FIRST TERM EXAMINATION [FEB. 2018]
EIGHTH SEMESTER [B.TECH]
ADHOC AND SENSOR NETWORK [ETEC-406]

ne : 1½ hrs. M.M. : 30

te: *Q. no. 1 is compulsory. Attempt any two more questions from the rest.*

Q.1. (a) What is an ad-hoc network? Why ad hoc network are needed? Discuss. (2.5)

Ans. Ad hoc wireless networks are defined as the category of wireless networks that ize multi-hop radio relaying and are capable of operating without the support of any d infrastructure (hence they are also called infrastructure less networks). The ence of any central coordinator or base station makes the routing a complex one pared to cellular networks.

Advantages of Ad Hoc Network: The rapid development in ad hoc technology is ely used in portable computing such as laptop, mobile phone used to access the web ices, telephone calls when the user are in travelling. Development of self-organizing work decrease the communication cost. The growth of 4G technology enhances anytime, where, anyhow communication in ad hoc network. Ad hoc network is simple to design install. The advantages of an ad hoc network include: Separation from central work administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it be connected and communicated quickly.

Q.1. (b) What are the various issues in designing MAC protocol for AD HOC works? (2.5)

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

Bandwidth efficiency: Bandwidth must be utilized in efficient manner Minimal ntrol overhead BW = ratio of BW used for actual data transmission to the total ilable BW

Quality of service support: Essential for supporting time-critical traffic sessions They have resource reservation mechanism that takes into considerations the nature vireless channel and the mobility of nodes.

Synchronization: MAC protocol must consider synchronization between nodes in network

Synchronization is very important for BW (time slot) reservation by nodes Exchange ontrol packets may be required for achieving time synchronization among nodes

Hidden and exposed terminal problems: The hidden terminal problem refers to e collision of packets at a receiving node due to the simultaneous transmission of ose nodes that are not within the direct transmission range of the sender but are within e transmission range of the receiver. Collision occurs when both nodes transmit ckets at the same time without knowing about the transmission of each other.

CamScanner

Q.1. (c)List the characteristics of ideal routing protocol for ad hoc wireless network. **(2.5)**

Ans. A routing protocol for ad hoc wireless networks should have the following characteristics:

1. It must be fully distributed, as centralized routing involves high control overhead and hence is not scalable. Distributed routing is more fault tolerant than centralized routing, which involves the risk of single point of failure.

2. It must be adaptive to frequent topology changes caused by the mobility of nodes.

3. Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired.

4. It must be localized, as global state maintenance involves a huge state propagation control overhead.

5. It must be loop-free and free from state routes.

Q.1. (d)Why is need of power management important in AD HOC network? **(2.5)**

Ans. The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance. In certain case, the recharging of the energy source is impossible. Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.

Q.2 Compare MACA with MACAW protocol. **(10**

Ans. MACAW (MACA for Wireless) is a revision of MACA.

- The sender senses the carrier to see and transmits a RTS (Request To Send) frame if no nearby station transmits a RTS.
- The receiver replies with a CTS (Clear to Send) frame.
- The MACAW protocol uses one more control packet called the request-for-request-to-send (RRTS)

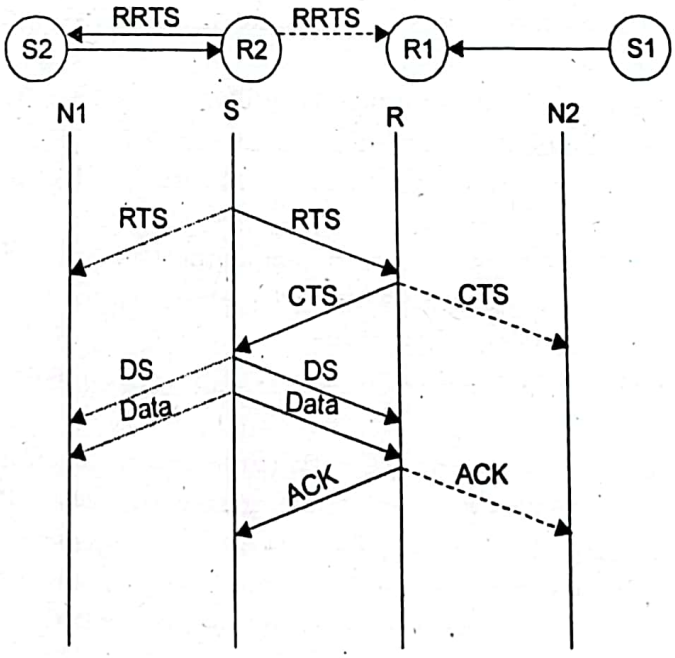


Fig. Packet exchange in MACAW.

CamScanner

Neighbors

- see CTS, then keep quiet.
- see RTS but not CTS, then keep quiet until the CTS is back to the sender.

The receiver sends an ACK when receiving an frame.

- Neighbors keep silent until see ACK.

Collisions

- There is no collision detection

The senders know collision when they don't receive CTS.

- They each wait for the exponential back-off time.

