Indirect TCP

- The simplest modification to TCP for wireless links
- The access point (AP) (e.g., foreign agent, base station), which is connected to the wired network, acts as the end point for the TCP connection

(Fig. 1)

- Packets that arrive at the AP are immediately acknowledged (TCP ACK) and are relayed to the mobile node
- Across the wireless link, the mobile node acknowledges packets as they arrive – these ACKs are only used by the AP
- The AP can quickly tell when packets are lost to noise – in this case the AP quickly retransmits without affecting the TCP connection (because all such packets have been acknowledged already by the AP)
- Whenever a packet is lost to congestion, the AP does not return ACK – this is how TCP is expected to work
- Thus, noise on the wireless link is completely isolated from TCP on the wired link
- Handover presents a big problem:
    - The AP holds several packets in its buffer at any given time
    - Say the mobile node switches to a new AP (e.g., new foreign network or foreign agent). The "state" of the old AP (buffered packets, sequence numbers, ports, etc.) must be forwarded to the new AP, since the buffered packets have already been acknowledged.

(Fig. 2)

- Disadvantages of indirect TCP:
    - AP crash is catastrophic: since packets in the AP's buffer have already been acknowledged, they will never be retransmitted – connection is effectively broken
    - Handover latency is a problem – all the buffered packets must be forwarded to the new AP before the TCP connection can resume.

Snooping TCP

- As we saw, segmentation causes disadvantages in indirect TCP – is it possible to maintain end-to-end TCP connection?
- Snooping TCP:
    - The AP/FA is on the path from source to mobile node, but does not segment the link into two; the mobile node is the endpoint of the TCP connection
    - The AP buffers packets as it forwards them, and watches (i.e. "snoops" the connection) for ACKs as the mobile node transmits them
    - If a packet is lost to noise, the AP does not see the ACK, and retransmits the packet from its buffer
    - if this happens fast enough, the mobile gets the packet and sends an ACK before the TCP link times out
    - The AP never acknowledges packets on its own! Thus, complicated handoffs are not needed, and AP crash is not catastrophic

(Fig. 3)

- Disadvantages of snooping TCP:
  - Isolation of wireless link is less effective
  - AP timeout must be much smaller than TCP timeout in order for this method to work properly

- A different problem: what about short disconnections (e.g., a dead zone between APs). This would lead to a lost connection or large buffers in the other two methods.

(Fig. 4)

Mobile TCP (note: not an official standard like Mobile IP)

- Mobile TCP keeps TCP connections alive during short disconnections
- Wireless signal strength is assumed to be good – any dropped packet (via noise or congestion) is forwarded directly from the source. (End-to-end connection is maintained, like in snooping TCP).
- AP monitors the TCP connection, like in snooping TCP – if several ACKs are missed, the AP assumes that the link is disconnected
- Once this happens, AP sends a control message setting source's window size to zero – TCP connection enters "persistent mode", keeping TCP connection alive but preventing source from sending packets
- Once AP sees ACKs again (either the old AP or a new one), TCP window size is reset to its previous value (control message)