	Solutions and Scheme IAT2)	Marks	OBE	
			CO	RBT
1.	What are the characteristics of routing protocol for ad-hoc networks? It must be fully distributed as centralized routing involves high control overhead and hence is not scalable. ▪ It must be adaptive to frequent topology changes caused by the mobility of nodes. ▪ Route computation and maintenance must involve a minimum number of nodes. Each node in the network must have quick access to routes, that is, minimum connection setup time is desired. ▪ It must be localized, as global state maintenance involves a huge state propagation control overhead. ▪ It must be loop-free and free from state routes. ▪ The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node. The transmissions should be reliable to reduce message loss and to prevent the occurrence of state routes. ▪ It must converge to optimal routes once the network topology becomes stable. The convergence must be quick. ▪ It must optimally use scarce resources such as bandwidth, computing power, memory, and battery power. ▪ Every node in the network should try to store information regarding the stable local topology only. Changes in remote parts of the network must not cause updates in the topology information maintained by the node. ▪ It should be able to provide a certain level of quality of service (QoS) as demanded by the applications, and should also offer support for time-sensitive traffic.	[10]	CO3	L1
2.	Explain any two-table driven routing protocol for adhoc wireless networks It is an enhanced version of the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. ▪ It incorporates table updates with increasing sequence number tags to prevent loops, to counter the count-to-infinity problem, and for faster convergence. ▪ As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times. ▪ The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. ▪ The table updates are of two types: o ***Incremental updates:*** Takes a single network data packet unit (NDPU). These are used when a node does not observe significant changes in the local topology. o ***Full dumps:*** Takes multiple NDPUs. It is done either when the local topology changes significantly or when an incremental update requires more than a single NDPU. ▪ Table updates are initiated by a destination with a new sequence number which is always greater than the previous one. ▪ Consider the example as shown in figure (a). Here node 1 is the source node and node 15 is the destination. As all the nodes maintain global topology information, the route is already available as shown in figure (b).	[10]	CO3	L5

- Here the routing table node 1 indicates that the shortest route to the destination node is available through node 5 and the distance to it is 4 hops, as depicted in figure (b)
- The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way.
- The end node of the broken link initiates a table update message with the broken link's weight assigned to infinity (∞) and with a sequence number greater than the stored sequence number for that destination.
- Each node upon receiving an update with weight ∞, quickly disseminates it to its neighbors in order to propagate the broken-link information to the whole network.
- A node always assign an odd number to the link break update to differentiate it from the even sequence number generated by the destination.
- Figure 7.6 shows the case when node 11 moves from its current position.

Wireless Routing Protocol (WRP)

- WRP is similar to DSDV; it inherits the properties of the distributed bellman-ford algorithm.
- To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and penultimate hop node on the path to every destination node.
- Maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network.
- It differs from DSDV in table maintenance and in the update procedures.
- While DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information.
- The table that are maintained by a node are :

o Distance table (DT): contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by the neighbor for a particular destination.

o Routing table (RT): contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor/penultimate node, the successor node, and a flag indicating the status of the path. The path status may be a simplest (correct) path or a loop (error), or destination node not marked (null).

3a	**Give classification of security attacks in adhoc wireless networks**	[05]	CO5	L1

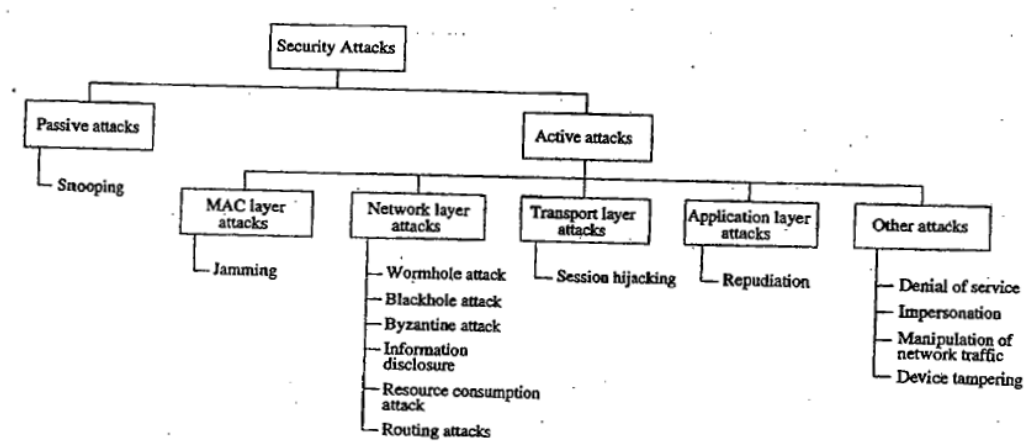

Figure 9.11. Classifications of attacks.

