Wireless Networks

Module 5
Wireless Adhoc Networks

5. Wireless Adhoc Networks

Module No.	Unit No.	Topic	Hours	Books
5		**Wireless Adhoc Networks**	**6**	
	5.1	**Wireless Adhoc Networks:** Features, advantages and Applications		**T2 Ch 8 (8.1)**
	5.2	**Mobile Adhoc Networks (MANET):** Network architecture, MAC Protocols		**T2 Ch 8 (8.2)**
	5.3	**Vehicular Adhoc Networks (VANET):** Characteristics, Protocols and Applications		**T2 Ch 8 (8.5)**

Text books and Reference Books

Text books(T):

1. Vijay K Garg, “Wireless Communication and Networking”, Morgan – Kaufmann Series in Networking, Elsevier.
2. Dr. Sunil Kumar Manvi, Mahabaleshwar S. Kakkasageri, “Wireless and Mobile Networks Concepts and Protocols”, Wiley India Pvt Ltd.
3. Raj kamal, “Internet of Things Architecture & Design Principles”, McGrawHill.

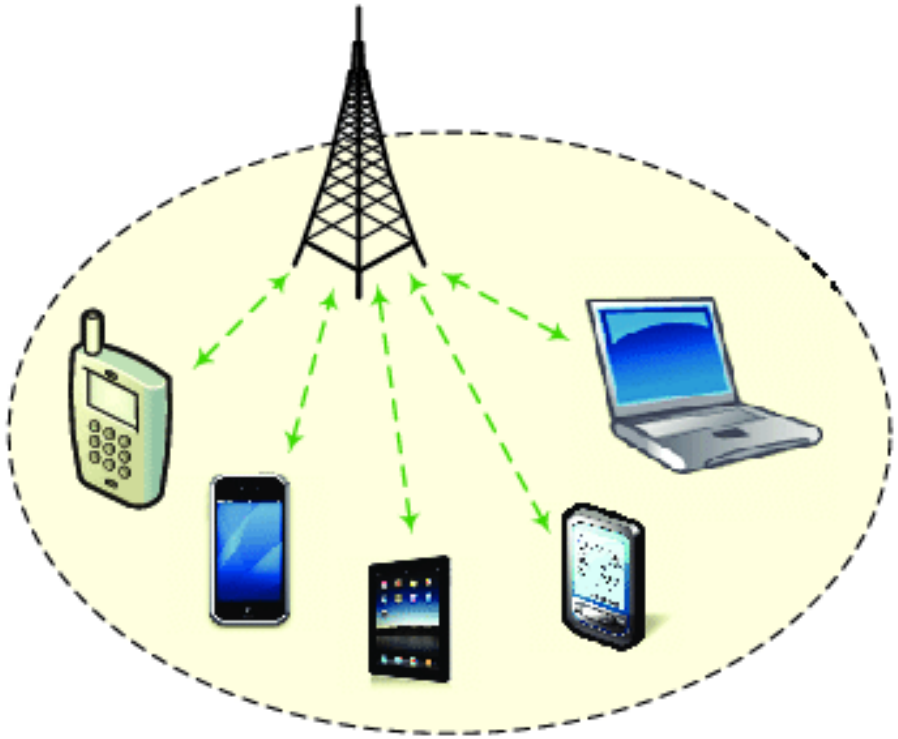
Reference Books (R):

4. Kazem Sohraby, Daniel Minoli and taieb Znati, Wireless Sensor Networks, Technology, Protocols and Applications, Wiley Student Edition.

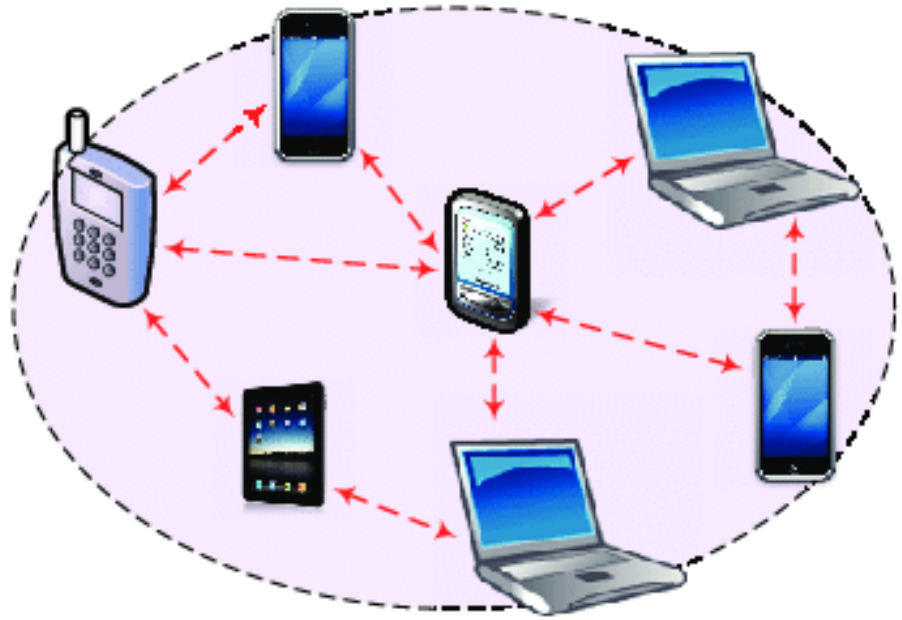
- Wireless networks can be classified in two types,

- infrastructure network and
- infrastructure less (adhoc) networks.

- Infrastructure network consists of a network with fixed and wired gateways.
- Adhoc is a Latin word, which means "for this or for this only". An ad hoc network is made up of multiple *nodes* connected by *links.*
- Adhoc networks have been proposed as a communication technology to deal with the unexpected change at a place, emergency situation such as disaster relief,



Infrastructure-based wireless networks



Wireless ad hoc networks

- Nodes can be the form of systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the networks. Links are wireless.

- An adhoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other adhoc network device in link range.

- Adhoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

- The rapid development of non-existing infrastructure makes the **adhoc network** easily to be used in emergency situation.
- In an ad hoc setup, the network is built spontaneously as and when devices communicate with each other.
- These devices should ideally be within close range of each other; however quality of connection and speed of the network will suffer as more devices are added to the network.
- These networks help to reduce administrative cost.

- *Wireless ad hoc network (WANet)* is a special structure of the wireless communication network, whose communication relies on their cooperation among the nodes and achieves it in the manner of wireless multi-hop.
- Therefore, this kind of network does not rely on any fixed infrastructure, and has the properties of self-organizing and self-managing.
- Each node in this network can function as a host and a router and the control of the network is distributed among the nodes.

- As the nodes communicate over wireless link, they have to suffer various wireless degradation effects such as noise, fading and interference. Also the wireless links typically have less bandwidth than those of a wired networks.

- The network configuration is dynamic, because the connectivity among the nodes may vary with time due to node departure, new node arrivals and mobile nature of nodes.

- Ad-hoc networks, which can be wired or wireless, are also known as P2P networks because the devices communicate directly and do not rely on servers.
- A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner.
- There are various types of wireless adhoc networks based on their applications. They are,

✓Mobile Ad hoc Networks(MANETs)
✓Wireless Sensor Networks(WSN)
✓Wireless Mesh Networks(WMN)
✓Vehicular Ad hoc Networks(VANETs)

Mobile Ad hoc Networks (MANETs): It is a self arranging infra structureless network of mobile devices communicating through wireless link.

Wireless Sensor Networks (WSN): It consists of autonomous sensors to control the environmental actions.

Wireless Mesh Networks(WMN): It is a self arranging infra structureless network of static devices communicating through wireless link.

Vehicular Ad hoc Networks (VANETs): It uses traveling cars as nodes in a network to create a mobile network.

Characteristic Features

The efficiency and effectiveness of a wireless adhoc network can be described by certain features.

These features are categorized in to **Quantitative features and Qualitative features**.

Quantitative Features: These features include,

1. **Network Scalability:** Scalability refers to the number of nodes that the ad hoc network can scale to and even then the communication is established reliably. The network should be able to scale from 10s nodes to thousands of nodes. However as the network size grows, Route acquisition, service location and encryption key exchanges will require considerable overheads.

2. Network settling time: It is the time required for a set of nodes to organize themselves automatically and to transmit first set of data reliably. This time is significant because if network is not in operation for some time, then in this time the network must start up and send messages promptly.

3. Network join time: It is the time required by a new node or group of nodes to integrate in to existing ad hoc network.

4. Network depart time: It is the time required by a network to identify the loss or failure of a node or group of nodes, and to reorganize by establishing new routes in existing ad hoc network.

5. Network recovery time: Due to node failure, traffic load and node mobility the network has to reorganize, the time required for the adhoc network to become functional again and resume reliable communication is called as network recover time. This time is extremely important as it dictates in how much time network will set up and will be in operation.

6. Frequency of updates: In order to maintain ad-hoc network operation proper, number of control packets (bytes) transmitted in a given period are termed as overheads.

7. Storage space: It is the memory required to store the data of routing table and other management tables. It is required in number of bytes.

Qualitative Features: *These features include,*

1. Location awareness: It is an important feature. Routing algorithms may need the position of node either local or global depending upon the size of the network.

2. Effect to topological changes: Routing algorithm may need node failure or movement of nodes information at a time or complete restructuring of the network.

3. Adaptation of wireless channel: Routing decision by nodes should be based on fading, shadowing or multi-user interference effects on the link.

4. **Power consumption:** The routing algorithm should consider the residual energy of each node while deciding a particular path for routing.

5. **Usage of Control channel:** The routing algorithm should check that the routing decision is to forwarded to all nodes via separate channel or in the data channel itself. The multichannel transmission may make the network vulnerable in certain applications.

6. **Type of link:** It is to be checked that the routing algorithm works better on which link unidirectional or bidirectional. Because sometimes due to node failure the bidirectional link may become unidirectional.

7. **Network security:** The routing algorithm should maintain the secrecy of data while transmission via different nodes. It should have low probability of detection, low probability of intercept and security at each node.

8. **Quality of Service (QoS):** Routing algorithm must support priority messaging, less delay for real time delay sensitive data.

9. **Real time voice and video services:** Apart from, regular traffic and routine services on the network, the nodes should be able to support multicast voice, receive or transmit video on demand simultaneously.

Advantages of WAN

1. **Easy configuration:** As adhoc networks do not require any infrastructure like base station, access point, cables etc.. Therefore these networks are easy to configure in the fastest way as and when required.

2. **Resilient:** Infrastructure less nature of network makes it resilient, there is no single point of failure. The network still works even if there is individual node failure.

3. **Efficient communication:** These networks offer an effective way to communicate with devices nearby when time is of the essence and running cable is not feasible. Nodes can make better use of the channel.

Advantages contd

4. **Useful for fast connection of small number of devices:** An ad hoc network linking a small number of devices might be better than a regular network with more users connected.

5. **Low deployment cost:** Adhoc networks do not require back bone infrastructures, access points, base stations etc.. These networks provide a low-cost way of direct client-to-client communication.

6. **Scalability:** The adhoc networks are scalable, new nodes/devices can be added at any time. However more number of devices can affect the quality of connection and speed of the network.

Disadvantages

1. It is to be noted that some Wi-Fi enabled technology, including Android devices, wireless printers and Google's Chromecast, do not support adhoc mode. They only connect to networks in infrastructure mode.

2. Lack of security: Security is a major concern in the adhoc networking standards. Adhoc wireless networking includes the lack of security. The adhoc network does not depend on any pre-existing infrastructure so that the node can leave and join the network in such a situation security may fall down. If an attacker comes within range of adhoc network, he or she won't have any trouble in connecting to the network.

Attacks in WAN

Passive attack: In this attack the transmitted data is not changed in the network. But, it can allow unauthorized user to discover the message.

Active attack: It is a severe attack and prevents the message flow between the node in the network.

- It may allow the unauthorized user to modify the message.
- The malicious node can be identified by dropped packet, battery drained, bandwidth consumption, unreliable packets, delay, connection break and false routing.

Applications of WAN

1. Military arena: In military the robustnesss and speed of deployment is critical. An adhoc network will allow the military battleground to maintain a network among the soldiers, vehicles and headquarters for search and rescue operations.

