CMR
INSTITUTE OF
TECHNOLOGY

Internal Assessment Test II – Scheme & Solutions

Sub:	Ad-hoc Networks						**Code:**	10IS841
Date:	09-03-17	Duration:	90 mins	Max Marks:	50	**Sem:** VI	**Branch:**	**ISE A&B**

Note: Answer any 5 questions. All questions carry equal marks. Total marks: 50

1a. What are the characteristics of routing protocol for ad-hoc networks? [6]

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

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 inthe 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.

Itmust 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.

1b. Give the classification of routing protocols in adhoc wireless networks
Diagram [1]
Explanation[3]

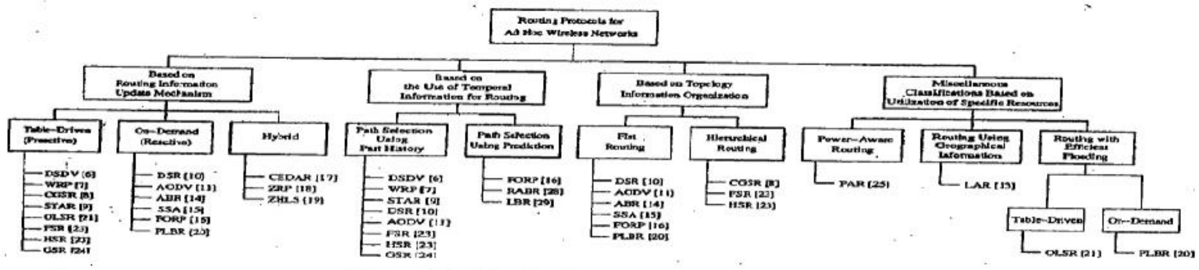


Figure 7.4. Classifications of routing protocols.

The routing protocol for adhoc wireless networks can be broadly classified into 4 categories based on

Routing information update mechanism.

Use of temporal information for routing

Routing topology

Utilization of specific resources.

Based on the routing information update mechanism

Ad hoc wireless network routing protocols can be classified into 3 major categories based on the routing information update mechanism. They are:

Proactive or table-driven routing protocols:

o Every node maintains the network topology information in the form of routing tables by periodically exchanging routing information.

o Routing information is generally flooded in the whole network.

o Whenever a node requires a path to a destination, it runs an appropriate path-finding algorithm on the topology information it maintains.

Reactive or on-demand routing protocols:

o Do not maintain the network topology information.

o Obtain the necessary path when it is required, by using a connection establishment process.

Hybrid routing protocols:

o Combine the best features of the above two categories.

o Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node.

o For routing within this zone, a table-driven approach is used.

o For nodes that are located beyond this zone, an on-demand approach is used.

Based on the use of temporal information for routing

The protocols that fall under this category can be further classified into two types :

Routing protocols using past temporal information:

o Use information about the past status of the links or the status of links at the time of routing to make routing decisions.

Routing protocols that use future temporal information:

o Use information about the about the expected future status of the wireless links to make approximate routing decisions.

o Apart from the lifetime of wireless links, the future status information also includes information regarding the lifetime of the node, prediction of location, and prediction of link availability.

Based on the routing topology

Ad hoc wireless networks, due to their relatively smaller number of nodes, can make use of either a flat topology or a hierarchical topology for routing.

Flat topology routing protocols:

o Make use of a flat addressing scheme similar to the one used in IEEE 802.3 LANs.

o It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc wireless network.

Hierarchical topology routing protocols:

o Make use of a logical hierarchy in the network and an associated addressing scheme.

o The hierarchy could be based on geographical information or it could be based on hop distance.

Based on the utilization of specific resources

Power-aware routing:

o Aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power.

o The routing decisions are based on minimizing the power consumption either logically or globally in the network.

Geographical information assisted routing :

o Improves the performance of routing and reduces the control overhead by effectively utilizing the geographical information available.

2a Explain any one table driven routing protocol for adhoc wireless networks [1+5]

Diagram[1]

Working [5]

Destination sequenced distance-vector routing protocol

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).

