MAC Protocol for Ad hoc Wireless Networks

Aim of MAC:

- provide fair access to shared broadcast radio channel.

Issues to deal with:

- Bandwidth efficiency: – must be maximized.

The radio spectrum is limited, the bandwidth available for communication is also very limited. The MAC protocol must be designed in such a way that the scarce bandwidth is utilized in an efficient manner. The control overhead involved must be kept as minimal as possible.

Bandwidth efficiency=ratio of the bandwidth used/ Total Bandwidth

- Real-time traffic support: – should be provided.

- QoS support to data sessions in such networks is very difficult. Bandwidth reservation made at one point of time may become invalid once the node moves out of the region where the reservation was made.
- QoS support is essential for supporting time-critical traffic sessions such as in military communications.
- The MAC protocol for ad hoc wireless networks that are to be used in such real-time applications must have some kind of a resource reservation mechanism

- Synchronization: – sometimes needed, e.g. TDMA.
  - Exchange of control packets may be required for achieving time synchronization among nodes. Very important for bandwidth (time slot) reservations by nodes.

- Shared broadcast medium: – collisions must be avoided/minimized.
  - A node should get access to the shared medium only when its transmissions do not affect any ongoing session.
  - Since multiple nodes may contend for the channel simultaneously, the possibility of packet collisions is quite high in wireless networks.
  - A MAC protocol should grant channel access to nodes in such a manner that collisions are minimized

- Lack of central coordination: – fully distributed MAC design.
  - Nodes must be scheduled in a distributed fashion for gaining access to the channel.
  - The MAC protocol must make sure that the additional overhead, in terms of bandwidth consumption, incurred due to this control information exchange is not very high.

MAC Protocol for Ad hoc Wireless Networks

- Mobility of nodes: – loss of connectivity; – network partitioning; – bit errors.
- The protocol design must take this mobility factor into consideration so that the performance of the system is not significantly affected due to node mobility.

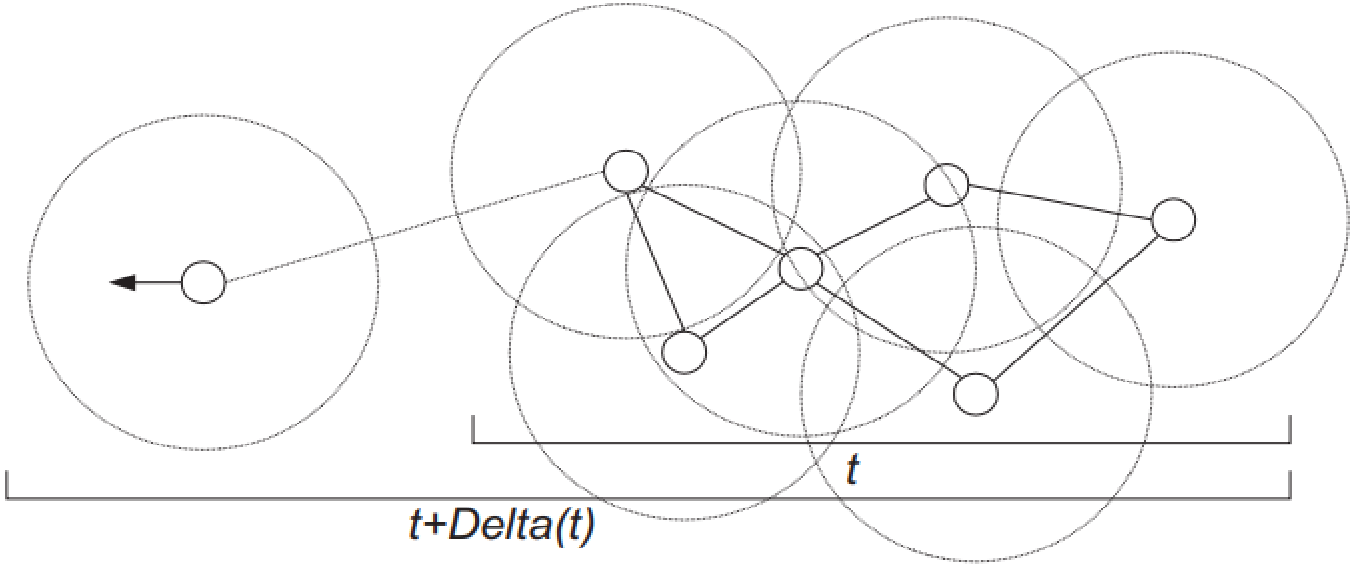


Figure 3: Network partitioning is one of the biggest problem to deal with at MAC sublayer.

MAC Protocol for Ad hoc Wireless Networks

- Hidden terminal problem: – collisions → inefficient bandwidth utilization.

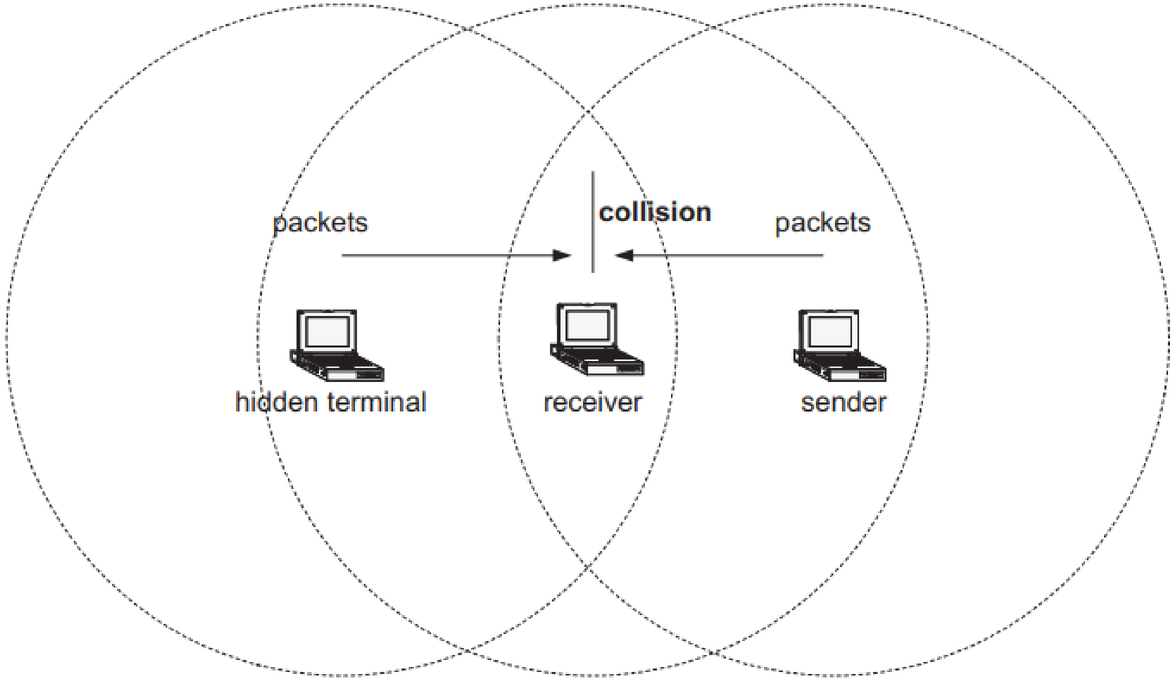


Figure 1: Illustration of the hidden terminal problems.

MAC Protocol for Ad hoc Wireless Networks

- Exposed terminal problem: – inability to transmit → inefficient bandwidth utilization.

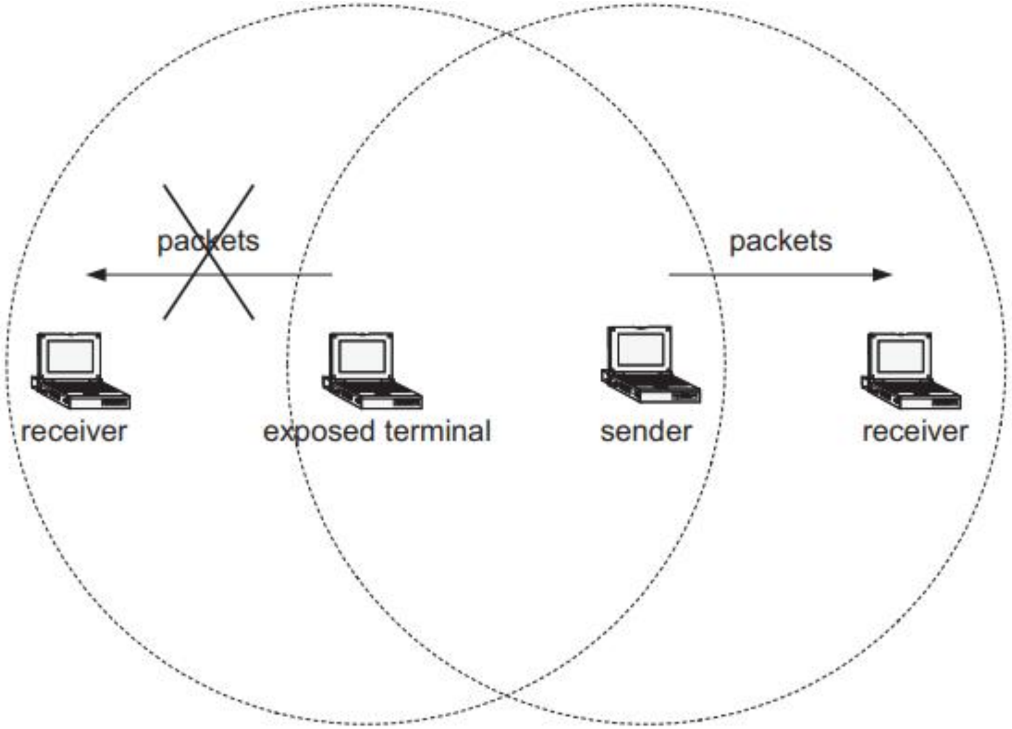


Figure 2: Illustration of the exposed terminal problem.

MAC Protocol for Ad hoc Wireless Networks

Design goals-What we want from MAC protocol?

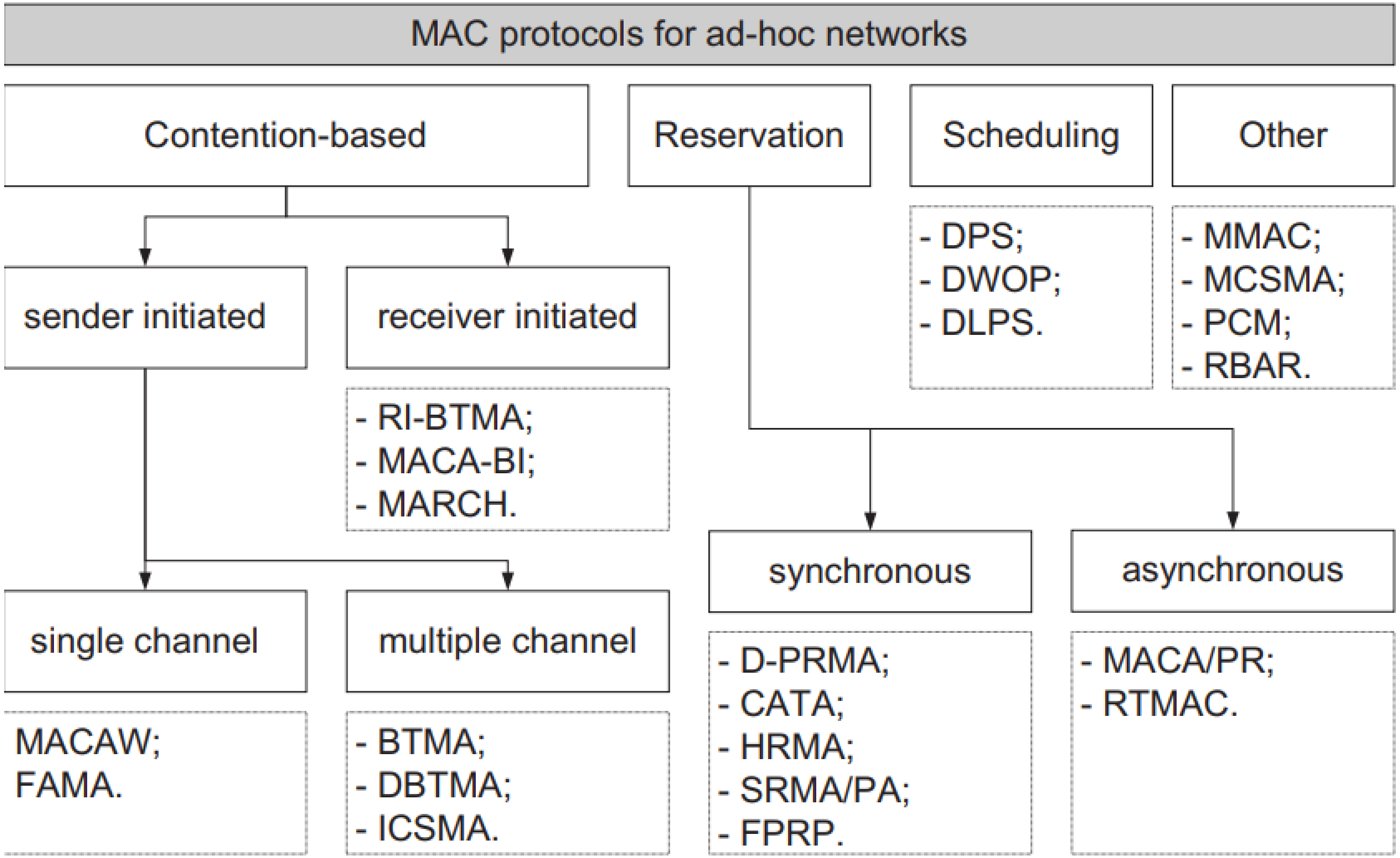
- allow fair access to the shared radio medium;
- operation of the protocol should be distributed;
- should support real-time traffic;
- the access delay must be minimized;
- available bandwidth must be utilized efficiently;
- fair bandwidth allocation to competing nodes;
- control overhead must be minimized;
- the effects of hidden/exposed terminals must be minimized;
- must be scalable;
- should minimize power consumption;
- should provide synchronization between nodes.

MAC Protocol for Ad hoc Wireless Networks

Classification of MAC protocols

- Contention-based protocols without reservation/scheduling:
  - no reservation of the bandwidth is made;
  - guarantees are not possible.
- Contention-based protocols with reservation mechanisms:
  - bandwidth for transmission is reserved in advance.
  - guarantees are possible.
- Contention-based protocols with scheduling mechanisms:
  - distributed scheduling between nodes is used.
  - guarantees are possible.
- Protocols that do not fall to any of these categories:
  - implement several features of different protocol groups or
  - use completely different approach

MAC Protocol for Ad hoc Wireless Networks



MAC protocols for ad-hoc networks

Contention-based

sender initiated

single channel

MACAW;
FAMA.

multiple channel

- BTMA;
- DBTMA;
- ICSMA.

receiver initiated

- RI-BTMA;
- MACA-BI;
- MARCH.

Reservation

synchronous

- D-PRMA;
- CATA;
- HRMA;
- SRMA/PA;
- FPRP.

asynchronous

- MACA/PR;
- RTMAC.

Scheduling

- DPS;
- DWOP;
- DLPS.

Other

- MMAC;
- MCSMA;
- PCM;
- RBAR.

MACA

- Contention based protocols w/o reservation/scheduling
  - The basic idea: contention for the resource, winning node transmits.
- **Multiple access collision avoidance (MACA) protocol (Extension of CSMA):**
- **CSMA operates as follows:**
  - the sender sense the channel for the carrier signal;
  - if the carrier is present it retries to sense the channel after some time (exp. back-off);
  - if not, the sender transmits a packet.
- The following shortcomings are inherent to CSMA/CA:
  - hidden terminal problem leading to frequent collisions;
  - exposed terminal problem leading to worse bandwidth utilization.
- To avoid it:
  - virtual carrier sensing;
  - RTS-CTS handshake before transmission.

MACA

- MACA does not make use of carrier-sensing for channel access.
- Two additional signaling packets: the request-to-send (RTS) packet and the clear-to-send (CTS) packet are used.
- When a node has data to transmit, it first transmits an RTS packet.
- The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.

