

WIRELESS SENSOR NETWORKS

(18MCA55E)

UNIT - II

“NETWORKING SENSORS”

FACULTY:

Dr. R. A. Roseline, M.Sc., M.Phil., Ph.D.,

Associate Professor and Head,

Post Graduate and Research Department of Computer Applications,

Government Arts College (Autonomous), Coimbatore – 641 018.

CONTENT



- Networking Sensors
 - Key Assumptions
 - Medium Access Control
 - The S-MAC Protocol
 - IEEE 802.15.4 Standard and ZigBee
 - Geographic, Energy-Aware Routing
 - Unicast Geographic Routing
 - Routing on a Curve
 - Attribute-Based Routing
 - Rumor Routing
 - Geographic Hash Tables

NETWORKING SENSORS

- A sensor network comprises a group of small, powered devices, and a wireless or wired networked infrastructure. They record conditions in any number of environments including industrial facilities, farms, and hospitals.
- Sensor networks consist of spatially distributed devices communicating through wireless radio and cooperatively sensing physical or environmental conditions.



KEY ASSUMPTIONS



1. Wireless communication between nodes utilizes radio links; each node talks directly only to its immediate neighbors within radio range. Within this range, communication is by broadcast: all immediate neighbors hear what a node transmits.
2. We assume that network deployment is ad hoc, so that node layout need not follow any particular geometry or topology; irregular connectivity has to be addressed.



- 
- 
3. Nodes operate untethered and have limited power resources. Directly or indirectly, this limits and shapes all aspects of the node architecture, including the node's processing, sensing, and communication subsystems.
 4. Most lightweight sensor nodes have limited or no mobility. This makes sensor networks somewhat different from their ad hoc mobile network counterparts. If mobility is to be added, a substantially larger form-factor is needed, leading to issues akin to those addressed in distributed robotics when swarms of robots need to be controlled. Even with no mobility, sensor nodes can sleep, or fail because of power drainage or other reasons; link connectivity as well can come and go as environmental conditions vary. Thus dynamic topology changes have to be considered.

MEDIUM ACCESS CONTROL

- The medium access control sublayer is the layer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium. The MAC sublayer and the logical link control sublayer together make up the data link layer.
- The MAC sublayer manages access to the physical network medium, and its fundamental goal is to reduce or avoid packet collisions in the medium.



- 
- 
- Several characteristics of wireless sensor networks point to the need for a specialized MAC protocol:
 - Sensor networks are collaborative systems, usually serving one or a small number of applications. Thus issues of fairness at the node level are much less important than overall application performance (unlike, say, on the Internet).
 - In many sensor network applications, most sensor nodes are idle much of the time. When events of interest occur and are detected, there is likely to be a flurry of activity in only some parts of the network, possibly far from where that information is needed. Because of this sporadic and episodic nature of the processing, applications must already be prepared to deal with rather large latency times.

- 
- 
- At the same time, collaboration among nodes sensing the same phenomenon can be facilitated by localized node scheduling for medium access.
 - In-network processing can greatly improve bandwidth utilization.
 - The assumed lack of mobility and therefore the relatively fixed neighborhood of each node can be exploited in medium access protocol design.
 - As mentioned earlier, issues of energy efficiency, scalability, and robustness remain paramount. We are typically willing to compromise on many standard protocol objectives (such as fairness or latency) for the sake of prolonging network lifetime.

- 
- 
- There are many MAC protocols that have been developed for wireless voice and data communication networks. Typical examples include the time division multiple access (TDMA), frequency division multiple access (FDMA), code division multiple access (CDMA) for wireless cellular networks, as well as carrier sense multiple access (CSMA) for the Ethernet and wireless local area networks (WLAN). So far, the most significant published work on developing a sensor network-specific MAC is the S-MAC from the University of California, Los Angeles.

