Chapter 9: From MANET To IETF ROLL Standardization_A Paradigm Shift in WSN Routing Protocols

Prof. Yuh-Shyan Chen

Department of CSIE

National Taipei University

Outline

- Abstract
- Introduction
- A Chronological Survey
- IETF MANET
- Geographical Routing
- Self-organizing coordinates
- Conclusion

Abstract

- In large networks, a data source may not reach the intended sink in a single hop, thereby requiring the traffic to be routed via multiple hops. An optimized choice of such routing path is known to significantly increase the performance of said networks. This holds particularly true for wireless sensor networks (WSNs) consisting of a large amount of miniaturized battery-powered wireless networked sensors required to operate for years with no human intervention.
- There has hence been a growing interest on understanding and optimizing WSN routing and networking protocols in recent years, where the limited and constrained resources have driven research towards primarily reducing energy consumption, memory requirements and complexity of routing functionalities.

Introduction

- The routing protocol, i.e. the process of selecting paths in a network along which to send network traffic, is a key building block in a protocol stack.
- It is part of the network layer in the OSI layer model and is central to the proper functioning of any multi-hop communication system, and hence the focus of this survey paper.
- The prime role of the routing protocol is to establish a route between source and sink, keep track of the availability of such route and facilitate successful transmission of data along the chosen route.

Challenges Faced by Routing Protocols

- A major obstacle to the ubiquitous deployment of WSNs is the absence of reliable and easy-to-implement communication stacks.
- The main design criteria are thus to lower algorithmic complexity to facilitate low-power solutions that can be embedded into low-cost microprocessors, and to extend the lifetime of the network without jeopardizing reliable and efficient communications from sensor nodes to other nodes as well as to data sinks.

approaches

- data centric approaches
  - data fusion, aggregation, source coding, signal processing, etc.
- protocol centric approaches
  - novel physical layers – called PHY–, Medium Access Control – or MAC – layers, networking paradigms, etc.
- cross-layer and cross-functionality designs
  - joint source/channel coding, etc.
- cooperative and distributed algorithms
  - cooperative PHY, distributed signal processing, etc.
- optimization of key functionalities
  - security, localization, self-*, synchronization, abstraction, ease of programming, etc.
- interdisciplinary approaches
  - principles borrowed from physics, etc

the architectural peculiarities of WSNs

- applications: very dispersed (= any wireless system)
- control: often decentralized (= cellular, broadcast, satellite)
- data: low load but highly directed (= ad-hoc)
- links: volatile due to channel and dynamics (= many wireless system)
- nodes: huge numbers, low complexity, energy limited (= any wireless system)
- run-time: very long (= any wireless system)

A Chronological Survey

- Historically, routing protocols initially developed for mobile ad hoc networks have been adapted to the new needs of WSNs. This has led to WSN flooding and clustering protocols.
- The potentials of using a better organizational state, i.e. geographical information, to lower energy consumption of routing protocols and hence to extend the WSN's lifetime has then been recognized and related protocols begun to appear.
- Recently, however, this has been extended further by routing protocols which rely on self-organizing coordinates and hence free themselves from geographical information altogether. Flooding Protocols

Flooding Protocols

- Flooding Protocols are particularly useful for coordinating small groups of mobile nodes.
- These protocols deliver data without the need for any routing algorithms and topology maintenance.
- Each sensor node broadcasting the data packet to all of its neighbors with this process continuing until the packet arrives at the destination, or the maximum number of hops for the packet is reached.
- Features:
  - requires large energy expenditures, albeit low memory and little computational complexity
  - since no attempt is undertaken to compute the shortest or optimum routing path, latency is clearly also an issue
  - the protocol class adapts very quickly to any link unreliability or network dynamics
  - it does not require any form of human intervention and hence facilitates autonomous network operation

Clustering Protocols

- Clustering Protocols do cater for parameter constrained routing as long as the clusters are built and maintained as a function of the energy state of the nodes and system.
- It allows for building structures according to the traffic patterns and, under some assumptions, is scalable and latency prone.
- Security is easier implemented as cluster heads can act as trusted entities in the network.
- The drawbacks of this class of routing protocols are that it has problems catering for the link dynamics, and alien configuration can be problematic as structures need to be created and maintained.

Geographical Routing Protocols

- Geographical Routing Protocols build the route using geographical information of the nodes.
- This allows to achieve network wide routing while maintaining only neighborhood information at each node, hence significantly reducing the complexity of the routing solution.
- It hence allows building routes which reflect the given traffic patterns; minimizes latency; and allows security to be implemented.
- The drawback of these protocols, however, is that each node needs to be located and with a very high precision, both of which are difficult to meet in reality.
- Any network dynamics are difficult to follow since this would require an update of the geographic information not only in the affected node(s) but also in the entire network.

Self-Organizing Coordinate Protocols

- Self-Organizing Coordinate Protocols counteract the biggest drawback of geographic routing protocols by building a viable coordinate system from scratch without any external input.
- This routing protocol family caters for parameter constrained routing, link unreliabilities and system dynamics, WSN specific traffic patterns, low latency and high scalability.
- The IETF has recognized gradient routing, a subclass of self-organizing coordinate protocols to be particularly suited for WSNs, and has based its future standard on this concept.

IETF MANET

WSNs as defined by IETF MANET and IETF ROLL differ mainly in the traffic patterns the protocols support. We name the traffic patterns as follows:

- Point-to-point (P2P) refers to traffic exchanged between any two nodes in the network;
- Point-to-Multipoint (P2MP) refers to traffic between one node and a set of nodes. A common WSN use case involves P2MP flows from or through a sink node outward towards other nodes contained in the network.
- Multipoint-to-Point (MP2P) is a common WSN use case in which packets collecting information from many nodes in the network flow inwards towards the sink node(s).

Flooding-Based Routing

- Flooding-based protocols enable P2P traffic patterns and rely on broadcasting data and control packets by each node into the entire network.
- In its purest incarnation, a source node sends a packet to all of its neighbors, each of which relays the packet to their neighbors, until all the nodes in the network – including the destination – have received the packet.
- Despite its simplicity, pure flooding suffers from the following flaws which render application to WSNs infeasible:
  - Implosion when extra copies of messages are sent to the same node by different neighbors or through different paths;
  - overlap due to the fact that sensors covering the same region send similar data to the same neighboring nodes;
  - resource blindness because flooding lacks consideration for energy constraints of nodes when transmitting packets.

Dynamic Source Routing (DSR)

- Dynamic Source Routing (DSR) discovers routes only when needed, and uses source routing to send packets over those multi-hop paths.
- When it needs to transmit a packet
  - the source node sends a route request which is flooded throughout the network.
  - Nodes which relay the route request add their identifier to a specific field in that packet.
  - Upon reception, the destination node knows the sequence of nodes traversed by the route request.
  - It reverses that list, and writes it in a specific field in the header of the data packet. This field is used to route back to the initial requester.
- Because this technique is inherently loop-free, no sequence numbers are needed to deal with inconsistent routing tables.