MACA

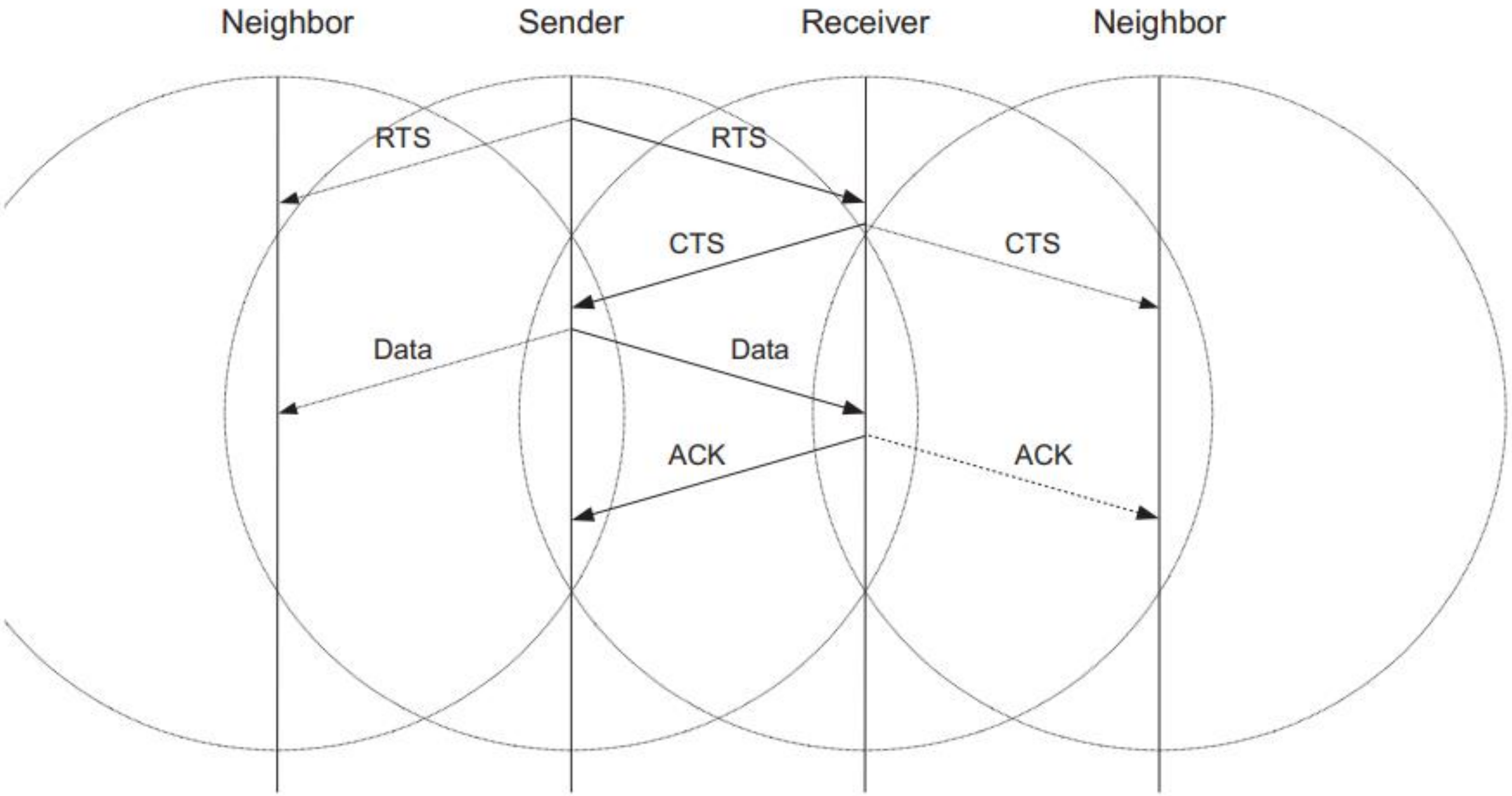


Figure 4: Packet transmission in MACA.

MACA

- If the transmission fails in MACA:
- The node uses the binary exponential back-off (BEB) algorithm
- In the binary exponential backoff mechanism, each time a collision is detected, the node doubles its maximum back-off window.
  - contention window: CW×2;
  - retransmission of RTS.

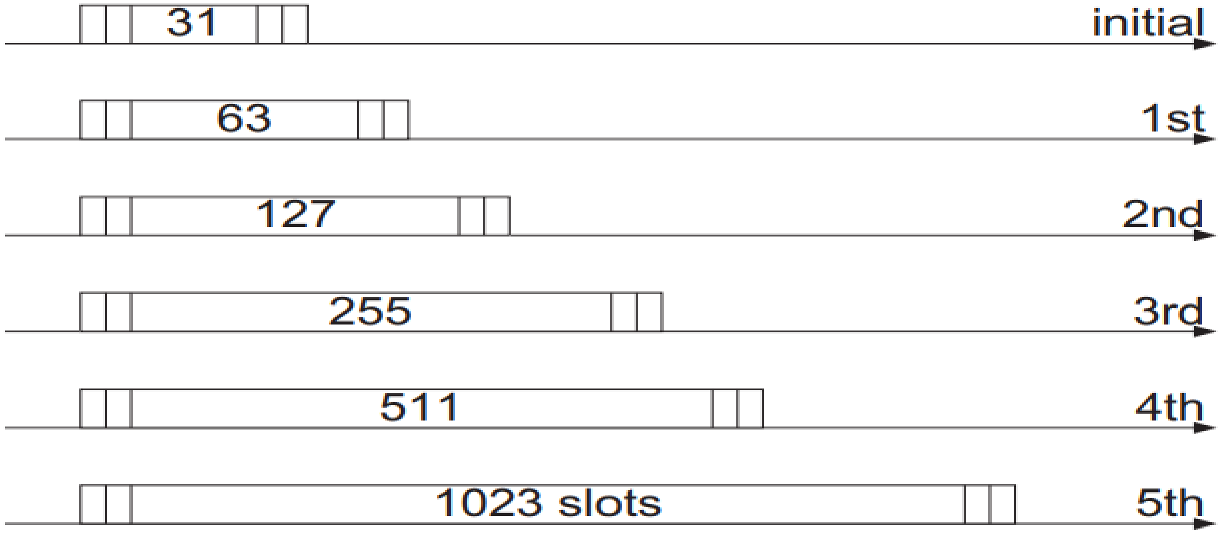


Figure 6: Evolution of the contention window with increasing of transmission attempts.

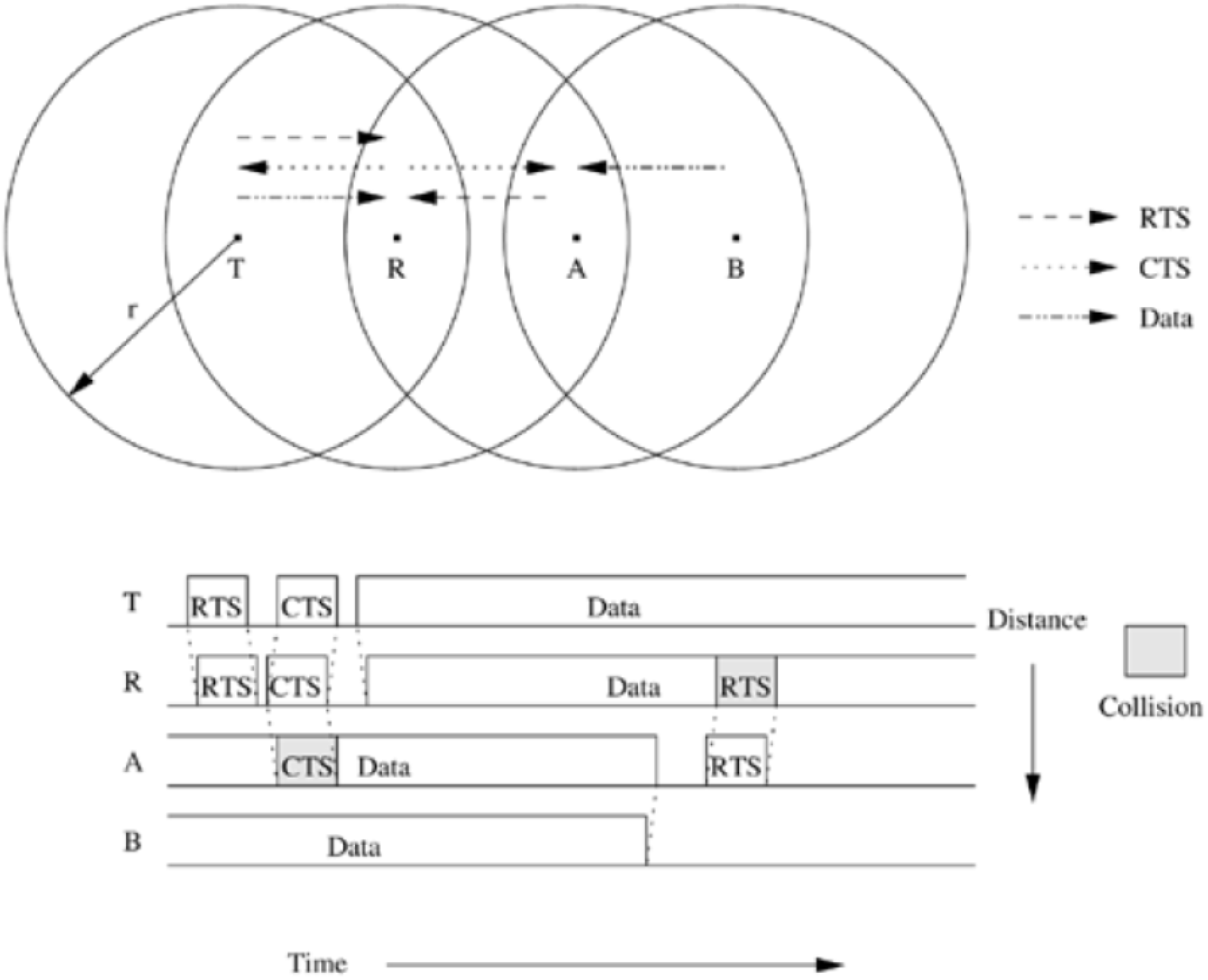
Solving Hidden and Exposed Terminal

- Both the RTS and the CTS packets carry the expected duration of the data packet transmission.
- Neighbor nodes near the sender that hear the RTS packet do not transmit for a long enough period of time so that the sender could receive the CTS packet.
- A node near the receiver, upon hearing the CTS packet, defers its transmission till the receiver receives the data packet. **Thus, MACA overcomes the hidden node**
- Similarly, a node receiving an RTS defers only for a short period of time till the sender could receive the CTS. If no CTS is heard by the node during its waiting period, it is free to transmit packets once the waiting interval is over.
- Thus, a node that hears only the RTS packet is free to transmit simultaneously when the sender of the RTS is transmitting data packets. Hence,
- Thus, the **exposed terminal problem is also overcome in MACA.**
- But MACA still has certain problems, which was why MACAW, described below, was proposed.

Hidden Terminal Problem with RTS-CTS

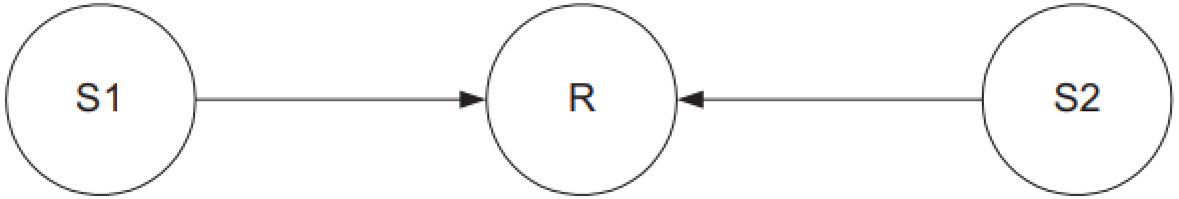
- The RTS-CTS control packet exchange cannot ensure collision-free data transmission that has no interference from hidden terminals.
- One very important assumption made is that every node in the capture area of the receiver (transmitter) receives the CTS (RTS) cleanly.
- Nodes that do not hear either of these clearly can disrupt the successful transmission of the Data or the ACK packet.

Hidden Terminal Problem with RTS-CTS



MACAW (MACA for Wireless)

- There are still some problems in MACA which are resolved by MACAW: an extension of MACA
- **Problem 1 of MACA: starvation of flows:**
  - both S1 and S2 have the high volume of traffic, S1 seizes the channel first;
  - packets transmitted by S2 get collided and it doubles CW (CW = 2CW);
  - the probability that the node S2 seizes the channel is decreasing.



Starvation of the flow from S2.

Solution:

- the packet header contains the field set to the current back-off value of the transmitting node;
- a node receiving this packet copies this value to its back-off counter (fairness);

MACAW

- **Problem 2 of MACA: fast adjustment of CW:**
  - when a node successfully transmits a packet;
  - when a collisions is detected by a node.

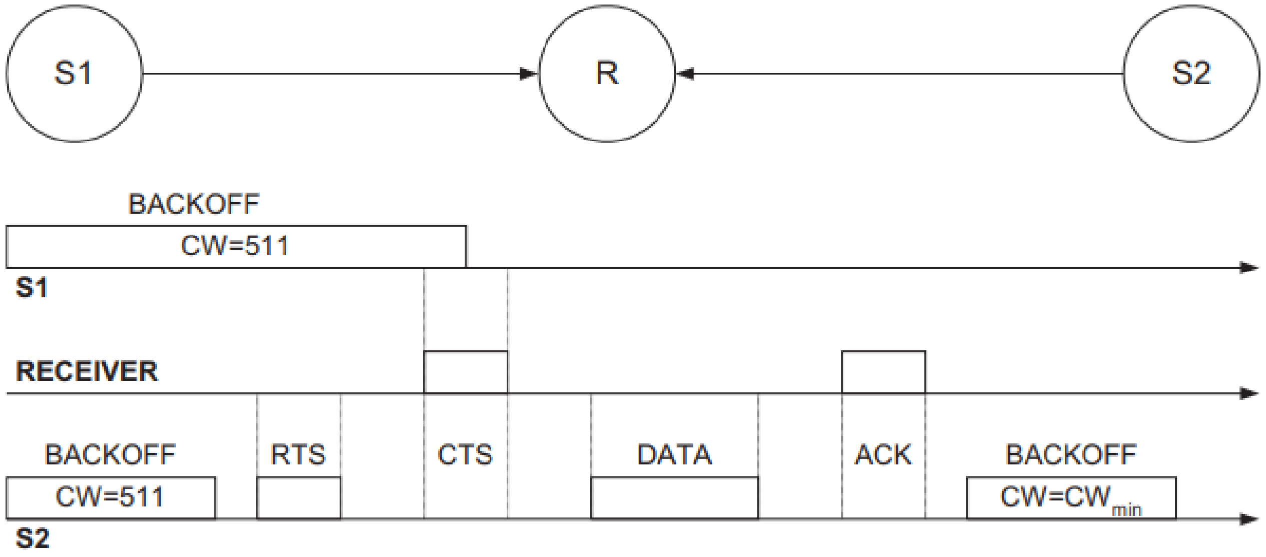


Figure 8: Rapid adjustments of the CW.

Solution: multiplicative increase when collision, linear decrease when success.

BEB in MACAW

- Multiplicative increase, linear decrease (MILD)
- MACAW sender:
  - CW0 = 2 and CWM = 64
  - Upon failed RTS/CTS

    CW =min[1.5CW, CWM]
  - Upon successful RTS/CTS but failed ACK, no change
  - Upon successful RTS/CTS/DATA/ACK

    CW=CW−1

- Another modification related to the back-off mechanism is that the MACAW implements per flow fairness as opposed to the per node fairness in MACA.
- This is done by maintaining multiple queues at every node, one each for each data stream, and running the backoff algorithm independently for each queue.
- A node that is ready to transmit packets first determines how long it needs to wait before it could transmit an RTS packet to each of the destination nodes.
- It then selects the packet for which the waiting time is minimal.

ACK in MACAW

- In MACA, the responsibility of recovering from transmission errors lies with the transport layer. As many TCP implementations have a minimum timeout period of about 0.5 sec, significant delay is involved while recovering from errors. Decreases the network throughput.
- But in MACAW, the error recovery responsibility is given to the data link layer (DLL).
- In MACAW, after successful reception of each data packet, the receiver node transmits an ACK packet.
- If the sender does not receive the ACK packet, it reschedules the same data packet for transmission.
- The sender would retry by transmitting an RTS for the same packet.
- But now the receiver, instead of sending back a CTS, sends an ACK for the packet received, and the sender moves on to transmit the next data packet.

MACAW

- **Problem 3 of MACA: an exposed node is free to transmit.**
    - node S2 hears RTS but not CTS (exposed node);
    - S2 initiates transfer to R2;
    - DATA from S1 and CTS from R2 may collide, CW unnecessary increases at S2.

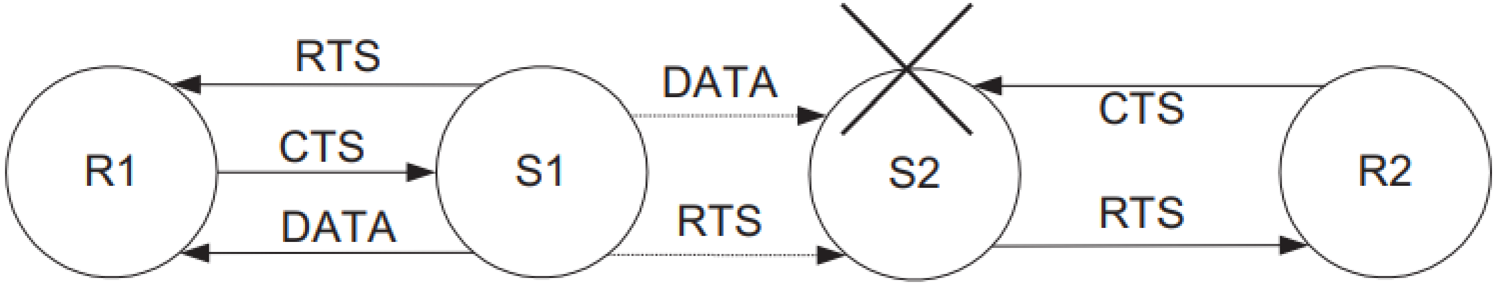


Figure 9: Problems with exposed node.

We conclude from this line of reasoning that S2 should defer transmission while S1 is transmitting data. Note that because S2 has only heard the RTS and not the CTS, station S2 cannot tell if the RTS-CTS exchange between S1 and R1 was a success and so does not know. So to confirm its successfulness a DS packet is used.

Solution: use of small data sending packet (DS) to update information.