Q.3 (a)What is the classification of MAC protocol? **(5)**

Ans. MAC protocols for ad hoc wireless networks can be classified into several categories based on various criteria such as initiation approach, time synchronization, and reservation approaches. Ad hoc network MAC protocols can be classified into three basic types:

- Contention-based protocols
- Contention-based protocols with reservation mechanisms
- Contention-based protocols with scheduling mechanisms

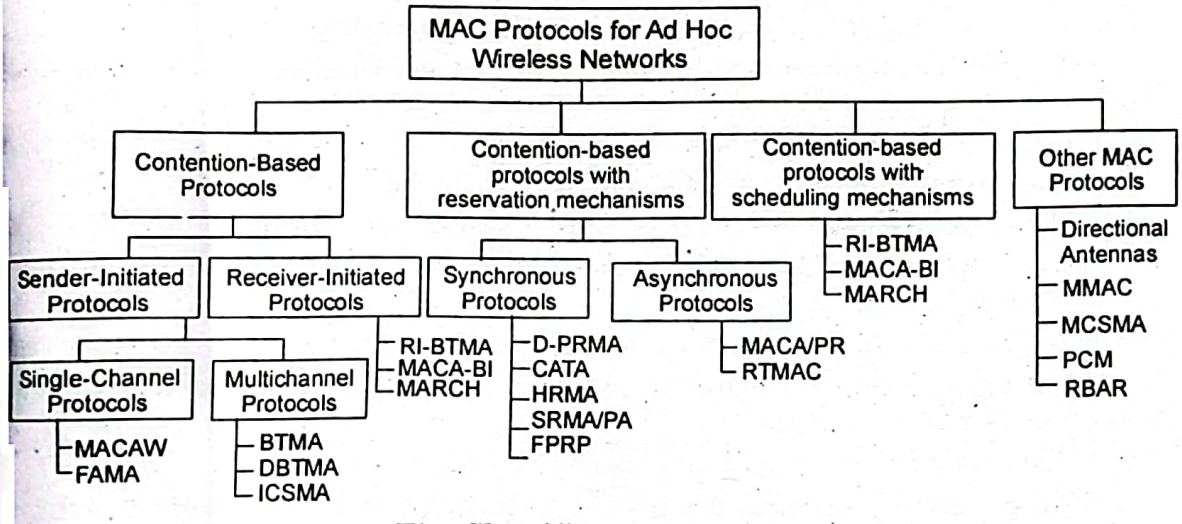


Fig. Classification of MAC

Contention-based protocols

- Sender-initiated protocols: Packet transmissions are initiated by the sender node.
- Single-channel sender-initiated protocols: A node that wins the contention to the channel can make use of the entire bandwidth.
- Multichannel sender-initiated protocols: The available bandwidth is divided into multiple channels.
- Receiver-initiated protocols: The receiver node initiates the contention resolution protocol.

Contention-based protocols with reservation mechanisms

- Synchronous protocols: All nodes need to be synchronized. Global time synchronization is difficult to achieve.
- Asynchronous protocols: These protocols use relative time information for effecting reservations.

CamScanner

Contention-based protocols with scheduling mechanisms

• Node scheduling is done in a manner so that all nodes are treated fairly and no node is starved of bandwidth.

• Scheduling-based schemes are also used for enforcing priorities among flows whose packets are queued at nodes.

• Some scheduling schemes also consider battery characteristics.

Q.3. (b) What are the characteristics and features of ad hoc networks? List the design goal of MAC protocol for ad hoc networks. (5)

Ans. Ad hoc networks are multi-hop network that use wireless communication for transmission without any fixed infrastructure. The networks are form and deform on-the-fly without the need for any system. Ad hoc structure does not require an access point, it is easy to setup, especially in a small or temporary network. Each node in the network forwards the packet without the need of central administration. In ad hoc network, node acts as a router to send and receive the data. An advantage of the system is robustness, flexibility and mobility. Ad hoc network are capable for analyzing radio propagation environment to optimize the performance. This typically requires that the network node have positioning capability as well as memory to recall geographical local condition. An ad hoc network typically refers to any set of network where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE802.11 wireless networks.

The design goal of MAC protocol for ad hoc networks.

The following are the important goals to be met while designing a medium access control

(MAC) protocol for ad hoc wireless networks:

• The operation of the protocol should be distributed.

• The protocol should provide QoS support for real-time traffic.

• The access delay, which refers to the average delay experienced by any packet to get transmitted, must be kept low.

• The available bandwidth must be utilized efficiently.

• The protocol should ensure fair allocation (either equal allocation or weighted allocation) of bandwidth to nodes.

• Control overhead must be kept as low as possible.

• The protocol should minimize the effects of hidden and exposed terminal problems.

• The protocol must be scalable to large networks.

• It should have power control mechanisms in order to efficiently manage energy consumption of the nodes.

Q.4. Classify and explain in details various types of routing protocol ADHOC wireless networks.

Ans. Refer of Q.3. First Term Exam 2017.

CamScanner

END TERM EXAMINATION MAY-JUNE 2018
EIGHTH SEMESTER [B.TECH]
ADHOC AND SENSOR NETWORK [ETEC-406]

Time : 3 hrs. **M.M. : 75**

Note: *Attempt any five questions in all including Q.no. 1. which is compulsory. Select one question from each unit.*

Q.1. (a) What is the difference between cellular and Ad Hoc wireless networks. **(3)**

Ans. Refer Q.2. (b) of First Term Exam Pg.3-2017.

Q.1. (b) What are the application of Ad Hoc wireless network. **(3)**

Ans. Refer Q.1 (b) of End Term Exam Pg. 8-2017.

Q.1. (c) Define Inter symbol Interference and method to avoid it. **(3)**

Ans. Inter symbol interference (ISI) is a form of distortion of a signal in which one ymbol interferes with subsequent symbols. This is an unwanted phenomenon as the revious symbols have similar effect as noise, thus making the communication less eliable. The spreading of the pulse beyond its allotted time interval causes it to interfere ith neighboring pulses. ISI is usually caused by multipath propagation or the inherent near or non-linear frequency response of a communication channel causing successive mbols to "blur" together.