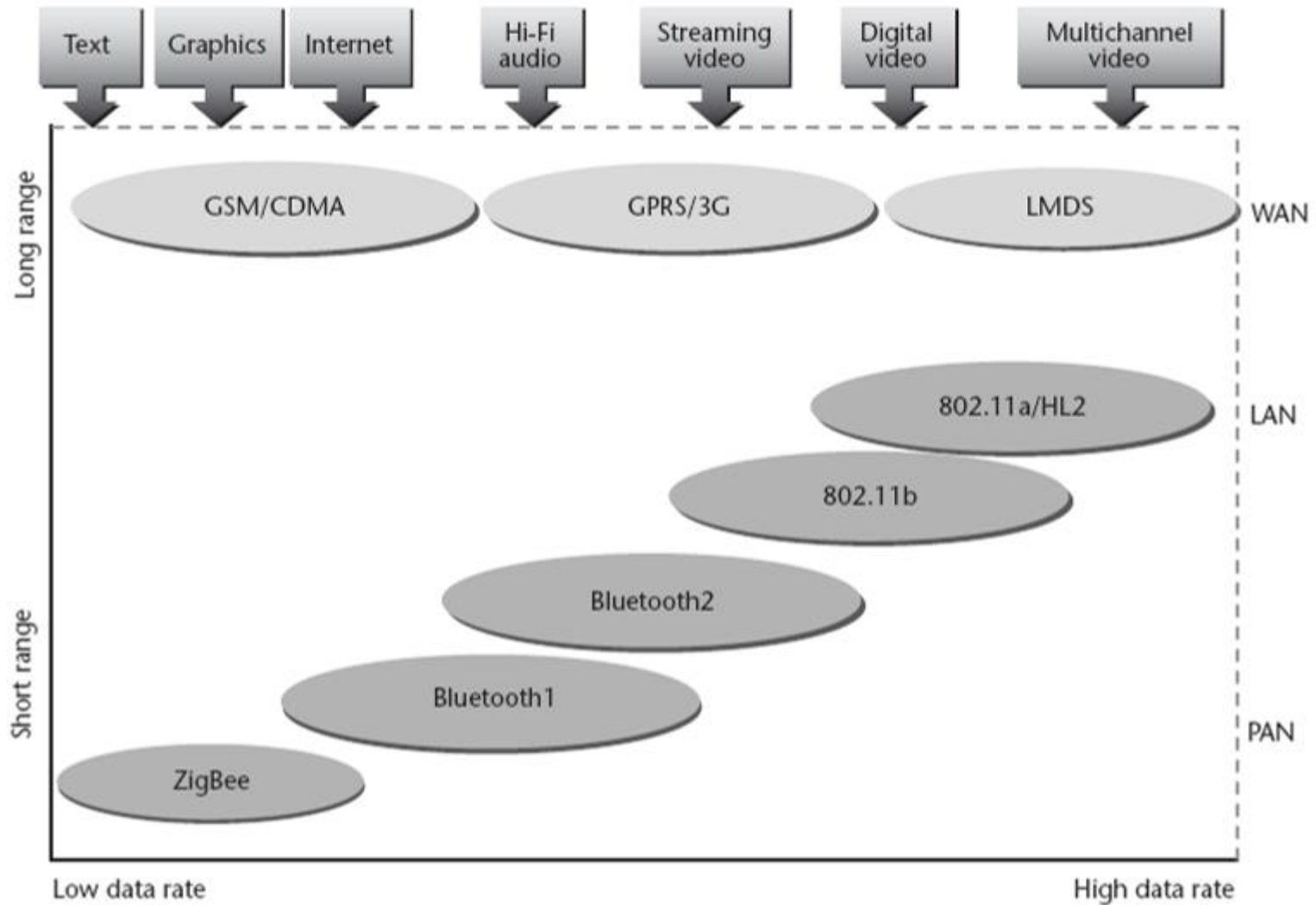
THE S-MAC PROTOCOL

- The main goal of the S-MAC protocol is to reduce energy waste caused by idle listening, collisions, overhearing, and control overhead.
- The protocol includes four major components: periodic listen and sleep, collision avoidance, overhearing avoidance, and message passing.

- 
- 
- Periodic listen and sleep is designed to reduce energy consumption during the long idle time when no sensing events happen, by turning off the radio periodically.
 - To reduce latency and control overhead, S-MAC tries to coordinate and synchronize sleep schedules among neighboring nodes by periodic (to compensate for clock drift) exchanges of the nodes' schedules, so that sleep times will be synchronized whenever possible.
 - Collision avoidance in S-MAC is similar to the distributed coordinated function (DCF) for IEEE 802.11 ad hoc mode, using an RTS/CTS exchange.

IEEE 802.15.4 STANDARD AND ZIGBEE

- The IEEE 802.15.4 standard defines both the physical and MAC layer protocols for most remote monitoring and control, as well as sensor network applications.
- ZigBee is an industry consortium with the goal of promoting the IEEE 802.15.4 standard.
- ZigBee ensures interoperability by defining higher network layers and application interfaces.
- The low-cost, low-power features of 802.15.4 are intended to enable the broad-based deployment of wireless networks able to run for years on standard batteries, for a typical monitoring application.





A bird's-eye view of wireless technologies, according to data rate and range.

GENERAL ISSUES

- Several strategies have been suggested to mitigate the demands of these dynamic changes on the network:
- The frequency of topology updates to distant parts of the network can be reduced, as in fisheye state routing [178].
- Reactive protocols can be used instead, constructing paths on demand only. Examples include dynamic source routing (DSR) as well as ad hoc on demand distance vector routing (AODV)

