TRANSPORT LAYER

INTRODUCTION

The objectives of transport layer protocol include the setting up of an end-to-end connection, end-to-enddelivery 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 throughneighbouring 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 thechannel
   - 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/delayunfairness 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 acrosscontending flows
3. Separation of congestion control, reliability and flow control:
   - A transport layer protocol can provide better performance if end-to-end reliability, flowcontrol 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 importantresources: (i) power source and (ii) bandwidth
   - The performance of a Transport layer protocol is significantly affected by these resourceconstraints
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, hiddenterminal 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

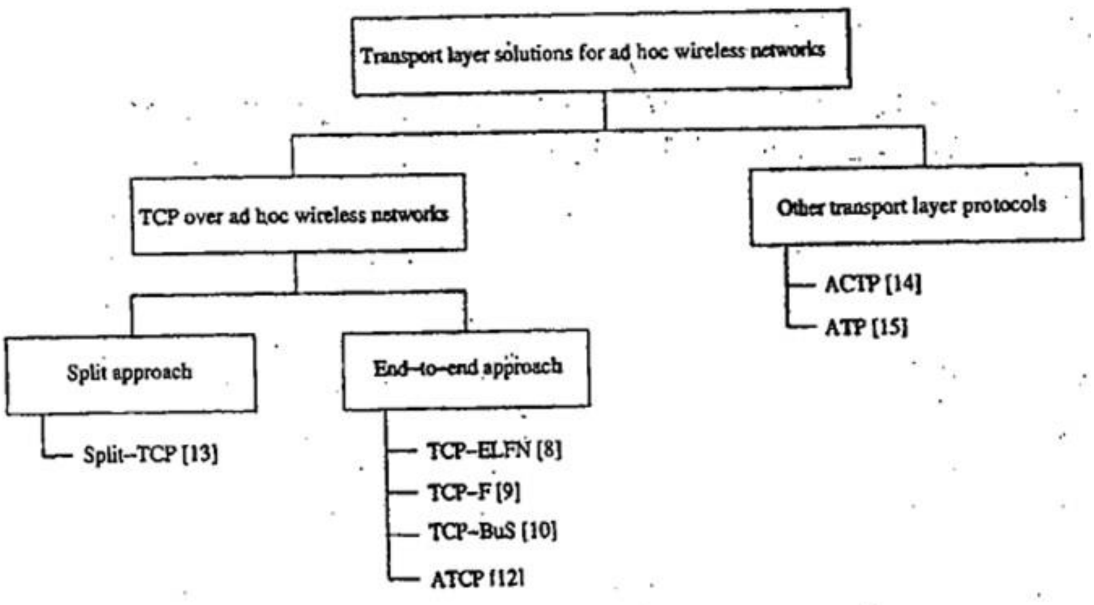

Figure 9.1. Classification of transport layer solutions.

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.

The major reasons behind throughput degradation that TCP faces when used in ad hoc wireless networks 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.

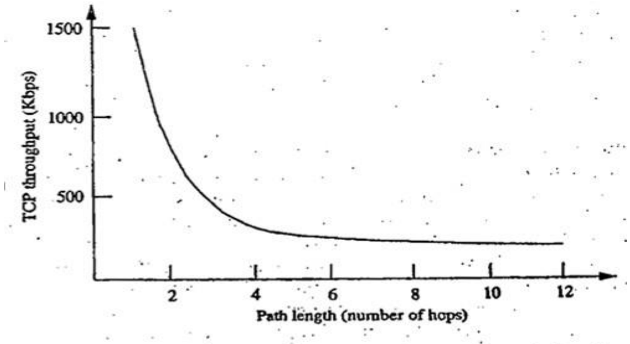

Figure 9.3. Variation of TCP throughput with path length.

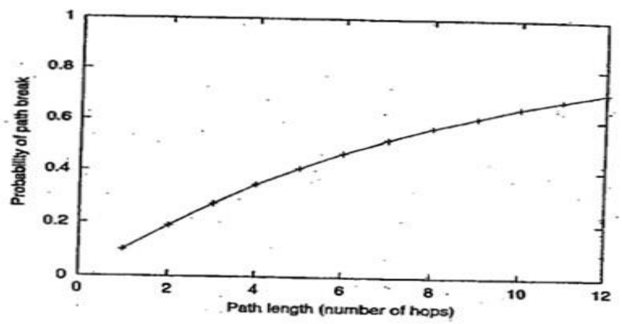

Figure 9.4. Variation of p_b with path length ($p_l = 0.1$).

