UNIT 3

Routing and MAC Protocols

Syllabus

Routing Protocols, MAC Protocols: Classification of MAC Protocols, S-MAC Protocol, B-MAC Protocol, IEEE 802.15.4 Standard and ZigBee.

Learning Objectives

- ✓ Various Design Issues of Routing Protocols
- ✓ Various Characteristics possessed by Routing Protocols
- ✓ Classification of Routing Protocols
- ✓ Different Classes of Routing Protocols
- ✓ Various Table Driven Routing Protocols
- ✓ Various On-demand Routing Protocols
- ✓ Different Hybrid Routing Protocols
- ✓ Design Issues of MAC Protocol
- ✓ Various Design Goals of MAC Protocol
- ✓ Classification of MAC Protocols
- ✓ Different Classes of MAC Protocol
- ✓ Introduction to S-MAC and B-MAC Protocols
- ✓ Introduction to IEEE 802.15.4 Standard and ZigBee.

Introduction

Routing Protocols can be defined as a set of rules that decides the path to be used for routing a packet from source router to the destination router. Routing Protocols are classified based on Routing information update mechanism, Use of temporal information, Routing topology and Utilization of Specific Resources.

MAC protocol can be defined as a protocol that allows access to a shared media network for multiple devices and also implement control packets to avoid collision. They are also classified based on Contention Based protocol, Scheduling Mechanism and Reservation Mechanism. And various classes of MAC protocols are Fixed assignment protocols, Demand assignment protocols and Random Access protocols.

PART-B ESSAY QUESTIONS WITH SOLUTIONS

3.1 ROUTING PROTOCOLS

Q9. Define routing protocol. Explain the classification of routing protocol.

Answer :

Routing Protocol

Routing protocol can be defined as a set of rules that decide the path to be used for routing a packet from source router to the destination router.

Classification of Routing Protocols

Classification of routing protocols in ad hoc wireless sensor networks is dependent on several reasons. It is not mutually exclusive and there exist some protocols which comes in more than one criteria. The criteria on which routing protocols are divided are as follows,

1. **Routing Information Based on Update Mechanism**

Routing protocols which are classified based on routing information update mechanism are as follows,

(i) **Table Driven (Proactive) Routing Protocols**

In table driven routing protocols, route information is exchanged periodically between different nodes. Hence, a routing table is always available with each node in the network. Generally, the entire topology is flooded with the routing information. Whenever a node requires a path to reach destination then it runs related pathfinding algorithm on the topology information maintained by that node.

Examples

- Destination Sequenced Distance Vector Routing (DSDV) Protocol
- Wireless Routing Protocol (WRP)
- Cluster-head Gateway Switch Routing (CGSR) Protocol
- Source Tree Adaptive Routing (STAR) Protocol.

(ii) **On-demand (Reactive) Protocols**

In on demand routing protocols, route information is not exchanged periodically between different nodes. That is, the information related to network topology is not maintained by the nodes. Hence, whenever a node requires a path to reach destination then it obtains through a connection establishment process.

Examples

- Dynamic Source Routing (DSR) Protocol
- Ad hoc On-demand Distance Vector Routing (AODV) Protocol.
- Temporally Ordered Routing (TORA) Protocol
- Associativity Based Routing (ABR) Protocol.

(iii) **Hybrid Routing Protocols**

Hybrid routing protocols combine the features of both table driven protocols and on-demand protocols. A table driven approach is used for the nodes that are within the routing zone (specific-geographical region) whereas on-demand approach is used for the nodes that are outside the routing zone.

2. **Use of Temporal Information for Routing**

Routing protocols which are classified based on the use of temporal information for routing depends on two categories.

(i) **Routing Protocols Using Past Temporal Information**

Protocols belonging to this category contains information regarding the past status of the links. It also provides information of the links at the time of routing to make routing decisions. For example, during the process of path-finding algorithm, an efficient and stable path is provided by the routing algorithm along with its shortest path-finding algorithm. Any topological changes may effect the path and may also lead to its breakage. Thus, making the path to go through a resource-wise expensive path reconfiguration process.

(ii) **Routing Protocols Using Future Temporal Information**

Protocol in this category uses information regarding future status of the links to provide good routing decisions. The information of future status contains not only the lifetime of wireless links but also the lifetime of its node.

3. Classification Based on the Routing Topology

In adhoc wireless networks, classification of routing protocols based on the routing topology depends on the number of nodes. It contains smaller number of nodes that is why it utilizes either flat topology or hierarchical topology.

(i) Hierarchical Topology Protocols

It utilizes an addressing scheme and logical hierarchy to decrease the maintenance cost in the internet. In order to maintain hierarchy in the network it needs either a geographical information or hop distance.

(ii) Flat Topology Protocols

It utilizes a flat addressing scheme which is same as addressing scheme of IEEE 802.3. It makes an assumption that all the nodes in the protocol have a unique address.

DSR and AODV are the examples of Flat topology protocols. Where as, Cluster-head Gateway Switch Routing (CGSR) Protocol is an example of Hierarchical topology protocols.

4. Utilization of Specific Resources

(i) Power Aware Routing

Power aware routing determines MANETs routing by using power-aware matrixs. These matrixs reduces the cost of packet routing by five to thirty percentage compared to shortest-hop routing. They also reduce energy consumption by forty to seventy percentage compared to MAC layer protocol. Besides reducing cost and energy consumption, they make sure that packet delays do not increase the mean time node failure.

(ii) Geographical Information Assisted Routing

It effectively utilizes geographical information to enhance the performance of routing and decreases the overhead.

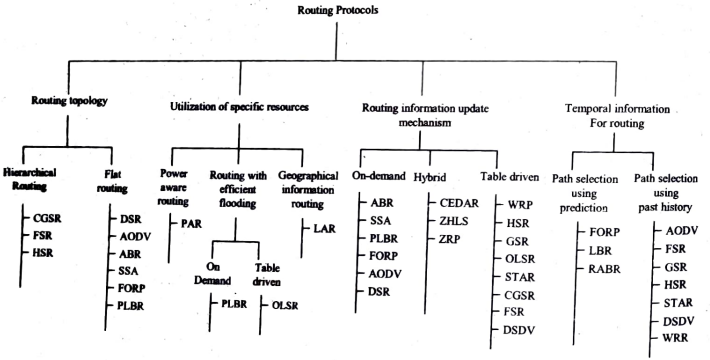


Figure: Classification of Routing Protocols

Q10. Mention the characteristics that should be possessed by routing protocols for adhoc wireless networks.

Answer :

The characteristics that should be possessed by routing protocol are as follows,

1. It should have the capability of handling modifications done in the topology information when nodes are moving from one place to another.
2. It should follow the routes which are error free and do not contain congestion.
3. It should completely adopt distributed routing but not centralized routing. Because centralized routing contains control overhead and does not support scalability whereas distributed routing is fault-tolerant and holds the possibility of single point failure but not all nodes.
4. It should try to use the limited resources like battery power, computing power and bandwidth in an efficient manner.
5. It should use local nodes instead of global nodes as it requires global state maintenance which contains an overhead.
6. It should impose some limit on every broadcast made by a node in order to avoid collision of packets.
7. It should also assure about the reliability of the transmissions which are being made by a node in order to avoid loss of data and to ignore state routes.
8. It should have the stability while maintaining the topology information and should not effect the stability even when changes are done.
9. It should maintain quality of service as required by the applications and should easily handle time-sensitive traffic.
10. It should acquire less amount of connection setup time and provide quick access to routes. It should involve few nodes in maintenance and computation.

Q11. Discuss the issues in designing a routing protocol for Adhoc wireless networks.

Answer : Model Paper-II, Q8(a)

Some of the issues faced while designing routing protocols for adhoc sensor networks are,

1. **Hidden Terminal Problem**

The collision of packets at receiving node occurs due to the simultaneous transmission of the nodes which are out of direct transmission range of sender and are in the transmission range of receiver. This type of collision occurs when both the nodes transmits at same point of time. It reduces the throughput of the network when the traffic load increases.

2. **Exposed Terminal Problem**

Exposed terminal problem occurs when a node gets blocked due to its incapability of transmitting node (nearby node) to transmit data to other node.

3. **Mobility**

Wireless sensors can be easily made to move from one region to another by rearranging the nodes of the network. Rearrangement of nodes takes place when a region of the network becomes unmonitored and therefore the node is shifted to the unmonitored region. But wireless networks have limited mobility when compared to adhoc networks, because they are equipped with batteries.

4. **Bandwidth Constraint**

Wireless routing protocol has a bandwidth constraint which leads to difficulties in maintaining topological information because as the changes are made is topology, it should be updated and should be consistent at all the nodes present in the network which consumes more bandwidth.

5. **Resource Constraint**

There are two resources i.e., battery life and processing power in adhoc wireless networks which have limitations. On the other hand, adhoc wireless network supports portability which have size and weight constraints. Thus, they are inversely proportional to each other with increase in processing power and battery power, there is a decrease in portability of the nodes.

6. **Error-prone Links**

Adhoc wireless networks face major difficulties due to its broadcast nature of the radio channel. It supports different features of link capacity and link error probability at different situations. This problem can be overcome by communication of adhoc routing protocol with MAC layer which determines routes that are error free.

Q12. What are the different classes of routing protocols?

Answer : Model Paper-I, Q8

Classes of Routing Protocols

There are two different classes of routing protocols. They are,

(i) Distance Vector Routing

Distance vector routing algorithm uses a routing table maintained by each router in a subnet for routing. Each router maintains a table (i.e., a vector) containing the information about the best known distance to each destination and the next hop to be followed to reach that destination. The metric used for routing could be the number of hops, the queue length or the time delay in milliseconds. The tables are updated by exchanging vectors to directly connected neighbours.

It is assumed that each router knows the distance to each of its directly connected neighbours. The distance is one hop if the metric is in hops, the distance is the number of packets per queue if the metric is in queue length. The router determines the distance to the time delay metric by sending a special ECHO packet to its neighbour which responds to it as fast as possible after the receiver time stamps.

If the delay metric is used then the router knows the time delay to reach each of its neighbors. After every T msec routers exchange their vectors to update their tables with newly estimated delay to each destination. Assume that the estimated delay of router X to reach the router i is X_i. The router knows, delay to reach the router X itself is m msec then the delay to reach to router i via X is $(X_i + m)$ msec.

The router calculates the estimated delay for each neighbor and chooses the best estimated delay which is the lowest value. The router uses this delay and its corresponding line in its new routing table.

For example consider the following subnet.

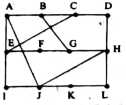


Figure (a): Example Subnet

Each router exchange their delay vector. Suppose that the router B receives the delay vectors from its neighbors A, C and G as shown in figure (b). A's delay vector shows that it can reach to router B in 12 msec, to router C in 20 msec, to router D in 9 msec etc. Suppose B's estimated delays to its neighbors A, C and G are 6 msec, 4 msec and 12 msec respectively.