Ad-hoc On Demand Vector Routing (AODV)

- Ad-hoc On Demand Vector Routing (AODV) is similar to DSR in that a route request floods the network when a node needs a route to another node, so as to discover the route with the minimum number of hops.
- Route replies are sent along the reverse path by the destination, or by a node which knows a path to the destination.
- To free up space in the packet's header, nodes along the reverse route can cache information (i.e. remember that they have relayed a route request from a specific node), and use that information when the reply message travels back to the requester.
- AODV floods error messages when a routing inconsistency is detected (e.g. when a route breaks due to a topological change), and issues a new route request.

Dynamic Mobile On-Demand routing (DYMO)

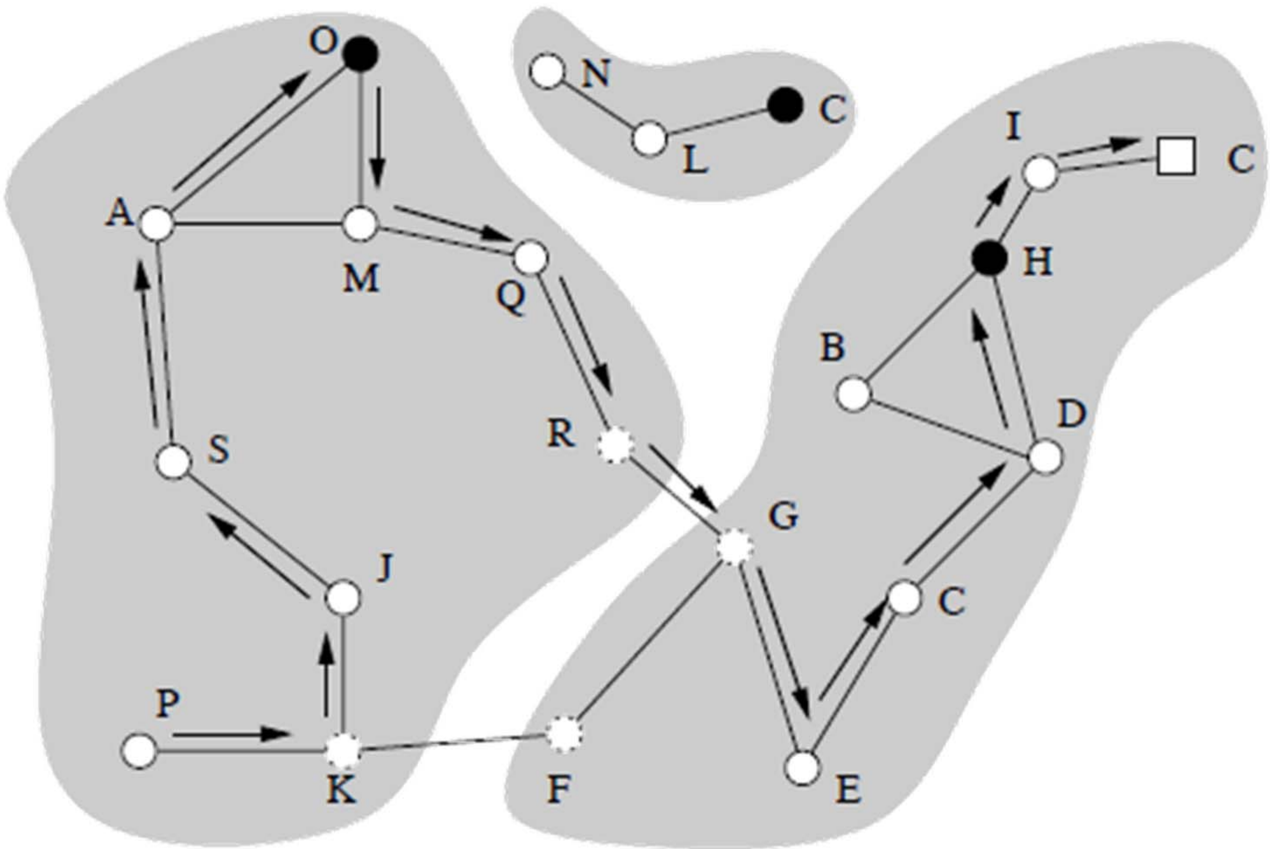
- Dynamic Mobile On-Demand routing (DYMO) uses the same principle as AODV to construct shortest length paths.
- In AODV, a route request builds a route to a single node, i.e. at least as many route requests as the number of nodes in the network are needed.
- DYMO improves this by path accumulation, where a single route request creates routes to all the nodes along the path to the destination it was initially intended for.
- Moreover, DYMO allows for unreliable links to be assigned a cost higher than one. Sequence numbers are moreover used to guarantee the freshness of the data in the nodes' routing table.

Cluster-Based Hierarchical Routing

- Cluster-based routing protocols are based on a hierarchical network organization. Nodes are grouped into clusters, with a cluster head elected for each one.
- Data transmission typically goes from cluster members to the cluster head, before going from the cluster head to the sink node. Because cluster heads perform more demanding tasks in processing and transmitting, they are typically higher-energy nodes. They support P2P traffic.

Fig. 1. Cluster-based network architecture

Clusters are shaded; cluster heads are represented by black disks, gateways by dotted circles, and the sink node by a square.



Cont.

- Fig. 1 depicts a typical clustered network. As a first step, a distributed election process identifies cluster heads (here nodes O, H and C). Nodes then join the cluster head which is typically closest (according to some distance function).
- Cluster members on the edge of the cluster are identified as gateway nodes (here nodes K, F, R, G); they are used as bridges between clusters. Communication is done hierarchically: when node P sends data to sink node C, it starts by sending the packet to the cluster head, which then relays it to the destination cluster. A packet sent from P hence follows the path identified in Fig. 1.

Low-Energy Adaptive Clustering Hierarchy (LEACH)

- Low-Energy Adaptive Clustering Hierarchy (LEACH) is one of the pioneering approaches in the literature of hierarchical routing protocols for WSNs. Depending on a predefined probability, nodes elect themselves as cluster head; other nodes then join the closest cluster head.
- Each cluster head creates and broadcasts a time-division multiple access (TDMA) schedule to coordinate intra-cluster communication; code-division multiple access (CDMA) is used for inter-cluster communications.
- LEACH exploits the randomized rotation of the role of cluster heads to evenly distribute the energy load. Note that the number of clusters grows linearly with the number of nodes, which may not be desirable.
- As cluster heads are placed randomly, some non-cluster head nodes may have no cluster head at communication range. As a result, they are disconnected from the network although physically there exists a multi-hop path to the sink node.