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. Uni directional 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:

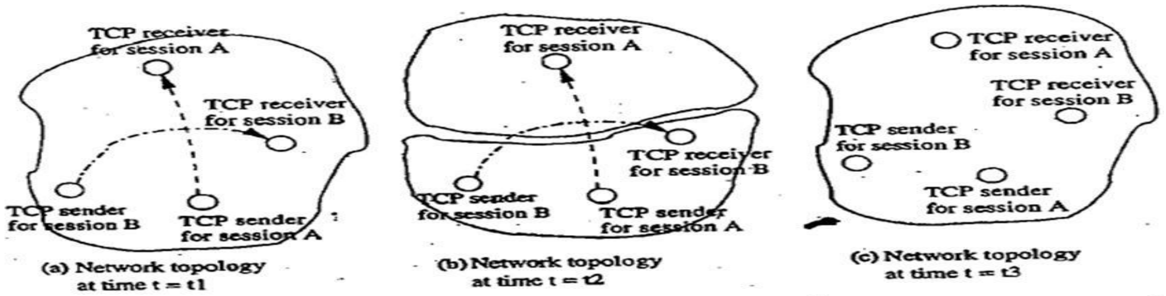

Figure 9.5. Effect of partitioning and merging of network.

- Fig below 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 experiencespath 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, 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.

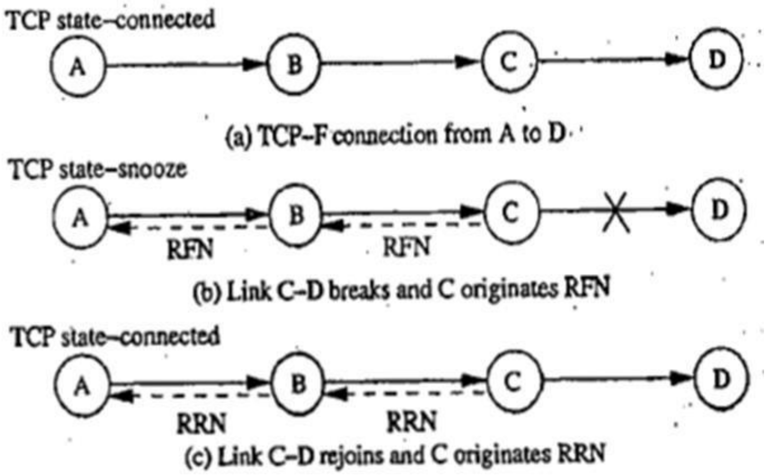

Figure 9.6. Operation of TCP-F.

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 acheivable transmission rate acceptable to the network and the TCP-F receiver.

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

- Improves 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 theorigination 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 ondetection 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.

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.

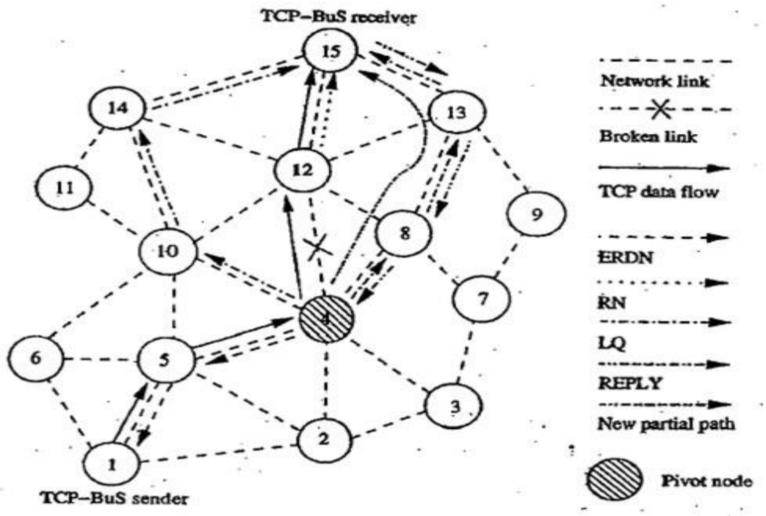

Figure 9.7. Operation of TCP-BuS.

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 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 or*
  - *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.