Delay to →	A's Vector	C's Vector	G's Vector
A	0	22	9
B	12	11	22
C	20	0	30
D	9	20	19
E	25	31	8
F	20	16	19
G	9	7	0
H	10	27	31
I	23	36	20
J	18	18	7
K	40	24	9
L	14	11	16
	B – A : 6	B – C : 4	B – G : 12

B's Estimated Delays

Figure (b): Delay Vectors Received by B

To	New estimated delay	Next hop
A	6	A
B	0	-
C	4	C
D	15	A
E	20	G
F	20	C
G	12	G
F	16	A
I	29	A
J	19	G
K	21	G
L	15	C

Figure (c): New Routing Table for B

Now, consider how the router *B* uses distance vector routing to compute its new route to router *F*. Router *B* knows its delay to its neighbour *A* is 6 msec which can reach to *F* in 20 msec. The total delay is 6 + 20 = 26 msec, if *B* forwards the packets bound for *F* via *A*. Similarly it calculates the delay via *C* and *G*. The delay via *C* = 4 + 16 = 20 msec. The delay via *G* = 12 + 19 = 31 msec. The best estimated delay is 20 msec which is possible if *B* forward packets via *C*. So, *B* makes an entry in its routing table the delay to *F* as 20 msec and the next hop to choose as *C*. Similarly the same calculation is used to calculate the delay to each destination using new routing table as shown above.

(ii) Link State Routing

Link state algorithm is a dynamic routing algorithm that takes into account the complete network topology, all delays and bandwidths when choosing routes. In this algorithm each router does the following.

1. Learn about its neighbours and their addresses.
2. Measure the line cost to each of its neighbours.
3. Build packets containing information it learned.
4. Distributes packets to all other routers.
5. Compute routes with shortest path to every other router.

The link state algorithm uses the Dijkstra's algorithm to find shortest path. The above five steps are discussed here in detail.

1. **Learn about Neighbours**

When a router joins the network, it first learns about its neighbours. To achieve this, it sends a special HELLO packet on each outgoing line that commence from it. When the packet arrive at the receiver, each receiver reply to it by telling its identity. The routers are named uniquely to avoid any conflicts.

2. **Measure the Line Cost**

Next, the routers must estimate the delay to reach each of its neighbours. To know this delay the router send a special ECHO packet on each point-to-point line. The router on the other end sends back it immediately. The router calculate the delay by dividing the round-trip time (the time a packet take to reach to destination router and come back) by two. To get better estimation of the delay, the ECHO packet can be send several times and use the average.

If the traffic load is to be taken into account when measuring the delay, the round-trip time should be started when ECHO packet is queued on the router, otherwise it should be started when ECHO packet is on top of the queue. Taking the load into account measuring delay results in better performance because a router having a choice between two lines with the same bandwidth can route the packets on the line with small load treating it as a shorter path rather than routing it on the heavily loaded line. The problem with including load into delay calculation is that routing tables will keep on changing, router sends all of its traffic over line with low load thus overloading that line as a consequence updating the routing table. The problem can be avoided by taking the bandwidth into account and ignoring the load.

3. **Build Link State Packets**

Once the router gets the information about its neighbours it calculates its delay to them, the next step for each router is to construct a packet including all the information it learned. The packet includes the identity of the sender, the sequence number and age, followed by the list of each of its neighbours with its delays to them.

For example consider the subnet shown in figure (d). The link state packets that each router construct for this subnet is shown in figure (e).

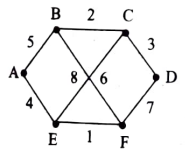


Figure (d): An Example Subnet

A	
Seq.no	
Age	
B	5
E	4

B	
Seq.no	
Age	
A	5
C	2
F	6

C	
Seq.no	
Age	
B	2
D	3
E	8

D	
Seq.no	
Age	
C	3
F	7

E	
Seq.no	
Age	
A	4
C	8
F	1

F	
Seq.no	
Age	
B	6
D	7
E	1

Figure (e): Link State Packets

The link state packets are easy to build. They can be constructed periodically or in response to some events such as a neighbour is going down or coming back up again or has changed its properties.

4. **Distributing Link State Packets**

The next step after building link state packets is to distribute them across the network. Flooding is used as the basic algorithm for distributing link state packets. To avoid flooding the same packet, each new packet is given a sequence number. When a packet arrives at a router for flooding then it checks whether this packet is already seen by using a pair (source router, sequence number) that each router have.

If the duplicate packet arrives then it is discarded otherwise it is sent on all outgoing lines except the one it arrived on. If a packet with lower sequence number arrives after seeing a packet with highest number then it is rejected as being obsolete.

Each router uses a data structure with the field source router, packets sequence number and age, send flags, acknowledgment flags and the data. The age field is included after the sequence number and it is decremented once per second. It also decrement by each router after the commence of flooding to ensure that no packet can get lost and wander aimlessly in the subnet for an infinite time. Once the age becomes zero, the router discards the information from it.

The send flags specify the line on which to send the incoming packet and the acknowledgment flags specify the line on which an acknowledgment is to be sent.

The table below shows the data structure for router *C* for the subnet shown in figure (a).

Sender	Seq. no	Age	Send flag		ACK flags		Data	
			B	D	E	B	D	B
A	15	59	1	0	1	0	1	0
B	15	60	0	1	1	1	0	0
F	15	60	0	1	0	1	0	1
E	14	59	1	1	0	0	0	1
D	15	60	1	1	0	0	0	1

Table: Data Structure for Router C

Send flags for the first row indicates that the packet came from *A* directly, so it should be routed to *B* and *E* and acknowledged to *D* as indicated by the acknowledged flags.

The third row indicates that packet arrived twice, once via FBC and once via FEC is to be sent to *D*. But it must be acknowledged to both *B* and *E*.

If the duplicate packet arrives while the original packet is still in the buffer, in that case bits will change.

5. **Compute the New Routes**

Once flooding is done and a router has gathered a set of link state packets, a router builds a graph for the subnet representing each link twice one for each direction. The value on links can be averaged or used separately.

The link state algorithm uses the Dijkstra's algorithm to compute the shortest path to all possible destinations. The routing tables store this result and normal operation is resumed.

Q13. Explain in detail the different table-driven or proactive routing protocols.

Answer : Model Paper-II, Q6(b)

The various proactive or table-driven routing protocols are as follows,

1. Destination-Sequenced Distance-Vector (DSDV).
2. Wireless Routing Protocol (WRP).
3. Topology Broadcast based on Reverse Path Forwarding (TBRPF)
4. Multipoint relays
5. Source Tree Adaptive Routing (STAR) protocol.

1. Destination-Sequenced Distance-Vector (DSDV) Protocol

DSDV is an improved routing protocol of the distributed Bellman-Ford routing algorithm. In this protocol, a table consisting of the shortest distance and the starting node of the shortest path is maintained at every node. Table updates are done with the increasing sequence number provided so as to,

- Prevent loops
- Provide a faster convergence
- Avoid the count-to-infinity problem.

Every node in the table-driven routing protocol has a route to destination. The tables are exchanged periodically among the neighbouring nodes, so that an up-to-date view of the topology is maintained. If a node sees a change in the network topology, then also the table is forwarded to its neighbor. The table updates are classified into the following types,

(i) **Incremental Update Packet:** Incremental update packet hold only a single Network Data Packet Unit (NDPU) and are used wherever a change is not seen by the node in the topology.

(ii) **Full Dump Packet:** Full dump update packet hold various NDPUs and are used wherever a significant change occurs in the network topology or when more than one NDPU is required by an incremental update.

A destination has the capability of performing the table updates by providing sequence number that is greater than the previous given numbers at all times.

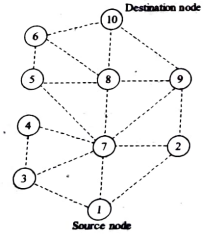


Figure (1): Network Topology

Destination node	Next node	Shortest distance	Sequence number
2	2	1	18
3	3	1	24
4	3	2	28
5	7	2	34
6	7	3	42
7	7	1	50
8	7	2	82
9	2	2	94
10	2	3	102

Table (1): Routing Table for Node 1

In figure (1), node 1 is the source node and node 10 is the destination node. Table (1) indicates that the topology information is associated with all the nodes in the network. Here, the shortest route to reach destination from node 1 to node 8 can be obtained via node 7 and the shortest distance is 2 hops as shown in table (1). Similarly, the shortest route and shortest distance from node 1 to node 2, 3, 4, 5, 6, 7, 8, 9, 10 is depicted in table (1). The next node in the routing table signifies the starting node on the shortest path from source to destination and an even sequence number is given to all the nodes in the increasing order.

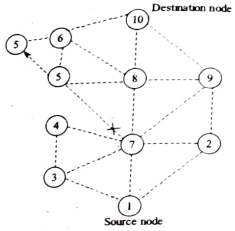


Figure (2): Reconfigured Path in the Topology

Destination node	Next node	Shortest distance	Sequence number
2	2	1	18
3	3	1	24
4	3	2	28
5	7	4	38
6	7	3	42
7	7	1	50
8	7	2	82
9	2	2	94
10	2	3	102

Table (2): Updated Routing Table

In figure (2), when the link of node 5 breaks, then paths that are passing through that link are assigned to infinity (∞) and all its neighbors are informed about the changes in the routing table. When an update message is sent from node 5 to node 6, then its neighbors are informed regarding the shortest distance to node 5 i.e., 4 hops. Thus, in the updated table, table (2) the shortest distance from node 1 to node 5 has increased from 2 hops to 4 hops. And also, the sequence number of node 5 is assigned with a new number greater than the previous one. This information is also broadcasted to the entire network.

Advantages

- Delays are not larger since the routing is available for each and every individual destination at any instant.
- The existing wired network protocols are easily modified to adhoc wireless network. Since the routing tables contains incremental updates.
- An up-to-date view is preserved by all the nodes in the topology.

Disadvantages

- It has a heavy control overhead.
- It does not possess any stability factor.
- It consumes more time for acquiring information regarding the particular destination.

2. Wireless Routing Protocol (WRP)

The distributed Bellman-Ford properties are inherited by WRP, which is similar to DSDV. WRP uses a unique method of maintaining the information about the shortest distance and penultimate node on the path to all destination nodes in the network. This method performs a faster convergence and avoids the count-to-infinity problem. Similar to DSDV, the nodes present in WRP also contain a route to all destination nodes in the network topology. But the difference is that, WRP has a unique table maintenance and update techniques. Also, a set of tables are employed by WRP, so that more accurate information about the routing is maintained. A node maintains the following tables,

(i) **Distance Table (DT):** Distance table has the network view of the neighbors of a particular node. It also comprises of a matrix wherein every element maintains the distance and the penultimate node for a destination informed by a neighbouring node.