3b	**Give the classification of routing protocols in adhoc wireless networks**	[05]	CO3	L3

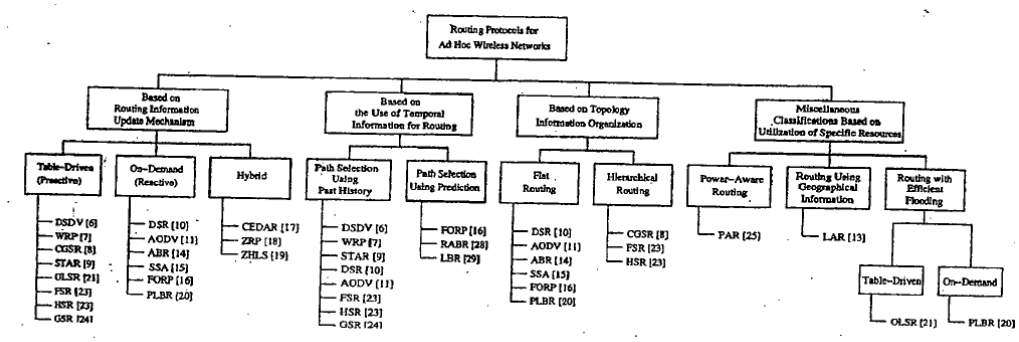

Figure 7.4. Classifications of routing protocols.

4a **Explain key management in ad-hoc wireless networks** [07] CO5 L5

Adhoc wireless networks pose certain specific challenges in key management, due to the lack of infrastructure in such networks.

 3 types of infrastructure have been identified, which are absent in adhoc wireless networks:

- The first is the network infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes.
- The second missing infrastructure is services, such as name resolution, directory & TTP's.
- The third missing infrastructure in adhoc wireless network is the administrative support of certifying authorities.

Password-Based Group Systems:

 A password-based system has been explored where, in the simplest case, a long string is given as the password for users for one session.

 However, human beings tend to favour natural language phrases as passwords, over randomly generated strings.

 Such passwords, if used as keys directly during a session, are very week & open to attack directly during a high redundancy, & the possibility of reuse over different sessions.

 Hence, protocols have been proposed to derive a strong key (not vulnerable to attacks).

 This password-based system could be two-party, with a separate exchange between any 2 participants, or it could be for the whole group, with a leader being elected to preside over the session.

 The protocol used is as follows :

- Each participant generates a random number, & sends it to all others.
- When every node has received the random number of every other node, a common pre-decided function is applied on all the numbers to calculate a reference value.
- The nodes are ordered based on the difference between their random number & the reference value.

Threshold Cryptography:

 Public Key Infrastructure (PKI) enables the easy distribution of keys & is a scalable method.

 Each node has a public/private key pair,& a certifying authority (CA) can bind the keys to a particular node. But CA has to be present at all times, which may not be feasible in Adhoc wireless networks.

 A scheme based on threshold cryptography has been proposed by which n servers exist in an adhoc wireless network, out of which any (t+1) servers can

jointly perform arbitration or authorization successfully, but t servers cannot perform the same. This is called an (n, t+1) configuration, where n >= 3t +1.

 To sign a certificate, each server generates a partial signature using its private key & submits it to a combiner. The combiner can be any one of the servers.

- In order to ensure that the key is combined correctly, t+1 combiners can be used to account for at most t malicious servers.
- Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.
- If verification fails, it means that at least one of the t+1 keys is not valid, so another subset of t+1 partial signature is tried. If combiner itself is malicious, it cannot get a valid key, because partial key itself is always invalid.

Self-Organised Public Key Management for Mobile Adhoc Networks:

 Self-organised public key system makes use of absolutely no infrastructure.

 The users in the adhoc wireless network issue certificates to each other based on personal acquaintance.