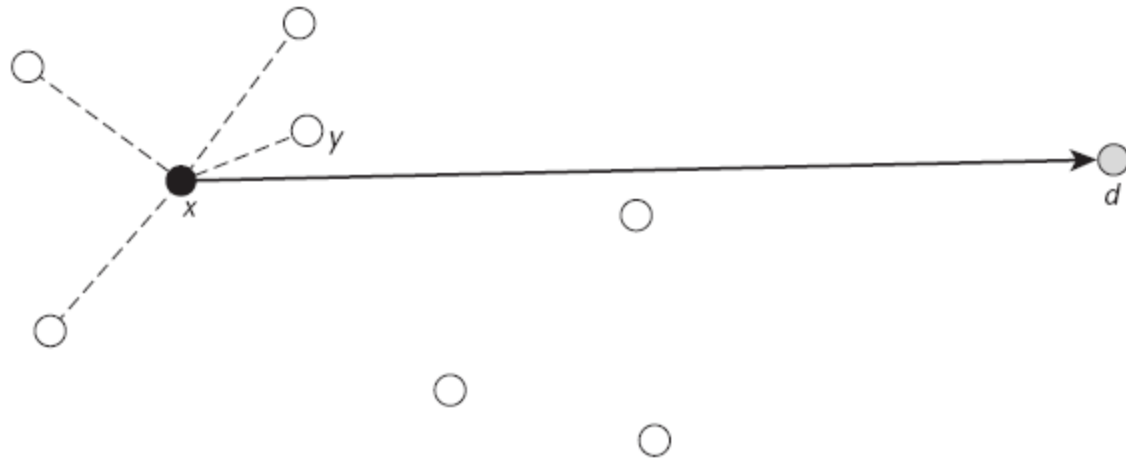
GEOGRAPHIC, ENERGY-AWARE ROUTING

- In this section we focus on Routing protocols whose aim is to deliver packets to nodes or areas of the network specified by their geographic location.
- As mentioned earlier, for sensor networks, the most appropriate protocols are those that discover routes on demand using local, lightweight, scalable techniques, while avoiding the overhead of storing routing tables or other information that is expensive to update such as link costs or topology changes.

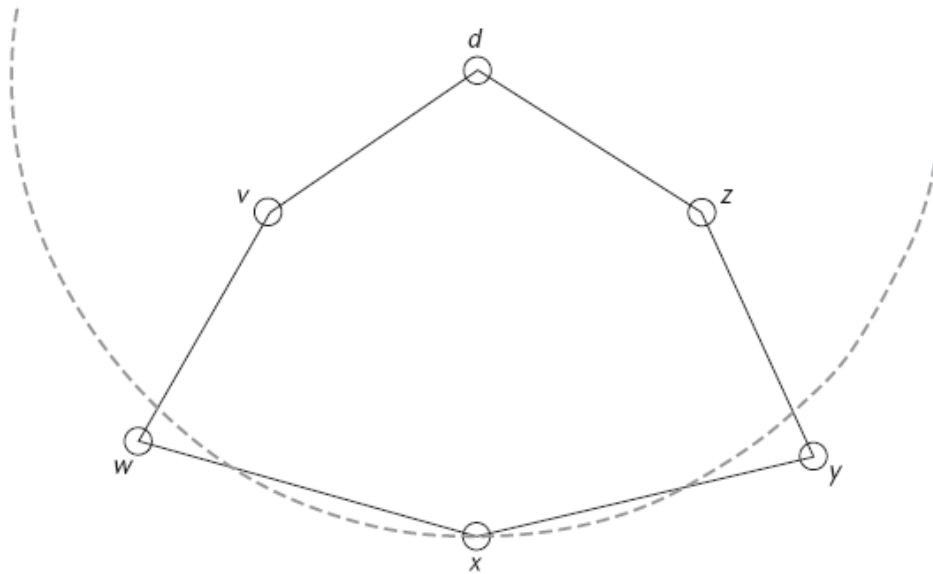
- 
- 
- This lack of global information creates challenges in discovering paths, especially paths that are both time- and energy-efficient for the particular transmission desired, as well as energy-aware in terms of load-balancing utilization across the entire network.
 - The assumptions we make are that
 - All nodes know their geographic location;
 - Each node knows its immediate one-hop neighbors (those within its radio range);
 - The routing destination is specified either as a node with a given location, or as a geographic region (more details later); and
 - Each packet can hold a bounded ($O(1)$) amount of additional routing information, to help record where it has been in the network.

