TCP

- TCP stands for Transmission Control Protocol
- suite of communication protocols used to interconnect network devices on the internet
- communications standard that enables application programs and computing devices to exchange messages over a network.
- designed to send packets across the internet and ensure the successful delivery of data and messages over networks
- organizes data so that it can be transmitted between a server and a client
- guarantees the integrity of the data being communicated over a network
- guarantees the integrity of the data being communicated over a network
- ensures remains live until communication begins
- then breaks large amounts of data into smaller packets

Traditional TCP

- one of the core protocols of the Internet protocol suite
- reliable, guarantees in-order delivery of data and incorporates congestion control and flow control mechanisms
- intermediate layer between the Internet layer and application layer
- supports many of the Internet's most popular application protocols.
- One of the main challenges of TCP in mobile networks is the frequent handovers of mobile devices between different base stations or access points, which can result in packet losses, delays, and disruptions in the TCP connection.
- To address this issue, several techniques have been proposed to improve TCP performance in mobile networks, such as Fast Retransmit/Fast Recovery, Selective Acknowledgment (SACK), TCP Snooping, Congestion Control
- major responsibilities of TCP in an active session
  - not allow losses of data
  - Control congestions in the networks: to not allow degradation of the network performance
  - not exceed the receiver's capacity

Congestion Control

- this mechanism to avoid overloading the network with too much traffic
- TCP has been designed for fixed networks with fixed end- systems
- Congestion may appear from time to time even in carefully designed networks.

- this mechanism can cause problems in mobile networks where the available bandwidth can change rapidly.
- packet buffers of a router are filled and the router cannot forward the packets fast
- because the sum of the input rates of packets destined for one output link is higher than the capacity of the output link
- only thing a router can do in this situation is to drop packets
- dropped packet is lost for the transmission, and the receiver notices a gap in the packet stream
- receiver does not directly tell the sender which packet is missing
- but continues to acknowledge all in-sequence packets up to the missing one
- sender notices the missing acknowledgement for the lost packet and assumes a packet loss due to congestion
- Retransmission
- Several modifications to the congestion control algorithm have been proposed to adapt to the changing network conditions in mobile networks

Slow start

- behavior that TCP shows after the detection of congestion is called slow start
- start size of the congestion window is one segment (TCP packet)
- sender sends one packet and waits for acknowledgement
- acknowledgement arrives, the sender increases the congestion window by one
- This scheme doubles the congestion window every time the acknowledgements come back, which takes one round trip time (RTT)
- This is called the exponential growth of the congestion window in the slow start mechanism
- A slow start in the mobile transport layer refers to a phenomenon where the performance of the network is initially slow when a new connection is established

