UNIT IV - TRANSPORT LAYER AND SECURITY PROTOCOLS

Transport Layer Protocols: Design Goals - Issue in Designing a Transport Layer Protocol - Classification of Transport Layer Solutions - TCP over MANET.
Security Protocols: Security over MANET - Security Requirements - Issue and Challenges in Security Provisioning - Network Security Attacks - Security Routing in MANET.

INTRODUCTION

The objectives of transport layer protocol include the setting up of an end -to-end connection, end-to-end delivery of data packets, flow control, congestion control.

ISSUES IN DESIGNING A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

1. Induced Traffic:
·In a path having multiple link, the traffic at any given link (or path) due to the traffic through neighboring links (or paths) is referred to as induced traffic.
·This is due to the broadcast nature of the channel and the location-dependent contention on the channel
·Induced Traffic affects the throughput achieved by the transport layer protocol.

2. Induced throughput unfairness:
·This refers to the throughput unfairness at the transport layer due to the throughput/delay unfairness existing at the lower layer such as the n/w and MAC layers.
·A transport layer should consider these in order to provide a fair share of throughput across contending flows

3. Separation of congestion control, reliability and flow control:
·A transport layer protocol can provide better performance if end-to-end reliability, flow control and congestion control are handled separately.
·Reliability and flow control are end-to-end activities, whereas congestion can at times be a local activity
·Objective minimization of the additional control overhead generated by them

4. Power and Band width constraints:
·Nodes in ad hoc wireless networks face resource constraints including the two most important resources:
(i) power source and
(ii) bandwidth
·The performance of a Transport layer protocol is significantly affected by these resource constraints

5. Interpretation of congestion:
·Interpretation of network congestion as used in traditional networks is not appropriate in ad hoc networks.
·This is because the high error rates of wireless channel, location-dependent contention, hidden terminal problem, packet collisions in the network, path breaks due to mobility of nodes, and node failure due to drained battery can also lead to packet loss in ad hoc wireless networks

6. Completely decoupled transport layer:
·Another challenge faced by Transport layer protocol is the interaction with the lower layers.
·Cross-layer interaction between the transport layer and lower layers is important to adapt to the changing network environment

7. Dynamic topology:

·Experience rapidly changing network topology due to mobility of nodes
·Leads to frequent path breaks, partitioning and remerging of networks & high delay in reestablishment of paths
·Performance is affected by rapid changes in network topology.

DESIGN GOALS OF A TRANSPORT LAYER PROTOCOL FOR AD HOC WIRELESS NETWORKS

·The protocol should maximize the throughput per connection.
·It should provide throughput fairness across contending flows.
·It should incur minimum connection set up and connection maintenance overheads.
·It should have mechanisms for congestion control and flow control in the network.
·It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
·It should be able to adapt to the dynamics of the network such as rapid changes in topology.
·Bandwidth must be used efficiently.
·It should be aware of resource constraints such as battery power and buffer sizes and make efficient use of them.
·It should make use of information from the lower layers for improving network throughput.
·It should have a well-defined cross-layer interaction framework.
·It should maintain End-to-End Semantics.