UNICAST GEOGRAPHIC ROUTING

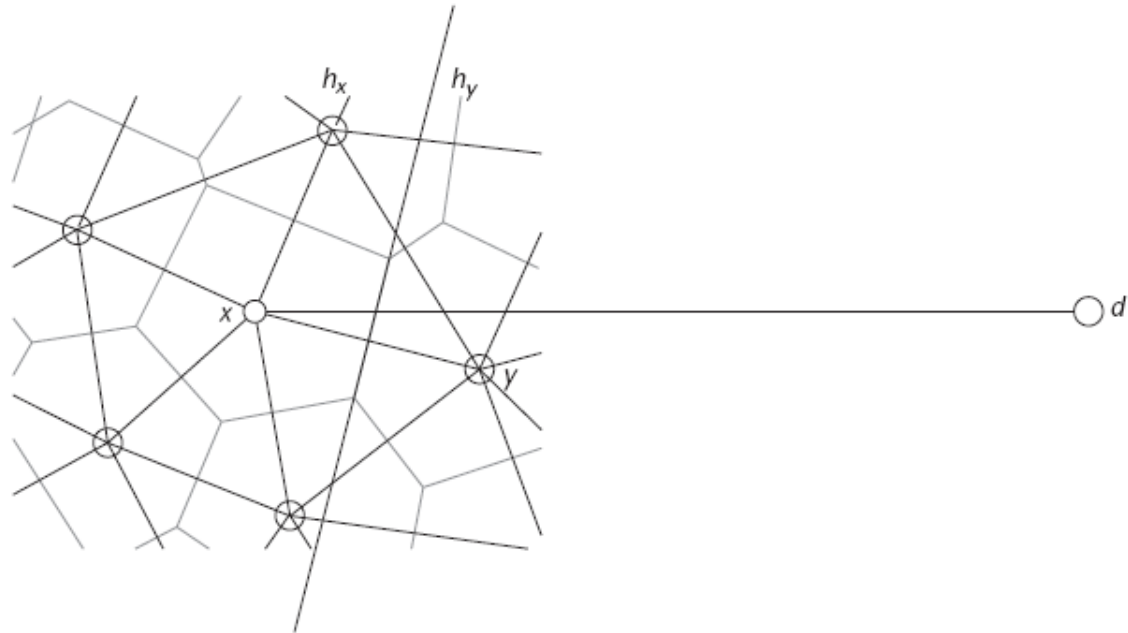
- The main task of the routing protocol is to choose a neighbor y of x to pass on the message. If we assume that no precomputation has been done to aid routing based on the topology of the network, a couple of obvious locally optimal strategies suggest themselves:
 - greedy distance routing: Among the neighbors y of x closer to d than x , pick the one closest to d .
 - compass routing: Among the neighbors y of x that make an angle $\angle dxy < \pi$, we pick one that minimizes the angle $\angle dxy$.





Node x selects node y as the locally optimal neighbor to hand off a packet whose destination is d .





A greedy forwarding strategy can get stuck at node x : both of x 's neighbors are farther from the destination D than x itself.





In the Delaunay triangulation, node x must have a neighbor y closer to d than itself.



- 
- 
- It is easy to see that y is both closer to d than x and a Delaunay neighbor of x . Since only a finite number of points are involved, the process must terminate with the packet arriving at d . Compass routing has guaranteed delivery when G is the Delaunay triangulation of V as well, however, unless the spacing of the nodes is very dense, it is unlikely that all Delaunay edges will be in the unit-distance graph of V .
 - Guaranteeing delivery when a path exists is not the only desideratum for such routing protocols.

- 
- 
- Though it is easy to tell when we are stuck at a local minimum, knowing that we are trapped in a cycle may be more challenging, unless we are allowed to leave some markers behind in the network or carry some information along in the packet about where it has been. Thus the task of discovering that no path from s to d exists may be nontrivial as well.
 - In many situations, we also want the path we find to be optimal, or at least close to optimal, among all possible paths between s and d in G .

- There are some difficulties in agreeing on what optimal means, as different criteria may be at odds with one another. For instance, minimum delay may favor paths with the fewest hops, while minimum energy may favor paths with many short hops. In general, we can express the cost $c(\pi)$ of a path π as



$$c(\pi) = \sum_{e \in \pi} \ell^k(e)$$

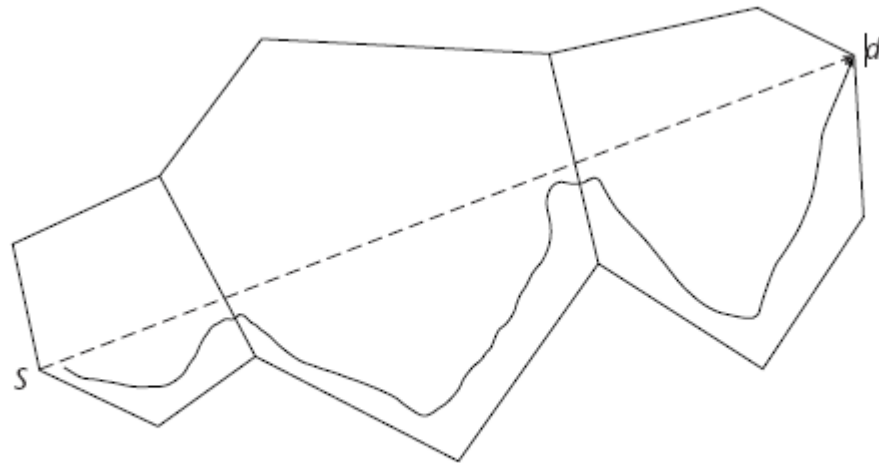
- 
- 
- Here (e) denotes the length of edge e in G , and the usual values for k are between 0 and 5. The value $k = 0$ captures the hop length of the path (number of edges) and is a measure of delay; the value $k = 1$ is the Euclidean path length; and, finally, $k \geq 2$ captures the energy of the path, depending on the attenuation model used.