(ii) **Routing Table (RT):** Routing table has an up-to-date view of the topology for every known destination. It maintains the shortest distance, penultimate (predecessor) node, next (successor) node and a flag specifying the path status which may be a loop (error), simple path (correct) or the unmarked destination node (null).

(iii) **Link Cost Table (LCT):** Link cost table contains the cost of the relaying messages placed via every link. Usually, the broken link's cost is infinity (∞). LCT also maintains the number of update periods occurred after the recent successful update obtained from that link. This information helps in identifying the link breaks.

(iv) **Message Retransmission List (MRL):** Message retransmission list maintain entries for all the update messages which are used for retransmission. In MRL, a counter is also maintained for all the entries and this counter depends upon an update message that is to be retransmitted.

A set of updates are present in every update message. Whenever, an update message is transmitted, an acknowledgment is sent by a node, which is marked in the RT. The unacknowledged entries on the update message are retransmitted as soon as the counter becomes zero. This results on the deletion of the update message. Hence due to this, a broken link is detected. Moreover, convergence in DSDV is much quicker when an update message is received by a node which updates and checks the distance for the transmitted neighbors and the other neighbors respectively.

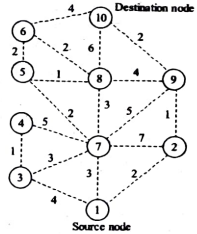


Figure (3): Routing Network in WRP

Node	Successor node	Predecessor node	Cost
10	10	10	0
9	10	9	2
8	10	8	6
7	9	9	7
6	10	6	4
5	6	6	6
4	7	9	12
3	7	9	10
2	9	9	3
1	2	9	5

Table (3): Routing Table in WRP

Figure (3) represents the routing topology wherein node 1 is the source node and node 10 is the destination node. The route from node 3 to 10 in the topology has node 7 as the successor node and node 9 as the predecessor node. The cost of this routing (i.e., from node 3 to node 10) is 10. And, during the link breaks, the predecessor information is used for an easier and faster convergence.

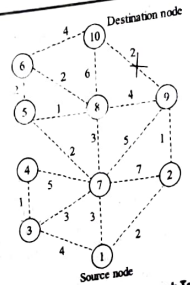


Figure (4): A Link Break in the Network Topology

Node	Successor node	Predecessor node	Cost
10	10	10	0
9	8	8	10
8	10	8	6
7	5	6	8
6	10	6	4
5	6	6	6
4	7	6	13
3	7	6	11
2	1	8	14
1	7	6	11

Table (4): Updated Routing Table

In figure (4) the link between the nodes 9 and 10 breaks. Hence in table (3) the entries with the predecessor node as 9 are deleted and a new updated table is created, as shown in table (4). Now, the cost between nodes 9 and 10 becomes infinity. This information is send to their neighbors and in order to reach the destination node 10, alternative routes are adopted by transmitting an update message. In figure (4), node 9 has a route to destination node 10 through node 8. Hence, this changed path information is broadcasted to the entire network. The nodes that have a route through node 9 modify their paths and choose an optimal path to the destination node 10. In figure (4), node 1 changes its path by considering the successor node as 7 and predecessor node as 6. Hence, the cost also changes from 5 to 11.

Advantage

WRP helps in quicker convergence during the link breaks.

Disadvantages

- The routing updates are difficult to maintain and require huge processing power and memory from the nodes.
- A greater control overhead exists in the updated routing table. Due to this, WRP is an appropriate protocol for very large and highly dynamic ad hoc wireless networks.

3. Topology Broadcast based on Reverse Path Forwarding (TBRPF) Protocol

TBRPF is a simple and practical protocol. It assumes every node of a network as broadcast topology information problem.

Routing based on link state is computed by using information of broadcast topology along with path selection algorithm. Link state routing protocols use flooding i.e., each link state update is transmitted to every link of network. This flooding works well in high bandwidth links. However, in networks with lower bandwidth, flooding does not work.

If spanning trees are used instead of flooding the network with update information, the cost of communication can be reduced despite of a marginal maintenance cost associated with spanning tree.

TBRPF is based on Extended Reverse Path Forwarding (ERPF) algorithm. In ERPF algorithm messages are broadcasted with directing spanning trees in reverse direction. The spanning trees are created by shortest path to the source for all the nodes. ERPF consider applying underlying routing algorithms for every node (b) in selecting next node $A_b(c)$ with shortest path for every broadcast source. This node $A_b(c)$ is considered b's parent at source c on the broadcast tree.

Further, every parent of node is informed about selection to keep updated about children of the source. A node b that receives broadcast message from source C from its parent $A_b(c)$ forwards the message to its children from C.

The ERPF algorithm does not work when the short path is vulnerable to change. Therefore, the underlying routing algorithm cannot be dependent to broadcast messages using ERPF.

TBRPF achieve reliability by integrating ERPF with sequence numbers and minimum-hop path computation of topology information. This information is received from source with broadcast tree. The minimum-hop path is already computed and every source node broadcast link-state upgrades its outgoing links with source minimum-hop tree. As a result of this computation and upgradation, each source get a separate broadcast tree. The application of minimum-hop tree results in few changes that occur frequently in broadcast ultimately reducing communication cost of trees.

TBRPF performs computation of broadcast tree paths on the basis of information received from trees. Therefore, the integrity of TBRPF is hard to determine. However, every mobile host is aware of appropriate topology when topology remains static.

Advantages

- It is very simple and feasible protocol.
- It produces low traffic when compared to flood.
- It is used in networks whose bandwidth is limited and topology is rarely modified.

4. Multipoint Relays

A multipoint relay (MPR) of a node in a network is a mobile host that chooses few neighboring mobile hosts for retransmitting data packets. A neighbor of a node that is not chosen in its MPR list if receives data packets, it does not retransmit them.

Further, any message from MPR selection of a given node is considered as a retransmitted message of that node. This set of host is changed over a period of time and is informed by the selected node using hello messages.

The set of multiple relays is selected by energy node from its neighbors who are one hop away in a manner such that the selection covers two hop away nodes. Moreover, optimal routing is achieved hen the multiple relay is smaller in size.

A typical m tipoint relay selection of mobile host k is depicted in figure (5).

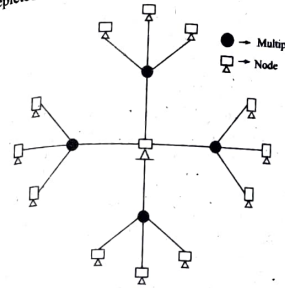


Figure (5): Multipoint Relay in a Network

Advantages

- Multipoint relays reduces the broadcast packets in a network by minimizing retransmission of duplicate data packets in same area.
- They select one-hop neighbor that contains bidirectional link. This eliminates the problems associated with unidirectional links for transmitting data.

5. Source Tree Adaptive Routing (STAR) Protocol

STAR is an adaptive version of table-driven routing protocols. In this protocol, instead of an Optimum Routing Approach (ORA), the Least Overhead Routing Approach (LORA) is applied. The ORA protocols were employed by the previously table-driven routing protocols. These protocols update the routing information that provide efficient paths in accordance to the specified metric. But, LORA contain less control overhead and provide some feasible paths which may be inefficient. The source-tree information of each node in STAR is transmitted to the entire network. This information contain wireless links in its routing path to reach destination. A partial graph of the network topology is created by,

(i) The adjacent links of each node

(ii) The source-tree information transmitted through the neighbors of each node.

At the time of initialization, an update message is broadcasted to all the neighbors of a node and each node is used so as to create update messages regarding new destinations, chances of routing loops occurred and paths cost that is more than the specified threshold. Thus, a path exists from every node to every destination but, mostly the paths may be sub-optimal.

When there exists no path (i.e., a reliable link layer broadcast mechanism) from node to destination, the following path-finding technique is used by STAR. A node 'i' attempts to send the data packets to a specific destination 'j' but there exists no path in its source-tree and hence an update message is created by it and transmitted to all its neighbors by specifying the absence of a path to destination 'j'. This update message inturn generates another update message from its adjacent node that contains the information about the route to reach destination. The update message is retransmitted periodically from node 'i' until a path is not received by it to destination j. The source-tree of node 'i' is updated upon receiving the source-tree update from its neighbor. Hence, this is used to determine a path to all nodes in the network topology. To avoid the formation of routing loops, the data packets must comprise of the information regarding the paths that are need to be traversed.

If a reliable broadcast technique exists in STAR, then the maintenance of routing is implicitly done. The link update message (regarding the absence of a next-hop node) is used to trigger an update message from a neighbor. This neighbor contains another source-tree which signifies another next-hop node to destination. The routing loops are handled not only by the path breaks, but also by the intermediate nodes in the topology. If a data packet is send from a node to the intermediate node 'n' to reach the destination j and a node existing in the packet's traversed path is also available in the path of the node n, then that packet is removed, thereby transmitting a RouteRepair update message to the node present in the head of the route repair path. This path is related to the path that exists from node n to 'r', where 'r' represents the final routes present in the traversed path of the data packet. This traversed path is initially determined in the path 'n' to 'j' which is associated with the k's source tree. Both the packet's traversed path and the k's entire source tree is present in the RouteRepair packet.

An intermediate node is discarded from the top of the route repair path and is transmitted reliable to the head of the route repair path. This is done when a RouteRepair update message is received by that intermediate node.

Advantage

The control overhead in STAR is very less, when compared to all the other table-driven routing protocols.

Disadvantage

The average control overhead in STAR is minimized when compared to the other on-demand routing protocols. This is because of the usage of the LORA mechanism.

Q14. Write notes on the on-demand routing protocols.

Answer :

The various reactive or on-demand routing protocols are,

1. Dynamic Source Routing (DSR)
2. Adhoc On-demand Distance Vector (AODV)
3. Temporally Ordered Routing Algorithm (TORA).

1. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is an on-demand routing protocol which is developed for controlling the bandwidth used by the control packets in the adhoc wireless network. This can be done by periodically removing the table update messages used in the table-driven method. This protocol is different from the other routing protocols because it restricts the sending of hello/beacon packets periodically for identifying its presence to the neighbors.

During the construction phase of routing, the key feature of DSR is that, a route should be created with the help of flooding RouteRequest packets in the topology. A RouteRequest packet is send by a source to destination, which inturn sends a RouteReply packet to the source. This packet contains the information about the route that is to be traversed through the received RouteRequest packet.

Suppose, if there exists no route from source node to destination node and data packets are required to be transmitted to the destination, then a RouteRequest packet is triggered. This packet is flooded across the entire network and after receiving the packet by every node in the topology, it is retransmitted to its neighbors. This retransmission is done when the RouteRequest packet has not been transmitted before or when the received node is not the destination and also based upon the packet's Time To Line (TTL) counter which has not been exceeded. The source node creates a sequence number and a traversing path which are send along with every RouteRequest packet. After receiving this packet, the node examines the sequence number before transmitting it to the destination node. If the packet is not a duplicate RouteRequest, then it is broadcasted. The RouteRequest packet has a sequence number which restricts the following,

(i) Formation of loop routing.