2. Provincial level: Adhoc networks can build instant link between multimedia network using notebook computers or palmtop computers to spread and share information among participants (e.g. Conferences).

3. Personal area network: A personal area network is a short range, localized network where nodes are usually associated with a given range like in a museum to obtain the information of monument.

4. Industry sector: Adhoc network is widely used for commercial applications.

5. Emergency situations: Adhoc network can also be used in emergency situation such as disaster relief. The rapid development of non-existing infrastructure makes the adhoc network easily to be used in emergency situation.

6. Campus networks: These networks can be formed in ad hoc fashion to share educational information among students and staff

7. Networks in historical buildings: Ad hoc network can configured in the buildings where wiring is not possible.

8. Vehicular communication: Each vehicle is equipped with a communication device known as node can be configured in ad hoc fashion to provide traffic information, road sign alarms and collision warning etc. in advance.

	Adhoc Networks	Cellular Networks
Infrastructure	No fixed infrastructure requirement, very rapid deployment	Fixed, Predfined cell sites and Base stations requirements
Topology	Highly dynamic topology with multihop	Static backbone network topology
Connectivity	Sporadic connectivity	Very stable connections
Network formation	Automatic formation of network according to requirement and changes	Detailed planning of installation of cell sites and base station

Mobile Adhoc Networks(MANETS)

MANET: Introduction

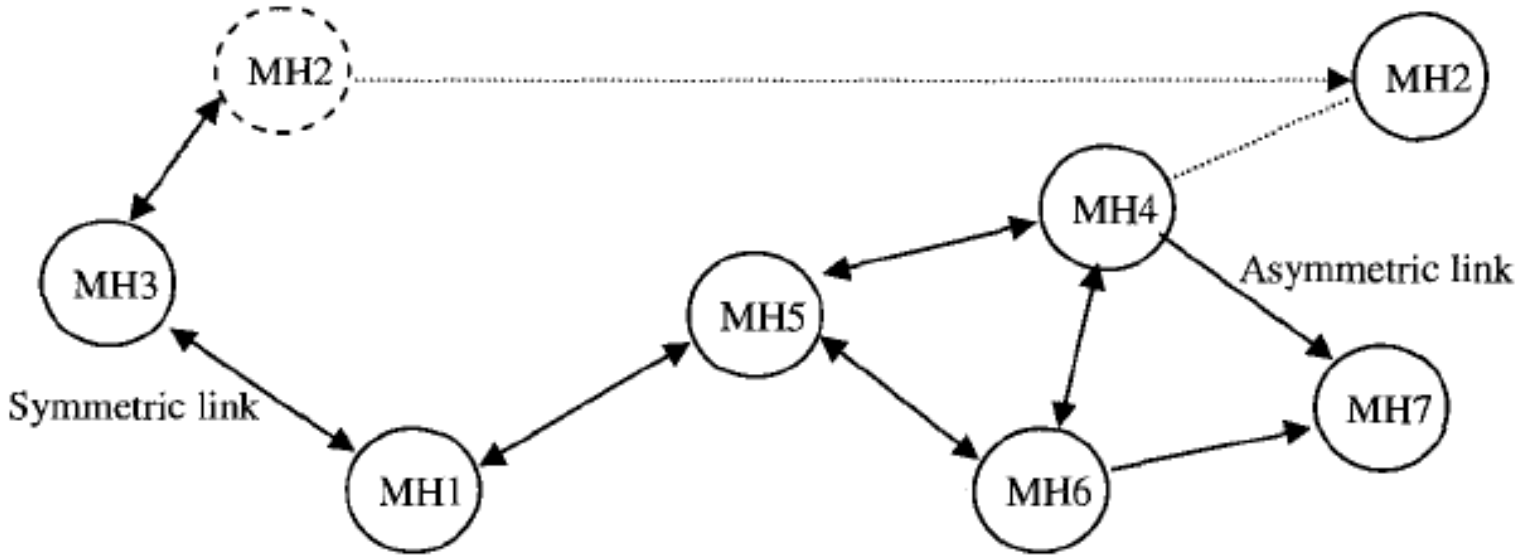
- MANET is called as Mobile Ad-hoc network.
- It is a collection of mobile node/ host, establishes a short-lived network dynamically when fixed infrastructure is absent.
- Each mobile node is equipped with a wireless transmitter and a receiver with an appropriate antenna.
- All the mobile nodes are connected by wireless links either symmetric or asymmetric that act as routers to all other mobile nodes.
- The symmetric links are bidirectional while asymmetric links are unidirectional.

Introduction contd

- Nodes in MANETs are free to move and can be organized in an arbitrary manner.
- It is a self configuring network of mobile nodes whose topology changes rapidly and unpredictably over time.
- These features make MANETs very practical and easy to deploy in places where existing infrastructure is not capable enough to allow communication, for instance, in disaster zones, wars or infeasible to deploy locations.

Easy collaboration, fast set up and efficient communication on the fly without need of costly infrastructure, self organizing and adaptive nature are the main features of MANET.

A MANET: MH: Mobile hosts



MANET Architecture

- An ad-hoc mobile wireless network is a network without any base stations, that is, an *infrastructure less network*.

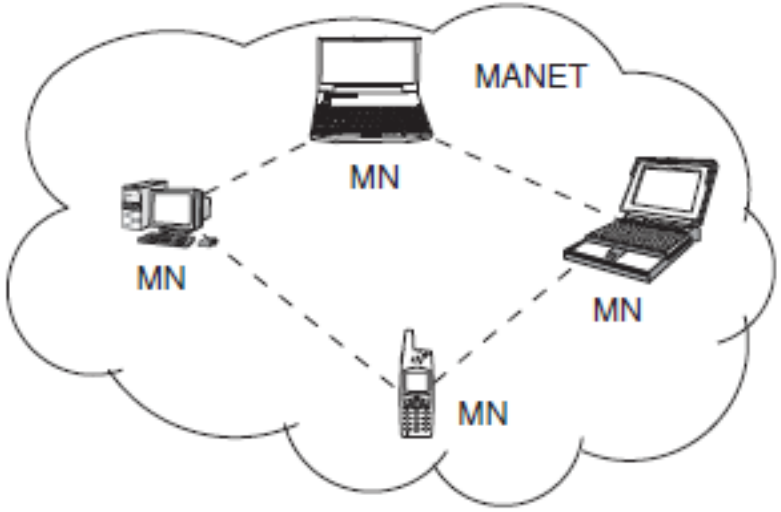
- It is an *autonomous system* of mobile nodes, mobile terminals, or Mobile Stations (for example, laptop, mobile phones, desktop machine with wireless facility) serving as routers interconnected by wireless links.

- As the nodes move or adjust their transmission and reception parameters, MANET topology may change from time to time, so it is very much *dynamic* in nature.

- The network is *decentralized*, where network organization and message delivery is executed by the nodes themselves.
- Network communications and management tasks are typically performed in a distributed manner.
- A wireless connectivity among all mobile nodes of MANET depends on,
  - locations,
  - antenna coverage patterns,
  - transmit power levels, and
  - co-channel interference levels.

- The connectivity is either in the form of *single hop or random multi-hop* transmissions.
- Based on this the architecture of MANET is classified as, Single hop architecture and Multi- hop architecture.

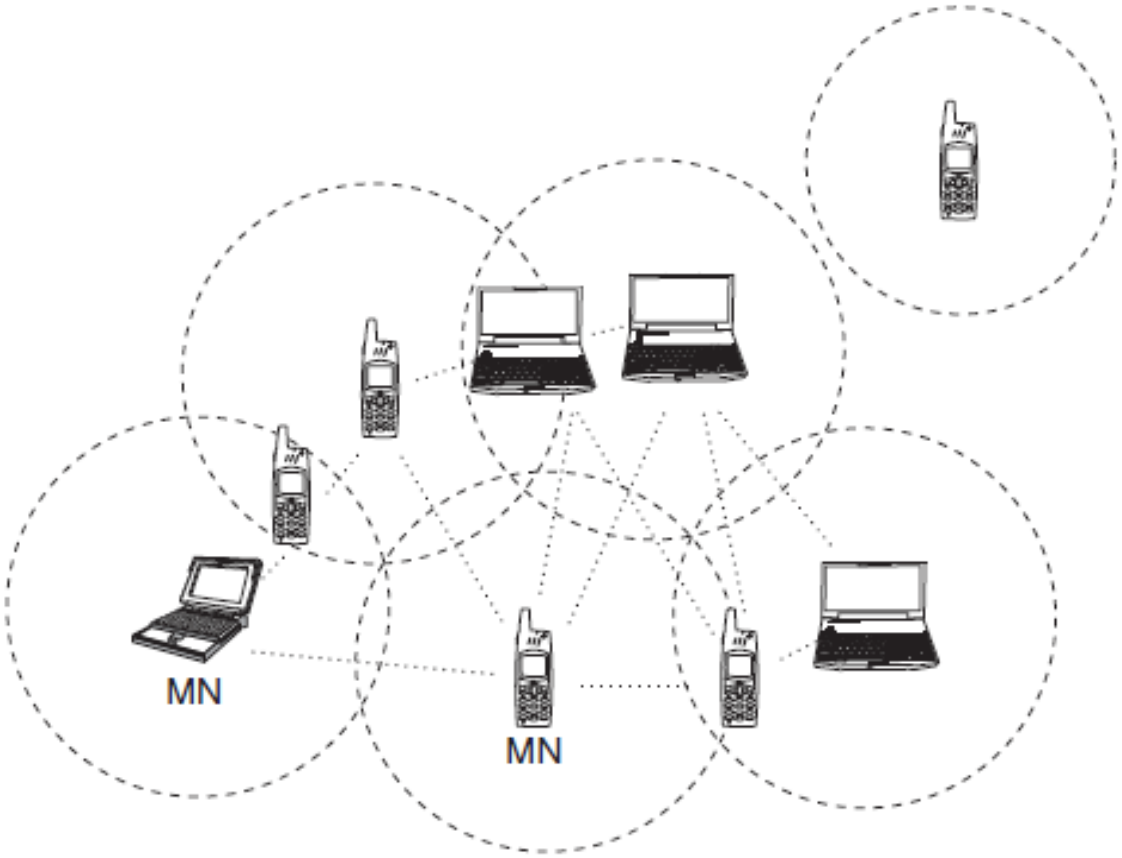
Single Hop Architecture: In this architecture, all the mobile nodes are in one coverage area. Here communication is directlv from one node to another node directly.



MANET single-hop architecture. MN: mobile node; −−: wireless link.

Multihop architecture

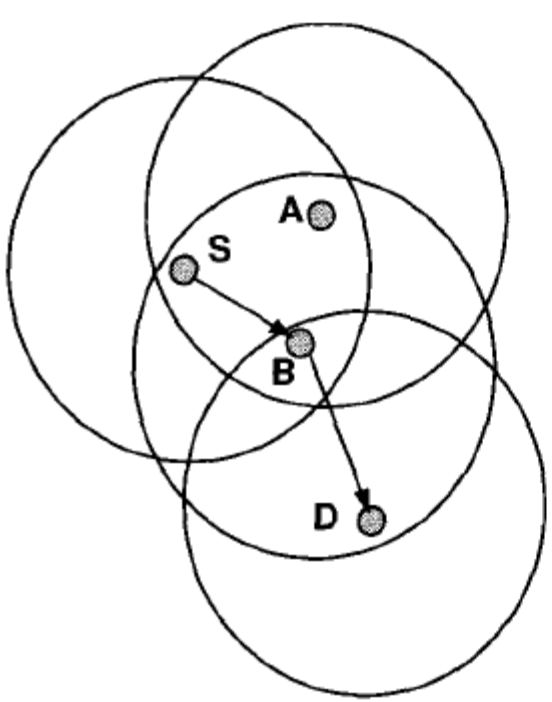
- In this architecture, one node connects to final destination via intermediate nodes. Therefore in this multiple hop communication data is transmitted in a store and forward method, where each node acts as router.
- The network may either operate as standalone or as an extension of an infrastructure network with the help of few selected routers.
- There are many coverage areas intersecting with each other, there may be some nodes which may be isolated, may not be present in any of the coverage areas of the network.



