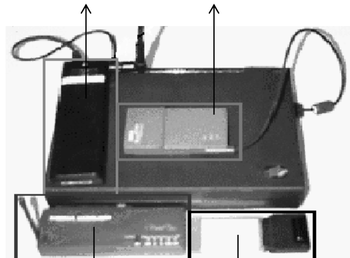
EEC173B/ECS152C, Winter 2006

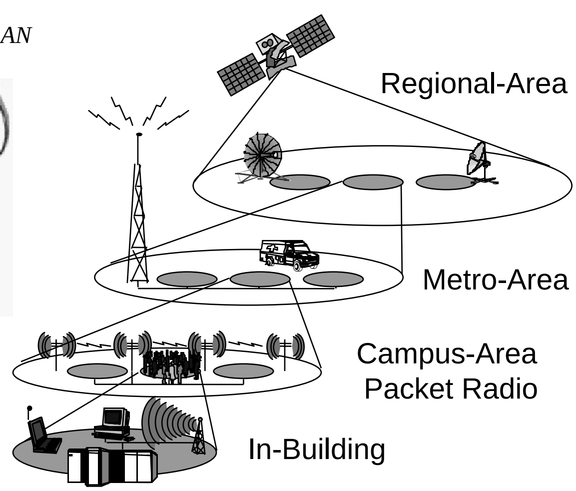
Reliable Data Transport over Wireless Networks

- Problems with TCP
- Snoop Protocol

* Acknowledgment: Slides from Prof. Hari Balakrishnan & Prof. Badri Nath

Wireless Heterogeneity





Wireless Performance

Technology	Rated Bandwidth	Typical TCP Throughput
IBM Infrared	1 Mbps	100-800 Kbps
Lucent WaveLAN	2 Mbps	50 Kbps-1.5 Mbps
Metricom Ricochet	100 Kbps	10-35 Kbps
Hybrid wireless cable	10 Mbps	0.5-3.0 Mbps

Goal: To bridge the gap between perceived and rated performance

Data Transport Over Wireless

- Packet loss in wireless networks may be due to
  - Bit errors
  - Handoffs
  - Congestion (rarely)
  - Reordering (rarely, except in mobile ad hoc networks)

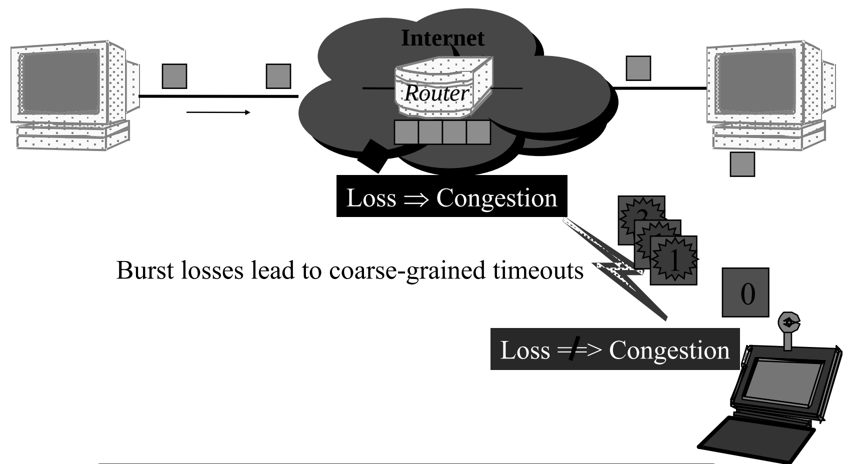
Poor Interaction with TCP

- TCP assumes loss is due to congestion or reordering
- Wireless loss is not due to congestion
  - TCP cannot distinguish between link loss and congestion loss => result in lower throughput
- Cumulative ACK not good with bursty losses
  - Missing data detected one segment at a time
  - Duplicate ACKs take a while to cause retransmission
  - TCP Reno may suffer coarse time-out -> slow start!
  - TCP New Reno still only retransmit one packet per RTT
- Non-congestion loss indicated by DUP ACKs
  - Fast retransmit & recovery (congestion window is halved)
- Non-congestion loss indicated by timeout
  - Enter slow start (Start from CongWin = 1)