CLASSIFICATION OF TRANSPORT LAYER SOLUTIONS TCP OVER

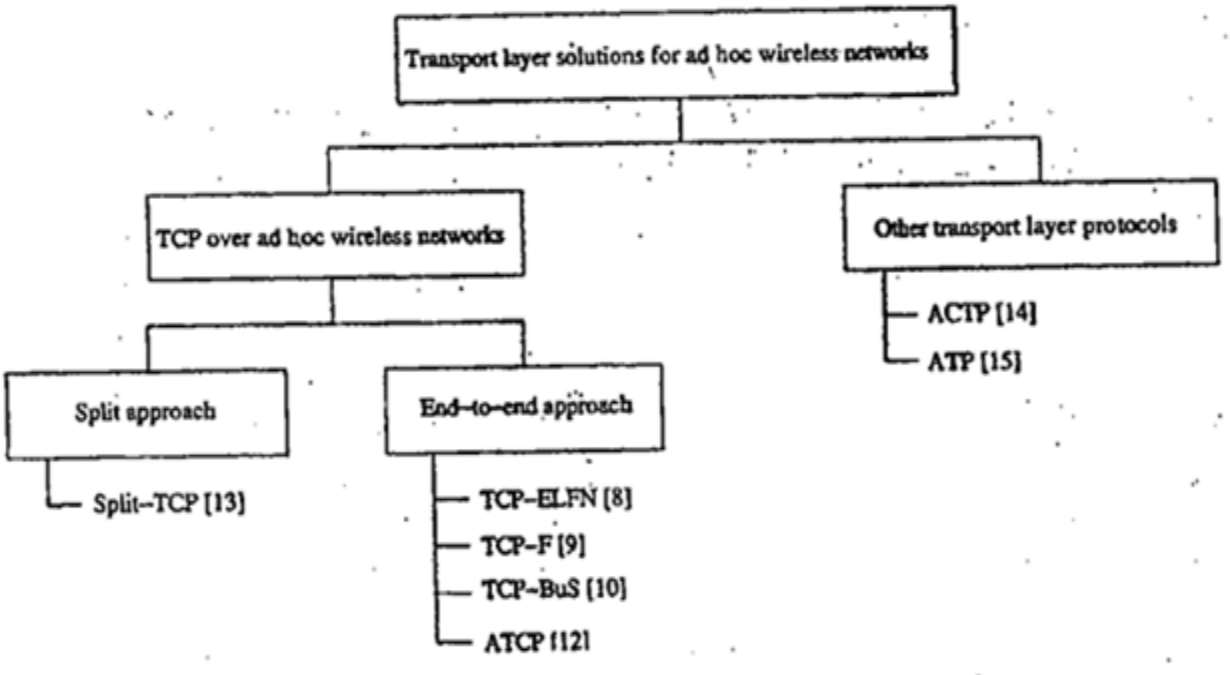

Figure: 4.1 Classification of Transport layer solutions

TCP OVER AD HOC WIRELESS NETWORKS:

·**TCP** is reliable, end-to-end, connection-oriented TL protocol that provides a byte stream based service.
·Major responsibilities of TCP include

- Congestion control.
- Flow control.
- In-order delivery of packets.
- Reliable transportation of packets.

Discussion of TCP performance in Adhoc wireless network

The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless net works are the following.

1. Misinterpretation of packet loss:
·In traditional TCP design, the packet loss is mainly attributed to network congestion.
·Ad hoc wireless network experience a much higher packets loss due to
·High bit rate
·Increased Collections etc

2. Frequent path breaks:
·If the route re-establishment time is greater than the RTO period of TCP sender, then the TCP sender assumes congestion in the n/w retransmits lost packets and initiates congestion control algorithm. This leads to wastage of bandwidth and battery power.

3. Effect of path length:
As path length increases, the throughput decreases.

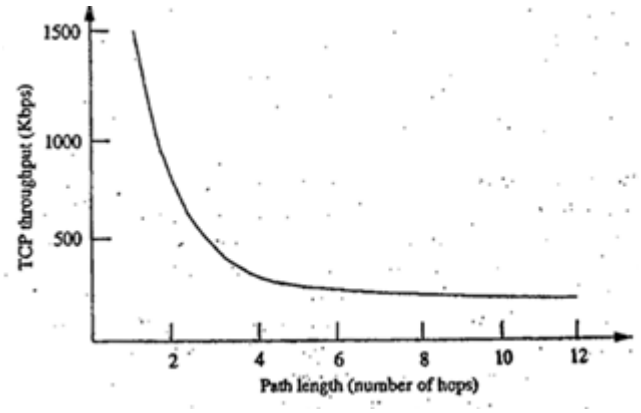

Figure: 4.2 Variation of TCP through with path length

4. Misinterpretation of congestion window:
·When there are frequent path breaks, the congestion window may not reflect the maximum transmission rate acceptable to the network and the receiver.

5. Asymmetric link behavior:
·Radio channel used in ad hoc wireless network has different properties such as location dependent contention, directional properties etc leading to asymmetric links.
·This can lead to TCP invoking the congestion control algorithm and several retransmissions.