The presence of ISI in the system introduces errors in the decision device at the ceiver output. Therefore, in the design of the transmitting and receiving filters, the jective is to minimize the effects of ISI, and thereby deliver the digital data to its stination with the smallest error rate possible.

In order to have no ISI at the receiver, we must treat this pulse-shaping filter, and y filtering done at the transmitter, the channel and the receiver all together as part of e channel.

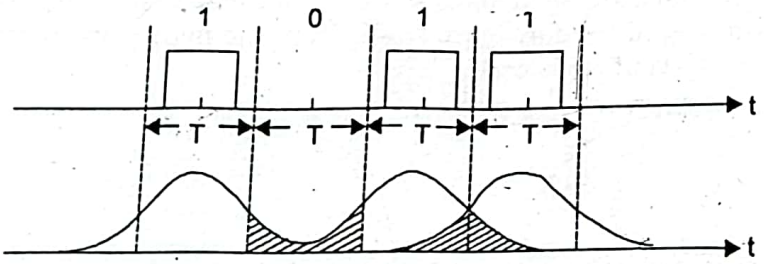


Fig. 1. Inter Symbol Interference.

Q.1. (d) What are the major functions performed by TCP? **(4)**

Ans. The objectives of a transport layer protocol include the setting up of an end-to d connection, end-to-end delivery of data packets, flow control, and congestion control. ere exist simple, unreliable, and connection-less transport layer protocols such as DP, and reliable, byte-stream-based, and connection oriented transport layer protocols ch as TCP for wired networks. These traditional wired transport layer protocols are t suitable for ad hoc wireless networks due to the inherent problems associated with e latter. The transmission control protocol (TCP) is the most predominant transport yer protocol in the Internet today. It transports more than 90% percent of the traffic n the Internet. Its reliability, end-to-end congestion control mechanism, byte stream ransport mechanism, and, above all, its elegant and simple design have not only ntributed to the success of the Internet, but also have made TCP an influencing protocol n the design of many of the other protocols and applications. Its adaptability to the

CamScanner

congestion in the network has been an important feature leading to graceful degradation of the services offered by the network at times of extreme congestion. TCP in its traditional form was designed and optimized only for wired networks.

Q.1. (e) Discuss the issues in designing a Transport Layer Protocol for Ad hoc wireless network. **(4)**

Ans. The various usues in designing transport layer protocol are: Induced traffic: Unlike wired networks, ad hoc wireless networks utilize multi-hop radio relaying. A link-level transmission affects the neighbor nodes of both the sender and receiver of the link. In a path having multiple links, transmission at a particular link affects one upstream link and one downstream link.

Induced throughput unfairness: This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layers such as the network and MAClayers

Separation of congestion control, reliability, and flow control: A transport layer protocol can provide better performance if end-to-end reliability, flow control, and congestion control are handled separately. Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity.

Power and bandwidth constraints

Misinterpretation of congestion: Traditional mechanisms of detecting congestion in networks, such as packet loss and retransmission timeout, are not suitable for detecting the network congestion in ad hoc wireless networks

Dynamic topology: Some of the deployment scenarios of ad hoc wireless networks about experience rapidly changing network topology due to the mobility of nodes

Q.1. (f) Why does TCP not work well in ad hoc network? Explain. **(4)**

Ans. Refer Q.4 (b) of First Term Exam 2017.

Q.1. (g) Discuss the load balancing in hybrid wireless networks. **(4)**

Ans. Load balancing refers to the distribution of relay traffic load uniformly throughout the network so that no region in the network is particularly overloaded. The need for load balancing arises from the fact that the amount of relay traffic (traffic relayed by a node) in a static multi-hop wireless network is dependent on the position of the nodes in the network and the node density in the region. As a result, the nodes close the center of the network need to relay more traffic than the nodes away from the center when the shortest path routing is used.

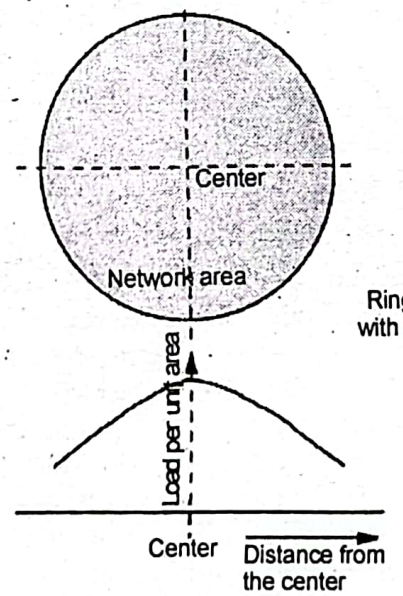
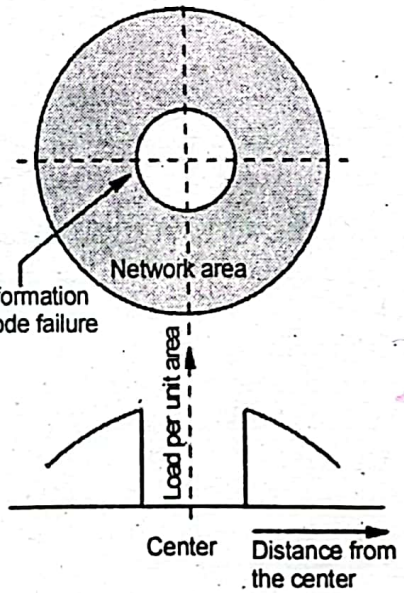


Fig. (a) Load density varies with distance from the center of the network



(b) Formation of ring due to the failure of nodes at the center of the network caused by excessive relay traffic

CamScanner

The load balancing is important in hybrid wireless networks such as MCNs, when the traffic locality is low (traffic locality is defined as the fraction of originated calls that gets terminated in the same cell). Traffic locality varies between 0 and 1, where locality = 0 refers to the case where the source and destination are in different cells and locality = 1 refers to a situation where all the calls get terminated within the cell. With low values of traffic locality, the probability that the BS will become saturated is high. Load balancing can improve performance in such situations.