Other Problems in Wireless Networks

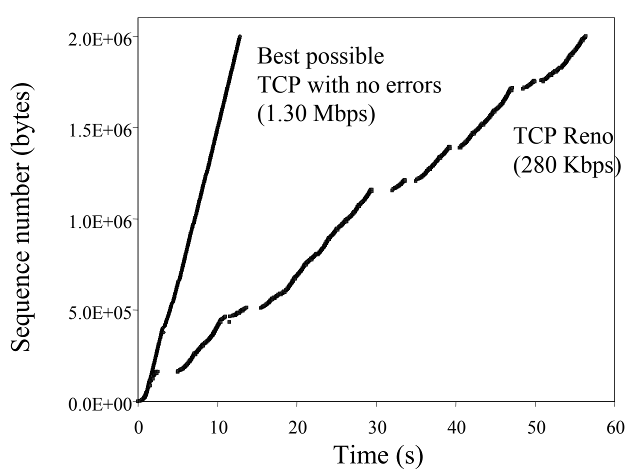
- Burst errors due to poor signal strength or mobility (handoff)
  - More than one packet lost in TCP window
- Delay is often very high
  - RTT quite long (tunneling, satellite)
  - True in telephone networks providing data services that deploy fixed gateways (non-optimal routes)
- Asymmetric effects
  - Bandwidth asymmetry & latency variability
- Low channel bandwidth

Challenge #1: Wireless Bit-Errors



Result: Low throughput

Performance Degradation



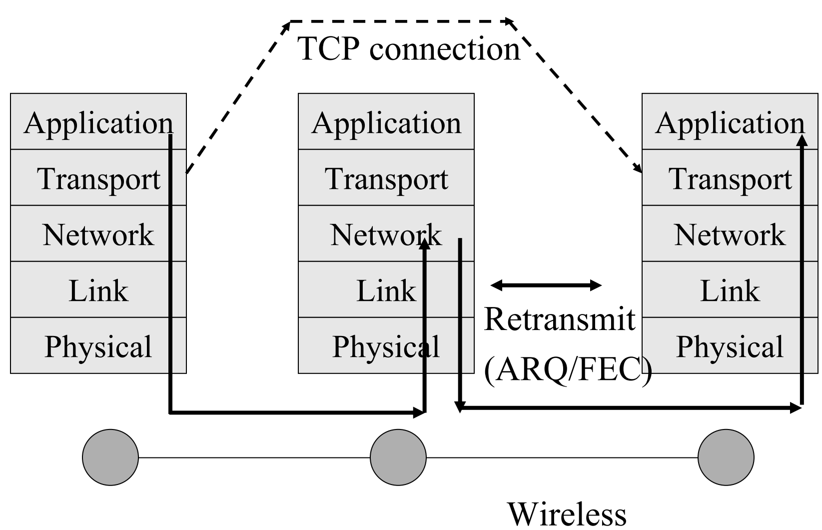
2 MB wide-area TCP transfer over 2 Mbps Lucent WaveLAN

Approaches

Question: how to reconcile between the two in an end-to-end transport mechanism?

- Link layer enhancement (FEC, retransmission)
  - **[LR99]** R. Ludwig and B. Rathony, "Link Layer Enhancements for TCP/IP over GSM," *IEEE Proc. Infocom*, pp. 415-422, 1999.
- Transport Layer
  - **[BB95]** A. Bakre and B. R. Badrinath, “I-TCP: Indirect TCP for mobile hosts,” *Proc. 15th International Conference on Distributed Computing Systems*, Vancouver, Canada, June 1995, pp. 136-143.
- TCP-aware Link-layer aware
  - **[BSK95]** Snoop protocol
- Explicit Loss Notification Schemes