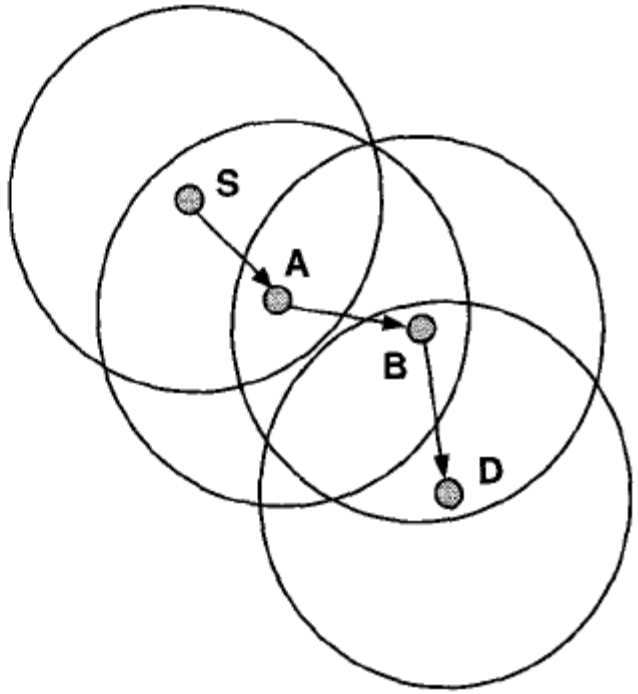
MANET Multihop Architecture.

- - -: coverage area;
.....: wireless link;
MN: Mobile Node.

- Each node is having constraint resources like memory, bandwidth, energy and processing power.
- And above all the wireless nature of channel put a fundamental limit on performance of each node.



(a) MH S uses B to communicate with MH D



(b) Due to movement of MHs, S now uses A and B to reach D

- As the mobile devices form a MANET without a network infrastructure, network can change constantly.
  - ✓ First, the devices can freely move in the network.
  - ✓ Second, the devices can leave and join the network at any time.
  - ✓ Finally, the network disappears when the last devices leave the network.
- The communication takes place within a group of two or more people.
- The communication group may be formed for one communication session only or for many communication sessions.
- The communication group may remain unchanged during the communication, or it may change constantly.

Functions of a Node

Routing: As a router a node receives packets from the neighboring nodes and forwards to other neighbors, so that packet reaches to the destination. Based on transmission range, it discovers the neighboring node and uses them as router for forwarding the data.

Host: A node acts as a host when it executes some network or host based application programs.

Access control: Each node is responsible for resolving the conflicts among different nodes for wireless channel access. A suitable Medium Access Control protocol (MAC) runs on each node to control the channel access.

- **Node authentication:** MANETs are infrastructure-less networks without any kind of central administration for the management of network. Due to this reason MANETs are comparatively more vulnerable to security threats than conventional wired or wireless networks.
- The network nodes in MANETs are susceptible a number of attacks due to the inherent nature and depicted properties of MANETs. Thus to prevent attacks it becomes very much mandatory to identify and authenticate each and every node during route discovery phase so that data can be communicated safely later on.

- These functions are performed by each node in cooperation with other.

MANET MAC Protocols

- MANET is a decentralized network; it has different characteristics than those of wired and wireless networks.
- In MANET, wireless nodes are mobile and the network topology can change frequently without any predictable pattern. The popular existing MAC and routing protocols cannot work in such a dynamic, ever changing topology based networks, problems such as “hidden terminal problem” and “exposed terminal problem.”
- MAC layer is responsible for resolving the conflicts among different nodes for channel access. A trustworthy and competent MAC protocol is needed to avoid transmission collision in MANET.

MAC schemes for MANETs

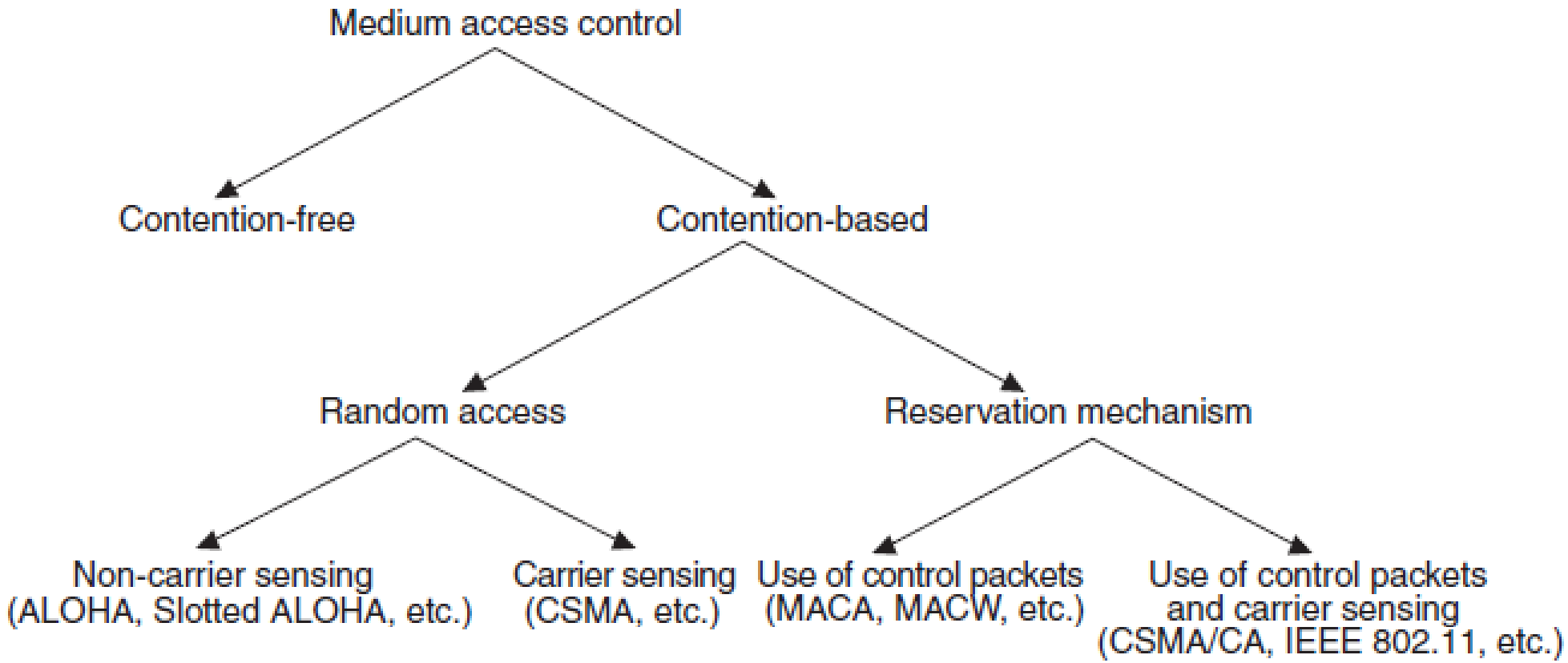


Figure 8.3 | Classification of MAC schemes.

Contention Free MAC Protocols:

A protocol is said to be contention free, if it does not allow any collisions.

Contention Based Protocols:

A MAC protocol is contention based if it detects or avoids the packet collisions.

They are further divided into categories;

- Random access and
- Reservation based.

Random Access:

- In this contention based protocol, node tries to access the channel in an uncoordinated way by sensing the carrier on the channel or without sensing.
- These methods are known *as non-carrier sensing* and *carrier sensing multiple Access.*

Non-carrier sensing: *Non-carrier-sensing protocols does not "listen" to the channel before transmitting.* The ALOHA, Slotted Aloha are the examples of non-carrier sensing protocols

Carrier sensing: *Carrier-sensing protocols "listen" to the channel before transmitting.* CSMA is the example of carrier sensing scheme.

Reservation based:

- As the name suggests, in these protocols, a communication channel is reserved either before transmission or after collisions.
- It can be implemented by using only control packets to detect collisions or combination of control packet and carrier sensing.
- Based on this, two protocols are defined; they are as follows,

✓ ***Use of control packets***:

✓ ***Use of control packets and carrier sensing***:

Use of control packets: Protocols under this category use only control packets to avoid or detect collisions.
Multiple Access Collision Avoidance (MACA) and *Multiple Access with Collision Avoidance for wireless* (MACAW) protocols are the examples of this category.

Use of control packets and carrier sensing:
These protocols use both control packets and carrier sensing mechanism to avoid or detect the collision.
Carrier Sense Multiple Access/ Collision Avoidance(CSMA/CD) and IEEE802.11 etc. are examples of this category.

1) Multiple Access Collision Avoidance (MACA)

- Hidden node and exposed node problems are unsolved in CSMA. MACA protocol is proposed to solve the problems of hidden and exposed node problems in Carrier Sense Multiple Access (CSMA) protocol.

- It uses two additional signaling or control packets, *Request To Send (RTS)* and *Clear To Send (CTS),* to reduce the collision at receiver.

- These packets are shorter than data packets, however, they contain the length of the data frame that will follow.

- The key idea of MACA protocol is that any neighboring node overhears an RTS packet; it defers its own transmission until its associated CTS packet would have finished and the node overhearing a CTS packet would also defer its transmission for the length of the expected data transmission.

- When node B wants to send a packet to node C, node B first sends an RTS to node C.
- All nodes within a single hop of the sending node hear the RTS and defer their transmissions.
- On receiving RTS, node C responds by sending CTS, provided node C is able to receive the packet.
- When another neighboring node of node C overhears a CTS, it keeps quiet for the duration of the transfer.

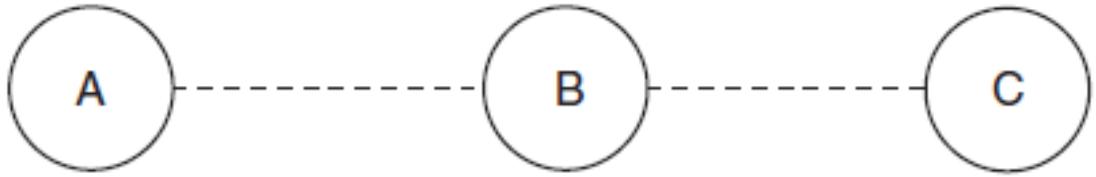
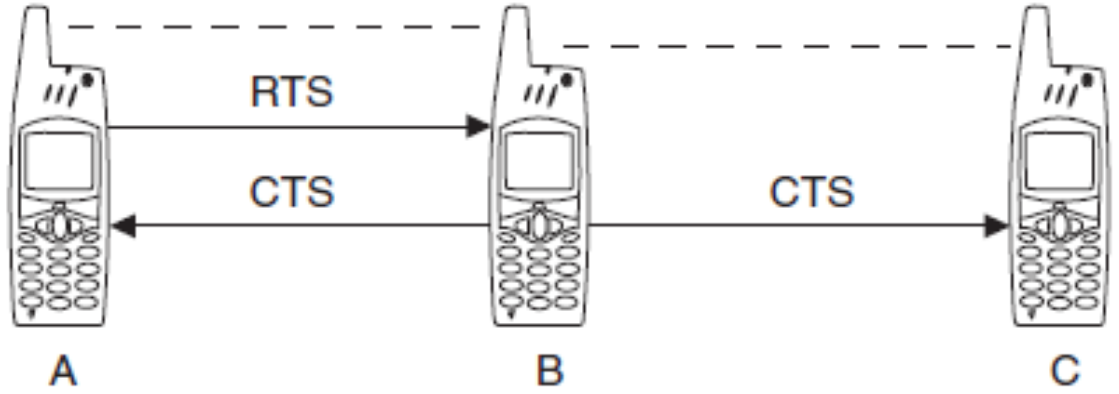


Figure 8.4 | Example topology of MACA.