6. Unidirectional path:
·TCP relies on end-to-end ACK for ensuring reliability. Path break on an entirely different reverse path can affect the performance of the network as much as a path breaks in the forward path.

7. Multipath Routing:
·For TCP, multipath routing leads to significant amount of out of order packets, when intern generates a set of duplicate acknowledgement (DUPACKs),which cause additional power consumption and invocation of congestion control.

8. Network partitioning and remerging:

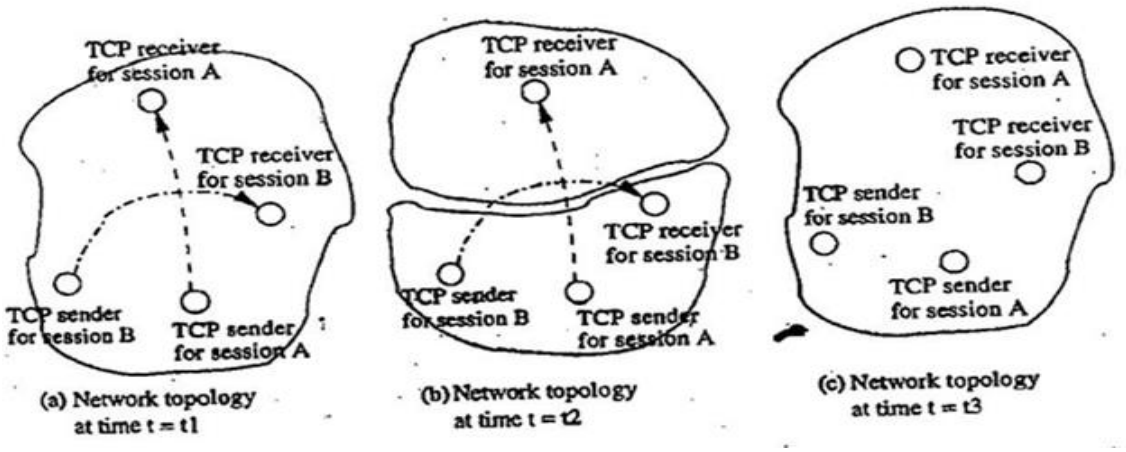

Figure: 4.3 Effect of partitioning and merging network

Fig 4.3 illustrates the effect of network partitions in ad hoc wireless networks.
·A network with two TCP sessions A & B is shown in (a) at time t1.
·At time t2, the network gets partitioned into two as shown in (b) due to dynamic topological changes.
·Now TCP session A's sender & receiver belong to two different partitions & TCP session B experiences path break.

9. The use of sliding window based transmission:
·TCP uses a sliding window for flow control.
·This can contribute to degraded performance in bandwidth constrained ad hoc wireless network.
·It can also lead to burstiness in traffic due to the subsequent transmission of TCP segments.

FEEDBACK BASED TCP (TCP – F)

·Improves performance of TCP
·Uses a feedback based approach.
·The routing protocol is expected to repair the broken path within a reasonable time period

Operation:
·In TCP-F, an intermediate node, upon detection of a path break, originates route failure notification (RFN) packet. This intermediate node is called Failure point (FP).
·This RFN packet is routed toward the sender of the TCP session, Sender information that is obtained from TCP packets.
·If any intermediate nodes that receive RFN has an alternate route to the same destination, then it discards the RFN packet and uses the alternate path for forwarding further data packets, thus reducing control overhead involved in the route reconfiguration process.

·When TCP sender receives an RFN packet; it goes into a state called snooze. In this state, a sender,

- ❖ Stops sending any more packets to the destination.
- ❖ Cancels all timers.
- ❖ Freezes its congestion window.
- ❖ Freezes the retransmission timer.
- ❖ Sets up a route failure timer.

·When route failure timer expires, the TCP sender changes from snooze state to connected state.
·When the route re-establishment has been done, and then the failure point sends Route Re-establishment Notification (RRN) packet to the sender and the TCP state is updated back to the connected state.