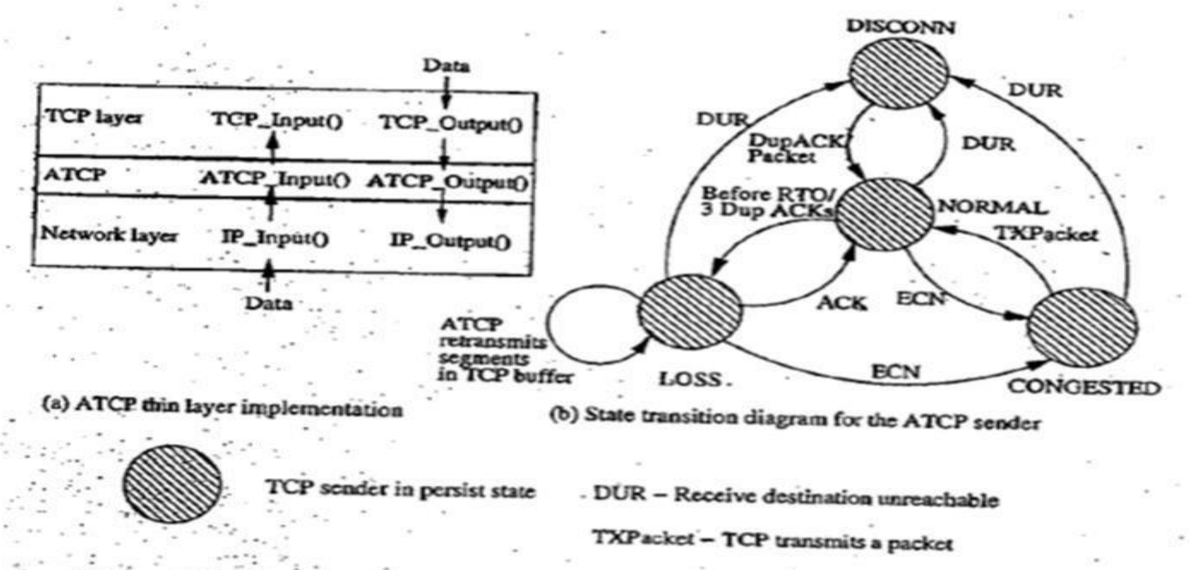

Figure 9.8. An illustration of ATCP thin layer and ATCP state diagram.

- Major function of the ATCP Layer is that it monitors the :
  - Packet sent and received by TCP sender,
  - The state of the TCP sender,
  - State of the network.

- 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 notinterfere 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 is the degradation ofthroughput with increasing path length.
- This can also lead to unfairness among TCP sessions where one session may obtain much higherthroughput 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 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.

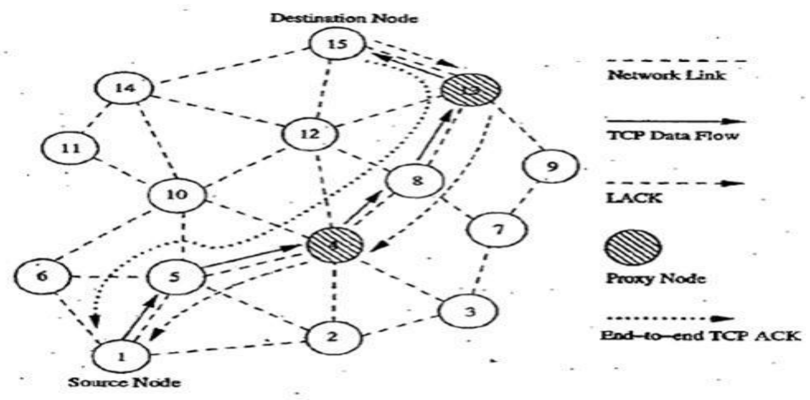

Figure 9.9. An illustration of Split-TCP.

Advantages:

Improved throughput.

Improved throughput fairness.

Lessened impact of mobility.

Disadvantages:

Requires modifications to TCP protocol.

End to End connection handling oftraditional TCP is violated.

The failure of proxy nodes can leadto throughput degradation.

OTHER TRANSPORT LAYER PROTOCOLS FOR AD HOC WIRELESS NETWORKS

APPLICATION CONTROLLED TRANSPORT PROTOCOL

- It is a light-weight transport layer protocol
- Assigns the responsibility of ensuring reliability to the application layer
- ACTP stands in between TCP and UDP where TCP experiences low performance with high reliabilityand UDP provides better performance with high packet loss in Adhoc wireless networks
- The key design philosophy of ACTP is to leave the provisioning of reliability to the application layer and provide a simple feedback information about the delivery status of packets to the application layer
- Supports the priority of packets to be delivered
- Each API function call to send a packet contains the additional information required for ACTP such as the maximum delay, message number and priority of the packet
- Delivery status is maintained at the ACTP layer. This reflect
    - Successful delivery of the packet
    - A possible loss of the packet
    - Remaining time for the packet
    - No state information exists at the ACTP layer

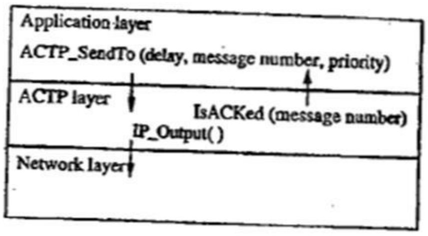

Figure 9.10. An illustration of the interface functions used in ACTP.

Advantages:

Provides freedom of choosing the requiredreliability level to the application layer

Scalable for large networks

Throughput is not affected by path breaks

Disadvantage:

Not compatible with TCP

AD HOC TRANSPORT PROTOCOL

- ATP is specifically designed for ad hoc wireless networks and is not a variant of TCP
- The major aspects by which ATP defers from TCP are
    - Coordination among multiple layers
    - Rate-based transmissions
    - Decoupling congestion control and reliability
    - Assisted congestion control
- ATP uses services from network and MAC layers for improving its performance
- ATP uses information from lower layers for
    - Estimation of the initial transmission rate
    - Detection, avoidance and control of congestion
    - Detection of path breaks
- ATP utilises timer-based transmission
- The network congestion information is obtained from the intermediate nodes
- Field in which delay information is included is referred as rate feedback field
- ATP has three phases namely: increase, decrease and maintain

Advantages:

- Improved performance
- Decoupling congestion control and reliability mechanisms
- avoidance of congestion window fluctuations

Disadvantage:

- lack of interoperability with TCP