Unit- V

TRANSPORT LAYER AND SECURITY PROTOCOLS

Introduction:

The objectives of a transport layer protocol include the setting up of an end-to-end connection, end-to-end delivery of data packets, flow control and congestion control. There exist simple, unreliable and connection-less transport layer protocol such as UDP, and reliable, byte-stream-based and connection-oriented transport lay Protocols such as TCP for wired networks.

These traditional wired transport layer protocols are not suitable for ad-hoc wireless networks. So we have to design the transport layer protocol that should suitable for ad-hoc wireless netwo

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

1. Induced Traffic:

Ad-hoc wireless network consist of multiple link path The traffic at any given link due to the traffic through neighbour links/path is referred to as induced traffic. This is due to

- The broadcast nature of the radio channel.
- the location-dependent contention on the channel.

This affects the throughput achieved by the protocol.

www.jntufastupdates.com

Scanned by CamScanner

2. Induced Throughput Unfairness:

This is refers to the Throughput unfairness at the trans-port Layer due to the throughput / delay unfairness existing at the lower layer such as the network and MAC Layer. So, we have to design a Transport Layer protocol, that should consider these in order to provide a fair share of Throughput across contending flows.

3. Separation of Congestion Control, Reliability and flow Control:

The protocol can provide better performance if reliability, flow control and congestion control are handled separately. Reliability and flow-control are end to end activities. whereas congestion control can at times be a local activity. while separating these, the main objective to be considered is the minimization of the additional control overhead generated by them.

4. Power & Bandwidth Constraints:

The important resource constraints are Power source and Bandwidth. The performance of a protocol is significantly affected by these resource constraints.

5. Misinterpretation of Congestion:

Tradition mechanisms of detecting congestion in networks, such as packet Loss and retransmission timeout, are not suitable in for adhoc Networks.

This is because following parameter can also lead to packet loss

→ high error rates of wireless channel.

www.jntufastupdates.com

Scanned by CamScanner

→ Location - dependent contention
→ hidden terminal problem
→ Packet collisions in the network
→ Path breaks due to mobility of node
→ node failure due to drained battery.

6. Completely Decoupled Transport Layer:

Another challenge faced by Transport Layer protocol is the interaction with the lower layers. wired network transport layer protocols are almost completely decoupled from the lower layer. In ad-hoc networks, cross-layer interaction between the transport layer and lower layers is important to adapt to the changing network environment.

7. Dynamic Topology:

Ad-hoc wireless networks experience rapidly changing network topology due to mobility of nodes. This leads to frequent path breaks partitioning and remerging of networks and high delay in re-establishm of paths. Hence, the performance of a transport layer protocol is significantly affected by the rapid changes in the network topology.