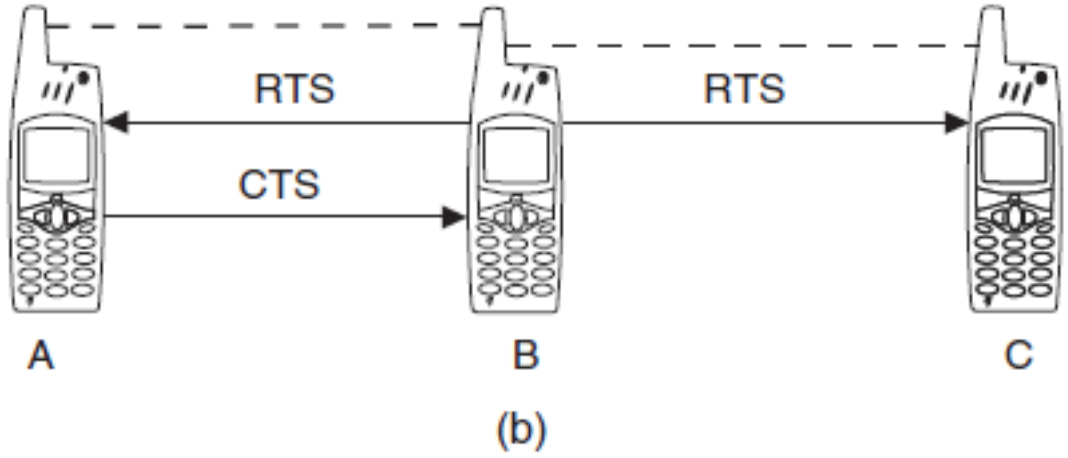
MACA handles the hidden node problem as follows:

1. A wishes to send the data to B. Hence, it sends RTS to B.
2. B replies with CTS to A. This CTS is overheard by C and it keeps silent.
3. Now A transfers the data to B.
In this fashion, the hidden node problem (here B is the hidden node) is solved.



MACA handles exposed node problem as follows:

1. B wishes to send the data to A. Hence, it sends RTS to A, which is overheard by C.
2. After hearing RTS from A, C waits for fixed time to send its packets to other neighbors.
3. B receives CTS from A, and B transmits data packets to A.
4. After fixed waiting time, C transmits RTS to its neighbors.

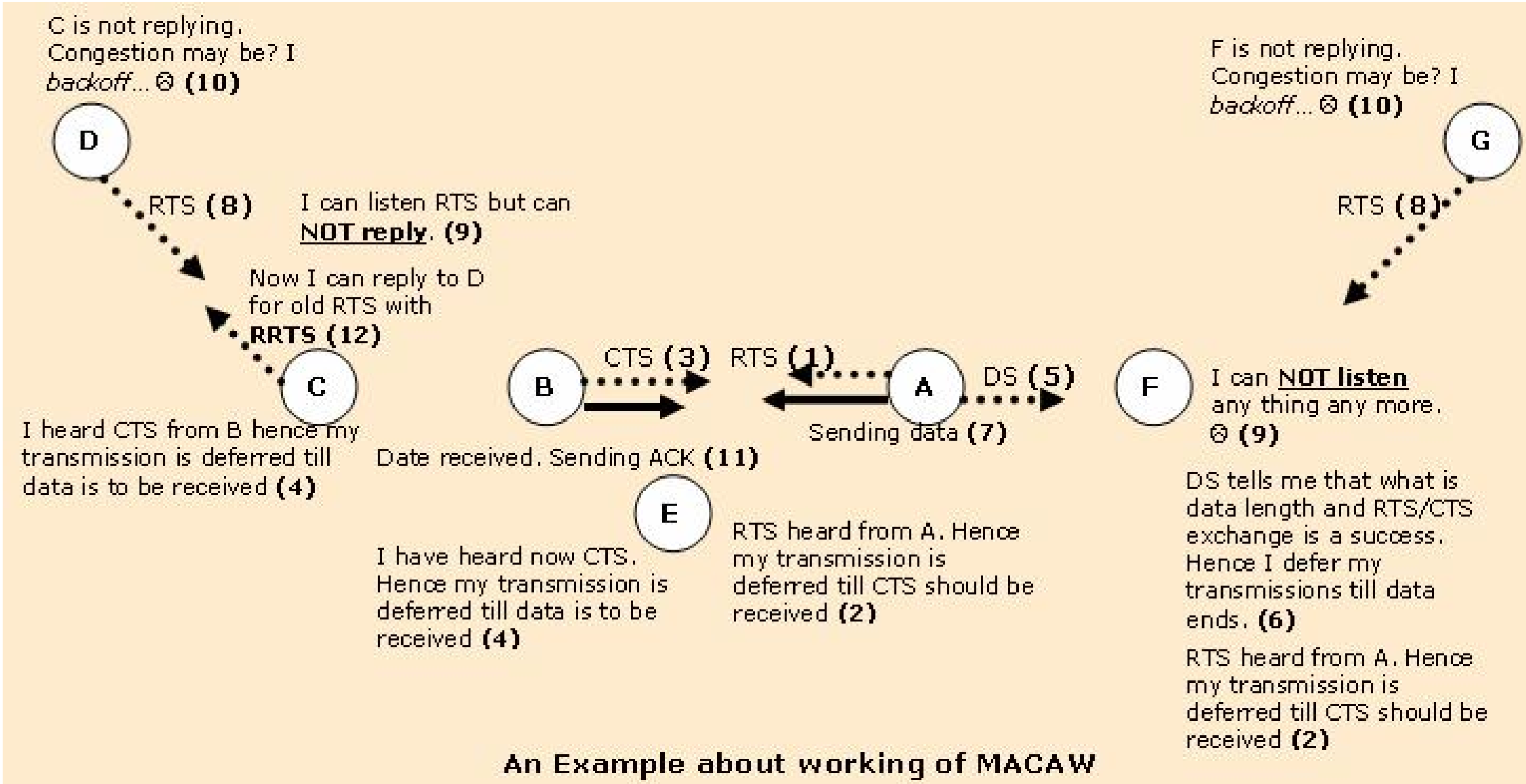


(b)

- MACA is effective because RTS and CTS packets are significantly shorter than the actual data packets, and therefore collisions among them are less expensive compared to those in the longer data packets.
- However, the RTS–CTS approach does not always solve the hidden terminal problem completely, and collisions can occur when different nodes send the RTS and the CTS packets.
- Another weakness of MACA is that it does not provide any acknowledgment (ACK) of data transmissions at the data link layer.
- If a transmission fails for any reason, retransmission has to be initiated by the transport layer. This can cause significant delays in the transmission of data.

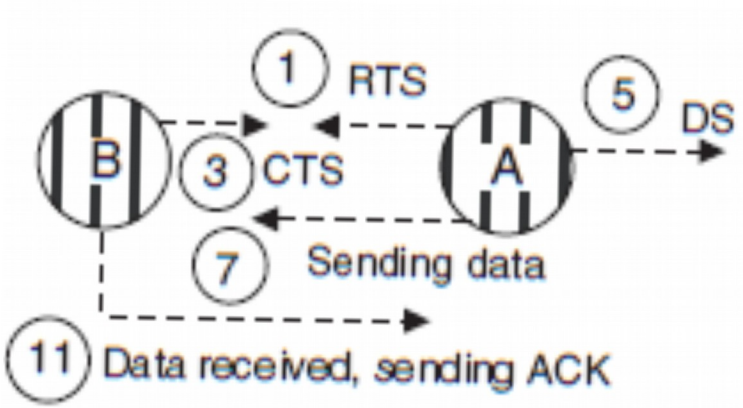
Multiple access with collision avoidance for wireless (MACAW)

- MACAW is a MAC protocol widely used in adhoc networks.
- It uses RTS–CTS–DS–DATA–ACK frame sequence (DS stands for data sending) for transferring data, sometimes preceded by an RTS–RRTS (where RRTS is request for RTS) frame sequence, in view to provide solution to the hidden terminal problem.
- To explain the principle operation of MACAW, consider the example scenario as shown in Fig.(Next slide)
- It is assumed that only adjacent nodes are in transmission range of each other.



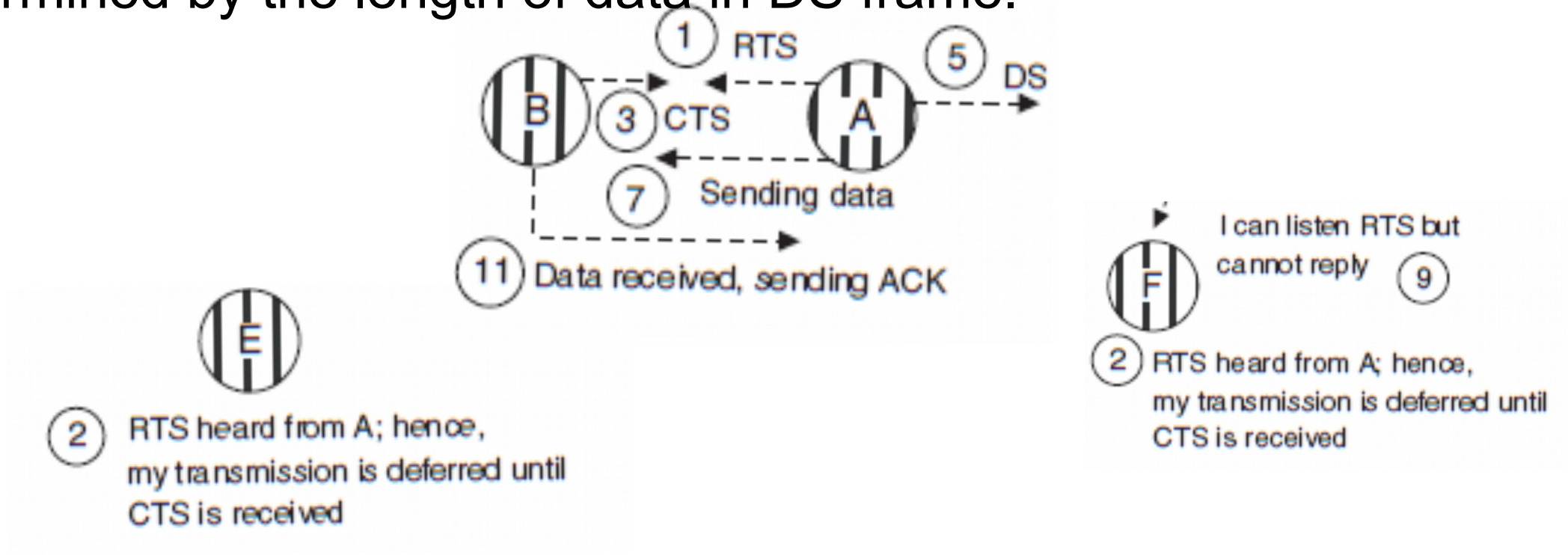
An Example about working of MACAW

1. A wishes to transfer data to node B. It initiates the process by sending a RTS frame to node B.(1)
2. The node B replies with a CTS frame.(3)
3. After receiving CTS, a short DS frame is sent. It provides the information about the length of the data frame. Every station that overhears this frame, and knows that RTS-CTS exchange was successful. (5)
4. After DS, node A sends data. After successful reception of data, node B replies with ACK frame.(7, 11)

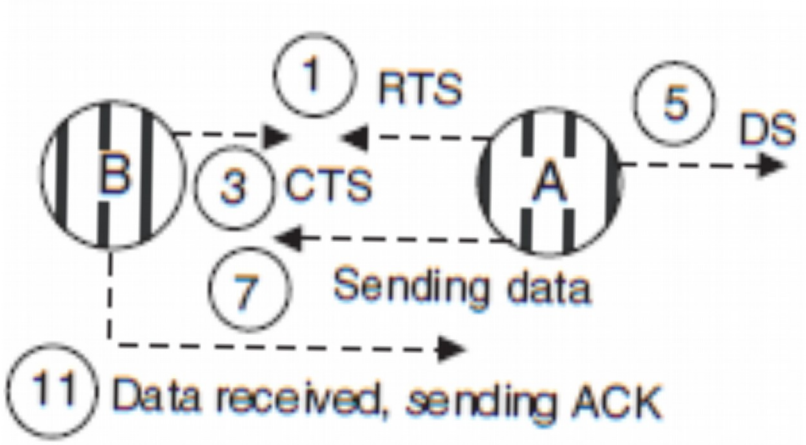


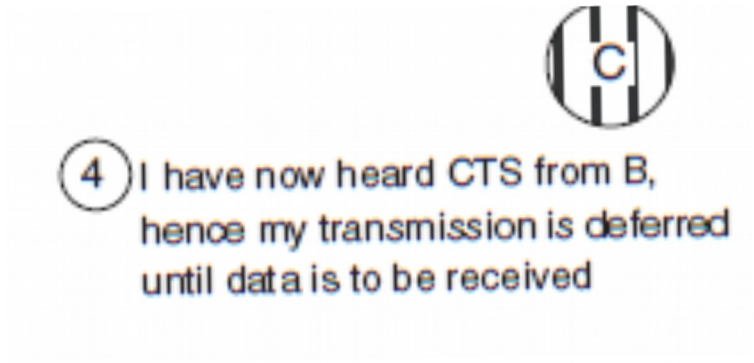
5. If node A has more data to send, it has to wait for random amount of time after each successful data transmission and has to compete a fresh for the medium with the adjacent node using CTS-RTS frames.
6. Nodes E and F overhear an RTS frame, so they defer from transmission until a CTS is received or after waiting a random amount of time. The maximum waiting time is the RTS propagation time and time until the data transmission is over by node A. This time is determined by the length of data in DS frame.
7. Nodes C & E overhear a CTS frame, they defer from sending anything until the data frame and its ACK have been received (Thus solves the problem of hidden terminal problem).