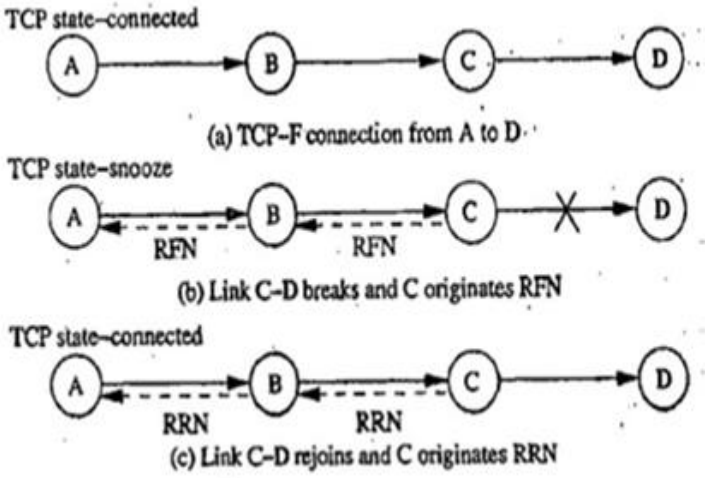

Figure:4.4 Operation of TCP-F

Advantages:

- ✓ Simple feedback solution for problem arising from path breaks.
- ✓ Permits TCP congestion control mechanism to respond to congestion in the network.

Disadvantages:

- ➢ If a route to sender is not available at the FP, then additional control packets may need to be generated for routing RFN packets.
- ➢ TCP-F has an additional state compared to traditional TCP state mechanism.
- ➢ Congestion window used after a new route is obtained may not reflect the achievable transmission rate acceptable to the network and the TCP-F receiver.

TCP WITH EXPLICIT LINK FAILURE NOTIFICATION: (TCP-ELFN)

·Improves the TCP performance in adhoc wireless network
·Similar to TCP-F

Operation:

·ELFN is originated by the node detecting a path break upon detection of a link failure to the TCP sender.
·This can be implemented in two ways:

1. By sending an ICMP Destination Unreachable (DUR) message to the sender.
   (or)
2. By piggy-backing this information to the sender.
   ·Once the TCP sender receives the ELFN packet; it disables its retransmission timers and enters a standby state.
   ·In this state, it periodically originates probe packets to see if a new route is established.

·Upon reception of an ACK by the TCP receiver for the probe packets, it leaves the standby state, and continues to function as normal.

Advantages:

- ✓ Improves TCP performance by decoupling the path break information from the congestion information by the use of ELFN.
- ✓ Less dependent on routing protocol & requires only link failure notification about the path break.

Disadvantages:

- ➢ When the network is temporarily partitioned, the path failure may last longer & this can lead to the origination of periodic probe packets consuming bandwidth & power.
- ➢ Congestion window used after a new route is obtained may not reflect the achievable transmission rate acceptable to the network and the TCP receiver.

TCP-BUS (TCP WITH BUFFERING CAPABILITY AND SEQUENCE INFORMATION)

·It is similar to TCP-F and TCP-ELFN in its use of feedback information from an intermediate node on detection of a path break. But it is more dependent on the routing protocol.

·TCP-Bus was proposed, with Associativity-Based Routing (ABR) protocol as the routing scheme. Hence it makes use of some special messages such as LQ and REPLY for finding partial path.

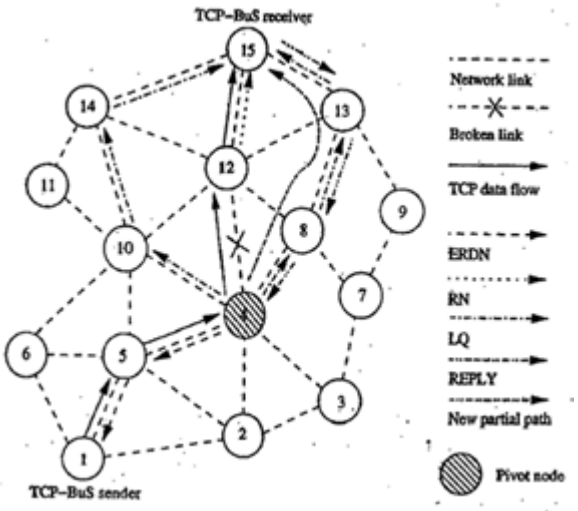

Figure: 4.5 Operation of TCP bus

Operation:

·Upon detection of a path break, an upstream intermediate node, called pivot node (PN), originates an explicit route disconnection notification (ERDN) message to the TCP-BuS sender.