UNIT-I

Q.2. Define AD HOC network. Explain in detail architecture of ad hoc network with its significant aspects. **(6.5)**

Ans. Ad hoc wireless networks are defined as the category of wireless networks that tilize multi-hop radio relaying and are capable of operating without the support of any xed infrastructure (hence they are also called infrastructure less networks). The bsence of any central coordinator or base station makes the routing a complex one mpared to cellular networks.

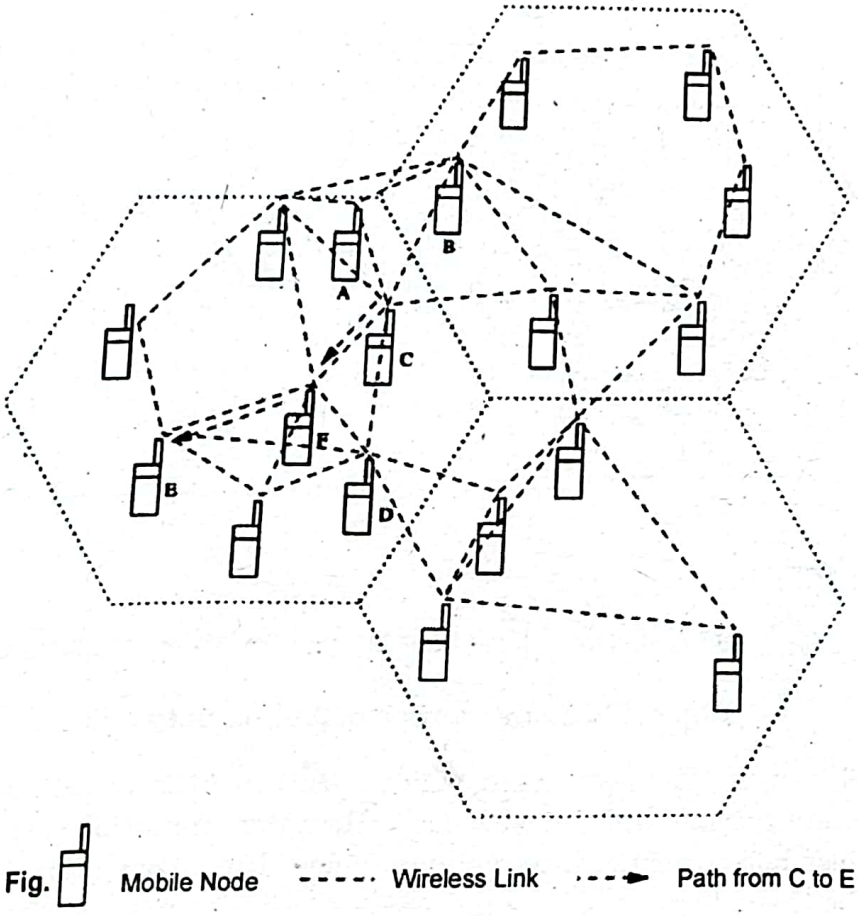


Fig. Mobile Node Wireless Link Path from C to E

d hoc wireless networks are defined as the category of wireless networks that utilize -hop radio relaying and are capable of operating without the support of any fixed tructure (hence they are also called infrastructure less networks). The absence of entral coordinator or base station makes the routing a complex one compared to ar networks. The rapid development in ad hoc technology is widely used in portable uting such as laptop, mobile phone used to access the web services, telephone calls the user are in travelling. Development of self-organizing network decrease the

communication cost. The growth of 4G technology enhances anytime, anywhere, anyhow communication in ad hoc network. Ad hoc network is simple to design and install. The advantages of an ad hoc network include: Separation from central network administration.

- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

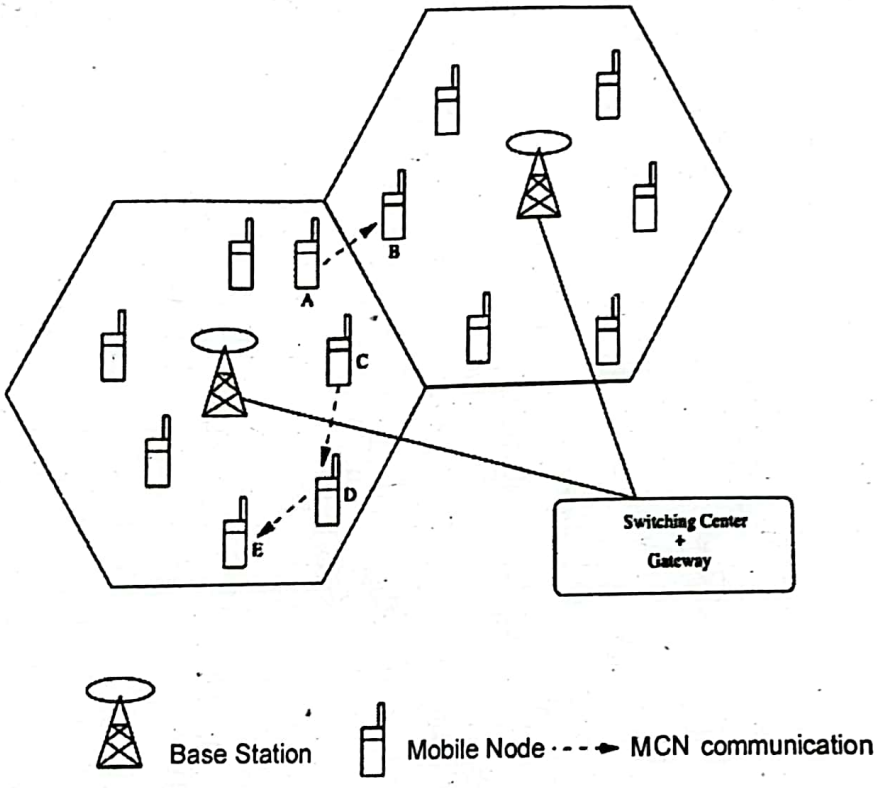


Fig: MCN Architecture of Adhoc network

In this architecture, when two nodes (which are not in direct transmission range) in the same cell want to communicate with each other, the connection is routed through multiple wireless hops over the intermediate nodes. The base station maintains the information about the topology of the network for efficient routing. The base station may or may not be involved in this multi-hop path. Suppose node A wants to communicate with node B. If all nodes are capable of operating in MCN mode, node A can reach node B directly if the node B is within node A's transmission range. When node C wants to communicate with node E and both are in the same cell, node C can reach node E through node D, which acts as an intermediate relay node. Such hybrid wireless networks can provide high capacity resulting in lowering the cost of communication to less than that in single-hop cellular networks.

CamScanner

Q. 2. (b) Explain the contention based protocols with scheduling and ervation in detail. **(6)**

Ans. Refer Q.2 (b) of End Term Exam Pg. 13-2017.

Q.3. (a) Explain the issues in designing a MAC protocol for ad hoc wireless tworks. **(6.5)**

Ans. The main issues in designing MAC protocol for ad hoc wireless network are:

ındwidth efficiency

- Bandwidth must be utilized in efficient manner.
- Minimal Control overhead
- BW = ratio of BW used for actual data transmission to the total available B W.

Quality of service support

- Essential for supporting time-critical traffic sessions.
- They have resource reservation mechanism that takes into considerations the ıre of wireless.
- Channel and the mobility of nodes.

Synchronization

- MAC protocol must consider synchronization between nodes in the network.
- Synchronization is very important for BW (time slot) reservation by nodes.
- Exchanges of control packets may be required for achieving time synchronization ng nodes.

Hidden and exposed terminal problems

- The hidden terminal problem refers to the collision of packets at a receiving node to the simultaneous transmission of those nodes that are not within the direct smission range of the sender but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without ning about the transmission of each other .

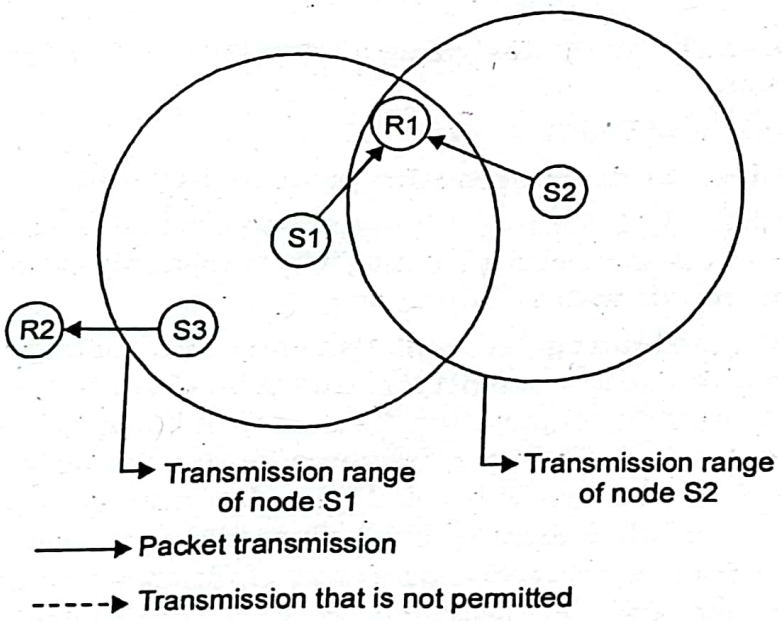


Fig. Hidden and exposed terminal problems

and S2 are hidden from each other & they transmit simultaneously to R1 which collision.

CamScanner

• The exposed terminal problem refers to the inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node.

• If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.

• The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high.

Error-prone shared broadcast channel

• When a node is receiving data, no other node in its neighbourhood should transmit a node should get access to the shared medium only when its transmission do not affect any ongoing session.

• MAC protocol should grant channel access to nodes in such a manner that collision are minimized.

• Protocol should ensure fair BW allocation.

• Distributed nature/lack of central coordination.

• Do not have centralized coordinates.

• Nodes must be scheduled in a distributed fashion for gaining access to the channel.

• MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high.

• Mobility of nodes.

• Nodes are mobile most of the time.

• The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility.