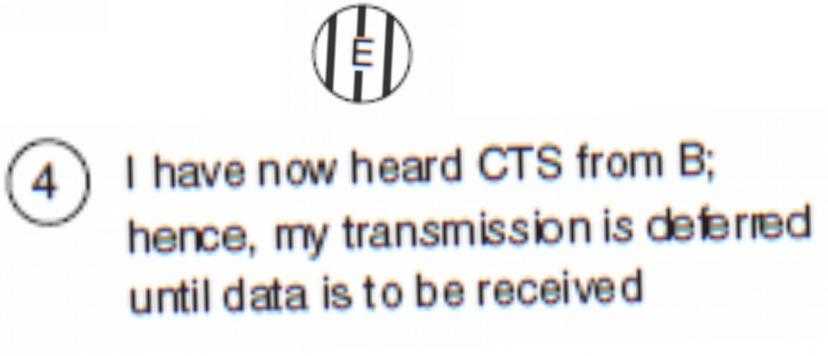
6. Nodes E and F overhear an RTS frame(2), so they defer from transmission until a CTS is received or after waiting a random amount of time. The maximum waiting time is the RTS propagation time and time until the data transmission is over by node A. This time is determined by the length of data in DS frame.



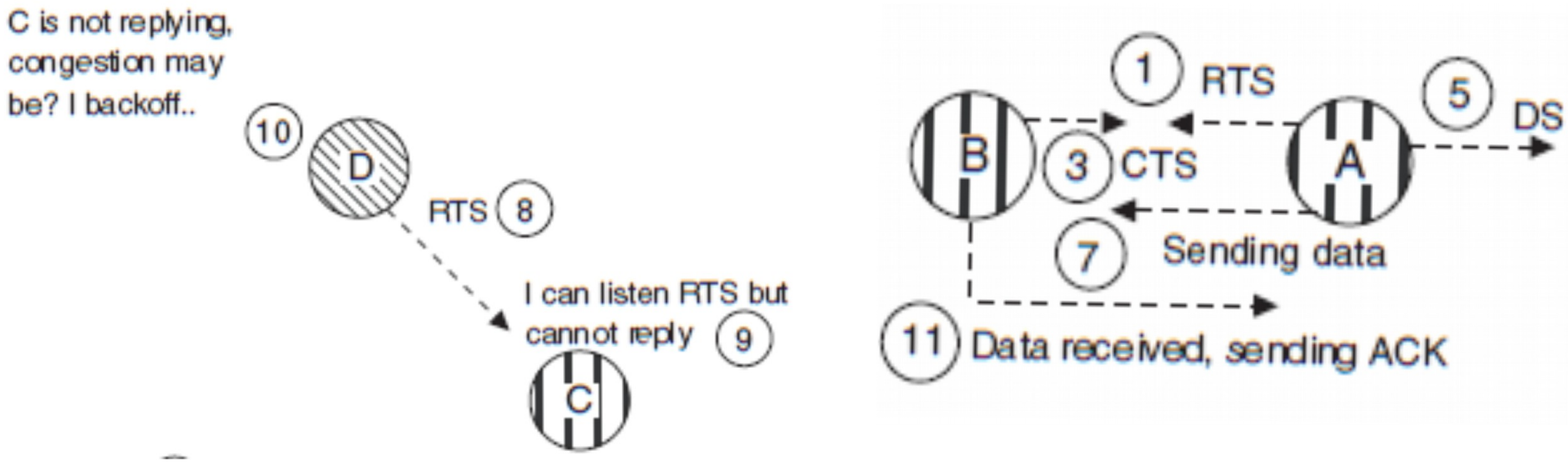
7. Nodes C & E overhear a CTS frame(4), they defer from sending anything until the data frame and its ACK have been received (Thus solves the problem of hidden terminal problem).





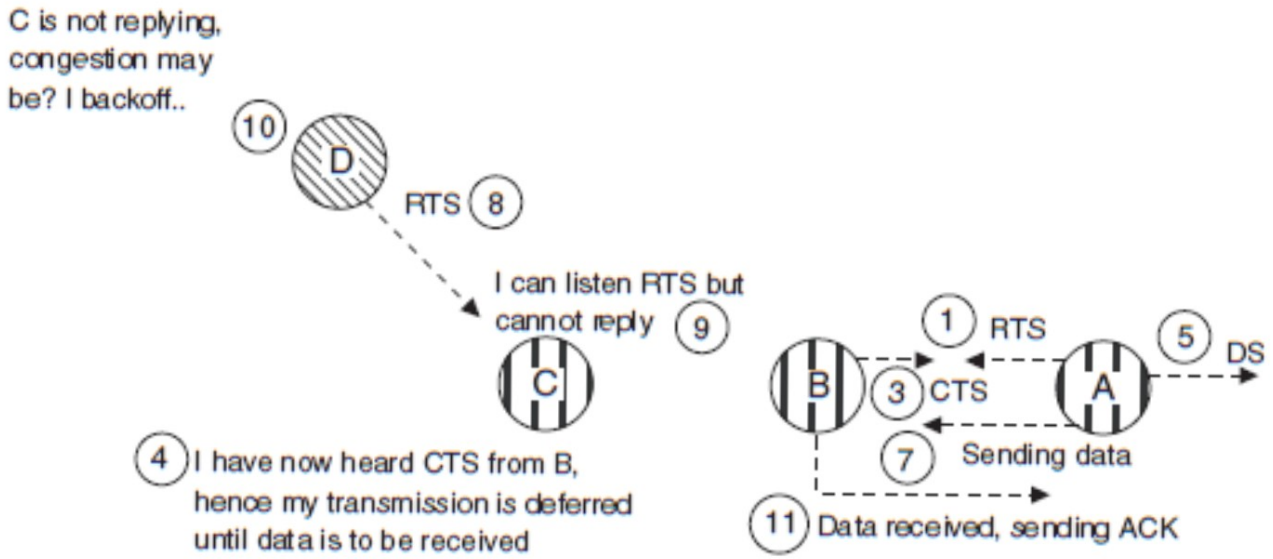


- 8. Node D is unaware of data transmission between node A and node B. it has data to transmit to node C, It sends a RTS to node C (as C is in the transmission range of D), Node C has already deferred its transmission until the data transmission is over between node A and node B to avoid co-channel interference between B and C. Thus, even node C receives RTS from node D, it does not reply by sending CTS. The node D assumes that its RTS transmission is not successful because of collision and hence goes to back-off.
-

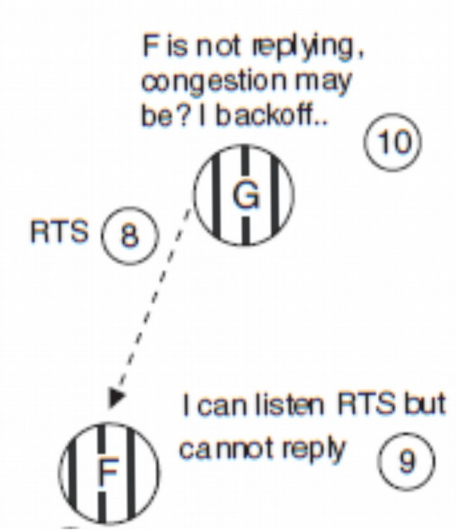


9. If node A has multiple data to transmit, after any successful transmission of frame it has to wait for random time and compete again for next transmission, this is the only instance when node D can initiate the process of transmission. However, due to back-off time of node D, the probability of capturing the medium during this small time interval is very small. To increase the per node fairness, a new control frame is introduced. It is Request for Request to Send (RRTS).

10.The node C, which was not able to reply by CTS to node D due to ongoing transmission between node A and node B, now sends RRTS frame to node D in next contention period. Node D immediately replies by RTS and exchange of CTS-DS- data takes place. Other nodes who overhear an RRTS, they defer their transmission for two time slots to hear successful RTS-CTS transmission between node C and node D.



11. Node G is also unaware of data transmission between node A and node B. It has some data to transmit to node F (Node F is in the transmission range of A but not of G). It initiates the process by sending RTS to node F. Node F cannot hear RTS from node G, as it is exposed to co-channel interference, so does not send CTS. Node G considers that its RTS is collided and hence backs off. In this case solution of RRTS does not work, as the data frames sent by node B are longer than any other frames. The probability that node F is exposed to transmission from node A is high than node



Power Control MAC (PCM)

- All mobile nodes are battery operated, it is very much necessary to save the energy and utilize the power efficiently.
- There are various power control MAC protocols, in which control frames (RTS, CTS, ACK and RRTS) and data frames are transmitted at different power level. Also if nodes have nothing to transmit then they go in OFF state.
- In PCM, the RTS and CTS packets are sent using the maximum available power, whereas the data and ACK packets are sent with the minimum power required to communicate between the sender and the receiver.

- PCM also stipulates that the source node periodically transmits the DATA packet at the maximum power level, for just enough time so that nodes in the carrier-sensing range may sense it.
- Thus, PCM achieves energy savings without causing throughput degradation.
- The operation of the PCM scheme requires a rather accurate estimation of received packet signal strength.
- Therefore, the dynamics of wireless signal propagation due to fading and shadowing effect may degrade its performance.
- Another drawback of this scheme is the difficulty in implementing frequent changes in the transmit power levels.

Power aware medium access control with signaling (PAMAS).

1. Separate Signalling and Data Channel: The basic idea of PAMAS is that all the RTS–CTS exchanges are performed over the signaling channel and the data transmissions are kept separate over a data channel.
2. While receiving a data packet, the destination node starts sending out a busy tone over the signaling channel.
3. Nodes listen on the signaling channel to deduce when it is optimal for them to power down their transceivers.
4. Every node makes its own decision whether to switch power OFF or not, such that there is no drop in the throughput.

5. A node itself switches the power OFF, if it has nothing to transmit and it realizes that its neighbor is transmitting.

6. A node also switches the powers OFF if at least one neighbor is transmitting and another is receiving at the same time.

Power controlled multiple access (PCMA)

1. PCMA relies on controlling transmission power of the sender so that the intended receiver is just able to decipher the packet.
2. This helps in avoiding interference with other neighboring nodes that are not involved in the packet exchange.
3. PCMA uses two channels, one for sending out busy tones and the other for data and other control packets.
4. Power control mechanism in PCMA has been used for increasing channel efficiency through spatial frequency reuse rather than only increasing battery life.

5. Therefore, an important issue for the transmitter and the receiver pair is to determine the minimum power level necessary for the receiver to decode the packet, while distinguishing it from noise or interference.
6. Also, the receiver has to advertise its noise tolerances so that no other potential transmitter will disrupt its ongoing reception.
7.In PCMA, the sender sends a request power to send (RPTS) packet on the data channel to the receiver. The receiver responds with an accept power to send (APTS) packet, also on the data channel.
8. This RPTS–APTS exchange is used to determine the minimum transmission power level that will cause a successful packet reception at the receiver.

9. After this exchange, the actual data are transmitted and acknowledged with an ACK packet.
10.In a separate channel, every receiver sets up a special busy tone as a periodic pulse.
11. The signal strength of this busy tone advertises to the other nodes about the additional noise power the receiver node can tolerate.
12.When a sender monitors the busy tone channel, it is essentially doing something similar to carrier sensing, as in carrier sense multiple access with collision avoidance (CSMA/CA) model.
13.When a receiver sends out a busy tone pulse,it is doing something similar to sending out a CTS packet.

14.The RPTS–APTS exchange is analogous to the RTS–CTS exchange.