Hybrid, Energy-efficient, Distributed clustering protocol (HEED)

- The Hybrid, Energy-efficient, Distributed clustering protocol (HEED) selects cluster heads based on a hybrid of the nodes' residual energy and some communication costs.
- Like LEACH, the clustering process formation is completely distributed and terminates in a fixed number of iterations (regardless of the network diameter). But in contrast to LEACH, HEED guarantees good cluster head distribution and assumes that cluster heads have relatively high average residual energy compared to regular nodes.
- The drawback of HEED is that it is based on the assumption that nodes can tune their communication range through transmission power: low power levels are used for intra-cluster communication, higher levels for inter-cluster communication.
- Real RF phenomena such as external interference and multipath fading make it hard to predict the communication range from the transmission power, especially indoors. This causes HEED to be of little practical use in a real deployment.

TEEN and APTEEN

- Threshold sensitive Energy Efficient sensor Network protocol (TEEN) and Adaptive threshold sensitive Energy Efficient sensor Network protocol (APTEEN) are designed for time-critical applications, where thresholding on the sensed data is used to limit the number of packets a node generates. Threshold enables the designer to trade-off energy-efficiency for data accuracy.
- Unlike LEACH, TEEN and APTEEN construct a multi-tier hierarchy, in which data is relayed by several cluster heads before arriving to the sink. Note that TEEN and APTEEN do not detail the cluster formation protocol.
- The main drawback of TEEN and APTEEN is the overhead and complexity associated with forming clusters at multiple levels.

Cont.

- Cluster-based protocols may differ in many aspects, among which the way clusters are organized and maintained, the criteria used for cluster head election and maintenance, the cluster heads' properties and roles, the way they communicate with other sensors and with the sink, etc.
- Using clusters has the benefit of limiting the area for flooding data to the cluster instead of the whole network, with positive consequences over scalability, lifetime, and energy efficiency.
- Additionally, because nodes physically close usually sense similar events, data can be efficiently aggregated at the cluster head to obtain a smaller amount of data.

IETF MANET to IETF ROLL, a Paradigm Shift

- WSNs and ad-hoc networks are both wireless multi-hop networks, they are different in mainly three aspects:
  - energy-efficiency is a primary goal for WSNs,
  - in most envisioned applications, the amount of data transported by a WSN is low and
  - all information flows towards a limited number of destinations in WSNs.
- Routing protocols designed for ad-hoc networks are hence inadequate in large and dense sensor networks.
  - Flooding-based solutions have been designed for the coordination of a small group of mobile wireless devices, but node for each packet sent in the network is not compatible with the constraints of a WSN.
  - Similarly, the benefits of cluster-based solutions must be balanced against the signaling cost for cluster formation, cluster-head selection and cluster maintenance.

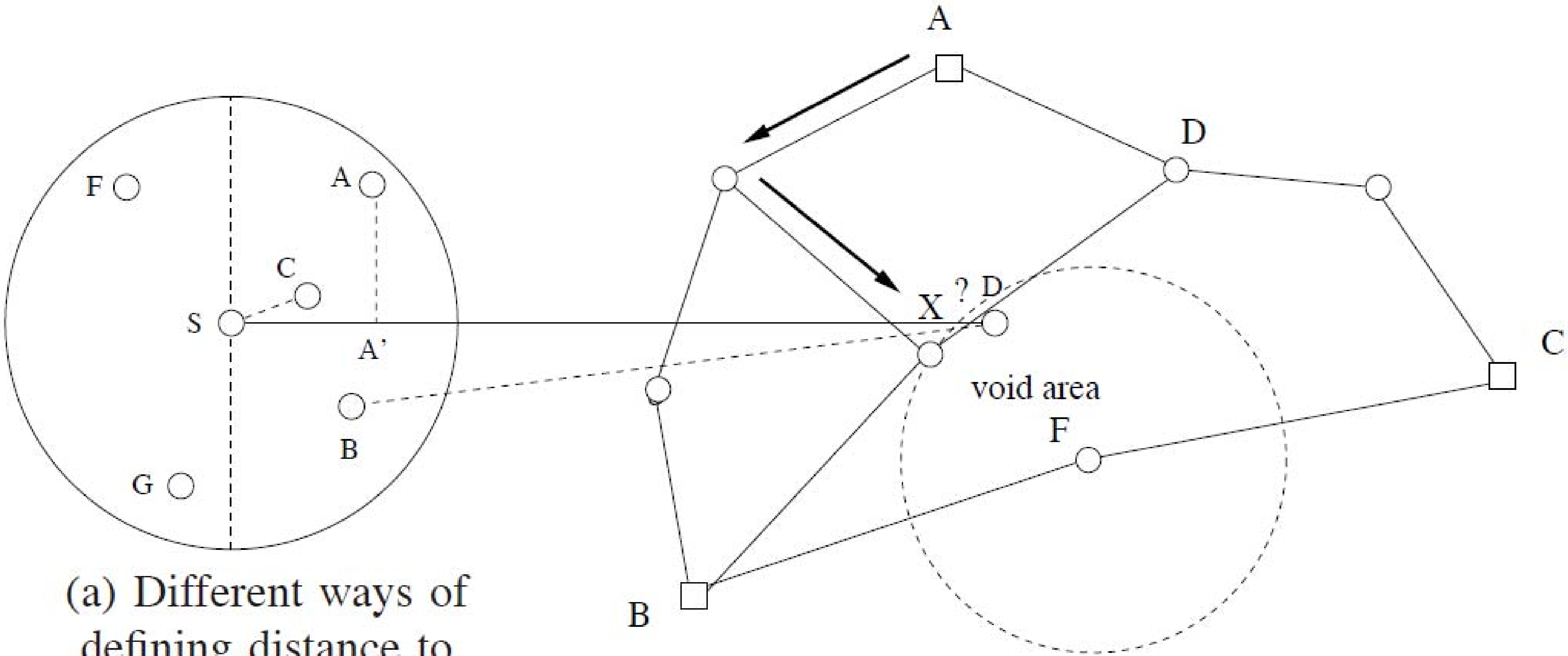
Cont.

- This paradigm shift is mainly driven by the evolution of commercially relevant applications of WSNs.
- From small networks of highly mobile nodes, commercial focus has veered towards large convergecast – most data converges to a small number of sink nodes – networks of static nodes, dragging with it standardization and research efforts.
- This document highlights this subtle relationship by presenting a chronological survey.
- As a result, the paradigm change is triggered by a shift in application requirements rather than by a clear technical superiority.

