Research experience with special types of Wireless Networks (MANet & Sensor Networks)

By

Dr. O.P. Vyas
Professor & Head (Computer Science & I.T.)
Pt. R.S. University Raipur (CG) India
Visiting Prof. – IIIT Allahabad, India
Email: dropvyas@gmail.com

Research experience with special types of Wireless networks

- Introduction
- Characteristics of MANet & Sensor networks
- Routing in MANET
- Performance issues In MANet
- Sensor networks & distinguishing features with MANet.

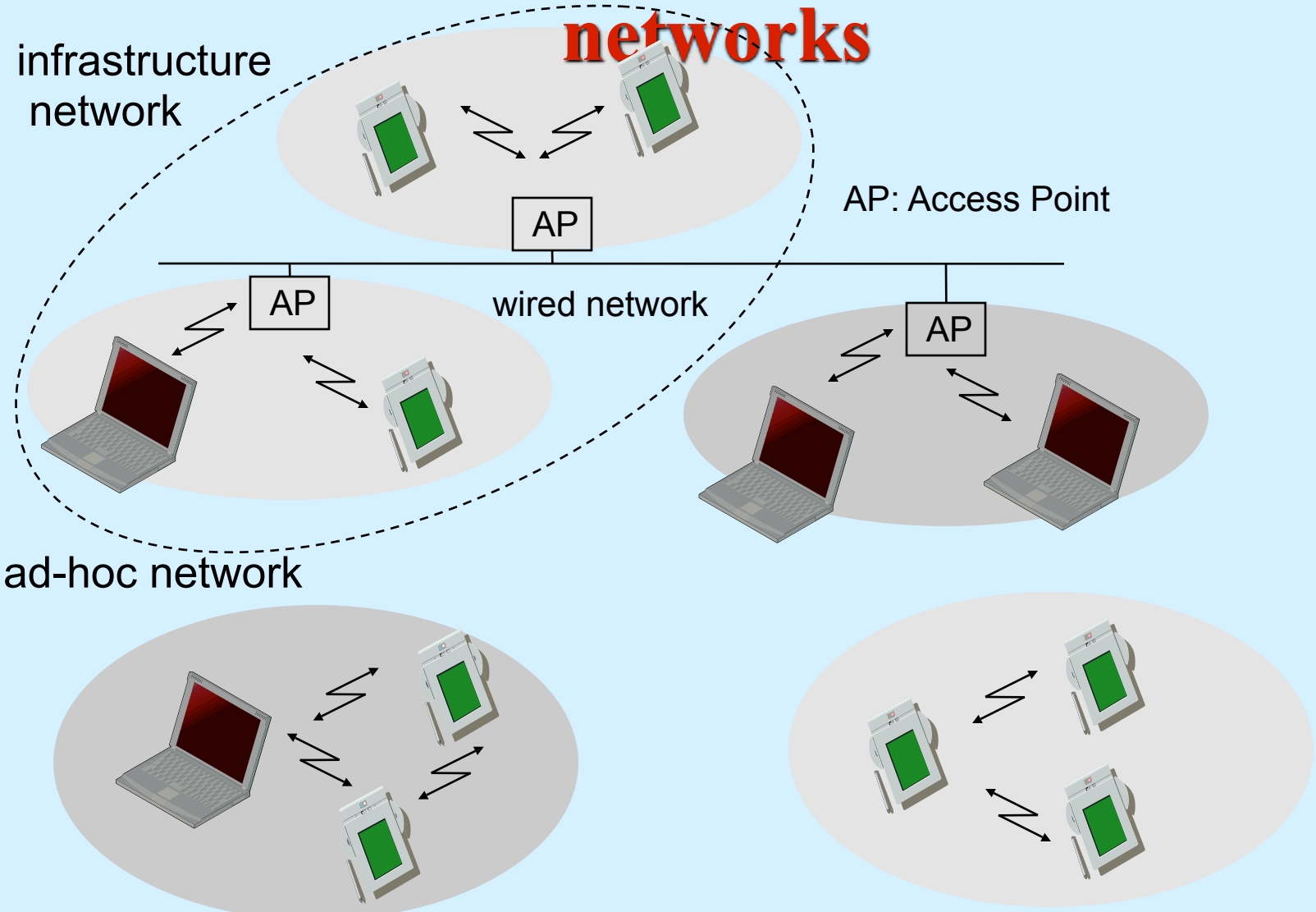
Introduction

- There are some special categories of Wireless networks which are attracting the industry and acdemia both since quite some time. Two of such networks namely Mobile Ad hoc Networks (MANET) and Wireless Sensor Networks are discussed here. Some issues related to such networks were explored and initial research findings with perormance issues related to mobility speeds and routing protocols are being discussed.
- These low cost, low power,low bandwidth but multifunctional special networks are in initial stages of conception and deployments.

Infrastructure and Ad hoc networks

- **Many Wireless Networks of today need an infrastructure network, which not only provide access to other networks, but also include forwarding functions, medium access control etc.**
- **In these infrastructure based networks, communication typically takes place only between the wireless nodes and the access point but not directly between the wireless nodes.**

Comparison: infrastructure vs. ad-hoc networks



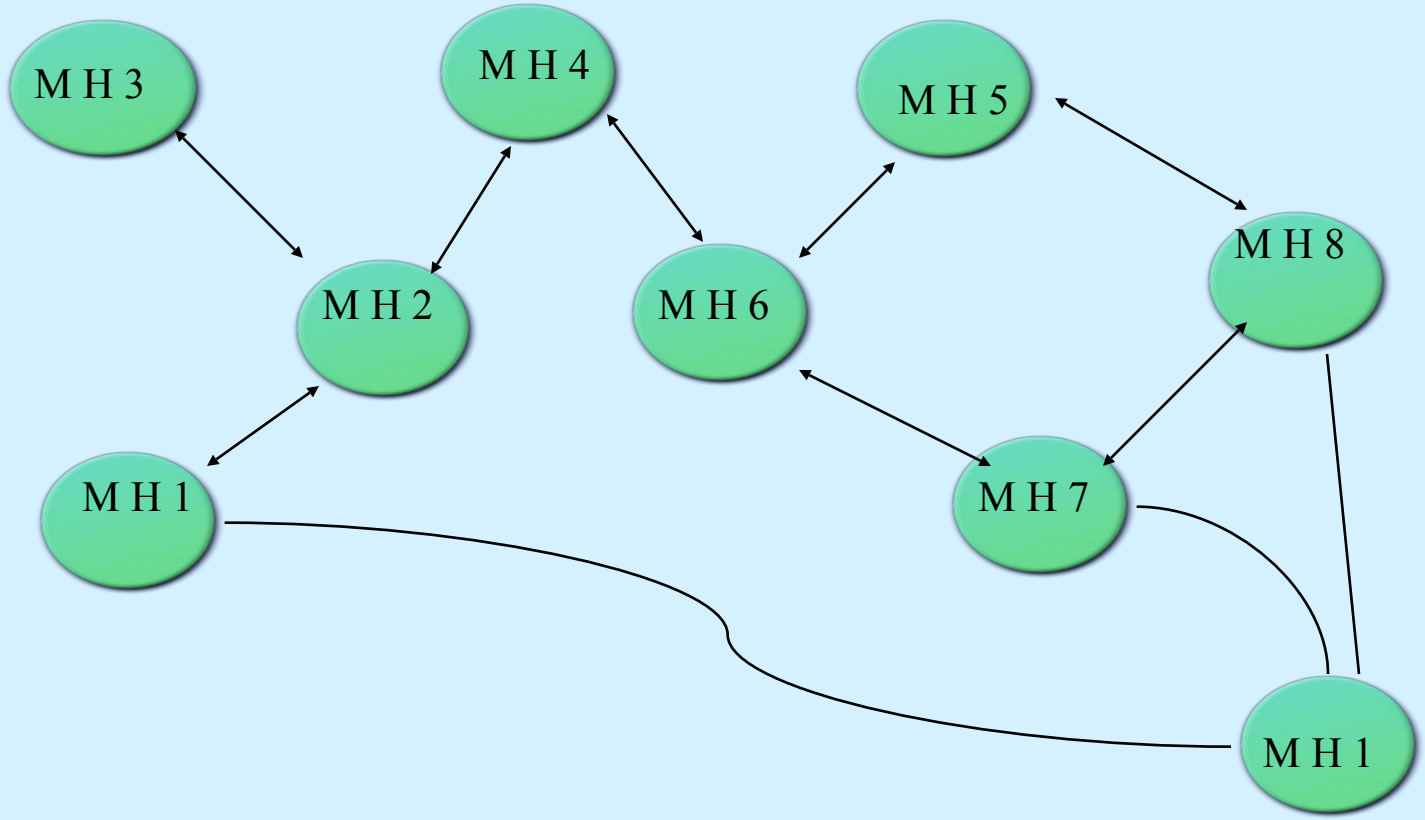
MANET

- The advancements in Wireless Communications allow mobile computer users with compatible wireless communication devices to set up a possibly shortlived network just for the communication needs of the moment- in other words an ad hoc network.
- A MANET consists of mobile platforms (e.g. a router with multiple hosts and wireless communication devices) – herein simply referred to as " nodes" – which are free to move about arbitrarily.
- The nodes may be located in or on airplanes, ships, cars, perhaps even on people, and there may be multiple hosts per router. Quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc.

MANET

- The earliest MANETs were called “Packet Radio" networks, and were sponsored by DARPA in the early 1970s. BBN Technologies and SRI International designed, built, and experimented with these earliest systems.
- The vision of Mobile ad-hoc network is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.
- Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links.
- A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network.

The small ad hoc network scenario when MH1 moves away from MH2 and establishes new links with MH7 and MH8 . Many algorithms also allow for the appearance of new mobile nodes and the disappearance of previously available nodes.



MANETS- Characteristics & Complexities

- MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof.

1. Dynamic topologies. Arbitrary movements thus multihop topology randomly changes having unidirectional or bidirectional links.
2. Bandwidth-constrained, variable capacity links. The realized throughput of wireless communication, because of multiple access, fading, noise,and interference conditions is often much less than a radio's maximum transmission rate.
3. Energy constrained operations. Some or all nodes in MANET may rely on batteries or other exhaustible means for their energy, the important design criteria for optimization may be energy conservation
4. Limited physical security the increased possibility of eavesdropping, spoofing and denial of service attacks should be carefully considered

Research Issues

- A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.
- We are also expoloring this exciting area of Wireless Sensor Networks (WSN), which holds a lot of potential for many scientific and industrial collection by forming a networks of wireless sensors spread across the field. Distinguishing features of these two networks are discussed.
- The complexity of MANet and specific requirements of Sensor networks makes it challenging for researchers worldwide.

Proactive Vs. Reactive Protocols

- One of the most interesting aspects of recent investigations

  Concerns whether or not nodes in an ad hoc networks should keep track of only those destinations ,or instead keep tracks of only those destinations of immediate interest .A node in an ad hoc networks does not need a route to destinations is to be the recipient of packets sent by the node ,either as the actual source to the destination. Protocols that keep tracks of routes for all destinations in ad hoc networks have the advantage that communications with arbitrary destinations experience minimal initial delay from point of view of the applications When the applications starts,route can be immediately selected from the route table Such protocols are called *proactive* because they store route information even before it is needed .They are also called table driven because we can imagine that routes are available as part of a well maintained table.

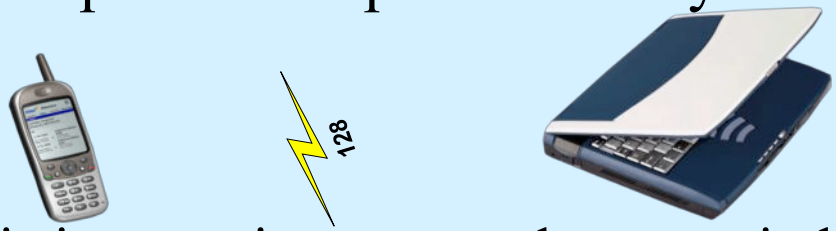
The Effects of Beaconing on the Battery life of Ad Hoc Mobile Computers

- Mobile computing is evolving rapidly with advances in wireless communications and wireless networking protocols. However , despite the fact that devices are getting smaller and more efficient , advances in battery technology have not yet reached the stage where a mobile computer can operate for days without recharging .

- Many existing routing protocols use periodic transmission of route updates to maintain the accuracy of route tables . In wireless networks , beaconing can also be used to signify the presence of neighboring nodes and to indicate the spatial ,temporal , connection and signal stability.

The Effects of Beaconing on the Battery life of Ad Hoc Mobile Computers

- Mobile computing is evolving rapidly with advances in wireless communications and wireless networking protocols. However , despite the fact that devices are getting smaller and more efficient , advances in battery technology have not yet reached the stage where a mobile computer can operate for days without recharging .



- Many existing routing protocols use periodic transmission of route updates to maintain the accuracy of route tables . In wireless networks , beaconing can also be used to signify the presence of neighboring nodes and to indicate the spatial ,temporal , connection and signal stability.

Beaconing

- Beaconing is a technique used by many routing protocols for ad hoc networks to update routing information or to simply denote the presence of a node in the net work and its use should not be a limiting factor .one particularly challenging task in mobile computing is to design for low power consumption . Although much has been done in terms of limiting the power consumption of system hardware devices , the same has not been done for communication protocols ,especially in relation to beacons .
- The findings of some experimental research underlines that the selecting an appropriate beaconing interval is imperative so as not to upset the overall power degradation characteristic of the system or to cause the noticeable side effects for existing applications.
- It was also concluded that the actions taken by the system in preparation for shutdown actually draw more power than usual.

MANET Routing Protocols

- An Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support devices.
- Each node in ad hoc network, if volunteers to carry traffic, participates in the formation of the network topology.
- Routing protocols are self starting, adapt to changing network conditions, and almost by definition offer multihop paths across a network from a source to the destination.

MANET Routing Protocols

- It is evident that within an ad hoc environment the design tradeoffs and the constraints under which a routing method has to operate are quite different.
- The protocols discussed are mainly targeted at layer 3 operation but it is possible to retool the protocol for use at layer 2. (IP address fields be enlarged to contain 48 (or more) bits instead of 32, as needed for IP, as the IEEE MAC address is typically 48 or 64 bits long)

1. Destination sequenced Distance Vector (DSDV) Protocol.
2. Dynamic Source Routing (DSR) Protocol.
3. Ad hoc On Demand Distance-vector based (AODV) Protocol.
4. Zone Routing Protocol (ZRP).
5. Link-Reversal routing (Temporarily ordered Routing Algorithm) Protocol.

- LINK STATE: It is the **reactive protocol** and route discovery and route maintenance occur whenever link [source node to destination node] breaks. It uses periodic broadcast for route discovery. It has a disadvantage of propagation delay for route-discovery.
- DISTANCE VECTOR: It is the **proactive protocol** i.e. table-driven. This protocol is easier to implement and requires much less storage space. It provides flat [non-hierarchical] type architecture.

DSDV

- DSDV models the mobile computers as routers cooperating to forward packets to each other as needed.
- It can be utilized either at network layer (layer-3) or below the network layer but still above the MAC layer software in layer 2.
- The latter case requires additional information to be included alongwith the route tables for the most convenient and efficient operation. (layer 3 protocol info.)
- The information in the route tables is similar to that found in route tables with distance-vector algorithm but it includes a sequence number as well as settling time data useful for damping out fluctuations in route table updates.

DSR: Route Maintenance

- When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted (up to maximum number of attempts) until this confirmation of receipt is received. For example, in the situation illustrated in Figure , node A has originated a packet for E using a source route through intermediate nodes B, C and D. In this case, node A is responsible for receipt of packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D and finally node D is responsible for receipt at E.
- This confirmation of receipt may in many cases be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use (such as the link level acknowledged frame defined by IEEE 802.11 [IEEE 97]) or by passive acknowledgement [Jub87] (in which, for example, B confirms receipt at C by overhearing C transmit the packet to forward it on to D).
- If neither of these confirmation mechanisms is available, the node transmitting the packet may set a bit in the packet's header to request that a DSR-specific software acknowledgement will normally be transmitted directly to the sending node, but, if the link between these two nodes is unidirectional, it may travel over a different, multihop path.

Detailed Operation.

Route Discovery

1. Originating a Route Request.
2. Processing a Route Request option.
3. Originating a Route Reply .
4. Processing a Route Reply Option.

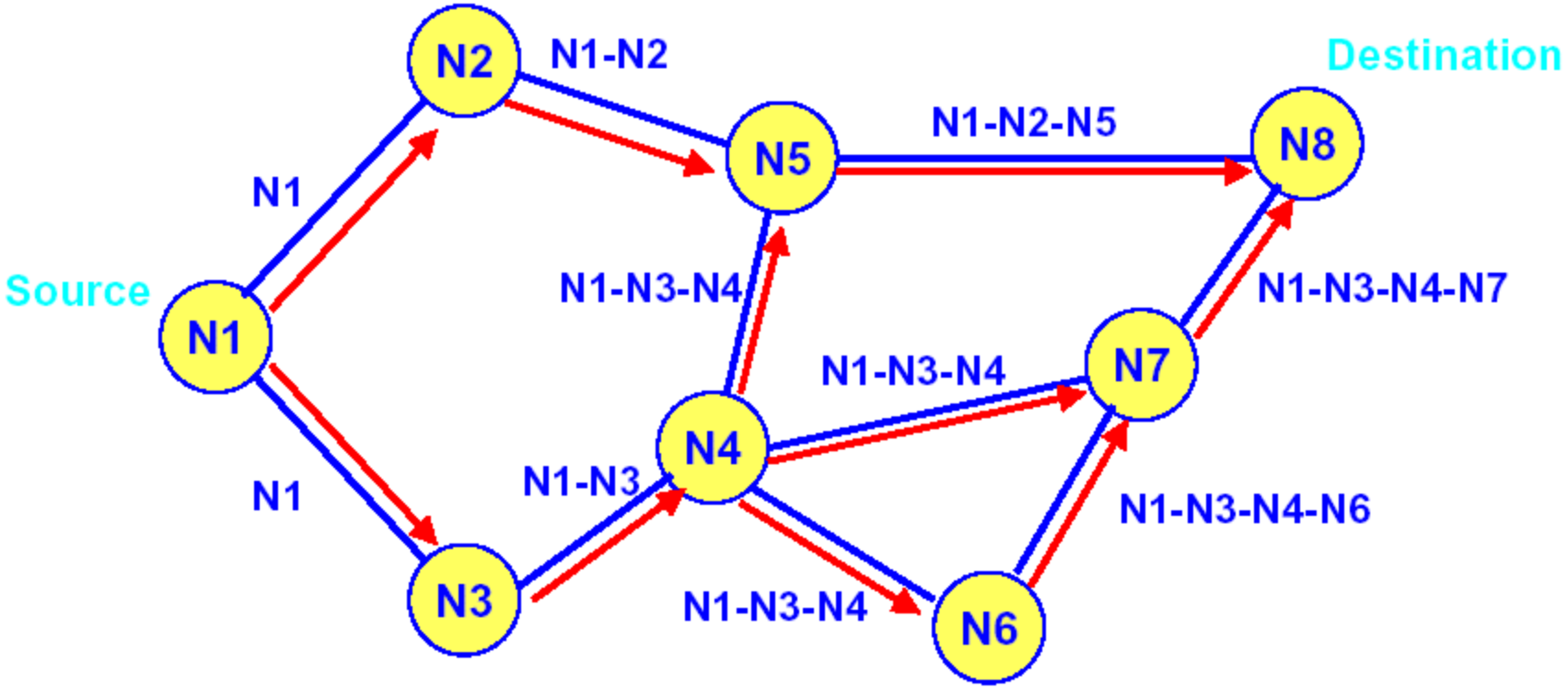
Route Maintenance.

1. Originating a Route Error.
2. Processing a Route Error option.
3. Processing a DSR acknowledgment option.

Processing a Routing Header.

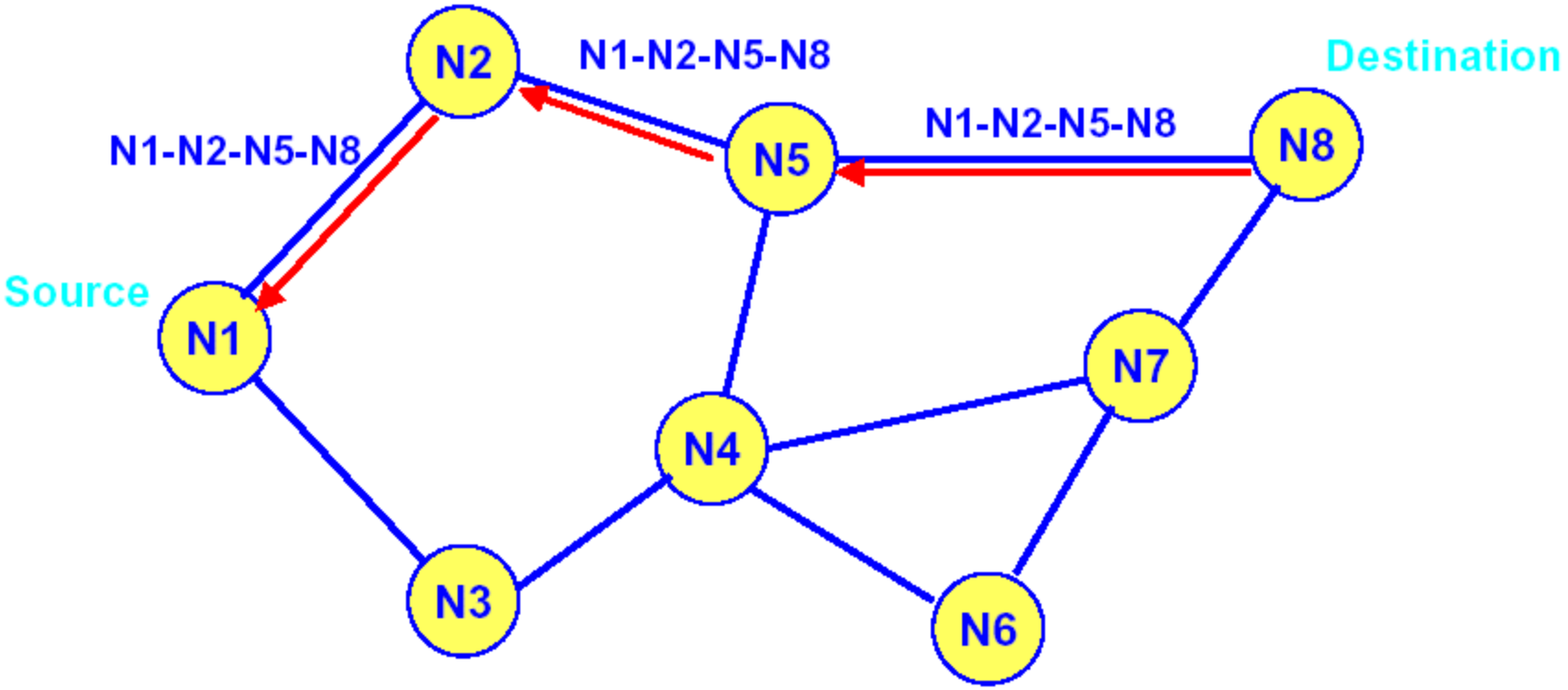
Route Discovery in DSR

- Building of the route record during route discovery



Route Reply in DSR

- Propagation of the route reply with the route record



Advantages

- There is no need of periodic routing messages.
- Due to above reason we can reduce network bandwidth, and conserve the battery power.
- It can also be applied in the presence of unidirectional links.

- Not a complex routing protocol.
- Low packet overhead.
- Routes efficiently.
- Does not require promiscuous mode.

Disadvantages.

- Broadcasting.
- Problems arise if the network is highly dynamic and links are bidirectional.
- Bandwidth is efficient only if the links are bidirectional.

Optimizations

- Promiscuous learning of source routes.
- Answering the route requests using the route cache.
- Improved handling of route errors.
- Rate limiting the Route Discovery process.

AODV

- AODV offers quick adoption to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times, avoiding problems associated with classical distance vector protocols.

ZRP

- The ZRP framework is a hybrid routing framework suitable for a wide variety of mobile ad-hoc networks,especially those with large networks spans and diverse mobility patterns.
- Each node proactively maintains routes within a local region (referred to as the routing zone). Knowledge of the routing zone topology is leveraged by the ZRP to improve the efficiency of globally reactive route query/reply mechanism.The proactive maintenance of routing zones also helps improve the quality of discovered routes,by making them more robust to changes in networks topology.The ZRP can be configured for a particular network by proper selection of a single parameter, the routing zone radius.

ZRP (Zone Routing Protocol)

- Why One more Routing protocol ?
- Reconfigurable Wireless Networks (RWN)
- Use of RWNs
- ZRP : Reactive / Proactive.

Why one more protocol?

- In general, the existing routing protocols can be classified either as proactive or as reactive.
- The advantage of the proactive schemes is that once a route is needed there is little delay until the route is determined .
- In reactive protocols, because route information may not be available at the time of datagram is received, the delay to determine a route can be quite significant.
- Because of this long delay, pure reactive routing protocols may not be applicable to real-time communication.
- However pure proactive schemes are likewise not appropriate for the ad hoc networking environment, as they continuously use a large portion of the network capacity to keep the routing information current.Since nodes in a ad hoc network moves quite fast, and as the changes may be more frequent than the route requests, most of this routing information is never even used. This results in a further waste of the network capacity.
- What is needed is a protocol that, on one hand, initiates the route determination procedure on-demand, but at limited cost. i.e. Hybrid one.