- The major difference, however, is that the RPTS–APTS exchange does not force other hidden transmitters to backoff.
- Collisions are resolved by the use of some appropriate backoff strategy.

Dual busy tone multiple access (DBTMA).

1. The DBTMA scheme uses out-of-band signaling to solve the hidden and the exposed terminal problems effectively.
2. DBMTA sends RTS packets on data channel to set up transmission requests. Subsequently, two different busy tones on a separate narrow channel are used to protect the transfer of the RTS and data packets.
3. The sender of the RTS sets up a transmit-busy tone (Btt). Correspondingly, the receiver sets up a receive-busy tone (BTr) to acknowledge the RTS, without using any CTS packet.

4. Any node that senses an existing BTr or BTt defers from sending its own RTS over the channel.
5. Therefore, both of these busy tones together guarantee protection from collision from other nodes in the vicinity.
6.Through the use of the BTt and BTr in conjunction, exposed terminals are able to initiate data packet transmissions.
7. Also, hidden terminals can reply to RTS requests, as simultaneous data transmission occurs between the receiver and the sender.

MANET Routing Protocols

- Routing protocol specifies the routes between the nodes and disseminating information which choose the routes between any two nodes on a network.
- In MANETs, nodes are mobile and can be connected dynamically in an arbitrary manner.
- All nodes of these networks behave as routers and take part in discovery and maintenance of routes to another nodes in the network.
- There are several routing protocols developed for MANETs with different specific requirements.

Due to mobility of nodes, it becomes difficult to perform routing in a MANET as compared to a conventional wired network.

Routing in a MANET depends on many factors such as,

- ✓ Topology of the network,
- ✓ Selection of routers,
- ✓ location of request initiator, and
- ✓ Specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently.
- ✓ **Numerous MANET routing** protocols have been proposed, both under and outside the umbrella of the IETF MANET working group.

Classification of routing protocols in MANETs can be done on routing strategy and network structure.

According to the network structure:

- ✓ *Flat routing,*
- ✓ *Hierarchical routing, and*
- ✓ *Geographic position-assisted routing.*

According to the routing strategy:

- ✓ *Table-driven and*
- ✓ *Source-initiated*

In *flat routing* approach, every node is equally responsible for forming and maintaining the routing information.

The *hierarchical routing* approach logically restructures the network into clusters with cluster heads (CHs) forming the virtual backbone for routing. Thus, the number of nodes participating in the formation and maintenance of routes is less as compared to that of flat routing approach.

Geographic position-assisted routing is to obtain the geographical location of destination node to optimize the route discovery.

Flat Routing over adhoc networks can be broadly classified as *topology based* or *position-based* approaches.

1) Topology-based routing protocols:

- These protocols work on the basis of information about existing links in the network.
- This information is utilized to carry out the task of data forwarding.
- They can be further subdivided as being-

✓ Proactive (or table-driven),
✓ Reactive (or on demand), or
✓ Hybrid protocols.

i) Proactive (Table driven) Routing Protocol: The main features of these protocols are as follows,

- Continuous Updates: In these protocols, all nodes keep track of routes of all possible destinations and whenever any topology change is there in the network, it is updated immediately.
- Table Driven: These protocols are also known as table driven protocols, as they maintain updated routing table for each node in the network all the time.
- Minimum Delay: These protocols have the advantage that whenever a node needs a route to forward data, a route is immediately obtained from the routing table and data is forwarded with minimum delay.

- Network size: These protocols are not suitable for large networks, as size of routing table will be large corresponding to large number of nodes. Which causes overheads in terms of memory and bandwidth.
- Network capacity: These protocols may not always be appropriate in MANETs with high mobility. It is because substantial fraction of the network capacity will be in use continuously so that the routing information could be kept updated.
- Channel conditions: The quality of channel may change with time due to the shadowing and fast fading and may not be good to use even if there is no mobility.

Some of the proactive protocols proposed in the literature are as follows,

Destination-Sequenced Distance-Vector Protocol (DSDV)

The Wireless Routing Protocol(WRP)

The Topology Broadcast based on Reverse Path Forwarding Protocol(TBRPF)

The Optimized Link State Routing Protocol(OLSR)

Multi Point Relay(MPR)

The Source Tree Adaptive Routing Protocol(STAR)

ii) Reactive (on demand) Routing Protocol: The main features of these protocols are as follows,

- Route discovery: It takes place by flooding the route request (RREQ) packets throughout the network.
- On demand: These protocols do not maintain any routing information at the network nodes, they search the routes to the destination only on demand. The protocols are event driven, in which routing information is exchanged between node only when there is a topology change or route discovery demand.
- Packet loss: The packets on route to the destination are likely to be lost if the route in use changes.

- Network size: Reactive protocols do not maintain routing table, so often consume much less bandwidth and memory than proactive protocols. These protocols are suitable for larger size network.
- Delay in route discovery: These protocols determine the route whenever a node needs it, so there may be significant delay in determining a route.
- Traffic on the network: In reactive protocols, even though route maintenance is limited to routes currently in use, it may still generate a significant amount of network control traffic when the topology of the network changes frequently.

Some of the reactive protocols are as follows,

Dynamic Source Routing (DSR)
The Ad Hoc On-Demand Distance Vector Protocol(AODV)
Link Reversal Routing and
TORA

Hybrid Protocols

- Hybrid protocols combine local proactive and global reactive routing in order to achieve a higher level of efficiency and scalability. For example, a proactive scheme may be used for close by nodes only, while routes to distant nodes are found using reactive mode.
- Hybrid protocols are associated with some sort of hierarchy which can either be based on the neighbors of a node or on logical partitions of the network.

The major limitation of hybrid schemes combining both strategies, is that it still needs to maintain at least those paths that are currently in use. This limits the amount of topological changes that can be tolerated within a given time span.

Some of the hybrid routing protocols are as follows,

- Zone Routing Protocol (ZRP)
- Fisheye State Routing (FSR)
- Landmark Routing (LANMAR) for MANET with Group Mobility
- Cluster-Based Routing Protocol

2) Position-based routing protocols:

- The position-based protocols require that the physical location information of the nodes be known.
- These protocols overcome some of the limitations of topology-based routing by relying on the availability of additional knowledge.
- Typically, each or some of the nodes determine their own position through the use of the *Global Positioning System* (GPS) or some other type of positioning technique (*Trilateration*).
- The sender normally uses a location service to determine the position of the destination node, and to incorporate it in the packet destination address field.

- Here, the routing process at each node is based on the destination's location available in the packet and the location of the forwarding node's neighbors.
- Position based routing does not require establishment or maintenance of routes, but this usually comes at the expense of an extra hardware.
- It supports the delivery of packets to all nodes in a given geographical region in a natural way, and this is called Geocasting.

Destination sequenced distance vector routing (DSDV).

- It is a *proactive hop-by-hop distance vector routing* protocol.
- In DSDV, each MN of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination, and a sequence number generated by the destination node.
- Using such routing table stored in each MN, the packets are transmitted between the nodes of an adhoc network.
- Each node of the adhoc network updates the routing table with advertisement periodically or when significant new information is available to maintain the consistency of the routing table with the dynamically changing topology of the ad hoc network.

- Periodically or immediately when network topology changes are detected, each MN advertises routing information using broadcasting or multicasting a routing table update packet.
- The update packet starts out with a metric of one to direct connected nodes.
- This indicates that each receiving neighbor is one metric (hop) away from the node. It is different from that of the conventional routing algorithms.
- After receiving the update packet, the neighbors update their routing table incrementing the metric by one and retransmit the update packet to the corresponding neighbors of each of them.
- The process is repeated until all the nodes in the ad hoc network have received a copy of the update packet with a corresponding metric.

Global state routing protocol (GSR).

- In GSR, each node maintains a neighbor list: a topology table, a next hop table, and a distance table. Neighbor list of a node contains the list of its neighbors (here all nodes that can be heard by a node are assumed to be its neighbors).
- For each destination node, the topology table contains the link state information as reported by the destination and the time stamp of the information.
- For each destination, the next hop table contains the next hop to which the packets for this destination must be forwarded.
- The distance table contains the shortest distance to each destination node.

- The routing messages are generated on a link change such as in link state protocols.
- On receiving a routing message, the node updates its topology table if the sequence number of the message is newer than that stored in the table.
- After this the node reconstructs its routing table and broadcasts the information to its neighbors.

Fisheye state routing protocol (FSR).

- In FSR, each node maintains a topology table, neighbor link list, and a routing table.
- The topology table is created by using the topology information obtained from the link-state messages.
- Each destination has an entry in the table (full topology map). An entry consists of two parts: the link-state information and a destination sequence number.
- Based on this table, the routing table will be calculated. The distance information will then be obtained from the routing table calculation.

- It is used to classify the node to a Fisheye scope.
- The topology table has following entries for every link state entry: destination address, destination sequence number, and link-state list.
- On receiving a link-state message, a node records/updates the sender in its neighbor list.
- If nothing is received for a timeout interval, the corresponding station will be removed from the neighbor list.
- The following information is maintained for each neighbor node: neighbor node link state and latest time stamp.

The routing table provides next hop information to forward a packet to a destination in the network.

The routing table consists of the following fields: destination address, next hop address, and distance.

Ad hoc on-demand distance vector (AODV)

- AODV is a method of routing messages between Mns.
- It allows the MNs to pass messages through their neighbors to the nodes with which they cannot directly communicate.
- AODV does this by discovering the routes along which messages can be passed.
- AODV makes sure that these routes do not contain loops and tries to find the shortest route possible.
- AODV is also able to handle changes in routes and can create new routes if there is an error.

- In AODV, to find a path to the destination, the source broadcasts an RREQ (Route Request) packet.
- The neighbors in turn broadcast the packet to their neighbors until the packet reaches an intermediate node that has a recent route information about the destination or until the packet reaches the destination.
- A node discards an RREQ packet that it has already seen.
- The RREQ packet uses sequence numbers to ensure that the routes are loop-free, and to make sure that if the intermediate nodes reply to RREQs.
- However, they reply with the latest information only.

- When a node forwards an RREQ packet to its neighbors, it also records in its tables the node from which the first copy of the request (REQ) came.
- This information is used to construct the reverse path for the route reply (RREP) packet.
- AODV uses only symmetric links because the RREP packet follows the reverse path of RREQ packet.
- As the RREP packet traverses back to the source, the nodes along the path enter the forward route into their tables.
- If the source moves then it can reinitiate route discovery to the destination.

- If one of the intermediate nodes moves then the moved node's neighbor realizes the link failure and sends a link failure notification to its upstream neighbors.
- This process repeats until it reaches the source upon which the source can reinitiate route discovery, if needed.
- In ad hoc networks, because of the limited range, each node can only communicate with the nodes next to it. Node that can be communicated directly is considered to be a neighbor.
- A node keeps track of its neighbors by listening for a HELLO message that each node broadcasts at set intervals.

- When one node needs to send a message to another node that is not its neighbor, it broadcasts an RREQ message.
- The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message, and a sequence number which serves as a unique ID.