- 
- 
- A particular consequence of clustering is that we can now assume that there is a minimum separation among the cluster-heads comparable with the radio communication distance and that as a consequence each cluster-head talks directly to only a bounded ($O(1)$) number of other cluster-heads.
 - The path measures given above for different exponents d all become equivalent to within a constant factor, and thus the differences among them can be ignored for our purposes.



PLANARIZATION OF THE ROUTING GRAPH



- Surprising as it may seem, a way to get protocols that guarantee geographic packet delivery is to remove some edges from the connectivity graph G so as to keep the same connectivity but make the graph planar.
- The advantage is that on planar graphs, there are simple exploration protocols based on the ancient idea of traversing a maze by keeping one's right hand against the wall.



- 
- 
- Then the line segment connecting the source node s to the target node d crosses a series of convex faces. In this case, we can route from s to d as follows:
 - Convex perimeter routing: Start in the face of G just beyond s along sd and walk around that face (say, counterclockwise). Stop if d is reached or if the segment sd is about to be crossed. In the latter case, cross over into the next face of G along sd and repeat the process.



The packet gets from node s to node d by walking around the faces of the planar subdivision.

- 
- 
- The main difference from the convex case is that the segment sd may intersect a face more than twice and the algorithm needs to determine all face boundary crossings with sd and select the one farthest from s . All this can be done while using only bounded storage in the packet. Note that if the destination d is not reachable from s , then the perimeter protocol will loop around an interior or exterior face loop of the planar graph G . Thus, to defect this, the packet must remember the first edge traversed when it starts going around a new face.

- 
- 
- A variant of perimeter routing is the other face routing (OFR) protocol . In OFR, after we go around a face F , we continue into a new face F' not from the farthest with F , but instead from the vertex of F' closest to d .
 - In general, not much can be said about the quality of paths discovered by these protocols. We can easily construct an example where, had we chosen to go around the faces clockwise, we would have found a path with $O(1)$ hops, while by going counterclockwise, our paths ends up having (n) hops—which is no better than flooding the network.

- 
- 
- Number of the standard geometric graph constructions for a set of points V can be used to define planarizations of the graph G . It is appealing to use local constructions, in which an edge xy is introduced for nodes $x, y \in V$, if a geometric region (the witness region) around the edge xy is free of other nodes. The most common such constructions are:
 - The relative neighborhood graph (RNG), where the edge xy is introduced if the lune [intersection of the circles centered at x and y with radius the distance $d(x, y)$] is free of other nodes
 - the Gabriel graph, where the edge xy is introduced if the circle of diameter xy is free of other nodes.

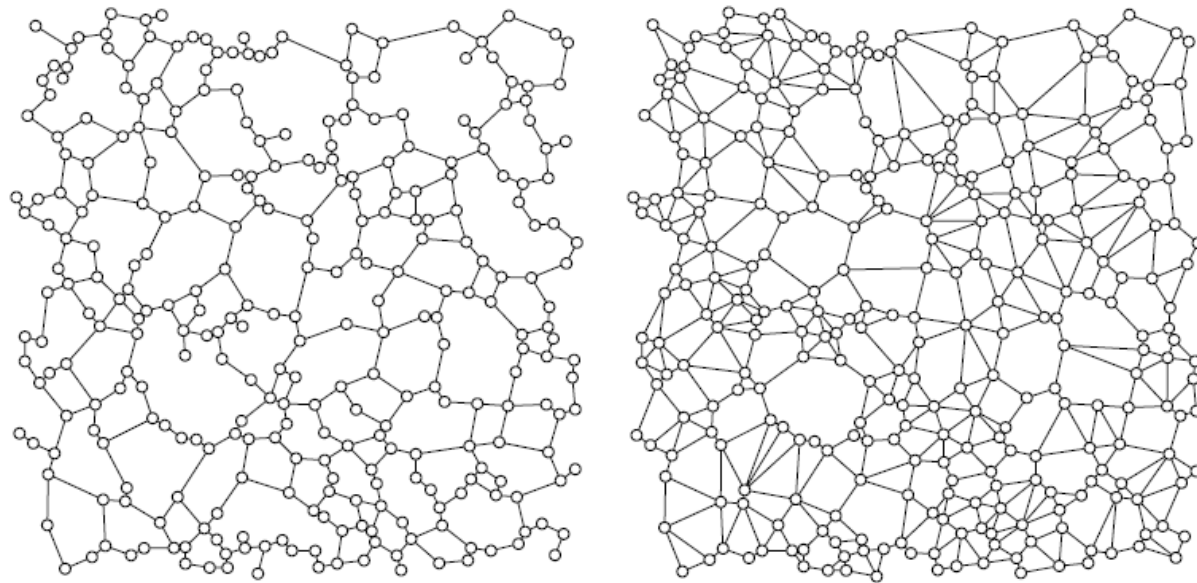




Figure 3.6 An example of the relative neighborhood graph (RNG) on the left, and of the Gabriel graph on the right.