MACAW

- **Problem 4 of MACA: neighbour receivers problem:**

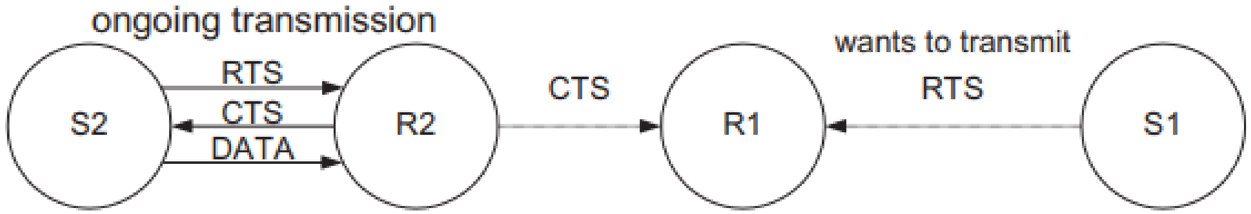


Figure 10: Illustration of the neighbor receivers problem.

- **Solution**: usage of request-for-request (RRTS) to send packets:
  - if R1 had received RTS (S1) and did not respond due to R2-S2 it backs off sends RRTS;
  - R2 hears RRTS waits for successive RTS-CTS between S1 and R1;
  - S1 hears the RRTS, transmits regular RTS and RTS-CTS-DATA-ACK takes place

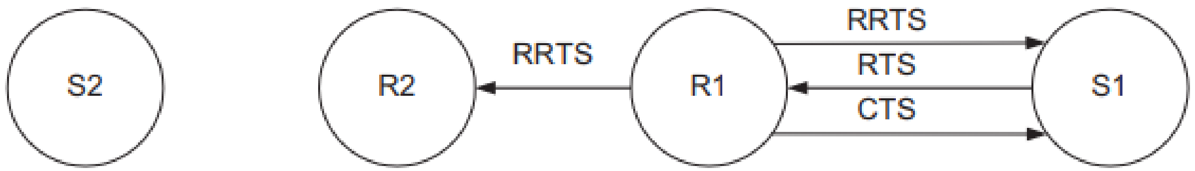


Figure 11: Solution of the neighbor receivers problem.

MACAW

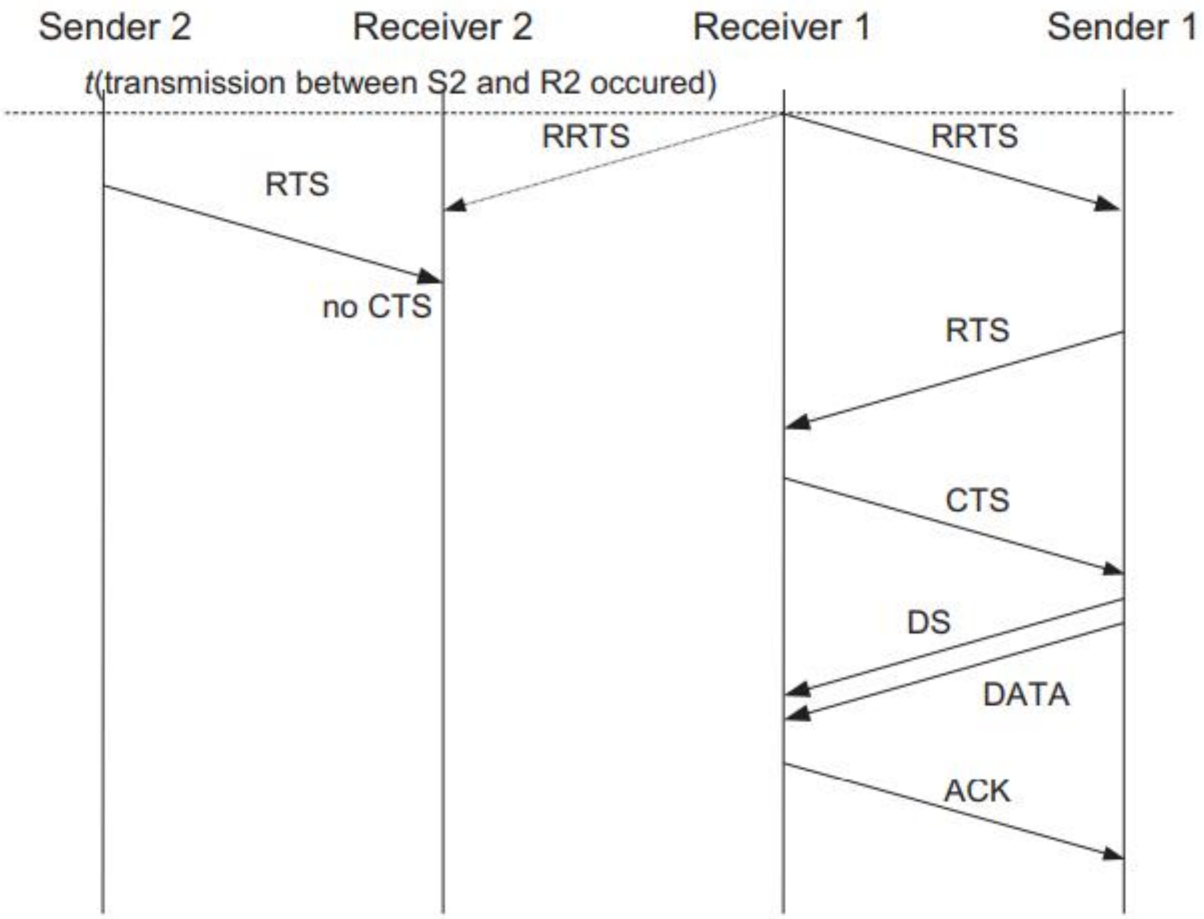
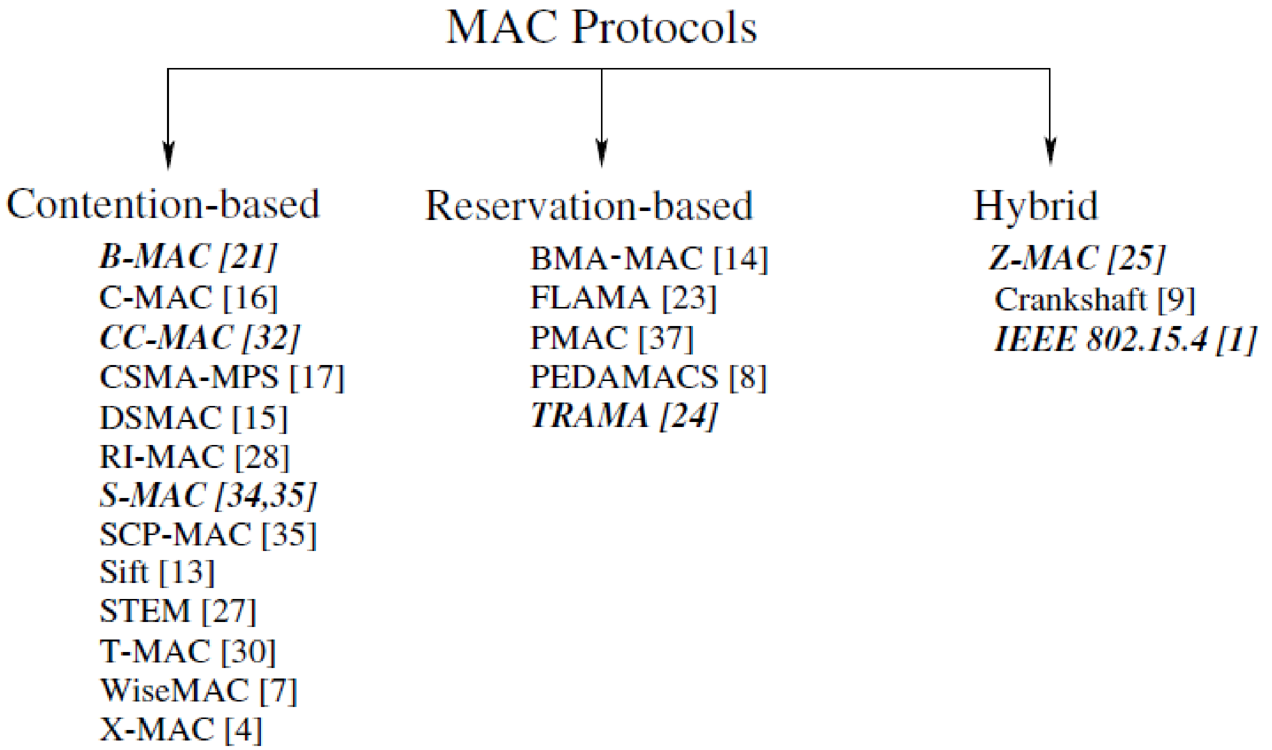


Figure 12: Packets exchange in neighbor receivers problem.

MAC for Sensor Networks

- The approaches can be classified into three main classes:
  - *contention-based medium access*,
  - *reservation-based medium access*, and
  - *hybrid solutions* that merge these two scheme
- These solutions depend on two fundamental multiple access schemes: carrier sense multiple access (CSMA) and time division multiple access (TDMA).



MAC Protocols

Contention-based

B-MAC [21]
C-MAC [16]
CC-MAC [32]
CSMA-MPS [17]
DSMAC [15]
RI-MAC [28]
S-MAC [34,35]
SCP-MAC [35]
Sift [13]
STEM [27]
T-MAC [30]
WiseMAC [7]
X-MAC [4]

Reservation-based

BMA-MAC [14]
FLAMA [23]
PMAC [37]
PEDAMACS [8]
TRAMA [24]

Hybrid

Z-MAC [25]
Crankshaft [9]
IEEE 802.15.4 [1]

Challenges for MAC in WSN

- Traditional protocol aim: Latency and throughput
- WSN's protocols: Energy conservation
- *Energy Consumption: Main sources* sensing, processing, and communication.
  - -Idle listening
  - -Collisions
  - -Protocol overhead
  - -Transmit vs. receive power
- *Architecture: Sparse vs Dense Deployment, Topological information, Single hop vs Multi-hop*
- *Event-Based Networking: Periodic traffic vs Bursty Traffic*
- *Correlation: Spatial and Temporal correlation can be utilized to optimize the MAC schedule*

Basic CSMA Mechanism

A node, first, listens to the channel for a specific time, which is generally referred to as the interframe space (IFS). Then, the node acts based on two conditions:

- *If the channel is idle* for the duration of the IFS, the node may transmit immediately.
- *If the channel becomes busy* during the IFS, the node defers transmission and continues to monitor the channel until the transmission is over.

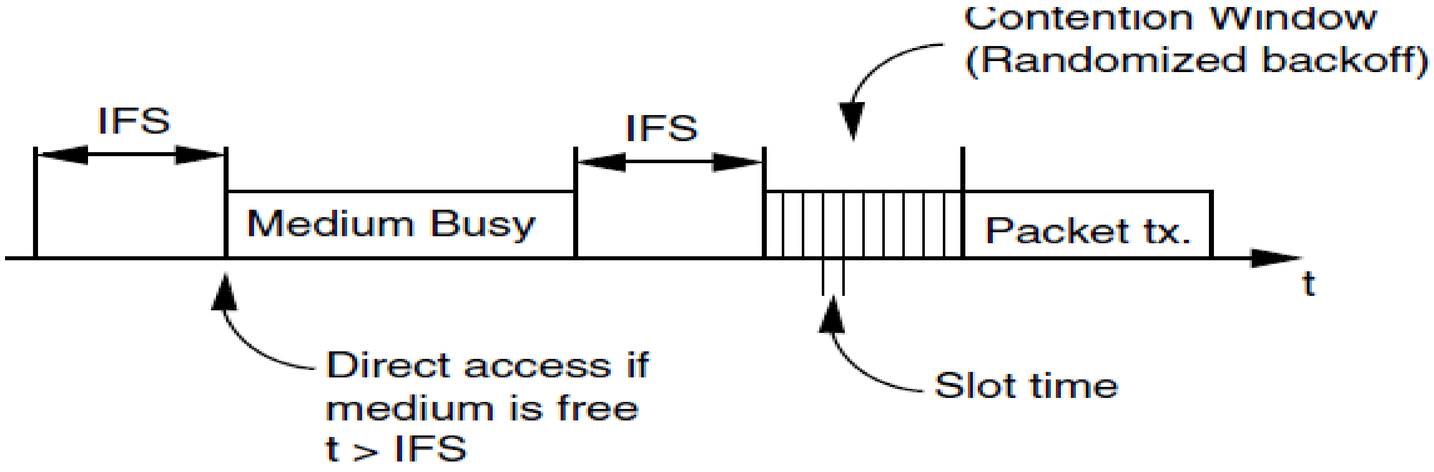


Figure 5.2 Basic CSMA protocol.

CSMA/CA Mechanism

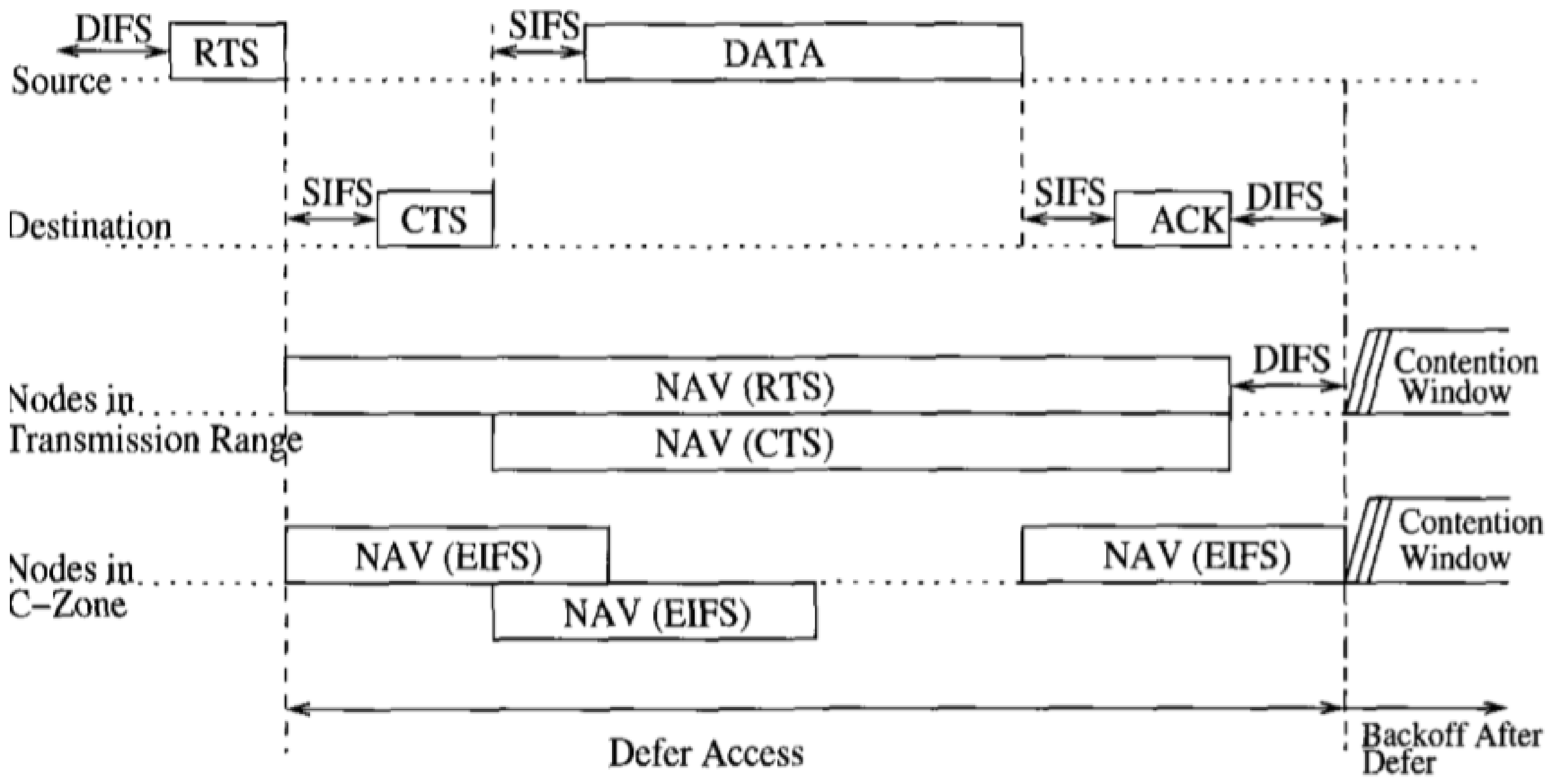


Figure 4.14 – Nodes in the transmission range and C-zone set their NAVs differently

Contention-Based Medium Access

- CSMA/CA performs poorly in terms of energy efficiency since nodes have to listen to the channel for contention and before transmission.
- Nodes also consume energy during the idle listening period
- As the density of the network increases, the collision avoidance mechanism becomes ineffective due to the increased number of hidden nodes

S-MAC

- Based on CSMA/CA protocol
- For handling continuous listening, *duty cycle operation* has been introduced.
- The activity of a node is scheduled according to a specific amount of time, called the *frame*
- During this frame a node sleeps for a specific amount of time and listens to the wireless channel for the rest of the frame
- Total duration of the frame is denoted as the *duty cycle*

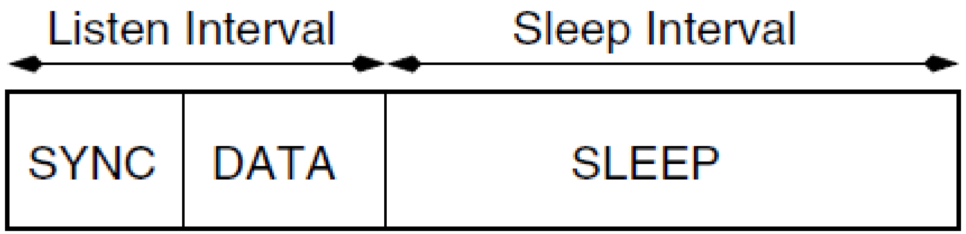


Figure 5.7 Listen and sleep intervals of S-MAC.