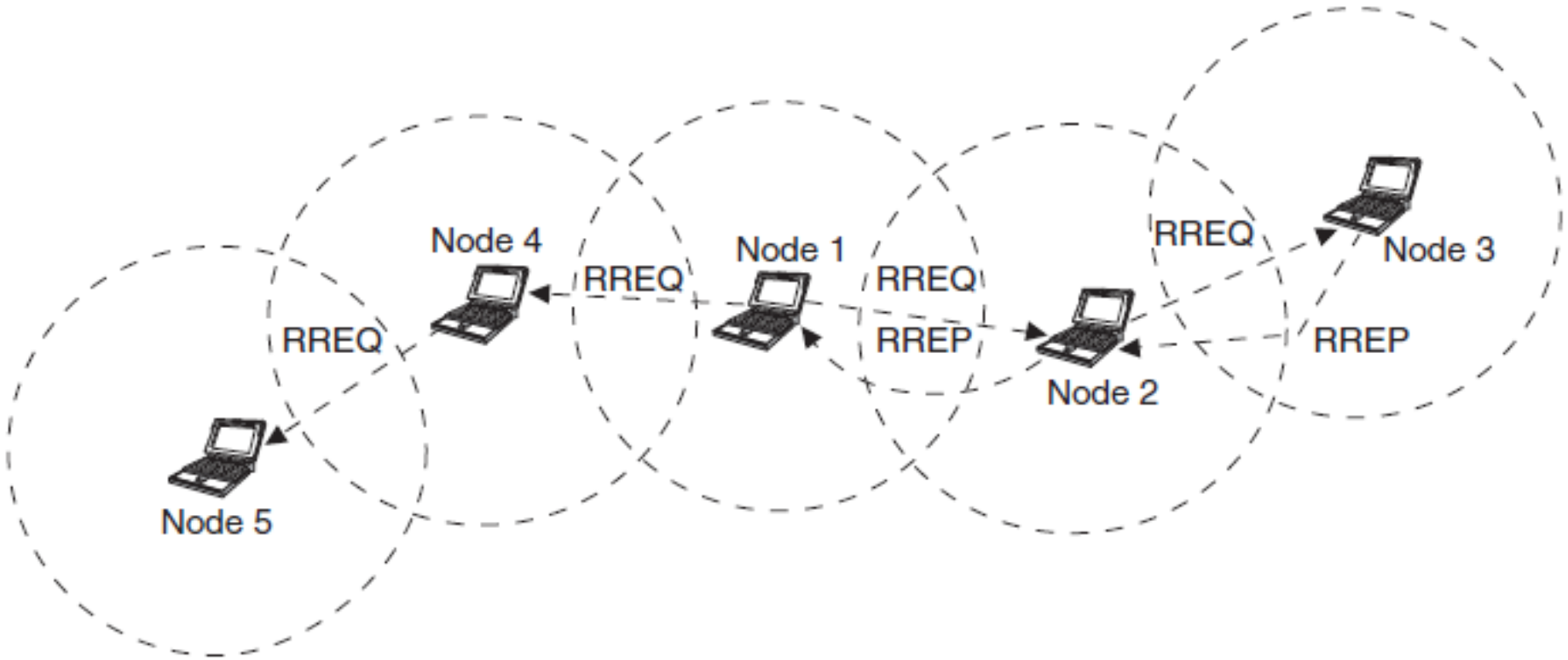
To explain the operation of AODV, consider a setup of four MNs as shown in Fig. In next slide

In the example, node 1 wishes to send a message to node 3.

Node 1’s neighbors are nodes 2 and 4.

1) As node 1 cannot directly communicate with node 3, node 1 sends out an RREQ.

AODV SCENARIO



2) The RREQ is heard by nodes 4 and 2. When node 1's neighbors (nodes 2 and 4) receive the RREQ message then they have two choices:

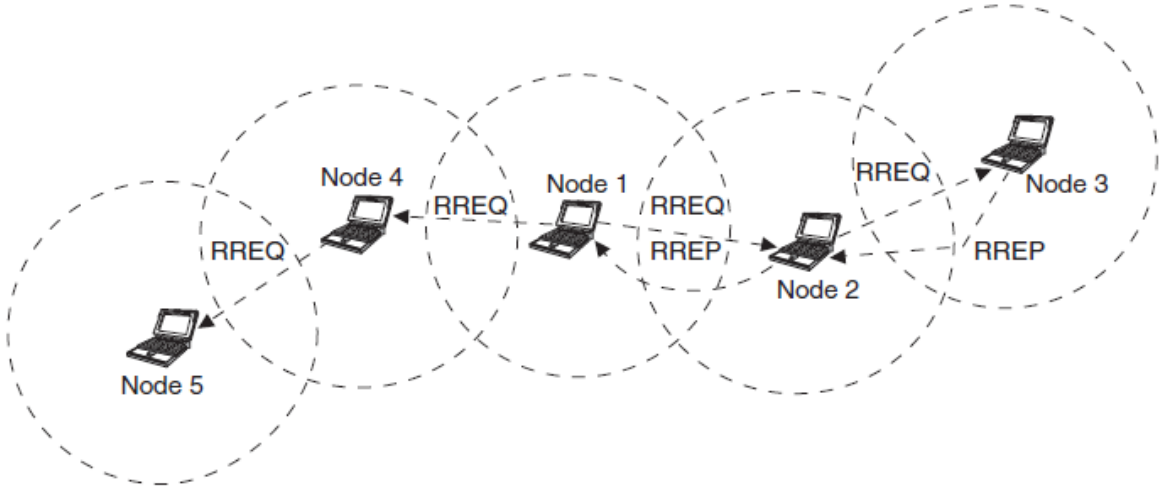
- if they know a route to the destination or
- if they are the destination then they can send an RREP message back to node 1,

otherwise they will have to rebroadcast the RREQ to their set of neighbors.

The message keeps getting rebroadcast until its lifespan is over.

3) If node 1 does not receive a reply in a set amount of time, it will rebroadcast the REQ except this time the RREQ message will have a longer lifespan and a new ID number.

- All of the nodes use the sequence number in the RREQ to ensure that they do not rebroadcast an RREQ.
- In the example, node 2 has a route to node 3 and it replies to the RREQ by sending out an RREP.
- Node 4, on the other hand, does not have a route to node 3 so it rebroadcasts the RREQ.

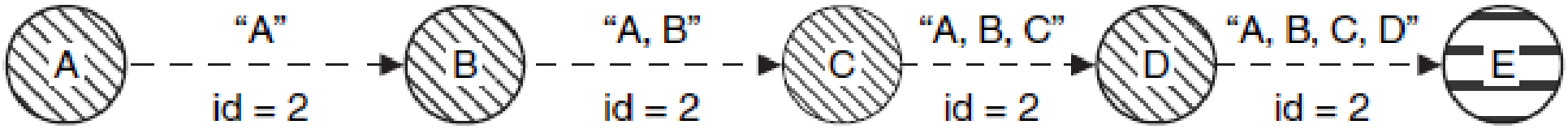


Dynamic source routing (DSR)

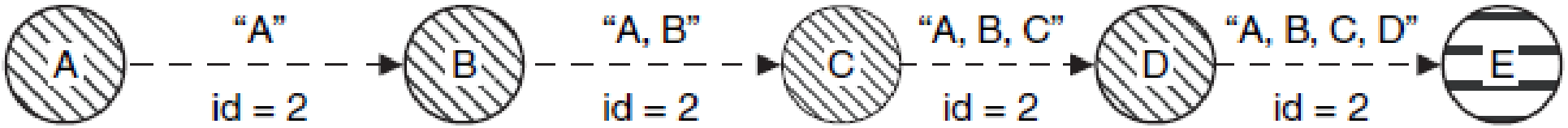
- DSR is a simple and efficient routing protocol designed specifically for use in multihop wireless ad hoc networks of MNs.
- DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration.
- The two major phases of the DSR protocol are: *route discovery* and *route maintenance*.
- When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination.

- If it finds that an unexpired route to the destination exists, then it uses this route to send the packet.
- But if the node does not have such a route, then it initiates the route discovery process by broadcasting a RREQ packet.
- The RREQ packet contains the addresses of the source and the destination, and a unique identification number.
- Each intermediate node checks whether or not it knows a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors.
- To limit the number of RREQs propagated, a node processes the RREQ packet only if it has not already seen the packet and its address is not present in the route record of the packet.

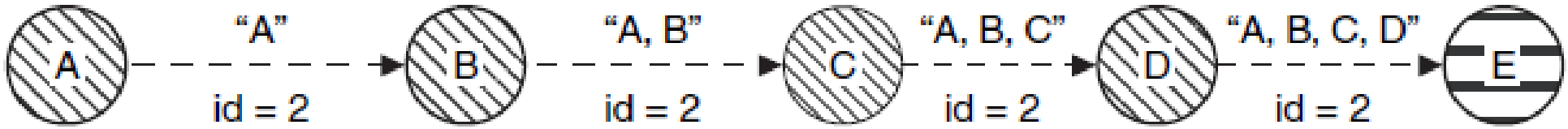
An RREP is generated when either the destination or an intermediate node with current information about the destination receives the RREQ packet.
An RREQ packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.
Fig. 8.9 illustrates an example of route discovery, in which node A is attempting to discover a route to node E.



To initiate the route discovery, A transmits an RREQ message as a single local broadcast packet, which is received by all nodes currently within wireless transmission range of A (here B is in A's communication range).
Each RREQ message identifies the initiator and target of the route discovery, and also contains a unique REQ id(here id = 2) determined by the initiator of the REQ.
Each RREQ also contains a record listing the address of each intermediate node through which this particular copy of the RREQ message has been forwarded (i.e., "A, B, C, D").



This route record is initialized to an empty list by the initiator of the route discovery.
In returning the RREP to the initiator of the route discovery, such as node E replying back to A in Fig., node E will typically examine its own Route Cache for a route back to A, and if found, will use it for the source route for delivery of the packet containing the RREP.
Otherwise, E may perform its own route discovery for target node A.



For example, in the situation illustrated in Fig. , node A originates a packet for node E using a source route through intermediate nodes B, C, and D.
In this case, node A is responsible for receipt of the packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D, and node D is responsible for receipt finally at the destination E.
This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use or by a passive acknowledgment (in which, e.g., B confirms receipt at C by overhearing C transmit the packet to forward it on to D).

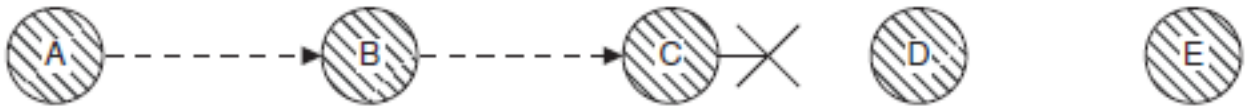


Figure 8.10 | Route maintenance example in DSR.

If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to REQ a DSR-specific software acknowledgment to be re turned by the next hop.
This software acknowledgment will normally be transmitted directly to the sending node, but if the link between these two nodes is unidirectional, this software acknowledgment may travel over a different, multihop path.
If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded.

For example, in Fig. 8.10, if C is unable to deliver the packet to the next hop D, then C returns a ROUTE ERROR to A, stating that the link from C to D is currently “broken.”
Node A then removes this broken link from its cache; any retransmission of the original packet is a function of upper layer protocols.
For sending such a retransmission or other packets to this same destination E, if A has in its route cache another route to E, it can send the packet using the new route immediately.

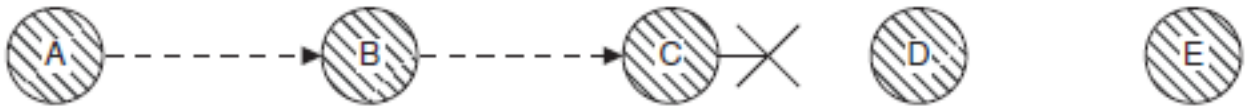


Figure 8.10 | Route maintenance example in DSR.

Technologies

Networking technologies that can facilitate implementation of MANETs are Bluetooth, ultrawide band (UWB), HIPERLAN/1, HIPERLAN/2, IEEE 802.11 WLAN, IEEE 802.15.3 Wireless PAN, and HomeRF. Except HomeRF, all the technologies are discussed in the previous lectures.

Vehicular AdHoc Networks (VANETs)

Vehicular Ad Hoc Networks (VANETs)

- Vehicular ad hoc networks (VANETs) are an envision of the intelligent transportation system (ITS).
- Vehicles communicate with each other in two ways:
  - ✓ Intervehicle communication and
  - ✓ Vehicle to roadside infrastructure communication.

- VANETs are based on short-range wireless communication between vehicles.
- Unlike infrastructure-based networks such as cellular networks, these networks are constructed on the fly (self-organizing).

- VANETs are a special case of networks (MANETs). The key differences as compared to MANETs are following:

1) Components building the network are vehicles, restricted vehicle movements, high mobility, and time-varying vehicle density.
2) One advantage of VANETs over MANETs is that most of the vehicles provide sufficient computational and power resources, thus eliminating the need for introducing complicated energy-aware algorithms.

- The optimal goal of VANETs is to provide safer and more efficient roads in future by communicating timely information to drivers and concerned authorities.