Here the routing table node 1 indcates 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)

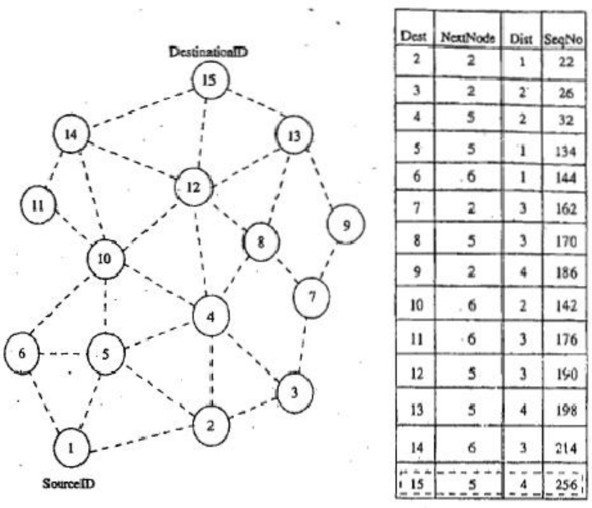
The reconfiguration of a path used by an on-going data transfer session is handled by the protocol in the following way.

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.

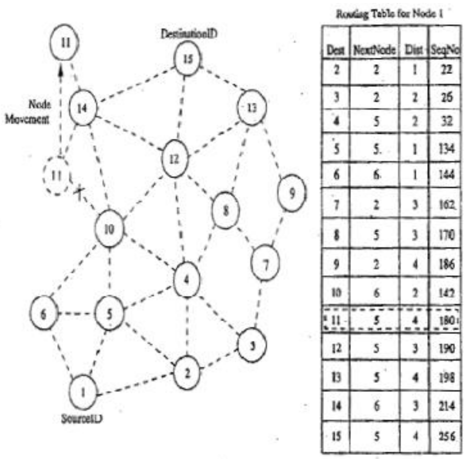


Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(a) Topology graph of the network

(b) Routing table for Node 1

Figure 7.5. Route establishment in DSDV.



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5.	1	134
6	6.	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Figure 7.6. Route maintenance in DSDV.

Advantages

Less delay involved in the route setup process.

Mechanism of incremental update with sequence number tags makes the existing wired network protocols adaptable to ad hoc wireless networks.

The updates are propagated throughout the network to maintain an up-to-date view of the network topology at all nodes.

Disadvantages

The updates due to broken links lead to a heavy control overhead during high mobility.

Even a small network with high mobility or a large network with low mobility can completely choke the available bandwidth.

Suffers from excessive control overhead.

In order to obtain information about a particular destination node, a node has to wait for a table update message initiated by the same destination node.

This delay could result in state routing information at nodes.

2b Give classification of security attacks in adhoc wireless networks [1+3]

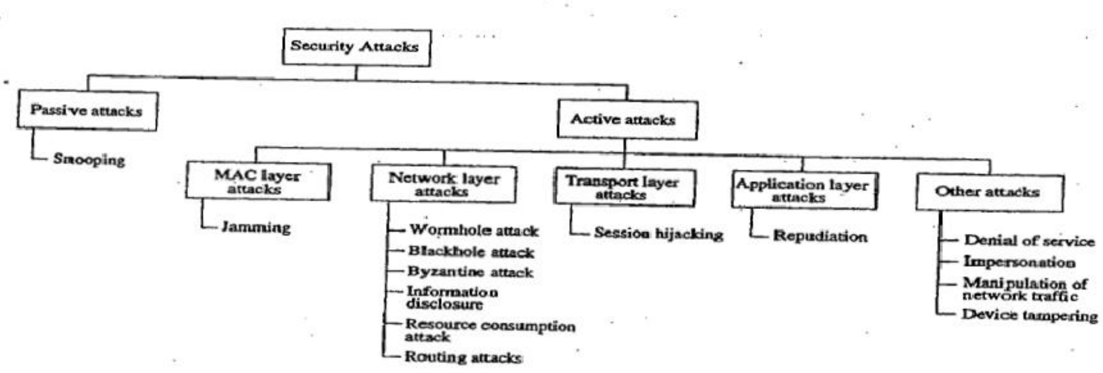


Figure 9.11. Classifications of attacks.

Attacks on adhoc wireless networks can be classified into 2 broad categories, namely:

1. *Passive attack*

a. It does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it.

b. One way to overcome such problems is to use powerful encryption mechanisms to encrypt the data being transmitted.

2. *Active attack*

a. An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

b. They can be further classified into 2 categories :

i. External attacks, which are carried out by nodes that do not belong to the network. They can be prevented using standard encryption techniques and firewalls.

ii. Internal attacks are from compromised nodes that are actually part of the network.

