter 4.3
Hierarchical Routing

Overview

- In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing of the target.
- Hierarchical routing is mainly two-layer routing where one layer is used to select cluster heads and the other layer is used for routing.
- Hierarchical routing (or cluster-based routing), e.g., LEACH, PEGASIS, TTDD, is an efficient way to lower energy consumption within a cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the base stations.

LEACH

Low-Energy Adaptive Clustering Hierarchy

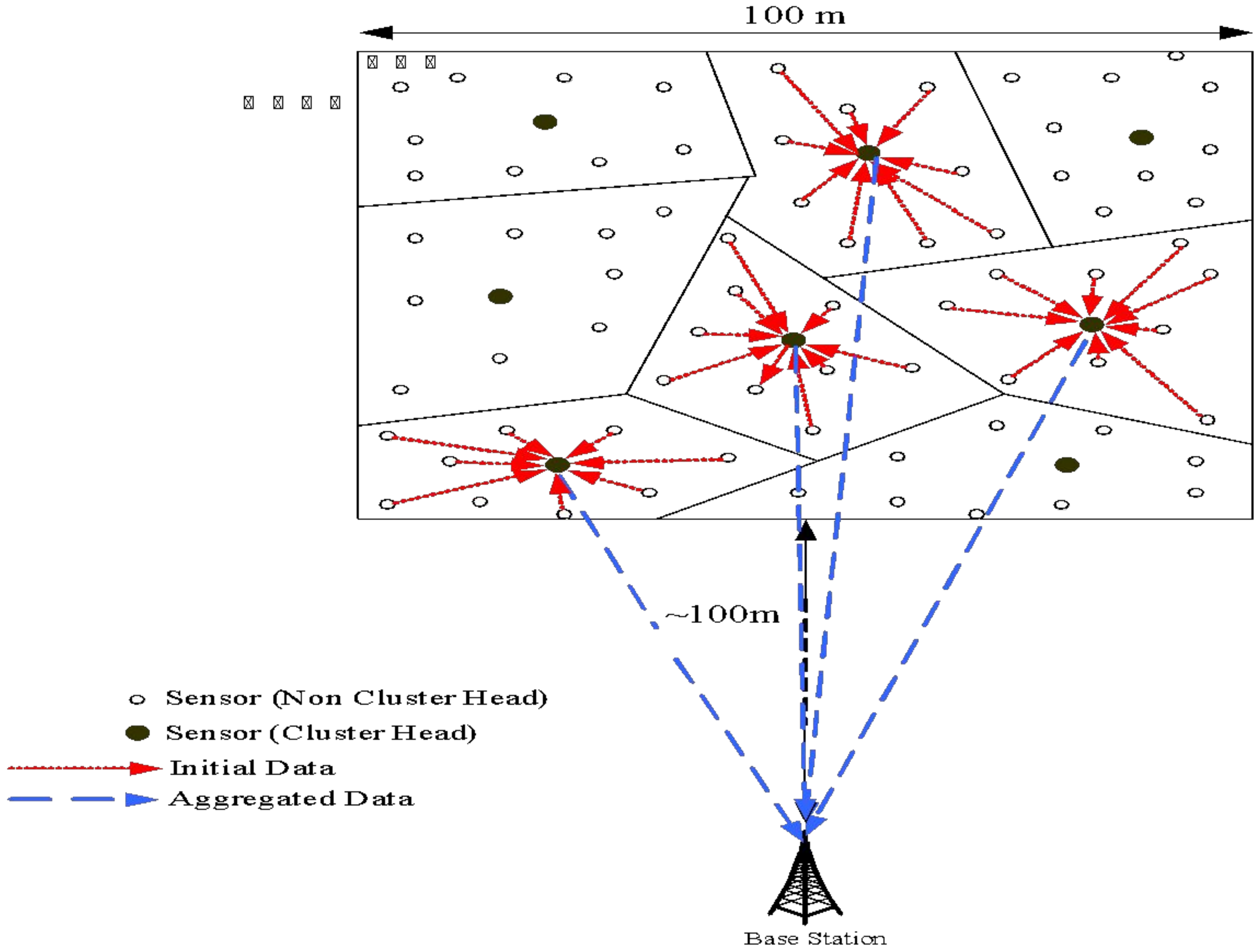
LEACH

- LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that minimizes energy dissipation in sensor networks.
- LEACH outperforms classical clustering algorithms by using adaptive clusters and rotating cluster-heads, allowing the energy requirements of the system to be distributed among all the sensors.
- LEACH is able to perform local computation in each cluster to reduce the amount of data that must be transmitted to the base station.
- LEACH uses a CDMA/TDMA MAC to reduce inter-cluster and intra-cluster collisions.