 A certificate is binding between a node & its public key. These certificates are stored & distributed by the users themselves. Certificates are issued only for specific period of time, before it expires; the certificate is updated by the user who had issued the certificate.

 Each certificate is initially stored twice, by the issuer & by the person for whom it is issued.

 If any of the certificates are conflicting (e.g: the same public key to different users, or the same user having different pubic keys), it is possible that a malicious node has issued a false certificate.

 A node then enables such certificates as conflicting & tries to resolve the conflict.

 If the certificates issued by some node are found to be wrong, then that node may be assumed to be malicious.

 A certificate graph is a graph whose vertices are public keys of some nodes and whose edges are public key certificates issued by users.

4b	**Explain one-way hash functions**	[03]	CO5	L5

5	**Explain Flow Oriented Routing Protocol** Employs a prediction-based multi-hop-handoff mechanism for supporting time-sensitive traffic in adhoc wireless networks ▪ Proposed for IPv6-based ad hoc wireless networks where QoS needs to be provided ▪ The multi-hop-handoff is aimed at alleviating the effects of path breaks on the real time packet flows ▪ A sender or an intermediate node initiates the route maintenance process only after detecting a link break ▪ It may result in high packet loss leading to a low QoS provided to the user	[10]	CO3	L5

- FORP utilizes the mobility and location information of nodes to estimate the link expiration time (LET)
- LET is the approximate lifetime of a given wireless link
- The minimum of the LET values of all wireless links on a path is termed as the route expiry time (RET)
- Every node is assumed to be able to predict the LET of each of its links with its neighbors
- The LET between two nodes can be estimated using information such as current position of the nodes, their direction of movement, and their transmission ranges
- FORP requires the availability of GPS information in order to identify the location of nodes
- When a sender node needs to setup a real time flow to a particular destination, it checks its routing table for the availability of a route to that destination
- If a route is available, then that is used to send packets to the destination
- Otherwise sender broadcasts a flow-REQ packet carrying information regarding the source and destination nodes
- The Flow-REQ packet also carries a flow identification number/sequence number which is unique for every session
- A neighbor node, on receiving this packet, first checks if the sequence number of the received Flow-REQ is higher than the sequence number corresponding to previous packet
- If the sequence number on the packet is less than that of the previous packet, then the packet is discarded
- This is done to avoid looping of flow-REQ packets

The Flow-REQ packet, when received at the destination node, contains the list of nodes on the path it had traversed, along with the LET values of every wireless link on that path

- FORP assumes all the nodes in the network to be synchronized to a common time by means of GPS information

Advantage

- Use of LET and RET estimates reduces path breaks
- Reduces the reduction in packet delivery
- Reduces number of out-of-order packets
- Reduces non-optimal paths

Disadvantage

- Works well when topology is highly dynamic
- Requirements of time synchronization increases the control overhead
- Dependency on GPS infrastructure affects the operability of this protocol wherever it is not available

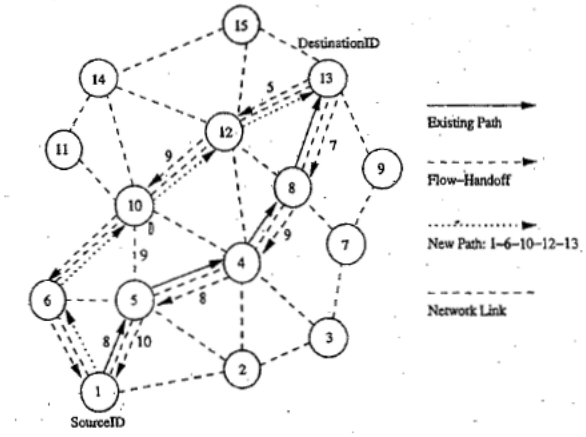

Figure 7.23. Route maintenance in FORP.