Unique Characteristics of VANETs

The fundamental characteristics that differentiate VANETs from other networks are as follows:

- Geographically constrained topology
- Partitioning and large-scale
- Self-organization
- Unpredictability
- Power Consumption
- Node reliability
- Channel Capacity
- Vehicle Density
- Vehicle Mobility

Geographically constrained topology

- Roads limit the network topology to one dimension - the road direction.
- Except for crossroads or overlay bridges, roads are generally located far apart.
- Even in urban areas, where they are located close to each other, there exist obstacles, such as buildings and advertisement walls, which prevent wireless signals from traveling between roads.
- This implies that vehicles can be considered as points of the same line; a road can be approximated as a straight line or a small angled curve.

- This observation is quite important, because it affects the wireless technologies that can be considered.
- For example, as the packet relays are almost all in the same one-directional deployment region, the use of directional antennas could be of great advantage.
- Self-organization: The nodes in the network must be capable to detect each other and transmit packets with or without the need of a base station.

Partitioning and large-scale:

- The probability of end-to-end connectivity decreases with distance; this is true for one-dimensional network topologies.
- In contrast, connectivity is often explicitly assumed in research for traditional ad hoc networks, sometimes even for the evaluation of routing protocols. In addition, VANETs can extend in large areas, as far as the road is available.
- This artifact together with the one-dimensional deployment increases the above probability.

Unpredictability: The nodes (or vehicles) constituting the network are highly mobile.

- Because of this reason, there is also a high degree of change in the number and distribution of the nodes in the network at given time instant.
- The nodes must be constantly aware of the network status, keep track of the hosts associated with the network, detect broken links, and update their routing tables whenever necessary.
- As vehicle mobility depends on the deployment scenario, the movement direction is predictable to some extent. In highways, vehicles often move at high speeds, whereas in urban areas they are slow.
- Mobility models can now include some level of predictability in movement patterns.

Power consumption:

- In traditional wireless networks, nodes are power-limited and their life depends on their batteries – this is especially true for ad hoc networks.
- Vehicles, however, can provide continuous power to their computing and communication devices.
- As a result, routing protocols do not have to account for methodologies that try to prolong the battery life.
- Older network protocols include mechanisms such as batterylife reports for energy-efficient path selection, sleep–awake intervals, as well as advanced network cross-layer coordination algorithms.
- These schemes cannot offer any additional advantages to vehicular networks.

Power consumption:

- In traditional wireless networks, nodes are power-limited and their life depends on their batteries – this is especially true for ad hoc networks.
- Vehicles, however, can provide continuous power to their computing and communication devices.
- As a result, routing protocols do not have to account for methodologies that try to prolong the battery life.
- Older network protocols include mechanisms such as batterylife reports for energy-efficient path selection, sleep–awake intervals, as well as advanced network cross-layer coordination algorithms.
- These schemes cannot offer any additional advantages to vehicular networks.

Node reliability:

- Vehicles may join and leave the network at any time and much more frequently than in other wireless networks.
- The arrival/departure rate of vehicles depends on their speed, the environment, as well as on the driver that needs to be connected to the network.
- In the case of ad hoc deployments, the communication does not easily depend on a single vehicle for packet forwarding.
- This occurs because of non-coverage of communication range between communicating vehicles. Thus, there is a need to take help of intermediate nodes for packet forwarding to destination vehicle.
- Intermediate nodes must be reliable to forward the packets efficiently.

Channel capacity:

- The channels in VANETs over which the terminals communicate aresubjected to noise, fading, interference, multipath propagation, path loss, and have less bandwidth. So high bit-error rates are common in VANETs.
- One end-to-end path can be shared by several sessions.
- In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.
- So smart algorithms are needed to overcome of fluctuating link capacity in networks.

Vehicle density:

- Multihop data delivery through VANETs is complicated by the fact that vehicular networks are highly mobile and sometimes sparse.
- The network density is related to the traffic density, which is affected by the location and time.
- Although it is very difficult to find an end-to-end connection for a sparsely connected network, the high mobility of vehicular networks introduces opportunities for mobile vehicles to connect with each other intermittently during moving.

Vehicle mobility:

- As the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time.
- VANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes.
- The MNs in the network dynamically establish routing among themselves as they move out, forming their own network on the fly.
- Moreover, a user in a VANET may not only operate within the network, but may also require access to a roadside infrastructure. Hence, there is a need of strong mobility patterns in VANETs.

Network Architecture

1. A typical VANETs architecture is as shown in Fig..
2. Vehicle-to-vehicle and vehicle-to road- side base station/gateway communication is possible for providing safety and other information services to vehicle users.
3. Group of vehicles together may form a cluster to disseminate information among themselves as well as to other clusters and base stations.
4. In a VANET, each vehicle in the system is equipped with a computing device, a short-range wireless interface, and a global positioning system (GPS) receiver.
5. GPS receiver provides location, speed, current time, and direction of the vehicle.

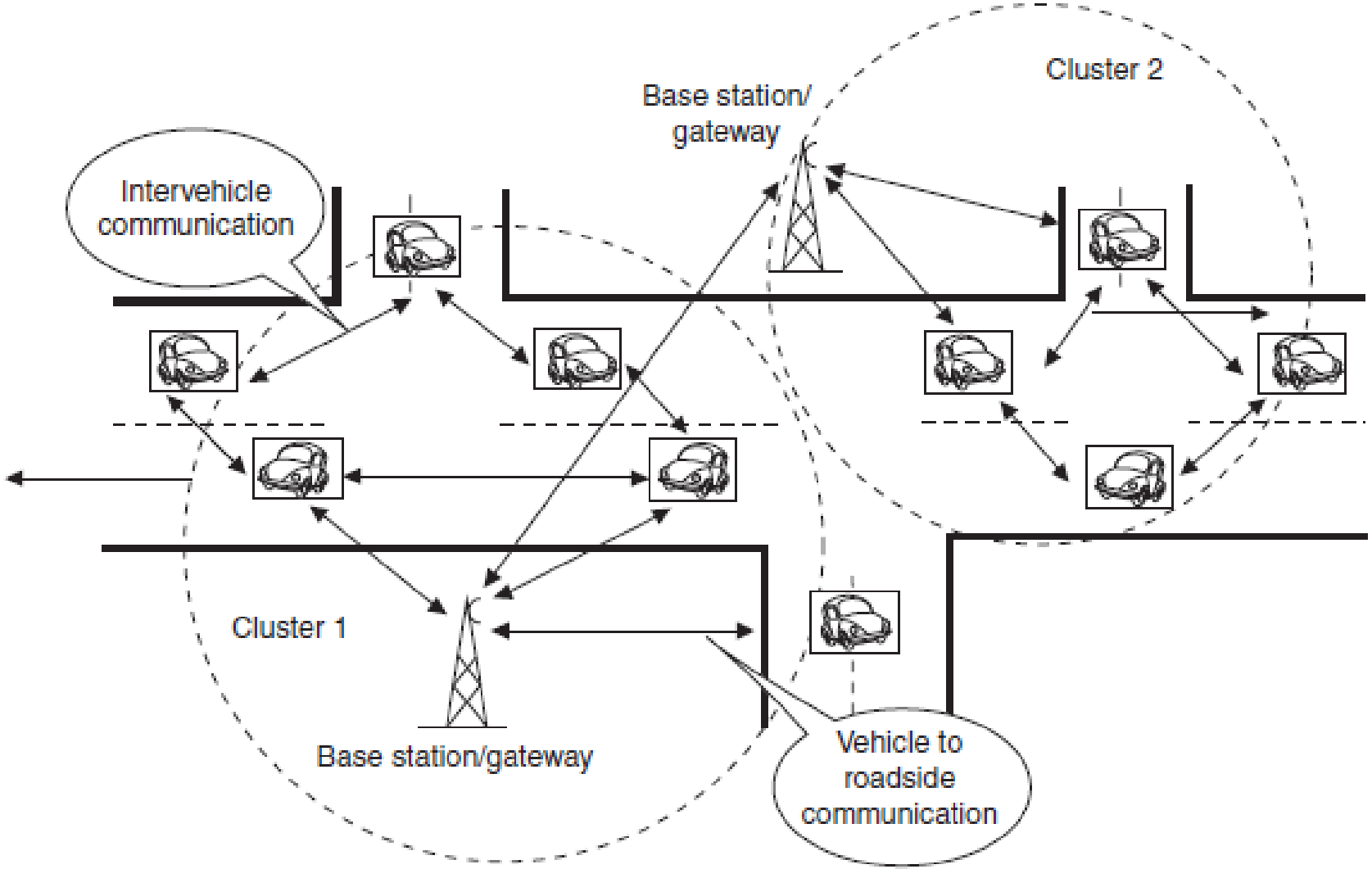


Figure 8.26 | VANET architecture.

- Each vehicle stores information about itself and other vehicles in a local database.

- The records in this database are periodically broadcasted.

A record consists of

- ✓ The vehicle identification,
- ✓ Position in the form of latitude and longitude,
- ✓ Current speed of the vehicle,
- ✓ Direction,
- ✓ Timestamps corresponding to when this record was first created and
- ✓ When this record was received.

VANET MAC Protocols:

- Design of VANET-MAC protocols should give more importance to fast topology changes and types of services rather than power constraints or time synchronization problems.
- Moreover, VANET-MAC protocols have to reduce the the medium access delay and increase the reliability, which is important in the case of safety applications.
- An IEEE working group is investigating a new PHY/MAC amendment of the 802.11 standard designed for VANETs, which is known as wireless access in vehicular environments (WAVE), also referred as IEEE 802.11p.

ADHOC MAC

- ADHOC MAC is a MAC protocol conceived within the European project CarTALK2000 with the purpose to design novel solutions for VANETs.
- ADHOC MAC works in slotted frame structure, where each channel is divided into time slots.
- The ADHOC-MAC protocol is devised for an environment in which the terminals can be grouped into clusters in such a way that all the terminals of a cluster are interconnected by broadcast radio communication.
- Such a cluster is defined as one-hop (OH). The access mechanism of ADHOC MAC can be classified as dynamic TDMA and channels are assigned to the terminals according to terminal needs.

Usage of directional antenna.

- Directional antenna transmission has a promising place in VANETs, in particular for MAC issues.
- In VANETs, node's movement is limited by roads and driving rules (e.g., opposite driving directions on the same road).
- So directional antennas would surely help in reducing interference and collisions with ongoing transmissions over parallel neighboring vehicular traffic.

Routing Protocols of VANET

- Routing protocol specifies the routes between the vehicles and disseminating information which choose the routes between any two vehicles on a network.
- As the topology of the network is constantly changing, the issue of routing packets between any pair of vehicles becomes a challenging task. So the protocols should be based on reactive routing (already discussed) instead of proactive routing.

Applications of VANET

Some of the important applications of VANETs are as follows:

- Message and file delivery
- Internet connectivity
- Communication-based longitudinal control
- Cooperative assistance systems
- Safety services
- Traffic monitoring and management services:

1. Message and file delivery: This application focuses on enabling the delivery of messages and files in a vehicular network to the target receivers (group communication) with acceptable performance.

2. Internet connectivity: This application focuses on connecting the vehicles to the Internet using roadside infrastructure and inter vehicle communications to facilitate browsing, send/read e-mails, chatting, etc.

3. Cooperative assistance systems: It focuses on coordinating vehicles at critical points such as blind crossings (a crossing without light control) and highway entries.

4.Communication-based longitudinal control: This application focuses on exploiting the 'look-through'' capability of VANETs to help avoiding accidents. For example, a vehicle can check the status of upfront vehicles status (speed, brake applied, road blocks, etc.).

5. Safety services:

- Safety applications include emergency braking, accidents, passing assistance, security distance warning, and coordination of cars entering a lane.
- Furthermore, sensors embedded in the car engine and elsewhere could be used for exchanging information, either with the on-board computer of the vehicle itself or vehicles with sophisticated computing and communication abilities, for diagnostic purposes.
- Also, safety applications are time-sensitive and should be given priority over non-safety applications.
- This could facilitate preventive maintenance and minimize road breakdowns

6. Traffic monitoring and management services:

- In such types of services, all vehicles are part of a ubiquitous sensor system.
- Each vehicle monitors the locally observed traffic situation such as density and average speed using an on-board sensor and the results are transferred to other vehicles via wireless data link through the network.
- Other applications are more related to multimedia communications such as entertainment and non-safety information. For example, information download at gas stations or public hotspots, car-to-car information exchange, etc.
- Some of these applications will be free, whereas others would require a service subscription or a one-time payment.