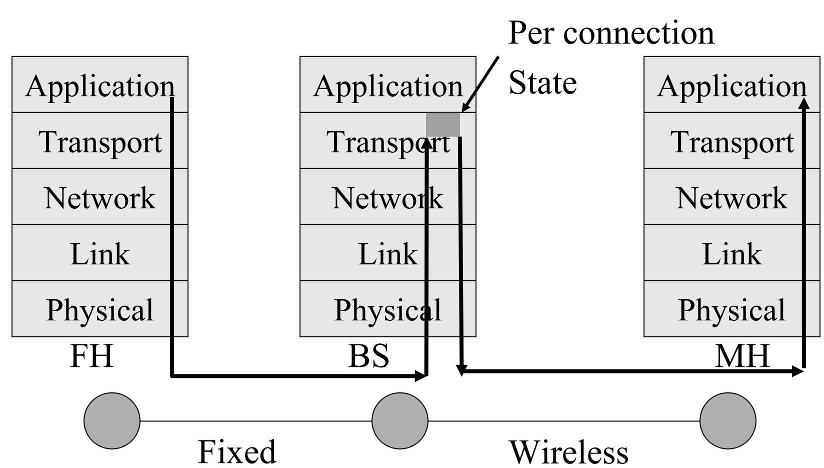
Link Level Retransmission



Link Level Retransmission: Issues

- How many times to retransmit at the link layer before giving up?
- How much time is required for a link layer retransmission?
  - Only beneficial if TCP timeout large enough to tolerate additional delays due to link level retransmission
- What triggers link level retransmission?
- Adverse interaction with transport layer
  - Timer interaction
  - Interaction with fast retransmit
  - Large variation in RTT

Transport-level Solution



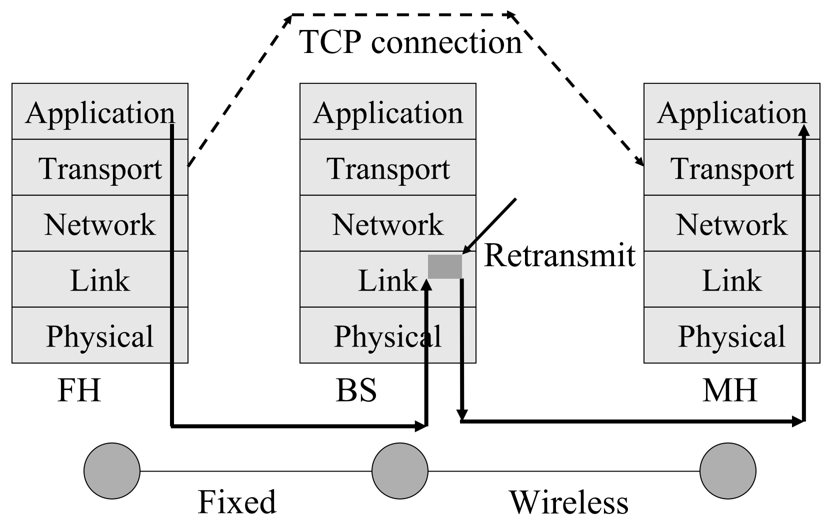
I-TCP

- Split end-to-end connection into two independent flows
  - One connection for the wired part, and another for the wireless part
  - Wireless part of the TCP can be optimized for wireless
    - Different flow/error control
    - Local recovery of errors: faster recovery due to shorter RTT on wireless link
  - On wireless, loss -> try harder
  - On fixed, loss -> backoff

I-TCP Disadvantages

- End-to-end semantics violated
  - ACK may be delivered to sender before data delivered to receiver
- Base station (BS) retains hard state; its failure can result in loss of data (unreliability)
- BS retains per-connection state -> not scalable
  - Buffered packets at BS must be transferred to new BS
  - Buffer space needed
- Hand-off latency increases due to state transfer
  - Extra copying of data at BS

Snoop [BSK95]: TCP-aware, Link-aware



Snoop Protocol

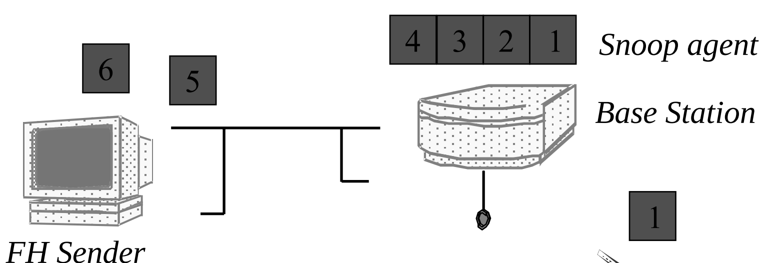
- Uses the same idea of local recovery as I-TCP
- Shield TCP sender from wireless vagaries
  - Eliminate adverse interactions between protocol layers
  - Congestion control only when congestion occurs
- Preserve current TCP/IP service model
  - Maintain end-to-end semantics

Fixed to mobile: transport-aware link protocol
Mobile to fixed: link-aware transport protocol

Snoop Features

- Snoop monitors every packet that passes through
  - Buffers packets from FH to MH as yet unacknowledged
  - Packets flushed when an ACK is received
  - When DUP ACK is received, retransmit from buffer
- Hide wireless loss from sender
  - Suppress DUP ACKs => prevent fast retransmit
  - Sender can still timeout
- Snoop state is soft state at base station, instead of hard state
  - Handoff -> new snoop state is built at new BS
  - Loss of soft state affects performance, but not correctness

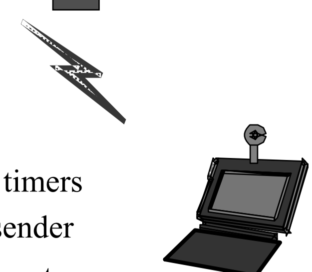
Snoop Protocol: FH to MH



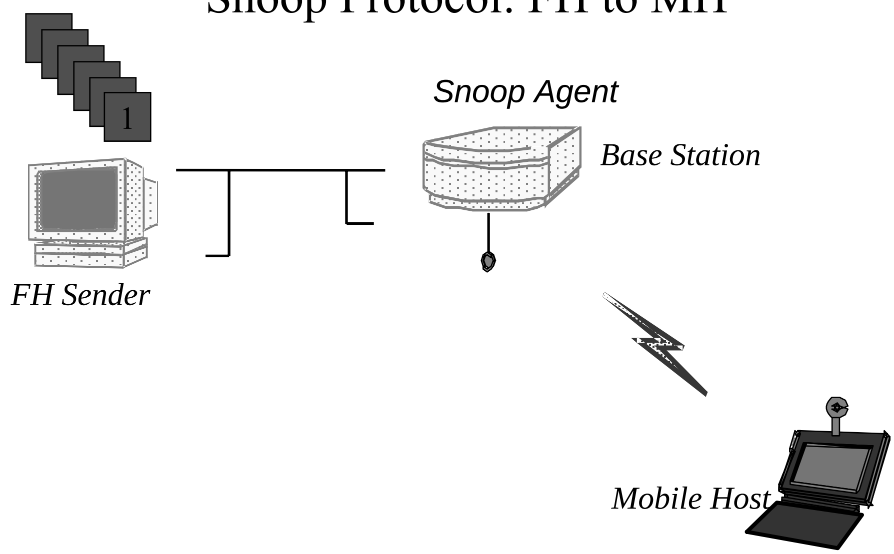
Snoop agent:

- Snoops on TCP segments and ACKs
- Detects losses by duplicate ACKs and timers
- Suppresses duplicate ACKs from FH sender

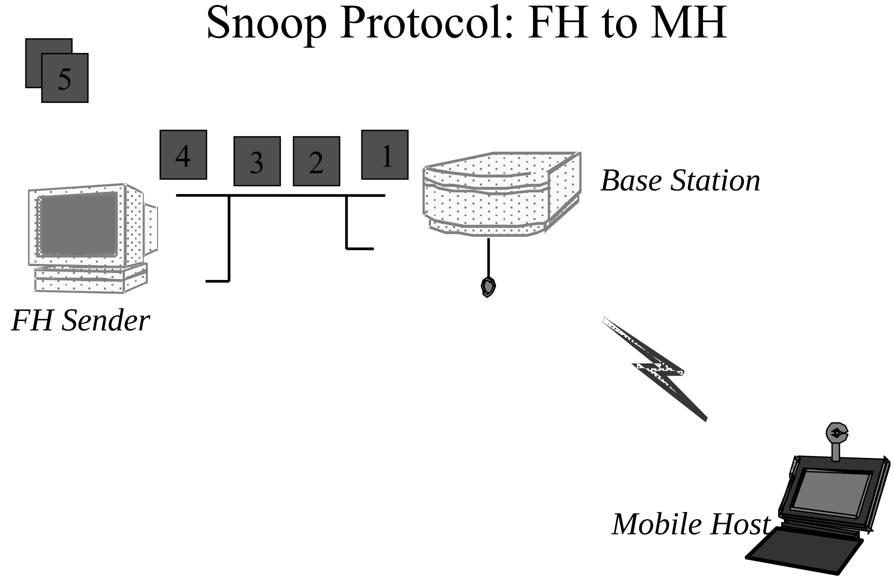
Cross-layer protocol design: Snoop agent state is *soft*