S-MAC

Periodic Listen and Sleep

- The operation of each node is maintained during frames. Each frame consists of two intervals, *listen* and *sleep*
- The listen interval is further divided into two intervals called SYNC and DATA.
- The main idea behind S-MAC is to construct virtual clusters of nodes that sleep and wake up at the same time.
- S-MAC ensures that nodes, which are in the transmission range of each other, synchronize according to a single sleep schedule by exchanging periodic SYNC messages.
- SYNC contains the ID of the sender node and the remaining time until the sender switches to sleep mode.
- Initially, a node listens to the channel for a specific amount of time, long enough to receive any SYNC packets sent by its neighbors. If no SYNC packet is received during this interval, the node determines its own sleep schedule and broadcasts a SYNC packet. This particular node is referred to as the *synchronizer*.
- It might happen that a node receives a neighbor’s schedule after it has selected its own schedule. In these cases, this node is referred to as the *border node*

Sender Node ID	Next Sleep Time

Figure 5.8 The structure of the S-MAC SYNC packets.

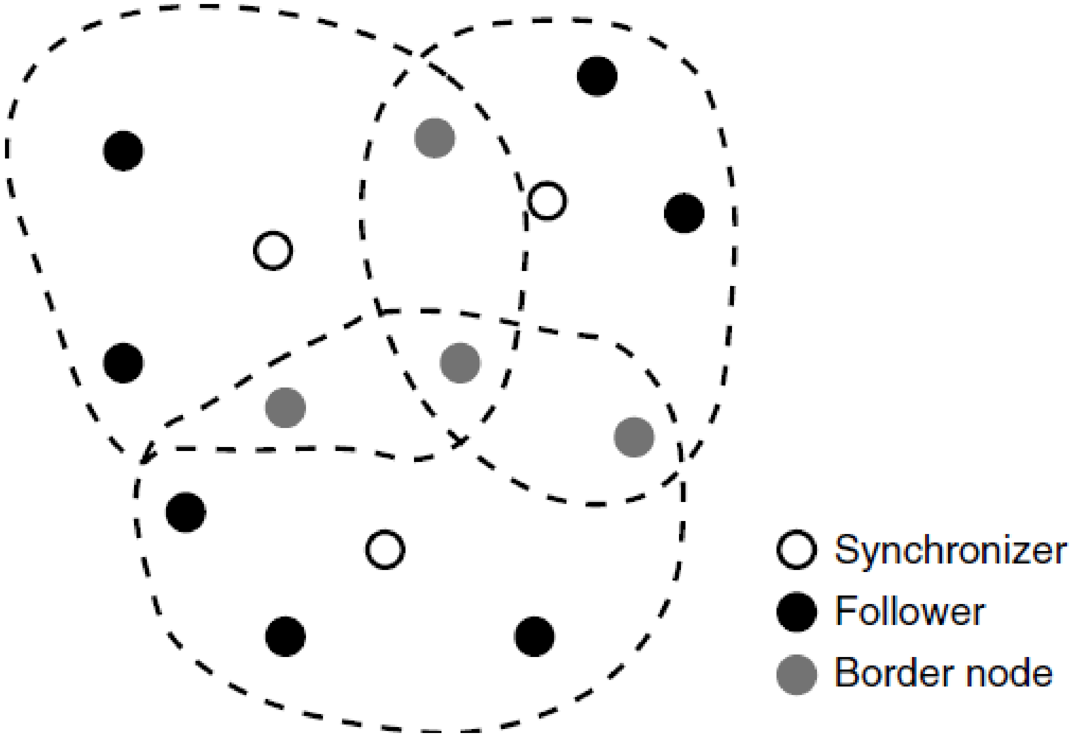


Figure 5.9 Virtual clusters of the S-MAC protocol.

S-MAC

- **Overhearing Avoidance**

  -When a node transmits its RTS packet, the intended receiver sends back a CTS packet during the “for CTS” interval. After the RTS–CTS exchange, the transmitter node starts to transmit its DATA packet.

  -Other nodes in the virtual cluster switch to sleep state until the end of the frame. This avoids wasting energy during idle listening and is referred to as *overhearing avoidance*

- **Multi-hop Awareness Problem**

  -During a single frame, a packet can only travel a single hop.

  -This results in an average delay proportional to the length of the path, which significantly affects the packet delivery delay of multi-hop networks.

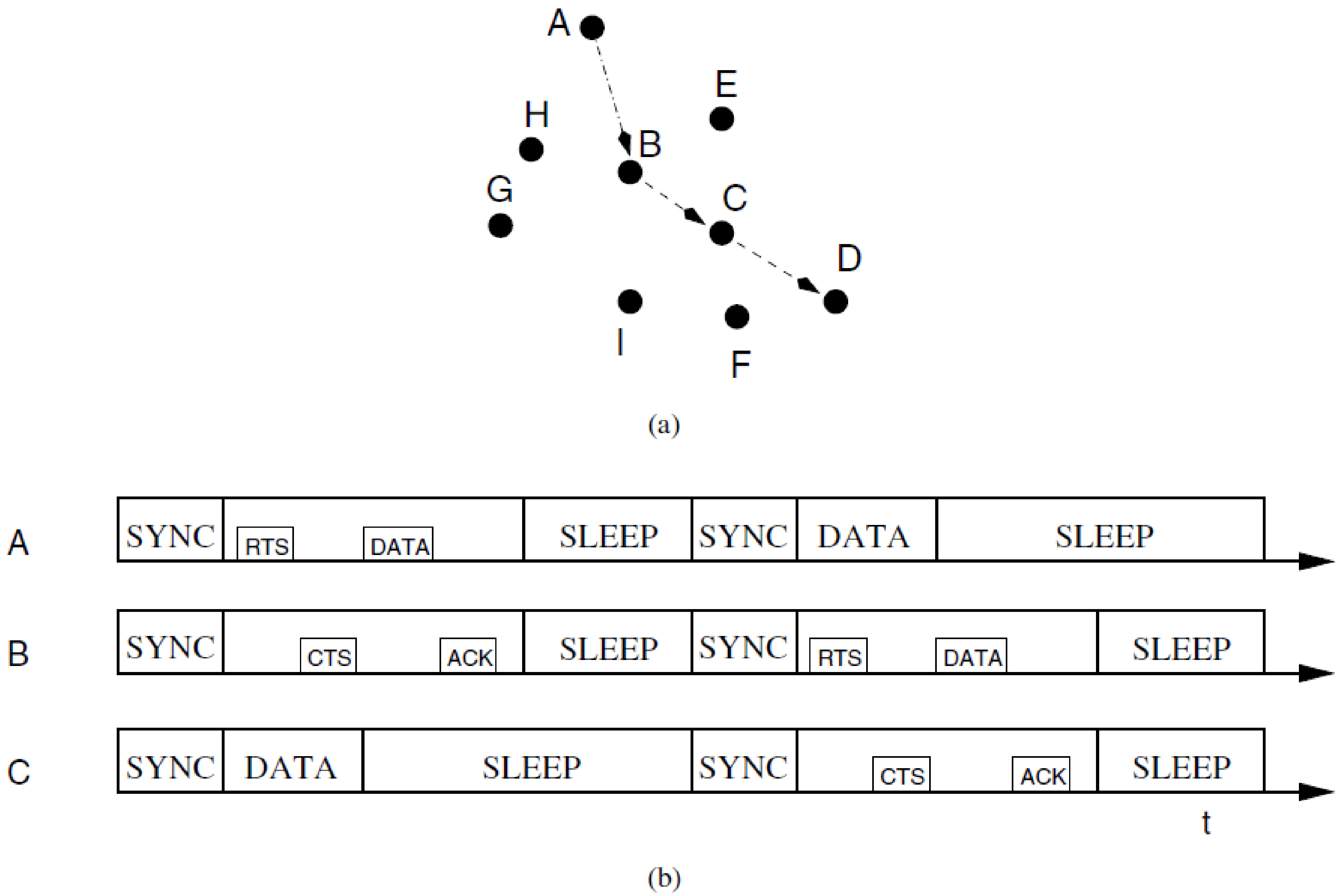


Figure 5.10 Multi-hop awareness problem: (a) topology and (b) MAC scheme.

S-MAC

- Ideal Solution for Multi-hop awareness Problem
  - An ideal way would be for each next hop to wake up when the transmission of the previous hop is finished.
  - Such a solution requires, firstly, a network-wide synchronization such that each node will wake up at the exact time and,
  - secondly, knowledge of the route a packet will take.
  - These requirements may not be feasible in a distributed WSN.
- Adaptive Listening a localized solution
  - Adaptive listening allows nodes that overhear a packet transfer to wake up at the end of this transfer in case they become the next hop.
  - adaptive listening mechanism reduces the latency of the basic S-MAC protocol by half.

S-MAC

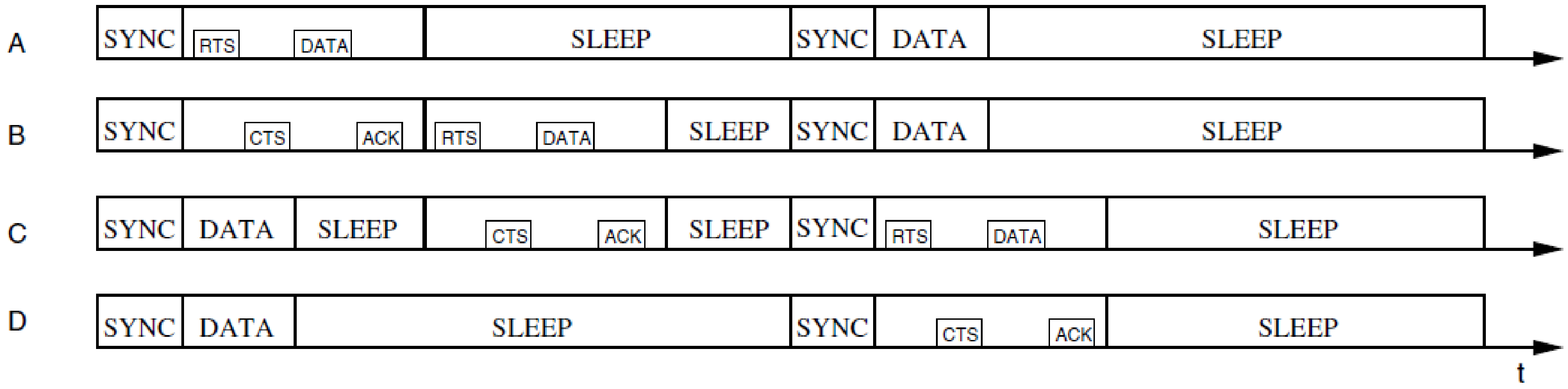

A SYNC RTS DATA SLEEP SYNC DATA SLEEP
B SYNC CTS ACK RTS DATA SLEEP SYNC DATA SLEEP
C SYNC DATA SLEEP CTS ACK SLEEP SYNC RTS DATA SLEEP
D SYNC DATA SLEEP SYNC CTS ACK SLEEP
t

Figure 5.11 Adaptive listening mechanism of S-MAC.

S-MAC

- **Message Passing**
  - Sending a burst of packets to transmit a large amount of information incurred a large overhead using RTS–CTS packets before each DATA packet.
  - Overhead is minimized in S-MAC through the message passing procedure.
  - When a node has a burst of packets to send, it uses the RTS–CTS exchange only for the first packet. Each packet is followed by an acknowledgment from the receiver.
  - The remaining duration of the burst transfer is included in each packet sent by the sender and the receiver nodes to prevent other nodes to access the channel

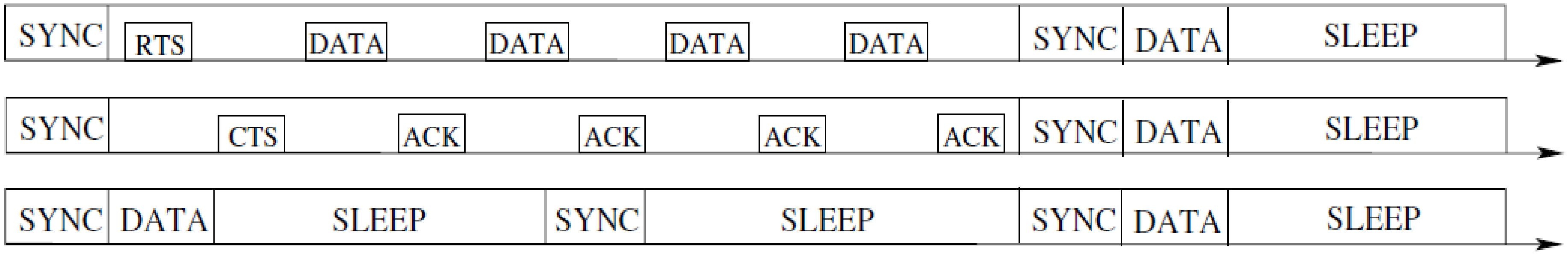


Figure 5.12 Message passing mechanism of S-MAC.

B-MAC

S-MAC Problems

- Duty cycle operation has two drawbacks in terms of energy inefficiency.
- Firstly, nodes need to send periodic messages, such as the SYNC packets used by S-MAC in each frame.
- Secondly, all the nodes need to be active during the listen period to wait for a possible incoming packet.
- As a result, even when there is no traffic, nodes consume energy at a rate at least equal to the duty cycle.

B-MAC

- B-MAC is based on sleep–wake scheduling using low-power listening (LPL) and carrier sensing using clear channel assessment (CCA) to improve the energy efficiency and channel utilization.

LPL

- Each node can determine its sleep and wakeup schedule without any synchronization with the other nodes. (Prob: to wakeup transmitter and receiver at same time)
- Handled by LPL to send a preamble before each packet to *wake up* the intended receiver
- Each node periodically wakes up, turns on its radio, and checks for activity on the channel.
- During this small period, if activity is detected on the channel, the node stays in the receive mode if no activity is detected, then the node switches back to sleep state.

B-MAC

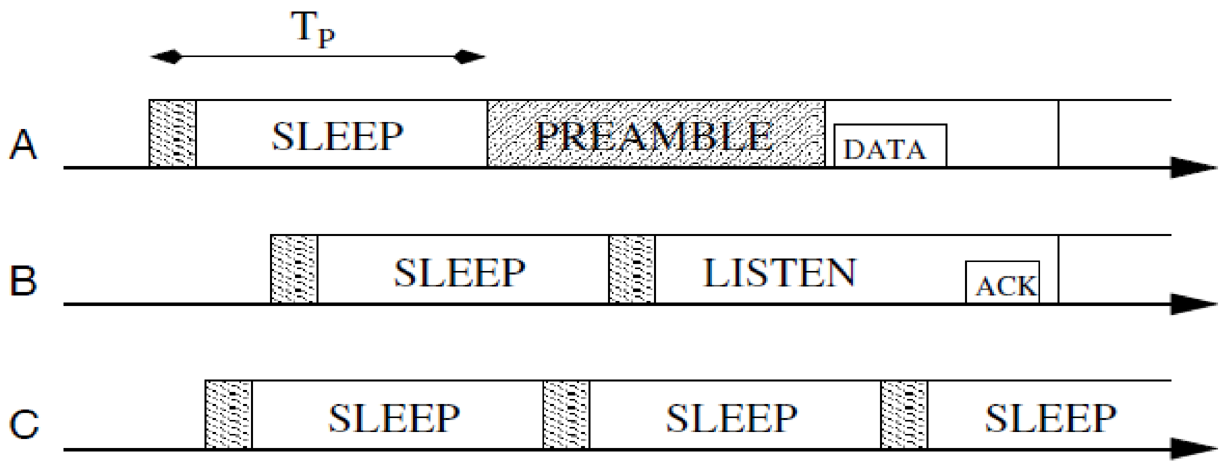


Figure 5.13 Preamble sampling.

This approach can be more energy consuming per packet transfer when compared to the sleep–wakeup schedule-based protocols.
However, it is certainly more energy efficient for the durations with no traffic.

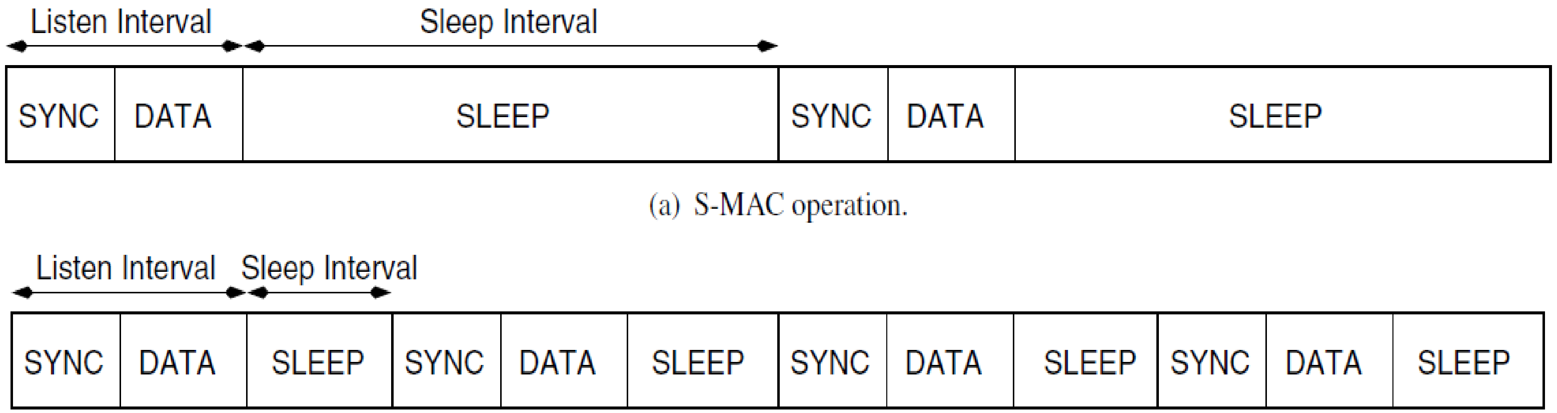
B-MAC

- **CCA**
- The success of the LPL technique, relies on the accuracy in sensing the activity on the channel.
- If a node assesses that there is an activity on the channel and wakes up when there is no activity (false positive), precious energy is wasted.
- On the other hand, if a receiving node cannot detect a preamble for itself (detection failure), the transmitter would waste energy because of the transmitted preamble and would have to wait for another sampling period to meet the receiver, which increases end-to-end latency and energy also.
- The main goal of the CCA mechanism is to differentiate between noise and a signal to accurately assess the channel activity.