ZRP : RWN

- There is a special class of ad hoc networks, which can be termed as Reconfigurable Wireless Networks (RWN), The current routing protocols do not provide a satisfactory solution for routing in this type of environment.
- The main features of RWNs are increased mobility of networks, a larger number of nodes, and a large network span.
- RWNs are intended to provide a data network that is immediately deployable in arbitrary communication environments and that is responsive to changes in network topology. RWNs are distinguished from other ad hoc networks by rapidly changing network topologies, influenced by network size and node mobility.
- Within a RWN there can be a significant variations in nodal speed (from a stationary node to high speed aircraft) Examples of RWNs are;

  Rescue missions – communication in unexplored area.

  Tactical Operation – fast establishment of military communication in unknown and hostile terrain.

  Commerce – Communications for exhibitions, conferences, sales presentations.

Requirements for RWNs

- Robust routing and mobility management algorithms-
  - To increase network's reliability and availability.
- Adaptive algorithms and protocols
  - To adjust to frequently changing radio propagation, network and traffic conditions.
- Low-overhead algorithms and protocols
  - To preserve the radio communication resource.
- Multiple (distinct) routes
  - Between a source and a destination to reduce congestion in the vicinity of certain nodes and to increase reliability and survivability.
- Nonhierarchical physical network architecture
  - To avoid susceptibility to network failures.

ZRP

- ZRP (zone routing protocol) is proposed to be the routing protocol for the RWN, allowing efficient and fast route discovery in the RWN communication environment.
- The ZRP framework is a hybrid routing framework suitable for a wide variety of mobile ad-hoc networks,especially those with large networks spans and diverse mobility patterns.
- In ZRP a proactive routing protocol provides a detailed and fresh view of each node's surrounding local topology (routing zone) at the local level.
- The knowledge of the local topology is used to support services such as proactive route maintenance, unidirectional link discovery and guided message distribution. Bordercasting is used in place of traditional broadcasting to improve the efficiency of a global reactive routing protocol.

ZRP

- Route discovery in ZRP is distinguished from standard broadcast-based route discovery through a message distribution service known as the Bordercast Resolution Protocol (BRP). Rather than blindly broadcasting a route query from a neighbor to neighbor, bordercasting allows the query to be directed outward, toward regions of the network(specifically toward peripheral nodes) that have not yet been "covered" by the query.
- The benefits provided by routing zones, compared with the overhead of proactively tracking routing zone topology, determine the optimal framework configuration. As network conditions change, the framework can be dynamically reconfigured through adjustment of each node's routing zone.

MANeT : New approach

Clustering

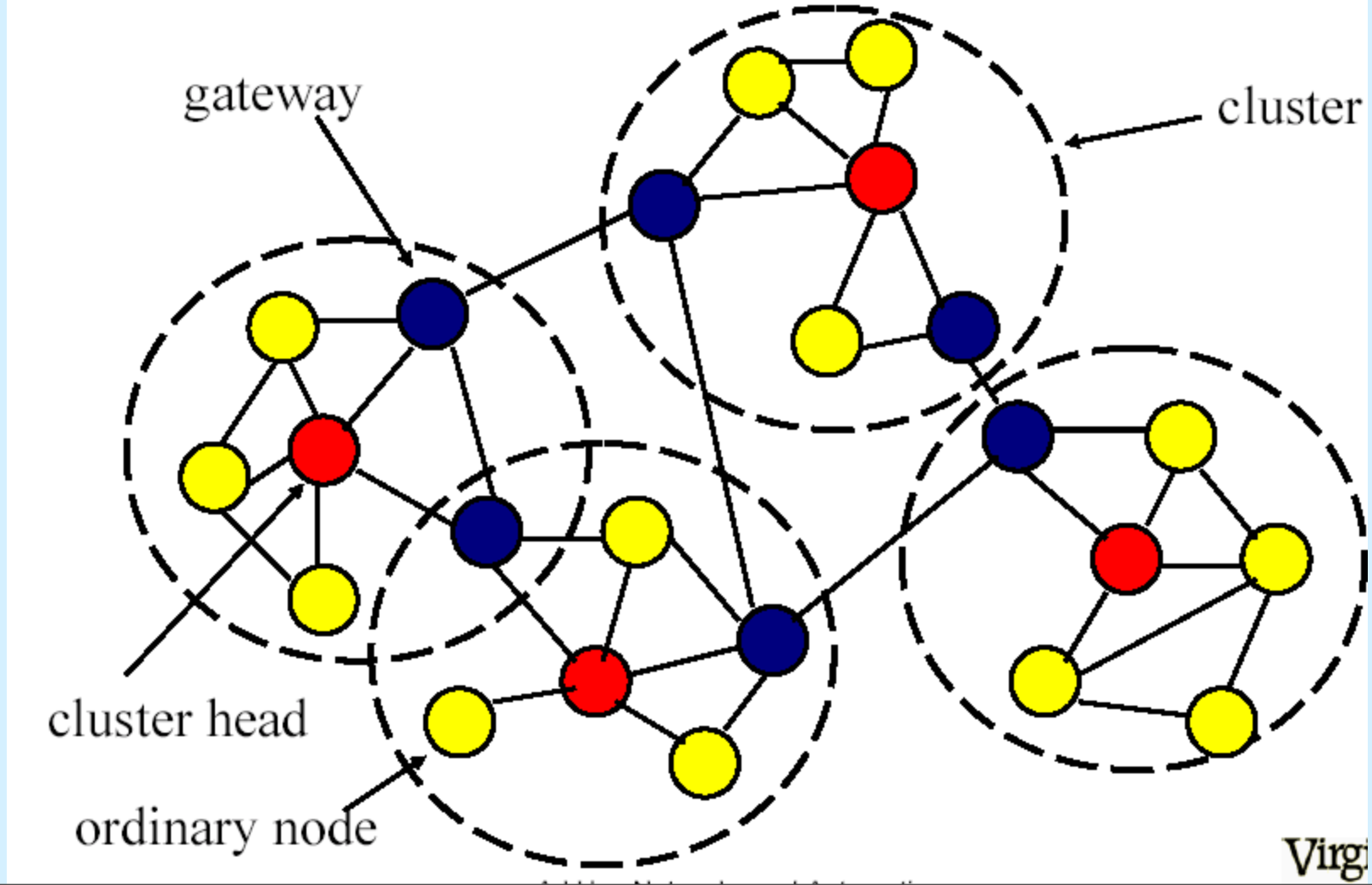
- Transforms the physical network into a virtual network of interconnected node clusters
- Cluster controllers act on behalf of other members of the cluster to make control decisions
- Gateways establish communication between clusters
- The objective is to improve efficiency of resource use by
  - Reducing channel contention
  - Forming routing backbones to reduce network diameter
  - Abstracting network state information to reduce its quantity and variability

Cluster-Based Networks

- Cluster based Control structures for large dynamic networks naturally lend themselves to managing a shared transmission medium, constructing routing backbones and building abstractions of network state, and this have a major impact on network efficiency.
- Ad hoc network possess two properties that make them ideal candidates for cluster based control : mobile nodes, which may cause frequent changes in network connectivity and wireless links, which have shared access, are susceptible to large and frequent fluctuations in quality.
- Cluster based control structures may be considered as a primary means of improving performance of these networks through reduced sensitivity to small changes in state and through localized control in response to significant changes in state.

MANeT : New approach

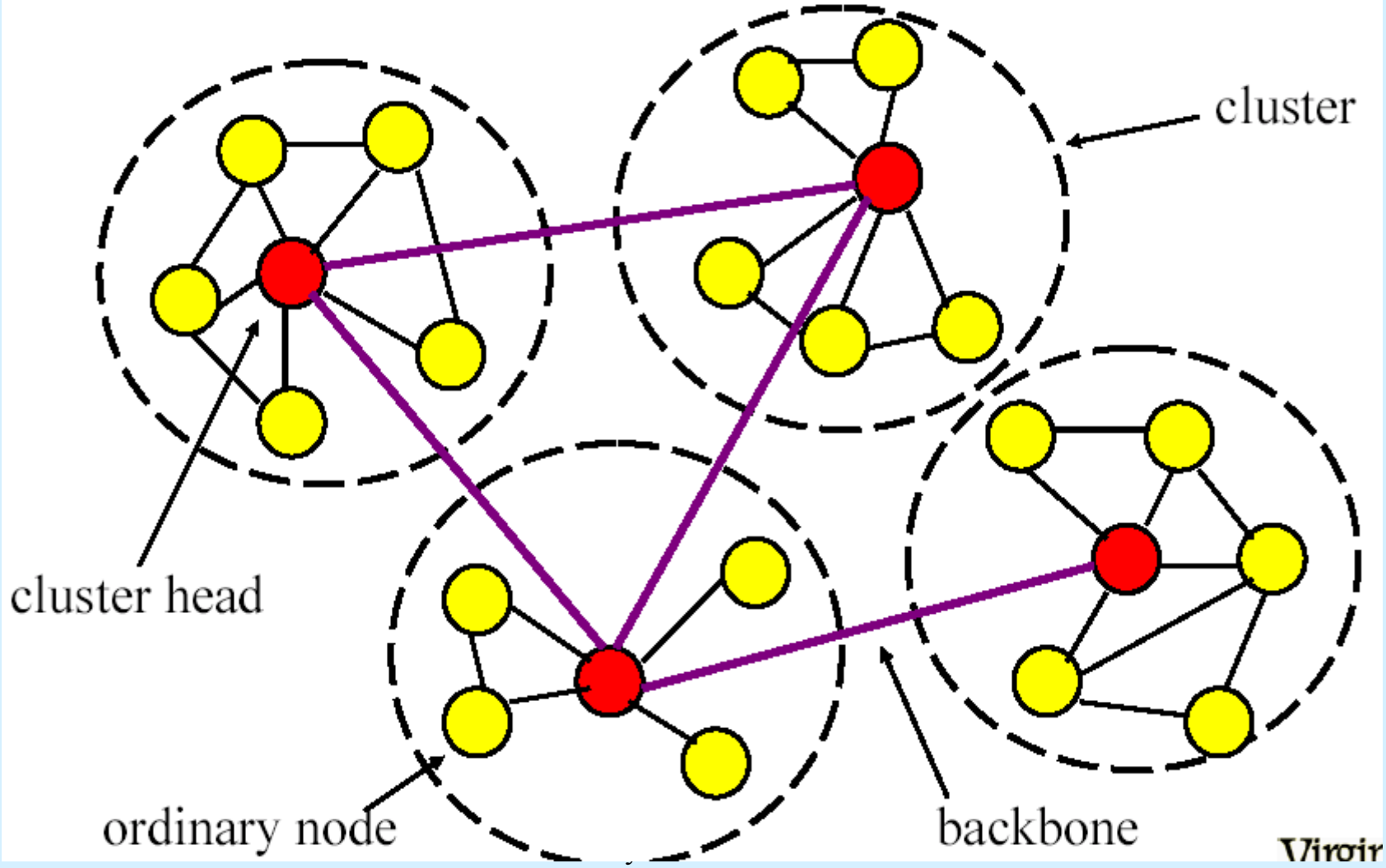
Link-Clustered Architecture (1)



Link-Clustered Architecture (2)

- Must have a protocol for electing clusterheads, choosing gateways
- Provides a natural routing backbone consisting of clusterheads and gateways
  - However, may reduce throughput and network robustness (single point of failure)
- Another option is to use the clusterhead for control purposes but not for routing
  - Each node distributes and collects routing information and chooses routes
  - Neither inter-cluster nor intra-cluster routing requires clusterhead traversal

Clustering for backbone formation Gateway and Head the Same(1)



Clustering for backbone formation (2)

- May create a backbone, reducing delay related to multiple hops
  - Long distance backbone links may be provided by increased transmit power for the clusterheads
- Need a protocol to elect clusterheads, decide cluster affiliation
- For fault-tolerant connectivity and load balancing, may create multiple disjoint routing backbones
  - Virtual Subnet Architecture

Link Reversal Routing

- LRR is a highly adaptive form of routing originally intended for use in networks with rapidly changing topologies. A key concept behind LRR is the decoupling of far-reaching control message propagation from the dynamics of the network's topology. Conceptually it can be thought of as appropriate for use in networks where the rate of topological changes is not so fast as to make flooding the only possible routing method, but not so slow as to make algorithms capable of supporting a shortest-path computation applicable.
- By flooding, we mean a distributed process of broadcasting a packet to all nodes in the network. Practically, results obtained thus far for one LRR algorithm indicate that the techniques range for applicability – relative to other methods-is not so simply stated; rather it is a function of network size, network topology, rate of topological changes, and available bandwidth.

MANeT Routing Protocol : Performance issues

- Amongst various routing protocols, one needs metrics – both qualitative and quantitative - with which to measure its suitability and performance. These metrics should be " independent" of any given routing protocol.
- The following is the desirable qualitative properties of MANeT routing protocols.

1. Distributed Operation : This is an essential property, as any routing protocol should possess the capability of Distributed Operations.
2. Loop-Freedom : Desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary periods.
3. Demand based operation: Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times).
4. Proactive operation: The flip side of demand based operation. In some contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.

MANET Protocols performance…

5. Security: Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet header, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs / wireless networks.

6. "Sleep" Period Operation: As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocols should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocols through a standardized interface.

MANeT Performance issues…

7. Unidirectional link support: Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links. Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, sufficient number of duplex links exist so that usage of unidirectional links is of limited added value. However in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional links (in opposite directions) from the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.

MANET Routing….

Quantitative metrics that can be used to assess the performance of any routing protocol are ;

1. End-to-end data throughput and delay: Statistical measures of data routing performance (e.g. means, variances, distributions) are important. These are the measures of a routing policy's effectiveness– how well it does its job- as measured from the ' external' perspective of other policies that make use of routing.
2. Route acquisition time: A particular form of ' external' end-to-end delay measurement – of particular concern with " on demand" routing algorithms – is the time required to establish route(s) when requested.
3. Percentage out-of-order delivery: An external measure of a connectionless routing performance of particular interest to transport layer protocols such as TCP which prefer in-order delivery.
4. Efficiency : If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can expand differing amounts of overhead, depending on their internal efficiency.

MANeT Routing Protocol : Performance issues

- Protocol efficiency may or may not directly affect data routing performance. If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control traffic often impacts data routing performance.Following are some of the ratios that illuminate the "internal" efficiency of a protocol;

1. Average number of data bits transmitted / data bit delivered – this can be thought of as a measure of the bit efficiency of delivering data within the network. Indirectly it also gives average hop count taken by data packets.
2. Average number of control bits transmitted / data bits delivered – this measures the bit efficiency of the protocol in expanding control overhead to delivery data. Note that this should include not only the bits in the routing control packets, but also the bits in the header of the data packets. i.e. Anything that is not data is control overhead, and should be counted in the control portion of the algorithm.
3. Average number of control and data packets transmitted / data packet delivered – rather than measuring pure algorithmic efficiency in terms of bit count, this measure tries to capture a protocol's channel access efficiency, as cost of C.A. is high.

MANeT Routing Protocol : Performance issues

Networking Context is significant in which a protocol's performance is measured., essential parameters that should be varied are;

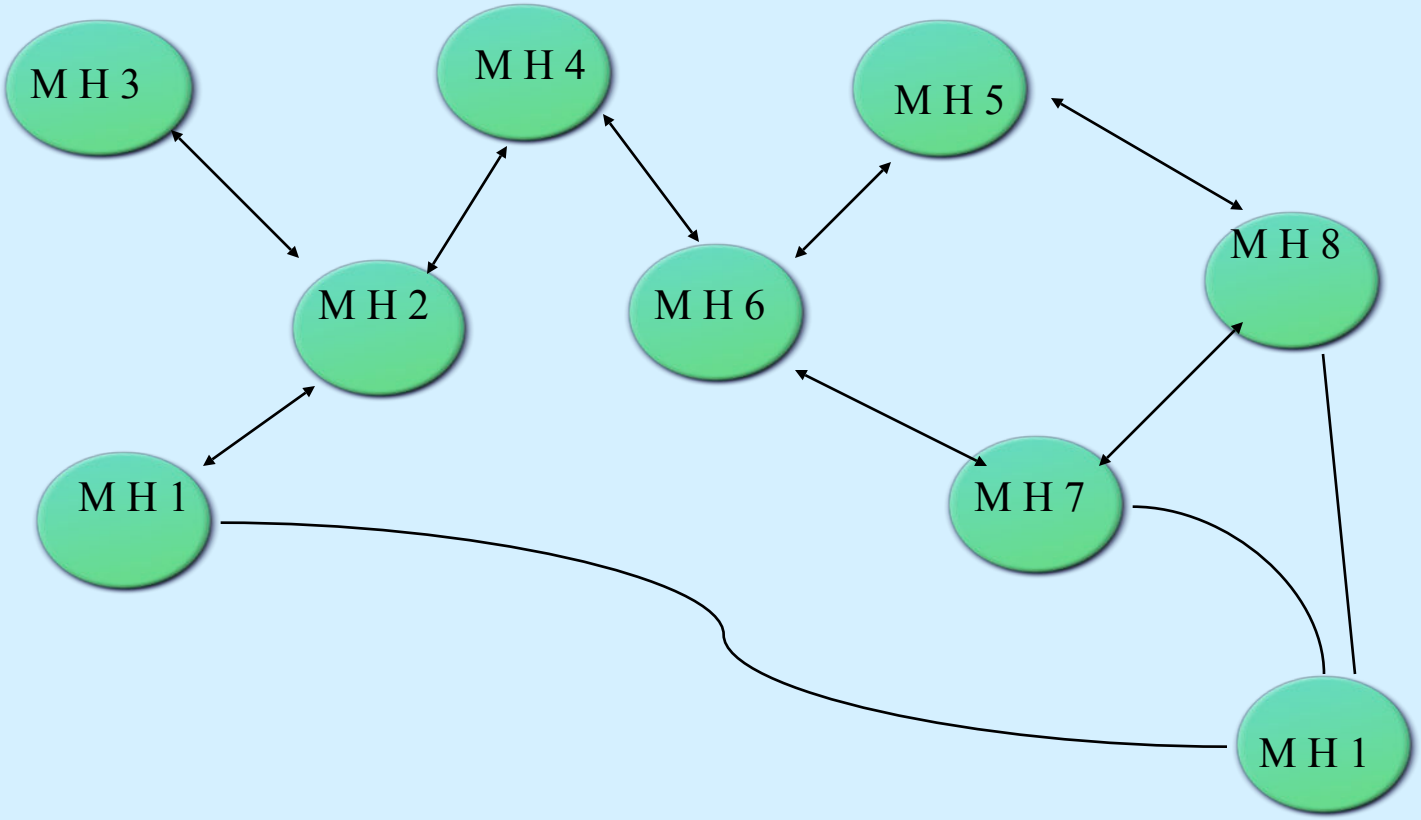
1. Network Size : measured in the number of nodes.
2. Network connectivity – the average degree of a node (i.e. the average number of neighbors of a node)
3. Topological rate of change – the speed with which a network's topology is changing.
4. Link Capacity- effective link speed measured in bits/second, after accounting for losses due to multiple access, coding, framing etc.
5. Function of unidirectional links - how effectively does a protocol perform as a function of the presence of unidirectional links?
6. Traffic patterns- adaption to non-uniform or bursty traffic.
7. Mobility- when and under what circumstances, is temporal and spatial topological correlations relavant to the performance of a routing protocol?
8. Fraction and frequency of sleeping nodes- how does a protocol perform in the presence of sleeping and awakening nodes.

Overview of Routing methods

- Each node in the network maintains for each destination a preferred neighbor (a next hop). Each data packet contains a destination node identifier in its header. When a node receives a data packet, it forwards the packet to the preferred neighbor for its destination. The forwarding process continues until the packet reaches its destination.
- The manner in which route tables are constructed, maintained, and updated differs from one routing method to another. Popular routing methods however attempt to achieve the common objective of routing packets along the optimal path. The next-hop routing methods can be categorized as two primary classes: Link state and distance vector .

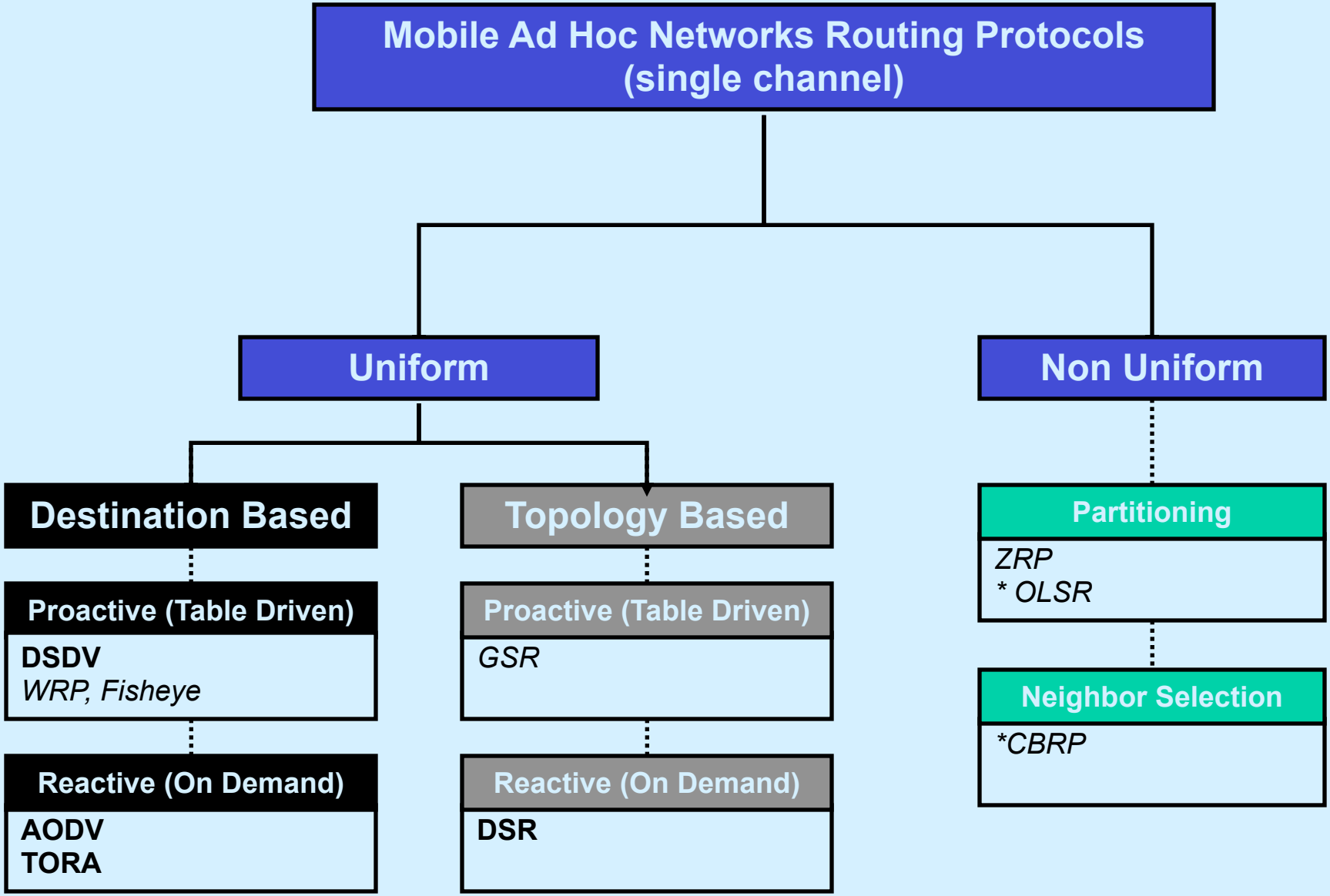
The small ad hoc network scenario when MH1 moves away from MH2 and establishes new links with MH7 and MH8 . Many algorithms also allow for the appearance of new mobile nodes and the disappearance of previously available nodes.

Figure-



DSDV

- DSDV models the each node or mobile computer as a specialized router cooperating to forward packets to each other as needed. Periodically advertises its view of the interconnection topology with other mobile nodes within the network.
- It can be utilized either at network layer (layer-3) or below the network layer but still above the MAC layer software in layer 2.
- The latter case requires additional information to be included alongwith the route tables for the most convenient and efficient operation. (layer 3 protocol info.)
- The information in the route tables is similar to that found in route tables with distance-vector algorithm but it includes a sequence number as well as settling time data useful for damping out fluctuations in route table updates

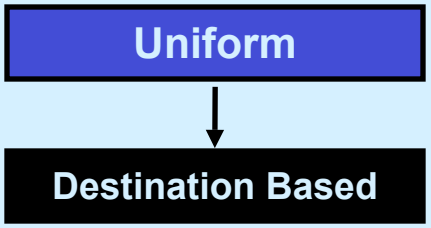

Mobile Ad Hoc Networks Routing Protocols
(single channel)
Uniform
Non Uniform
Destination Based
Topology Based
Partitioning
ZRP
* OLSR
Proactive (Table Driven)
DSDV
WRP, Fisheye
Proactive (Table Driven)
GSR
Neighbor Selection
*CBRP
Reactive (On Demand)
AODV
TORA
Reactive (On Demand)
DSR

Introduction

Uniform

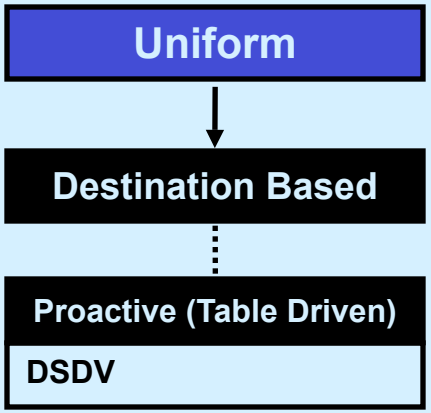
- DSDV is Uniform
  - Each node sends and responds to routing control message the same way
  - No hierarchical structure
  - Avoids the resource costs involved in maintaining high-level structure
  - Scalability may become an issue in larger networks

Introduction



- DSDV is Destination Based
  - Nodes maintain only local topology information
    (e.g. 1 or 2-hop neighborhood)
  - No global view of topology
  - Possible inconsistencies (e.g. loops)

Introduction

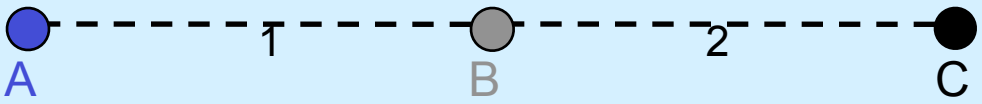


- DSDV is Proactive (Table Driven)
  - Each node maintains routing information for all known destinations
  - Routing information must be updated periodically (no sleeping nodes)
  - Traffic overhead even if there is no change in network topology
  - Maintains routes which are never used

Distance Vector

- Basic Routing Protocol [2]
  - known also as Distributed Bellman-Ford or RIP
- Every node maintains a routing table
  - all available destinations
  - the next node to reach to destination
  - the number of hops to reach the destination
- Periodically send table to all neighbors to maintain topology
- Bi-directional links are required!