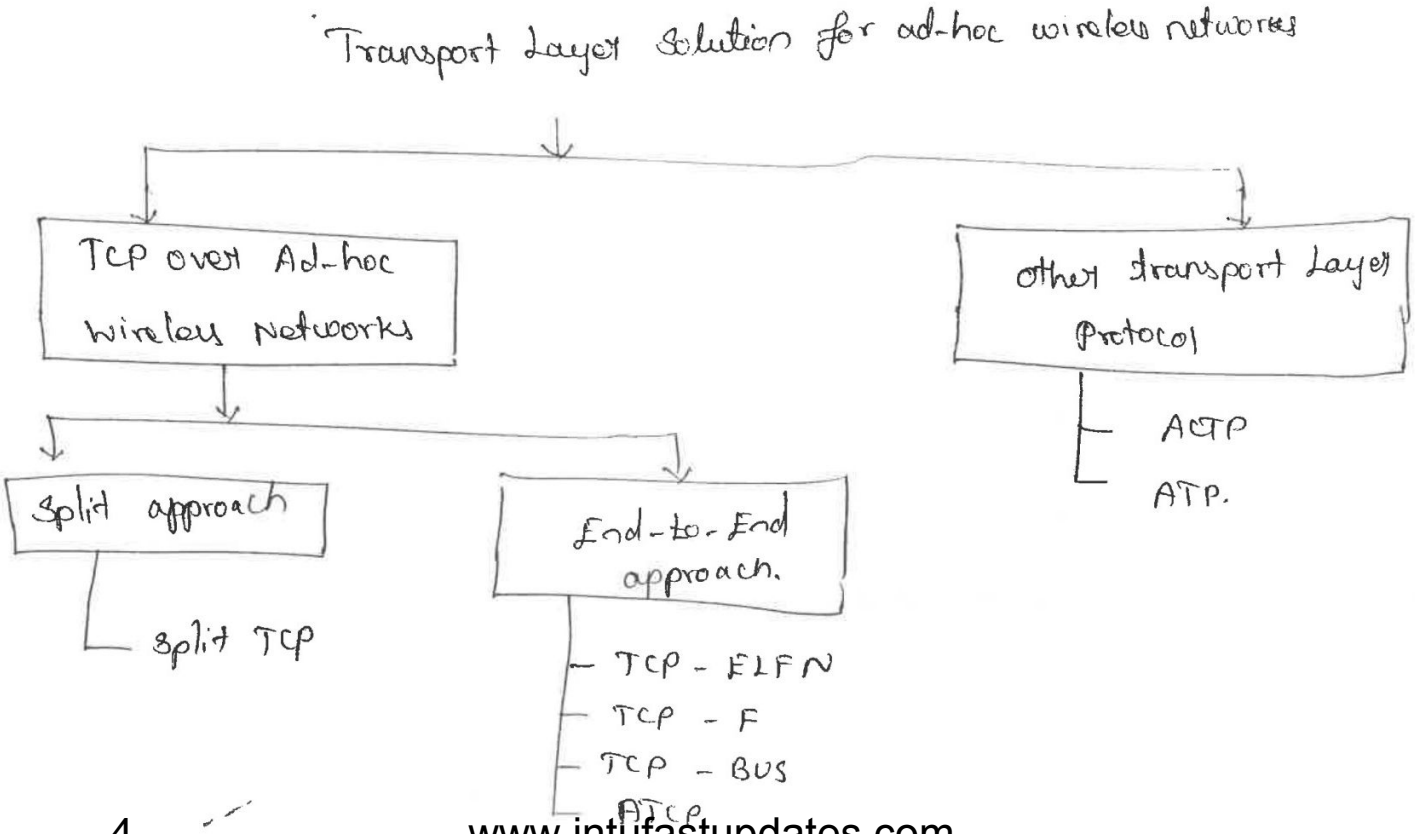
Design Goals of Transport Layer Protocol:

- The protocol should maximize the throughput per connection.
- It should provide throughput fairness across contending flows
- It should incur minimum connection setup and connection maintenance overheads.
- It should have mechanisms for congestion control and flow control in the network.

www.jntufastupdates.com
Scanned by CamScanner

- 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 dynamic changes in network 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 for effective, scalable and protocol-independent interaction with lower layer.
- It should maintain End-to-end semantics.

Classification of Transport Layer Solution:



www.jntufastupdates.com
Scanned by CamScanner

TCP OVER AD-HOC WIRELESS NETWORKS:

The transmission Control protocol (TCP) is the most predominant transport layer protocol in the Internet today.

TCP is a reliable, end-to-end, connection-oriented Transport layer Protocol, that Provides a byte stream based service [The stream of bytes from the application layer is split into TCP segments, the length of each segment limited by a Maximum Segment Size]

The major responsibilities of TCP include

→ Congestion Control : It deals with excess traffic in the netw which may lead to degradation in the performance of the netw

→ Flow control : flow control controls the pot-flow traffic such th the receiver capacity is not exceeded. TCP regulates the num of packet sent to the network by expanding and shrinking th Congestion Window

→ In order delivery of packet

→ Reliable transportation of packet.

Why Does TCP Not perform well in Ad-hoc Wireless Networks:

The Major reasons behind throughput degradation that TCP faces when used in ad-hoc wireless networks are the following.

Misinterpretation of packet Loss:

In traditional TCP design, the packet loss is mainly attributed to network congestion.

www.jntufastupdates.com

Scanned by CamScanner

In Adhoc wireless network, there are somany reasons for packet loss. They are

- high error rate of wireless channel
- location - dependent contention
- hidden terminal problem
- packet collision in the network
- Path breaks due to mobility of nodes and
- node failure due to drained battery.

2. Frequent Path Breaks:

Ad-hoc wireless network experience dynamic changes in network topology because of the unrestricted mobility of the nodes in the network. Once a path is broken, the routing protocol initiates a route reestablishment process. This process takes a significant amount of time to obtain a new route to the destination. The route re-establishment time is a function of the number of nodes in the network, transmission ranges of nodes, current topology of the network, bandwidth of the channel, traffic load in the network and the nature of the routing protocol.

If the route reestablishment time is greater than the RTO period (Retransmission Time out) of the TCP sender, then the TCP sender assumes congestion in the network, retransmits the lost packets and initiates the congestion control algorithm. These retransmission can lead to wastage of bandwidth and battery power.

3. Effect of path length:

It is found that the TCP throughput degrades rapidly

www.jntufastupdates.com

Scanned by CamScanner

with an increase in path length of the adhoc wireless Networks. This is shown in figure. The possibility of a path break increases with path length. Given that,

The probability of a link break $= P_l$

The probability of path break $= P_b$

path length (no. of hops to reach destination) $= k$

$$\therefore \quad P_b = 1 - (1 - P_l)^k$$

Hence as the path length increases, the probability of a path break increases, resulting in the degradation of the throughput in the network.

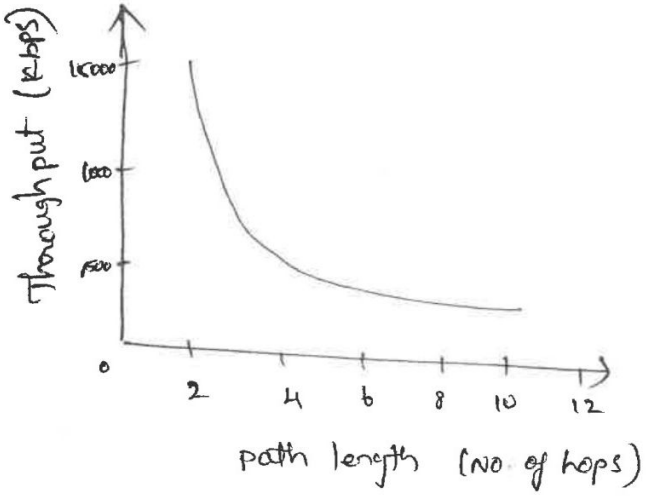


fig: Variation of TCP Throughput with path length

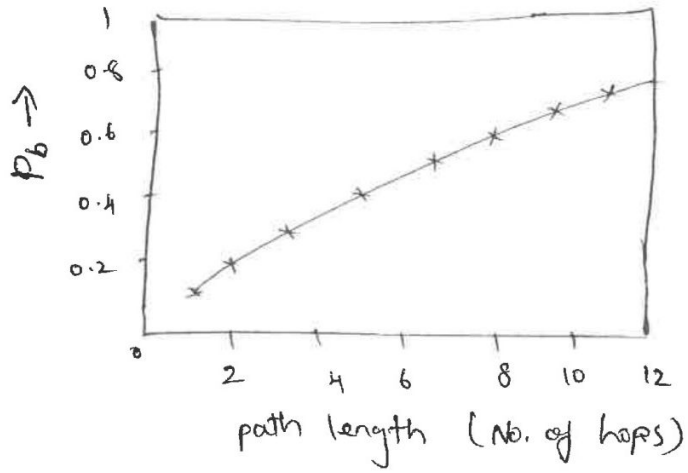


fig: Variation of P_b with path length ($P_l = 0.1$)

Misinterpretation of Congestion Window:

TCP considers the congestion window as a measure of rate of transmission that is acceptable to the network and the receiver. In ad-hoc wireless networks, the congestion control mechanism is invoked when the network get partitioned or when a path break occurs.

www.jntufastupdates.com

Scanned by CamScanner

This reduces the congestion window and increases the RTO period. When the route is reconfigured, the congestion window may not reflect the transmission rate acceptable to the new route, as the new route may actually accept a much higher transmission rate. Hence, when there are frequent path breaks, the congestion window may not reflect the maximum transmission rate acceptable to the network and the receiver.

Asymmetric Link behavior:

The radio channel used in ad-hoc wireless networks has different properties such as location-dependent contention, environmental effects on propagation and directional properties leading to asymmetric links. The directional links can result in delivery of a packet to a node, but failure in the delivery of the acknowledgment back to the sender. This can also lead to TCP invoking congestion control algorithm and several retransmission.

Uni-directional path:

Traditional TCP relies on end-to-end ACK for ensuring reliability. Since the ACK packet is very short compared to a data segment, it consumes less bandwidth in wired Network.

In ad-hoc wireless network, every TCP-ACK packet requires RTC-CTS-DATA-ACK exchange. This can lead to an additional overhead of more than 70 bytes if there are no retransmissions. This can lead to significant bandwidth consumption on the reverse path.

Some routing protocol select the forward path as the reverse path whereas certain other routing protocols use entirely or partially different path for the ACKs.

www.jntufastupdates.com

Scanned by CamScanner

∴ A path break on an entirely different reverse path can affect the performance of the network as much as a path break in the forward path

Multipath Routing:

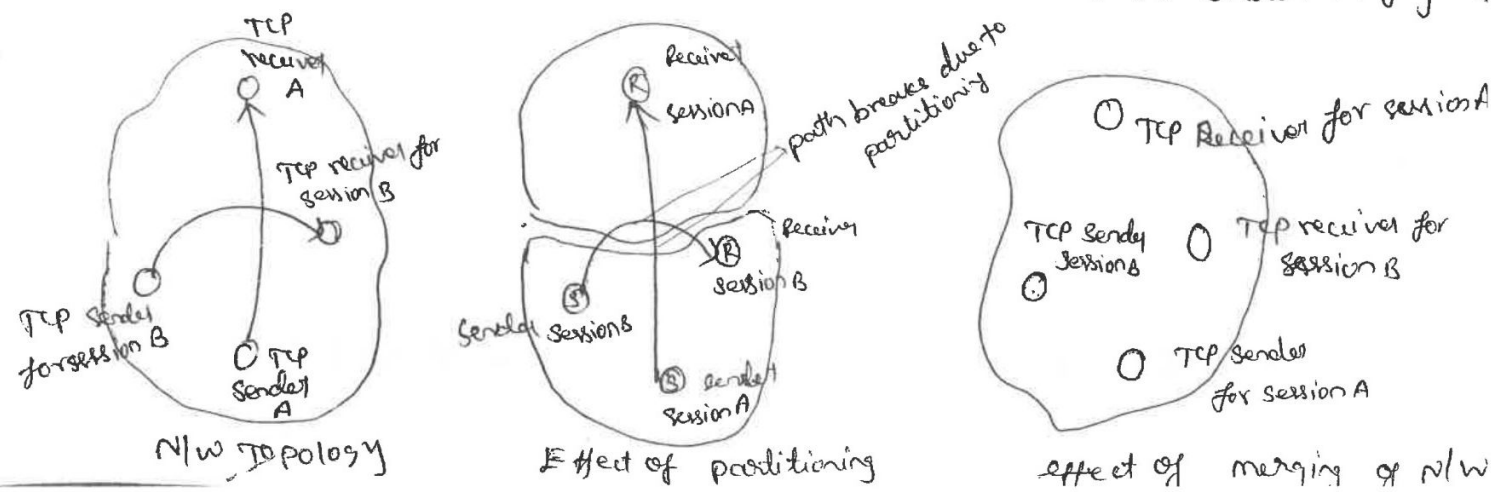
There exists a set of QoS routing and best-effort routing Protocols that use multiple paths between a source-destination pair. There are several advantages in using multipath routing. Some of these advantages include the reduction in route computing time, the high resilience to path breaks and better security.

For TCP, these advantages may add to throughput degradation These can lead to a significant amount of out-of-order packets, which in turn generates a set of duplicate acknowledgments (DUPACKS) which cause additional power consumption and invocation of congestion control.

Network partitioning and remerging:

The randomly moving nodes in an ad-hoc wireless network can lead to network partitions. As long as the TCP sender, the TCP receiver and all the intermediate nodes remain in the same partition, the TCP connection will remain intact. If sender and receiver of the TCP section will remain in different partition, then only the intermediate nodes are effected by partitions.

A network with two TCP session A & B is shown in figure.



www.jntufastupdates.com

Scanned by CamScanner

The use of sliding-window based transmission:

TCP uses a sliding window for flow control. The transmission of packets is decided by the size of the window and when the ACK arrive from a destination, further packets are transmitted.

The use of a sliding window can also contribute to degraded performance in bandwidth-constrained ad-hoc wireless network.

— x —

TCP over ad-hoc wireless networks Protocols

Feedback based TCP [TCP-F]:

- Improves performance of TCP
- Uses a feedback based approach
- TCP-F requires the support of a reliable link layer and a routing protocol that can provide feedback to the TCP sender about the path breaks.
- The routing protocol is expected to repair the broken path within a reasonable time period.
- TCP-F aims to minimize the throughput degradation resulting from the frequent path breaks that occur in ad-hoc wireless networks.

Operation:

- An intermediate node, upon detection of path break, originates route-failure-notification (RFN) packet. This intermediate-node is called Failure-point (FP).

www.jntufastupdates.com

Scanned by CamScanner

- The RFN packet is routed towards the sender of the TCP session.
- If any intermediate node that receive RFN packet has an alternate route to the same destination, then it
  - → discards the RFN packet &
  - → uses the alternate path for forwarding further data packets, thus reducing control overhead involved in the route reconfiguration process.
- When sender receives an RFN packet, it goes into state called Snooze.
- In Snooze state, a sender,
  - → stops sending any more packets to the destination
  - → cancels all timers
  - → freezes its congestion window
  - → freezes the retransmission timer
  - → setup a route failure timer.
- When route failure timer expires, the 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.

Advantage:

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

www.jntufastupdates.com

Scanned by CamScanner

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 a 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.

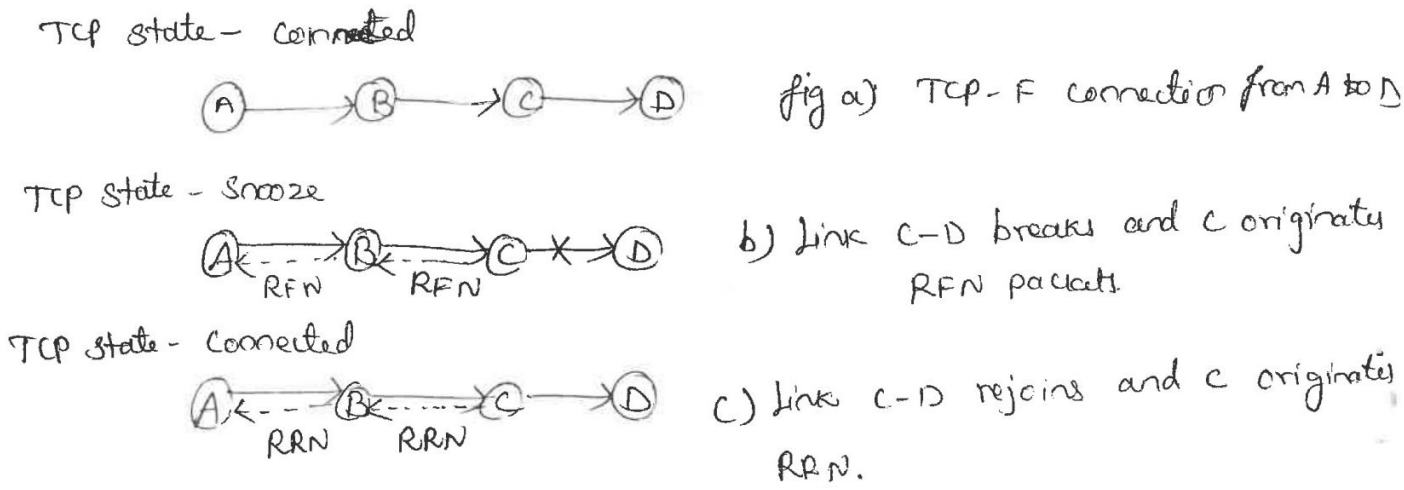


figure: operation of TCP-F

TCP with Explicit Link Failure Notification (TCP-ELFN):

- Improves TCP performance in ad-hoc network
- Similar to TCP-F

Operation:

- An intermediate node, upon detection of a path break, originates ELFN packet.

www.jntufastupdates.com
Scanned by CamScanner

- It uses the TCP- probe packets for detecting the route reestablishment.

- The ELFN can be implemented in two ways.

  → By sending an ICMP destination unreachable (DUR) message to the sender (or)

  → By piggy-backing this information on the Route Error message that is sent to the sender.

- Once the sender receives the ELFN packet, it disables its retransmission timers and enters a standby state.

- In standby state, it periodically originates probe packets to see if a new route is established.

- Upon reception of an ACK by the 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.

DisAdvantage:

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

—x—

www.jntufastupdates.com

Scanned by CamScanner

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.

Operation:

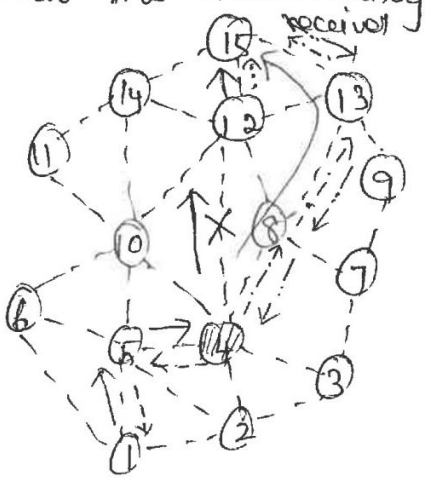
- An upstream intermediate node, upon detection of path break, Originates ERDN (Explicit route disconnection notification) message.
- This ERDN packet is propagated to the TCP-Bus sender, upon receiving this packet, the TCP-sender
  → Stops transmission & freezes all timers and windows as in TCP-F.
- The intermediate node which ~~receives~~ originates ERDN packet is called Pivot node (PN).
- The packets in transit at the intermediate nodes from the TCP sender to the PN are buffered until a new partial path from the PN to the TCP-receiver is obtained by the PN.
- The downstream node, upon detection of a path break, Originates Route Notification (RN) packet to TCP-Receiver.
- PN attempts to find new partial path (route) to the TCP-receiver, and the availability of such a partial path to destination is intimated to the sender through an explicit route ~~successful~~ successful notification (ERSN) packet.

www.jntufastupdates.com

Scanned by CamScanner

- TCP utilizes route reconfiguration mechanism of ABR to obtain partial path to the destination.

- TCP - sender also periodically originates probe packets to check the availability of a path to the destination.



TCP - Bus sender

- - - - Network Link
-X- Broken Link
⟶ TCP data flow
- - -> ERDN
. . . .> RN
-.-.-> Local Query packet
-..-> Reply.
—— Note path
pivot node.

Advantage:

- 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

DisAdvantage:

- 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.

Scanned by CamScanner

Ad-hoc TCP: (ATCP)

- Similar to TCP-F and TCP-ELFN, ad-hoc TCP (ATCP) also uses feedback Mechanism.
- 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.
- If an intermediate node loses a packet due to error, then the ATCP at the TCP sender immediately retransmits it without invoking the Congestion Control Algorithm.
- ATCP is implemented as a thin layer 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.
- The 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:

  NORMAL, CONGESTED, LOSS, DISCONN.

www.jntufastupdates.com

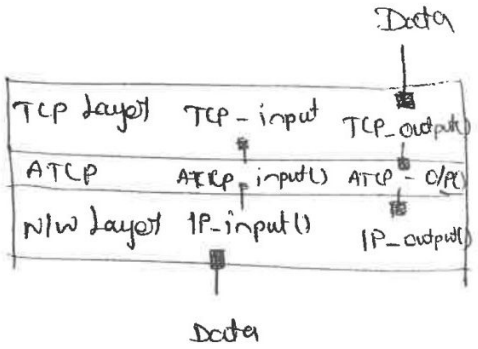
Scanned by CamScanner

- When packet are lost or arrive out of order at the destination, it generates duplicate ACKs, In traditional TCP, upon reception of duplicate ACKS, the TCP sender retransmits the segment under consideration and shrinks the contention window.

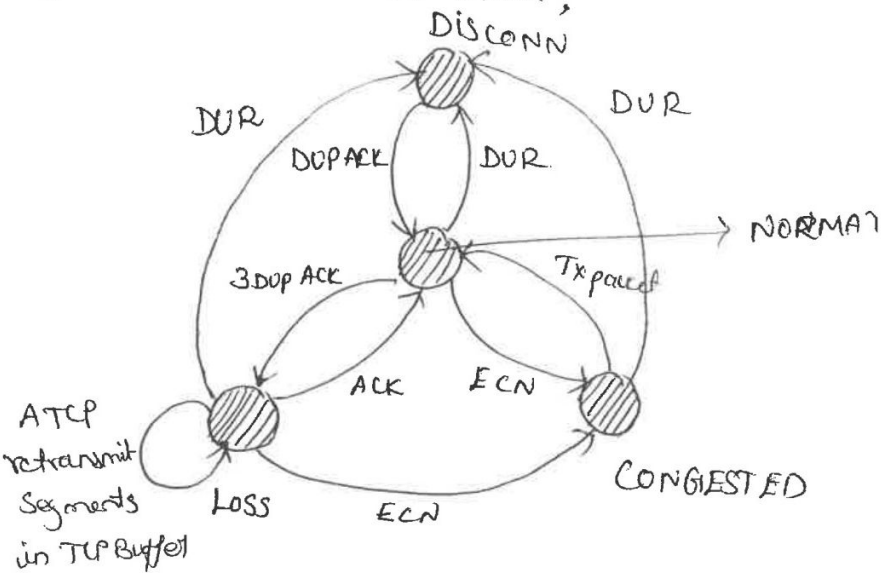
- But the ATCP sender counts the number of duplicate ACKs received and if it reaches three, instead of forwarding the duplicate ACKs to TCP, It puts TCP in the Persist state and ATCP in the Loss state.