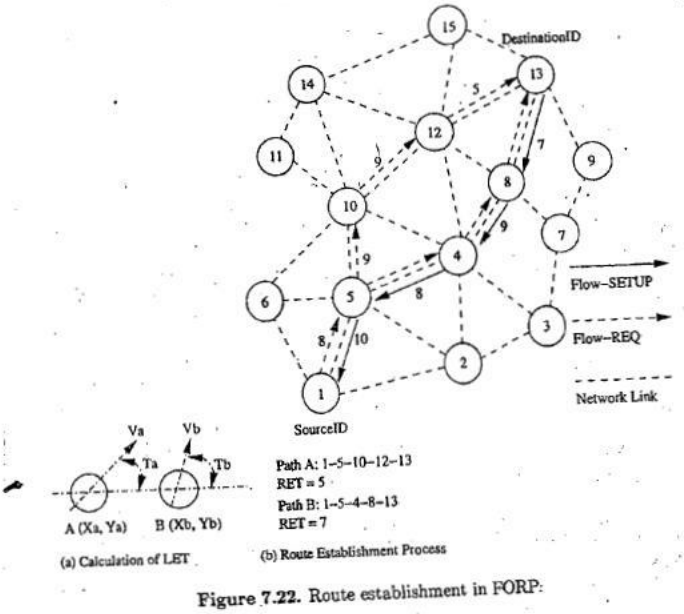

Figure 7.22. Route establishment in FORP.

6 **Illustrate AODV routing protocol with an example.** [10] CO3 L3

Route is established only when it is required by a source node for transmitting data packets

- It employs destination sequence numbers to identify the most recent path
- Source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission
- Uses DestSeqNum to determine an up-to-date path to the destination
- A RouteRequest carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier and the time to live field
- DestSeqNum indicates the freshness of the route that is accepted by the source
- When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination
- The validity of the intermediate node is determined by comparing the sequence numbers
- If a RouteRequest is received multiple times, then duplicate copies are discarded
- Every intermediate node enters the previous node address and its BcastID
- A timer is used to delete this entry in case a RouteReply packet is not received
- AODV does not repair a broken path locally
- When a link breaks, the end nodes are notified

- Source node re-establishes the route to the destination if required

Advantage

- Routes are established on demand and DestSeqNum are used to find latest route to the destination
- Connection setup delay is less

Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old

Multiple RouteReply packets to single RouteRequest packet can lead to heavy control overhead

- Periodic beaconing leads to unnecessary bandwidth consumption

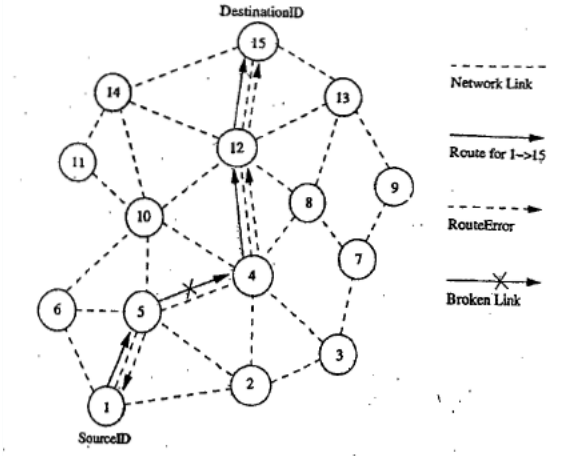

Figure 7.13. Route maintenance in AODV.

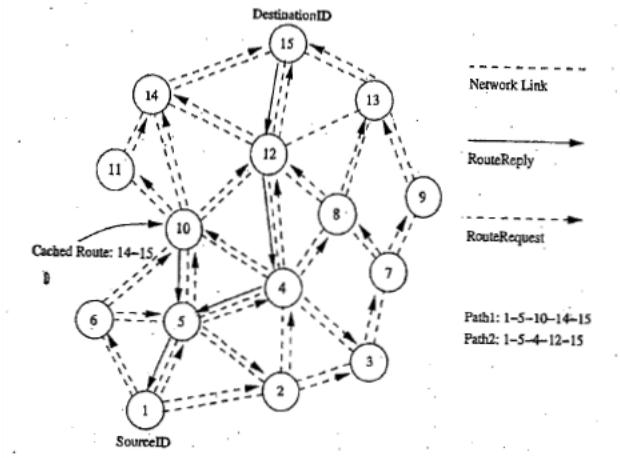

Figure 7.12. Route establishment in AODV.