Geographical Routing

- Many WSN applications (e.g. tracking the location of lions in a National Park) require all nodes to know where they are, physically. In outdoor applications, this may be achieved through GPS, but any other method is possible.
- With the application requiring location-awareness, there is no overhead to reuse this location information for communication purposes.
- This is the philosophy behind geographic routing, which uses the knowledge of a node's position together with the positions of its neighbors and the sink node to elect the next hop.
  - Greedy Approach
  - Face Routing to Guarantee Delivery
  - Principal Protocols Variants
  - Discussion on Propagation Models

Greedy Approach



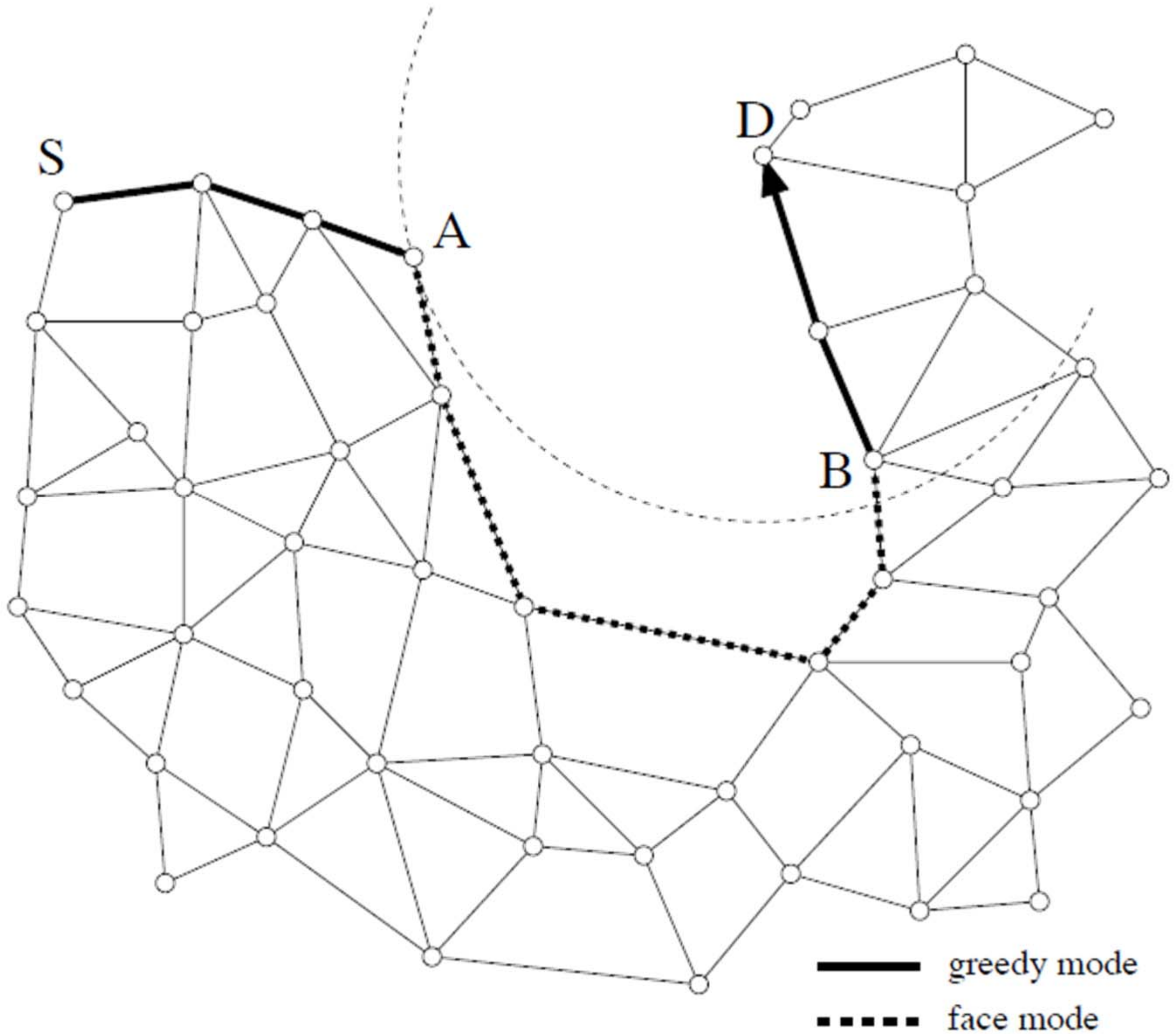
(a) Different ways of defining distance to destination.

(b) Geographic routing fails when a message is sent from A to F.

Face Routing to Guarantee Delivery

- More advanced geographic routing protocols guarantee delivery under the assumption of reliable links and nodes.
- The key idea of these protocols is to switch between two modes. The default mode uses the greedy approach described above.
- In case this mode fails, a second mode is used to circumnavigate the void area. Once on the other side of this void area, the greedy mode is resumed.

Greedy-Face-Greedy (GFG)



Principal Protocols Variants

- Both the Greedy and the Face routing modes have been optimized to reduce energy consumption.
- The main idea is for a node to select its neighbor which minimizes cost over progress.
- In the purely geographical spirit, progress is defined as the reduction in Euclidean distance to destination when hopping to the next node; cost is defined as the energy spent for that hop, following any suitable energy model.
  - End-to-End routing process (EtE)
  - Beaconless Greedy Routing (BGR)
  - Angular Relaying

Discussion on Propagation Models

- The solutions based on distributed graph planarization techniques rely heavily on two unrealistic assumptions: (1) nodes know their position perfectly and (2) the connectivity graph is a unit disk graph.
- As a result, when those assumptions are broken (which they are in real-world deployments), routing protocols relying on them fail, and the delivery ratios drop.
- When nodes do not know their position perfectly, as illustrated in Fig. 10, distributed planarization techniques take wrong decisions, which may cause network partitioning.
- The same can happen when the unit disk graph assumption is broken. Fig. 11 details the problem faced by distributed planarization when faced with non-UDGs. The four nodes u, v, w, y are represented by small circles; nodes which are able to communicate are linked by either plain or dashed lines. The two dashed circles are represented for construction only and have no physical meaning.

Fig. 10. GFG can not guarantee delivery with imperfect positioning

(a) nodes are positioned at their geographical location;

(b) depicts the linkswhich remain after the Gabriel graph transformation. Note that Gabriel Graph preserves connectivity in this case.