Distance Vector (Tables)

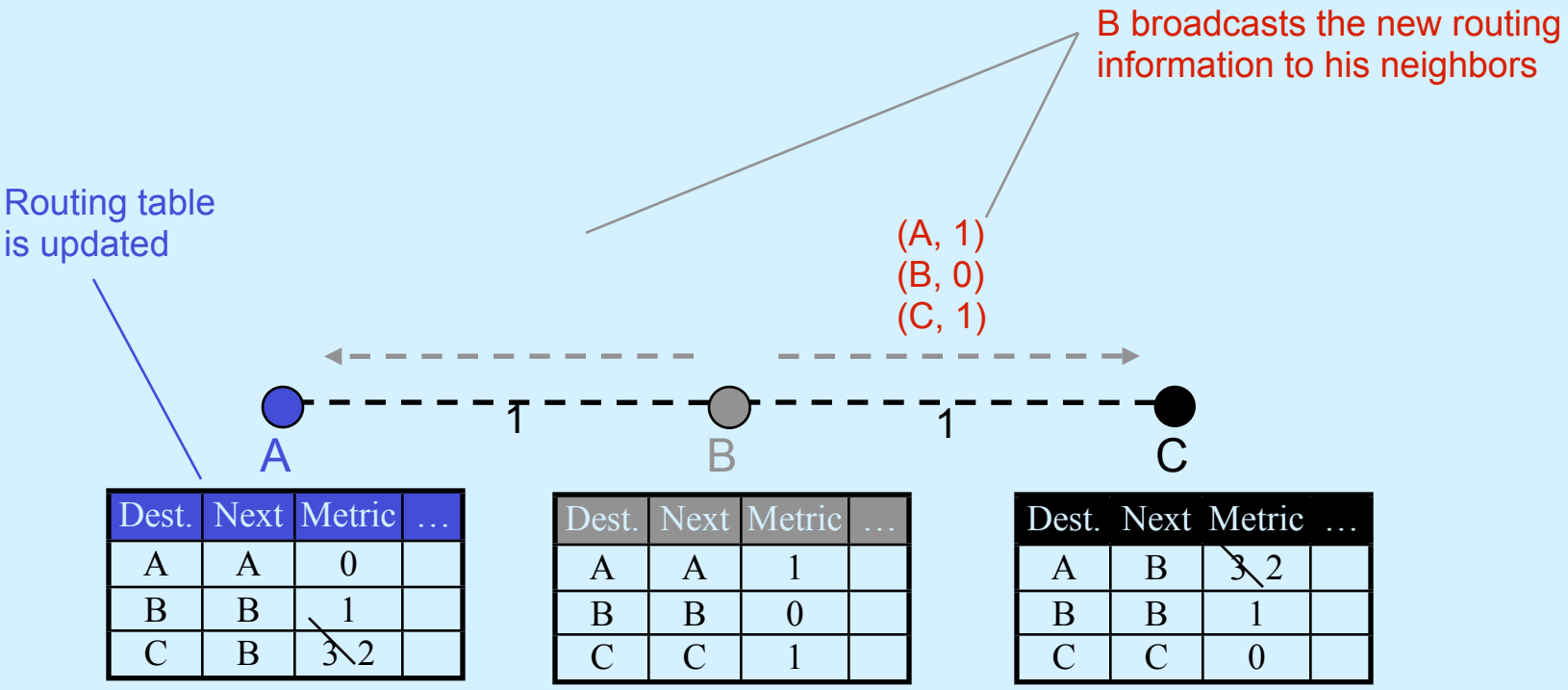


Dest.	Next	Metric	…
A	A	0	
B	B	1	
C	B	3	

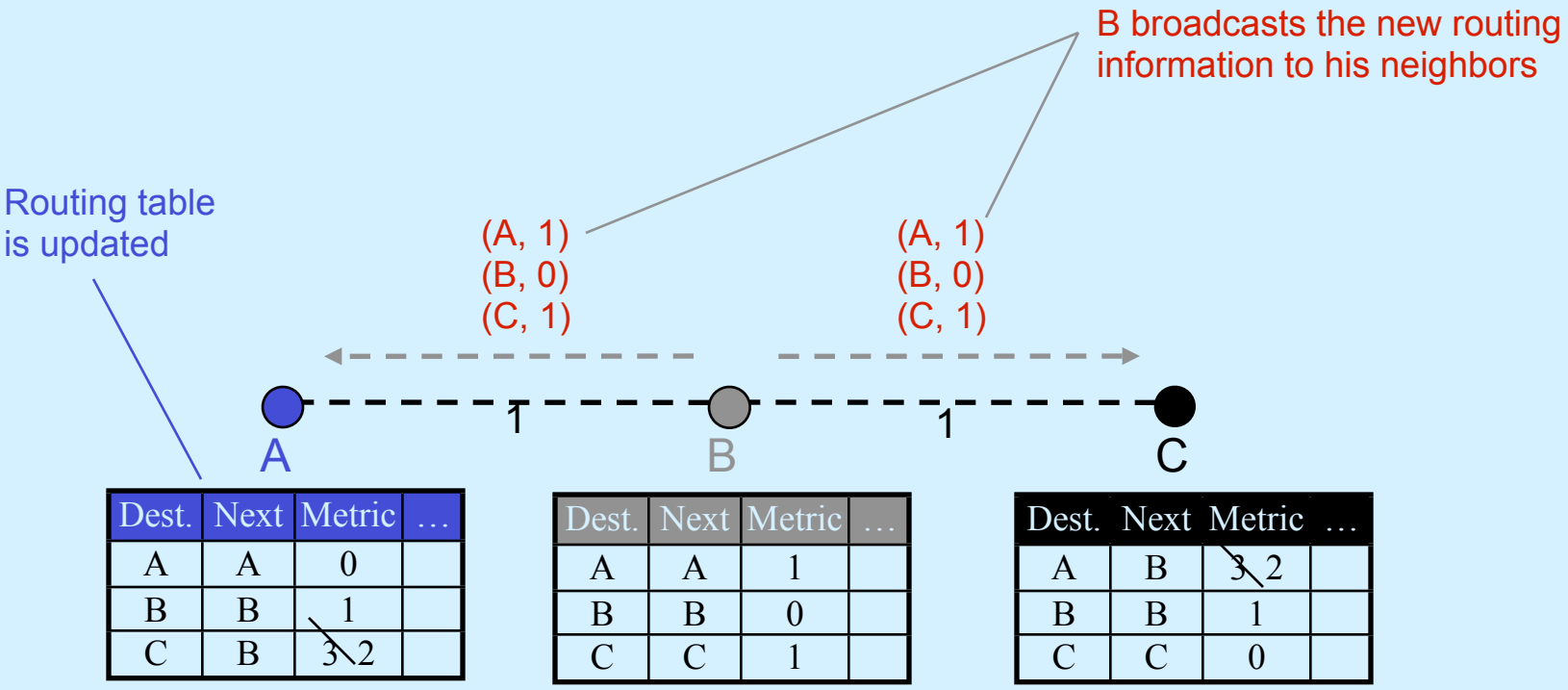
Dest.	Next	Metric	…
A	A	1	
B	B	0	
C	C	2	

Dest.	Next	Metric	…
A	B	3	
B	B	2	
C	C	0	

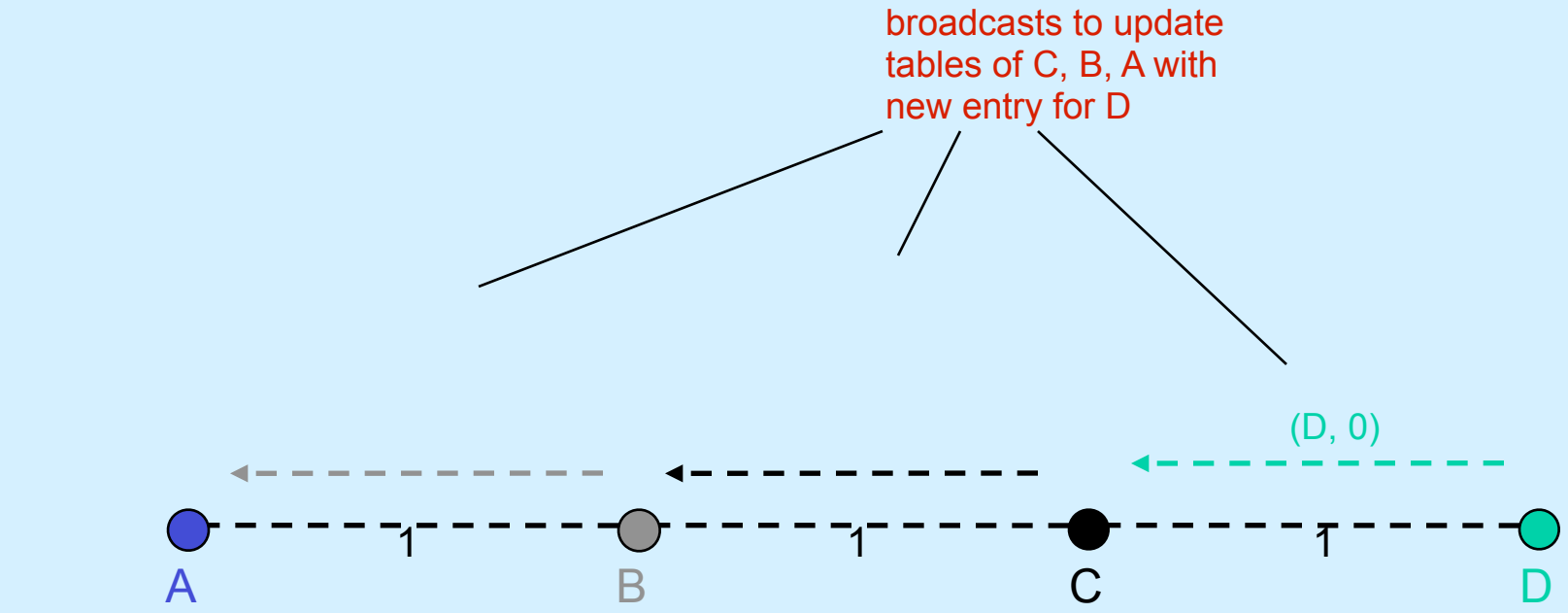
Distance Vector (Update)



Distance Vector (Update)



Distance Vector (New Node)

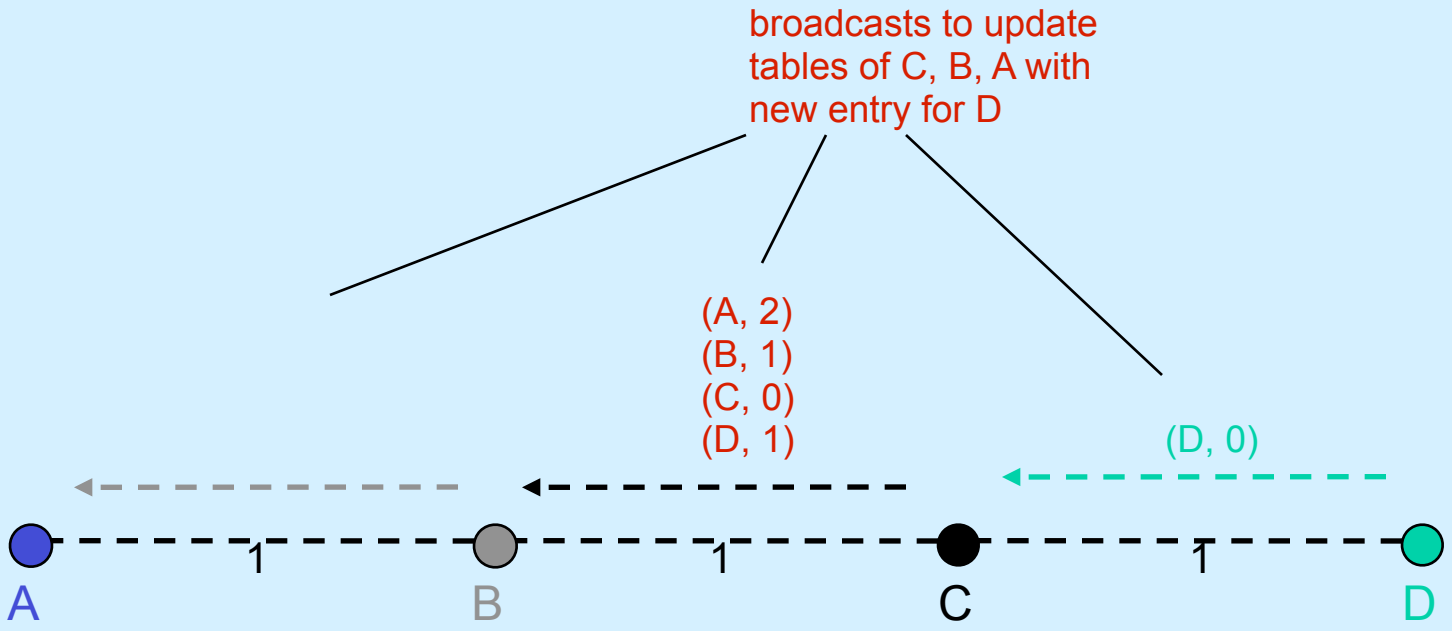


Dest.	Next	Metric	…
A	A	0	
B	B	1	
C	B	2	
D	B	3	

Dest.	Next	Metric	…
A	A	1	
B	B	0	
C	C	1	
D	C	2	

Dest.	Next	Metric	…
A	B	2	
B	B	1	
C	C	0	
D	D	1	

Distance Vector (New Node)

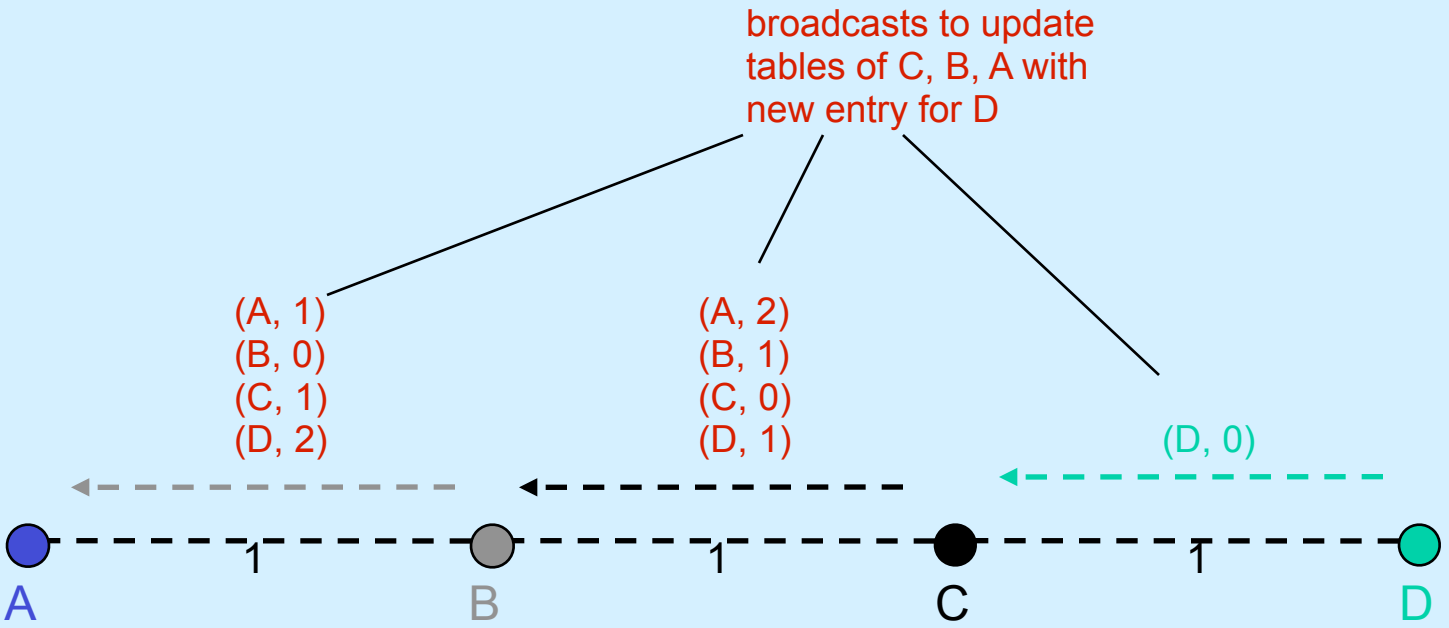


Dest.	Next	Metric	…
A	A	0	
B	B	1	
C	B	2	
D	B	3	

Dest.	Next	Metric	…
A	A	1	
B	B	0	
C	C	1	
D	C	2	

Dest.	Next	Metric	…
A	B	2	
B	B	1	
C	C	0	
D	D	1	

Distance Vector (New Node)

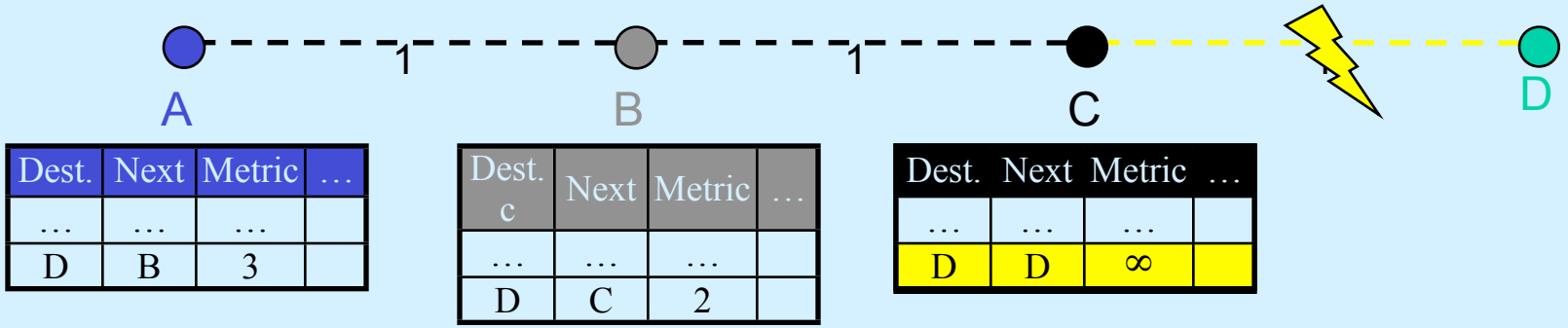


Dest.	Next	Metric	…
A	A	0	
B	B	1	
C	B	2	
D	B	3	

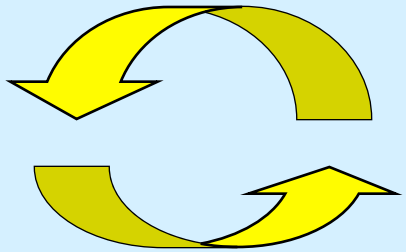
Dest.	Next	Metric	…
A	A	1	
B	B	0	
C	C	1	
D	C	2	

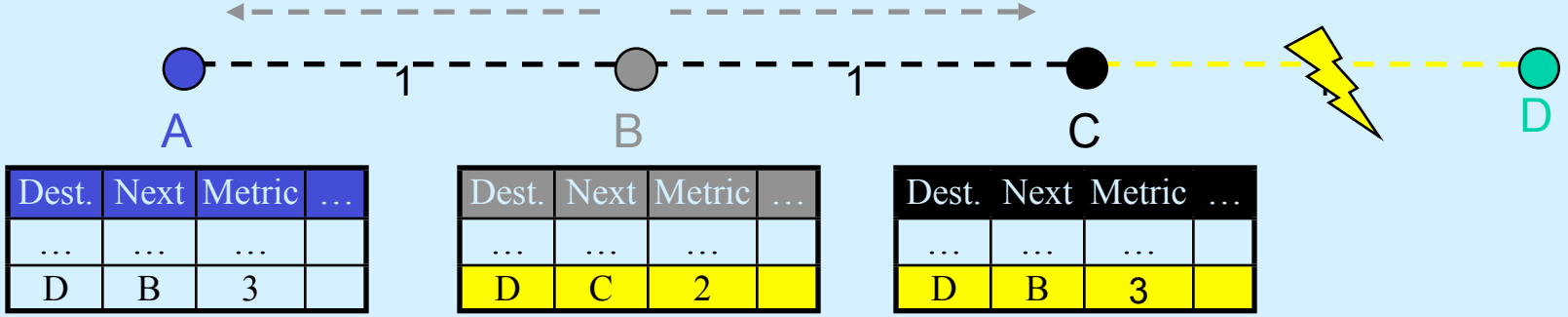
Dest.	Next	Metric	…
A	B	2	
B	B	1	
C	C	0	
D	D	1	

Distance Vector (Broken Link)

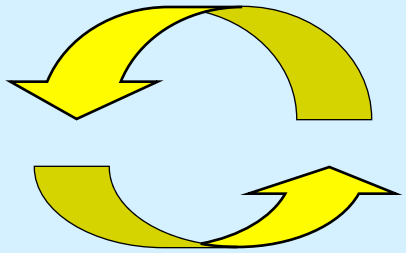


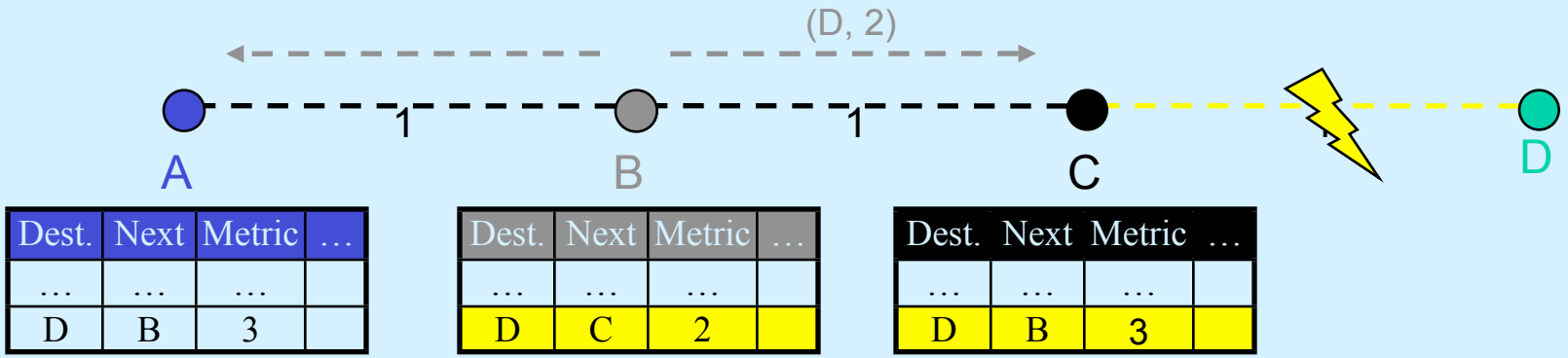
Distance Vector (Loops)



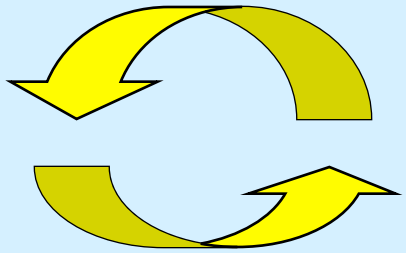


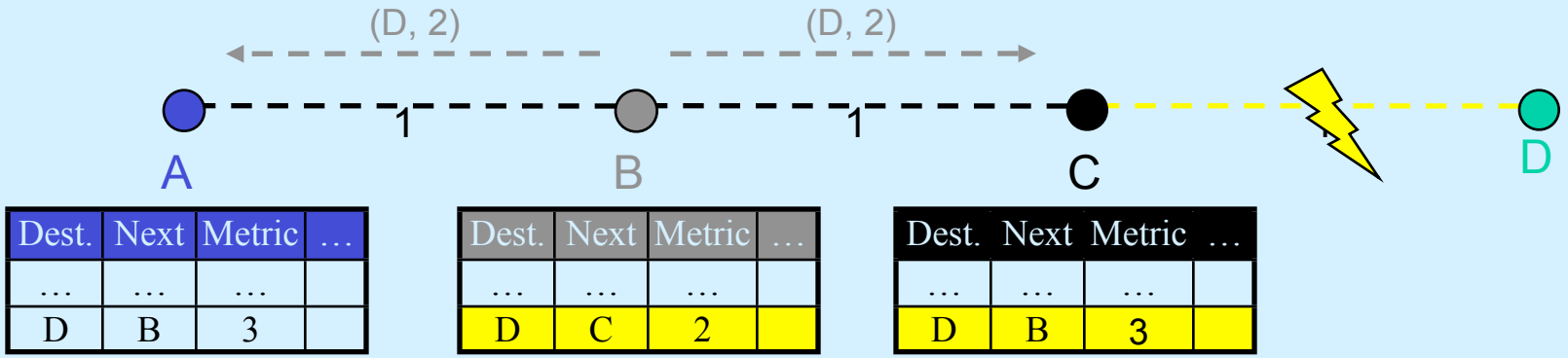
Distance Vector (Loops)