7. **Explain TORA protocol in detail.** [10] | CO5 | L5

Source-initiated on-demand routing protocol

- Uses a link reversal algorithm
- Provides loop free multi path routes to the destination
- Each node maintains its one-loop local topology information
- Has capability to detect partitions
- Unique property → limiting the control packets to a small region during the reconfiguration process initiated by a path break

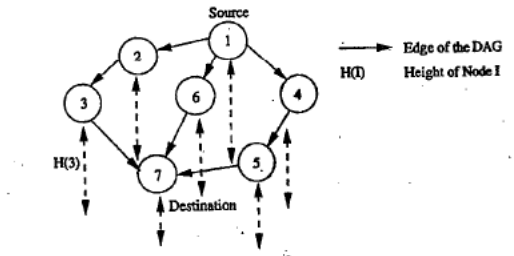

Figure 7.14. Illustration of temporal ordering in TORA.

TORA has 3 main functions: establishing, maintaining and erasing routes

- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link
- This process establishes a destination-oriented directed acyclic graph using a query/update mechanism
- Once the path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the re-configurations that may take place during the course of data transfer session
- If the node detects a partition, it originated a clear message, which erases the existing path information in that partition related to the destination

Advantages

- Incur less control overhead
- Concurrent detection of partitions
- Subsequent deletion of routes

Disadvantages

- Temporary oscillations and transient loops

Local reconfiguration of paths result in non-optimal routes

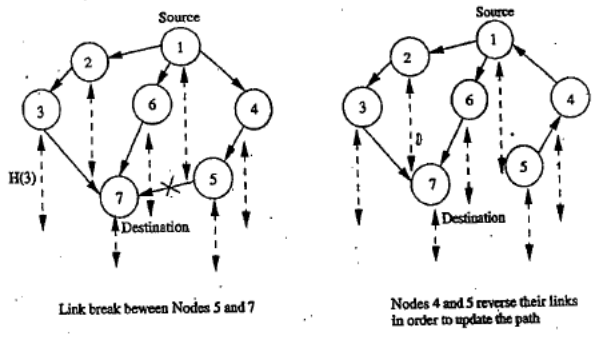

Figure 7.15. Illustration of route maintenance in TORA.

8.	**Explain Security aware routing protocol.**	[10]	CO5	L5

This routing protocol uses security as one of the key metrics in path finding.

- In adhoc wireless networks, communication between end nodes through possibly multiple intermediate nodes is based on the fact that the two end nodes trust the intermediate nodes.
- SAR defines level of trust as a metric for routing & as one of the attributes for security to be taken into consideration while routing.
- The routing protocol based on level of trust is explained in below figure.

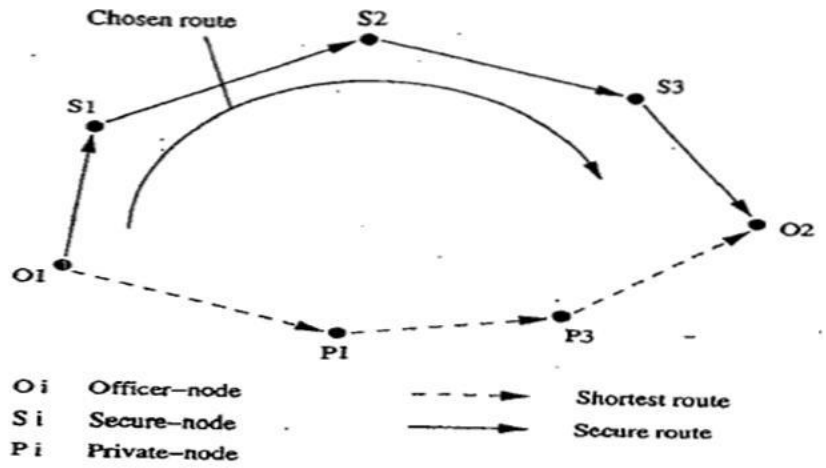

Figure 9.14. Illustration of the level of trust metric.

Two paths exist between the two officers O1 and O2 who want to communicate with each other

- One of these paths is a shorter path which runs through private nodes whose trust levels are very low
- Hence, the protocol chooses a longer but secure path which passes through other secure nodes
- Nodes of equal levels of trust distribute a common key among themselves and with those nodes having higher levels of trust
- The SAR mechanism can be easily incorporated into the traditional routing protocols for ad hoc wireless networks
- It could be incorporated into both on-demand and table-driven routing protocols
- The SAR protocol allows the application to choose the level of security it requires
- But the protocol requires different keys for different levels of security
- This tends to increase the number of keys required when the number of security levels used increase