- 
- 
- The Delaunay triangulation is known to be both planar (or course, being a triangulation) and a spanner (best-known stretch factor = 2.42) of the complete Euclidean graph on V . However, the Delaunay triangulation is globally defined. For a local version, we can consider a subgraph U consisting only of Delaunay edges of V whose length is at most l .

GREEDY PERIMETER STATELESS ROUTING

- While greedy distance protocols are extremely simple, they can get stuck in local minima. In contrast, protocols based on planar subgraphs can provide guaranteed delivery, but require both preprocessing and a significantly more complex routing algorithm.
- In many situations where sensor nets are deployed, we can expect that node distribution will be fairly uniform over large areas of the sensor field, but there will be a number of holes or uncovered areas, due to obstacles, node depletion, and the like. Thus it makes sense to consider merging these two approaches, to get the best of both worlds.

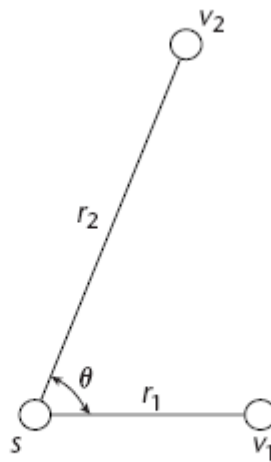
ROUTING ON A CURVE

- Another form of geographic routing, applicable in a number of dense node coverage settings, is to specify an ideal curve that a packet should follow, as opposed to the packet's final destination this has been called trajectory based forwarding (TBF).

- 
- 
- The curve is specified analytically and its description is carried along on the packet, as the latter hops from node to node following a trajectory that approximates the ideal curve. This can be useful in situations where such curves correspond to natural features of the environment in which the nodes are embedded.
 - It is also worth observing that such geometric route specifications completely decouple the route description from the actual locations of the network nodes involved in transport. This makes such schemes very robust to network or link failures resulting in topology changes, as long as an appropriate level of node density is maintained along the packet trajectory.

ENERGY-MINIMIZING BROADCAST

- We have repeated several times the need to be energy-aware in communications involving a sensor network. Two aspects of the energy cost in a sensor network make it challenging to reason about optimizing energy:
- Multi-hop communication can be more efficient than direct transmission.
- When a node transmits, all other nodes within range can hear.
- These are both a consequence of the fact that nodes communicate using radio links, where the signal amplitude drops with distance according to a power law of the form $O(1/r^\alpha)$, where typically $2 \leq \alpha \leq 5$.



A simple broadcast scenario: Node s wishes to reach nodes v_1 and v_2 .

- The source s wishes to broadcast a packet to nodes v_1 and v_2 , having distances r_1 and r_2 to s , respectively. Let θ be the value of the angle $\angle v_1 s v_2$. In this example there are two broadcast strategies:
 - s transmits to v_2 ; both v_1 and v_2 are reached, or
 - s transmits to v_1 and then v_1 transmits to v_2 .
- The energy needed for the first strategy is r_2^α , while that for the second is $r_1^\alpha + r_{12}^\alpha$, where r_{12} denotes the distance between v_1 and v_2 . When $\alpha = 2$, it is easy to see that the first strategy is advantageous if and only if $r_1 > r_2 \cos \theta$. A little more algebra shows that this condition becomes

$$(1 + x^2 - 2x \cos \theta)^{\alpha/2} > x^\alpha - 1,$$

- for general α , where $x = r_2/r_1$.

ENERGY-AWARE ROUTING TO A REGION

- Instead of broadcasting to all nodes in the network, a more common situation is the wish to reach all nodes in a certain geographic region.
- The problem of routing a message to a region combines two of the problems we have discussed so far: unicast geographic routing and energy-minimizing broadcast





- The GEAR protocol operates in two phases:

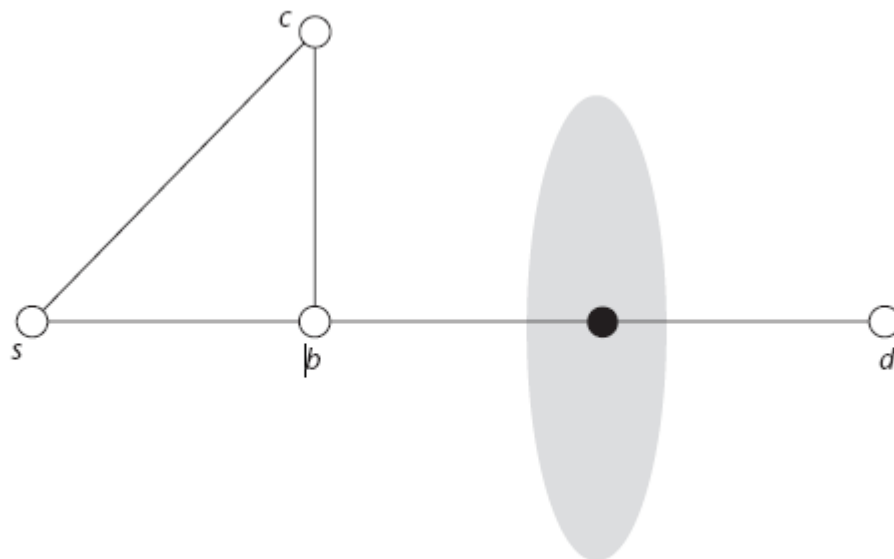
1. deliver the packet to a node in the desired region
2. distribute the packet within the region