DSMAC (Dynamic Sensor MAC)

- The main motivation behind this protocol is to minimize the medium access delay that may occur due to high traffic rate.
- If a node generates (or receives) more packets than it can immediately transmit, the delay that will be experienced by the packet will increase.
- It becomes intolerable with increased queue length which may cause congestion in the network.
- The solution is to double the duty cycle in case the medium access delay of a packet exceeds a pre-specified value.
- When a node decides to double its duty cycle, it broadcasts this value inside the SYNC packet that is sent at the beginning of each original frame. The node also includes its intended receiver in the SYNC message.

DSMAC (Dynamic Sensor MAC)



(a) S-MAC operation.

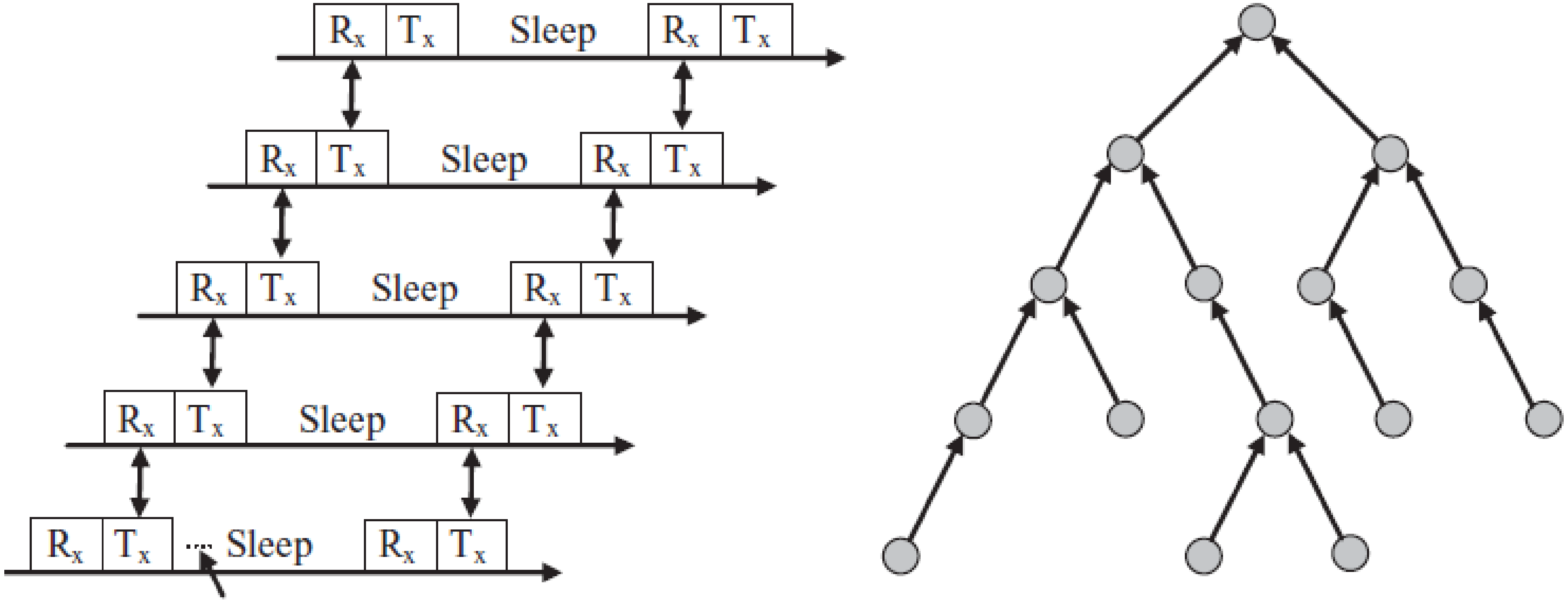
(b) DSMAC operation

Figure 5.17 Listen and sleep intervals of DSMAC.

D-MAC

- D - MAC is an energy - efficient and low - latency MAC protocol
- D - MAC employs a staggered wake - up schedule to enable continuous data forwarding on a multihop path
- In the schedule, an interval is divided into three periods (or states): receiving, sending, and sleeping.
- In the receiving period, a node is expected to receive a packet and send an ACK packet back to the sender. In the sending period, a node tries to send a packet to its next hop and receive an ACK packet. In the sleeping period, a node turns off its radio to save energy.
- Transmitting and receiving period have same length of μ , which is long enough for transmitting and receiving one packet.
- Depending on its depth d in the data gathering tree, a node sets its wake - up schedule $d\mu$ ahead from the schedule of the sink.

D-MAC



More slots if necessary

A data aggregation tree

Fig. 3.4 An aggregation tree in D-MAC and its implementation.

D-MAC

- D – MAC employs a slot - by - slot renewal mechanism to handle increased data transfer.

- A *more data* flag is piggybacked in the MAC header to indicate the request for an additional active period with little overhead.

- Before a node transmits a packet, it first sets the *more data* flag in the packet if either its buffer is not empty or it received a packet with a *more data* flag from its previous hop.

- The receiver will check if the *more data* flag is set in the received packet, and if the flag is set, it will also set the *more data* flag of its ACK packet to the sender. With this slot - by - slot renewal mechanism

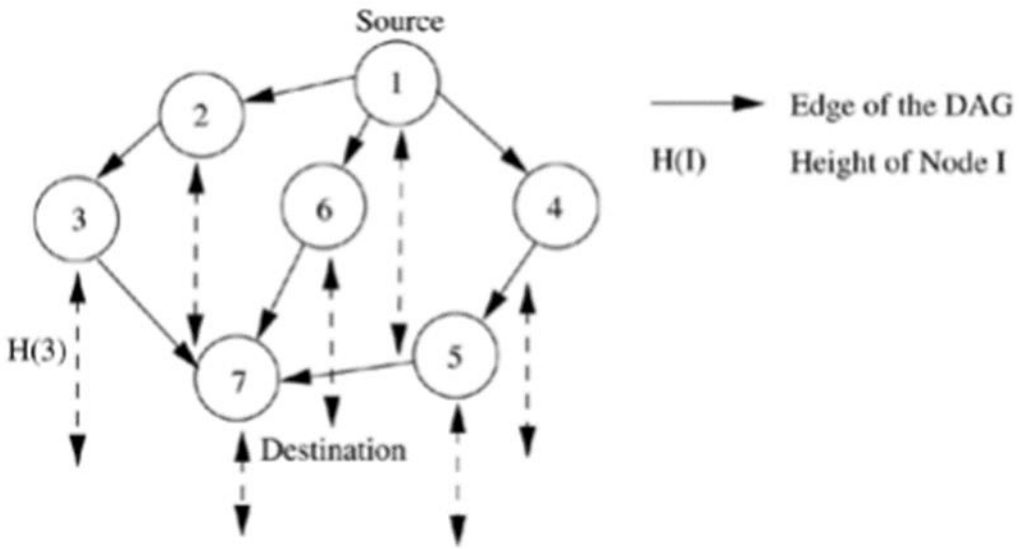
- D – MAC can adaptively adjust the duty cycles to the traffic load.

Temporally Ordered Routing Algorithm (TORA)

- Is a source-initiated on demand routing protocol.
- Uses a link reversal algorithm and provides loop-free multipath routes to a destination node.
- Each node maintains its one-hop local topology information and also has the capability to detect partitions.
- TORA has three main functions: establishing, maintaining, and erasing routes
- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link.
- A destination-oriented directed acyclic graph (DAG) is created using a Query/Update mechanism.
- A node require a route to a destination initiates a query packet containing destination address.

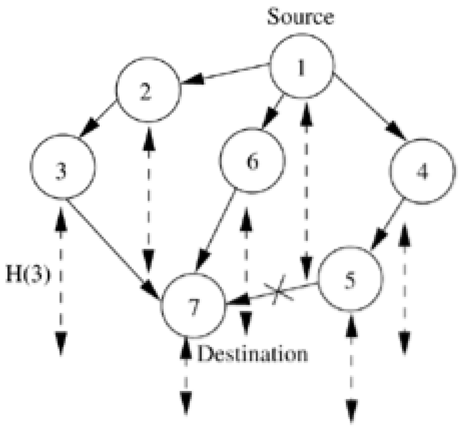
TORA

- The node have a valid route to that destination/ destination itself reply with an Update packet containing its distance from the destination (it is zero at the destination node).
- Each node that receives the Update packet sets its distance to a value higher than the distance of the sender of the Update packet.
- A set of directed links from the node which originated the Query to the destination is created

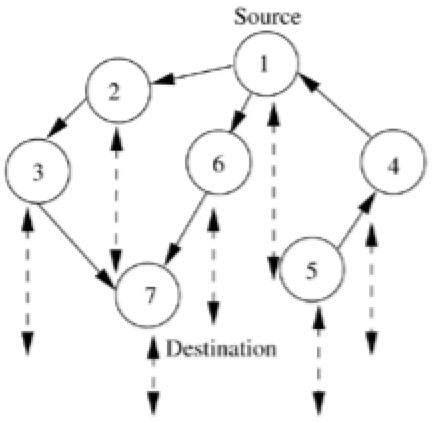


TORA

- When an intermediate node (say, node 5) discovers that the route to the destination node is invalid, it changes its distance value to a higher value than its neighbors and originates an Update packet.
- The neighboring node 4 that receives the Update packet reverses the link between 1 and 4 and forwards the Update packet.
- If the source node has no other neighbor that has a path to the destination, it initiates a fresh Query/Update procedure.



Link break beween Nodes 5 and 7



Nodes 4 and 5 reverse their links
in order to update the path

TORA

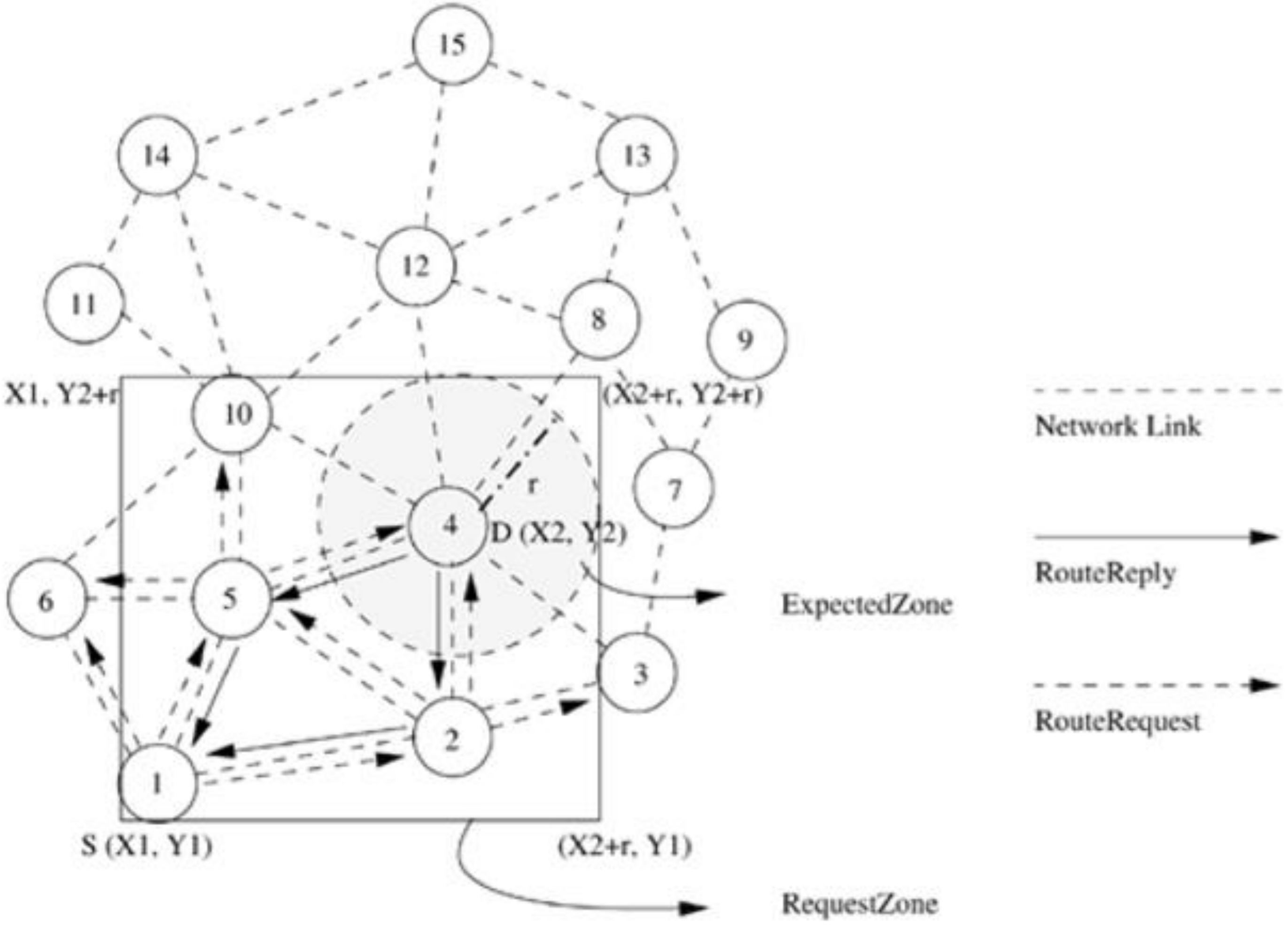
- Assume that the link between nodes 1 and 4 breaks.
- Node 4 reverses the path between itself and node 5, and sends an update message to node 5.
- Since this conflicts with the earlier reversal, a partition in the network can be inferred. I
- if the node detects a partition, it originates a Clear message, which erases the existing path information in that partition related to the destination.
- Advantages: less control overhead, partition detection.
- Disadvantages: Not uses optimal routes

Location Aided Routing (LAR)

- Utilizes the location information (by GPS) for improving the efficiency of routing by reducing the control overhead.
- Designates two geographical regions for selective forwarding of control packets.
- **ExpectedZone:** is the region in which the destination node is expected to be present.
- **RequestZone** is a geographical region within which the path-finding control packets are permitted to be propagated.
- This area is determined by the sender of a data transfer session.
- The control packets used for path-finding are forwarded by nodes which are present in the RequestZone and are discarded by nodes outside the zone.
- When the requested nodes are not present in the RequestZone, additional area is included for forwarding the packets.
- This is done, when the first attempt for obtaining a path to a destination using the initial RequestZone fails to yield a path within a sufficiently long waiting time.
- The nodes decide to forward or discard the control packets based on two algorithms, namely, LAR1 and LAR2.