·ERDN propagated in a reliable way.

·Upon receiving ERDN packet, the TCP-BuS sender stops transmission and freezes all timers and windows as in TCP-F.

·The packets in transmit at the intermediate nodes from the TCP-BuS sender to the PN are buffered until a new partial path from the PN to the TCP-BuS receiver is obtained by the PN.

·Upon detection of a path break, the downstream node originates a Route Notification (RN) packet to the TCP-BuS receiver, which is forwarded by all the downstream nodes in the path.

·PN attempts to find new partial path (route) to the TCP-BuS receiver, and the availability of such a partial path to destination is intimated to the TCP-BuS sender through an explicit route successful notification (ERSN) packet.TCP utilizes route reconfiguration mechanism of ABR to obtain partial path to the destination.

·Upon a successful LQ-REPLY process to obtain a new route to the TCP-BuS receiver, PN informs the TCP-BuS sender of the new partial path using ERSN Packet.(it is sent reliably)
·TCP-BuS sender also periodically originates probe packets to check the availability of a path to the destination.
·Below figure illustrates the operation of TCP-BuS.

Advantages:

- ✓ Performance improvement.
- ✓ Avoidance of fast retransmission due to the use of buffering, sequence numbering, and selective acknowledgement.
- ✓ Also takes advantage of the underlying routing protocols.

Disadvantages:

- ➢ Increased dependency on the routing protocol is high and the buffering at the intermediate nodes. The failure of intermediate nodes that buffer the packets may lead to loss of packets and performance degradation.
- ➢ The dependency on the routing protocol may degrade its performance with order routing protocols that do not have similar control messages as in ABR.

AD HOC TCP

- Based on feedback information received from the intermediate nodes, the TCP sender changes its state to the
  - ❖ *Persist state*
  - ❖ *Congestion control state*
  - ❖ *Retransmission state*
- When an intermediate node finds that the network is partitioned, then the TCP sender state is changed to the persist state where it avoids unnecessary retransmissions.
- Figure shows the thin layer implementation of ATCP between the traditional TCP layer and the IP layer.
- This does not require changes in the existing TCP protocol.
- This layer is active only at the TCP sender.

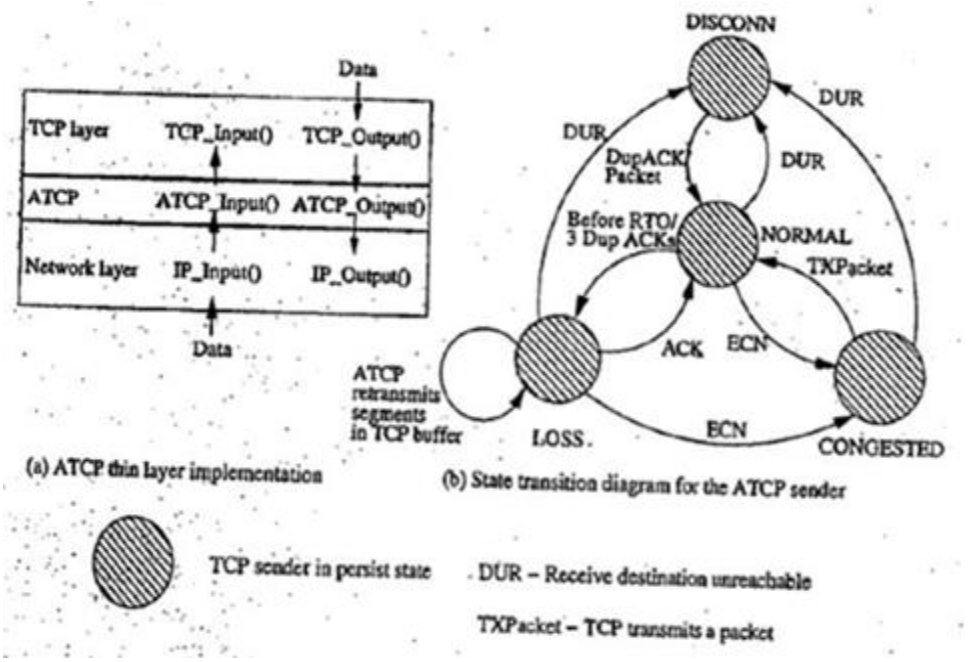

Figure:4.6 ATCP thin layer and ATCP state diagram

Major function of the ATCP Layer is that it monitors the following:

- Packet sent and received by TCP sender,
- The state of the TCP sender,
- State of the network.

