MOBILE TCP

Dr. A. Beulah

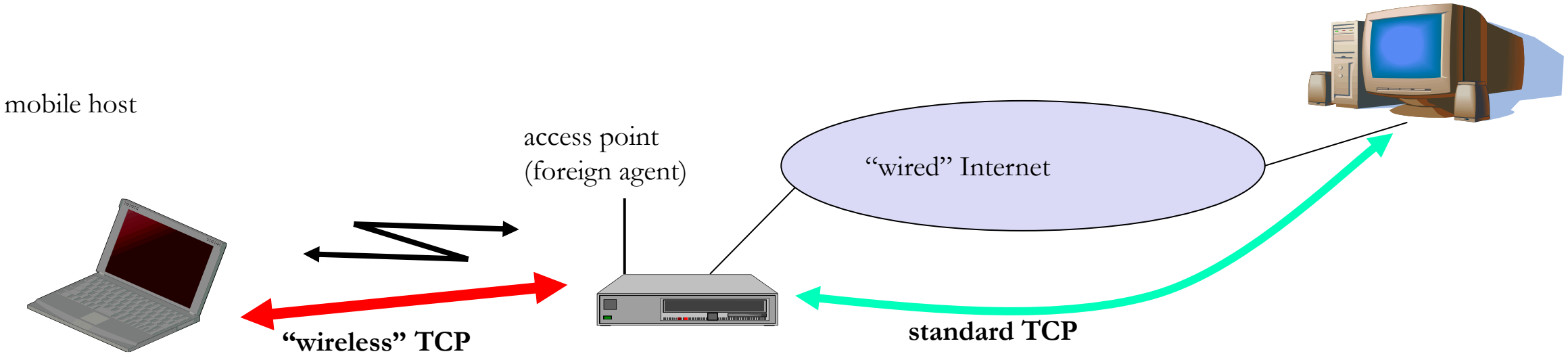
AP/CSE

TCP in Mobile Networks

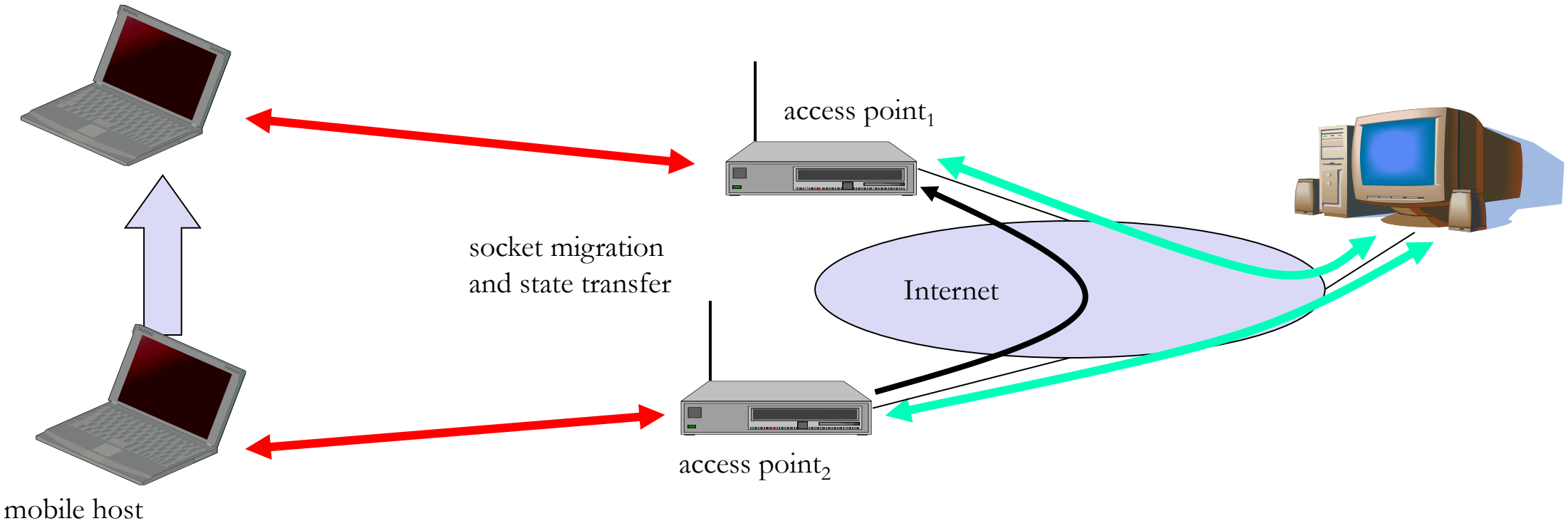
- TCP in Single-Hop Wireless Networks (Wireless LAN)
  - Indirect TCP (I-TCP)
  - Fast Retransmission
  - Snooping TCP (S-TCP)
- Mobile TCP - TCP for Cellular Networks
  - Freeze TCP
- TCP in Multi-Hop Wireless Networks (Ad hoc)
  - TCP Feedback (TCP-F)

Indirect TCP (I-TCP)

- Indirect TCP or I-TCP segments the connection
  - The access point is seen as the mobile host for the fixed host and as the fixed host for the mobile host.
  - Splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
  - Hosts in the fixed part of the net do not notice the characteristics of the wireless part



I- TCP Socket and State Migration



Indirect TCP (I-TCP)

- Advantages
  - No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
  - Transmission errors on the wireless link do not propagate into the fixed network
  - Simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
  - Very fast retransmission of packets is possible, the short delay on the mobile hop is known
- Disadvantages
  - Loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash
  - Higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

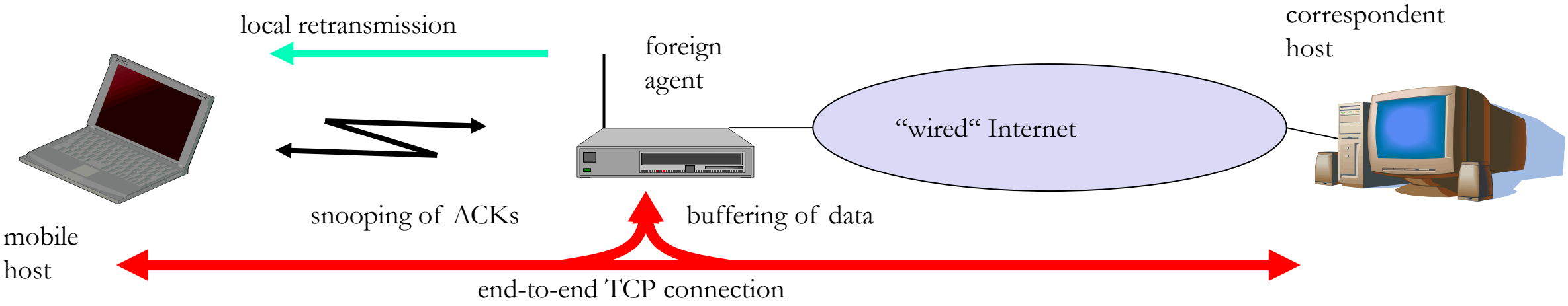
Fast Retransmit/Fast Recovery

- Change of foreign agent often results in packet loss
  - TCP reacts with slow-start although there is no congestion
- Forced Fast retransmit
  - As soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
  - This forces the fast retransmit mode at the communication partners
  - Additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration
- Advantage
  - Simple changes result in significant higher performance
- Disadvantage
  - Further mix of IP and TCP, no transparent approach

Snooping TCP(S-TCP)

- Drawback of I-TCP
  - Segmentation of a single TCP into 2 TCP connections.
- The extension done on traditional TCP is transparent
  - Buffer the packets sent to the mobile host
  - Lost packets on the wireless link will be retransmitted immediately by the mobile host or foreign agent, respectively → "Local" Retransmission
  - Foreign Agent "snoops" the packet flow and recognizes acknowledgements in both directions
  - FA filters the ACKs
  - Extension of TCP is done within the Foreign Agent

Snooping TCP(S-TCP)



Snooping TCP(S-TCP)

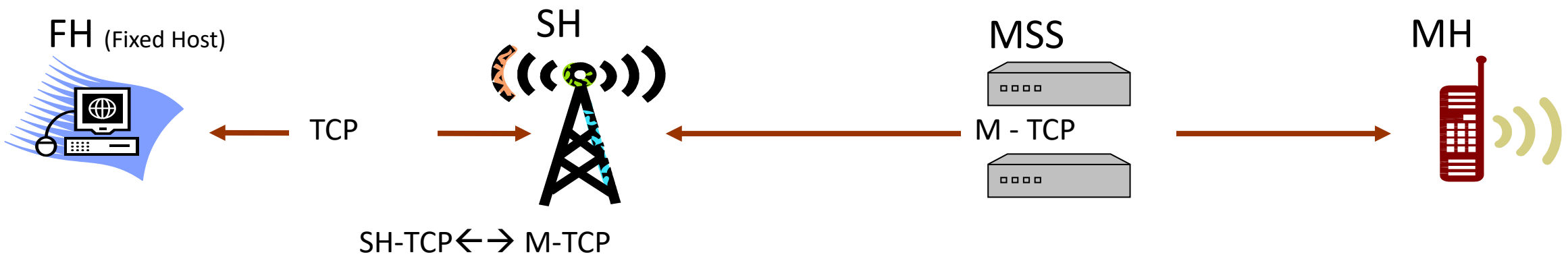
- Data transfer to the mobile host
  - FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
- Data transfer from the mobile host
  - FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
  - MH can now retransmit data with only a very short delay
- Integration of the MAC layer
  - MAC layer often has similar mechanisms to those of TCP
  - thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them

Snooping TCP(S-TCP)

- Advantages
  - End to end TCP semantic is preserved
  - No change in CN. Changes are done only in FA.
- Disadvantages
  - Snooping TCP does not isolate the wireless link as good as I-TCP
  - Snooping might be useless depending on encryption schemes

Mobile TCP

- Major thing to consider → Handling of lengthy and/or frequent disconnections
- Traditional TCP (Disconnections)
  - The sender tries to retransmit an unacknowledged packet every minute and gives up after 12 retransmission.
- I-TCP (Disconnections)
  - The FA / Proxy has to buffer more and more data.
  - Long disconnection period requires lengthy buffer to store more data.



Mobile TCP

- M-TCP splits as I-TCP does (ie. 2 segmentation connection)
  - Unmodified TCP fixed network to Supervisory Host (SH)
  - Optimized TCP between SH and MH
- Supervisory Host
  - No caching, No retransmission
  - Packet loss → Retransmission done by original sender and not by SH. (End to end Semantics)
  - Monitors all packets and acknowledges it.
  - If disconnection detected
    - Set sender window size to 0
    - Sender automatically goes into persistent mode
  - Old or new SH reopen the window

Mobile TCP

- Advantages
  - Maintains End to end semantics
  - SH does not send ACK itself, but forwards ACK from MH
  - Supports disconnection and no buffer forwarding
- Disadvantages
  - Loss on wireless link propagated into fixed network
  - adapted TCP on wireless link

Freeze TCP

- Mobile hosts can be disconnected for a longer time
  - No packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux. with higher priority traffic
  - TCP disconnects after time-out completely
- TCP freezing
  - MAC layer is often able to detect interruption in advance
  - MAC can inform TCP layer of upcoming loss of connection
  - TCP stops sending, but does now not assume a congested link
  - MAC layer signals again if reconnected
- Advantage
  - Scheme is independent of data
- Disadvantage
  - TCP on mobile host has to be changed, mechanism depends on MAC layer

TCP Feedback (TCP-F)

- TCP-F allows the sender to be informed about a route disconnection.
- When a link in a route is broken, the upstream node that detects the disconnection will send a Route Failure Notification (RFN) message back to the sender.
- Upon receiving this message, the source enters SNOOZE state.

TCP Feedback (TCP-F)

- In SNOOZE state:
  - The sender stops transmitting all data packets(new or retransmitted)
  - The sender freezes all its timers, cwnd size, retransmission timer etc.
- When the route repair complete message is received, data transmission will be resumed and all timers and state variables will be restored.

Summary

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Freeze TCP	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant

Test your understanding

- How are handoffs handled in snooping TCP??

- Is the following statement true or false?

  The multicast group membership of a packet is defined by the source IP address.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.