Fast retransmit/fast recovery

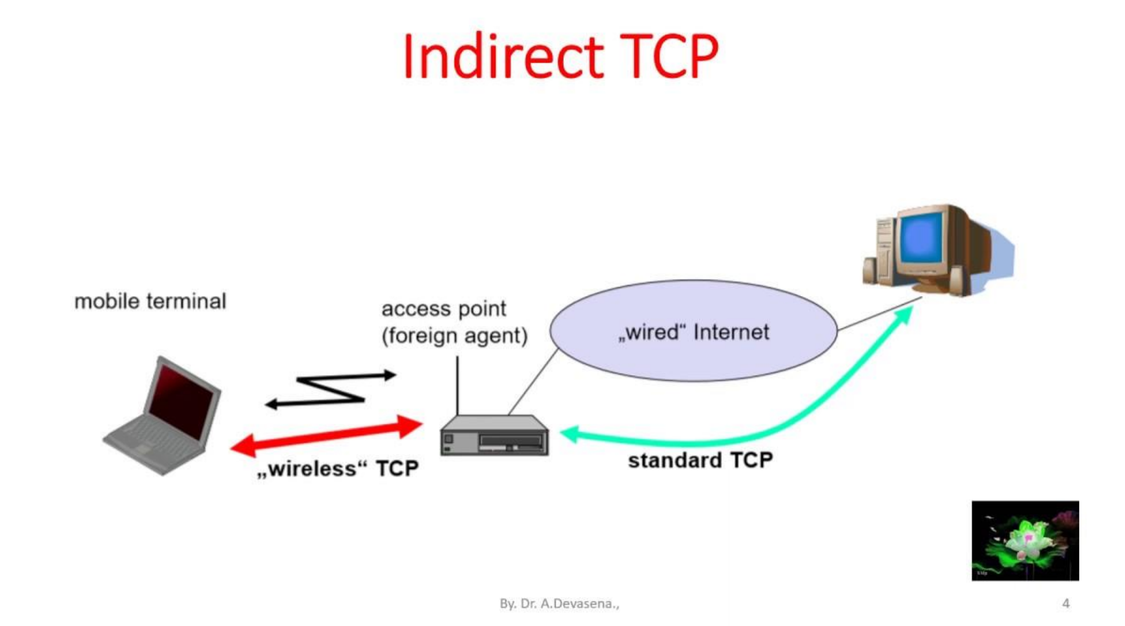
- used in the transport layer of the Internet Protocol (IP) to quickly recover from packet loss in a network
- commonly used in mobile networks to improve the reliability and performance of data transmission over wireless links
- Fast retransmit is a technique that allows the sender to detect packet loss without waiting for a timeout.
- When the sender receives three duplicate ACKs from the receiver, it assumes that the packet has been lost and immediately retransmits the packet without waiting for a timeout.

- This technique can significantly reduce the delay and improve the overall throughput of the network
- congestion threshold can be reduced because of two reasons
- First sender receives continuous acknowledgements for the same packet
- informs the sender that the receiver has got all the packets upto the acknowledged packet in the sequence and also the receiver is receiving something continuously from the sender
- gap in the packet stream is not due to congestion, but a simple packet loss due to a transmission error
- sender can now retransmit the missing packet(s) before the timer expires. This behavior is called fast retransmit

Problems with Traditional TCP in wireless environments

- Slow Start mechanism in fixed networks decreases the efficiency of TCP if used with mobile receivers or senders
- Mobility itself can cause packet loss
- many situations where a handover from one access point to another is not possible for a mobile end-system
- Standard TCP reacts with slow start if acknowledgements are missing
- does not really help during handover
- Packet loss is common in wireless networks due to interference, signal fading, and mobility.
- Traditional TCP assumes that packet loss is due to network congestion and reduces the sending rate. However, in wireless networks, packet loss can be due to factors other than congestion, and reducing the sending rate may not be the best approach

Indirect TCP



Indirect TCP

By. Dr. A.Devasena.,

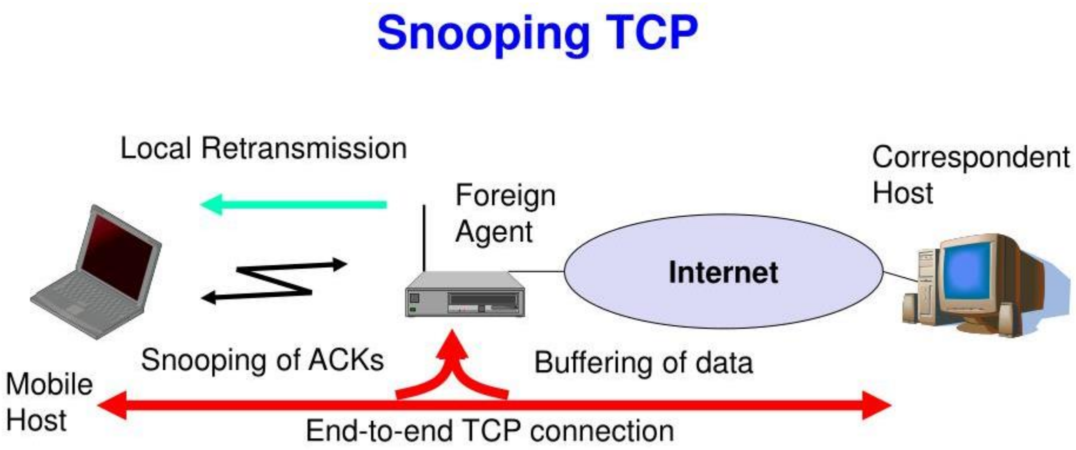
- Indirect TCP segments a TCP connection into a fixed part and a wireless part
- Standard TCP is used between the fixed computer and the access point
- No computer in the internet recognizes any changes to TCP.
- Instead of the mobile host, the access point now terminates the standard TCP connection, acting as a proxy.
- access point is now seen as the mobile host for the fixed host and as the fixed host for the mobile host
- Between the access point and the mobile host, a special TCP, adapted to wireless links, is used
- changing TCP for the wireless link is not a requirement
- suitable place for segmenting the connection is at the foreign agent
- it not only controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on.