LEACH (cont.)

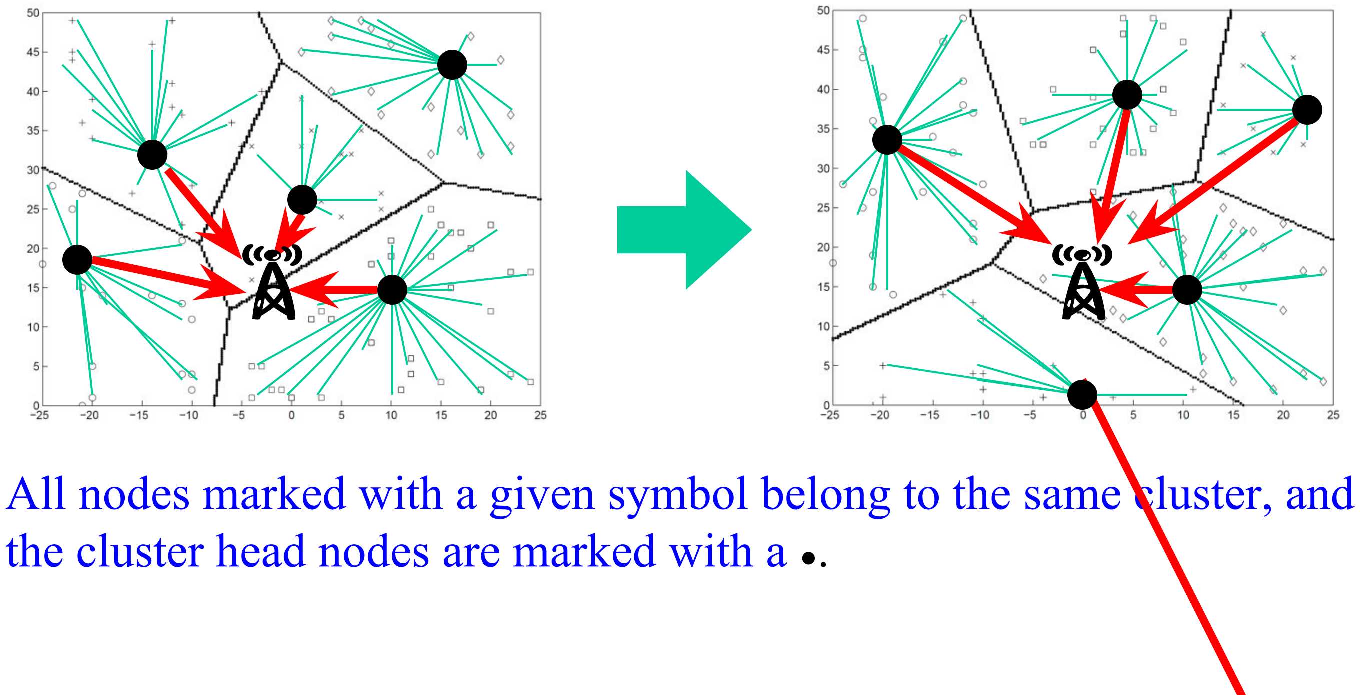
- Sensors elect themselves to be local cluster-heads at any given time with a certain probability.
- Each sensor node joins a cluster-head that requires the minimum communication energy.
- Once all the nodes are organized into clusters, each cluster-head creates a transmission schedule for the nodes in its cluster.
- In order to balance the energy consumption, the cluster-head nodes are not fixed; rather, this position is self-elected at different time intervals.

LEACH


100 m
~100m
Sensor (Non Cluster Head)
Sensor (Cluster Head)
Initial Data
Aggregated Data
Base Station

LEACH: Adaptive Clustering

- Periodic independent self-election
  - Probabilistic
- CSMA MAC used to advertise
- Nodes select advertisement with strongest signal strength
- Dynamic TDMA cycles

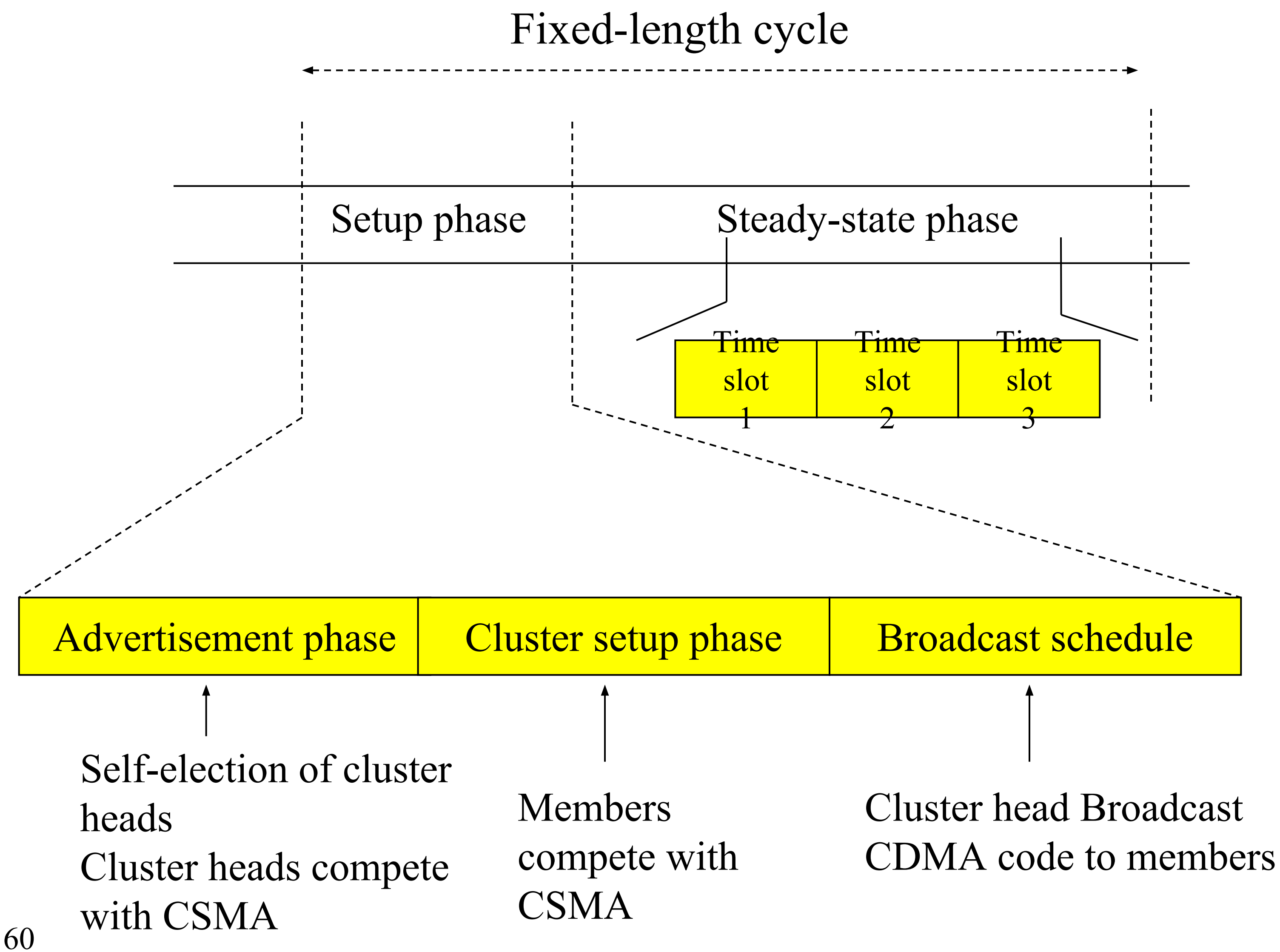


All nodes marked with a given symbol belong to the same cluster, and the cluster head nodes are marked with a •.