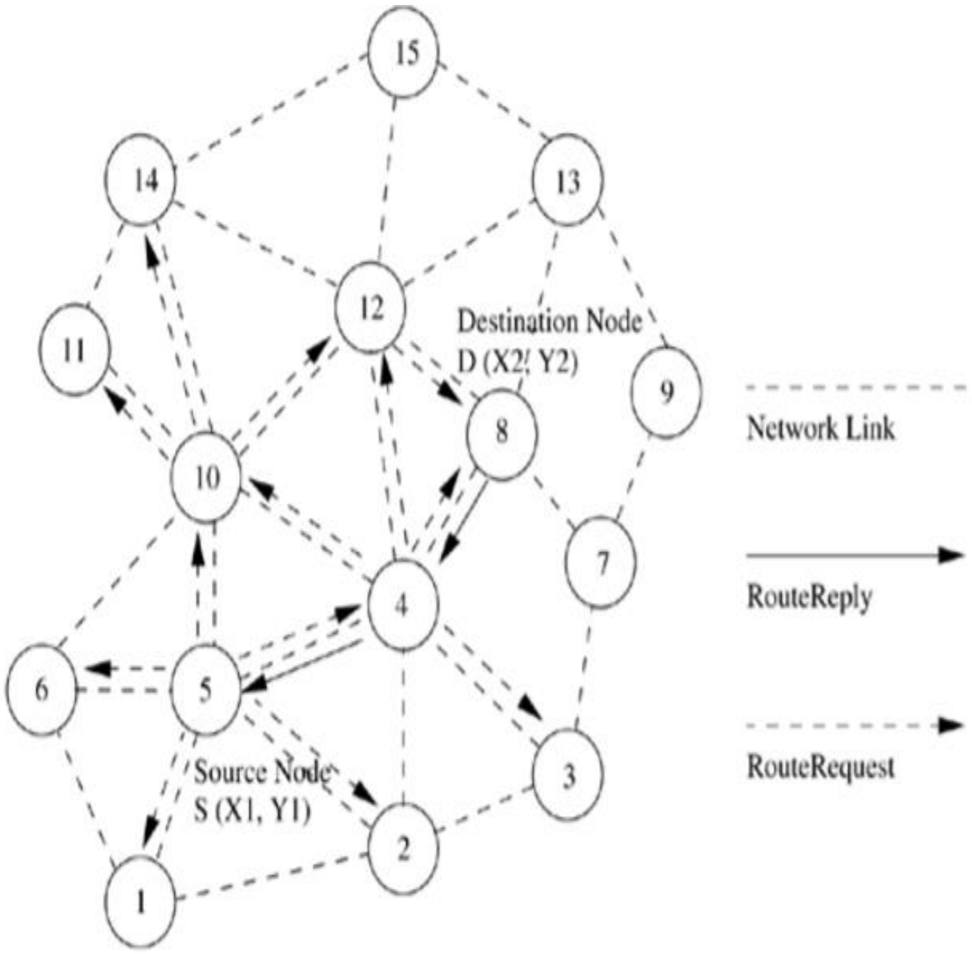
LAR1

- RequestedZone and ExpectedZone in LAR1



LAR2

- Source node S (node 5) includes the distance between itself and the destination node D along with the (X, Y) coordinates of the destination node D in theRouteRequest.
- Intermediate node computes the distance to the node D.
- If this distance is less than the distance from S to node D + δ, then the RouteRequest packet is forwarded. Otherwise, discarded
- Where δ is a parameter of the algorithm decided based on the error in location estimation and mobility

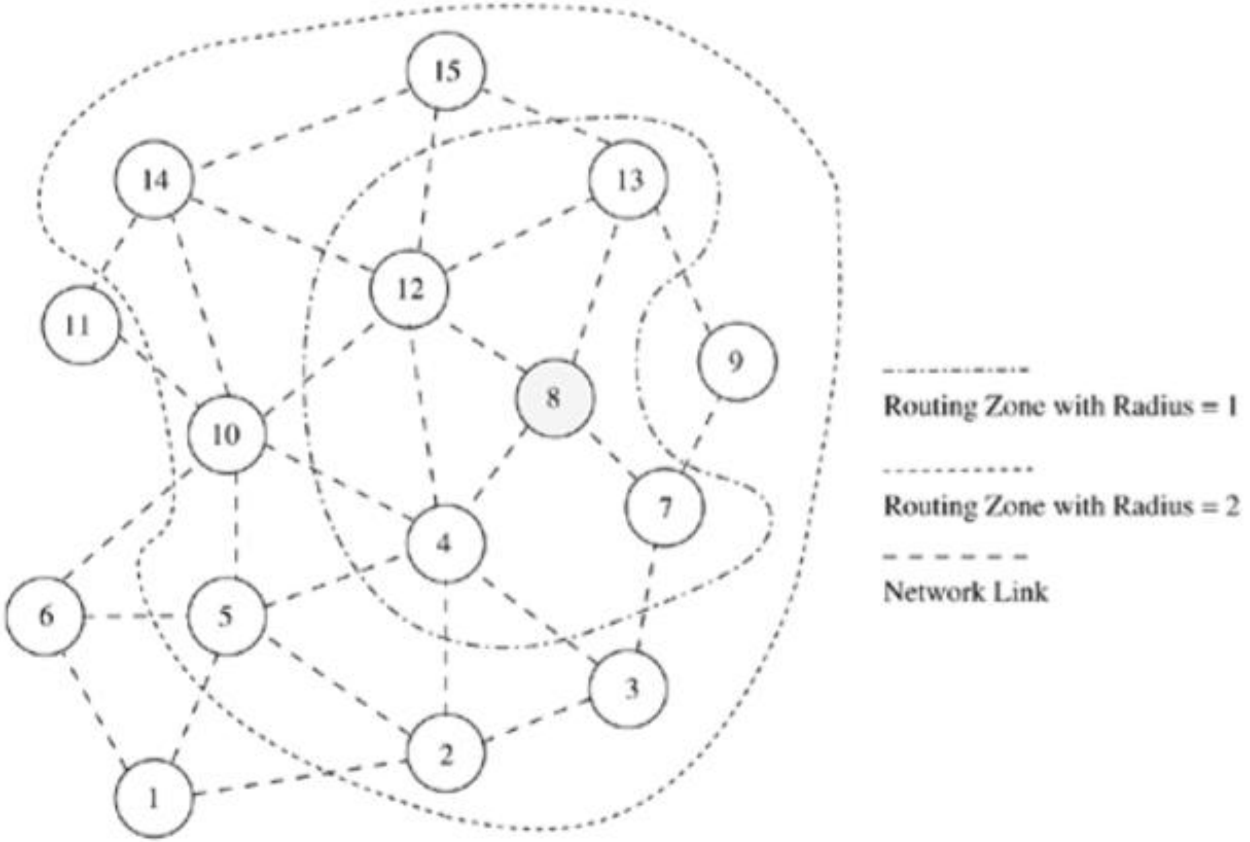


Zone Routing Protocols (ZRP)

- A hybrid routing protocol, combines the best features of both proactive and reactive routing protocols.
- Use a proactive routing scheme within a limited zone in the r-hop neighborhood of every node, and use a reactive routing scheme for nodes beyond this zone.
- An intra-zone routing protocol (IARP) is used in the zone where a particular node employs proactive routing.
- The reactive routing protocol used beyond this zone is referred to as inter-zone routing protocol (IERP)
- The routing zone of a given node is a subset of the network, within which all nodes are reachable within less than or equal to zone radius hops.

Zone Routing Protocols (ZRP)

- With zone radius = 2, the nodes 7, 4, 12, and 13 are interior nodes, whereas nodes 2, 3, 5, 9, 10, 13, and 15 are peripheral nodes



Routing Zone for Node 8

Zone Routing Protocols (ZRP)

- If source and destination are within zone of each other than packet is transferred directly using IARP, otherwise IERP finds the path.
- For Exapmle
- When a node s (node 8) has a packet for a destination node d (node 15), it checks whether node d is within its zone.
- If the destination belongs to its own zone, then it delivers the packet directly. Otherwise, node s bordercasts a RouteRequest to its peripheral nodes.
- If any peripheral node finds node d to be located within its routing zone, it sends a RouteReply back to node s indicating the path; otherwise, the node rebordercasts theRouteRequest packet to the peripheral nodes.
- This process continues until node d is located.

Zone Routing Protocols (ZRP)

- During RouteRequest propagation, every node that forwards the RouteRequest appends its address to it. This information is used for delivering theRouteReply packet back to the source.
- The path-finding process may result in multiple RouteReplypackets reaching the source, in which case the source node can choose the best path among them.
- When an intermediate node in an active path detects a broken link in the path, then broken link is bypassed by using the alternate path available.

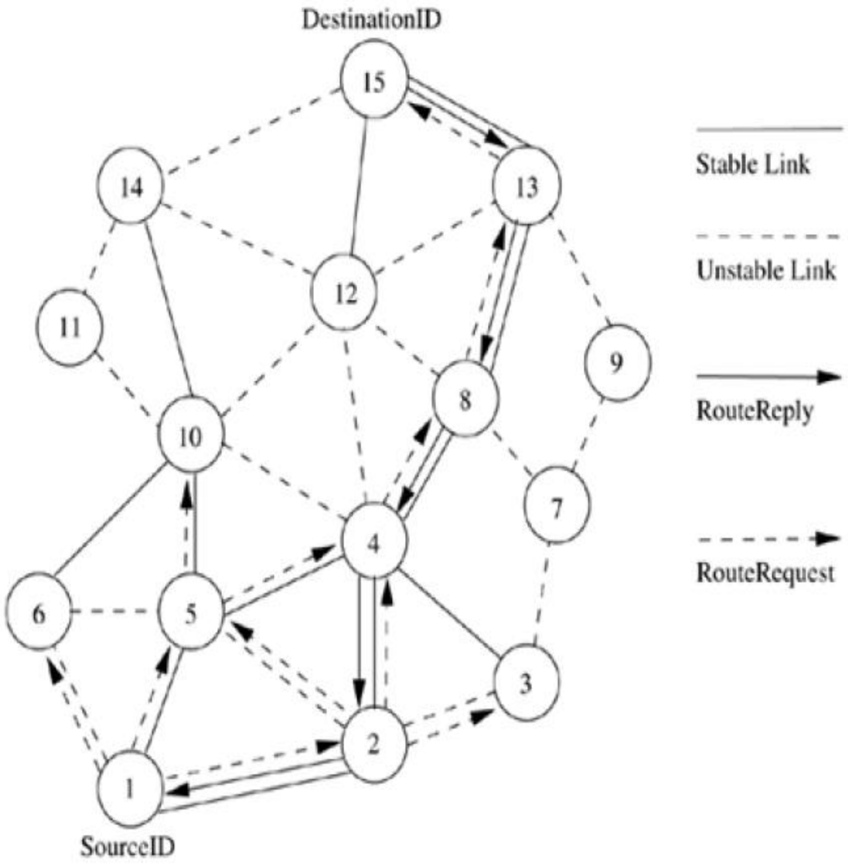
Signal Stability-Based Adaptive Routing Protocol

- *Beacon*-based, in which the signal strength of the *beacon* is measured for determining link stability as *stable* or *unstable*.
- This protocol consists of two parts: forwarding protocol (FP) and dynamic routing protocol (DRP) and use an extended radio interface that measures the signal strength from *beacon*s.
- Every node maintains a table that contains the *beacon* count and the signal strength of each of its neighbours.
- If a node has received strong *beacon*s for the past few *beacons*, the node classifies the link as a *strong*/*stable* link otherwise classified as a *weak*/*unstable* link.
- Each node maintains signal stability table (SST), is used by the nodes in the path to the destination to forward the incoming *RouteRequest* over strong links for finding the most stable end-to-end path.
- If the attempt of forwarding a *RouteRequest* over the stable links fails, the protocol floods the *RouteRequest* throughout the network without considering the stability of links.

Signal Stability-Based Adaptive Routing Protocol

- A source (node 1) which needs route to the destination floods the network with *RouteRequest*packets. The *RouteRequest is forwarded further* only if it is received over a strong link. A *RouteRequest* received through a weak link is dropped without being processed.

- The destination selects the first *RouteRequest* packet received over strong links. The destination initiates a *RouteReply* packet to notify the selected route to the source.

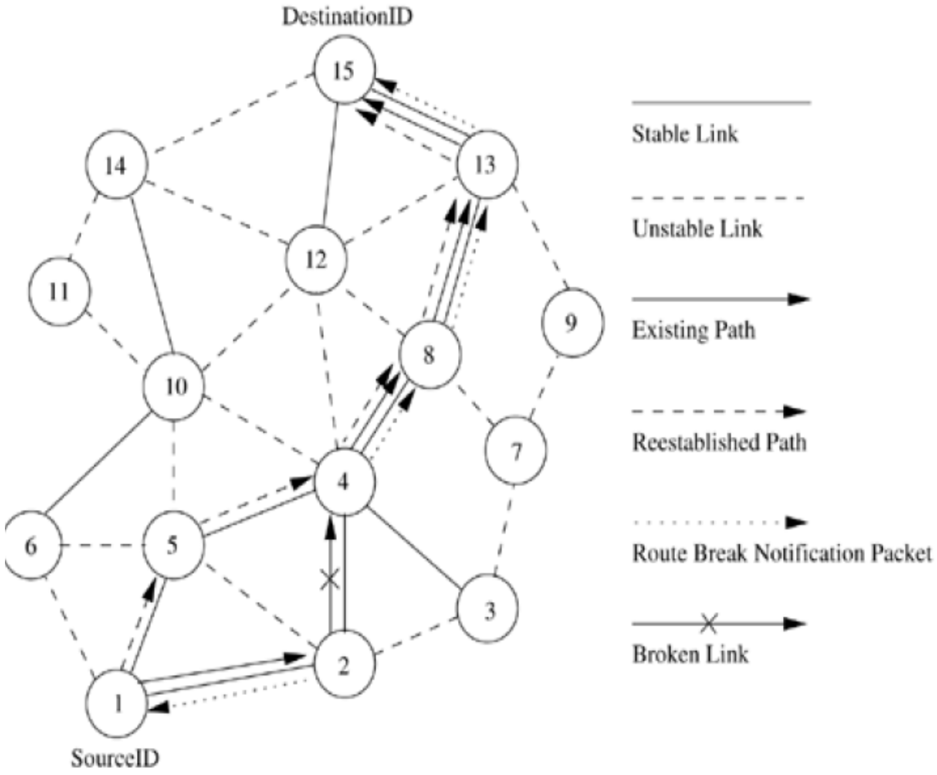


Signal Stability-Based Adaptive Routing Protocol

- On a link breaks, the end nodes of the broken link notify the corresponding end nodes (nodes 2 and 4) of the path (nodes 1 and 15). A source node, after receiving a route break notification packet, rebroadcasts the *RouteRequest* to find another stable path to the destination.

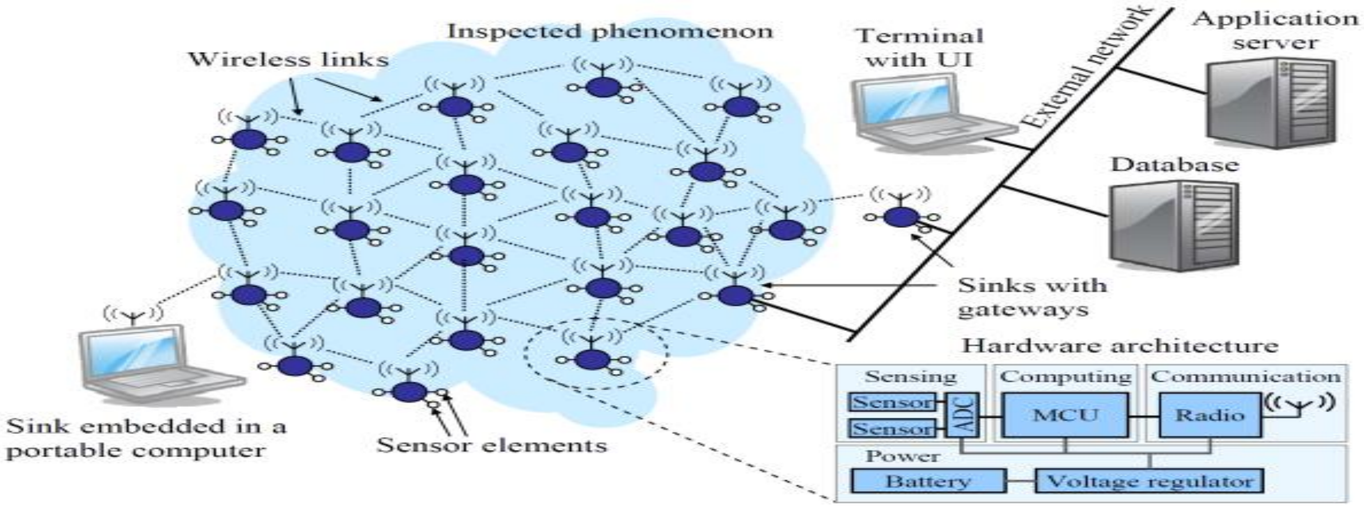
Advantages: finds more stable routes as compared to DSR and AODV

Disadvantages: However in case when it not found stable route it re-initiate *RouteRequest* again resulting more traffic and delay, sometimes the routes are longer.



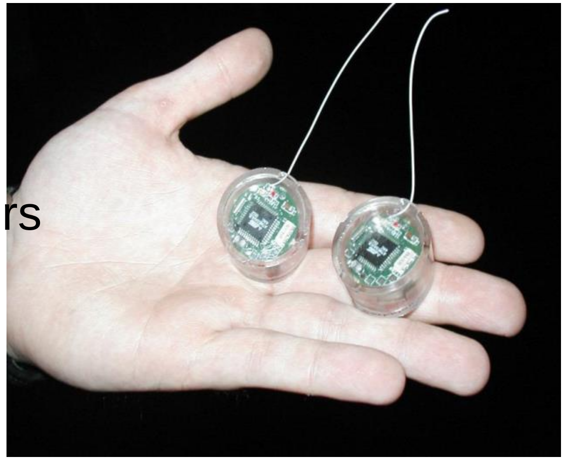
Wireless Sensor Networks (WSNs)

- A **wireless sensor network** (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors (sensor nodes), to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.

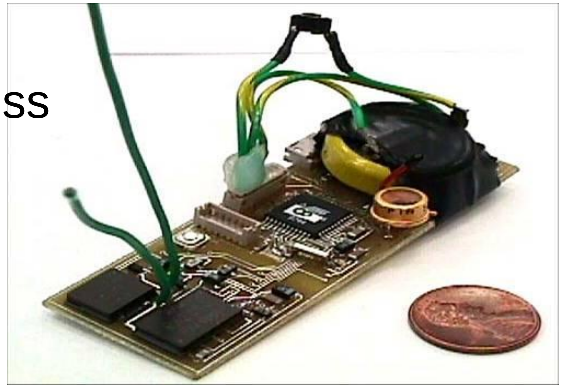


Wireless Sensor Networks (WSNs)

- A typical sensor node consist sensing, communicating, processing, memory and power unit



Sensors



Wireless Radio

Benefits:

- No need of fixed infrastructure.
- Capable of surviving harsh environments (heat, humidity, corrosion, pollution, radiation, etc)
- Implementation cost is cheap.
- A Large range of sensors are available like- Pressure, Temperature , Light , Biological , Chemical , Strain, fatigue ,Tilt , and many others.

