TRANSPORT LAYER

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 neighbouring 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 → minimisation 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 re-establishment 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 thruput.
- ✓ It should have a well-defined cross-layer interaction framework.
- ✓ It should maintain End-to-End Semantics.

CLASSIFICATION OF TRANSPORT LAYER SOLUTIONS

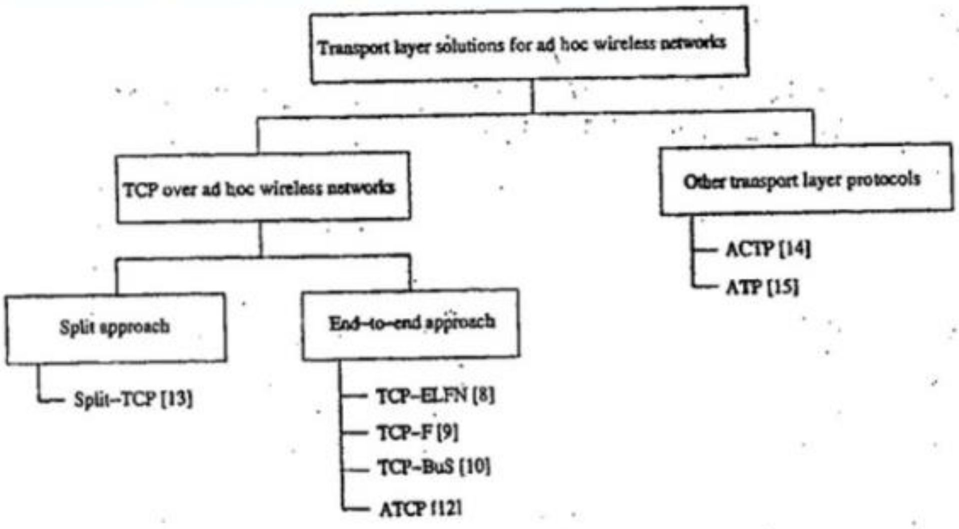
Transport layer solutions for ad hoc wireless networks
TCP over ad hoc wireless networks
Other transport layer protocols
ACTP [14]
ATP [15]
Split approach
End-to-end approach
Split-TCP [13]
TCP-ELFN [8]
TCP-F [9]
TCP-BuS [10]
ATCP [12]

Figure 9.1. Classification of transport layer solutions.

SECURITY

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 pont 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.

NETWORK SECURITY ATTACKS

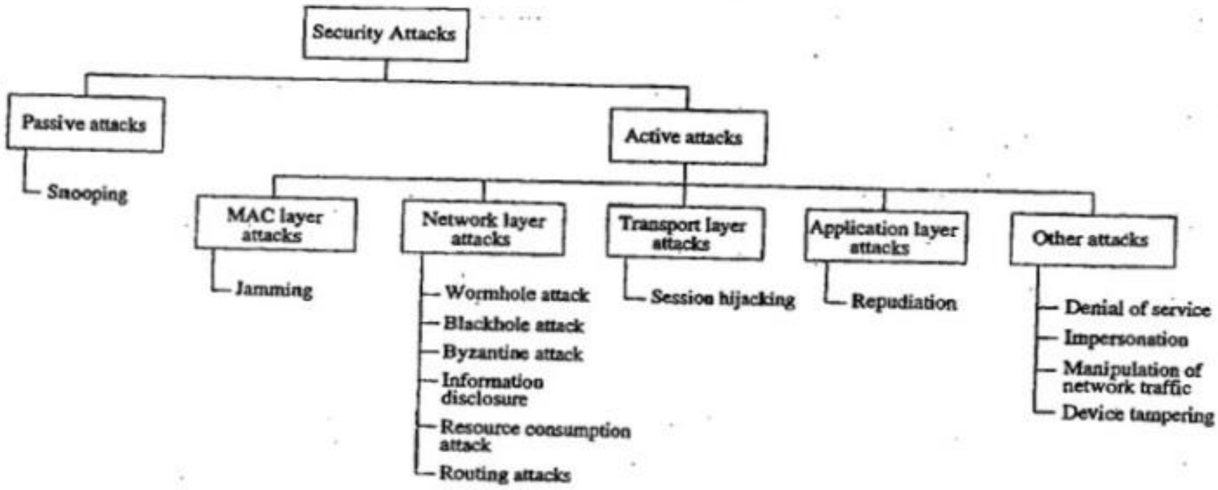

Figure 9.11. Classifications of attacks.

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.

NETWORK LAYER ATTACKS

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:*

      - 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.