Q. 3. (b) classify the MAC protocol and what are the advantages of reservation based MAC ptorocol over contention based MAC protocol? (6)

Ans. Refer Q. 3 (a) & (b) of End Term Exam Pg.14-2017.

UNIT-II

Q. 4. (a) List the issues in designing a transport layer protocol for Ad Hoc wireless networks. (6)

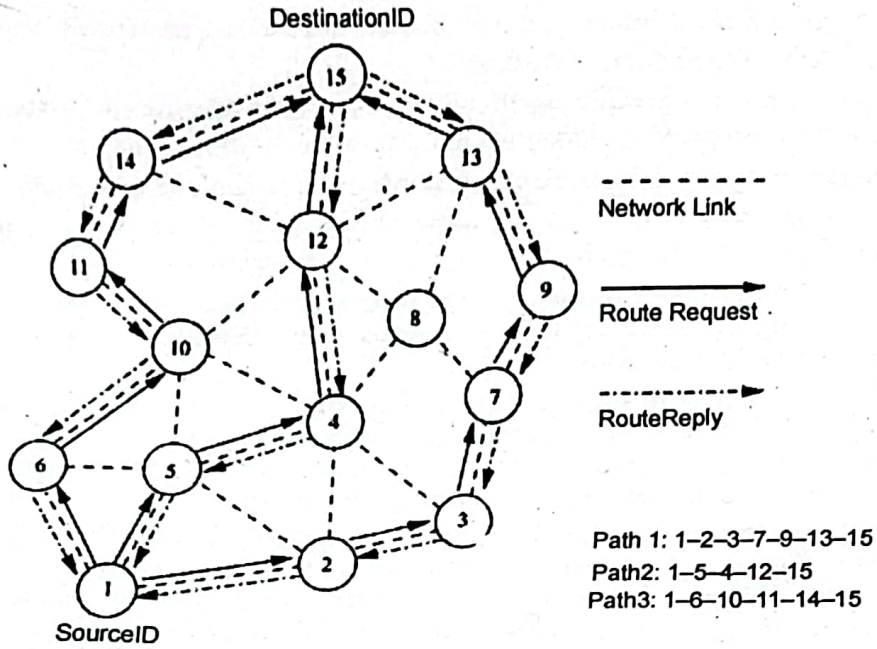
Ans. Refer Q.1. (e) of End Term Exam 2018.

Q. 4. (b) Explain the demand routing protocol in detail. (6.5)

Ans. Unlike the table-driven routing protocols, on-demand routing protocols execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination

Dynamic Source Routing Protocol: Dynamic source routing protocol (DSR)is an on-demand protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The major difference between this and the other on demand routing protocols is that it is *beacon-less* and hence does not require periodic *hello*packet (*beacon*) transmissions, which are used by a node to inform its neighbors of its presence. The basic approach of this protocol (and all other on-demand routing protocols) during the route construction phase is to establish a route by flooding *RouteRequest* packets in the network. The destination node, on receiving a *RouteRequest* packet, responds by sending a *RouteReply* packet back to the source, which carries the route traversed by the *RouteRequest* packet received.

CamScanner



Ad Hoc On-Demand Distance-Vector Routing Protocol:

Ad hoc on-demand distance vector (AODV) routing protocol uses an on demand proach for finding routes, that is, a route is established only when it is required by a rce node for transmitting data packets. It employs destination sequence numbers to ntify the most recent path. The major difference between AODV and DSR stems out n the fact that DSR uses source routing in which a data packet carries the complete h to be traversed. However, in AODV, the source node and the intermediate nodes e the next-hop information corresponding to each flow for data packet transmission. n ondemand routing protocol, the source node floods the *RouteRequest* packet in the ork when a route is not available for the desired destination. It may obtain multiple es to different destinations from a single *RouteRequest*. The major difference between V and other on-demand routing protocols is that it uses a destination sequence ber (DestSeqNum) to determine an up-to-date path to the destination. A node es its path information only if the DestSeqNum of the current packet received is r than the last DestSeqNum stored at the node.

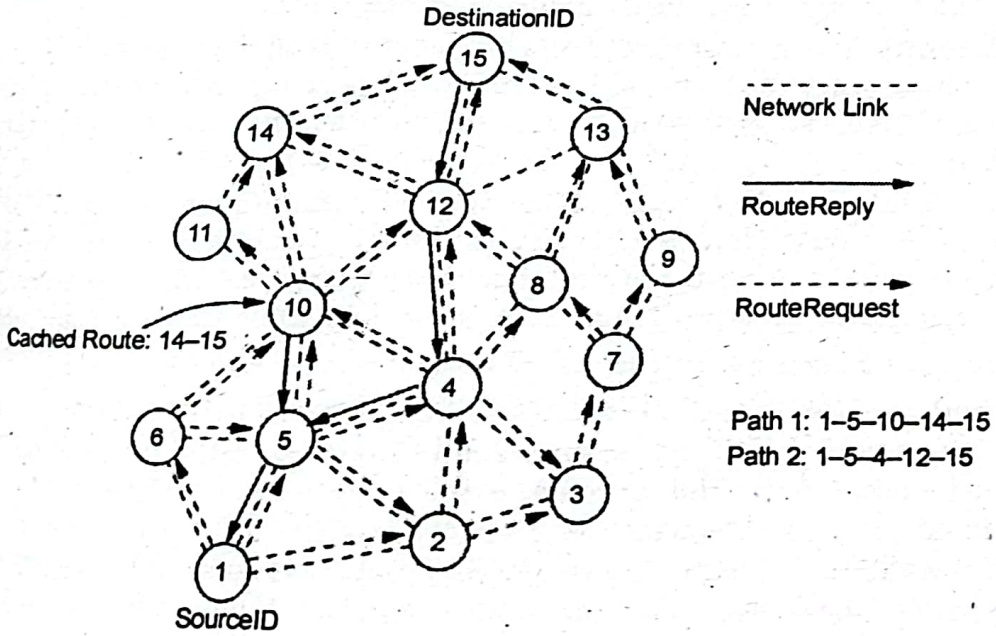


Fig. 2

CamScanner

Q.5 (a) Describe the types of ad hoc network routing protocol based on the routing information update mechanism. **(6)**