Network Characteristics

- Dense Node Deployment.
- Battery - Powered Sensor Nodes.
- Severe Energy, Computation, and Storage Constraints.
- Self - Configurable.
- Application Specific
- Unreliable Sensor Nodes.
- Frequent Topology Change. (node failure, damage, addition, energy depletion, or channel fading)
- No Global Identification.
- Many - to - One Traffic Pattern.
- Data Redundancy.

Applications of WSNs

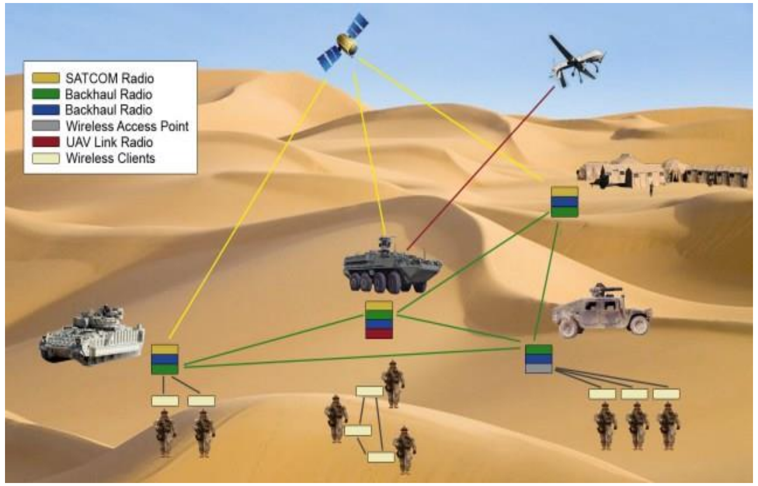
Sensors can detect or monitor a variety of physical parameters or conditions-

  - Light
  - Sound
  - Humility
  - Pressure
  - Temperature
  - Soil composition
  - Air or water quality
  - Attributes of an object such as size, weight, position, speed, and direction.

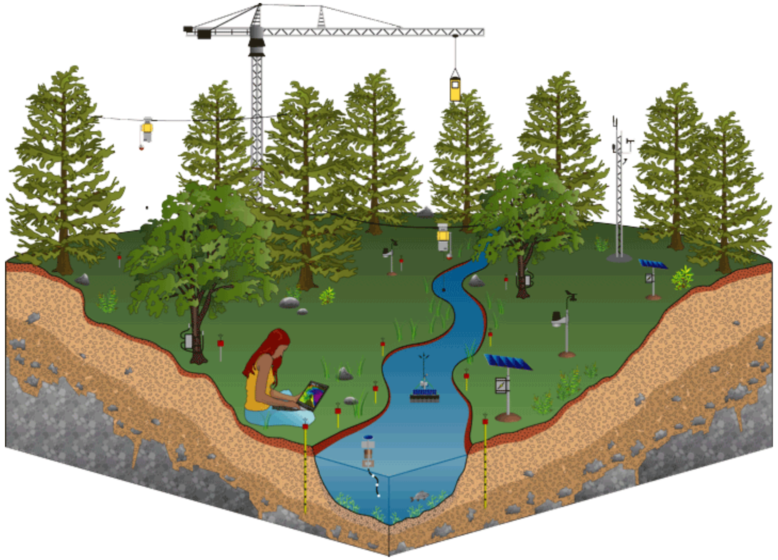
- Reduce the cost and delay in deployment.
- Deployed in any environment like, inhospitable terrains, battlefields, outer space, or deep oceans.

Applications of WSNs

- Military Applications
  - Battlefield surveillance and monitoring, guidance systems of intelligent missiles, detection of attack by weapons of mass destruction such as chemical, biological, or nuclear



- Environmental Monitoring
  - Forest fire, flood detection, habitat exploration of animals, Air and water quality monitoring, Hazard Monitoring



- Building infrastructure Monitoring
  - Airflow and temperature of different parts of the building can be automatically controlled

Applications of WSNs

- Health Monitoring
  - Monitor the patient’s heart rate or blood pressure, and sent regularly to alert the concerned doctor, provide patients a greater freedom of movement, Behavior Monitoring.

- Smart Home
  - Sensor node can built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled

- Warehouse Monitoring
  - Improve their inventory control system by installing sensors on the products to track their movement
- Industrial Process Control
  - monitor and control production processes, monitor the condition of miles of pipelines in chemical plants and refineries, monitor the condition of the machine and alert for any failure.
- Security and Surveillance
  - For example, sensors can be deployed in buildings, airports, subways, and other critical infrastructure to identify and track intruders, and provide timely alarms and protection from potential attacks.

Network Design Objectives

- Small Node Size.
- Low Node Cost.
- Low Power Consumption.
- Self -Configurability.
- Scalability
- Adaptability.
- Reliability and Fault Tolerance.
- Security.
- Channel Utilization.
- QoS Support.

Challenges of WSNs

- Limited Energy Capacity

- Limited Hardware Resources

- Massive and Random Deployment

- Diverse Applications

- Dynamic and Unreliable Environment

Sensor Node Structure

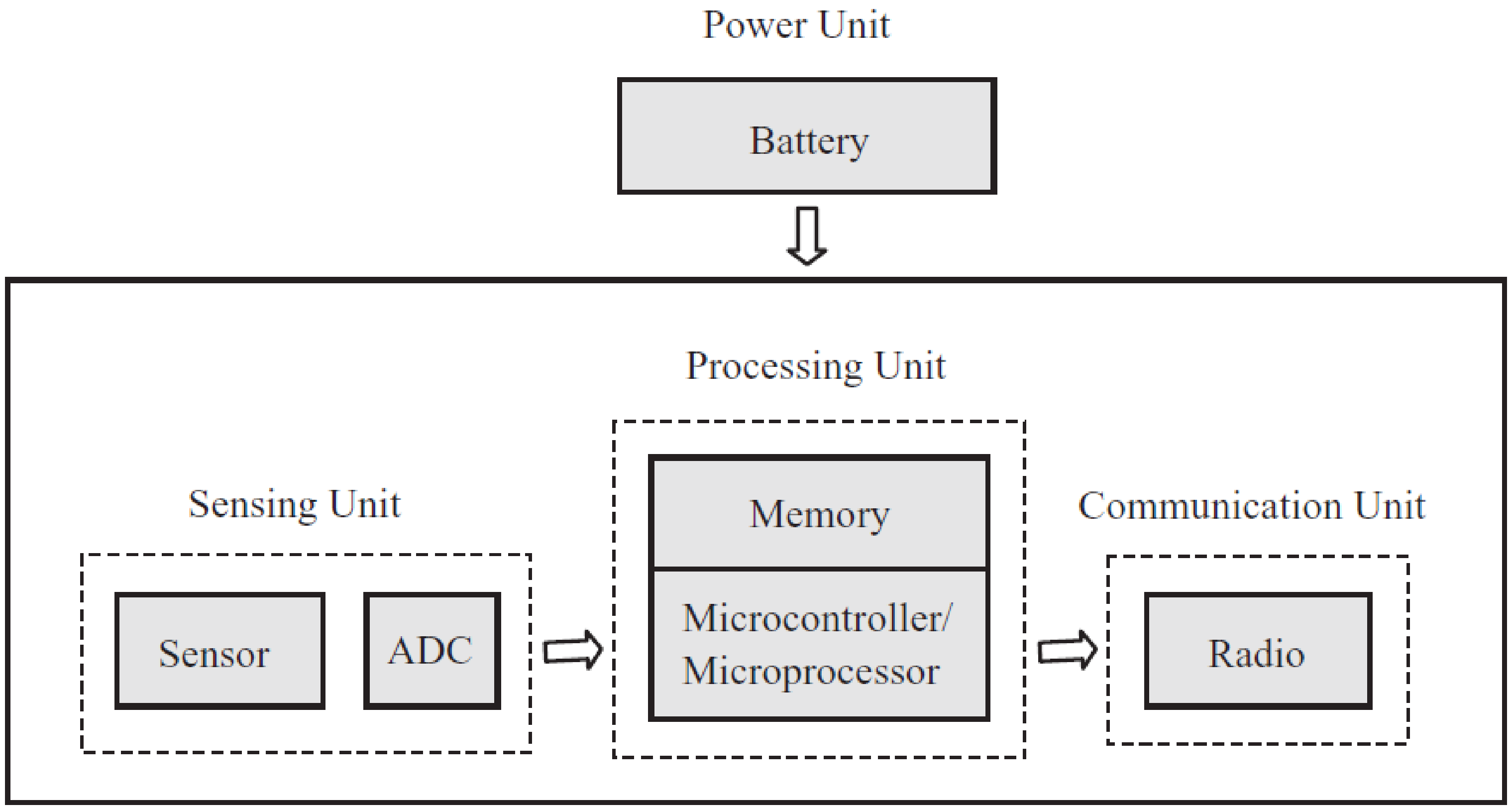


Fig. 2.1 Sensor node structure.

Network Architectures

- A sensor network typically consists of a large number of sensor nodes densely deployed in a region of interest, and one or more data sinks or base stations that are located close to or inside the sensing region.
- The sink(s) sends queries or commands to the sensor nodes in the sensing region while the sensor nodes collaborate to accomplish the sensing task and send the sensed data to the sink(s).
- Sink(s) perform task as a gateway node.

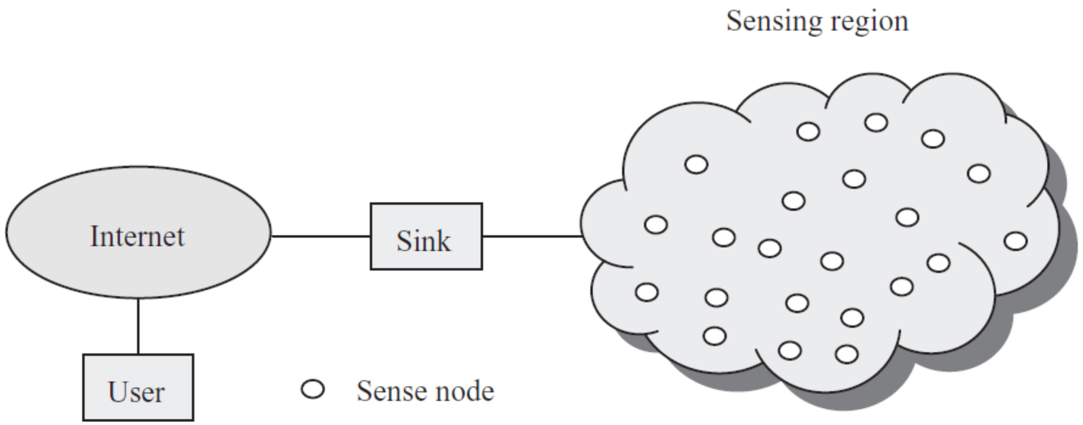


Fig. 2.2 Sensor network architecture.

Single hop Network

- Each node directly send data to sink node.
- Communication distance is high and energy is consumed exponentially with respect to distance.
- Multi-hop communication is favorable.

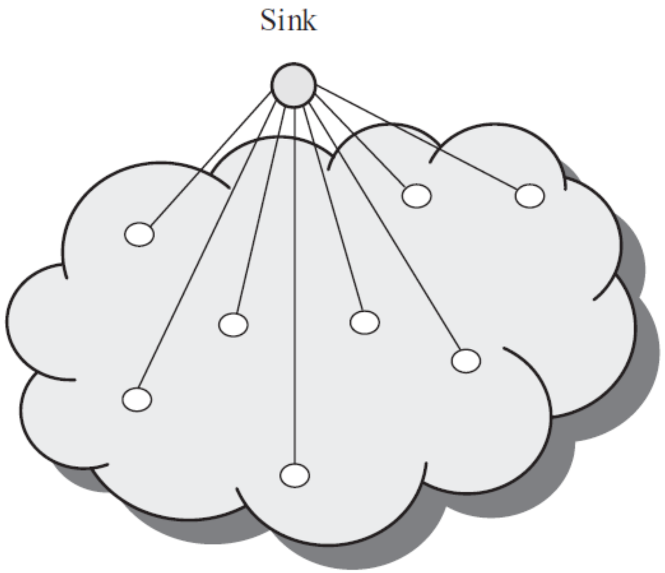


Fig. 2.3 Single-hop network architecture.

Multi-hop Networks

- In multi-hop communication, a sensor node transmits its sensed data toward the sink via one or more intermediate nodes, which can reduce the energy consumption
- The architecture of a multi-hop network can be organized into two types: **flat** and **hierarchical**

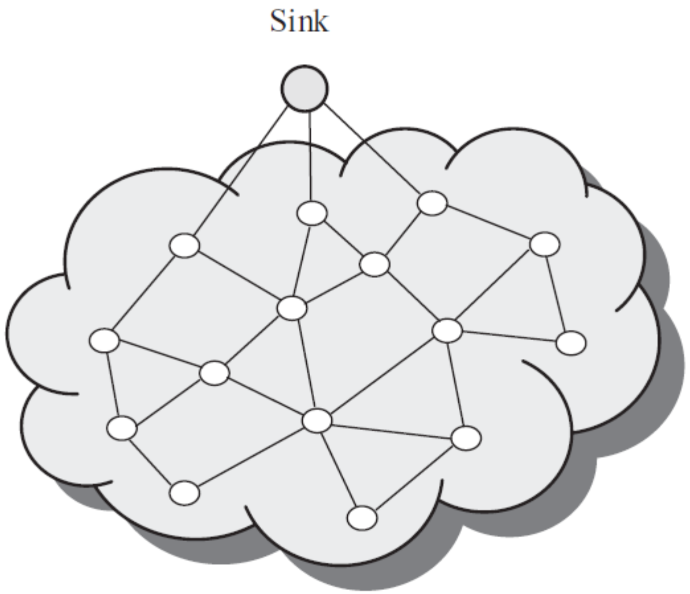


Fig. 2.4 Flat network architecture.

- In a flat network, each node plays the same role in performing a sensing task and all sensor nodes are peers.
- Data gathering is usually accomplished by using data - centric routing.
- Sink transmits a query to all nodes in via flooding and only the sensor nodes that have the data matching the query will respond to the sink.

Multi-hop Networks

- **Hierarchical Architecture-**Sensor nodes are organized into clusters, where the cluster members send their data to the cluster heads while the cluster heads serve as relays for transmitting the data to the sink.
- Better energy utilization, scalability, etc.

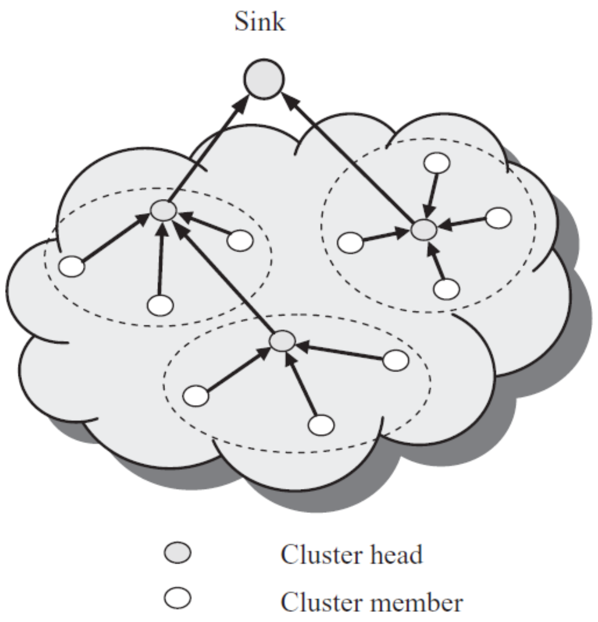


Fig. 2.5 Single-hop clustering architecture.

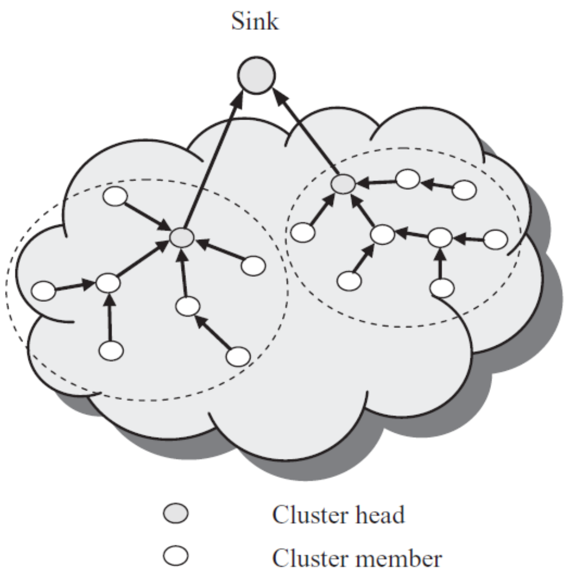


Fig. 2.6 Multihop clustering architectures.