3a Explain key management in ad-hoc wireless networks [2+2+2+2]
Cryptography[2]
3 types of key management [2+2+2]

Cryptographyis one of the most common & reliable means to ensure security & can be applied to any communication network.

In the parlance of cryptography, the original information to be sent from one person to another is called ***plaintext*** The plaintext is converted into ***ciphertext*** by the process of ***encryption.*** An authentic receiver can decrypt / decode the ciphertext back into plaintext by the process of ***decryption.*** The process of encryption and decryption are governed by keys, which are small amounts of information used by the cryptographic algorithms. When the keys is to be kept secret to ensure the security of the system, it is called a ***secret key.***

The secure administration of cryptographic keys is called ***Key Management.***

The 4 main goals of cryptography are confidentiality, integrity, authentication & non-repudiation.

There are 2 major kinds of cryptographic algorithms:

1. ***Symmetric*** *key algorithms*, which use the same key for encryption & decryption.

2. ***Asymmetric** key algorithms,* which use two different keys for encryption & decryption.
The asymmetric key algorithms are based on some mathematical principles which make it feasible or impossible to obtain one key from another; therefore, one of the keys can be made public while the others is kept secret (private). This is called public key cryptography

KEY MANAGEMENT IN ADHOC WIRELESS NETWORKS

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:
o The first is the network infrastructure, such as dedicated routers & stable links, which ensure communication with all nodes.
o The second missing infrastructure is services, such as name resolution, directory & TTP's.
o 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 :

o Each participant generates a random number, & sends it to all others.
o 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.
o 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.
o In order to ensure that the key is combined correctly, t+1 combiners can be used to account for at most t malicious servers.
o Using t+1 partial signatures, the combiner computes a signature & verifies its validity using a public key.
o 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.

3b Explain one way hash functions. [2]

SEAD uses authentication to differentiate between updates that are received from non-malicious nodes and malicious nodes

This minimizes resource consumption attacks caused by malicious nodes

SEAD uses a one-way hash function for authenticating the updates

A one-way hash function (H) generates a one-way hash chain (h1, h2,......).

The function H maps an input bit-string of any length to a fixed length bit-string

To create a one-way hash chain, a node generated a random number with initial value x € (0,1)p, where p is the length in bits of the output bit-string

h0 is the first number in the has chain is initialised to x

The remaining values are computed using a general formula hi= H(hi-1) for $0 \le i \le n$, for some *n*.

SEAD avoids routing loops unless the loop contains more than one attacker

The protocol is robust against multiple coordinated attacks

SEAD protocol would not be able to overcome attacks where the attacker uses the same metric and sequence number which were used by the recent update message, and sends a new routing update

Explain Flow oriented routing protocol [1+2+2+5]

Diagram [1]

Advantages & Disadvantages [2+2]

Working [5]

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

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

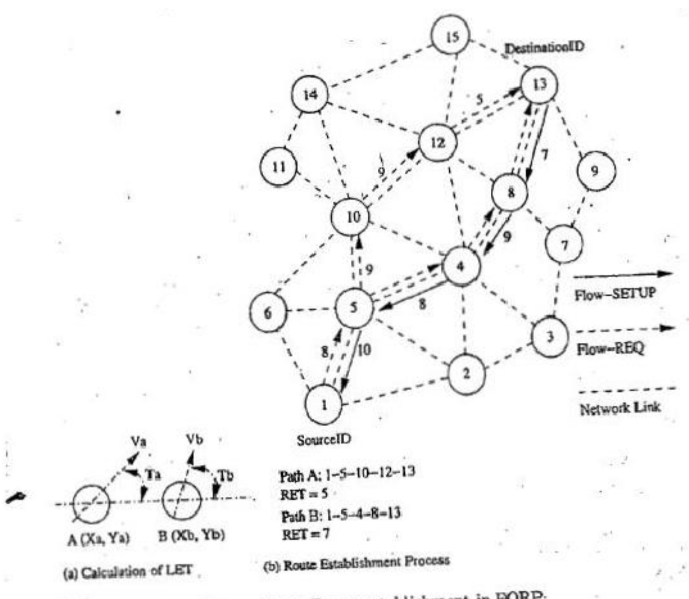


Figure 7.22. Route establishment in FORP.