- During the delivery phase, GEAR behaves like a unicast protocol routing the message to the centroid d of the region R , except that it considers the energy resources of each node as well.

- In addition, GEAR does not use any specialized subgraphs to route around holes. Instead, it relies on a generic A^* -type search algorithm, the Learning Real-Time A^* (LRTA*) algorithm of Korf.

- 
- 
- The GEAR protocol works by performing the following steps at each visited node x :
 - If x has neighbors closer to d than x in both the Euclidean sense and the learned cost sense, choose among these neighbors the one with the smallest learned cost and pass the packet to that neighbor.
 - Otherwise, forward the packet to the neighbor of minimum learned cost.

$$h(x, d) \leftarrow \min\{c(x, y) + h(y, d), h(x, d)\}$$



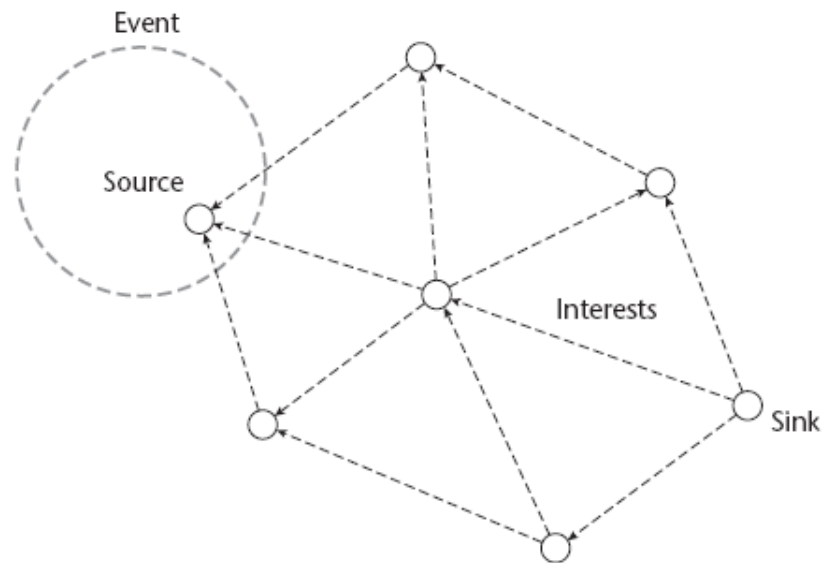
A routing example for the GEAR protocol. Node *s* wishes to route a packet to node *d*, but there is a network hole in between.

ATTRIBUTE-BASED ROUTING

- In more general settings of data-centric routing, however, we cannot assume that we know either the network address or the geographic location of the node we wish to communicate with.
- Geographic location services can be used to map from node IDs to locations.
- For instance, a node tasked to look for animals in an environmental monitoring setting might detect a horse, based on its sensor readings (the details of how this is done do not concern us here).

DIRECTED DIFFUSION

- Directed diffusion is a very general approach toward problems of this type. Nodes requesting information are called sinks, while those generating information are called sources.
- Records indicating a desire for certain types of information are called interests. Interests are propagated across the network, looking for nodes with matching event records.
- Key to directed diffusion is the assumption that interests are persistent—that is, if a source has information relevant to a sink, then the sink will be interested in repeated measurements from that source for some period of time.



The directed diffusion algorithm propagates interests from a sink, until an appropriate information source is reached (adapted from [104]).