Algorithm

- Periodic process
- Two phases per round:
  - Setup phase
    - Advertisement: Execute election algorithm
    - Members join to cluster
    - Cluster-head broadcasts schedule
  - Steady-State phase
    - Data transmission to cluster-head using TDMA
    - Cluster-head transfers data to BS (Base Station)

Algorithm (cont.)



60

Algorithm Summary

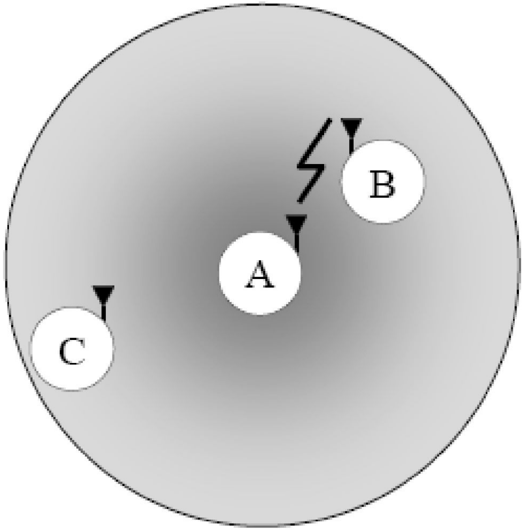
- Set-up phase
  - Node n choosing a random number m between 0 and 1
  - If $m < T(n)$ for node n, the node becomes a cluster-head where

$$T(n) = \begin{cases} \dfrac{P}{1 - P[r * \operatorname{mod}(1/P)]} & if \;\; n \in G \\ 0 & otherwise, \end{cases}$$

  - where P = the desired percentage of cluster heads (e.g., P= 0.05), r=the current round, and G is the set of nodes that have not been cluster-heads in the last 1/P rounds. Using this threshold, each node will be a cluster-head at some point within 1/P rounds. During round 0 (r=0), each node has a probability P of becoming a cluster-head.

Algorithm Summary (cont.)

- Set-up phase
  - Cluster heads assign a TDMA schedule for their members where each node is assigned a time slot when it can transmit.
  - Each cluster communications using different CDMA codes to reduce interference from nodes belonging to other clusters.
- TDMA intra-cluster
- CDMA inter-cluster
  - Spreading codes determined randomly
  - Broadcast during advertisement phase

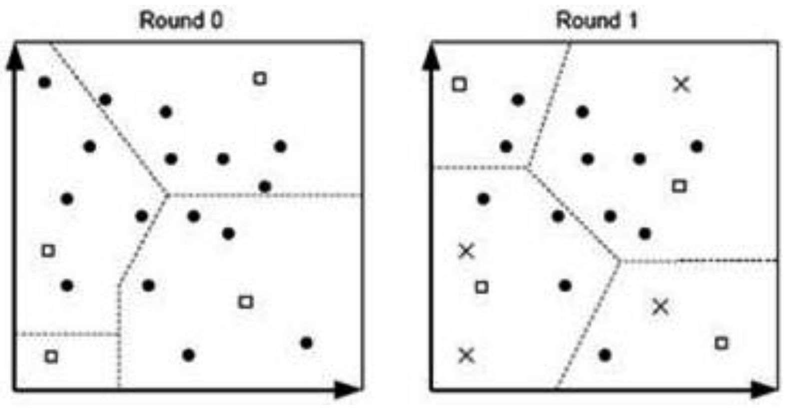


Algorithm Summary (cont.)