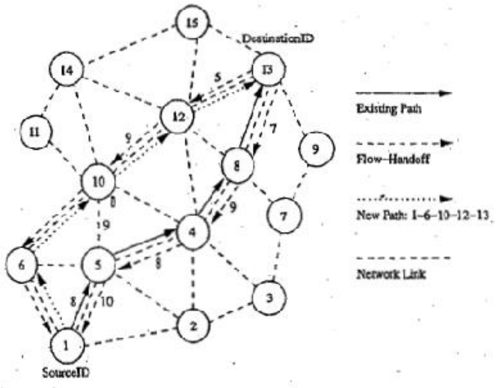


Figure 7.23. Route maintenance in FORP.

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

6a Illustrate AODV routing protocol with an example. [1+2+2+5]

Diagram [1]

Advantages & Disadvantages [2+2]

Working [5]

Ad Hoc On-Demand Distance Vector Routing Protocol

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 isreceived 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
Connectionsetup 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

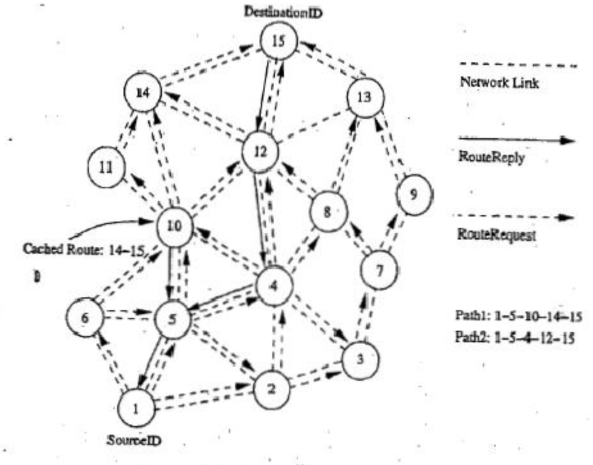


Figure 7.12. Route establishment in AODV.

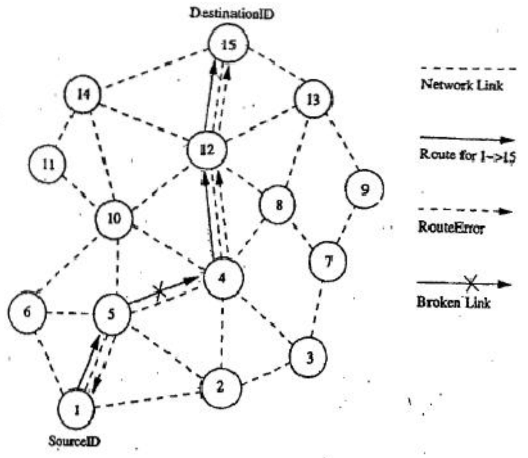


Figure 7.13. Route maintenance in AODV.

7a List and give brief explanation of network layer attacks. [10]

There are many types of attacks pertaining to the network layer in network protocol stack. Some of them are as follows:

1. ***wormhole attack:***

a. In this attack, an attacker receives packets at one location in the network & tunnels them (possibly selectively) to another location in the network, where the packets are resent into the network. This tunnel between 2 colliding attackers is referred to as a wormhole.
b. If proper mechanisms are not employed to defend the network against wormhole attacks, existing routing protocols for adhoc wireless networks may fail to find valid routes.

2. ***Blackhole attack:***
a. In this attack, a malicious node falsely advertises good paths to destination node during path-finding process or in route update messages.
b. The intention of malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node.

3. ***Byzantine attack:***
a. Here, a compromised intermediate note or a set of compromised intermediate nodes work in collusion & carries out attack such as creating routing loops, routing packets on non-optimal paths & selectively dropping packets.

4. *Information disclosure:*

a. A compromised node may leak confidential or important information to unauthorized nodes in the network.

5. *Resource consumption attack:*

a. In this attack, a malicious node tries to consume/waste resources of other nodes present in the network.

b. The resources targeted are battery power, bandwidth & computational power, which are limitedly available in adhoc wireless networks.

6. *Routing attacks:*

a. There are several types of attacks mounted on routing protocol & they are as follows:

i. Routing table overflow:

o In this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network.

o The main objective of this attack is to cause an overflow of routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.

ii. *Routing table poisoning*:

o Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.

o This may result in sub-optimal routing, congestion in network or even make some parts of network inaccessible.

iii. *Packet replication:*

o In this attack, an adversary node would replicate state packets.

iv. *Route cache poisoning:*

o Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar activities.

v. Rushing attack:

o On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack.