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
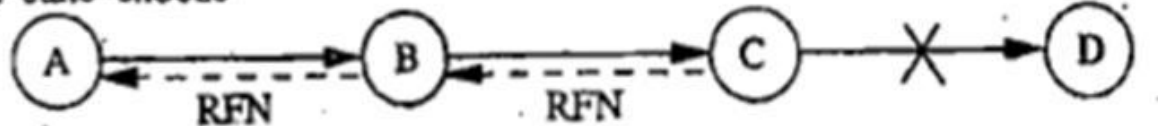
Operation:
▪ In TCP-F, an intermediate node, upon detection of a path break, originates route failure notification (RFN) packet. This intermediate node is called Failure point (FP).
▪ This RFN packet is routed toward the sender of the TCP session, Sender information that is obtained from TCP packets.
▪ 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.
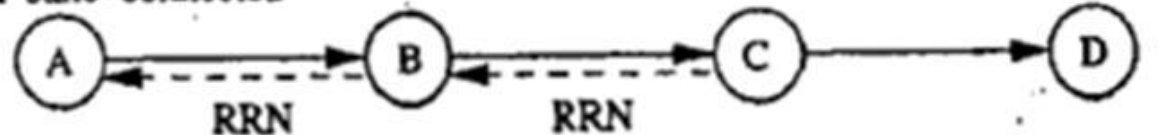

Figure 9.6. Operation of TCP-F.

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 achievable 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 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.

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.
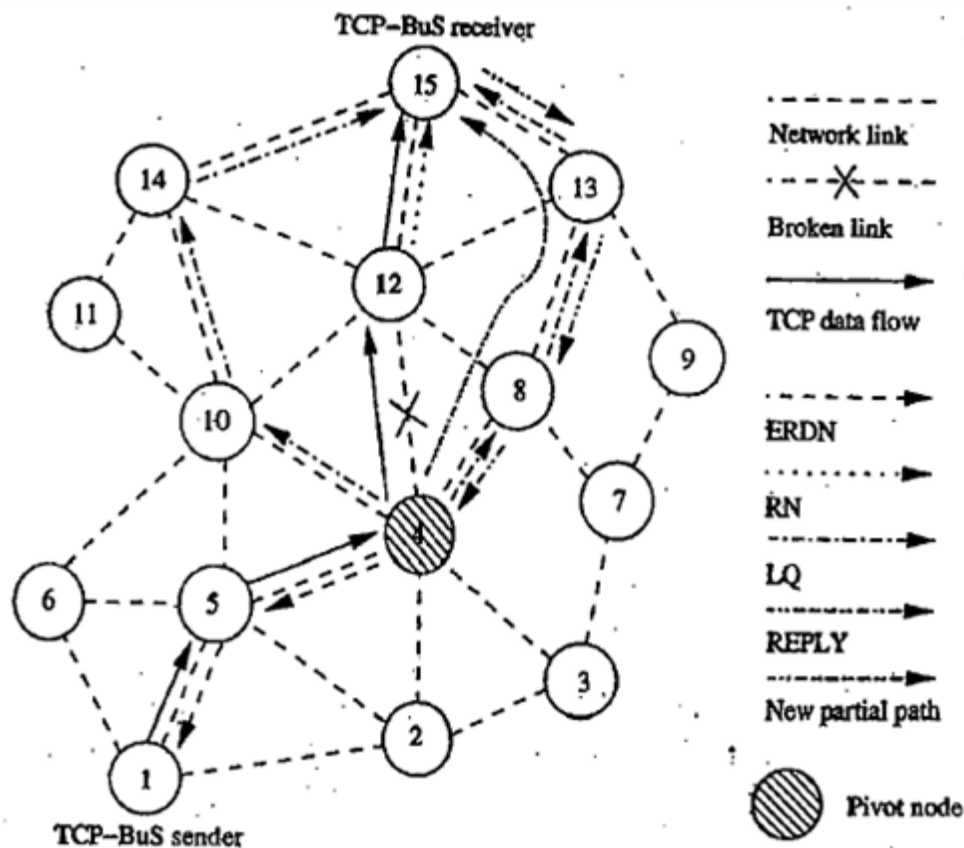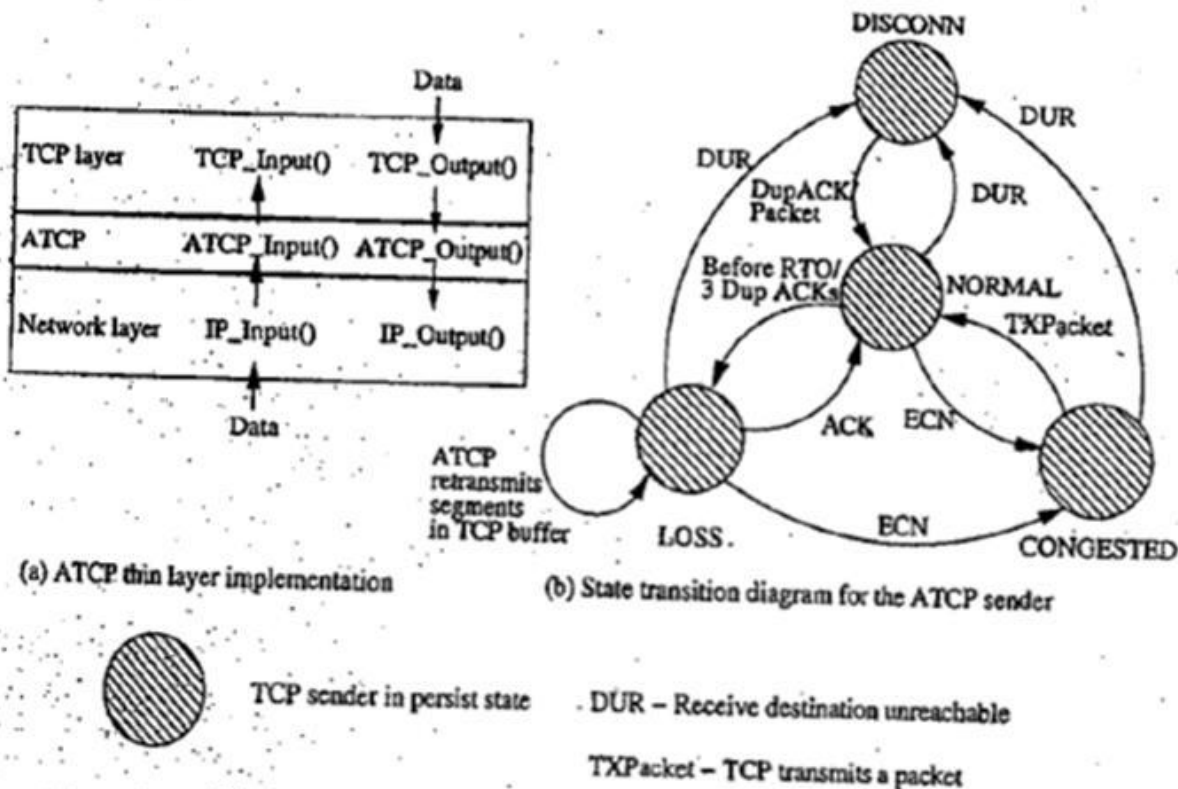

Figure 9.7. Operation of TCP-BuS.

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.

(a) ATCP thin layer implementation

(b) State transition diagram for the ATCP sender

TCP sender in persist state

DUR – Receive destination unreachable

TXPacket – TCP transmits a packet

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.
- 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 is 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 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.
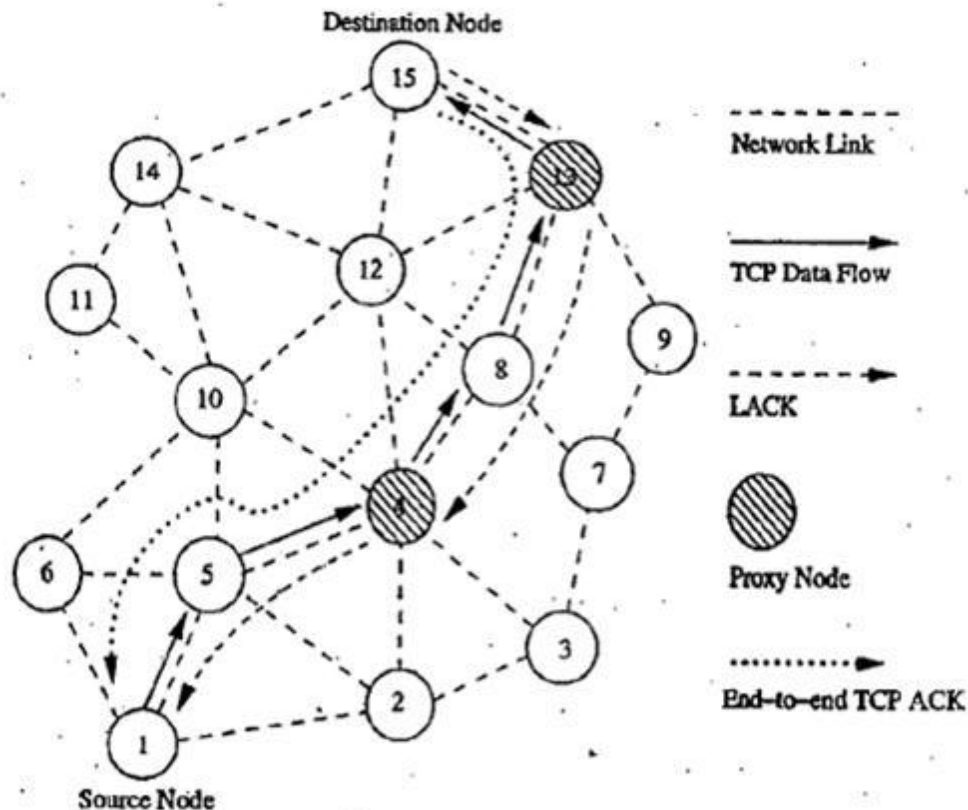

Figure 9.9. An illustration of Split-TCP.

Advantages:
- ☐ Improved throughput.
- ☐ Improved throughput fairness.
- ☐ Lessened impact of mobility.

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