·Fig (b) shows the state transmission diagram for the ATCP at the TCP sender.··

·The four states in the ATCP are:

1. *NORMAL.*
2. *CONGESTED*
3. *LOSS*
4. *DISCONN*

When a TCP connection is established, the ATCP sender state is in NORMAL, here ATCP does not interfere with the operation of TCP and it remains invisible.

Advantages:

- ✓ It maintains the end to end semantics of TCP.
- ✓ It is compatible with traditional TCP.
- ✓ Improves throughput of TCP in adhoc wireless network.

Disadvantages:

- ➢ Dependency on the network layer protocol to detect the route changes and partitions.
- ➢ Addition of thin ATCP layer to TCP/IP protocol stack requires changes in the interface functions
- ➢ currently being used

Split TCP

Major issues that affect the performance of TCP over adhoc wireless network are the degradation of throughput with increasing path length.

·This can also lead to unfairness among TCP sessions where one session may obtain much higher throughput than other sessions.

·This unfairness problem is further worsened by the use of MAC protocols, which are found to give a higher throughput for certain link level sessions, leading to an effect known as channel capture.

·Split TCP provides a unique solution to this problem by splitting the transport layer objectives into:

- Congestion control
- End to End reliability

·In addition, split TCP splits a long TCP connection into a set of short concatenated TCP connections (called segments or zones) with a number of selected intermediate nodes (known as proxy nodes) as terminating points of these short connections.

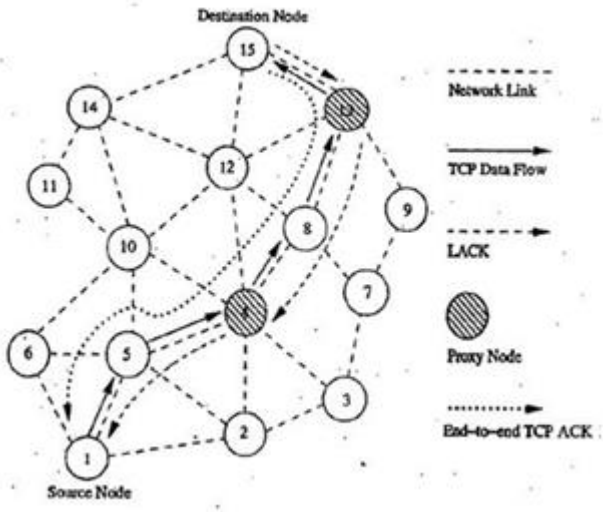

Figure: 4.7 Illustration of spilt TCP

·Figure illustrates the operation of split-TCP where a three segment split –TCP connection exists between source node1 and destination node 15.
·A proxy node receives the TCP packets, reads its contents, stores it in its local buffer, and sends an acknowledgement to the source (or the previous proxy)
·This acknowledgement is called Local acknowledgement (LACK) does not guarantee end to end delivery.
·The responsibility of further delivery of packets is assigned to the proxy node.
·In figure, node 1 initiates a TCP session to node 15, node 4 and node 13 are chosen as proxy nodes.
·The number of proxy nodes in a TCP session is determined by the length of the path between source & destination node.
·Based on a distributed algorithm, the intermediate nodes that receive TCP packets determine whether to act as a proxy node or just as a simple forwarding node.
·In figure, the path between nodes 1 & 4 is the first zone (segment), the path between nodes 4 to 13 is the second zone (segment), and the last zone is between node 13 and 15.
·The proxy node 4, upon receipt of each TCP packet from source node1, acknowledges it with a LACK packet, & buffers the received packets. This buffered packet is forwarded to the next proxy node at a transmission rate proportional to the arrival of LACKs from the next proxy node or destination.