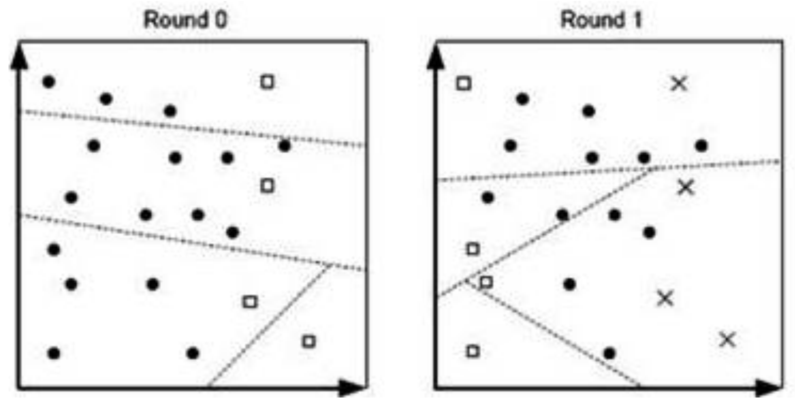
- Steady-state phase
  - All source nodes send their data to their cluster heads
  - Cluster heads perform data aggregation/fusion through local transmission
  - Cluster heads send aggregated data back to the BS using a single direct transmission

An Example of a LEACH Network

- While neither of these diagrams is the optimum scenario, the second is better because the cluster-heads are spaced out and the network is more properly sectioned



Good case scenario



Bad case scenario

● Node
□ Cluster-Head Node
X Node that has been cluster-head in the last 1/*P* rounds
\- - - Cluster Border

Conclusions

- Advantages
  - Increases the lifetime of the network
  - Even drain of energy
  - Distributed, no global knowledge required
  - Energy saving due to aggregation by CHs
- Disadvantages
  - LEACH assumes all nodes can transmit with enough power to reach BS if necessary (e.g., elected as CHs)
  - Each node should support both TDMA & CDMA
  - Need to do time synchronization
  - Nodes use single-hop communication

Reference

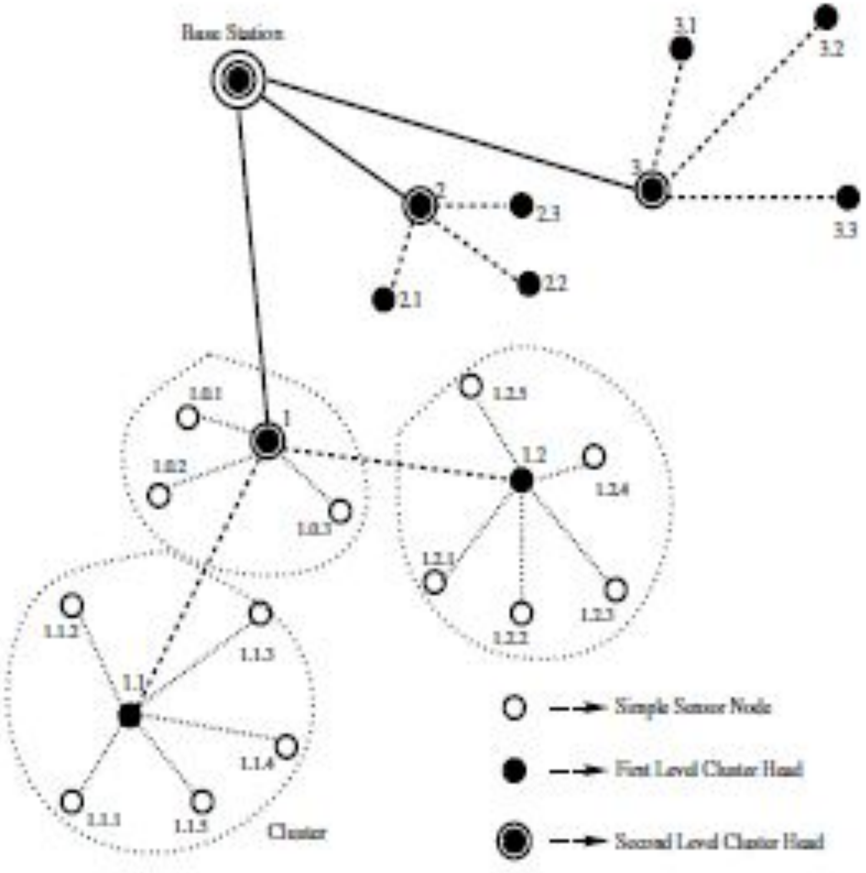
- W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," *Proceedings of the 33rd Hawaii International Conference on System Sciences*, January 2000.