- Hence, the TCP sender avoids invoking congestion control. In the Loss state, ATCP retransmits the unacknowledged segments from the TCP buffer.

- When a new ACK comes from the TCP receiver, it is forwarded to TCP and the TCP sender is removed from the persist state and then the ATCP sender changes to the normal state.



a) ATCP thin layer implementation.



DUR – Receive destination Unreach

TCP sender in persist state.

b) State transition diagram.

ECN - Explicit congestion Notification

www.jntufastupdates.com
Scanned by CamScanner

- The ATCP Layer essentially make use of the explicit Congestion notification (ECN) for maintain states.

- When the ATCP Sender is in the Loss State, if it receives ECN message, changes it state to the congested state. Along with this state, the ATCP sender removes the TCP sender from the persist state.

- When the Network gets congested, the ECN flag is set in data and Ack packet. Then ATCP Sender receives this, it change the state from Normal to Congestion. Then TCP invoke congestion control Mechanism.

- When Route failure / Network partition, the Network Layer Send ICMP - Destination Unreachable (DUR) packet to ATCP. Upon reception of the DUR, ATCP put TCP in to persist state and enters in to Disconn State.

- It remains in the DISCONN state until it is connected and receives any data / DUP Ack packets. On the occurrence of any of these events, ATCP changes to the NORMAL state.

In summary, ATCP tries to perform the Activities listed in Table.

Event	Action
1. Packet Loss due to high BER	Retransmits the lost packets without reducing congestion window.

www.jntufastupdates.com

Scanned by CamScanner

Event	ACTION
* Route recomputation delay	Makes the TCP Sender go to persist State and Stop transmission until new route has been found.
* Transient partitions	Makes the TCP Sender go to persist State and stop transmission until new route has been found.
* Out-of-order packet delivery due to multipath routing	Maintains TCP Sender unaware of this and retransmits the packets from TCP buffer.
* Change in route	Recomputes the congestion window.

Advantages:

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

Disadvantage:

- 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.

—— x ——

www.jntufastupdates.com

Scanned by CamScanner

SPLIT TCP:

- Major issues that affect the performance of TCP over ad-hoc network is the degradation of throughput with increasing path length.
- the short connections generally obtain much higher throughput than long connections.
- 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.
- A proxy node
  - → receives the TCP packets
  - → reads its contents
  - → stores it in its local buffer and
  - → sends local acknowledgement (LACK) to the source (or) the previous proxy.
- LACK does not guarantee end to end delivery.
- The responsibility of further delivery of packet is assigned to the proxy node.
- A proxy node clears a buffer packet once it receives

www.jntufastupdates.com
Scanned by CamScanner

LACK from the immediate successor proxy node for that packet.

- The number of proxy nodes in TCP session is determined by the length of the path between source and 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.

fig: An illustration of Split-TCP.

- In the above figure, node 1 initiates a TCP session to node 15. Node 4 and node 13 are chosen as proxy nodes.

- In figure, The path between node 1 and node 4 is the first zone (segment), the path between node 4 and node 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 node 1, acknowledges it with a LACK packet, and buffers the received packets. This buffered packet is forwarded to the next proxy node.

- The transmission control window at the TCP sender is also

www.jntufastupdates.com
Scanned by CamScanner

split into two windows, that is, the congestion window and the end-to-end window.

- Congestion window changes according to the rate of arrival of LACKs from proxy node.
- End-to-end window is updated based on the arrival of end-to-end ACKs.

Advantages:

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

Disadvantage:

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

—— x ——

Note:

Split-TCP maintains the end-to-end acknowledgment mechanism intact, irrespective of the addition of zone-wise LACKs. The source node clears the buffered packets only after receiving the end-to-end acknowledgment for those packets.

www.jntufastupdates.com

Scanned by CamScanner

A Comparison of TCP Solution for Ad-hoc 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

www.jntufastupdates.com

Scanned by CamScanner

Other transport layer protocols for ad-hoc wireless Networks:

Application Controlled Transport Protocol (ACTP)

- It is a light-weight transport layer protocol.
- It assigns the responsibility of ensuring reliability to the application layer. It is more like UDP with feedback of delivery.
- It stands in between TCP and UDP where
  - → TCP experiences low performance with high reliability &
  - → UDP provides better performance with high packet loss in Adhoc wireless network.
- The key design philosophy is to
  - → Leave the provisioning of reliability to the application layer &
  - → Provide simple feedback information about the delivery status of packets to the application layer.
- It support the priority of packets to be delivered.
- Each API function call to send a packet contains information such as
  - → maximum delay, message number & priority of the packet.
- Delivery status is maintained at the ACTP layer, this reflect
  - → successful delivery of the packet.
  - → possible loss of packet
  - → Remaining time for the packets

www.jntufastupdates.com
Scanned by CamScanner

→ No state information exists at the ACTP Layer.