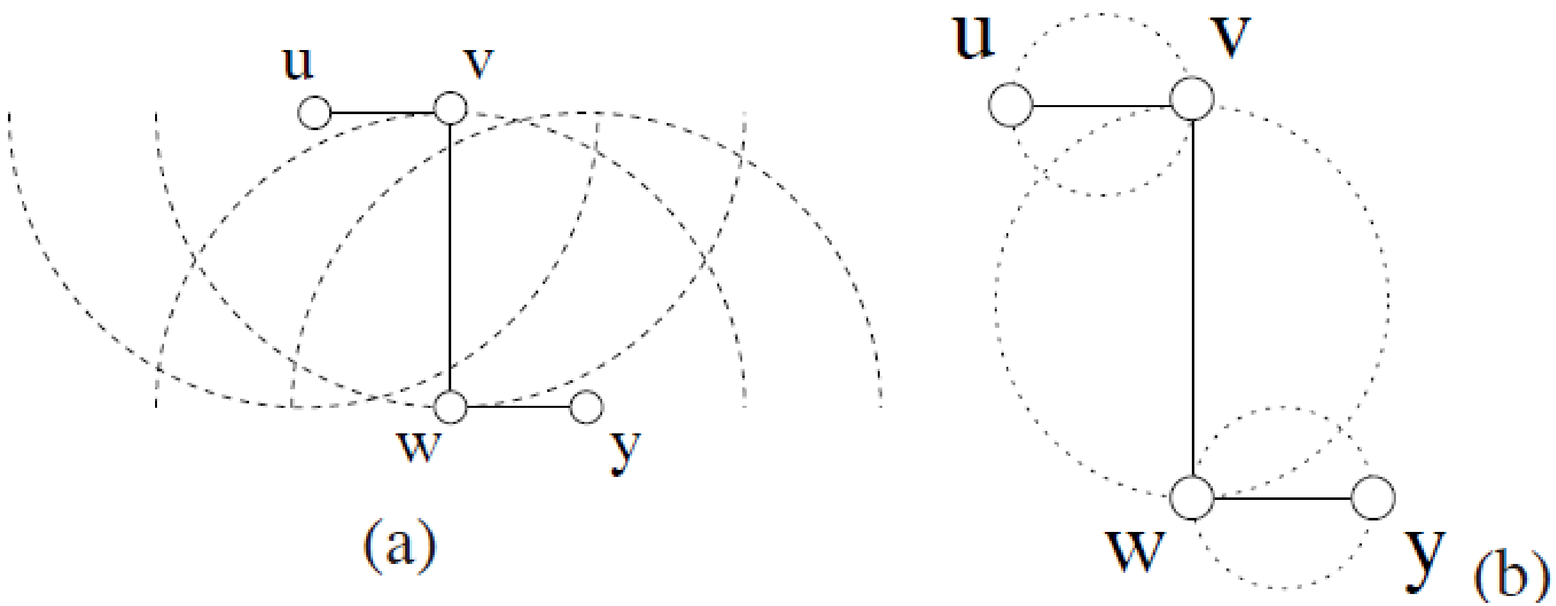
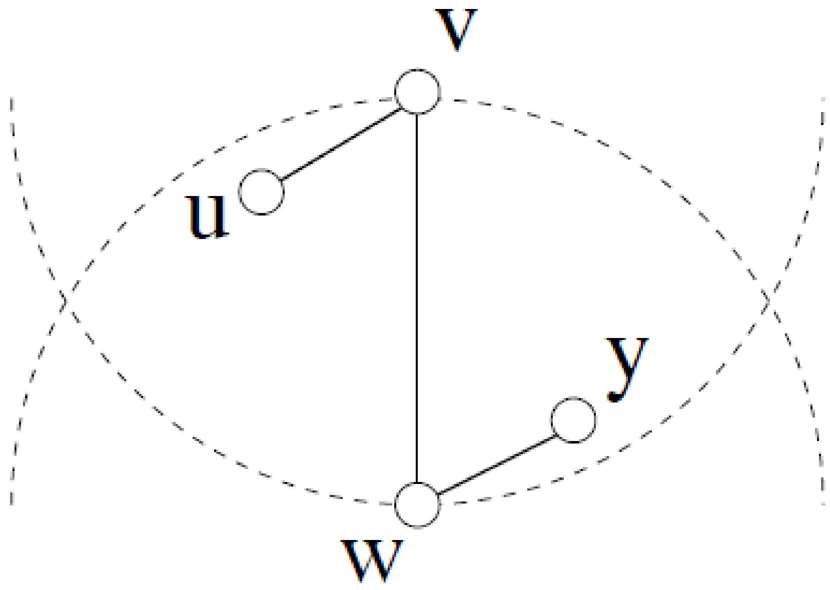


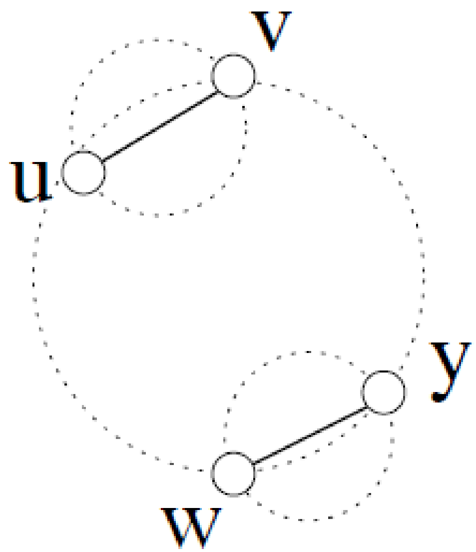
Fig. 10. GFG can not guarantee delivery with imperfect positioning

(c) depicts the nodes at their approximated positions, i.e. where they believe they are.

(d) depicts the network after the Gabriel graph transformation: removing the edges not part of the Gabriel Graph results in a disconnected graph, because Gabriel Graph transformation is run using the positions approximated by nodes.



(c)



(d)

3rule routing protocol

- The 3rule routing protocol is a unique point in the design space of geographic routing protocols as it uses the sequence of already traversed nodes to help the hop-by-hop forwarding decision.
- Each node traversed by a message is asked to append its unique2 identifier to the header of that message; a node receiving a message thus knows whether it has already relayed this same message.
- The current node applies 3 simple rules to filter through its list of neighbors, and to forward the message to the appropriate one.
- This technique is equivalent to depthfirst search, and that it guarantees delivery as the graph is exhaustively searched, in the worst case.
- By favoring neighbors which are geographically closer to the destination, the authors show that the resulting 3rule routing protocol finds paths which have the same length as the one found by GFG, while guaranteeing delivery on any arbitrary stable graph.