Advantages:

- ✓ Improved throughput.
- ✓ Improved throughput fairness.
- ✓ Lessened impact of mobility.

Disadvantages:

- ➢ Requires modifications to TCP protocol
- ➢ End to End connection handling of traditional TCP is violated.
- ➢ The failure of proxy nodes can lead to throughput degradation

COMPARISION OF TCP SOLUTIONS FOR ADHOC WIRELESS NETWORKS

Issue	TCP-F	TCP-ELFN	TCP-BuS	ATCP	Split-TCP
Packet loss due to BER or collision	Same as TCP	Same as TCP	Same as TCP	Retransmits the lost packets without invoking congestion control	Same as TCP
Path breaks	RFN is sent to the TCP sender and state changes to snooze	ELFN is sent to the TCP sender and state changes to standby	ERDN is sent to the TCP sender, state changes to snooze, ICMP DUR is sent to the TCP sender, and ATCP puts TCP into persist state	Same as TCP	Same as TCP
Out-of-order packets	Same as TCP	Same as TCP	Out-of-order packets reached after a path recovery are handled	ATCP reorders packets and hence TCP avoids sending duplicates	Same as TCP
Congestion	Same as TCP	Same as TCP	Explicit messages such as ICMP source quench are used	ECN is used to notify TCP sender. Congestion control is same as TCP	Since connection is split, the congestion control is handled within a zone by proxy nodes
Congestion window after path reestablishment	Same as before the path break	Same as before the path break	Same as before the path break	Recomputed for new route	Proxy nodes maintain congestion window and handle congestion
Explicit path break notification	Yes	Yes	Yes	Yes	No
Explicit path reestablishment notification	Yes	No	Yes	No	No
Dependency on routing protocol	Yes	Yes	Yes	Yes	No
End-to-end semantics	Yes	Yes	Yes	Yes	No
Packets buffered at intermediate nodes	No	No	Yes	No	Yes

NETWORK SECURITY REQUIREMENTS

A security protocol for ad hoc wireless networks should satisfy the following requirements

1. Confidentiality:

a) The data sent by the sender must be comprehensible only to the intended receiver.
b) Though an intruder might get hold of the data being sent, he / she must not be able to derive any useful information out of the data.
c) One of the popular techniques used for ensuring confidentiality is *data encryption.*

2. Integrity:

a) The data sent by the source node should reach the destination node without being altered.
b) It should not be possible for any malicious node in the network to tamper with the data during transmission

3. Availability:

a) The network should remain operational all the time.
b) It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it.
c) It should be able to provide guaranteed services whether an authorized user requires them

4. Non-Repudiation:

a) It is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.
b) *Digital signatures* are used for this purpose.

ISSUES AND CHALLENGES IN SECURITY PROVISIONING

1. ***Shared broadcast radio channel:***

a) The radio channel used for communication in adhoc wireless networks is broadcast in nature & is shared by all nodes within its direct transmission range.
b) Data transmitted by a node is received by all nodes within its direct transmission range. So a malicious node could easily obtain data being transmitted in the network.
c) This problem can be minimized to a certain extent by using *directional antennas.*

2. Limited resource availability:

a) Resources such as bandwidth, battery power, & computational power are scarce in adhoc wireless networks.
b) Hence it is difficult to implement complex cryptography-based security mechanisms in networks.

3. Insecure operational environment:

a) The operating environments where adhoc wireless is used may not always be secure.
b) One important application of such networks is in battlefields.

4. Physical Vulnerability:

a) Nodes in these networks are usually compact & hand-held in nature.
b) They could get damaged easily & are also vulnerable to theft.

5. Lack of central authority:

a) In wired networks & infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points & implement security mechanisms at such points.
b) Since adhoc –wireless networks do not have central points; these mechanisms cannot be applied in ad hoc wireless networks.