(ii) Retransmission of RouteRequest packets that are similar. This can be done by making use of intermediate node via different routing paths.

Hence, during the construction phase of routing, a RouteRequest packet is send to every node in the topology except the destination node. When the first RouteRequest packet is received by a destination node, then this node responds to the source node by the reverse path that had traversed the RouteRequest packet.

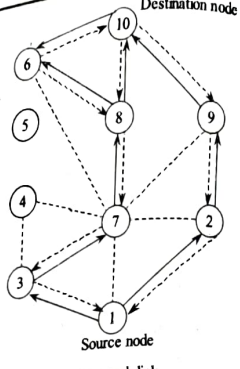


Figure (1): Routing Network in DSR

In figure (1), a RouteRequest packet is triggered from source node 1, so that a path is obtained for the destination node 10. The following paths are used to transmit the RouteRequest packet.

Path 1 : 1 – 2 – 9 – 10

Path 2 : 1 – 3 – 7 – 8 – 10

Path 3 : 1 – 3 – 7 – 8 – 6 – 10

A data packet contains the information which is gathered from the source route. This information is stored in a route cache employed by the DSR protocol. In the promiscuous mode (i.e., the mode in which the received packets can neither be broadcasted nor addressed), the information about the neighboring routes over which the data packets are transmitted are known to the source node. During the construction phase of routing, the route cache can be used. A RouteRequest packet is send to an intermediate node and if this node receives the packet and contains a route path to the destination present in its route cache, then the intermediate node transmits a RouteReply back to the source node along with the complete routing information obtained from source to destination.

Optimizations

DSR protocol includes different optimization methods in order to improve its performance. It make use of route cache for the intermediate nodes. It consist of routing information that are restored from the data packets which are to be transmitted. After receiving a route request packet and verifying the destination route, the intermediate node uses the route cache information and reply to the source node. When an intermediate node is performed in the promiscuous mode, then it gains the knowledge about the route breaks. Hence, this information is used for the route cache updation so that the routes available in the route cache does not use broken links. While partitioning the network into various sets, the affected nodes trigger the RouteRequest packets. If the destination exists in a different disjoint set and

the RouteRequest packets are frequently flooding in the network, then in order to prevent this, an algorithm called exponential backoff is employed. A data packet can be transmitted with the RouteRequest packets. This is because of the DSR protocol, that permits the piggy-backing to be performed on the RouteRequest.

When no optimization is granted in the DSR protocol, then the construction phase of routing is very easy to built. The redundant or duplicate RouteRequest packets are not flooded by the intermediate nodes.

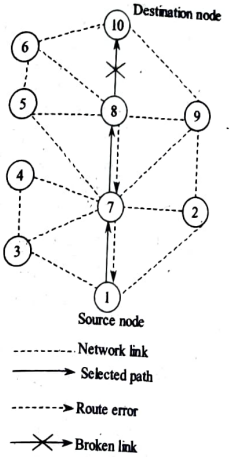


Figure (2): A Link Break in DSR Topology

In figure (2), node 1 sends the RouteRequest packet to all its neighbouring nodes i.e., nodes 2 and 3. These two nodes forward the packet, which is received by the node 7. This node receives two RouteRequest packets and the one which is received first is accepted and forwarded, while the other packet (redundant or duplicate) is discarded. The RouteRequest packet is forwarded until it reaches the destination. Here, the RouteReply is triggered and if optimization is allowed then the RouteReply packets are originated at the intermediate nodes also, thereby sending multiple replies to the source from the intermediate nodes. To transmit the data packets to the destination, an efficient route is chosen from the source node. Every data packet that is to be transmitted contains the entire information about the entire route path to reach its corresponding destination.

In figure (2), a link breaks between the nodes 8 and 10. This information about the broken link is send to the source node by creating a RouteError message from the neighbouring node of the broken link. Upon receiving the RouteError packet, the route establishment procedure is initiated again and cached entries present at the source and the intermediate nodes are deleted. If a broken link occur, because of the movement of edge nodes, then the route establishment process is initiated again by the source node.

Advantages

- DSR protocol uses an reactive approach which eliminates the frequent flooding and table update messages.
- It does not require the path-finding approach. Since the routes are build depending up on the requirements.
- It reduces the control overhead by allowing the intermediate nodes to use route cache information in an efficient manner.

Disadvantages

- The route discovery process is restarted when ever a broken link is found.
- The route cache information may result to inconsistent route paths during the reconstruction phase.
- DSR consumes more time for the connection setup in comparison with the table driven routing protocol.
- The performance of the protocol is decreased as the mobility of nodes increases.
- It uses a source-routing approach that leads to a large routing overhead which is dependent on the length of the path.

2. Ad Hoc On-demand Distance Vector (AODV)

AODV is based on on-demand routing approach for locating routes. Whenever, a source node needs a path for forwarding data packets, then only a route is established. The packet consists of the sequence numbers of the destination node so as to identify the current path used for transmitting data packets. The difference between AODV and DSR routing protocols is that the latter employs source routing where the data packets itself maintains the entire path from source to destination, whereas in the former the source node and all the intermediate nodes maintain the information about the next hop taken for transmitting data packets.

When there is no route established for reaching the destination, the source node broadcasts the RouteRequest packet through the network. When the intermediate nodes receive the RouteRequest, they identify the individual routes to reach the destination. These nodes either forward the packet to its neighboring node or prepares a RouteReply packet only if it identifies the valid route for reaching the destination.

Therefore, multiple routes to distinguishable destinations are obtained from a single RouteRequest.

AODV is different from the other on-demand routing protocols. In this protocol, data packet make use of the destination sequence numbers to find the up-to-date paths which helps in to reaching the desired destination. If the destination sequence number of present packet is greater than the sequence number of previously received packet then it is essential for a node to modify/alter the information of its path.

The RouteRequest packet contains the following,

(a) Source identifier (SrcID)

(b) Destination identifier (DestID)

(c) Source Sequence Number (SrcSeqNum)

(d) Destination Sequence Number (DestSeqNum)

(e) Broad Cast Identifier (BcastID)

(f) Time To Live (TTL)

A valid route is established by comparing the sequence number of the packet present at the intermediate node with the sequence number of the destination node specified in the RouteRequest packet. This packet is transmitted to the source either by the intermediate node (that contains a valid route to reach destination) or by the destination node itself. But, before forwarding the packet to its neighbor node, the intermediate node that receives the RouteRequest packet stores the address of the previous node as well as its BcastID.

Every RouteRequest packet consists of a timer, which is basically used, so as to delete the previous node address entry, if the RouteReply packet have not arrived before the timer expires. The benefit of units timer is that, the intermediate nodes maintain the information about the recent path (unlike other on-demand routing protocols, AODV doesn't use source routing approach for forwarding the data packets). When the intermediate nodes receive the RouteReply packet, they store the address of the previous node (that transmitted the RouteReply packet) so as to transmit the data packet to its adjacent node. This type of transmission signifies that packets are forwarded by taking a single-hop in order to reach destination.

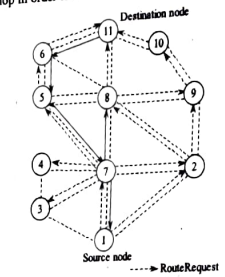


Figure (3): Routing Network in AODV

In the figure (3), the source node 1 reaches a RouteRequest packet, which is broadcasted throughout the network so as to find the route to a destination node 11. In the RouteRequest packet, assume that DestSeqNum = 5 and SrcSeqNum = 1. The path traverses the network and reaches the nodes 2, 3 and 7. When these nodes receive the RouteRequest packet, they search their respective routing table to find a route to destination. If a route is not available, then these nodes forward the packet to their adjacent nodes (i.e., nodes 9, 4, 8). Among these nodes, consider that nodes 9 and 8 have path to destination via the path 9 – 10 – 11 and path 8 – 11 respectively. The destination sequence number at nodes 9 and 8 is 6 and 2 respectively. In such situation, node 9 is allowed only to send a reply to the source along with the cached path as it contains the recent route to destination. Node 3 is not chosen, since it doesn't contain the most recent path to node 11 (i.e., destination sequence number at node 8 is 2, but the destination sequence number of source node is 5). The RouteReply packet is send by destination to the source by using the same path used while forwarding the RouteRequest packet (i.e., path 6-11). There will be multiple RouteReply packets that are generated in response to single RouteRequest packet. Once the intermediate node receives the RouteReply packet, they perform all the necessary updation in their respective routing tables and also update the routing information only, if the recent path have less number of hops between the end nodes.

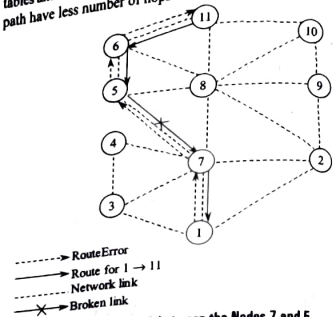


Figure (4): A Link Break between the Nodes 7 and 5

AODV fails to repair the path which is broken locally. Whenever, the breakage of link is identified either through regular beacons or via link level acknowledgments, then the source as well as the destination node are notified about the broken link. After receiving the breakage notification, the source node reestablishes a valid route for reaching the destination only, if it is required by the higher layer. The unsolicited RouteReply packets that consist of hop count value as infinity (∞) is transmitted by the intermediate nodes (if they detect the link breakage) to the source and destination nodes. For example in figure (4), if a link is broken between the nodes 7 and 5, then these nodes create a RouteError message and transmit it to their respective end nodes to inform them about the path breakage. When the end nodes receive the message, they remove the entry relative to these nodes (i.e., 7 and 5) from their tables. A new route reestablished by the source node with the new BcastID and the previous DestSeqNum.

Advantages

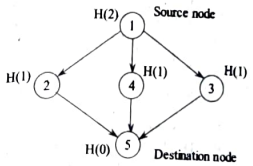
- Routes are established on demand basis.
- The recent path towards the destination is identified using destination sequence numbers.
- The delay time for establishing a connection is very less.

Disadvantages

- Incorrect routes are identified by the intermediate nodes when the destination sequence number of intermediate node is higher than the sequence number of the source node.
- If multiple RouteReply packets are generated as a reply to a single RouteRequest packet, then a greater control overhead may occur.
- High amount of bandwidth is consumed because of the periodic beaconing.

3. Temporally Ordered Routing Algorithm (TORA)

TORA is an on-demand routing protocol whose operations are initiated from the source node. Hence, it is referred to as a source-initiated on-demand routing protocol. This protocol employs a link reversal algorithm and produce multi-path routes without any loop to reach the destination. In TORA, every node detects the network partitions and has the information about the one-hop local topology stored in it. During the reconfiguration process, if a link breaks occur, then TORA has the capability of controlling the data packets upto a limited region.



H(N) → Height of node n from destination

H(1) → Height of nodes 2, 3 and 4 from destination

H(2) → Height of node 1 from destination

Figure (5): Network Topology in TORA

In the figure (5), the length or height of path from destination node is measured. The following are the basic operations in TORA.

(i) Establishing routes

(ii) Maintaining routes

(iii) Deleting routes.

(i) Establishing Routes

This operation is performed for obtaining path containing no directed links from source node to destination node. The route establishment process uses a Query/Update mechanism using which a destination-oriented Directed Acyclic Graph (DAG) can be established. In figure (5), node 1 is the source node and node 5 is the destination node. Here, node 1 creates a Query packet along with the address of node 5 stored in it. This Query packet can be passed to the destination node 5 by any of the intermediate nodes 2, 3 or 4. Thus, a set of directed links are created from source node to destination node, thereby resulting in the formation of DAG.

After receiving the Query packet, the destination node replies with an Update packet. This update packet includes the distance from the destination node (i.e., the distance is zero at the destination). The update packet originated from the destination node is send to the intermediate nodes and the source node. Since, the intermediate nodes 2, 4 and 3 are at a higher level than the destination, its distance will also be incremented. That is, as the distance of node 5 is H(0), the distance of nodes 2, 3 and 4 will be a value higher than the node 5 i.e., H(1). And, since source node is two levels greater than destination, the distance from the destination node 5 to it will be H(2).

While transferring the data, the reconfigurations existing in the network topology changes the length of the path. But, this does not affect the available paths whenever a path to destination is completely obtained.

(ii) Maintaining Routes

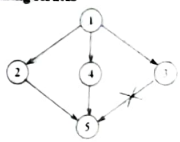


Figure (6): Link Breaks between the Nodes 3 and 5

In the figure (6), a link break occur between the nodes 3 and 5. Thus, the route of node 3 to destination node 5 becomes invalid. And, also the distance of node 3 changes to a value higher than its neighboring node, thereby originating an update packet. This update packet is received by the node 1, which further transmits the packet and reverses the link that exists between nodes 1 and 3. This is shown in figure (6).

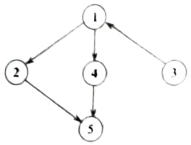


Figure (7): Nodes 1 and 3 Reverse their Links so as to Update the Path

The change in path also leads to a change in DAG. When the neighboring node of the source node does not contain any path to reach destination, a new Query/Update procedure is initiated.

(iii) Deleting Routes

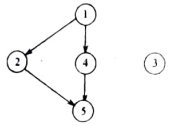


Figure (8): Link Break between Nodes 1 and 3

Suppose, if the link between nodes 1 and 3 break (as shown in figure (8)) then a partition between the nodes exist in the network, thereby originating a clear message which has the capability of deleting the information about the route that helps in reaching the destination.

Advantage

Since control packets are limited upto a small region, a less control overhead exists during the path reconfigurations.

Disadvantages

- Due to the partitions in the network and the deletion of routes, transient loops and temporary oscillations may occur.
- The path reconfiguration that is done locally may lead to non-optimal routes.

Q15. Describe about various types of hybird routing protocols.

Answer :

The various hybrid routing protocols are,

1. Core Extraction Distributed Adhoc Routing (CEDAR)

CEDAR is a partitioning protocol for MANETs that comprise ten to hundred nodes in small to medium sized networks. It establishes a network basis dynamically and propagates the link state gradually to the core nodes.

It functions using three main components.

(a) Core Extraction

A collection of nodes is chosen to create the core. This core maintains the local topology of nodes and computes route. The core is selected by approximating a MANET's minimum dominating set.

(b) Link State Propagation

All core nodes that are located far away in a network receives the information about the available high bandwidth stable links whereas the low bandwidth or dynamic link information is restricted to the local area. This information helps CEDAR to propagate QoS routing.

(c) Route Computation

A core path between the source and destination is created by route computation. CEDAR uses this core path information and finds a partial route in iterative manner between a source and the node that is located at furthest possible location with the core path that satisfies the predefined bandwidth.

This furthest node thereafter acts as a source for the next iteration. The core offers low overhead information and efficient way for routing.

The state propagation scheme makes sure that link-state information is available at the core node without resulting in high overheads.

2. Zone Routing Protocol (ZRP)

ZRP is a hybrid routing protocol that has an ability of combining the basic metrics of both table-driven and on-demand routing protocols. The table-driven routing is used within a limited zone for every node in the topology i.e., in the zr-hop neighborhood. Hence, this routing is referred to as Intra-zone Routing Protocol (IARP). The on-demand routing is used beyond the specified zone. Thus, this routing is referred to as the Inter-zone Routing Protocol (IERP). Within the specified routing zone, all nodes are reachable to a particular node with equal or less than the zone radius hops.

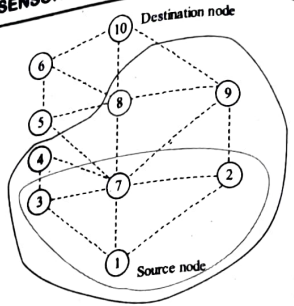


Figure (1): Routing Zone for Node 1 in ZRP

In the figure (1), the nodes inside the routing zone of node 1 with $zr = 1$ are 3, 7 and 2 (interior nodes) whereas the nodes beyond this routing zone are 4, 8 and 9 (peripheral nodes). Every node in the routing zone maintains the information about the routes available in the network. This is done by periodically exchanging the updated route packets, thereby generating a high update control overhead.

The information present at each nodes routing zone is used by IERP. The IERP helps in finding the paths that are not available in the routing zone. In figure (1), the node 1 is the source node and node 10 is the destination node. If node 1 attempts to transmit the packets to destination then the availability of node 10 within its routing zone is checked.

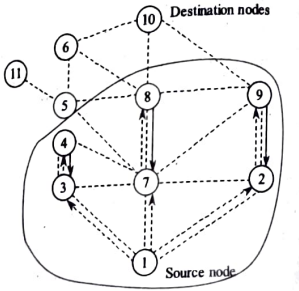


Figure (2): Path Finding between Node 1 and 11

If node 10 is available in routing zone of node 1 with radius = 2, then the packets are transmitted directly. Otherwise, a RouteRequest is broadcasts to nodes 2, 3, 4, 7, 8 and 9. A RouteReply is send to node 1 whenever a peripheral node finds node 10 inside its routing zone (this indicates the presence of the path). If node 10 is not found then the RouteRequest packet is broadcasted again to its peripheral nodes. This process continues till node 10 is found.

Nodes 7 and 8 detect a new node i.e., 11 and thus, the RouteReply packets are send back to the node 1 informing about its presence. When the RouteRequest packet is flooded throughout the network, the intermediate node that receives the packet attaches its address and forwards the packet to the adjacent node. The purpose of appending the address information is to transmit the RouteReply packet back to the source node. Hence, during the path-finding process, various RouteReply packets reach at the source node, wherein an optimal path is chosen. The factors that deal while selecting an efficient path are shortest path, least delay path etc.

While transmitting the packets through a routing path, if an intermediate node finds a broken link in that path, then path reconfiguration is done locally wherein another simple path is used to connect the ends of the broken link. The change in the route path is informed to the sender by means of an update message. This will lead to a sub-optimal path that exists between the two end points, but helps in a faster reconfiguration of broken links. After performing various local path reconfigurations, the sender node reoriginates the path-finding process so that an efficient path can be obtained.

Q16. Explain in detail about hierarchical routing protocols.

Answer :

The two hierarchical routing protocols are as follows,

1. Hierarchical State Routing

Hierarchical routing is performed by using following two methods,

(a) Terminodes routing

(b) Grid routing.

(a) Terminodes Routing

In terminodes routing, data packets are routed based on proactive distance vector scheme, wherein the distance between the sender node and receiving node is less in terms of number of hops. When the distance is large between the sender and the receiving nodes, a greedy position mechanism is used for routing data packets.

However, when a long distant packet comes closer to the receiver's area, the packets are forwarded using local routing algorithm. The sending node add position information in the packet header to prevent greedy forward from happening for long distance routing from suffering a local maximum. The packets are then transmitted to the sender.

Further, the sending node requests for position information from the nodes which are in its contact. When it receives this information it validates the position or any enhancement if needed at regular intervals.

(b) Grid Routing

The grid routing ensures that atleast one node is available in every area that is aware of its own position. This node is used as proxy. This position-aware node allows the packets that are intended to be transmitted to a node that is not aware of its position to arrive at a proxy, aware of its position. The proxy is forwarded based on the proactive distance vector protocol.

Besides using position aware node, grid routing also use Intermediate Node Forwarding (INF).

INF is an enhanced mechanism of greedy long-distance routing protocol. In this mechanism, when a node has no neighbor with information of forward progress it discards the packet and informs the sender by sending a notification. The sender selects a single intermediate position on random basis between itself and the receiver to circle around these two node lines. The packets are traversed to assign intermediate position. Further if packet is discarded, the circle radius is increased and a new position is selected on random basis. This process is repeated unless all packets are transmitted to the receiver or the packets are retransmitted a number of times when a sender notices that its defined destination is unreachable.

Advantages of Hierarchical Routing

Hierarchical routing enhance the ratio of success in delivering packets and reduces overhead of routing compared to traditional reactive ad hoc routing protocols.

2. Fisheye State Routing Protocol

Fisheye state routing protocol unveils multilevel fisheye scope. This scope reduces the overhead caused due to routing update in MANETs.

Generally, nodes exchange entries of link state with their neighbor in a frequency. This frequency is based on distance between the sender and destination. The entries exchanged are used to construct the map of topology of entire network as well as to compute the optimal route.

It focuses on view on nearby changes by keenly monitoring them with highest resolution in time. Contrarily, changes at nodes situated at far distance are monitored less frequently and with a lower resolution.

Q17. Explain about power-aware routing protocols.

Answer :

Power-aware Routing Protocol

Power aware routing determines MANETs routing by using power-aware metrics. These metrics reduces the cost of packet routing by five to thirty percentage compared to shortest-hop routing. They also reduce energy consumption by forty to seventy percentage compared to MAC layer protocol. Besides reducing cost and energy consumption, they make sure that packet delays do not increase and mean time node failure increase on a notable scale.

Power-aware Routing Metrics

Some of the routing metrics are as follows.

1. **Enhance Network Connectivity**

This routing metric balances the load in the network. Load balancing is important in environments thus networks connectivity should be distributed equally. For environments where the origination rate and unbounded contention varies then it becomes difficult to acquire an equally battery draining rate for the cut-set.

2. **Decreasing the Routing Cost**

This routing metric reduces the routing cost of the node at a period of time or after delivering few packets. It will lead to delay in failure of nodes which usually happens when forwarding packets at higher speed.

3. **Reduces the Cost of each Packet**

This routing metric reduces the cost of each packet in the network by adopting a mechanism in which the cost of the node increases as the decrease in its battery charge and cost of the node decreases with increase in battery charge thus enhancing the life of the node in the network.

4. **Reduce Power Levels in the Nodes by Balancing Load**

This routing metric reduces the power consumption by equally distributing the load among all the nodes present in the network irrespective of their rate and size, but there are chances that the nodes with variant size and rate may possess some problems, which can be overcome by routing packets to the least loaded next-hop node.

5. **Reduced Energy Consumption**

This routing metric helps in reducing the power consumed by each packet while travelling from source to destination. This energy is obtained from intermediate node hop in the path. It can be load as a function of distance among the distinct nodes which generates the link and load on that link. Load balancing is not done thus power distribution is not consistent in the network.

Some of the drawbacks of these metrics are,

- It do not have the capability of computing power consumption variations node to node in the network.
- It do not have the capability of preventing draining out of batteries at a very high speed at few nodes.
- It requires choosing paths which possess large hop length.

3.2 MAC PROTOCOLS

Q18. What are the issues that needs to be addressed while designing a MAC protocol for Ad hoc wireless networks?

Answer : **Model Paper-I, Q7(a)**

The issues that need to be addressed while designing a MAC protocol for Ad hoc wireless networks are as follows,

(i) Synchronization

Synchronization is a crucial factor in case of bandwidth required by the nodes. Synchronization is achieved among the nodes through the interchange of control packets where in the network bandwidth must not be used more by the control packets.

(ii) Quality of Service Support

This is crucial in case of time-critical traffic sessions. In Ad hoc sensor network bandwidth reservation which is fixed for a particular node at one point of time may not be useful when the node changes its location. This is due to the mobile nature of the nodes. Thus, providing quality of service support is difficult to the Ad hoc sensor network.

Thus to ensure quality of service, the MAC protocol employed for the Ad hoc wireless networks must possess a resource reservation mechanism which takes into account, the mobility of the nodes as well as the nature of the wireless channel.

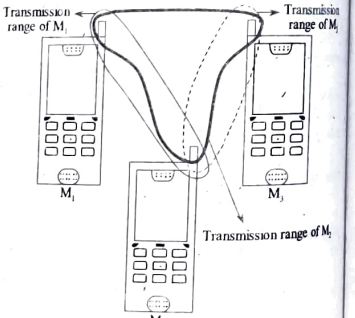
(iii) Bandwidth Efficiency

Bandwidth efficiency consideration are necessary due to the limitations in radio spectrum. Bandwidth efficiency is the ratio of bandwidth employed for actual data transfer to the entire available bandwidth.

Thus MAC protocol must be developed in a way that it must support less utilization of bandwidth in an efficient manner.

(iv) Problems Caused due to Hidden and Exposed Terminals

Terminals involved in communication have different transmission and interference ranges. This difference classifies the terminals. Consider the figure,



Figure

The three mobiles M_1, M_2 and M_3 all have different transmission ranges. Only mobile M_2's transmission range reaches both M_1 and M_3. The transmission range of neither M_1 nor M_3 reaches each other. Not even this, the detection ranges of M_1 and M_3 are not reachable by each of them. Thus, the two terminals M_1 and M_3 are called hidden terminals. For example, when M_3 wants to send a signal to M_2 even when M_1 is already transmitting signals, a collision occurs at M_2, but not detected either by M_1 or M_3.

Not only collisions, hidden terminals also results in delays. For example, when M_3 wants to send a signal to a terminal other than M_1 and M_2, having an interference range different from M_1 and M_2. In the meanwhile, M_1 is already transmitting data to M_2, but since M_1 is hidden for M_3, M_3 cannot detect the transmission continues with its own transmission. Thus, a collision occurs at M_2, which anyways is not carried to M_1. Here, terminal M_3 is said to be exposed to terminal M_2. The problems associated with hidden and exposed terminals reduces network throughput to a great extent.

(v) Mobility of Nodes

Node mobility needs to be considered while designing the protocol as it effects the bandwidth reservation or information exchanged. If the mobility of the node becomes high then there may be chances of ending up the bandwidth reservation or the information exchanged. Thus, this is a very crucial factor which affects the performance of the protocol.

(vi) Error Susceptible Shared Broadcast Channel

In wireless networks, multiple nodes can have access to the channel simultaneously which may lead to higher packet collision. Thus, a MAC protocol must be designed in a way that it should allow multiple node to access the channel with decreasing amount of collisions. That is a node should be granted for the channel access if it does not affect the current session of data transmission. Moreover, every node must be handled fairly in case of bandwidth allocation.

(vii) Distributed Nature

The MAC protocol must be designed by considering the distributed nature of the Ad hoc network. This must allow the protocol to schedule the nodes in distributed manner to have the channel access which may need exchange of control information. Moreover, the protocol must focus on reducing the overhead of bandwidth utilization involved due to this exchange of control information.

Q19. What are the goals that need to be achieved while designing MAC protocol for adhoc wireless networks?

Answer :

Design Goals of a MAC Protocol

The goals that need to be achieved while designing MAC protocol for ad hoc wireless networks are,

(i) Decrease of control overhead as much as possible.

(ii) The protocol scalability for large networks.

(iii) Efficient use of available bandwidth.

(iv) Distributed operations of the protocol.

(v) Minimum access delay (the time required for packet transmission).

(vi) Minimization in the effects of hidden and exposed terminal problems.

(vii) Support of power control mechanism which helps in maintaining energy utilization of the nodes efficiently.

(viii) Assurance for fair allocation.

(ix) Support to the quality of service for real-time traffic.

(x) Time synchronization among the nodes.

(xi) Support for the mechanism that helps to provide data rate control.

(xii) Support for directional antennas so as to achieve the following,

(a) More spectrum

(b) Less interference

(c) Less power consumption.

Design Constraints of Wireless MAC Protocols

For answer refer Unit-III, Q18.

3.2.1 Classification of MAC Protocols, S-MAC Protocol

Q20. Explain how MAC protocols can be classified into various categories depending on different criteria.

Answer : **Model Paper-II, Q7(a)**

The classification of MAC protocols into various categories depending on different criteria is discussed below as follows,

1. Contention-based protocol
2. Contention-based protocol having scheduling mechanism
3. Contention-based protocol having reservation mechanisms.

1. Contention-based Protocol

As the name implies, this protocol implements a contention-based policy for the use of channel. Here the nodes do not make reservation for the resources. Rather, the node contends with its neighbour nodes in order to use the shared channel upon receiving of the packet that has to be transmitted. This protocol cannot assure the quality of service to sessions due to the uncertainty of regular use of the channel by the nodes. This protocol are in turn classified into two types. These are,

(i) Sender-initiated Protocols

These are the protocols which initiate the transfer of packet by the sender node. These protocols are further classified as,

(a) Single channel

(b) Multi channel.

(a) Single Channel Sender-initiated Protocol: This protocols allow a single channel with total available bandwidth to be used by a node that wins the contention.

(b) Multi Channel Sender-initiated Protocol: This protocols divide the total available bandwidth among multiple channels allowing the multiple nodes to make use of separate channel.

(ii) Receiver-initiated Protocols

These are protocols which initiate the transfer of packet by the receiver.

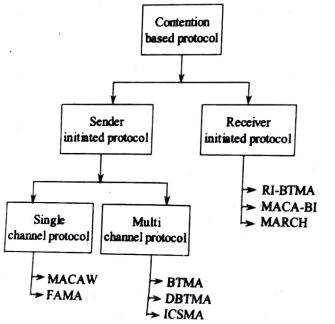


Figure: Classification of Contention based Protocol

2. Contention-based Protocol having Scheduling Mechanism

These protocols employ scheduling mechanism for scheduling of packets at nodes as well as for the nodes to gain access to the channel. Scheduling of the nodes is accomplished in a way that the no node has to wait for the bandwidth treating every node fairly.

These protocols also make use of some scheduling based strategies to allocate priorities to the flows whose packets are at nodes. The factors queued related battery like, battery power left, may be considered nodes has to scheduled so as to use the channel.

3. Contention-based Protocol having Reservation Mechanism

These protocols employ mechanisms for reserving bandwidth a priori so as to allow the nodes to support real-time traffic. This is required to provide quality of service assurance as in contention-based protocols.

Q21. Explain in detail low duty cycle MAC protocol.

Answer :

Low Duty Cycle MAC Protocol

Low duty cycle protocol basically lowers the communicative responsibilities of a sensor node to a least extent by preventing it in spending time in idle state for long duration.

The low duty cycle concept in this protocol helps to perform the following,

(i) Selection of low duty cycle makes the transceiver to be in sleep mode for long duration which in addition avoids idle listening and conserving energy.

(ii) It makes the traffic that flows between neighbour nodes and current node to focus on small time window (i.e., listen period). However, incase of heavy load there could be a noticeable competition.

The long sleep periods in this protocol lead to per-hop latency. This is because, expecting transmitter node need to wait for an average of half of the sleep duration prior to the receiver node receives the packets. However, the sleep phase should not also be much small otherwise startup cost can overweight the benefits.

The low duty cycle protocol is said to be ideal other than when a node wakes up only for transmitting or receiving packets. But this in impractical. However, some alternative methods are possible which includes,

(i) Sparse Topology and Energy Management (STEM)

Sparse Topology and Energy Management (STEM) protocol is suitable for reactive sensor network because all the sensor nodes in this network are in monitoring state for massive amount of time. The main purpose of this protocol is to preserve both time and energy that are used by sensor nodes in sensing the environment that where waiting for the occurrence of event. Inorder to conserve time and energy, the STEM protocol enables the sensor nodes and preprocessor circuit during the monitoring states. If an event is detected during this state, the main processor is woken so to analyze the

data and then transmit it to data sink. If the event is not detected, then the radio of all the next hop in data sink are discarded. This problem can be solved by periodically switching on the radio of each node for short interval of time. This is done to check whether other nodes wishes to initiate the communication. Inorder to perform this, the initiator node that want to communicate, transmits a signal which carries the ID of target sensor nodes. Thereby activating the communication link between initiator and target sensor node. Upon receiving the signal the target signal replies back to the initiator by switching on its radio. At this point both sensor nodes should make their radio active. The packet propagates further to next neighbouring nodes through target sensor node which now becomes an initiator node and the process is continued.

STEM proposes a wake up protocol so to minimize the interference that arises when both the nodes have their radio on. This protocol allows nodes to transfer data at distinct frequency bands.

(ii) Sensor MAC

Sensor MAC protocol uses design consideration inorder to conserve energy in MAC layer. This can be done by minimizing the radio energy consumption from sources like collision, control overhead, overhearing of unnecessary traffic and idle listening. The primary strategy of this protocol is to keep all the sensor nodes of wireless network in a low-duty cycle mode that is periodic listen and sleep. When the sensor nodes are placed in listen mode then they are allowed to access a medium such as IEEE 802.11 DCF by contention rule. When the sensor nodes are placed in sleep mode then they do not take decision to sleep on their own instead they synchronize and coordinate their sleeping schedule with other sensor node. That is before starting their periodic sleep each sensor node of wireless network initially select their sleep schedule.

This sleep schedule is then broadcasted to all the neighbouring nodes in form of SYNC packet so to avoid long-term clock drift. Inorder to reduce control overhead and ease the broadcast, SMAC encourages all the neighbouring nodes in network to adopt the same sleep schedule broadcasted by sender sensor node. After this, the destination sensor node listen for fixed time to receive the SYNC packet. If a packet is received these nodes from any of its neighbour, then it will adopt the same schedule specified by sender. Otherwise, an independent schedule is choosen by the destination sensor node after the initial listen period. If the schedules maintained by two neighbouring sensor nodes are known to each other then this schedule can be accessed in two ways,

- One option is to follow with both the schedule by considering schedule listen time.
- And the other is to follow only their own schedule but at the time of broadcast transmit the packet twice according to both schedules.

The problems that arises when the two sensors nodes are unaware of the presence of each other and when their listen interval do not overlap can be overcome by two mechanisms. These mechanisms are as follows,

(a) Neighbour discovery mechanism

(b) Low duty cycle operation.

(a) Neighbour Discovery Mechanism

This mechanism allow all the sensor nodes to periodically discover their unknown neighbour on different schedule.

(b) Low Duty Cycle Operation

This mechanism creates overlap between the listen interval by dividing it into two parts. In which one part consist of SYNC packets and the other consist of data packets. Inorder to randomly sense time before transmitting these packet a contention window is used by the sensor nodes.

(iii) Wakeup Radio Concept

A node is said to be a wakeup receiver, when it is turned on only when the packet starts towards it. It is necessary to turn on the node when it is only waiting for the packet.

The purpose of the wakeup receivers is to wakeup only the necessary receiver without wasting much of the power. The wakeup receivers overcome the problems related to WSNs. The main receiver is waked up by specifying the address of the intended receiver at the beginning of the message packet.

(iv) The Mediation Device Protocol

The mediation device protocol often period sleeping mode for every node such that the node can wakeup for small period for accepting packets from the neighbouring node. Whenever the node wakesup, it discloses its address and its desire for receiving packets, by transmitting a small query beacon. The node then remains in wakeup mode for small period tracking the query beacon and opens a window for the arriving packets. In this window period, if the packets are not received then the node switches to sleep mode.

Incase of packet transmission to a neighbour node, synchronization between the neighbour and transmitting node is required.

Q22. Generalize the concepts on important classes of MAC protocol.

Answer :

The important classes of MAC protocol are as follows,

1. Fixed assignment protocols
2. Demand assignment protocols
3. Random access protocols.

1. Fixed Assignment Protocols

Fixed assignment protocols are the types of MAC protocols that assigns the available resources by distributing them to the nodes for particular duration such as minutes, hours etc. Such assignment of resources enables the nodes to have access thereby avoiding collisions. These protocols require signalling mechanism to have change in topology for negotiating resource assignment change in topology occurs due to different reasons such as mobility, change in load pattern, deployment of new node or dying of the node.

The common protocols that belong to this category includes.

- ❖ TDMA
- ❖ FDMA
- ❖ CDMA
- ❖ SDMA

2. Demand Assignment Protocols

The demand assignment protocols are the MAC protocols that assign the resources to the nodes based on short term usually for the duration of data burst. There are two types of protocols. They are as follows,

(i) Centralized Demand Assignment

(a) In centralized demand assignment, central node is responsible for allocation of bandwidth.

It sends the request for band width to the central node. Once the allocation is done then the success message is sent back to the requesting node. The request is always contention based through random access protocol on a logical signalling channel piggybacking.

(b) Central node can even poll to its associated nodes. The nodes can even piggyback the data packets that are transmitted in data slots without the need for sending separately.

The de location of resources in this protocol do not rely on any condition. Simply, the time slots of an node which are not in use are allotted to other node.

In this protocol, most of the work is accomplished by the central node and thus it needs to active all the time thereby consuming more amount of energy.

However, these types of protocols are suitable in the cases where there are enough amount of nodes that are not restricted in terms of energy and capable of handling responsibilities of the central node. IEEE 802.15.4 protocol is an example for this case.

Some of the examples of this protocol type includes DQRUMA, MASCARA, HIPERLANE/2 and polling schemes.

(ii) Distributed Demand Assignment

The distributed demand assignment protocols are based on the concept of token passing protocols such as IEEE 802.4 token bus. The nodes in this type can begin transmissions only when they receive a token frame. The token frame is circulated between the nodes that are present on upper level of broadcast medium in logical ring format.

This type of demand assignment protocol requires specific procedures for the management of logical ring. Managing of logical ring includes addition, removal of nodes from the ring and handling of failure due to the token loss.

The transceiver of a node need to be constantly switched on as the circulation time of the token is not fixed and the node has to receive the token otherwise there will be breakage in logical ring.

Moreover, incase of repeated charge in topology the token ring management becomes difficult which thereby leads to a noticeable signaling traffics.

3. Random Access Protocol

In random access or contention methods, no station allows another station to transmit data and no station is assigned the control over another station. A station that has data to send follows a predefined procedure defined by the protocol to decide whether or not to send data. This decision of sending data relies on the state (i.e., idle or busy) of the medium.

(i) ALOHA: The ALOHA system was designed to provide radio broadcasting between the central computer and various data terminals at the university of Hawaii. There are two Versions (or) Protocols of ALOHA. They are Pure ALOHA and Slotted ALOHA.

(ii) CSMA: CSMA stands for carrier sense multiple access. With the help of the CSMA protocol, stations can detect what the other stations are doing by listening to the carrier i.e., (a transmission line) and adapt to their behavior accordingly.

(iii) CSMA/CD: CSMA/CD is the modification of pure carrier sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected and appending a jam signal to the frame to alert other stations.

Q23. Design the approaches and performance of S-MAC protocol.

Answer :

S-MAC Protocol

S-MAC is a MAC protocol that is designed particularly for the purpose of wireless sensor networks. It tries to retain the flexibility feature of contention based protocols there by improving the energy efficiency in multihop networks. It has various methods to reduce the energy consumption from major sources of energy waste.

Design Approaches of S-MAC

The S-MAC makes use of coarse-grained sleep/makeup cycle to make the nodes to spend much of their time in sleeping. The cycle of listen/sleep is called as frame. Every frame starts at listen period for the nodes which need to send the data to coordinate. This will be followed by the sleep period. If the nodes are required in communication, they remain awake. The S-MAC will establish schedules in multihop network, the nodes contend for channels in the period of listening and various optimizations improve throughput. This is illustrated as follows,

(i) Scheduling

The initial technique in S-MAC is to implement the low-duty-cycle operation on the nodes in multihop network. The sensor nodes should have the duty cycles of upto 1-10%. The nodes of S-MAC are free for selecting the listen/sleep schedules. The schedules are shared between the neighbors for communication. The transmissions are scheduled by the nodes while destination nodes are in listen mode. It supports multihop operation by providing various schedules in the network. Every node will broadcast the schedule in SYNC packet to prevent the timing errors caused by long term clock drift.

(ii) Data Transmission

The collision avoidance mechanisms of S-MAC and IEEE 802.11 DCF are similar. S-MAC makes use of virtual and physical carrier sense. The CSMA and RTS-CTS-DATA-ACK are combined between the sender and receiver by unicast packets. But the broadcast packet makes use of only CSMA procedure.

The durations field is placed in the packet that indicates the time required in present transmission. If the neighbor sends or receives the packet then it knows the time of sleep.

S-MAC Performance

The implementation of S-MAC allows the user to configure it into various modes. The topology in measurement is linear network with 11 nodes where front node acts as source and rear node acts as sink.

Energy Consumption

The energy consumed can be measured in ten-hop network with S-MAC configured in sleep and listen nodes. In every test the source node sends a fixed amount of data, with 20 messages of 100 bytes each. The below figure shows the change in energy consumption on all nodes in network as traffic load changes from heavy to light.

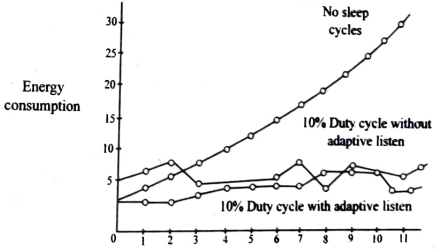


Figure: Aggregate Energy Consumption on Radius in 10 hop Network Using There MAC Modes

The figure shows the importance of adaptive listening in heavy traffic. Without adaptive listening the 10% of duty cycle will consume more energy than listening because some opportunities need more time to send the same amount of data. The adaptive sending allows S-MAC to be efficient as MAC.

Latency

The latency of message sending can be increased. This is a drawback for S-MAC. Latency in the above figure is measured by time that a message takes to travel over various hops when there is only one message.

Energy vs Latency and Throughput

S-MAC will reduce the energy consumption but it increases the latency. Therefore, it has a reduced throughput.

The periodic sleep in above figure will provide excellent performance at light traffic load. The adaptive listen can adjust to the traffic thereby achieving the good performance because of non sleep node at heavy node. Therefore, S-MAC with adaptive listen is a good choice for sensor networks.

Q24. What are the key features of S-MAC? Explain in detail.

OR

What are the causes behind energy wastage in wireless sensor networks? Explain.

Answer :

Key Features of S-MAC

Sensor MAC(S-MAC) protocol uses design consideration in order to conserve energy in MAC layer. The key features of s-mac is saving energy. It also incorporates combined scheduling and contention schemes to acquire good stability and collision avoidance.

The major causes behind energy waste in wireless sensor network are as follows,

(i) Collision

(ii) Overhearing

(iii) Control packet overhead

(iv) Ideal channel listening.

(i) Collision

The collision corrupts the packet which must be rejected and retransmitted. This consumes high energy due to which there is a greater increase in latency.

(ii) Overhearing

The sensor nodes can overhear the ongoing transmission of the other sensor nodes. Unlike unicast communication where the frames are generated from one source and reaches one destination, wireless medium performs broadcast communication. Here, the source's neighbors present at the receiver state can hear the packet and also drop it if it is not destined to their address. Here, the sensor nodes performs the process of overhearing, where in they overhear the on going transmission of other sensor nodes. On the other hand the process of overhearing causes loss in energy. The overhearing avoidance can be easily performed in higher node densities, saving large amount of energy.

The overhearing is mostly useful for in assessment of current traffic load for management purposes and gathering neighborhood information.

(iii) Control Packet Overhead

The overhead is occurred during the transmission and reception of control packet as they consume high amount of energy and also minimizes the payload. This extent of overhead raises as the node density increases. Beside this more energy is require to tolerate with the failure of sensor nodes by issuing more control messages so that the failed nodes can get self configured.

(iv) Idle Channel Listening

The idle listening node occur when the channels are empty. Due to this, sensor nodes does not sense any data and remain idle for long time.

The mechanisms adopted for saving energy and improving performance are,

- Low duty cycle
- Adaptive listening
- Message passing
- Data aggregation.

Q25. Explain in detail about self organizing medium access control for sensor networks.

Answer :

Self Organizing Medium Access Control for Sensor Networks

SMAC is a distributed protocol. It is used to build the infrastructure and form flat topology for the sensor networks. Basically it consist of two phases,

(i) Neighbour discovery phase

(ii) Channel allocation phase.

In the first phase it enables the sensor nodes to identify their neighbour and in the second phase it prepares the schedule and assign TDMA slots for transmission/reception among the sensor nodes. This schedules enables all the sensor nodes to communicate with each other without any local and global master. As soon as the presence of the neighbouring node is identified, SMAC allocates a channel to the ongoing link. When all the nodes identifies their neighbour a final connected network with atleast one multipath between any two different nodes is established. As the complete information of radio connectivity is not known to the sensor nodes the assigned time interval of link may collide with the slots which are assigned adjacent links. The collision usually occurs, since the presence of adjacent links are hidden from the channel. To minimize this collision all the links of the channel are insisted to operate on different frequency band. This frequency band is randomly selected from a pool of potential choices during the link formation.

In order to assign non-synchronous slots in a network that allow nodes to change link dynamically a method called non-synchronous scheduled communication is used. This method allow quick scheduling of links across the network. After the allocation of link, the sensor nodes can communicate with other sensor nodes by turning on its transceivers. If no schedule is available for communication the sensor nodes turn of its transceivers. This schedule mode of communication significantly saves energy among the sensor nodes. In addition to this, a concept known as subnet is also defined by SMAC. This subnet consist of subset of atleast two nodes that creates a connected graph and also have intersecting superframe at regular interval.

3.2.2 B-MAC Protocol

Q26. Explain in detail about B-MAC protocol and its performance.

Answer :

Model Paper-I, Q7(b)

B-MAC protocol is a carrier sense media access protocol which avoids collision, utilizes high channel and perform low power operation. It employs adaptive sampling schemes which reduce duty cycle and idle listening.

Design goals of B-MAC protocol are as follows,

1. Effective collision avoidance.
2. Low Power Listening (LPL)
3. Utilize channel effectively
4. Scalable for huge number of nodes
5. Tolerant changes in radio frequencies and network topology.
6. Easy implementation, with less code and small RAM size.

To achieve these goals BMAC protocol provides certain interfaces. Some of them are as follows,

```
interface   MacControl
{
    command result-t EnableCCA( );
    command result-t EnableCCA( );
    command result-t DisableCCA( );
    command result-t EnableAck( );
    command result-t DisableAck( );
    command void * HaltTx( );
}
interface   MacBackoff
{
    event   uint16-t initialBackoff(void * msg);
    event   uint 16-t congestionBackoff (void * msg);
}
```

```
interface LowPowerListening
{
    command result-t SetListeningMode(uint8-t mode);
    command uint8-t GetListeningMode( );
    command result-t SetTransmitMode(uint8-t mode);
    command uint8-t GetTransmitMode( );
    command result-t SetPreambleLength(uint16-t bytes);
    command uint16-t GetPreambleLength( );
    command result-t SetCheckInterval(uint16-t ms);
    command uint16-t GetCheckInterval( );
}
```

Protocol Design

BMAC protocol uses CCA and packet backoff for sensing the transmission channel. Whenever the transmission channel is free, the signal strength can be sampled. Usually the channel is free if the ongoing transmission is completed or the communicating device is not receiving any data.

When the transmission channel is free, the sample data enters into the queue, then the median is calculated and added to exponential weight moving average along with decay (α). And noise floor is estimated and request for monitoring is sent. The received signal strength starts monitoring the transmission channel.

After this, B-MAC protocol tries to search for outlier in the signal strength. If any outlier is sensed, it is said that the channel is free else if outlier is not found it means channel is busy.

To "turn-on"-or-"turn-off" the CCA, B-MAC protocol make use of MacControl interface. If CCA is disabled, the scheduled protocol is implemented and if CCA is enabled, protocol uses packet back off. In B-MAC protocol, packet back off is used to run the algorithm. It make use of the event-driven approach, which either returns a back off time or ignore the event. To ignore the event small back off time is set. If initial back off time is completed, CCA outlier algorithm runs. And if the channel is busy to control congestion back off time is signalled by the event.

B-MAC protocol also support link layer Ack. If the application is in need of Ack, it sends Ack from source node to receiver node. When the receiver receives Ack it sets a bit in the sender's transmission message buffer.

For periodic transmission channel sampling, B-MAC make use of LPL (Lower Power Listening). Each node in B-MAC checks for activity in transmission channel. If it observes/senses an ongoing data transmission, then it waits till the completion. After completion, nodes move to sleep state. To minimize the time spent in sampling the transmission channel the interval between two LPL sample is maximized.

Performance Evaluation of B-MAC

When compared to S-MAC and T-MAC, B-MAC performs better in throughput and energy consumption. It make use of flexible interface and perform on low power operations, has high channel utilization and can avoid collision effectively. It has clear channel estimation and provides bidirectional interface for system services. Also it supports adaptive permeable sampling scheme which helps in reduction of duty cycle, minimization of idle listening and perform low power operation. Hence, it avoids overhead synchronization and state maintenance.

3.2.3 IEEE 802.15.4 Standard and ZigBee

Q27. Briefly specify IEEE 802.15.4 MAC protocol.

Model Paper-II, QP4

Answer :

The Institute of Electrical and Electronics Engineers (IEEE) have finalized the IEEE 802.15.4 standard in october 2003. It includes the physical as well as the MAC layer of low rate Wireless Personal Area Network (WPAN). Most of the applications of IEEE 802.15.4 are home automation, connecting devices to PC, wireless sensor networks, home security, home networking etc. These applications need low to medium bitrates, medium average delays without any stringent delay guarantor and less energy consumption for certain nodes. The bitrates of 40 kbps, 20 kbps and 250 kbps are provided by the physical layer. The MAC protocol does not support multiple channel, it only makes use of 1 among the 27 channels at a time. It provides the combination of schedule based and contention-based schemes.

The MAC protocol is asymmetric and uses several types of nodes with different roles defined as follows.

1. A Full Function Device (FFD) has three roles determined as follows.
   (i) PAN coordinator
   (ii) Simple coordinator
   (iii) Device
2. A Reduced Function Device (RFD) has only one role i.e., device.

The device can only be combined with coordinator node thereby forming star network. It works in the form peer to peer network. Personal Area Network (PAN) involves multiple coordinators. It has a unique 16-bit PAN identifier. It also has a PAN coordinator.

A coordinator can handle the below tasks compared to others.

(i) It can manage a set of associated devices.

(ii) It can transmit the regularly frame beacon packets with PAN identifier, a set of out standing frames etc., in the beaconed mode of IEEE 802.15.4.

(iii) It can allocate small addresses to its devices. Every IEEE 802.15.4 node has a 64 bit device address but for associating with device it can ask for 16 bit address. This address is used for the communication between the device and the coordinator. Thus, address is contained in the association response packet.

(iv) It sends and receives data packets to devices as well as peer coordinators.

Q28. Write short notes on ZigBee.

Answer :

ZigBee

ZigBee is a communication protocol followed in wireless systems to minimize the cost and power usage. It is based on IEEE 802.15.4 standard and gets operated on ISM 2.4 GHz unlicensed frequency band. It can support the data rate of about 250 kbps and can cover around 30 meters of area. It can allow over 255 devices to be connected within a single system. Some examples of such systems include light switches which are based on wireless technology, electrical meters etc.

It is used to inter connect a large number of sensors, lighting devices, industrial controller, air conditioning, office and home automation devices.

The characteristics of zigbee protocol are,

1. The operating frequency of zigbee is 2.4 GHZ band carrier with direct sequence spread spectrum.
2. The zigbee protocol supports a communication range of 70 m with a data transfer rate of 250 kbps and sixteen channels.
3. Zigbee network is self organizing i.e. it detects and established a communication network among the near zigbee devices.
4. Each node in a zigbee network acts as both requesting and responding device ie, it supports peer-to-peer network where data transfer takes place between two devices.
5. Zigbee also supports mesh networks i.e., each network functions as a mesh. That is, the transfer of data carried in between a single device is done and multiple device in the mesh network.
6. The communication latency and protocol stack overhead of a zigbee network are 30ms and 28kB respectively.

The network consists of zigbee router to transfer packets to adjacent sources. A co-ordinator is required to connect on zigbee network to another end device which are the transceiver of the information.

The figure below shows a hand held device connected to other hand held device using zigbee wireless protocol.

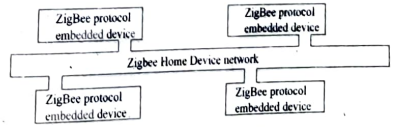


Figure: Communication Using Zigbee Wireless Protocol

IMPORTANT QUESTIONS

SHORT QUESTIONS

Q1. Define routing protocol. Write the classification of routing protocols.

Ans: For answer refer Unit-III, Q1. Important Question

Q2. What are salient features of on demand protocols routing?

Ans: For answer refer Unit-III, Q3. Important Question

Q3. List few goals that are required for designing MAC protocol for Adhoc Wireless Network.

Ans: For answer refer Unit-III, Q6. Important Question

Q4. Write short notes on classification of MAC protocols.

Ans: For answer refer Unit-III, Q7. Important Question

Q5. Write about STEM protocol.

Ans: For answer refer Unit-III, Q8. Important Question

ESSAY QUESTIONS

Q6. Define routing protocol. Explain the classification of routing protocol.

Ans: For answer refer Unit-III, Q9. Important Question

Q7. Discuss the issues in designing a routing protocol for Adhoc wireless networks.

Ans: For answer refer Unit-III, Q11. Important Question

Q8. What are the different classes of routing protocols?

Ans: For answer refer Unit-III, Q12. Important Question

Q9. Explain in detail the different table-driven or proactive routing protocols.

Ans: For answer refer Unit-III, Q13. Important Question

Q10. Describe about various types of hybird routing protocols.

Ans: For answer refer Unit-III, Q15. Important Question

Q11. What are the issues that needs to be addressed while designing a MAC protocol for Ad hoc wireless networks?

Ans: For answer refer Unit-III, Q18. Important Question

Q12. Explain how MAC protocols can be classified into various categories depending on different criteria.

Ans: For answer refer Unit-III, Q20. Important Question

Q13. Design the approaches and performance of S-MAC protocol.

Ans: For answer refer Unit-III, Q23. Important Question

Q14. Explain in detail about B-MAC protocol and its performance.

Ans: For answer refer Unit-III, Q26. Important Question

Q15. Briefly specify IEEE 802.15.4 MAC protocol.

Ans: For answer refer Unit-III, Q27. Important Question

Q16. Write short notes on ZigBee.

Ans: For answer refer Unit-III, Q28. Important Question