Self-organizing coordinates

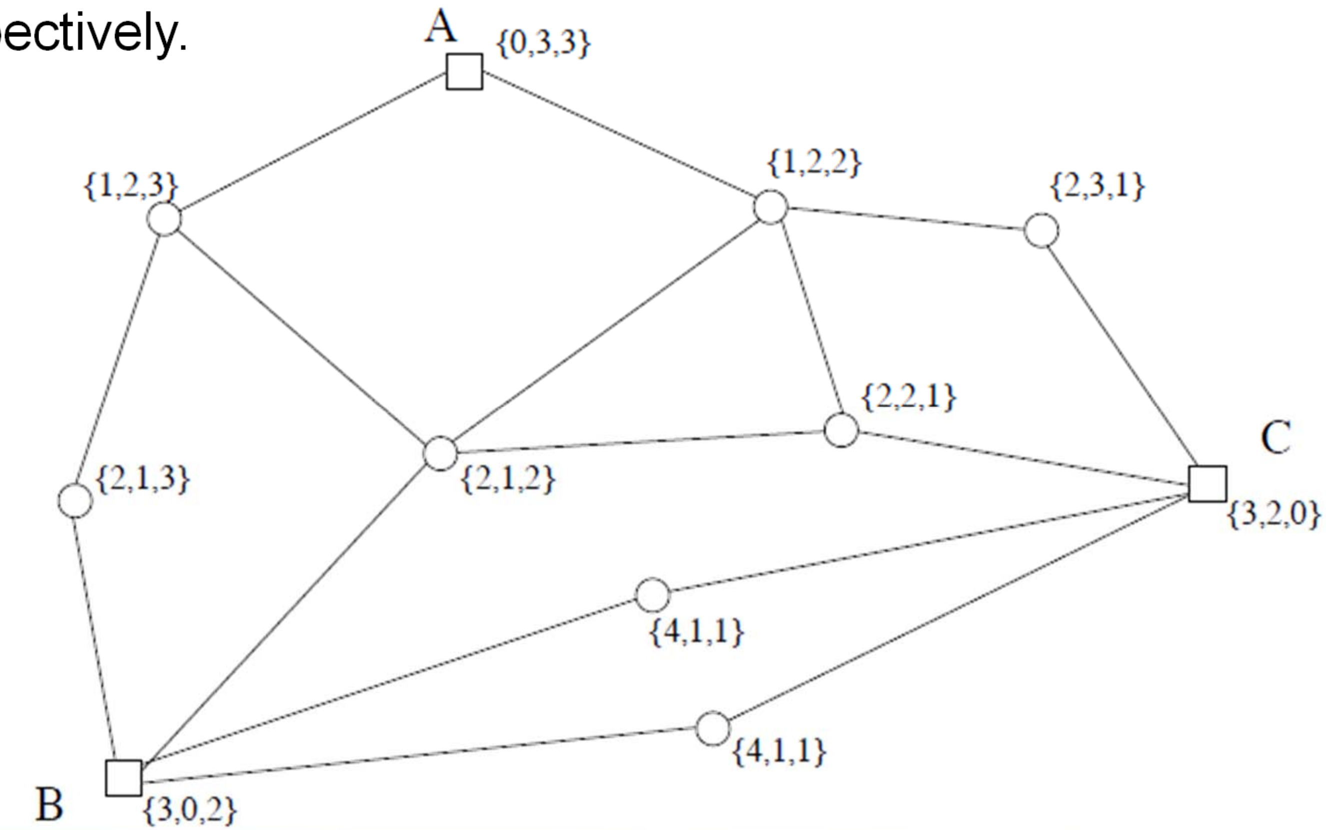
- If at all possible, having each node know its location comes at a price.
- The cost of location-awareness can be monetary (e.g. the cost of a GPS chip), energy-related (e.g. to power a GPS chip), related to man-power (e.g. manually programming a node's position during deployment) or any combination thereof. One solution is to replace real coordinates by "virtual" coordinates, and use geographic routing-inspired routing protocols on top of these coordinates.

Inferring Location From Anchor Nodes

- A first step is to have location-unaware nodes infer their location relative to a subset of location-aware anchor nodes.
- Each anchor node is assumed to know its position (e.g. a set of x, y coordinates in a two-dimensional deployment).
- Nonanchor nodes then use local measurements and localization protocols to infer their location.
- When using anchor nodes, there is a clear distinction between localization (i.e. determining the physical positions in space/plane of the nodes) and routing.
- The nodes in the network typically determine their coordinates first; the geographic routing protocol then uses this information to send a message from any node to the sink.

Virtual Coordinate Routing for P2P traffic

An example topology where each node is assigned virtual coordinates. Each small white circle represents a node; edges interconnect nodes capable of communicating. A small white square represents an anchor node. A virtual coordinate is a vector of number of hops to anchor nodes *A*, *B* and *C*, respectively.



Beacon Vector Routing (BVR)

- Beacon Vector Routing (BVR) is an example of a virtual coordinate-based routing protocol. In BVR, anchor nodes are randomly chosen and need not adhere to any particular structure.
- BVR uses greedy forwarding over virtual coordinates. presents experimental results obtained by implementing BVR on a two testbeds (42 mica2dot motes in an indoor office environment of approximately 20x50m; 74 mica2dot motes deployed on a single office floor).
- This work serves as a proof-of-concept experiment for virtual coordinate routing in WSNs.

The Virtual Coordinate Assignment Protocol (VCap)

- The Virtual Coordinate Assignment Protocol (VCap) elects anchor nodes dynamically during an initialization phase.
- A distributed protocol is designed to elect a predefined number of anchor nodes, evenly distributed around the edge of the network.
- This obviates the need for manual selection and enhances the efficiency of the routing protocol as anchor nodes are placed far from each other.

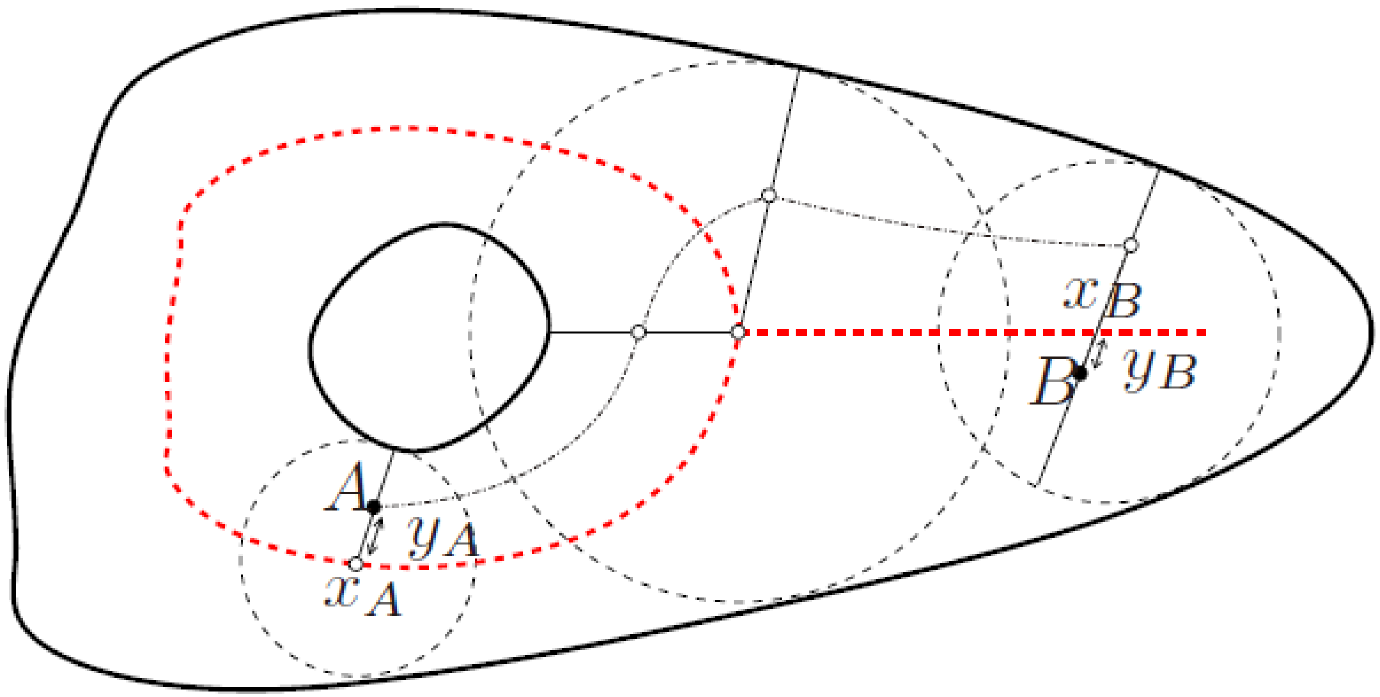
Hector is an Energy effiCient Tree-based Optimized Routing protocol (HECTOR)

- Hector is an Energy effiCient Tree-based Optimized Routing protocol (HECTOR) [66] and combines the strengths of VCost and LTP.
- Each node obtains a tuple coordinate consisting of a VCost relative coordinate and an LTP label (the VCost anchor nodes and LTP root node can be chosen randomly among the network nodes).
- The routing strategy is a hybrid between VCost and LTP: while LTP guarantees delivery, VCost enables energy-efficient routing. Simulation results presented show that obtained paths are 30% longer than the ones obtained by a centralized approach.

Medial Axis Based Geometric Routing (MAP)

- Medial Axis Based Geometric Routing (MAP) is a unique point in the design space of virtual coordinatebased routing protocols.
- The nodes' coordinates are calculated relatively to anchor nodes located on the medial axis of a network topology.
- In Fig. 14, the deployment area of the nodes is outlined by strong black lines.
- The medial axis is defined as the set of nodes with at least two closest boundary nodes, i.e. anode is part of the medial axis iff its two closest boundary nodes are at the same hop count4.
- The resulting set of medial axis nodes (connected by a strong dashed red line in Fig. 14) serve as anchor nodes.

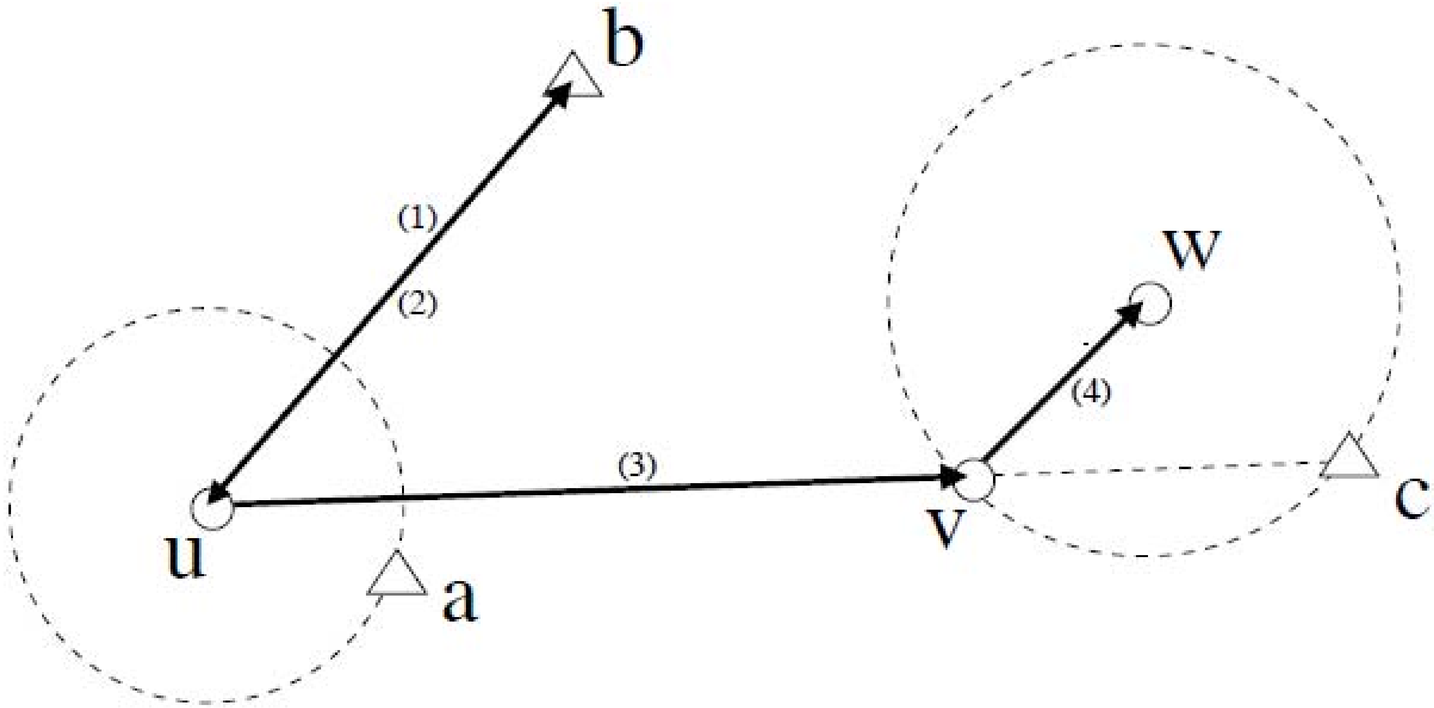
Fig. 14. Illustrating MAP



Resilient Beacon Distance Vector (RBDV)

- Resilient Beacon Distance Vector (RBDV) is used by S4 for inter-cluster communication.
- Because each beacon node periodically floods the network, each node knows its distance to every beacon in the network, and the next-hop neighbor to get to that beacon.
- S4 uses a location directory scheme similar BVR, where beacon nodes store the mapping between non-beacon nodes and their closest beacons.
- The closest beacon information for node *s* is stored at *H*(*s*), where *H* is a hash function that maps *nodeid* to *beaconid*.

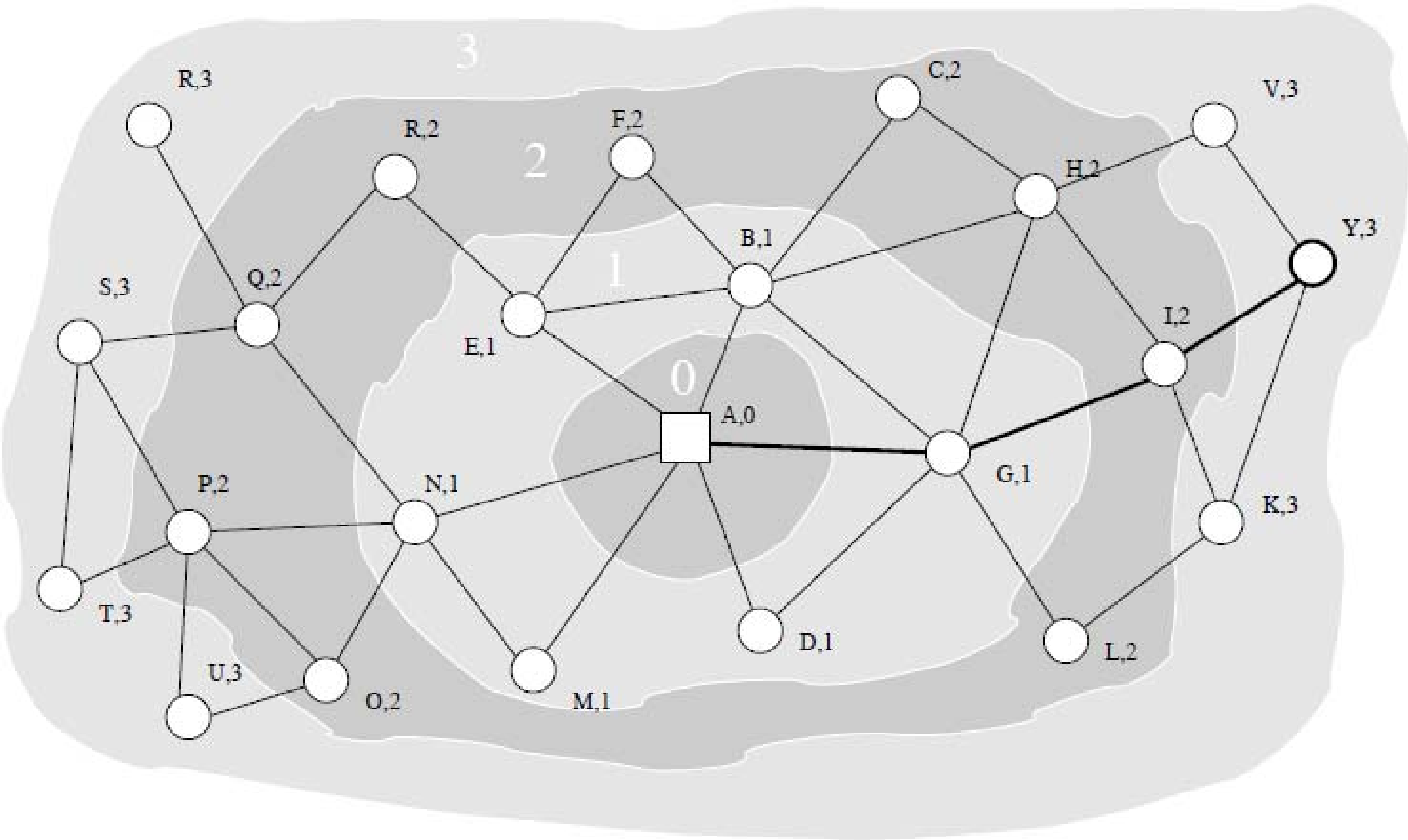
Fig. 15. Illustrating the forwarding process in S4.



Gradient Routing for MP2P traffic

- The concept of gradient is particularly useful for convergecast networks such as WSNs. In the simplest convergecast scenario, all traffic is sent to a single sink node.
- In this case, a single gradient – rooted at the sink node – is built and maintained in the network.
- Fig. 16 depicts a topology where nodes are assigned heights calculated as a function of hop count. When node Y at height 3 sends a message, it sends it to its neighbor of smallest height I; similarly I relays the message to G, and G to A.

Fig. 16. Illustrating gradient routing. Nodes are identified by *[Id,Height]*.



Gradient-Based Routing (GBR)

- Gradient-Based Routing (GBR) is the canonical gradient routing protocol.
- On top of the basic idea described above, an energy-based scheme can be used as a data dissemination technique, where a node increases its height when its energy drops below a certain threshold so that other sensors are discouraged from sending data to it.
- GRAdient Broadcast (GRAB) enhances the reliability of data delivery trough path diversity.
- Similar to EAR, GRAB builds and maintains a gradient, providing each sensor the direction to forward sensing data.
- However, unlike all the previous approaches, GRAB forwards data along a band of interleaved mesh from each source to the receiver.

Collection Tree Protocol (CTP)

- The Collection Tree Protocol (CTP) [76] uses Expected Transmission Count (ETX) as a link metric for setting up the gradient.
- Using ETX, the height of a node indicates how many times a message originated at that node is transmitted before it reaches the sink.
- These transmissions include the hops from node to node, as well as the retransmissions needed upon link failure.

Conclusion

- Table I lists the proposals described in this document in chronological order, and indicates the main characteristic of each.
- Flooding protocols were introduced in the early 2000's.
- The IETF MANET working group standardized protocols which flood requests inside a network to find route on-demand (DSR , AODV , DYMO) and which optimize the number of relaying nodes (OLSR [23]).

Table I

year	protocol	Section II		Section III		Section IV		
		flooding	clustering	greedy geo.	guaranteed geo.	localization	virtual coord.	gradients
1999	GFG [46]				✓			
	DSR [28]	✓						
	directed diffusion [27]	✓						
2000	GPSR [48]				✓			
	TEEN [34]		✓					
2001	GBR [73]							✓
	APTEEN [35]		✓					
2002	LEACH [24]		✓					
	AODV [29]	✓						
	OLSR [23]	✓						
	Niculescu *et al.* [54]					✓		
2003	Centroid [71]					✓		
	Flossiping [21]	✓						
	HEED [33]		✓					
	Cao [60]						✓	
2004	EAR [75]							✓
	Rossi *at al.* [43]			✓				
	Kim *et al.* [59]				✓			
	GPS-Free-free [57]					✓		
	VCap [63]						✓	
	BVR [61]						✓	
	MAP [68]						✓	
2005	GRAB [74]							✓
	Frey *et al.* [49]				✓			
2006	AVCS [69]						✓	
	3rule [52]				✓			
	Chen *et al.* [44]				✓			
	S4 [72]						✓	
	VCost [64]						✓	
	Benbadis *et al.* [58]						✓	
	Zhao *et al.* [67]						✓	
	LTP [65]						✓	
2007	GSpring [70]						✓	
	Hamdi *et al.* [22]	✓						
	DYMO [30]	✓						
	Zhou *et al.* [31]		✓					
	Kalosha *et al.* [51]				✓			
	Elhafsi *et al.* [50]				✓			
	Destino *et al.* [55]					✓		
2008	HECTOR [66]						✓	
	Lanzisera [56]					✓		
2009	CTP [76]							✓
2010	RPL [18]							✓

Homework #9:

1. What’s the four class of WSNs Routing protocol?
2. What’s the drawback of Geographical Routing?