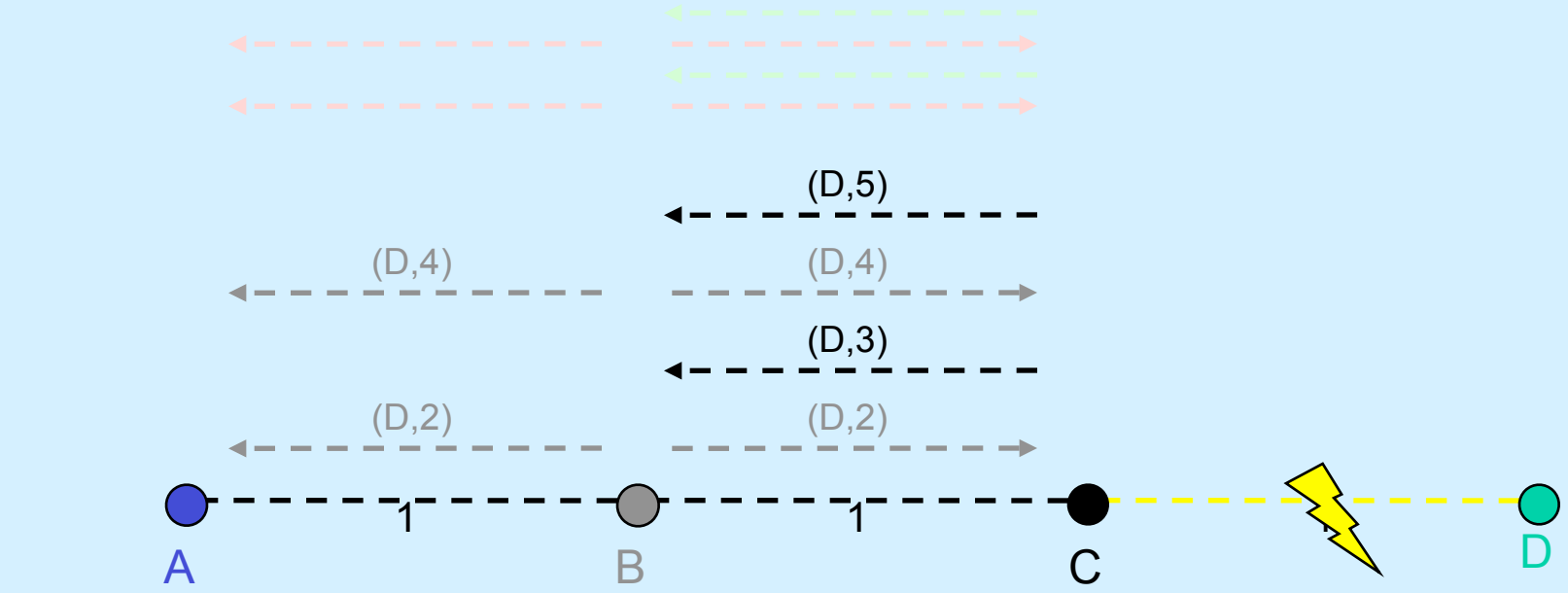


Distance Vector (Loops)





Distance Vector (Count to Infinity)



Dest.	Next	Metric	…
…	…	…	
D	B	3, 5, …	

Dest. c	Next	Metric	…
…	…	…	
D	C	2, 4, 6…	

Dest.	Next	Metric	…
…	…	…	
D	B	3, 5, …	

Distance Vector

- DV not suited for ad-hoc networks!
  - Loops
    - Bandwidth reduction in network
    - Unnecessary work for loop nodes
  - Count to Infinity
    - Very slow adaptation to topology changes.
- Solution -> DSDV

DSDV Protocol

- Keep the simplicity of Distance Vector
- Guarantee Loop Freeness
  - New Table Entry for Destination Sequence Number
- Allow fast reaction to topology changes
  - Make immediate route advertisement on significant changes in routing table
  - but wait with advertising of unstable routes (damping fluctuations)

DSDV (Table Entries)

Destination	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr_C
D	B	4	D-312	001200	Ptr_D

- **Sequence number** originated from destination. Ensures loop freeness.
- **Install Time** when entry was made (used to delete stale entries from table)
- **Stable Data** Pointer to a table holding information on how stable a route is. Used to damp fluctuations in network.

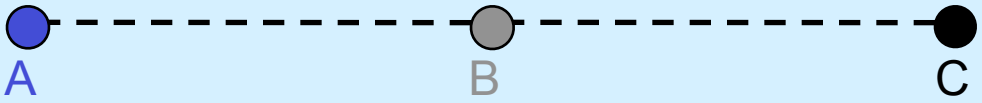
DSDV (Route Advertisements)

- Advertise to each neighbor own routing information
  - Destination Address
  - Metric = Number of Hops to Destination
  - Destination Sequence Number
  - Other info (e.g. hardware addresses)
- Rules to set sequence number information
  - On each advertisement increase own destination sequence number (use only even numbers)
  - If a node is no more reachable (timeout) increase sequence number of this node by 1 (odd sequence number) and set metric = ∞.

DSDV (Route Selection)

- Update information is compared to own routing table
  - 1. Select route with higher destination sequence number (This ensure to use always newest information from destination)
  - 2. Select the route with better metric when sequence numbers are equal.

DSDV (Tables)



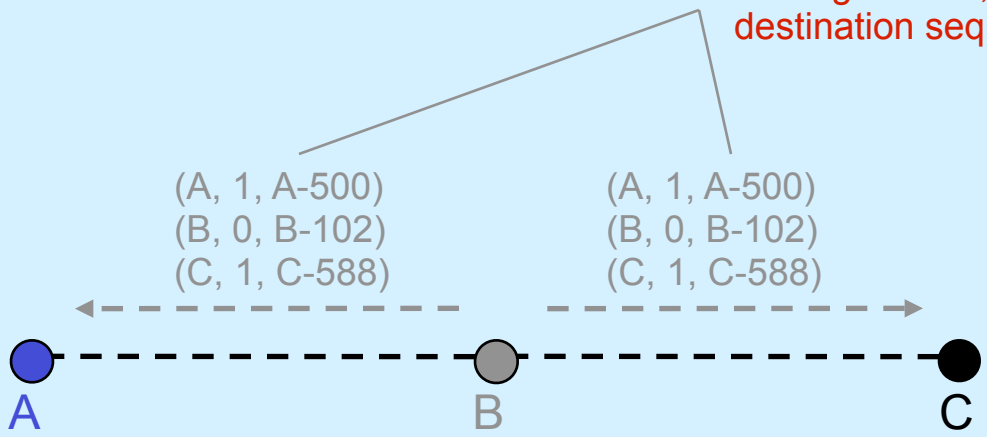
Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	2	C-586

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	2	C-588

Dest.	Next	Metric	Seq.
A	B	1	A-550
B	B	2	B-100
C	C	0	C-588

DSDV (Route Advertisement)

B increases Seq.Nr from 100 -> 102
B broadcasts routing information to Neighbors A, C including destination sequence numbers



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

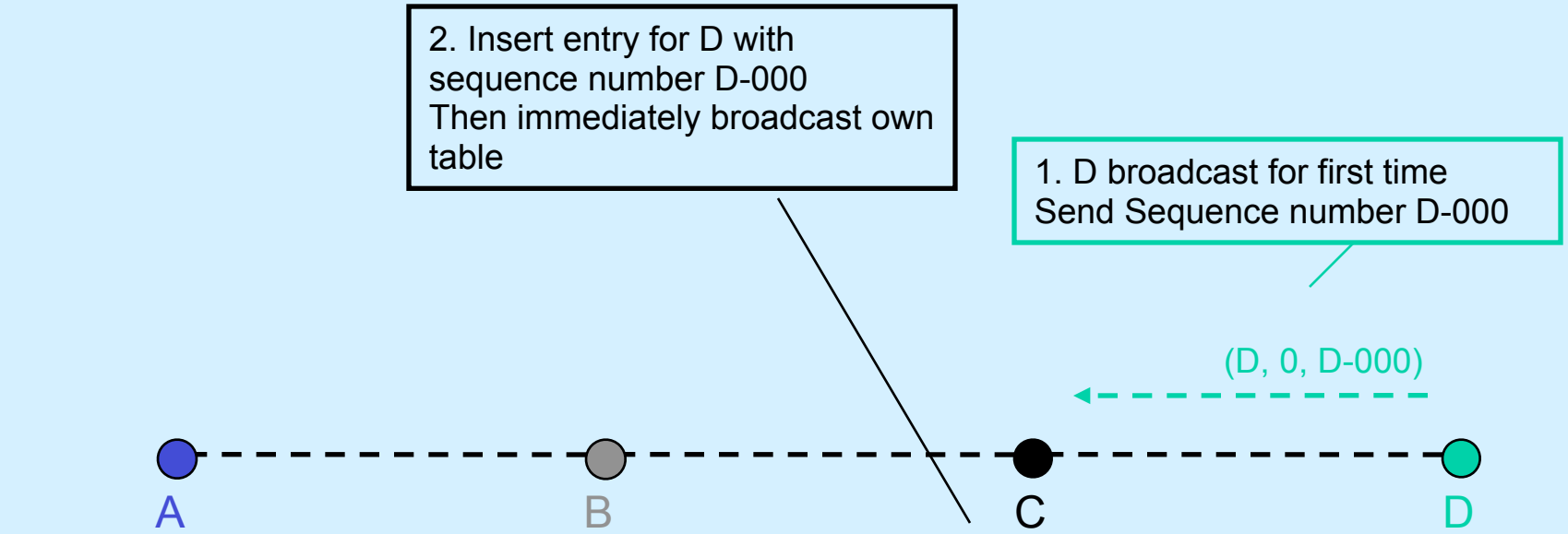
Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

DSDV (Respond to Topology Changes)

- Immediate advertisements
  - Information on new Routes, broken Links, metric change is immediately propagated to neighbors.

- Full/Incremental Update:
  - Full Update: Send all routing information from own table.
  - Incremental Update: Send only entries that has changed. (Make it fit into one single packet)

DSDV (New Node)

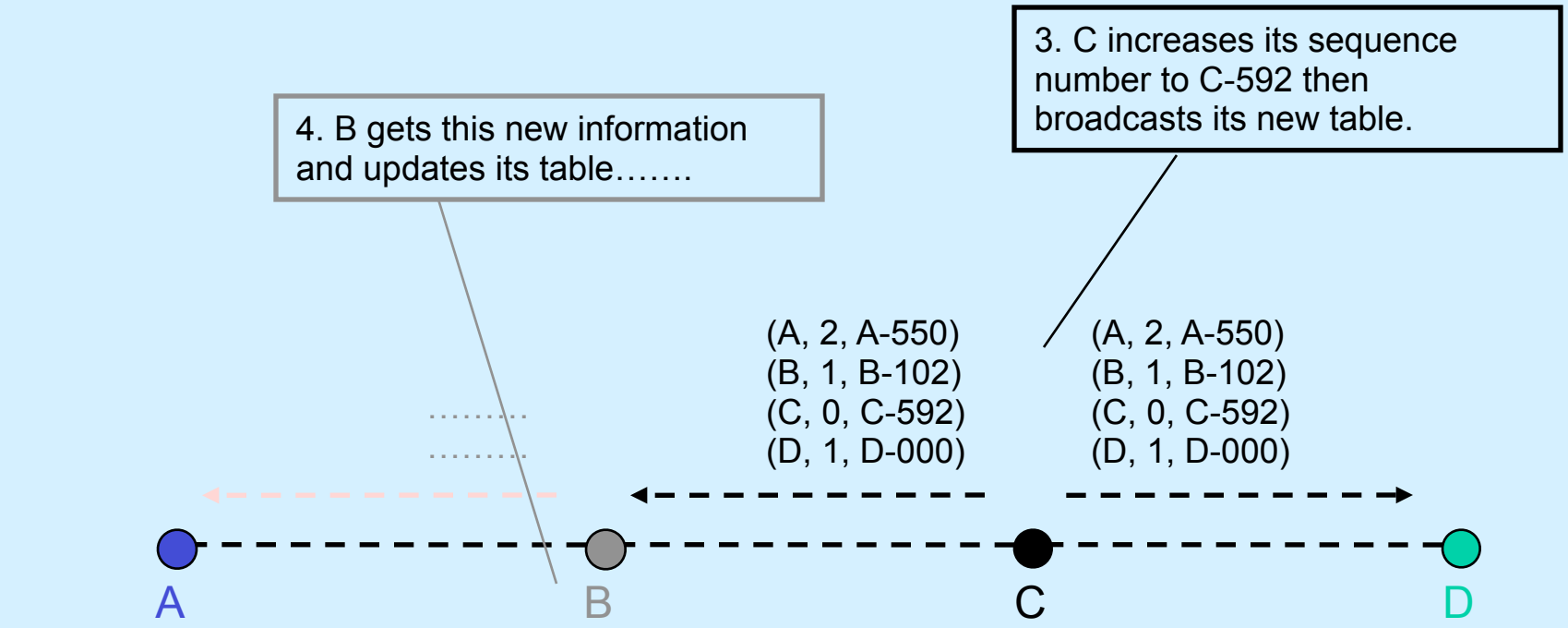


Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-104
C	C	1	C-590

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-104
C	C	0	C-590
D	D	1	D-000

DSDV (New Node cont.)



Dest.	Next	Metric	Seq.
A	A	0	A-550
B	B	1	B-104
C	B	2	C-590

Dest.	Next	Metric	Seq.
A	A	1	A-550
B	B	0	B-102
C	C	1	C-592
D	C	2	D-000

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-592
D	D	1	D-000

DSDV (no loops, no count to infinity)

2. B does its broadcast
-> no affect on C (C knows that B has stale information because C has higher seq. number for destination D)
-> no loop -> no count to infinity

1. Node C detects broken Link:
-> Increase Seq. Nr. by 1
(only case where not the destination sets the sequence number -> odd number)

Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

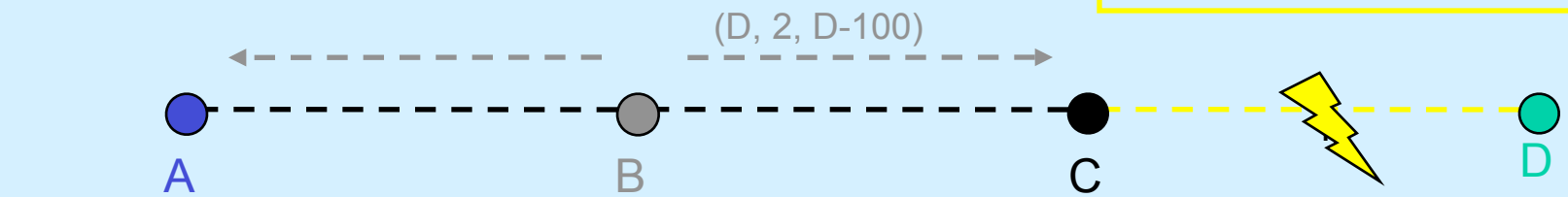
Dest. c	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

Dest.	Next	Metric	Seq.
…	…	…	
D	D	∞	D-101

DSDV (no loops, no count to infinity)

2. B does its broadcast
-> no affect on C (C knows that B has stale information because C has higher seq. number for destination D)
-> no loop -> no count to infinity

1. Node C detects broken Link:
-> Increase Seq. Nr. by 1
(only case where not the destination sets the sequence number -> odd number)



Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

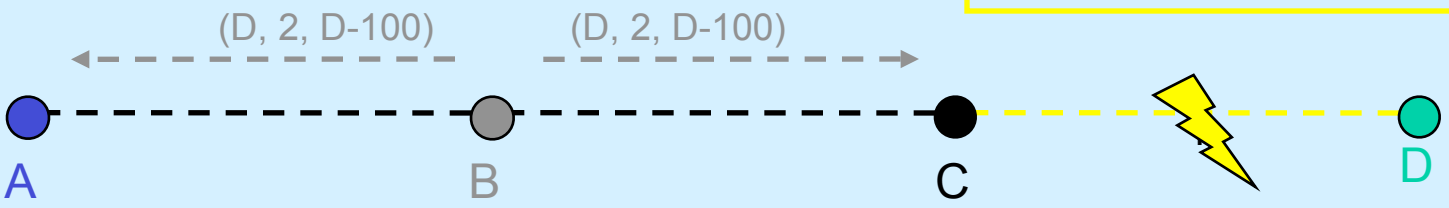
Dest. c	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

Dest.	Next	Metric	Seq.
…	…	…	
D	D	∞	D-101

DSDV (no loops, no count to infinity)

2. B does its broadcast
-> no affect on C (C knows that B has stale information because C has higher seq. number for destination D)
-> no loop -> no count to infinity

1. Node C detects broken Link:
-> Increase Seq. Nr. by 1
(only case where not the destination sets the sequence number -> odd number)

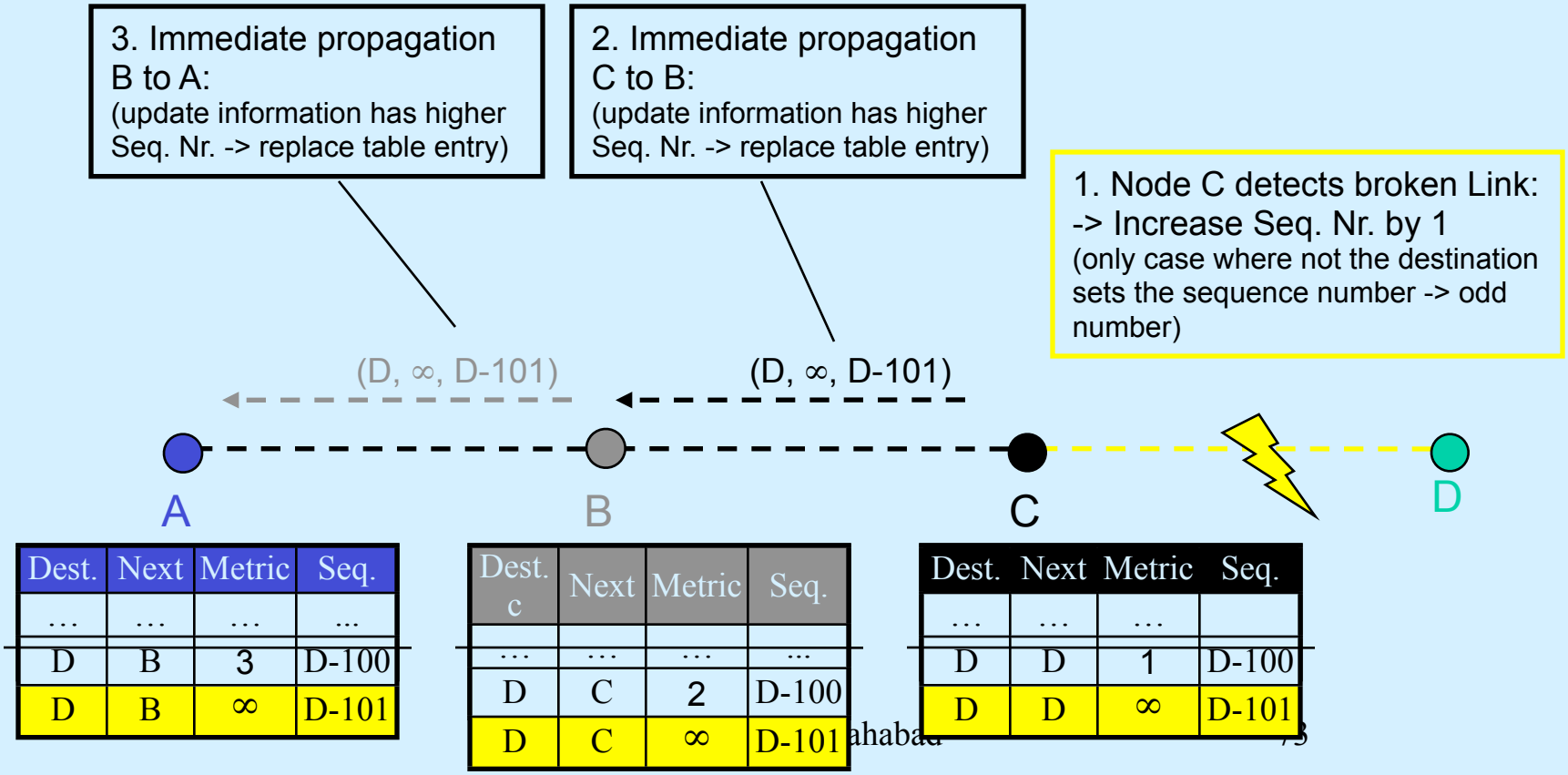


Dest.	Next	Metric	Seq.
…	…	…	
D	B	3	D-100

Dest. c	Next	Metric	Seq.
…	…	…	
D	C	2	D-100

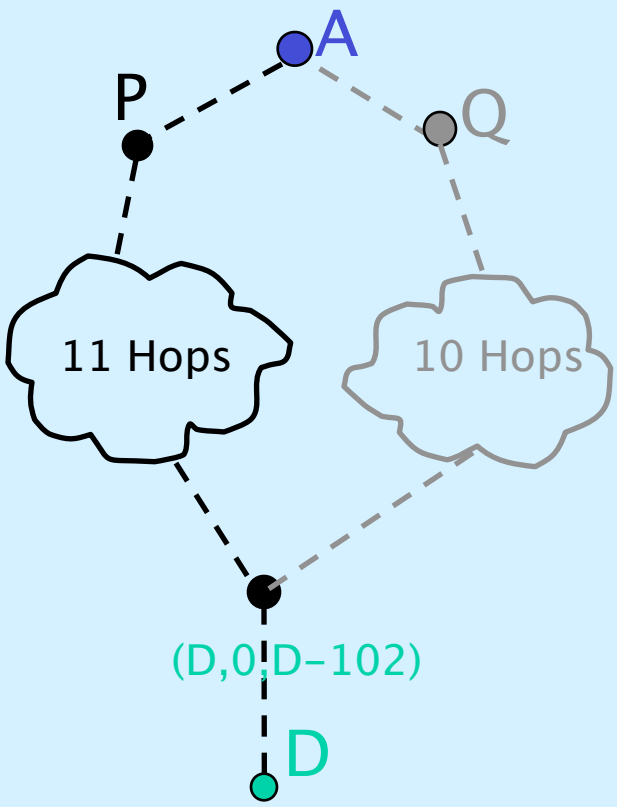
Dest.	Next	Metric	Seq.
…	…	…	
D	D	∞	D-101

DSDV (Immediate Advertisement)



DSDV (Problem of Fluctuations)

What are Fluctuations



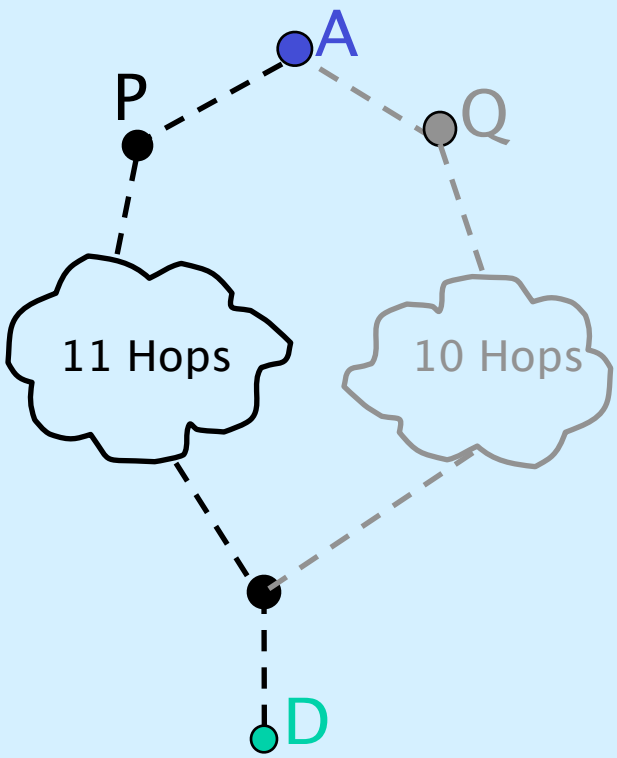
- Entry for D in A: [D, Q, 14, D-100]

- D makes Broadcast with Seq. Nr. D-102
- A receives from P Update (D, 15, D-102)
  -> Entry for D in A: [D, P, 15, D-102]
  A must propagate this route immediately.
- A receives from Q Update (D, 14, D-102)
  -> Entry for D in A: [D, Q, 14, D-102]
  A must propagate this route immediately.

This can happen every time D or any other node does its broadcast and lead to unnecessary route advertisements in the network, so called fluctuations.

DSDV (Damping Fluctuations)

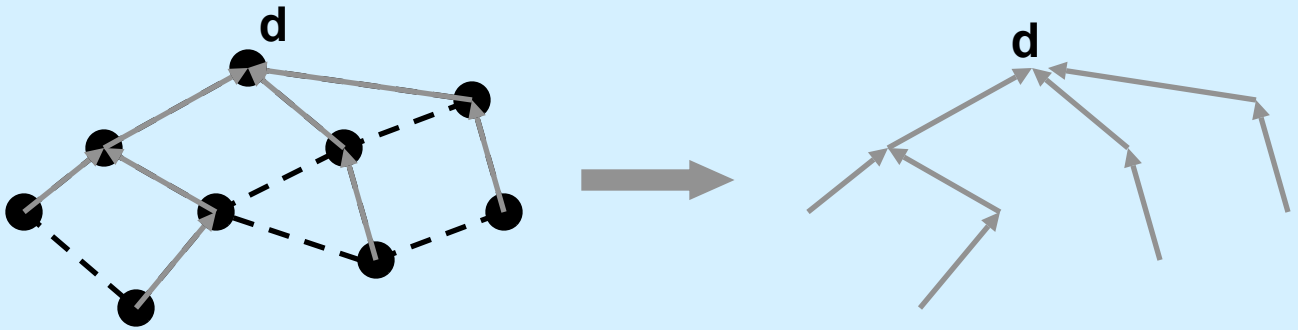
How to damp fluctuations



- Record last and avg. Settling Time of every Route in a separate table. (Stable Data) Settling Time = Time between arrival of first route and the best route with a given seq. nr.
- A still must update his routing table on the first arrival of a route with a newer seq. nr., but he can wait to advertising it. Time to wait is proposed to be 2*(avg. Settling Time).
- Like this fluctuations in larger networks can be damped to avoid unececarry adverdisment, thus saving bandwith.

DSDV (Loop Free Property)

- Prove Part I:
  - Assume we start with no loops
    All routes to destination d form a directed tree G(d) with d as root



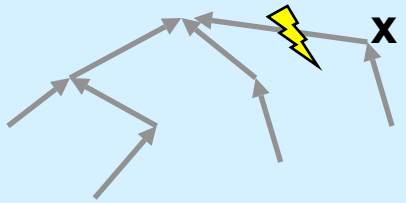
  - **Invariant of DSDV:**
    Graph G(d) is loop free ó G(d) = Set of disjoint directed trees

DSDV (Loop Free Property)

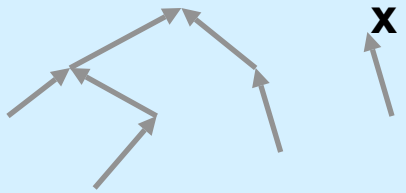
- Prove Part II:
  - Case A: Node **x** sets metric for next hop to infinity

This operation is equal to

deleting the arrow outgoing from x
in the graph.



=> Set of disjoint directed trees **P**



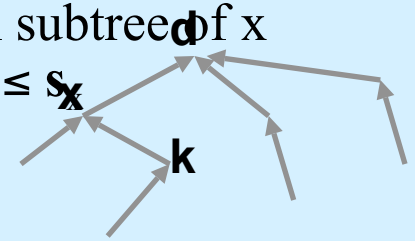
DSDV (Loop Free Property)

- Prove Part II:
  - Case B: Node **x** receives an update from a node **k** for the route to destination **d**

1) $\mathbf{s_k} > \mathbf{s_x}$ (k has higher sequence number from d)

Loop = x sets route to k and k is in subtree of x
But for nodes k in subtree of x: $\mathbf{s_k} \leq \mathbf{s_x}$

Contradiction => no loop possible



2) $\mathbf{s_k} = \mathbf{s_x}$ & $\mathbf{m_k} < \mathbf{m_x}$ (better metric to reach d over k)

distance vector is always loop free in the case of decreasing metrics

(theorem proved by Jaffe and Moss [3])

Summary

- Advantages
  - Simple (almost like Distance Vector)
  - Loop free through destination seq. numbers
  - No latency caused by route discovery
- Disadvantages
  - No sleeping nodes
  - Bi-directional links required
  - Overhead: most routing information never used
  - Scalability is a major problem

Sensor Networks: Outline

- Introduction
- Applications of sensor networks
- Issues in Sensor networks
  - Attributes & Generation of Sensor networks.
  - Research Projects in various aspects of Sensor networks.
  - QoS & Communication.
- Factors influencing sensor network design
- Communication architecture of sensor networks
- Conclusion

Introduction

Recent advances in Wireless communication and electronics has enabled the development of low cost, low power, multifunctional sensor nodes forming a sensor network.

A **sensor network** is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it.

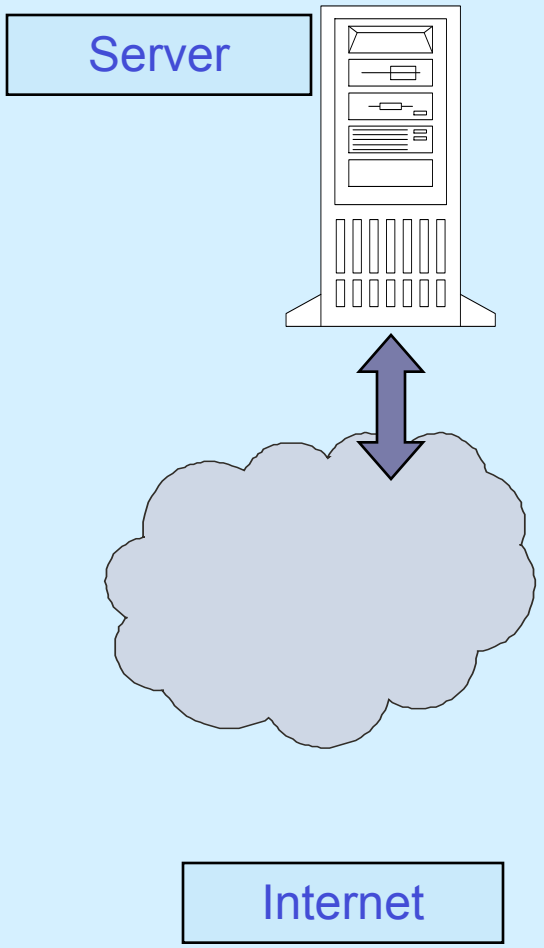
- Random deployment – *need not be engineered !*
- Cooperative capabilities – *they use their local processing capabilities to carry out simple computations and transmit only the required and partially processed data*
- Sensor nodes are fitted with an onboard processor

Wireless Sensor networks

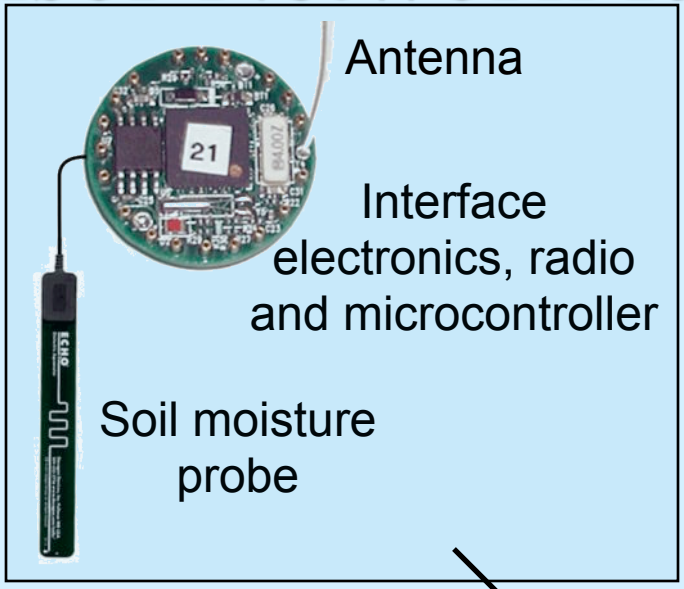
- Background: Wireless networks are becoming sufficiently low-cost that deploying hundreds of individual sensors in a distributed sensor network now is realistic.
- Objective: Configure a small wireless sensor network to deploy in a field setting demonstrating the availability of the sensor data in real-time.
- Conclusion: The abundance of wireless sensors will increase over time because they can be reliably deployed in any field setting.

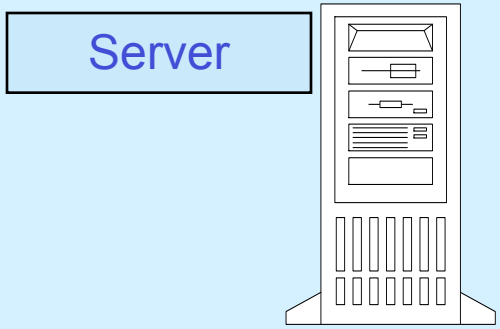
Sensor Network functioning

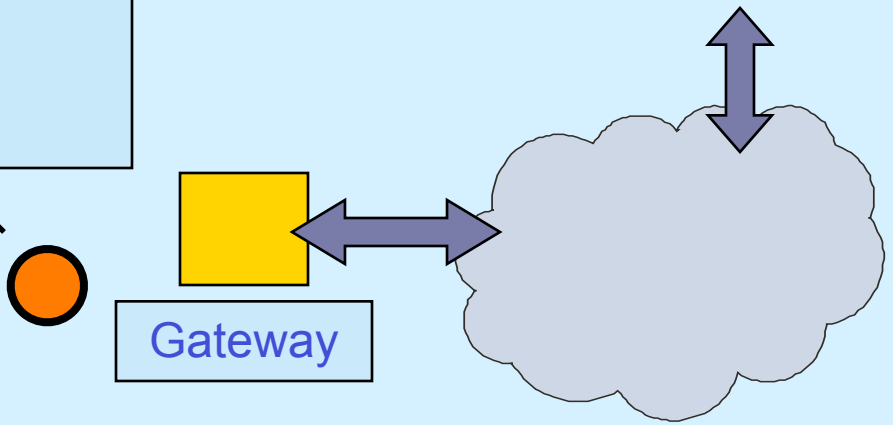
Sensor Network functioning



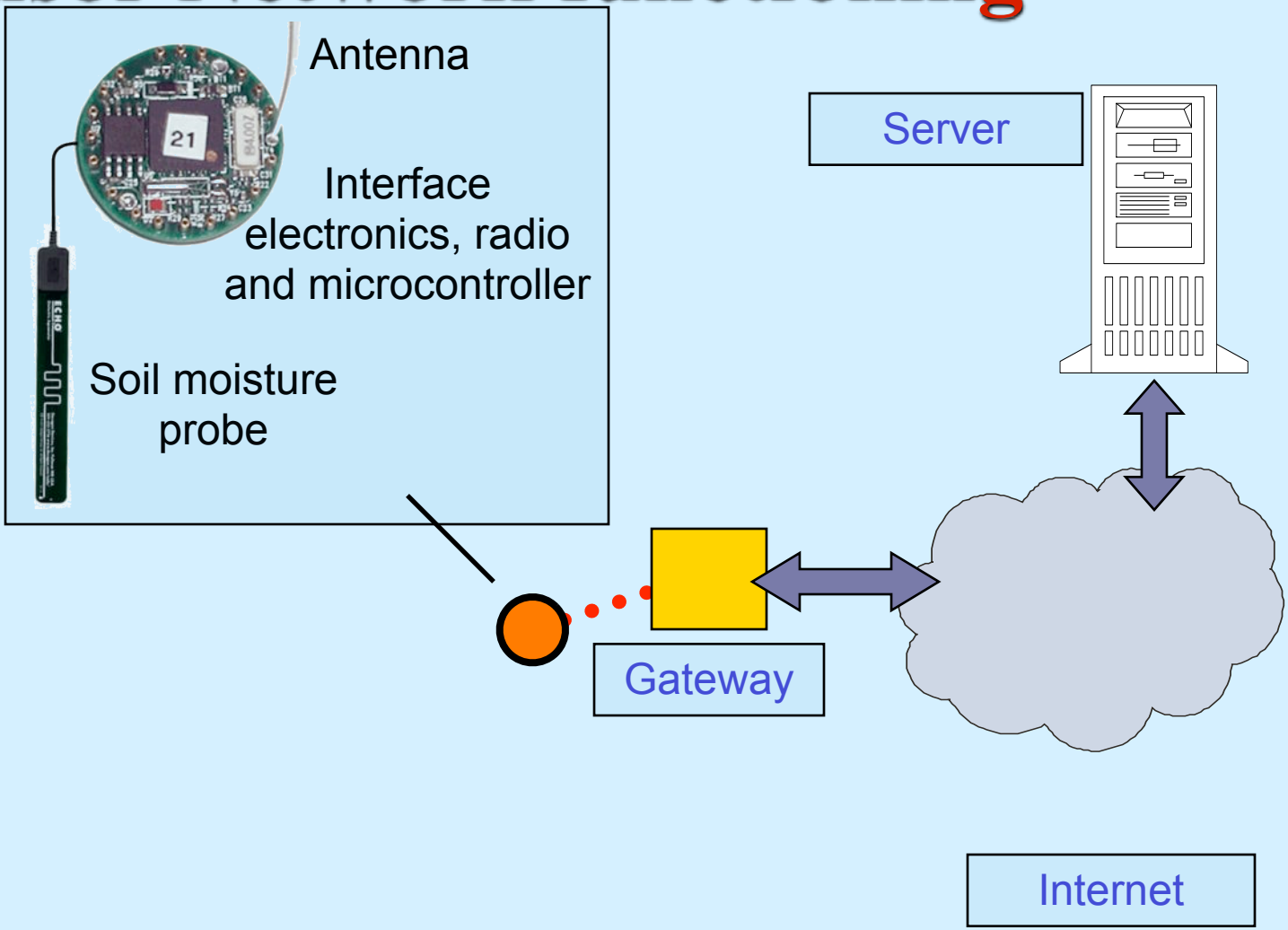
Sensor Network functioning



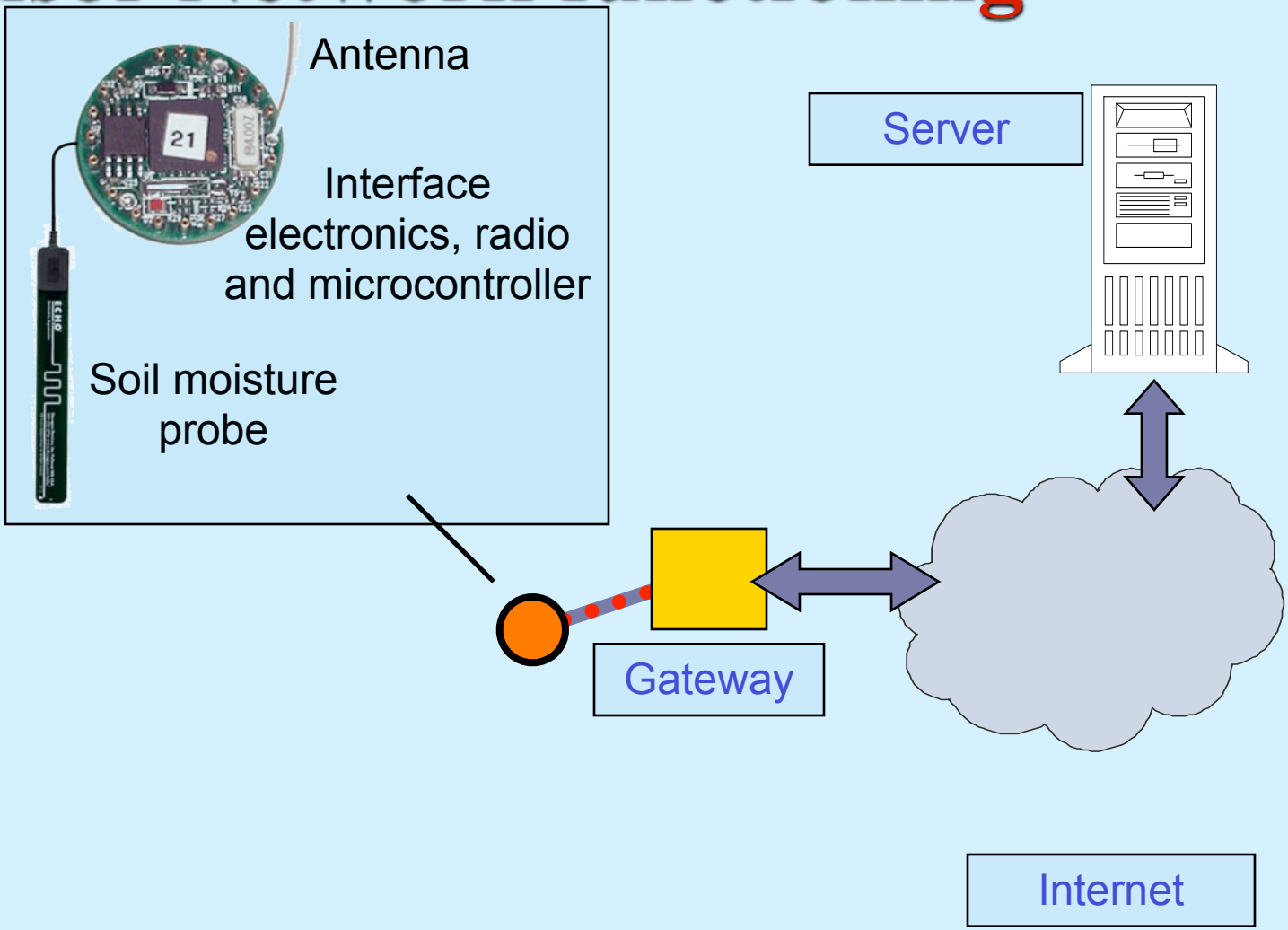




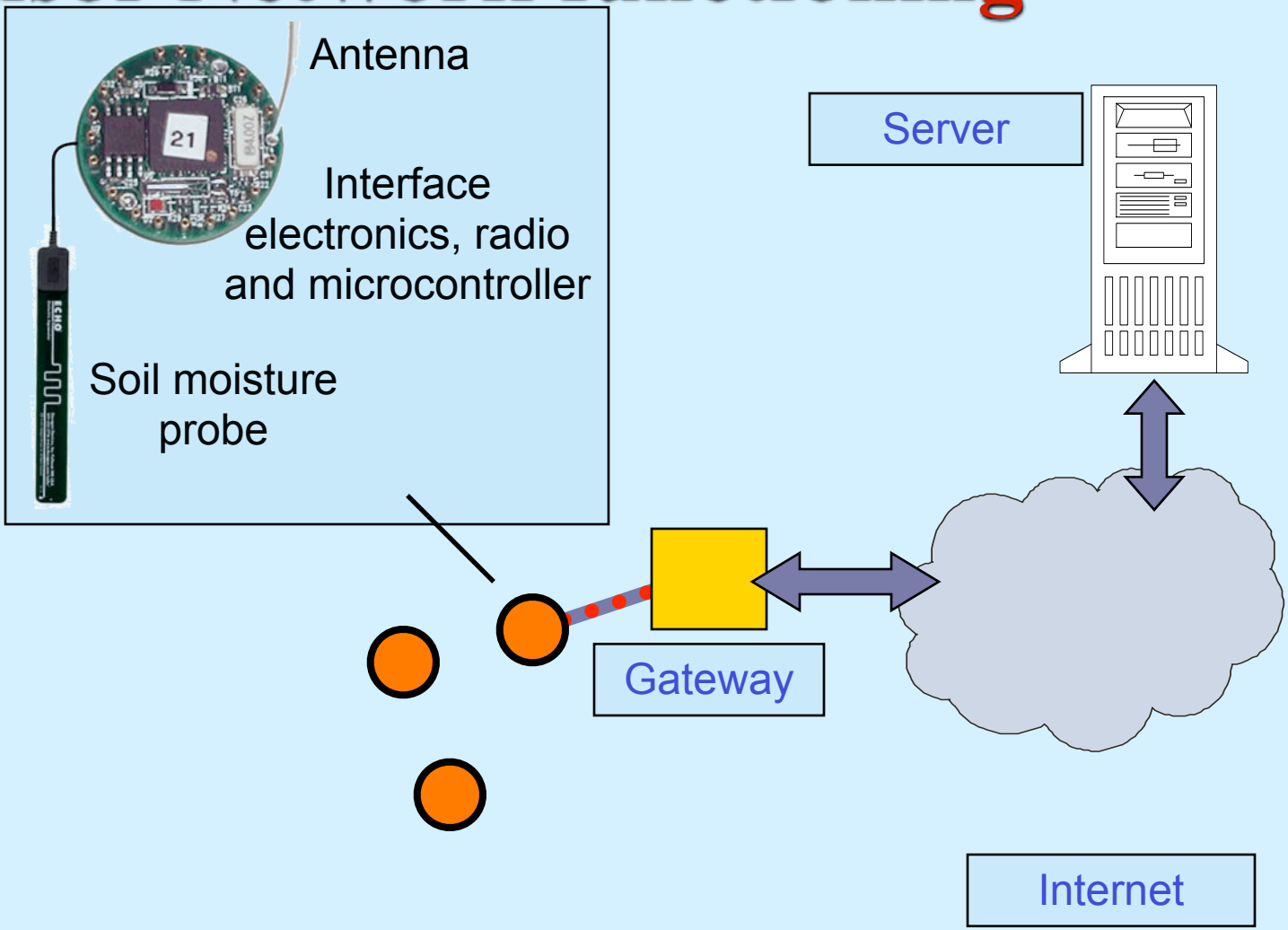
Sensor Network functioning



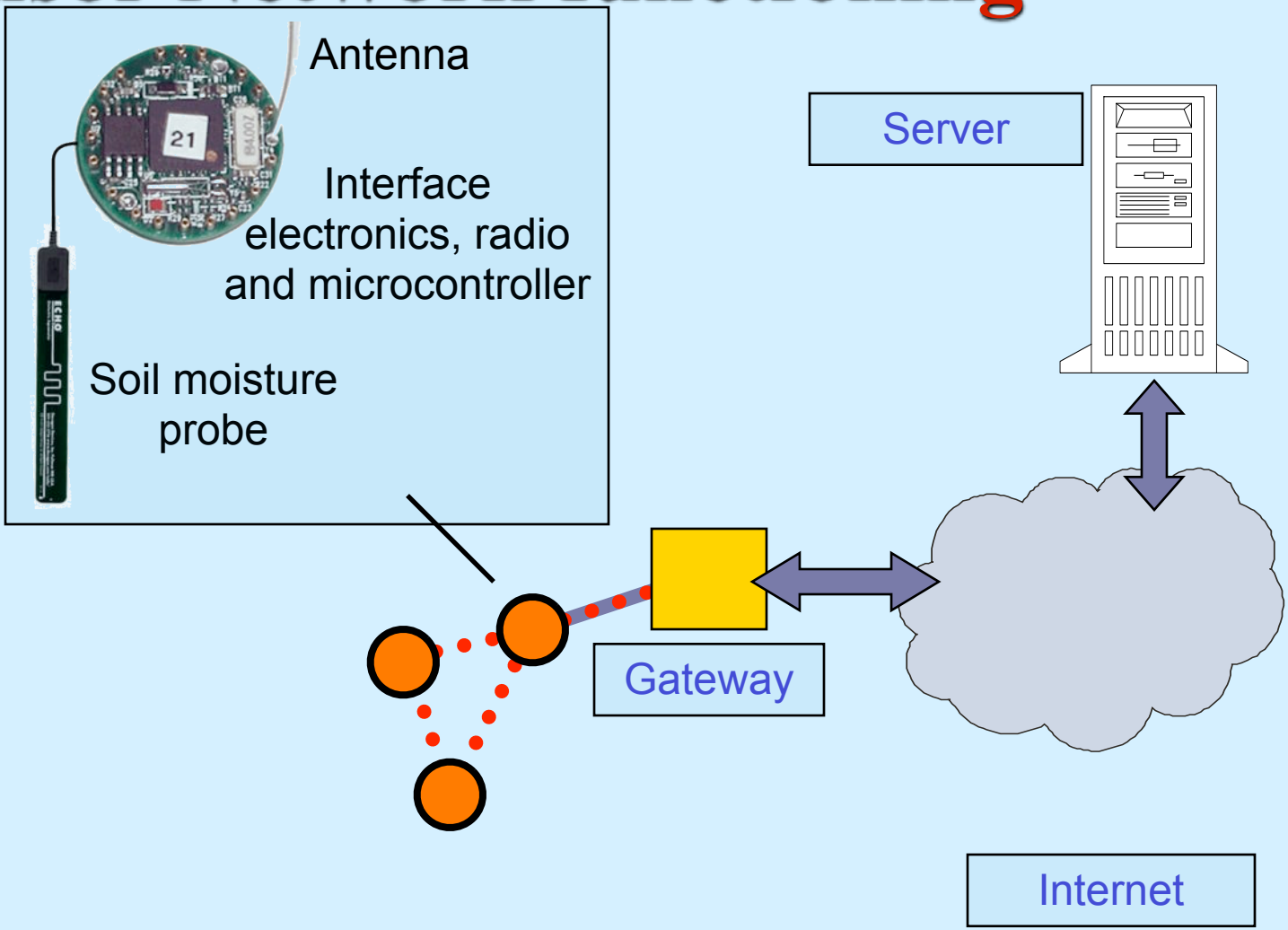
Sensor Network functioning



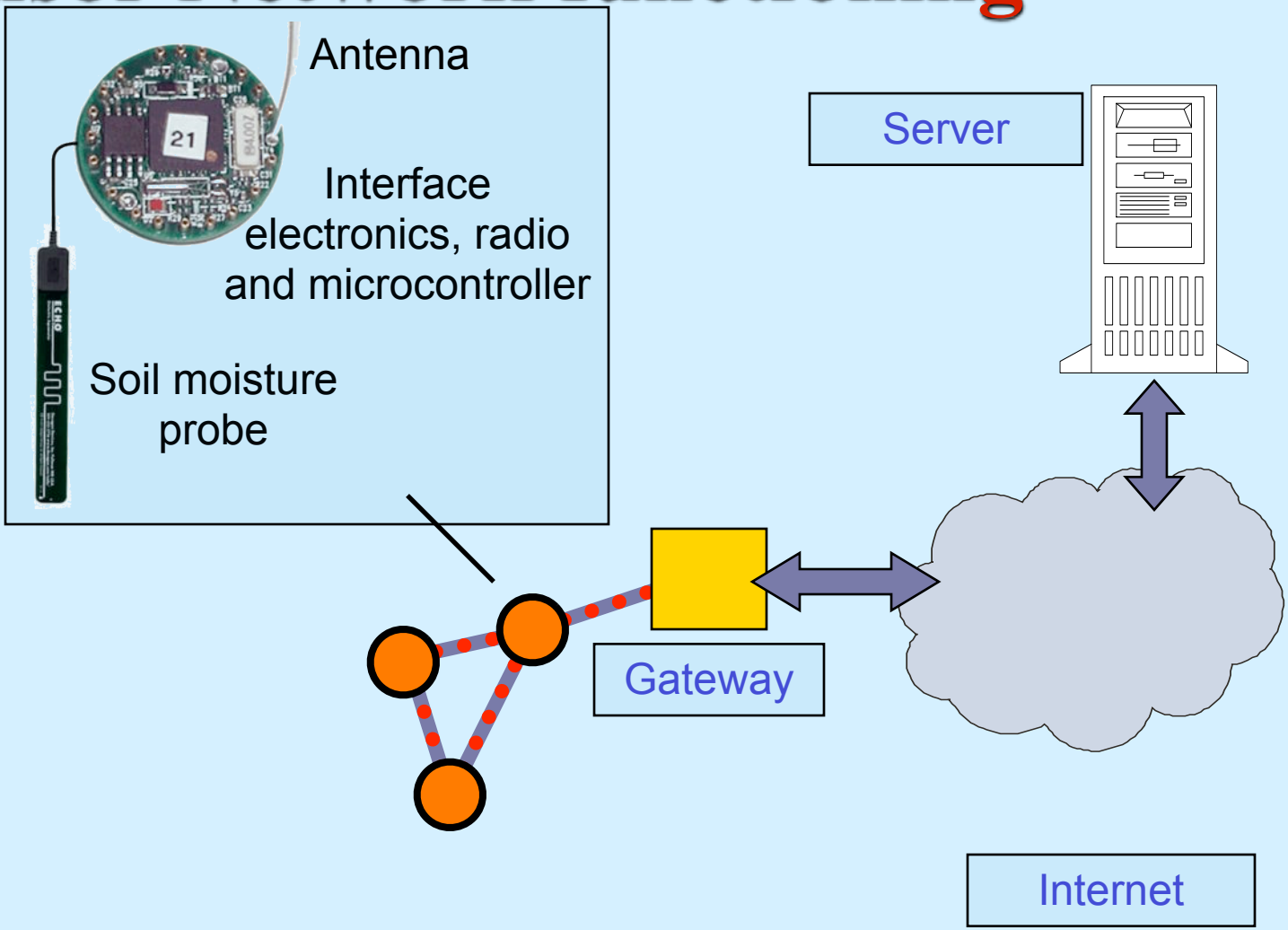
Sensor Network functioning



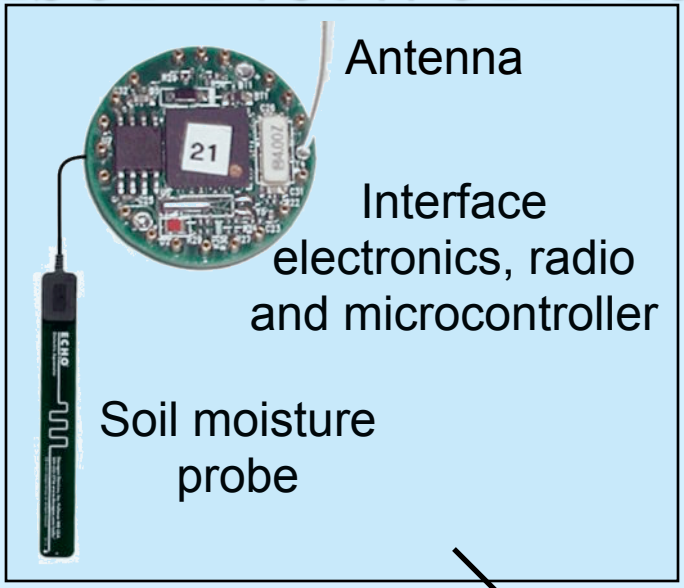
Sensor Network functioning



Sensor Network functioning



Sensor Network functioning

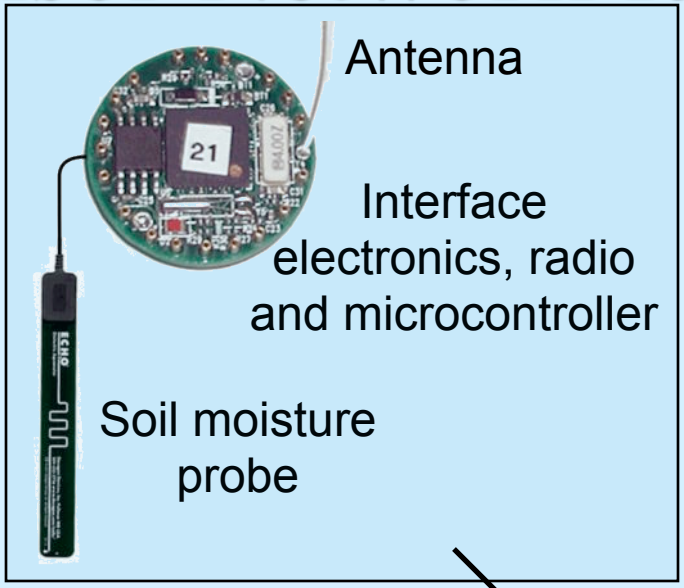


Server

Gateway

Internet

Sensor Network functioning

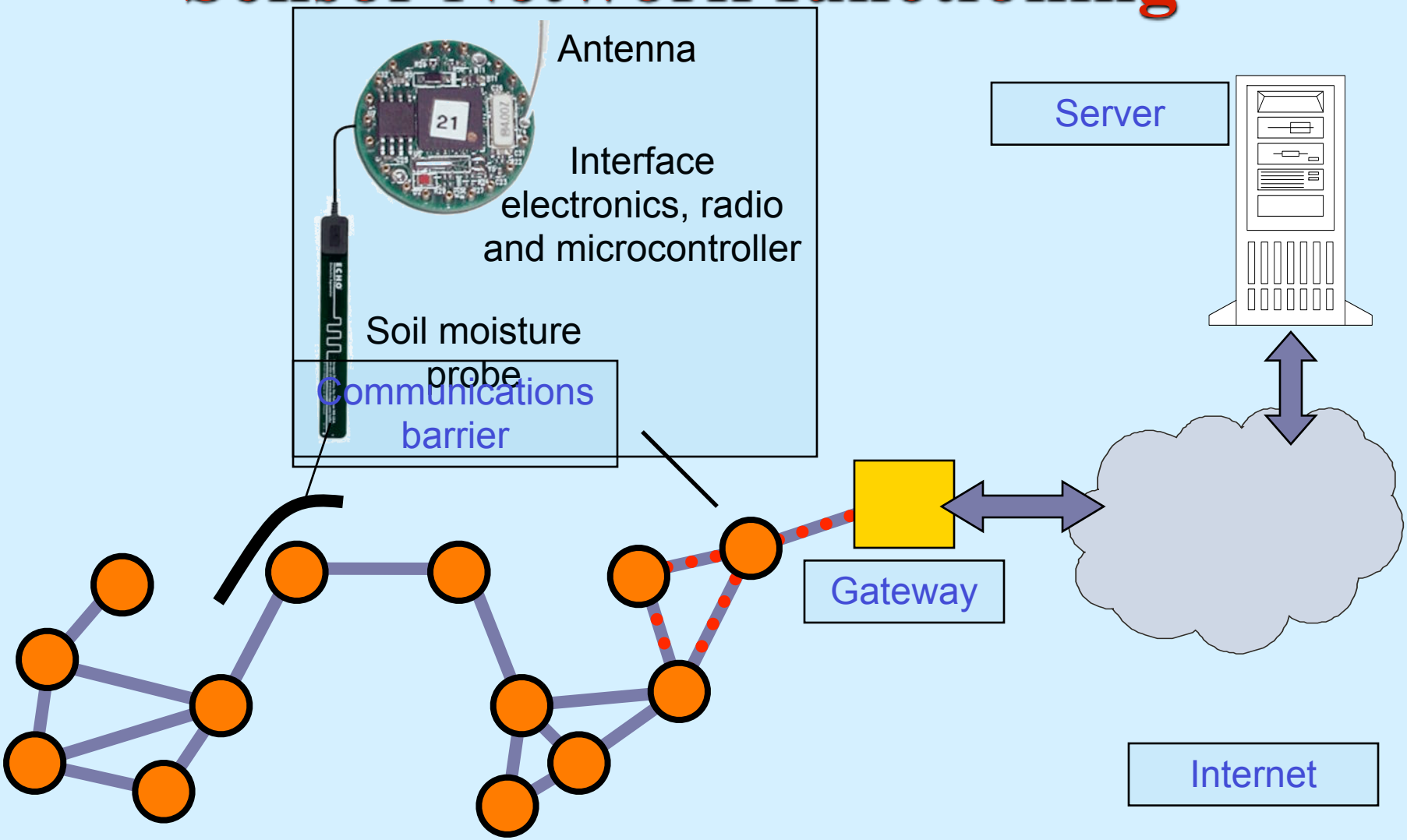


Server

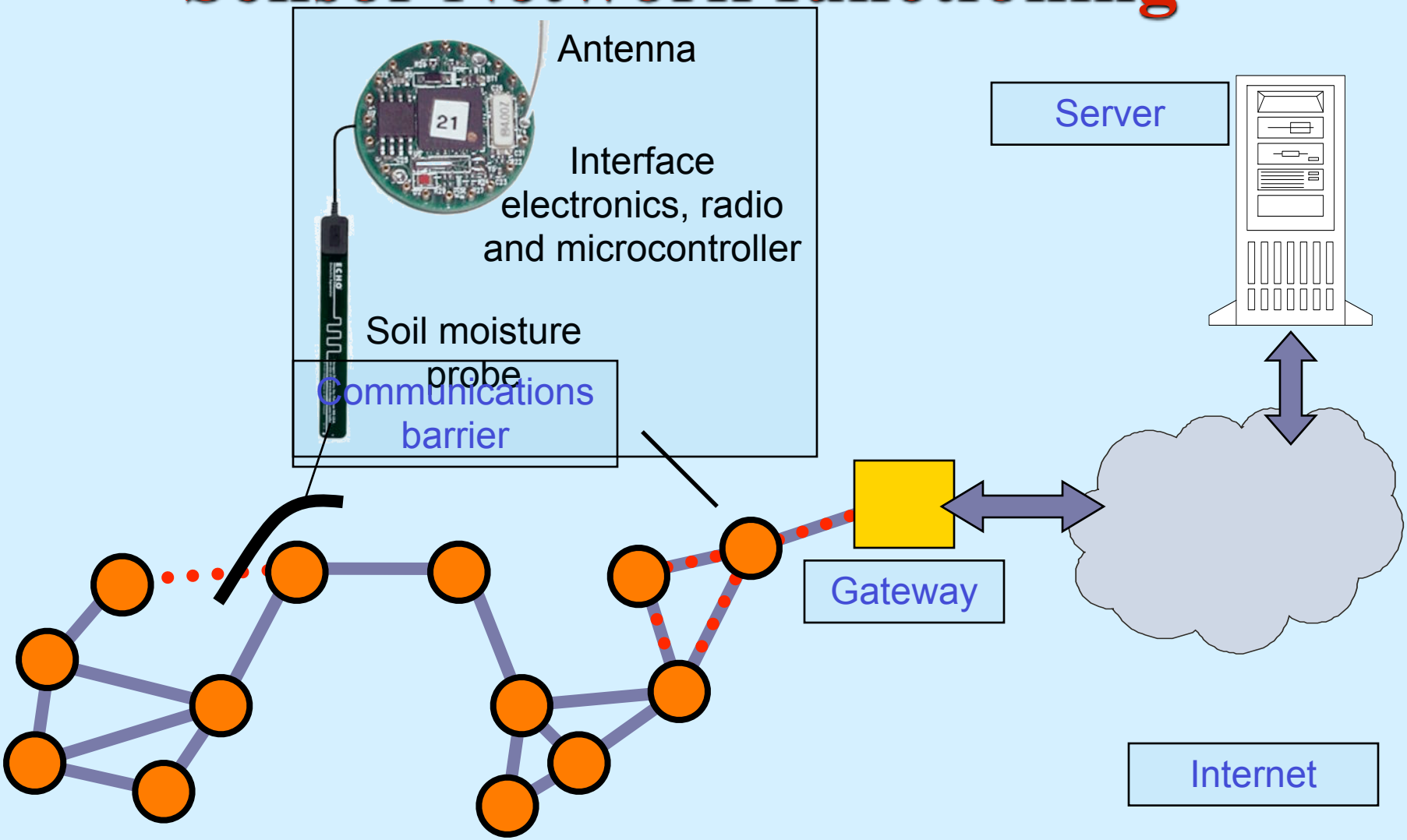
Gateway

Internet

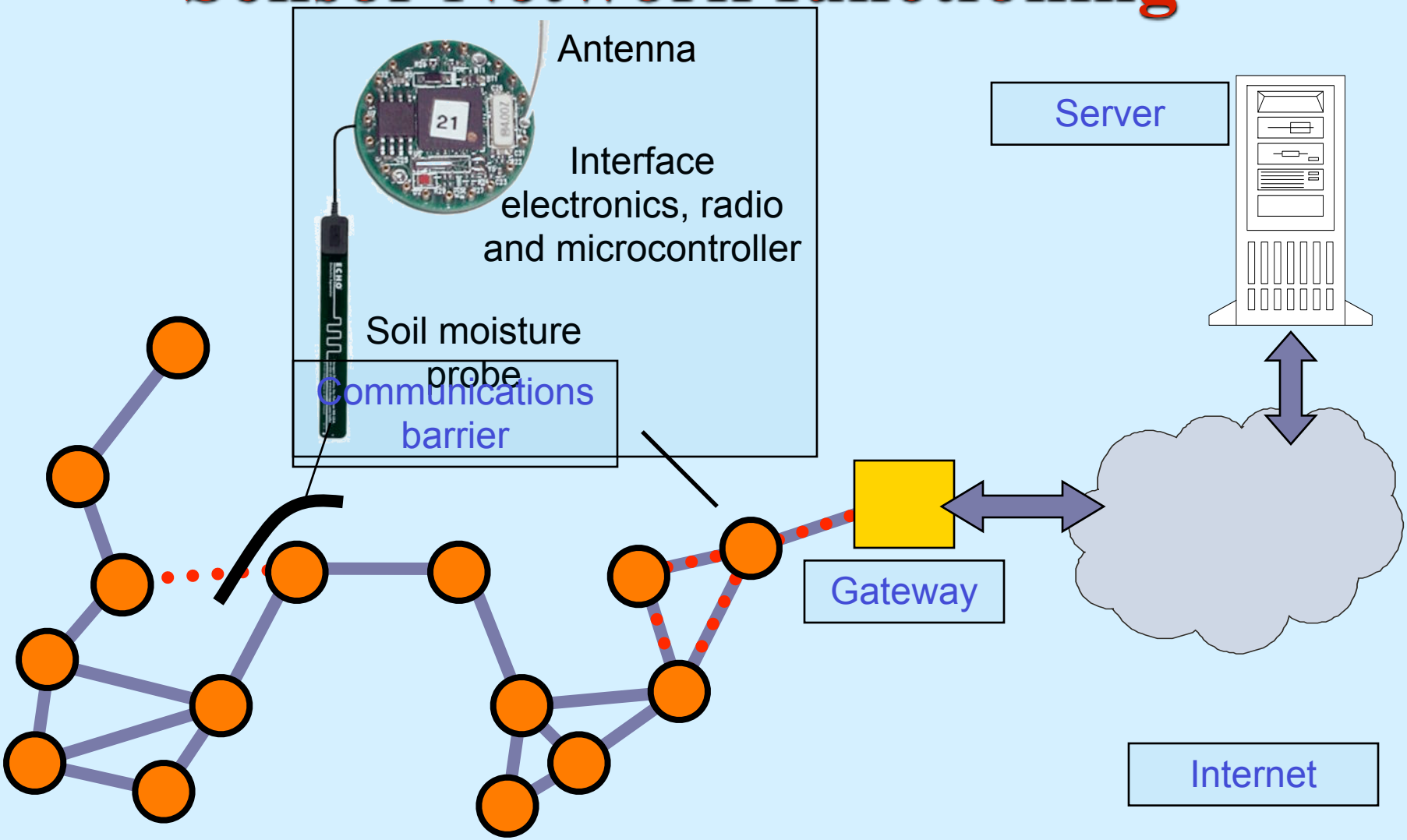
Sensor Network functioning



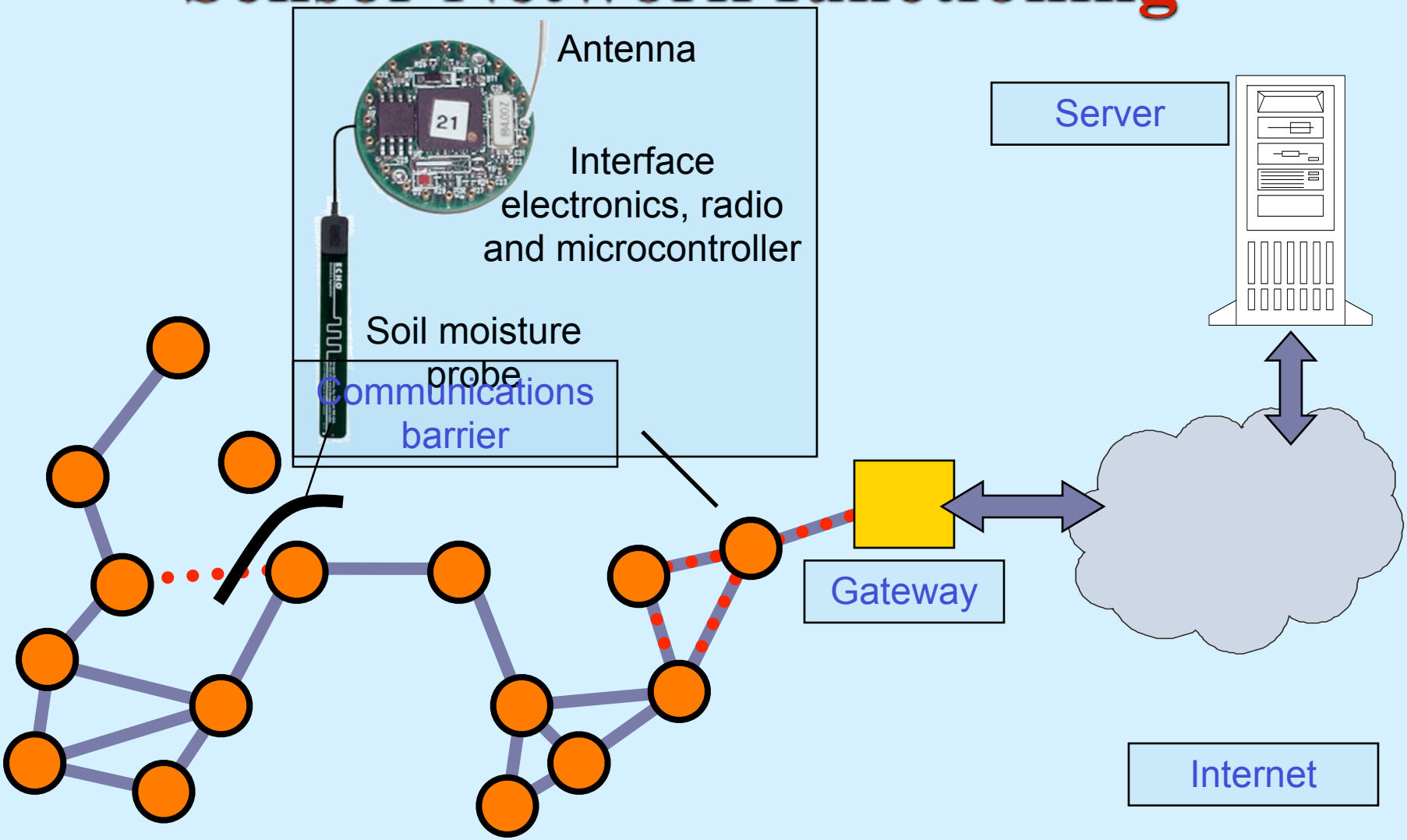
Sensor Network functioning



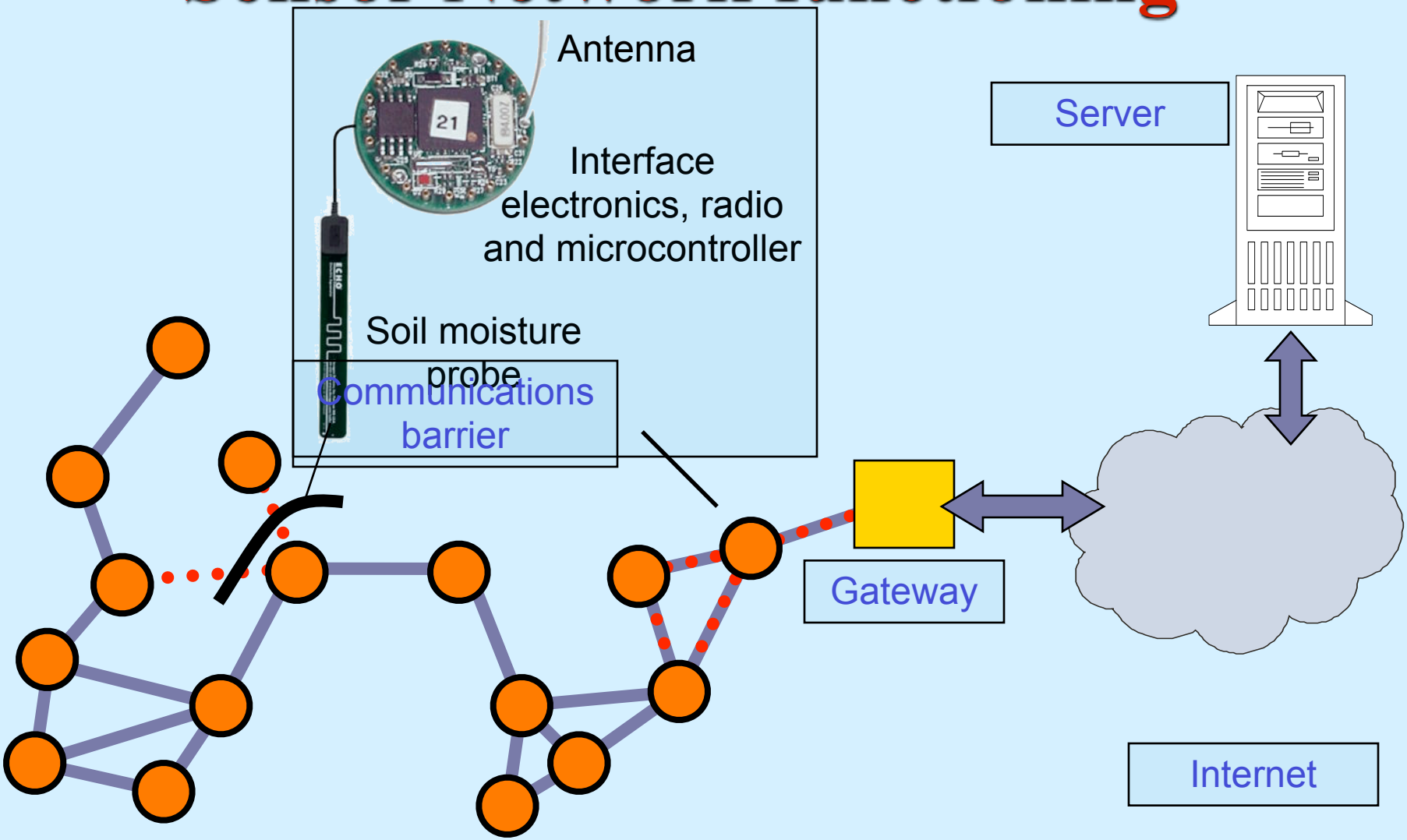
Sensor Network functioning



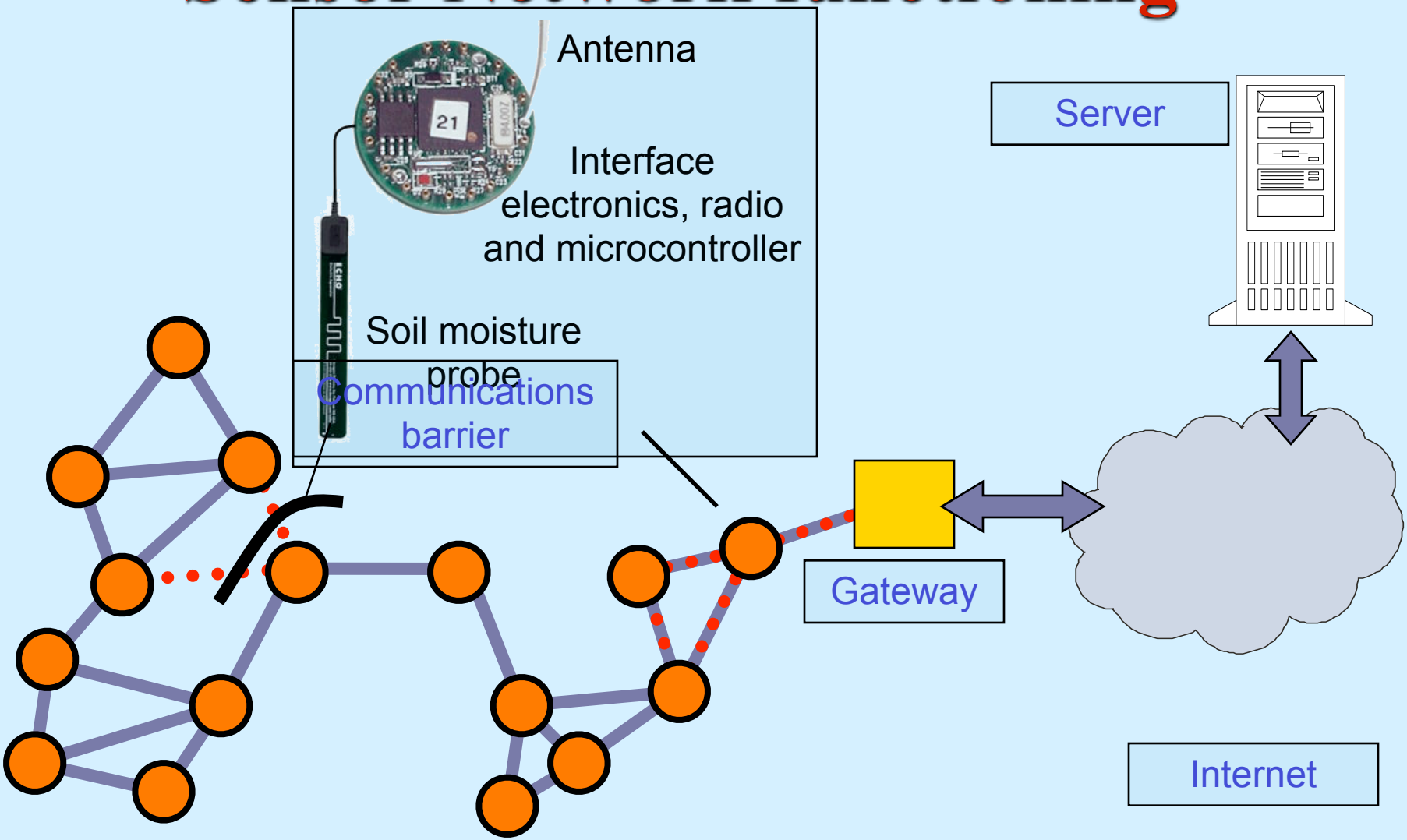
Sensor Network functioning



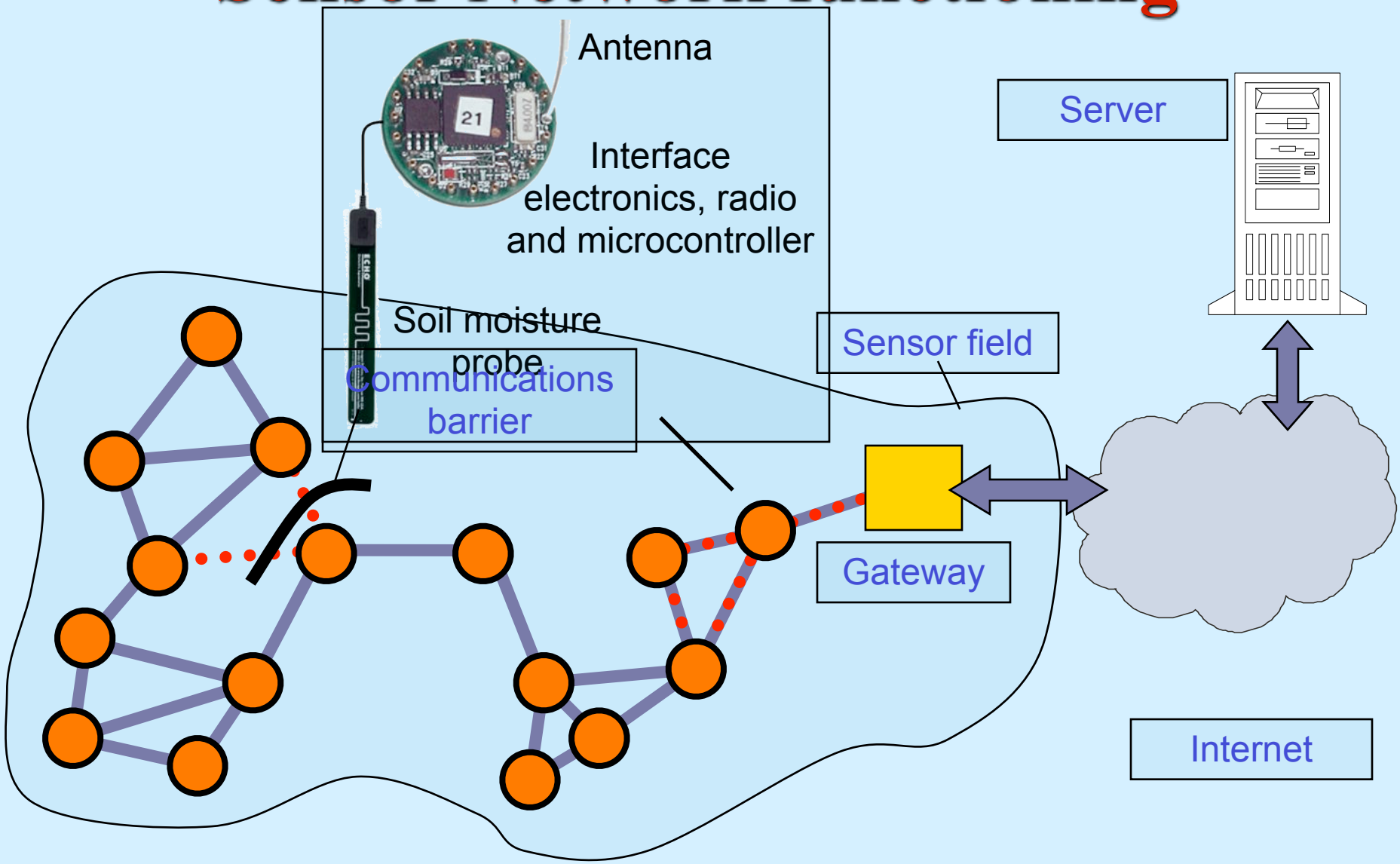
Sensor Network functioning



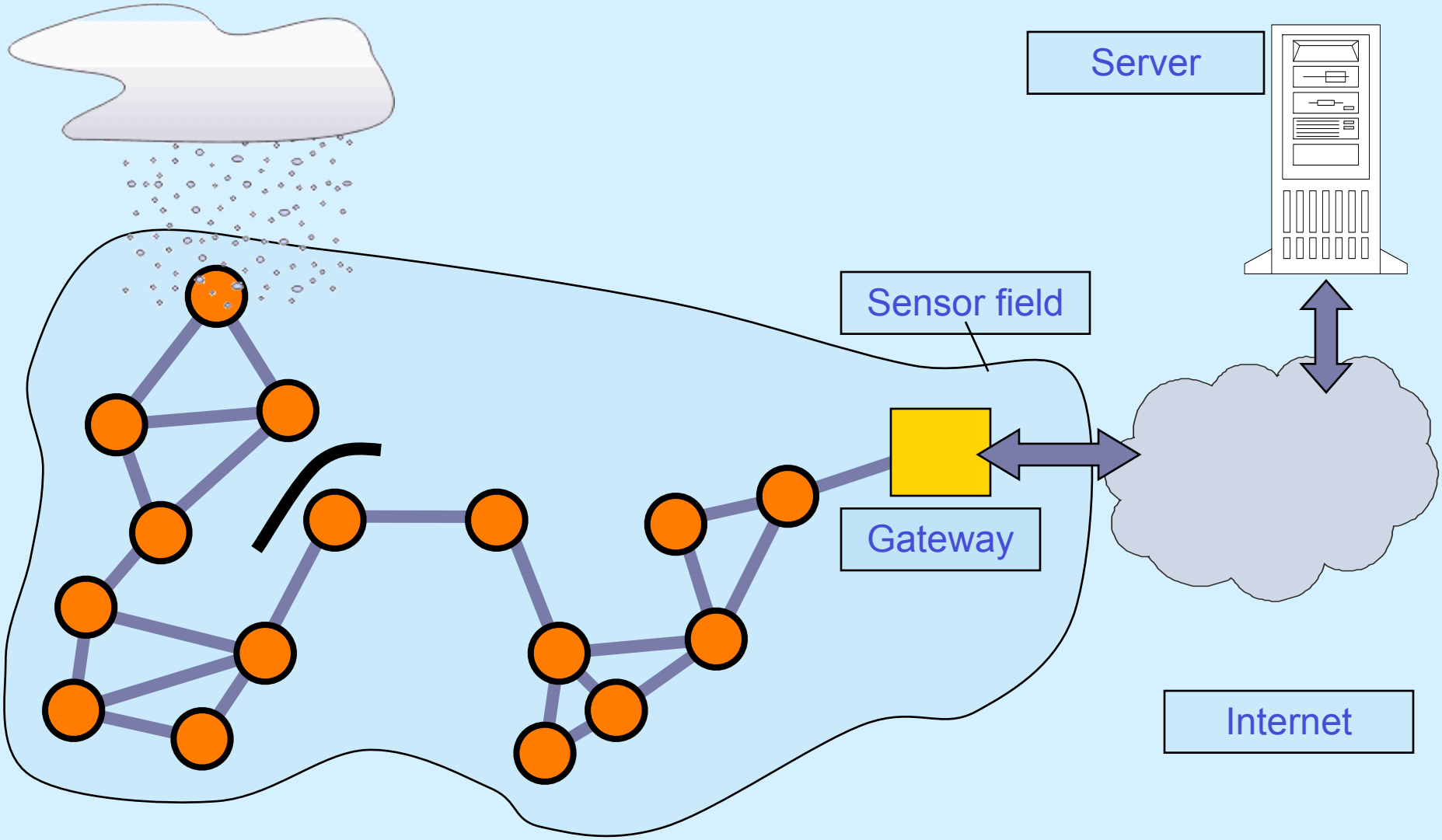
Sensor Network functioning



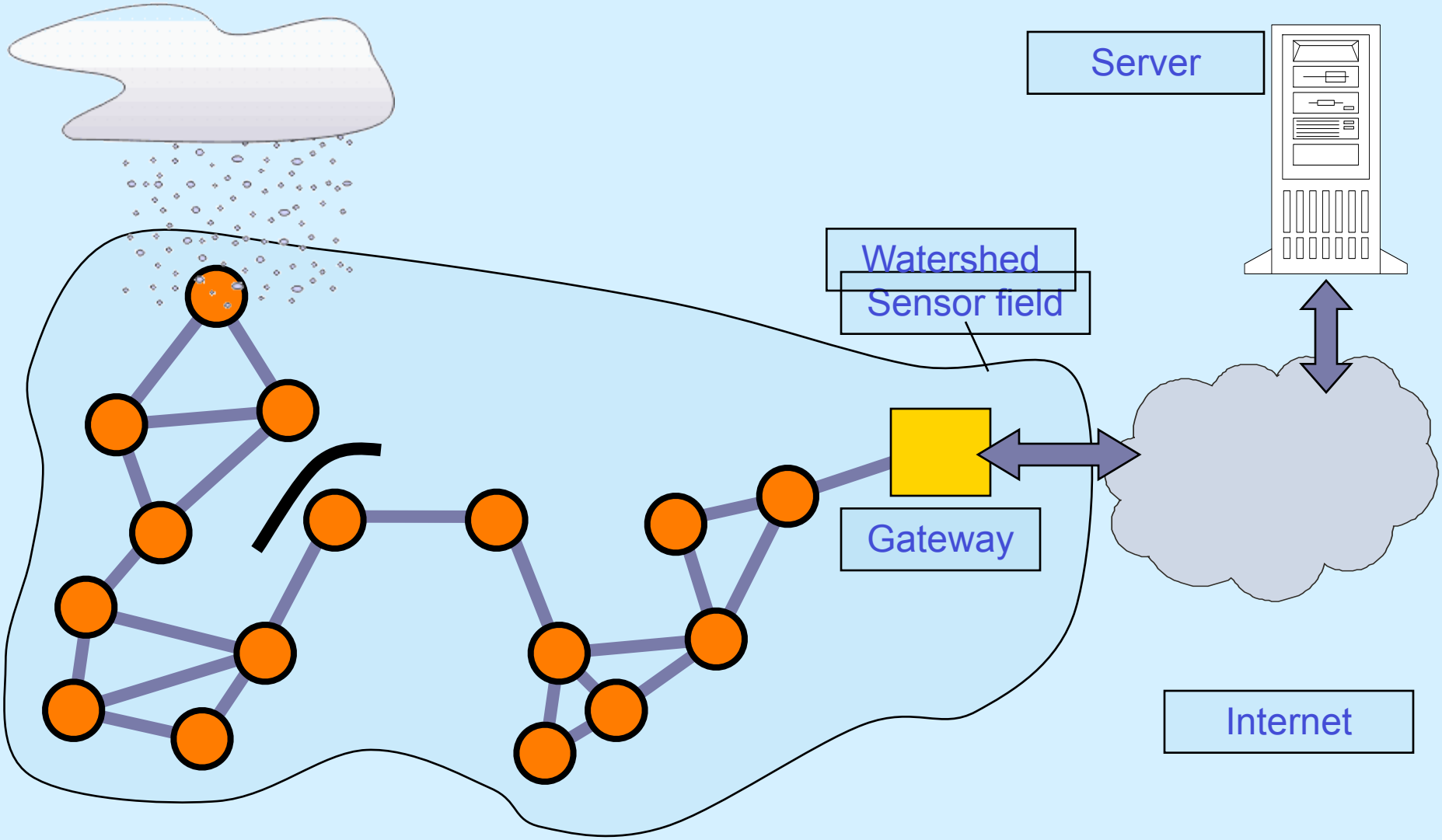
Sensor Network functioning



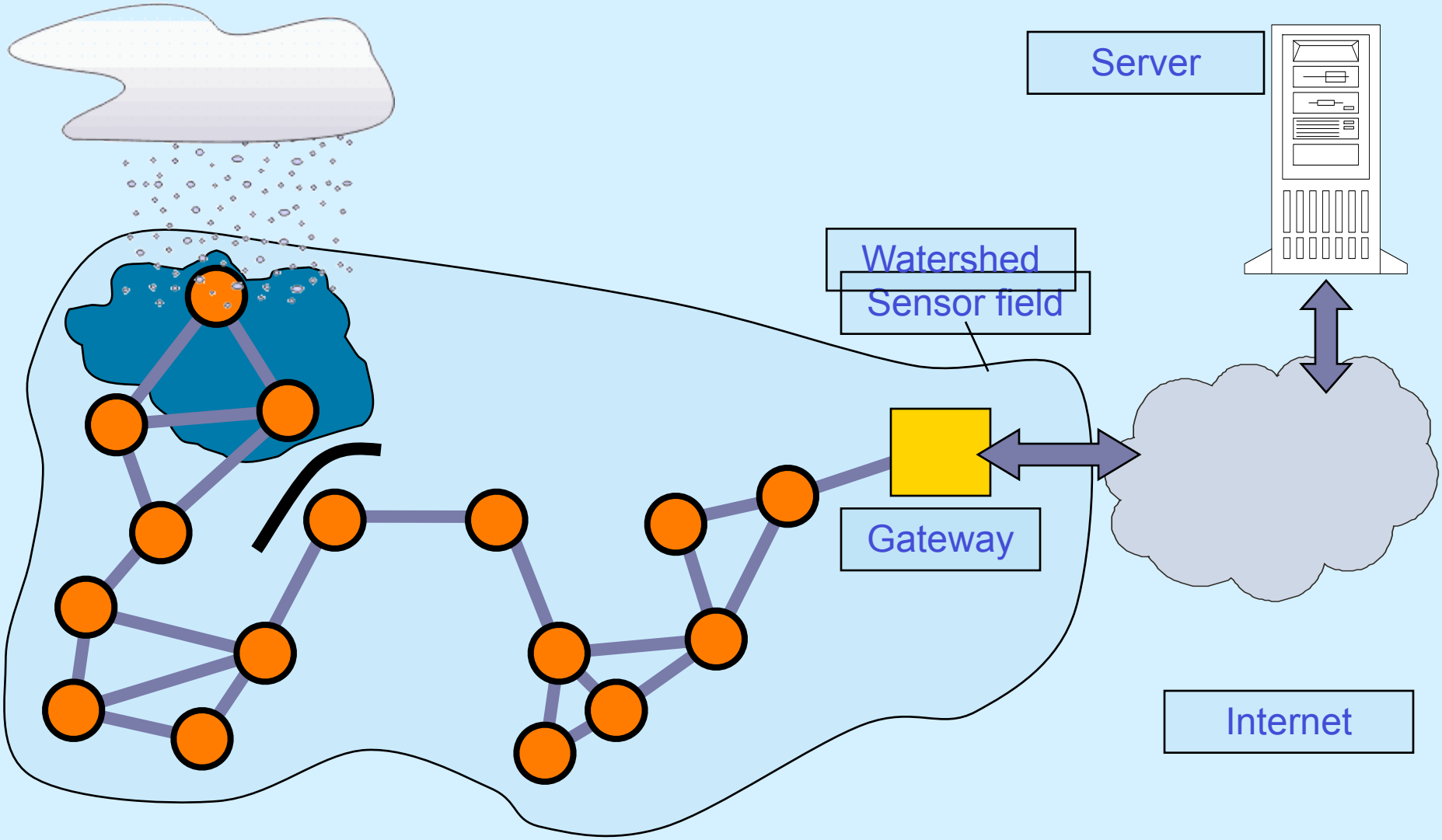
Sensor Network functioning



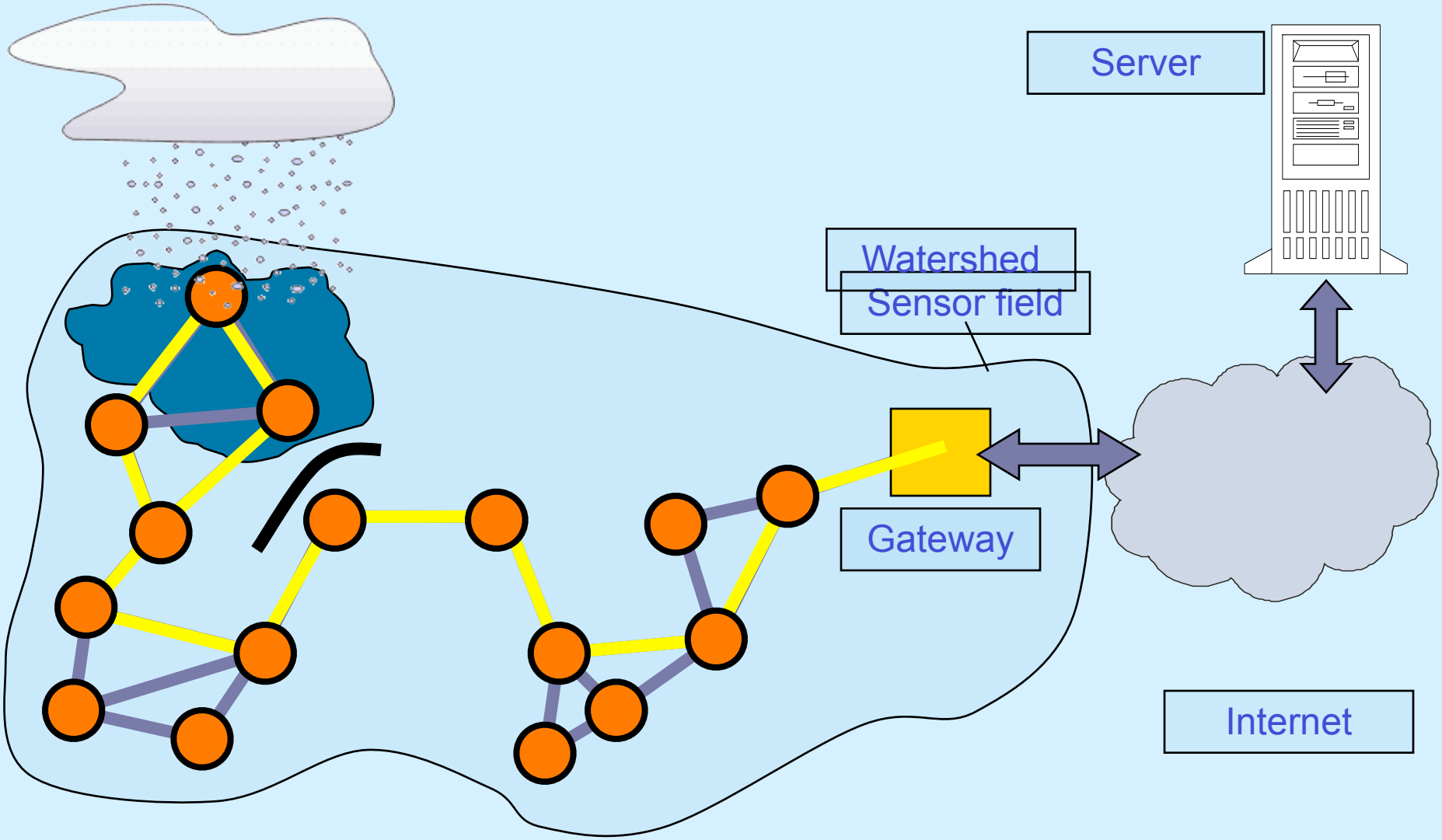
Sensor Network functioning



Sensor Network functioning



Sensor Network functioning



Applications of sensor networks

- temperature
- humidity
- vehicular movement
- lightning condition
- pressure
- soil makeup
- noise levels
- the presence or absence of certain kinds of objects
- mechanical stress levels on attached objects
- the current characteristics such as speed, direction, and size of an object

Applications of sensor networks

Health applications

- Telemonitoring of human physiological data
  - » **Monitoring of blood sugar, cholesterol etc., blockages of heart arteries.**
- Tracking and monitoring patients and doctors inside a hospital
- Drug administration in hospitals

Home applications

- Home automation
- Smart environment

Applications of sensor networks

Military applications

- Monitoring friendly forces, equipment and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces and terrain
- Battle damage assessment
- Nuclear, biological and chemical attack detection and reconnaissance

Applications of Sensor Networks

Environmental applications

- Forest fire detection
- Biocomplexity mapping of the environment
- Flood detection
- Precision agriculture

Applications of sensor networks

Other commercial applications

- Environmental control in office buildings
- Interactive museums
- Managing inventory control
- Vehicle tracking and detection
- Detecting and monitoring car thefts

Sensor Networks Vs. Ad hoc Networks:

- The number of nodes in a sensor network can be several orders of magnitude higher than the nodes in an **ad hoc network**.
- Sensor nodes are densely deployed. **Ad hoc nodes** may/may not be so densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently?
- Sensor nodes mainly use broadcast, most **ad hoc networks** are based on p2p.
- Sensor nodes are limited in power, computational capacities and memory.
- Sensor nodes may not have global ID, because of large amount of overhead and large number of sensors.

Attributes of Sensor Network

Attributes of Sensor Networks

Sensors	*Size*: small (e.g., micro-electro mechanical systems (MEMS)), large (e.g., radars, satellites) *Number*: small, large *Type*: passive (e.g., acoustic, seismic, video, IR, magnetic), active (e.g., radar, ladar) *Composition or mix*: homogeneous (same types of sensors), heterogeneous (different types of sensors) *Spatial coverage*: dense, sparse *Deployment*: fixed and planned (e.g., factory networks), ad hoc (e.g., air-dropped) *Dynamics*: stationary (e.g., seismic sensors), mobile (e.g., on robot vehicles)
Sensing entities of interest	*Extent*: distributed (e.g., environmental monitoring), localized (e.g., target tracking) *Mobility*: static, dynamic *Nature*: cooperative (e.g., air traffic control), non-cooperative (e.g., military targets)
Operating environment	Benign (factory floor), adverse (battlefield)
Communication	*Networking*: wired, wireless *Bandwidth*: high, low
Processing architecture	Centralized (all data sent to central site), distributed (located at sensor or other sites), hybrid
Energy availability	Constrained (e.g., in small sensors), unconstrained (e.g., in large sensors)

Three Generations of Sensor nodes

	Yesterday (1980's – 1990's)	Today (2000 – 2003)	Tomorrow (2010)
Manufacturer	Custom contractors, e.g., for TRSS	Commercial: Crossbow Technology, Inc. Sensoria Corp., Ember Corp.	Dust, Inc. and others to be formed
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particle
Weight	Kilograms	Grams	Negligible
Node architecture	Separate sensing, processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client server, peer to peer	Peer to peer
Power supply lifetime	Large batteries; hours, days and longer	AA batteries; days to weeks	Solar; months to years
Deployment	Vehicle-placed or air-drop single sensors	Hand-emplaced	Embedded, "sprinkled" left-behind

Current Research Projects

Project name	Research area	HTTP location
SensoNet [20]	Transport, network, data link, and physical layers. Power control, mobility, and task management planes.	http://www.ece.gatech.edu/research/labs/bwn/
WINS [6]	Distributed network and Internet access to sensors, controls, and processors.	http://www.janet.ucla.edu/WINS/
SPINS [7]	Data dissemination protocols.	http://nms.lcs.mit.edu/projects/leach
SPINS [15]	Security protocol.	http://paris.cs.berkeley.edu/~perrig/projects.html
SINA [20]	Information networking architecture.	http://www.eecis.udel.edu/~cshen/
mAMPS [8]	Framework for implementing adaptive energy-aware distributed microsensors.	http://www-mtl.mit.edu/research/icsystems/uamps/
LEACH [16]	Cluster formation protocol.	http://nms.lcs.mit.edu/projects/leach
Smart Dust [7]	Laser communication from a cubic millimeter. Mote delivery. Submicrowatt electronics. Power sources. Macro Motes (COTS Dust).	http://robotics.eecs.berkeley.edu/~pister/SmartDust/
SCADDS [3, 5]	Scalable coordination architectures for deeply distributed and dynamic systems.	http://www.isi.edu/scadds/
PicoRadio [4]	Develop a "system-on-chip" implementation of a PicoNode.	http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/PicoNode.htm
PACMAN	Mathematical framework that incorporates key features of computing nodes and networking elements.	http://pacman.usc.edu
Dynamic Sensor Networks	Routing and power aware sensor management. Network services API.	http://www.east.isi.edu/DIV10/dsn/
Aware Home	Requisite technologies to create a home environment that can both perceive and assist its occupants.	http://www.cc.gatech.edu/fce/ahri
COUGAR Device Database Project	Distributed query processing.	http://www.cs.cornell.edu/database/cougar/index.htm
DataSpace	Distributed query processing.	http://www.cs.rutgers.edu/dataman/

Sensor networks Communication Architecture

The sensor nodes are usually scattered in a ***sensor field*** as shown in Fig 1. Each of theses scattered sensor nodes has the capabilities to collect data and route back to the ***sink***. Data are routed back to the sink by a multihop infrastructureless architecture through the sink as shown in Fig 1.The sink may communicate with the ***task manager node*** via Internet or satellite. The design of the sensor network as described by Fig 1 is influenced by many factors. Including ***Fault tolerance***, ***Scalability***, ***Production costs***, ***Operating environments***, ***Sensor network topology***, ***Hardware constraints***, ***Transmission media***, and ***Power consumption***.