TEEN (Threshold sensitive Energy Efficient Network protocol)

- Reactive, event-driven protocol for time-critical applications
  - A node senses the environment continuously, but turns radio on and transmission only if the sensor value changes drastically
  - No periodic transmission
    - Don't wait until the next period to transmit critical data
    - Save energy if data is not critical

TEEN-Multi-Level Hierarchical Clustering

- Each cluster has a cluster head which collects data from its cluster members, aggregates it and sends it to the *BS or an upper* level cluster head.
  - For example, nodes 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5 and 1.1 form a cluster with node 1.1 as the cluster head.
  - Similarly there exist other cluster heads such as 1.2, 1 etc.
- These cluster-heads, in turn, form a cluster with node 1 as their second level cluster-head.
- This pattern is repeated to form a hierarchy of clusters with the uppermost level cluster nodes reporting directly to the *BS*.
- *The BS forms the root of this* hierarchy and supervises the entire network



Hierarchical Clustering

TEEN Functioning (First Reactive Network Protocol)

▪Functioning

- Every node in a cluster takes turns to become the CH for a time interval called cluster period
- At every cluster change time, in addition to the attributes, the cluster-head broadcasts to its members, a hard & a soft threshold
- ***Hard Threshold(HT)***
  - threshold value for the sensed attribute.
  - A Cluster member only reports/sends data to CH by switching on its transmitter, only if data values are in the range of interest
- ***Soft Threshold(ST)***
  - small change in the value of the sensed attribute
  - A Cluster member only reports/sends data to CH by switching on its transmitter, if its value changes by at least the soft threshold

TEEN Functioning

- The nodes sense their environment continuously.
  - first time a parameter from the attribute set reaches its hard threshold value, the node switches on its transmitter and sends the sensed data.
  - The sensed value is stored in an internal variable in the node, called the *sensed value (SV).*
- The nodes will transmit data in the current cluster period only when the following conditions are true:
  - The current value of the sensed attribute is greater than the hard threshold.
  - The current value of the sensed attribute differs from SV by an amount equal to or greater than the soft threshold.

TEEN Functioning

- Whenever a node transmits data, *SV is set equal to the current* value of the sensed attribute.
- Result
  - hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest.
  - Soft threshold further reduces the number of transmissions by eliminating all the transmissions which might have otherwise occurred when there is little or no change in the sensed attribute once the hard threshold.

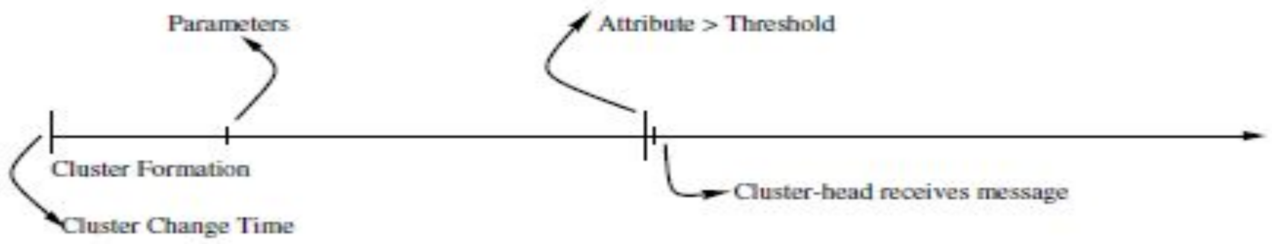


Figure 3. ***Time Line for TEEN***

APTEEN

- In order to provide periodic information retrieval, the adaptive threshold-sensitive energy efficient sensor network (APTEEN) protocol has been developed as an advancement of TEEN .
- APTEEN provides a TDMA-based structure for information transmission in each cluster.
- Consequently, each node transmits its information periodically to the cluster head.
- Moreover, the hard and soft threshold values control when and how frequently to send the data. As a result, both event-based and monitoring applications can be served.