6. ***Lack of associations:***

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

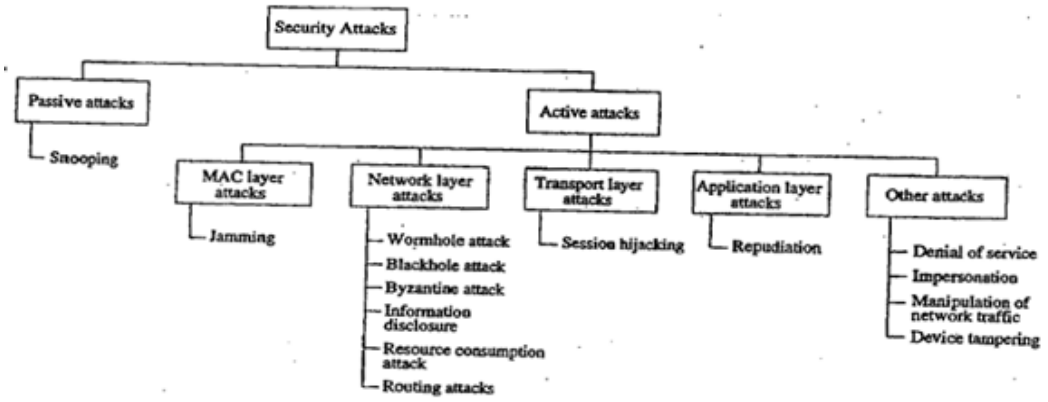

Figure: 4.8 Network attacks

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.

<u>NETWORK LAYER ATTACKS</u>

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. *Black hole 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
b) 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
c) Limitedly available in adhoc wireless networks.

6. *Routing attacks:*

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

i. Routing table overflow:

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

- Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes.
- This may result in sub-optimal routing, congestion in network or even make some parts of network inaccessible.

iii. *Packet replication:*

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

iv. *Route cache poisoning:*

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

v. Rushing attack:

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

SECURE ROUTING IN AD HOC WIRELESS NETWORKS

Ensuring secure communication in adhoc wireless networks include the mobility of nodes, a promiscuous mode of operation, limited processing power & limited availability of resources such as battery power, bandwidth & memory.

REQUIREMENTS OF A SECURE ROUTING PROTOCOL FOR ADHOC WIRELESS NETWORKS

The fundamental requirements for a secure routing protocol for adhoc wireless networks are listed as below:

- **Detection of malicious nodes:**
  - A secure routing protocol should be able to detect the presence of any malicious node in the network & should avoid the participation of such nodes in the routing process.
- **Guarantee of correct route discovery:**
  - If a route between the source & destination node exist, the routing protocol should be able to find the route, & should also ensure the correctness of the selected route

- **Confidentiality of network topology**:
  - Once the network topology is known, the attacker may try to study the traffic pattern in the network. If some of the nodes are found to be more active compared to others, the attacker may try to mount attacks.
  - This may ultimately affect the ongoing routing process. Hence, confidentiality of network topology is important.

- **Stability against attacks:**
  - The routing protocols must be self-stable in the sense that it must be able to revert to its normal operating state within a finite amount of time after passive or an active attack.
  - Some of the security-aware routing protocols proposed for adhoc wireless networks are discussed.

Part A Questions

1. List the types of attacks in ad hoc wireless networks.
2. What do you mean by passive attacks?
3. What do you mean by active attacks?
4. Define Denial of attack.
5. List the major types of resource consumption attacks.
6. List the major security threats that exist in ad hoc wireless networks.
7. Give the major objectives of the transport layer protocol.
8. List the issues and challenges in security provisioning of transport layer.
9. Define secure routing.
10. What are not supported by the traditional TCP for handling Adhoc network?
11. How is secure routing done on wireless channels?
12. Why secure routing protocols are needed?
13. Why does TCP not work well in ad hoc network?
14. What are the issues in designing transport layer protocol?
15. List the network security requirements.
16. List some of the network layer attacks.
17. What are the effects of induced traffic in Adhoc network?
18. Define Wormhole attack.

Part B Questions

1. Explain feedback based TCP and TCP BUS in detail.
2. Explain the issues in designing a transport layer protocol for adhoc wireless networks.
3. Why does TCP not perform well in adhoc wireless network? Explain.
4. List and brief various network and transport layer attacks in detail.
5. Explain various network and application layer security attacks in detail.
6. Discuss the effect of multiple breaks on a single path at the TCP- F sender.
7. What is the impact of the failure of proxy nodes in split- TCP?