Multi-hop Networks

- The major problem is how to select the cluster heads and how to organize the clusters.
- There are many clustering strategies.
- According to the distance between the cluster members and their cluster heads: **a single - hop** clustering architecture or a **multihop clustering** architecture.
- According to the number of tiers in the clustering hierarchy: **single - tier clustering** architecture or **a multitier clustering architecture**

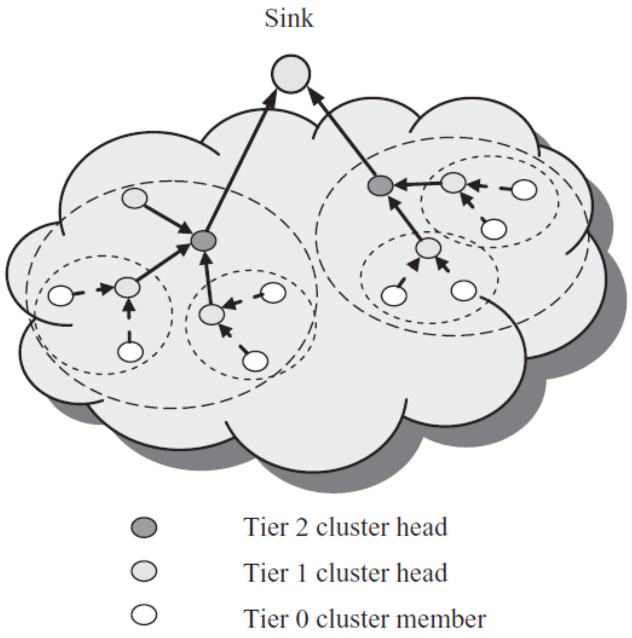


Fig. 2.7 Multitier clustering architectures.

CLASSIFICATIONS OF WIRELESS SENSOR NETWORKS

- Static and Mobile Network.
- Deterministic and Nondeterministic Network.
- Static - Sink and Mobile - Sink Network.
- Single - Sink and Multisink Network.
- Single - Hop and Multihop Network.
- Homogeneous and Heterogeneous Network.

PROTOCOL STACK FOR WIRELESS SENSOR NETWORKS

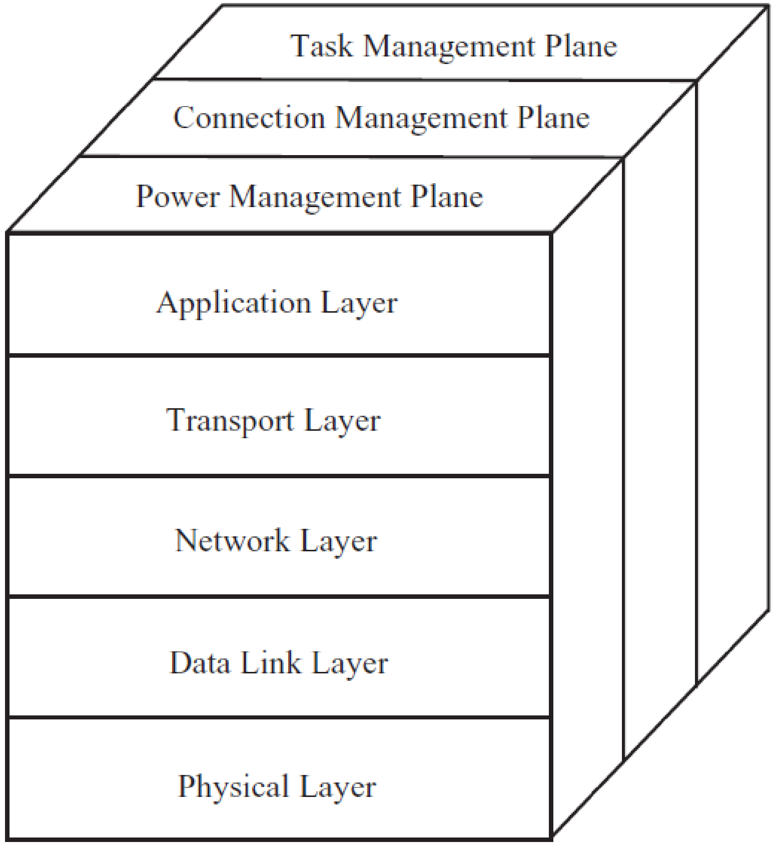


Fig. 2.8 Protocol stack for sensor networks.

Routing and Data Dissemination in WSNs

Overview

- Routing in WSNs is challenging due to distinguish from other wireless networks like mobile ad hoc networks or cellular networks.
  - First, it is not possible to build a global addressing scheme for a large number of sensor nodes. Thus, traditional IP-based protocols may not be applied to WSNs. In WSNs, sometimes getting the data is more important than knowing the IDs of which nodes sent the data.
  - Second, in contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular BS.

Overview (cont.)

- Third, sensor nodes are tightly constrained in terms of energy, processing, and storage capacities. Thus, they require carefully resource management.
- Fourth, in most application scenarios, nodes in WSNs are generally stationary after deployment except for, may be, a few mobile nodes.
- Fifth, sensor networks are application specific, i.e., design requirements of a sensor network change with application.
- Sixth, position awareness of sensor nodes is important since data collection is normally based on the location.
- Finally, data collected by many sensors in WSNs is typically based on common phenomena, hence there is a high probability that this data has some redundancy.

Overview (cont.)

- The task of finding and maintaining routes in WSNs is nontrivial since energy restrictions and sudden changes in node status (e.g., failure) cause frequent and unpredictable topological changes.
- To minimize energy consumption, routing techniques proposed for WSNs employ some well-known routing strategies, e.g., data aggregation and in-network processing, clustering, different node role assignment, and data-centric methods were employed.

Routing Challenges and Design Issues in WSNs

Overview

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

Node Deployment

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

Energy Considerations

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

Data Delivery Model

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

Node/Link Heterogeneity

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

Fault Tolerance

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

Scalability

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

Network Dynamics

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

Transmission Media

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

Connectivity

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

Coverage

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

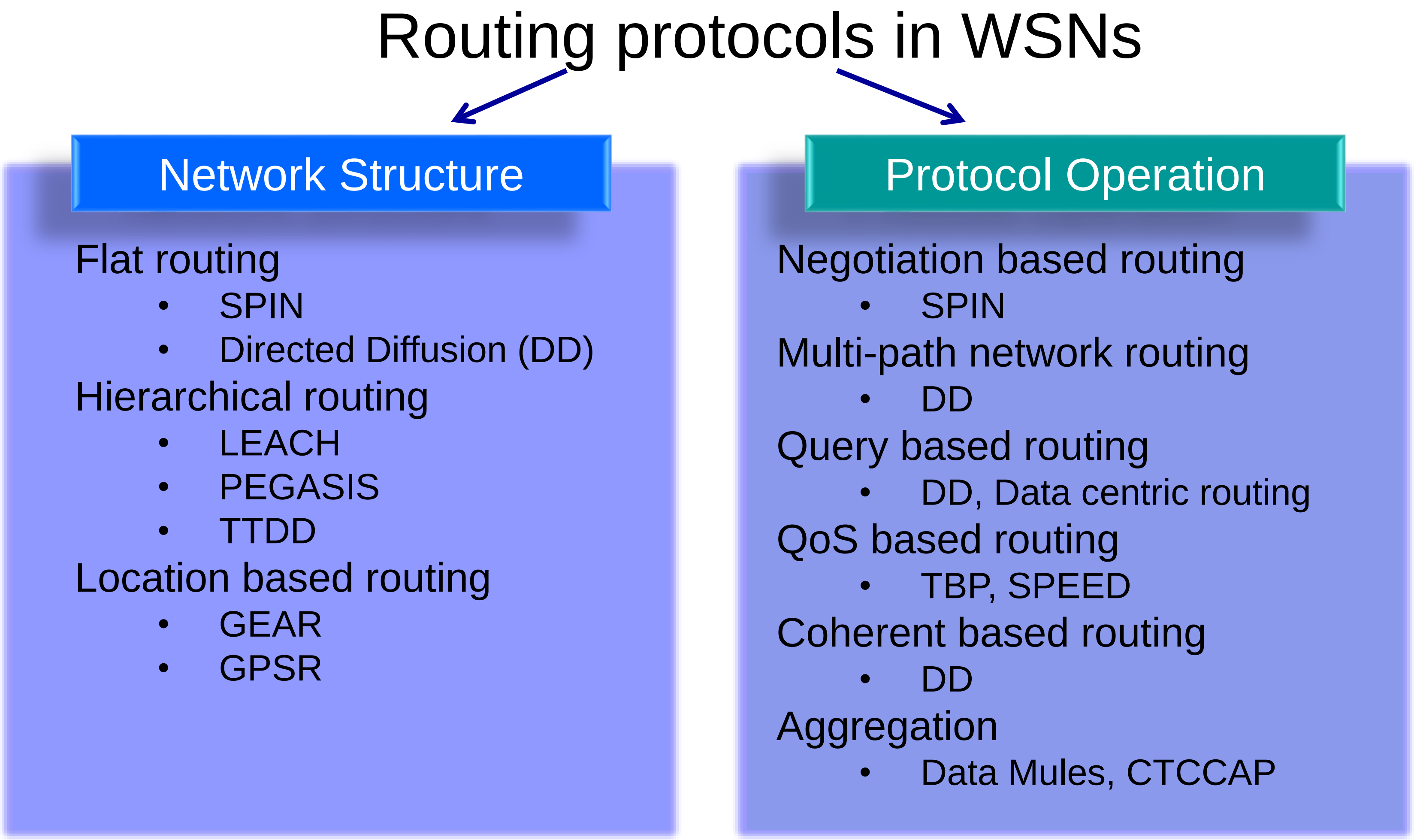
Data Aggregation

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

Quality of Service

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

Routing Protocols in WSNs: A taxonomy



Routing protocols in WSNs

Network Structure

Flat routing
- SPIN
- Directed Diffusion (DD)

Hierarchical routing
- LEACH
- PEGASIS
- TTDD

Location based routing
- GEAR
- GPSR

Protocol Operation

Negotiation based routing
- SPIN

Multi-path network routing
- DD

Query based routing
- DD, Data centric routing

QoS based routing
- TBP, SPEED

Coherent based routing
- DD

Aggregation
- Data Mules, CTCCAP

Flat Routing

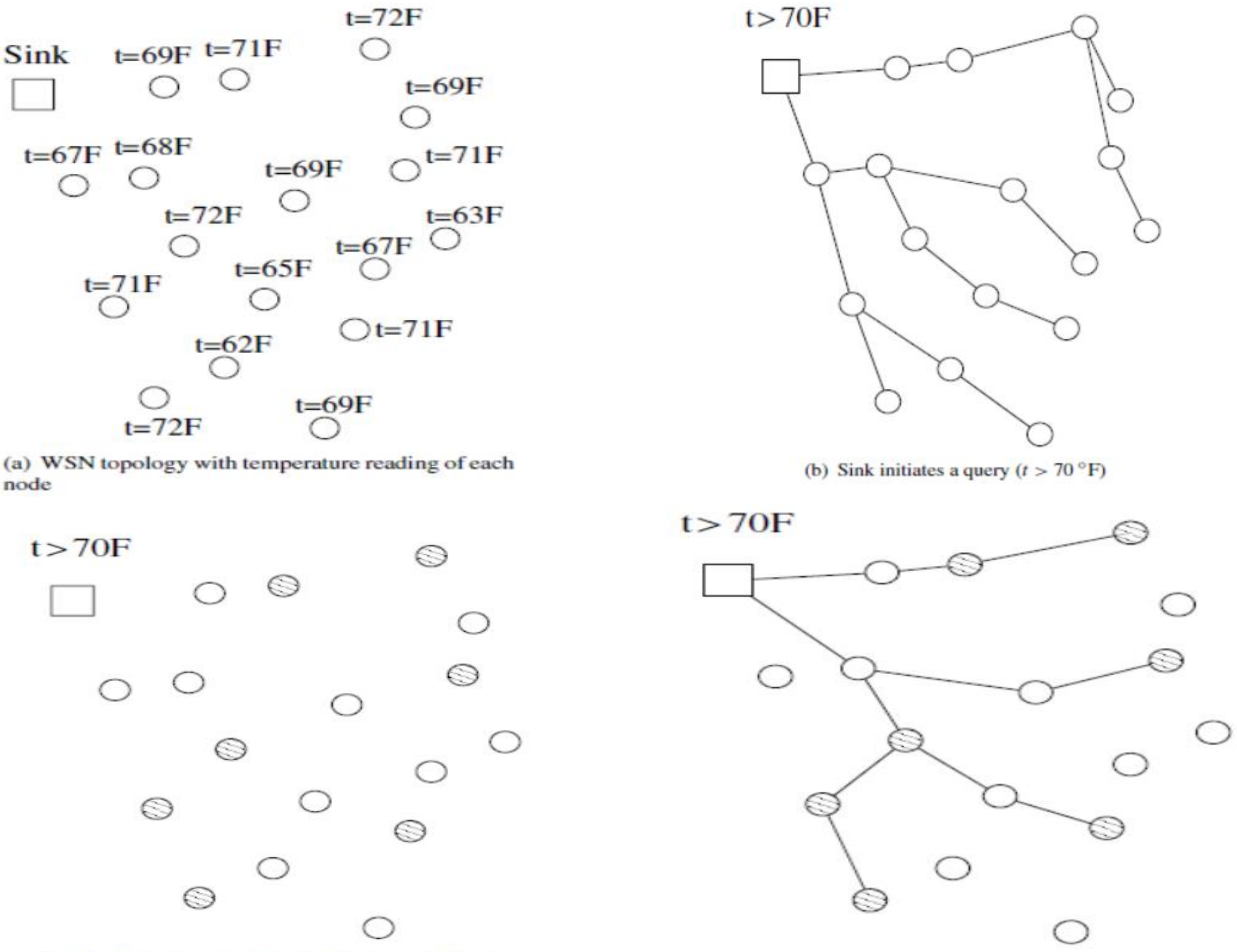
Overview

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

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

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

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



(a) WSN topology with temperature reading of each node

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

(c) Nodes with matching readings are addressed

(d) Routes are generated

Flooding

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

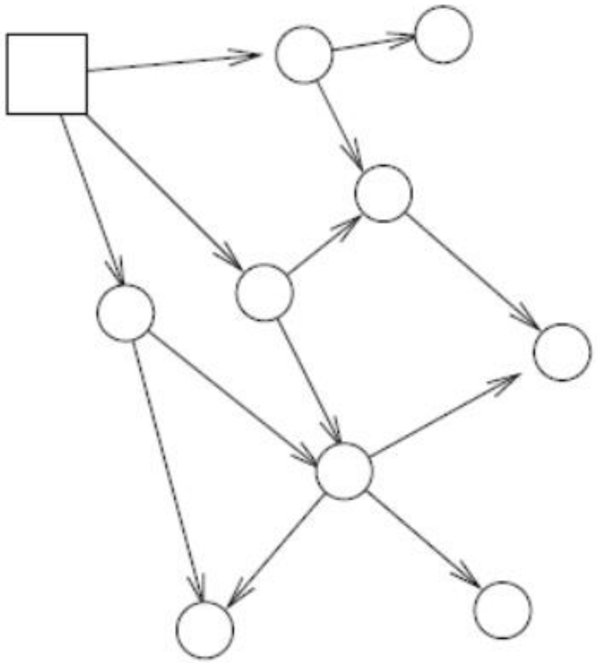
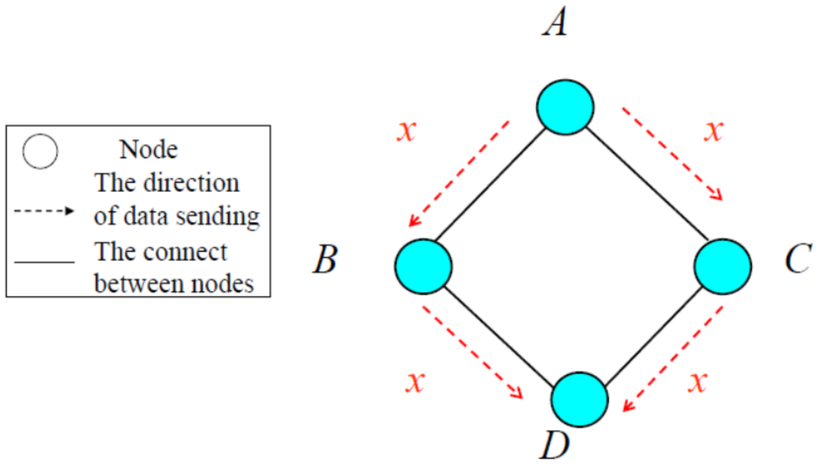


Figure 7.3 Flooding.

Flooding Drawbacks

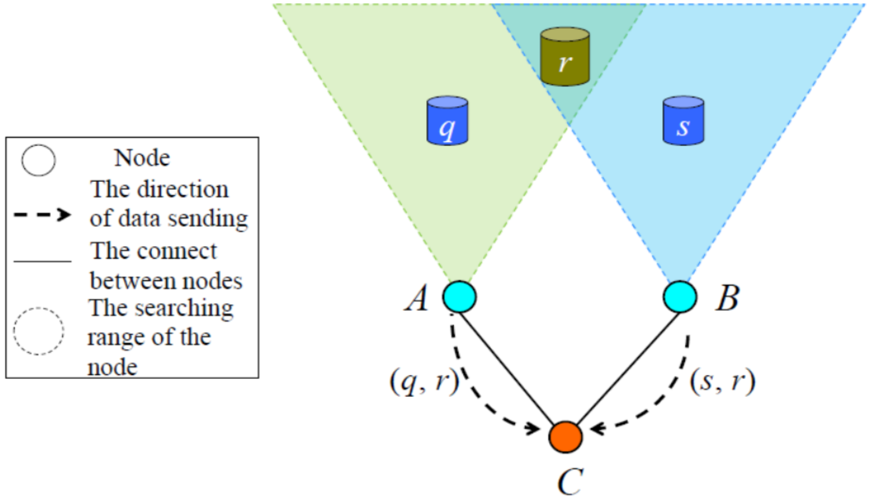
- Implosion

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



- Overlap

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


Node
The direction of data sending
The connect between nodes
The searching range of the node
r
q
s
A
B
(q, r)
(s, r)
C

- Resource Blindness: Consumes much energy and bandwidth.

Gossiping

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