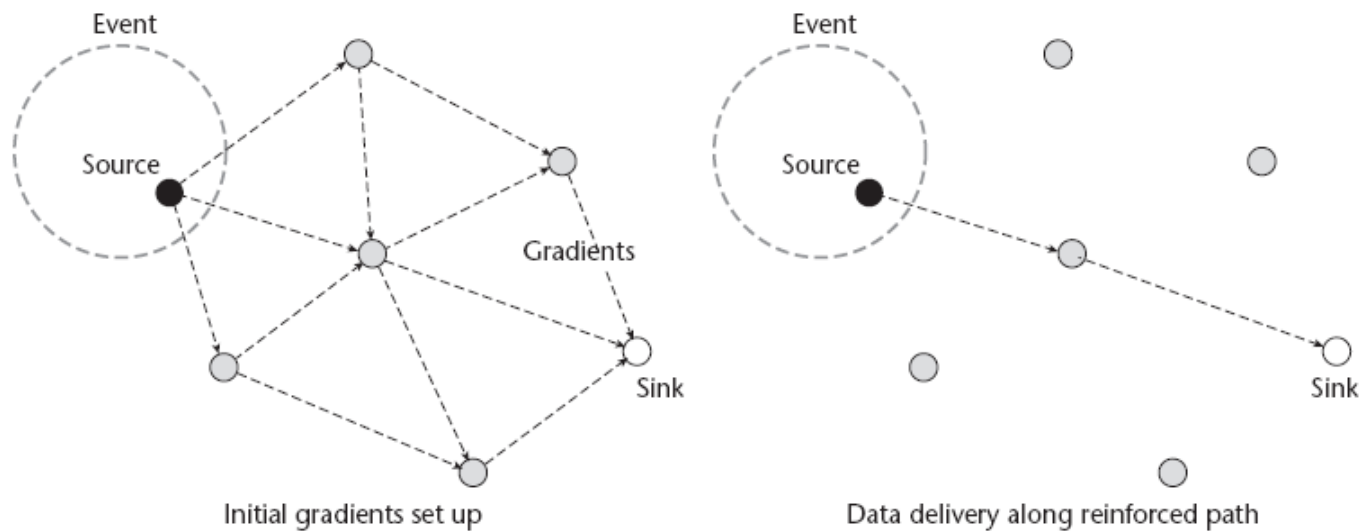




Figure 3.10 Directed diffusion sets up gradients for information delivery from the source to the sink (left), giving rise to multiple delivery paths. Reinforcement eventually redirects most of the information along the best path (right) (adapted from [104]).

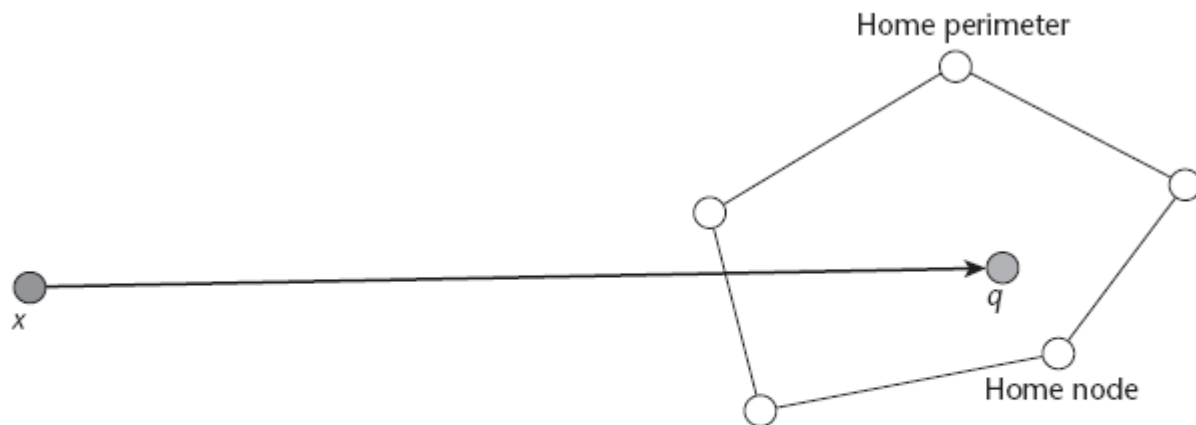
RUMOR ROUTING

- Directed diffusion resorts to initial flooding of the network in order to discover good paths between information sources and information sinks.
- But there are many situations in which, because the amount of data to be exchanged is small, the quality of the paths does not matter so much.
- In such situations, an attractive alternative is the technique of rumor routing, presented in . Conceptually, in order to get sources and sinks to meet each other, we must spread information from each to regions of the sensor field, so that the two growing regions eventually intersect.

- 
- 
- An interesting intermediate alternative is to spread information out of both sources and sinks, but in a one-dimensional fashion, effectively following a curve out of each—so as to reduce energy usage.
 - Related to rumor routing is the ACQUIRE query answering mechanism described in.
 - The ACQUIRE approach is most appropriate for situations when we need to process one-shot complex queries, whose answers depend on information obtained in several nodes of the network.

GEOGRAPHIC HASH TABLES

- There are many situations in which it is useful to view a sensor network as a distributed database storing observations and readings from the sensors for possible later retrieval by queries injected anywhere on the network.
- The geographic hash table (GHT) technique proposed in accomplishes this by using sensor reading attributes to hash information to specific geographic locations in the network.
- Information records meeting those attributes are stored in nodes close to the hashed location



A packet is routed using GPSR to a location where no node exists. The home perimeter defines a ring of nodes around that location, and one of these is selected to be the home node for the packet.



THANK YOU

THE CONTENTS IN THIS E-MATERIAL IS TAKEN FROM THE TEXTBOOKS AND
REFERENCE BOOKS GIVEN IN THE SYLLABUS