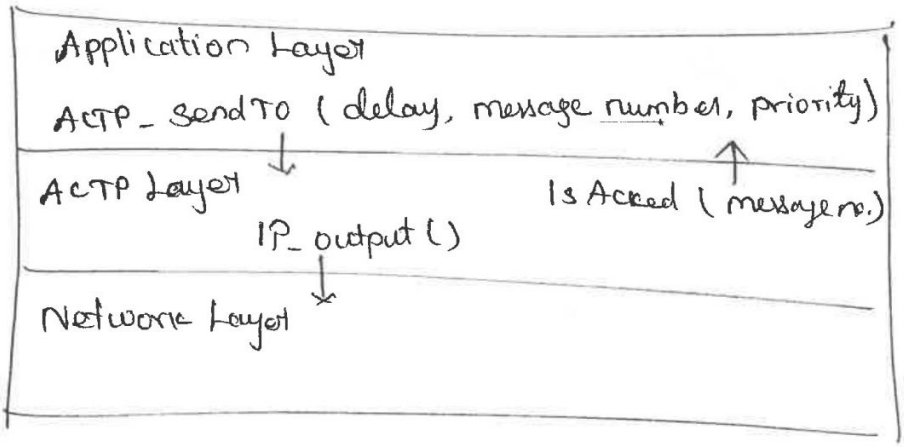


fig: An illustration of the interface function used in ACT

Advantages:

- Provides freedom of choosing the required reliability level to the application Layer.
- Scalable for large networks.
- Throughput is not affected by path breaks.

DisAdvantage:

- Not Compatible with TCP.

—x—

ADHOC TRANSPORT PROTOCOL (ATP):

- It is specifically designed for ad-hoc networks and is not a variant of TCP.
- It differs from TCP in following Major Aspects
  - → Co-ordination among multiple Layers
  - → Rate-based transmissions
  - → Decoupling congestion control & reliability

Scanned by CamScanner

→ Assisted Congestion control

- It uses services from network & MAC layer for improving its performance.
- It uses information from Lower layers for
  - → Estimation of the initial transmission-rate
  - → Detection, Avoidance and control of congestion
  - → Detection of path breaks.
- It utilizes timer-based transmission (RTO).
- The network congestion information is obtained from the intermediate nodes.
- Field in which delay information is included is referred as rate feedback field.
- It has three phases namely: increase, decrease and maintain.

Advantages:

1) Improved performance
2) Decoupling congestion control and reliability Mechanism
3) Avoidance of congestion window fluctuations

DisAdvantage:

1. Lack of interoperability with TCP.

—— x —— x —— x ——

www.jntufastupdates.com

Scanned by CamScanner

→ The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path. [Depends upon distance b/w nodes that form a link and Load on link]

→ This metric does not balance the load on that link. so that uniform consumption of power is maintained throughout the network.

→ The Disadvantages of this metric include selection of paths with large hop length, inability to measure the power consumption of a link in advance when load varies, and the inability to prevent the fast discharging of batteries at some nodes.

- Maximize Network Connectivity:

  - This metric attempts to balance the routing load among the cut-set [the subset of the nodes in the network, the removal of which result in network partitions].

  - This assumes significance in environments where network connectivity is to be ensured by uniformly distributing the routing load among the cut-set.

  - with a variable traffic rate and unbounded contention in the network, it is difficult to achieve a uniform battery draining rate for the cut-set.

- Minimum Variance in Node Power levels:

  - This metric proposes to distribute the load among all nodes in the network so that the power consumption pattern remains uniform across them.

  - This problem is very complex when the rate and size of the data packets vary.

- Minimum cost per packet:

  - In order to maximize the life of every node in the

www.jntufastupdates.com

Scanned by CamScanner

network, this routing metric is made as a function of the state of the node's battery.

- A node's cost decreases with an increases in its battery charge and vice versa.
- Cost of node can be easily computed
- Advantage → congestion handling + cost calculation.

Minimize Maximum node cost:

- This metric minimizes the maximum cost per node for a packet after routing a number of packets or after a specific period.
- This delays the failure of a node, occuring due to higher discharge because of packet forwarding.

— x —

www.jntufastupdates.com

Scanned by CamScanner