- it not only controls the mobility of the mobile host anyway and can also hand over the connection to the next foreign agent when the mobile host moves on.

- If CH (correspondent host) sends a packet to the MH, the FA acknowledges it and forwards it to the MH
- MH acknowledges on successful reception, but this is only used by the FA
- packet is lost on the wireless link, CH doesn’t observe it and FA tries to retransmit it locally to maintain reliable data transport
- MH sends a packet, the FA acknowledges it and forwards it to CH
- packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet
- packet lost in the wired network is now handled by the foreign agent
- The middlebox performs a number of functions, including packet buffering, error correction, and retransmission.

- The mobile device communicates with the middlebox using a modified TCP protocol, known as iTCP

Snooping TCP



- One of the drawbacks of I-TCP is the segmentation of the single TCP connection into two TCP connections. This loses the original end-to-end TCP semantic
- Main function of the enhancement is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss
- good place for the enhancement of TCP could be the foreign agent in the Mobile IP context
- foreign agent buffers all packets with destination mobile host and additionally 'snoops' the packet flow in both directions to recognize acknowledgements
- reason for buffering packets toward the mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link
- foreign agent buffers every packet until it receives an acknowledgement from the mobile host
- foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost
- foreign agent could receive a duplicate ACK which also shows the loss of a packet
- foreign agent retransmits the packet directly from the buffer, performing a much faster retransmission compared to the correspondent host.
- time out for acknowledgements can be much shorter, because it reflects only the delay of one hop plus processing time.
- **Advantage**
  - ➢ end-to-end TCP semantic is preserved : packet is not acknowledged by the FA. foreign agent (FA) or base station (BS) fails, the solution reverts to standard TCP
  - ➢ No Modifications at Fixed Host : fixed computer TCP does not need any changes. The majority of the changes are made at the foreign agent (FA)

    - No packet loss during handovers : data is not passed to the new foreign agent, there will be a time-out at the fixed host and activating retransmission of the packet, via mobile IP, to a new COA
- **Disadvantage**
    - behavior of the wireless link : Snooping TCP does not isolate the behavior of the wireless link or I-TCP. Transmission errors can spread to the correspondent nodes (CH)
    - mobile node needs additional mechanisms – The use of NACK between the foreign agent and the mobile node requires the mobile node to have additional mechanisms
    - Snooping TCP may be used if encryption is used above the transport layer