Ans. Ad hoc wireless network routing protocols can be classified into three major categories based on the routing information update mechanism. They are:

1. Proactive or table-driven routing protocols: In table-driven routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.

Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

2. Reactive or on-demand routing protocols: Protocols that fall under this category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. Hence these protocols do not exchange routing information periodically.

3. Hybrid routing protocols: Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located beyond this zone, an on-demand approach is used.

Q.5. (b) Why secure routing protocols are needed? List the issues and challenges in security provision of transport layer. **(6.5)**

Ans. Due to the unique characteristics of ad hoc wireless networks, such networks are highly vulnerable to security attacks compared to wired networks or infrastructure-based wireless networks. A security protocol for ad hoc wireless networks should satisfy the following requirements.

- **Confidentiality:** The data sent by the sender (source node) must be comprehensible only to the intended receiver (destination node). Though an intruder might get hold of the data being sent, he/she must not be able to derive any useful information out of the data. One of the popular techniques used for ensuring confidentiality is data encryption.
- **Integrity:** The data sent by the source node should reach the destination node as it was sent: unaltered. In other words, it should not be possible for any malicious node in the network to tamper with the data during transmission.
- **Availability:** The network should remain operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it. It should be able to provide the guaranteed services whenever an authorized user requires them.
- **Non-repudiation:** Non-repudiation is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Digital signatures, which function as unique identifiers for each user, much like a written signature, are used commonly for this purpose.

The issues and challenges in secure routing of ad hoc wireless networks are

- **Shared broadcast radio channel:** Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

CamScanner

• **Insecure operational environment:** The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

• **Lack of central authority:** In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations, and access points) and implement security mechanisms at such points. Since ad hoc wireless networks do not have any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

• **Lack of association:** Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

• **Limited resource availability:** Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

• **Physical vulnerability:** Nodes in these networks are usually compact and hand-held in nature. They could get damaged easily and are also vulnerable to theft.

UNIT-III

Q. 6 (a) Discuss the mechanism for location discovery. **(6)**

Ans. The location information of sensors has to be considered during aggregation of sensed data. This implies each node should know its location and couple its location information with the data in the messages it sends. A low-power, inexpensive, and reasonably accurate mechanism is needed for location discovery. A global positioning system (GPS) is not always feasible because it cannot reach nodes in dense foliage or indoors. It also consumes high power and makes sensor nodes bulkier. Two basic mechanisms of location discovery are

Indoor Localization: Indoor localization techniques use a fixed infrastructure to estimate the location of sensor nodes. Fixed beacon nodes are strategically placed in the field of observation, typically indoors, such as within a building. The randomly distributed sensors receive beacon signals from the beacon nodes and measure the signal strength, angle of arrival, and time difference between the arrival of different beacon signals. Using the measurements from multiple beacons, the nodes estimate their location. Some approaches use simple triangulation methods, while others require a preliminary database creation of signal measurements. The nodes estimate distances by looking up the database instead of performing computations. However, storage of the database may not be possible in each node, so only the BS may carry the database.

Sensor Network Localization: In situations where there is no fixed infrastructure available and prior measurements are not possible, some of the sensor nodes themselves become beacons. They have their location information, using GPS, and these send periodic beacons to other nodes. In the case of communication using RF signals, the received signal strength indicator (RSSI) can be used to estimate the distance, but this is very sensitive to obstacles and environmental conditions. Alternatively, the time difference between beacon arrivals from different nodes can be used to estimate location, if RF or ultrasound signals are used for communication. This offers a lower range of estimation than RSSI, but is of greater accuracy.

CamScanner

Q.6. (b) What are various design challenges in mobile Ad Hoc network and wireless sensor networks. **(6.5)**

Ans. Wireless Sensor Networks

• Sensor networks are special category of Adhoc wireless network that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain.

• Sensor nodes are tiny devices that have capability of sensing physical parameters processing the data gathered, & communication to the monitoring system.

The issue that make sensor network a distinct category of adhoc wireless network are the following:

1. Mobility of nodes

• Mobility of nodes is not a mandatory requirement in sensor networks.

• For example, the nodes used for periodic monitoring of soil properties are not required to be mobile & the nodes that are fitted on the bodies of patients in a post-surgery ward of a hospital are designed to support limited or partial mobility.

• In general, sensor networks need not in all cases be designed to support mobility of sensor nodes.

2. Size of the network

The number of nodes in sensor network can be much larger than that in a typical ad hoc wireless network.

3. Density of deployment

The density of nodes in a sensor network varies with the domain of application. For example, Military applications require high availability of the network, making redundancy a high priority.

4. Power constraints

The power constraints in sensor networks are much more stringent than those in ad hoc wireless networks. This is mainly because the sensor nodes are expected to operate in harsh environmental or geographical conditions, with minimum or no human supervision and maintenance.