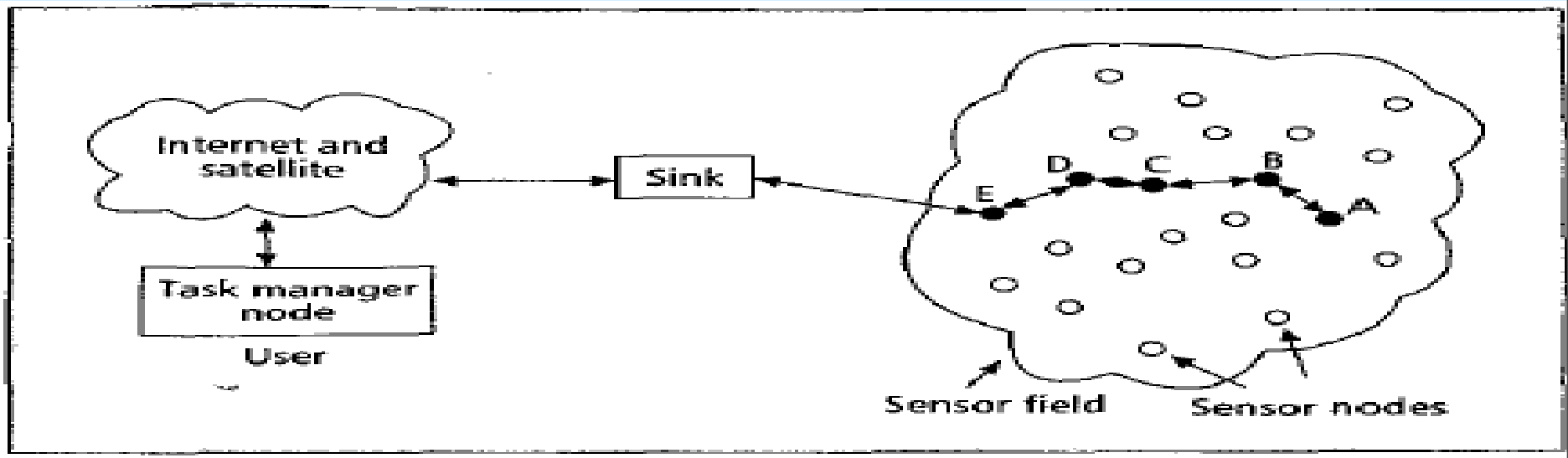


Figure 1. *Sensor nodes scattered in a sensor field.*

Factors influencing sensor network design

Fault tolerance

- Fault tolerance is the ability to sustain sensor network functionalities without any interruption due to sensor node failures.
- The fault tolerance level depends on the application of the sensor networks.

Factors influencing sensor network design

Scalability

- Scalability measures the density of the sensor nodes.
- Density = $\mu(R) = (N * \pi R^2)/A$

where N is number of scattered sensor nodes in region A. R is radio transmission range. Number of nodes within the transmission radius of each node in A is μ

Factors influencing sensor network design

Production costs

- The cost of a single node is very important to justify the overall cost of the networks.
- The cost of a sensor node is a very challenging issue given the amount of functionalities with a price of much less than a dollar.

Factors influencing sensor network design

Hardware constraints: A sensor node is made up of four basic components : A sensing unit, a Processing unit, a transceiver unit, and power unit.

Additionally application dependent components such as Location finding system, Mobilizer and Power generator

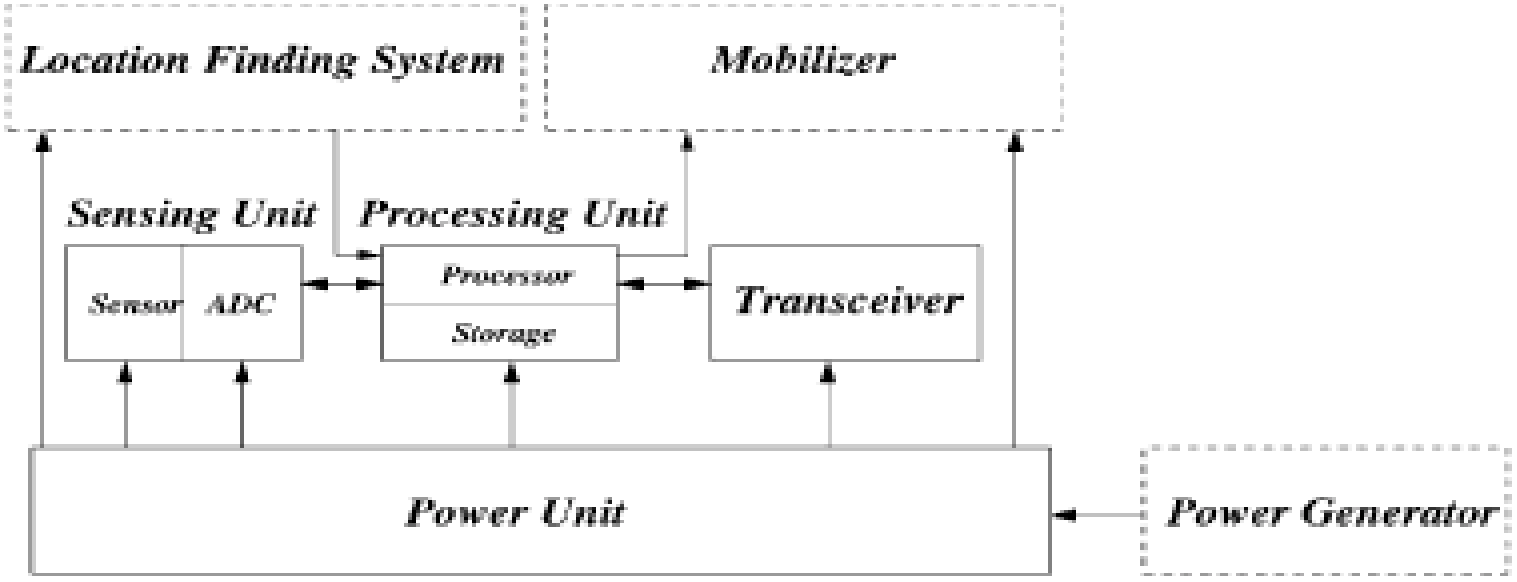


Fig. 1. The components of a sensor node.

Factors influencing sensor network design

Sensor network topology

- Pre-deployment and deployment phase
- Post-deployment phase
- Re-deployment of additional nodes phase

Factors influencing sensor network design

Environment

- Busy intersections
- Interior of a large machinery
- Bottom of an ocean
- Inside a twister
- Surface of an ocean during a tornado
- Biologically or chemically contaminated field
- Battlefield beyond the enemy lines
- Home or a large building
- Large warehouse
- Animals
- Fast moving vehicles
- Drain or river moving with current.

Factors influencing sensor network design

Transmission media

In a multihop sensor network, communicating nodes are linked by a wireless medium. To enable global operation, the chosen transmission medium must be available worldwide.

- Radio
- infrared
- optical media

Factors influencing sensor network design

Power consumption : In multihop ad hoc sensor network, each node plays the dual role of data originator and data router. Power consumption can thus be divided into three domains.

1. Sensing
2. Communication
3. Data processing

Design of power aware protocols and algorithms for sensor networks is needful & being researched.

- ***The more you sleep, the more you gain.***
- ***The less you spend, the longer life you live.***

QoS Issues

- Multimedia and the Internet
  - QoS widely studied
  - Can have different meanings
    - Resolution and frame rate in video streams
    - Latency, bandwidth in wired links
- Sensor networks
  - Ability to detect events
  - Latency of detection (and reporting)
  - Accuracy
    - Will depend strongly on errors and noise

Sensor networks: Protocol stack

The Protocol stack used by the sink and sensor nodes is shown. This protocol Stack combines power and routing awareness, integrates data with networking Protocols and promotes cooperative efforts of sensor nodes.

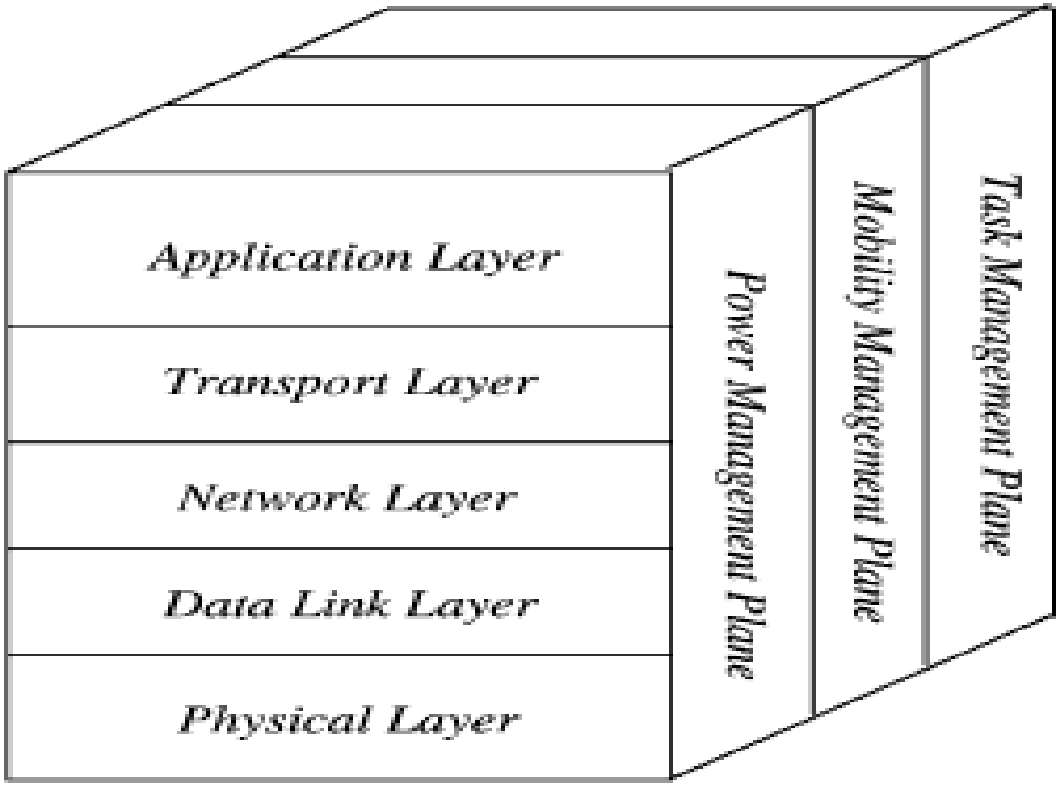


Fig. 3. The sensor networks protocol stack.

PROTOCOL STACK

The Power Management plane manages how a sensor node Uses its power. WHEN THE POWER LEVEL OF THE SENSOR NODE IS LOW, THE SENSOR NODE BROADCASTS TO ITS NEIGHBORS THAT IT IS LOW IN POWER AND CAN NOT PARTICIPATE IN ROUTING.

The task management plane balances and schedules the sensing tasks given to a specific region. Not all sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than others depending on their power level. These management planes are needed so that sensor nodes can work together in a power-efficient way, route data in a mobile sensor network, and share resources between sensor nodes.

Communication architecture of sensor

Physical layer

The physical layer is responsible for frequency selection, frequency generation, signal detection, modulation and data encryption. Thus far, the 915 Mhz industrial, Scientific, and Medical (ISM) band has been widely suggested for sensor network. Long distance wireless communication can be expensive, in terms of both energy and implementation complexity. While designing the physical layer for sensor network, energy minimization assumes significant importance, over and above the propagation and fading effects. In general, the minimum output power required to transmit a signal over a distance d is proportional to dn, where $2 <= n < 4$. The exponent n is closer to four for low-lying antennae and near-ground channels (6), as is typical in sensor network communication.

Communication architecture of sensor networks

Open research issues

- Modulation schemes
- Strategies to overcome signal propagation effects
- Hardware design

Communication architecture of sensor networks

Data link layer

The data link layer is responsible for the medium access and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

Communication architecture of sensor networks

Medium access control

- Creation of the network infrastructure
- Fairly and efficiently share communication resources between sensor nodes

Medium Access Control Protocol in Sensor network

The MAC protocol in a wireless multihop self-organizing sensor network must achieve two goals. The first is the creation of the network infrastructure. Since thousands of sensor nodes are densely scattered in a sensor field, the MAC scheme must establish communication links for data transfer. This forms the basic infrastructure needed for wireless communication hop by hop and gives the sensor network self-organizing ability. The second objective is to fairly and efficiently share communication resources between sensor nodes.

MAC Protocol

- Existing MAC Protocols can not be used because of the sensor network characteristics.

In a *cellular system*, the base stations form a wired backbone. A mobile node is only a single hop away from the nearest base station. This type of network is also referred to as *infrastructure-based* in literature. The primary goal of the MAC protocol in such systems is the provision of high quality of service (QoS) and bandwidth efficiency. Power conservation assumes only secondary importance since base stations have unlimited power supply and the mobile user can replenish exhausted batteries in the handset. Hence, medium access is invariably inclined toward a dedicated resource assignment strategy. Such an access scheme is impractical for sensor networks since there is no central controlling agent like the base station. This makes networkwide synchronization a difficult task. Moreover, power efficiency directly influences network lifetime in a sensor network and hence is of prime importance.

MAC in Sensor Vs. Ad hoc

Bluetooth and the *mobile ad hoc network* (MANET) are probably the closest peers to sensor networks. Bluetooth is an infrastructureless short-range wireless system intended to replace the cable between electronic user terminals with RF links. The Bluetooth topology is a star network where a master node can have up to seven slave nodes wirelessly connected to it to form a piconet. Each piconet uses a centrally assigned time-division multiple access (TDMA) schedule and frequency hopping pattern. Transmission power is typically around 20 dBm and the transmission range is on the order of tens of meters.

MAC Protocol in a MANET has the task of forming the network infrastructure and maintaining it in the face of mobility. Hence the primary goal is provisioning of high QoS under mobile conditions.

MAC in Sensor

In contrast to these two systems, the sensor network may have a much larger number of nodes. The transmission power (~0 dBm) and radio range of a sensor node is much less than those of Bluetooth or MANET. Topology changes are more frequent in a sensor network and can be attributed to both node mobility and failure. The mobility rate can also be expected to be much lower than in the MANET. In essence, the primary importance of power conservation to prolong network lifetime in a sensor network means that none of the existing Bluetooth or MANET MAC protocols can be directly used.

Communication architecture of sensor networks

Power saving modes of operation

Operation in a power saving mode is energy efficient only if the time spent in that mode is greater than a certain threshold.

Communication architecture of sensor networks

Error control

- Forward Error Correction (FEC)
- Automatic Repeat Request (ARQ).

Simple error control codes with low-complexity encoding and decoding might present the best solutions for sensor networks.

Communication architecture of sensor networks

Open research issues

- MAC for mobile sensor networks
- Determination of lower bounds on the energy required for sensor network self-organization
- Error control coding schemes.
- Power saving modes of operation

Communication architecture of sensor networks

Open research issues

New schemes that split the end-to-end communication probably at the sinks may be needed.

Communication architecture of sensor networks

Open research issues

- New protocols need to be developed to address higher topology changes and higher scalability.
- New internetworking schemes should be developed to allow easy communication between the sensor networks and external networks.

Current Research Projects

Project name	Research area	HTTP location
SensoNet [20]	Transport, network, data link, and physical layers. Power control, mobility, and task management planes.	http://www.ece.gatech.edu/research/labs/bwn/
WINS [6]	Distributed network and Internet access to sensors, controls, and processors.	http://www.janet.ucla.edu/WINS/
SPINS [7]	Data dissemination protocols.	http://nms.lcs.mit.edu/projects/leach
SPINS [15]	Security protocol.	http://paris.cs.berkeley.edu/~perrig/projects.html
SINA [20]	Information networking architecture.	http://www.eecis.udel.edu/~cshen/
mAMPS [8]	Framework for implementing adaptive energy-aware distributed microsensors.	http://www-mtl.mit.edu/research/icsystems/uamps/
LEACH [16]	Cluster formation protocol.	http://nms.lcs.mit.edu/projects/leach
Smart Dust [7]	Laser communication from a cubic millimeter. Mote delivery. Submicrowatt electronics. Power sources. Macro Motes (COTS Dust).	http://robotics.eecs.berkeley.edu/~pister/SmartDust/
SCADDS [3, 5]	Scalable coordination architectures for deeply distributed and dynamic systems.	http://www.isi.edu/scadds/
PicoRadio [4]	Develop a "system-on-chip" implementation of a PicoNode.	http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/PicoNode.htm
PACMAN	Mathematical framework that incorporates key features of computing nodes and networking elements.	http://pacman.usc.edu
Dynamic Sensor Networks	Routing and power aware sensor management. Network services API.	http://www.east.isi.edu/DIV10/dsn/
Aware Home	Requisite technologies to create a home environment that can both perceive and assist its occupants.	http://www.cc.gatech.edu/fce/ahri
COUGAR Device Database Project	Distributed query processing.	http://www.cs.cornell.edu/database/cougar/index.htm
DataSpace	Distributed query processing.	http://www.cs.rutgers.edu/dataman/

Conclusion

- When the concept of DSNs was first introduced more than two decades ago, it was more a vision than a technology ready to be exploited. The early researchers in DSN were severely handicapped by the state of the art in sensors, computers, and communication networks.
- Technological advances in the past decade have completely changed the situation. MEMS (micro electromechanical system) technology, more reliable wireless communication, and low-cost manufacturing have resulted in small, inexpensive, and powerful sensors with embedded processing and wireless networking capability.
- However realization of sensor networks needs to satisfy the constraints such as fault tolerance, scalability, cost, hardware , topology change, environment and power consumption require new wireless ad hoc networking techniques and specifically it is required to develop technologies for different layers of the sensor networks protocol stack.

MANET : FUTURE WORK

Many questions about ad hoc networks remain unanswered. The areas inviting further investigations include :

- Scalability - how large can an adhoc network grow.
- Quality of service - can bandwidth or delay constrained applications operate well?
- Client server model shift - what happens when a client cannot count on traditional methods to locate a suitable server?
- Security- is there a good way to protect against attacks from malicious adhoc nodes?
- Interoperations with the Internet how can an adhoc network take advantage of evanescent or dynamically changing points of connection to the Internet?
- Power Control - how can battery life be maximized?

Scalability -

• Researchers have run the simulation of adhoc network with up to 10,000 nodes, but the simulation definitely interferes with such experiments. One simulation can easily take over a gigabyte of memory and equal amounts of disk storage depending on which parameters are being measured.

• With on demand protocols, one can deploy larger populations of mobile nodes in the adhoc network by accepting *worse performance for route acquisition latency*.

•Looking at it the other way around demanding very short latencies for route acquisition can place heavy (or impossible) constrains on network size.

•Starting from a network without structure or valid route cache entries, the **minimum route acquisition latency that allows full connectivity** is the product of the maximum diameter of the network multiplied by the minimum node traversal time for route request.

•At any point, the average route acquisition latency can be much better or much worse than this depending on average dissemination of valid route information and network congestion.

Scalability

- Lastly, It should be mentioned that adhoc networking ideas that exhibit sufficient scalability while still allowing subnet aggregation may find natural application in the Internet at large.

- This would help the problem of route threshing in the Internet, which is partially caused by routes that change too fast to be faithfully managed by the routing protocols in use [Dieering + 2000].
- Conversely we might find that the continued scalability to larger node population may require some advanced routing techniques from wide area routing protocols. However, I believe that such techniques are rendered necessary by the on demand nature of several adhoc network protocols. It seems likely that the Internet will ever barrow this idea of on demand route acquisition.

QoS: Special issues in MANET

- MANETs differ from the traditional wired Internet infrastructures. The differences introduce difficulties for achieving Quality of Service in such networks. The following list intemizes some of the problems:
- • *DYNAMIC APOLOGIES*: Nodes are free to move arbitrarily; thus , the network topology –which is typically multihop –may change randomly and rapidly at unpredictable links.
- • *BANDWIDTH – CONSTRAINED ,Variable capacity links* : Wireless links will continue to have significantly lower capacity than their hardwired counterparts . In addition, the realized throughput of wireless communications - after accounting for the effects of multiple access ,fading, noise, and interference conditions etc. –is often much less than a radio's maximum transmission rate.

QoS in MANETs

One effect of the relatively low to moderate link capacities is that congestion is typically the norm rather that the exception, i.e. aggregate application demand will likely approach or exceed network capacity frequently . As the mobile network is often simply an extension of the fixed network infrastructure ,mobile ad hoc users will demand similar services. These demands will continue to increase as multimedia computing and collaborative networking applications rise.

- *ENERGY-CONSTRAINED OPERTION:* some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

QoS Adptation

- In contrast to a wired network, the QoS situation in MANET may change rapidly and dramatically all the time due to wireless link characteristic or mobility. For example even if the signaling provides vary fast local repair mechanisms, it is not guaranteed that after a path breaks, same QOS can be granted in new path.
- Under certain circumstances it may happen that an active flow is re-routed to a bottleneck node, which causes end-to-end bandwidth of the flow to decrease.
- On the other hand, the available bandwidth will increase if less traffic is in the network or if any application releases its reserved bandwidth. So application cant rely on the QoS investigation done during session establishment.To sole the problem the QOS framework has to actively monitor the network dynamics and adapt flow in response to observe changes based on some adaptation strategy.

Quality of Service

•Many of the candidate protocol in this book operate to establish end-to-end connectivity between network applications by finding a communication path between intermediate points. Thus for these approaches it would be difficult to know whether any particular application bandwidth or delay requirement can be supported by communication path.

•For many traditional audio and video application specifically 2 way voice communication. It is quite likely that the chosen communication path between the end points will have to meet additional constraints. The application will have to supply its constraints parameters to the routing layers so that suitable path can be found.

•The path can be found in several ways for instance with a protocol maintain full link state information dynamically for every link in the adhoc network, the well known Dijkstra's algorithm can be applied, taking in to account whether each link under consideration meets the application requirement.

•Alternatively almost any on demand protocol can be equipped with extensions describing the requirements so that only appropriate paths are returned during route discovery. This is the approach taken by AODV a more sophisticated link state approach to the problem is discussed.

QoS

- Constraint parameter i.e. QoS parameter is supplied to the routing layer to find suitable path.
- To find path for full link state information Dijkstra's algorithm is applied.
- AODV protocol is used to find appropriate path to discover route.
- Existing protocols are integrated to overcome dynamic link failure.

Client Server Model Shift –

- Network client is automatically configured with the identity of Server.
- Dynamic discovery algorithm is used for automatic configuration.
- Adhoc network is characterized by dynamic nature.
- Automatic configuration depends on Client transaction with a configuration server such as DHCP.
- DHCP manages client parameter based on the subnet to which client is connected.

Connecting to the Internet -

- If a node in an adhoc network to global internet that node can offer internet connectivity to other nodes.
- Internet gateway acts as a default router so that other nodes in adhoc network consider themselves connected to default router by multihop path through other nodes.
- For internet connectivity point of view consider entire adhoc domain as a single hop.
- A default router can be made foreign agent for mobile IP.

Security –

- Security for routing protocol is difficult because of key distribution & refresh.
- Public Key Infrastructure (PKI) algorithms have disadvantages from using algorithms that are more CPU intensive than are symmetric key algorithm.
- In adhoc network without infrastructure it is difficult to make good use of Certificate Revocation List (CRL).
- Symmetric key algorithms rely on secured distribution of secret key shared between partners.
- Multicast data distribution in adhoc network plays major role in security.

Power Control -

- Two important aspects to power control for wireless mobile nodes to extend battery life –
    - Reducing power to communication interfaces
    - Entering sleep mode
- Power saving techniques are crucial to cellular telephones & wireless PDAs.
- Some scheduling is required to enable sleep mode which uses synchronization between wireless nodes.
- Special signaling channel is used to wake up wireless nodes.
- The alternative is to use signals with paging subsystems.

Researching with MANet & Sensor

- **Our research efforts have been focussed mostly on the perofrmance issues of MANet routing protocols.**
- **As newer concepts needs some "cooking time" before they can be deployed as technolgies, same goes with these new Wireless developments as well.**
- **We have taken into acount various issue such as mobility of nodes, network load and behaviour of various routing protocols of MANet.**
- **Though we have used some of models for our job but mostly have used the one of the most widely used Network simulator, named NS2.**

About – Network Simulator

- NS2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, It has many advantages such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms.
- NS2 started as a variant of the REAL network simulator in 1989 . REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks.
- Currently NS2 development by VINT group is supported through DARPA with SAMAN and through NSF with CONSER, available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS2 also builds and runs under Windows.

About – Network Simulator

- NS2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, It has many advantages such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms.
- NS2 started as a variant of the REAL network simulator in 1989 . REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks.
- Currently NS2 development by VINT group is supported through DARPA with SAMAN and through NSF with CONSER, available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS2 also builds and runs under Windows.

About – Network Simulator

- NS2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, It has many advantages such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms.
- NS2 started as a variant of the REAL network simulator in 1989 . REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks.
- Currently NS2 development by VINT group is supported through DARPA with SAMAN and through NSF with CONSER, available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS2 also builds and runs under Windows.