Mobile TCP

- M-TCP (mobile TCP)1 approach has the same goals as I-TCP and snooping TCP
- prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems
- M-TCP wants to improve lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover
- M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections
- M-TCP splits the TCP connection into two parts as I-TCP does
- unmodified TCP is used on the standard host-supervisory host (SH) connection, while an optimized TCP is used on the SH-MH connection
- supervisory host is responsible for exchanging data between both parts similar to the proxy in I-TCP
- packet is lost on the wireless link retransmitted by the original sender retransmitted by the original sender
- SH monitors all packets sent to the MH and ACKs returned from the MH
- If the SH does not receive an ACK for some time, it assumes that the MH is disconnected
- chokes the sender by setting the sender’s window size to 0.
- Setting the window size to 0 forces the sender to go into persistent mode, i.e., the state of the sender will not change no matter how long the receiver is disconnected
- sender will not try to retransmit data SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value.
- sender can continue sending at full speed
- This mechanism does not require changes to the sender’s TCP. The wireless side uses an adapted TCP that can recover from packet loss much faster.
- This mechanism does not require changes to the sender’s TCP. The wireless side uses an adapted TCP that can recover from packet loss much faster.
- **Advantage**

    - ➢ SH does not send any ACK itself but forwards the ACKs from the MH
    - ➢ MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender’s window to 0
    - ➢ Since it does not buffer data in the SH as I-TCP does, it is not necessary to forward buffers to a new SH.
    - ➢ Lost packets will be automatically retransmitted to the new SH
- **Disadvantage**
    - ➢ modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager

Transmission/time-out freezing

- advantage of this approach is that it offers a way to resume TCP connections even after longer interruptions of the connection
- independent of any other TCP mechanism, such as acknowledgements or sequence numbers, so it can be used together with encrypted data

Selective retransmission

- useful extension of TCP is the use of selective retransmission.
- TCP acknowledgements are cumulative, i.e., they acknowledge in-order receipt of packets up to a certain packet
- single packet is lost, the sender has to retransmit everything starting from the lost packet
- obviously wastes bandwidth
- TCP can indirectly request a selective retransmission of packets.
- The receiver can acknowledge single packets, not only trains of in-sequence packets.
- The sender can now determine precisely which packet is needed and can retransmit it.
- advantage of this approach sender retransmits only the lost packets
- lowers bandwidth requirements and is extremely helpful in slow wireless links
- improve the performance of data transmission over unreliable wireless links
- only the lost or corrupted packets are retransmitted, rather than retransmitting the entire data stream
- help to reduce the delay and improve the throughput of data transmission, especially over networks with high packet loss rates or limited bandwidth

TCP over 2.5/3G wireless networks

- Large windows : support large enough window sizes based on the bandwidth delay product experienced in wireless systems
- larger initial window of 2 to 4 segments may increase performance particularly for short transmissions
- Limited transmit: extension of Fast Retransmission/Fast Recovery and is particularly useful when small amounts of data are to be transmitted
- Large MTU: The larger the MTU (Maximum Transfer Unit) the faster TCP increases the congestion window
- Selective Acknowledgement (SACK): SACK allows the selective retransmission of packets and is almost always beneficial compared to the standard cumulative scheme
- used protocol in computer networking to establish a reliable communication channel between two hosts.
- In the case of wireless networks, such as 2.5G and 3G, the performance of TCP can be affected due to the specific characteristics of these networks
- One of the main challenges for TCP over wireless networks is the high packet loss rate. To overcome these challenges, several techniques have been proposed for TCP optimization over wireless networks.
- Explicit Congestion Notification (ECN) : used to prevent network congestion and improve network performance. ECN can be used to provide early notification of congestion in the network, allowing TCP to react more quickly and avoid congestion. When a network becomes congested, packets may be delayed or lost, leading to decreased performance and lower throughput. ECN allows network devices to signal congestion to the endpoints by setting a flag in the IP header of packets that indicates congestion. This allows the endpoints to adjust their transmission rates and avoid further congestion
- Timestamp: connections with large windows may benefit from more frequent RTT samples provided with timestamps by adapting quicker to changing network conditions. With the help of timestamps higher delay spikes can be tolerated by TCP without experiencing a spurious timeout
- No header compression: header compression mechanism does not perform well in the presence of packet losses this mechanism should not be used. Header compression is not compatible with TCP options such as SACK or timestamps