In certain case, the recharging of the energy source is impossible:

• Running such a network, with nodes powered by a battery source with limited energy, demands very efficient protocol at network, data link, and physical layer.

The power sources used in sensor networks can be classified into the following three categories:

1. Replenishable Power source: The power source can be replaced when the existing source is fully drained.

2. Non-replenishable Power source: The power source cannot be replenished once the network has been deployed. The replacement of sensor node is the only solution.

3. Regenerative Power source: Here, power source employed in sensor network have the capability of regenerating power from the physical parameter under measurement.

5. Data/Information fusion

• Data fusion refers to the aggregation of multiple packets into one before relaying it.

• Data fusion mainly aims at reducing the bandwidth consumed by redundant headers of the packets and reducing the media access delay involved in transmitting multiple packets.

CamScanner

• Information fusion aims at processing the sensed data at the intermediate nodes nd relaying the outcome to the monitor node.

6. Traffic Distribution

• The communication traffic pattern varies with the domain of application in sensor etworks.

• For example, the environmental sensing application generates short periodic ackets indicating the status of the environmental parameter under observation to a ntral monitoring station.

• This kind of traffic requires low bandwith.

• Ad hoc wireless networks generally carry user traffic such as digitized & packetized oice stream or data traffic, which demands higher bandwidth.

Issues in ADHOC Wireless Netoworks

The major issues that affect the design, deployment, & performance of an ad hoc ireless network system are:

1. Medium Access Scheme.
2. Transport Layer Protocol.
3. Routing.
4. Multicasting.
5. Energy Management.
6. Self-Organisation.
7. Security.
8. Addressing & Service discovery.
9. Deployment considerations.
10. Scalability.
11. Pricing Scheme.
12. Quality of Service Provisioning.

Q.7. (a) What is hybrid rouling protocol? Describe hybrid routing protocol. **(6)**

Ans. Refer Q.7. (b) of End Term Exam Pg. 26-2017.

Q.7. (b) Explain the security issues in ad hoc wireless network. **(6.5)**

Ans. The issues and challenges in security of ad hoc wireless networks are.

• **Shared broadcast radio channel:** Unlike in wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc wireless networks is broadcast in nature and is shared by all nodes in the network. Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network. This problem can be minimized to a certain extent by using directional antennas.

• **Insecure operational environment:** The operating environments where ad hoc wireless networks are used may not always be secure. One important application of such networks is in battlefields. In such applications, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

• **Lack of central authority:** In wired networks and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations, and access points) and implement

CamScanner

security mechanisms at such points. Since ad hoc wireless networks do not have any such central points, these mechanisms cannot be applied in ad hoc wireless networks.

• **Lack of association:** Since these networks are dynamic in nature, a node can join or leave the network at any point of the time. If no proper authentication mechanism is used for associating nodes with a network, an intruder would be able to join into the network quite easily and carry out his/her attacks.

• **Limited resource availability:** Resources such as bandwidth, battery power, and computational power (to a certain extent) are scarce in ad hoc wireless networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

• **Physical vulnerability:** Nodes in these networks are usually compact and hand-held in nature. They could get damaged easily and are also vulnerable to theft.

UNIT-IV

Q.8. What is wireless geolocation? Discuss the technologies and standards for wirelesss gelocation. **(6.5)**

Ans. Refer Q.8 of End Term Exam Pg. 27-2017.

Q.9. Explain the following.

Q.9. (a) Wireless fidelity systems **(6)**

Ans. Refer Q.9 (a) of End Term Exam Pg. 29-2017.

Q.9. (b) Vehicular Sensor Networks:

Ans. Vehicular Sensor Networks (VASNET) inherits its characteristics from both Wireless Sensor Networks (WSN) and Vehicular Ad Hoc Networks (VANET). There is no infrastructure for VANET, therefore the vehicular nodes do perform data collection as well as data routing. Therefore, the necessity of designing a new architecture to overcome the mentioned challenges is transpicuous. VASNET is a fusion of WSNs and MANET, which can be divided in to three layers. The upper layer consisting of traffic monitor stations, e.g. traffic police located at the cities. These are connected by either fiber optic cables to form the backbone of traffic information network. The middle layer is region layer, consisting of traffic check post located through highways. These stations can be connected via the Internet or local networks, and finally the lower layer is the field layer, consisting of WSN nodes deployed on beside the highway and onboard sensors which are carried by the vehicles. These nodes are connected by short-range or medium-range wireless communication. The components are as follows:

(1) Vehicular Sensor Nodes; which are carried by the vehicles. These nodes are supposed to sense the real phenomena e.g. the velocity of the vehicle. The sensor readings are to be sent to the base stations via RSS nodes. These nodes can communicate with each other or the roadside sensor via short-range communication.

(2) Road Side Sensors (RSS); are deployed in a fixed distance beside the road. RSSs act as cluster heads for vehicular nodes. RSS nodes receive the data from mobile nodes and retransmit towards the BSs. These nodes are equipped with two kinds of antenna, unidirectional and bidirectional. Unidirectional antenna is for broadcasting and directional antenna are intended for geo-casting. We need to satisfy the following requirements for deploying the sensor nodes on a road side, such as; (a) high reliability, (b) long time service and (c) high real time.

(3) Base Station (BS); are Police Traffic Control Check-Post, Rescue Team Buildings or Fire Fighting Stations in some fixed point trough the roads. We can have mobile BS like, Traffic Police patrolling team, Firefighting Truck, or ambulance.

CamScanner