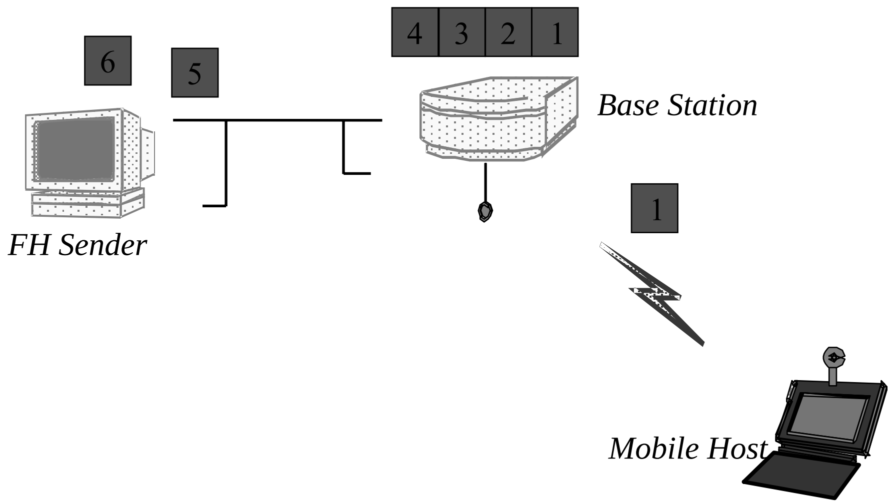
Snoop Protocol: FH to MH



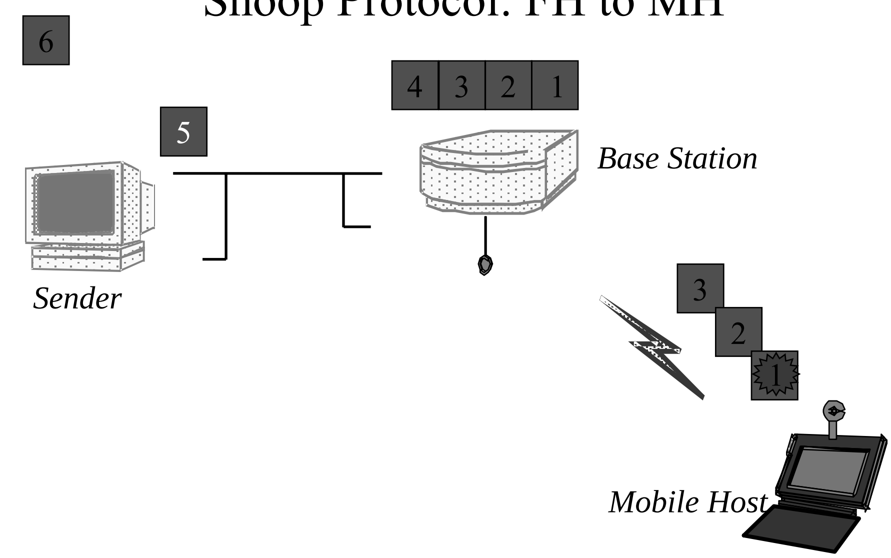
Snoop Protocol: FH to MH



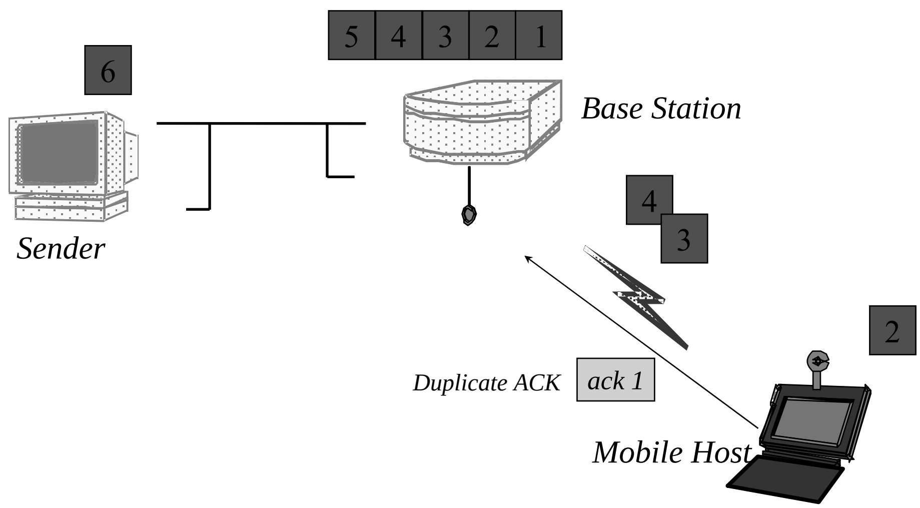
Snoop Protocol: FH to MH



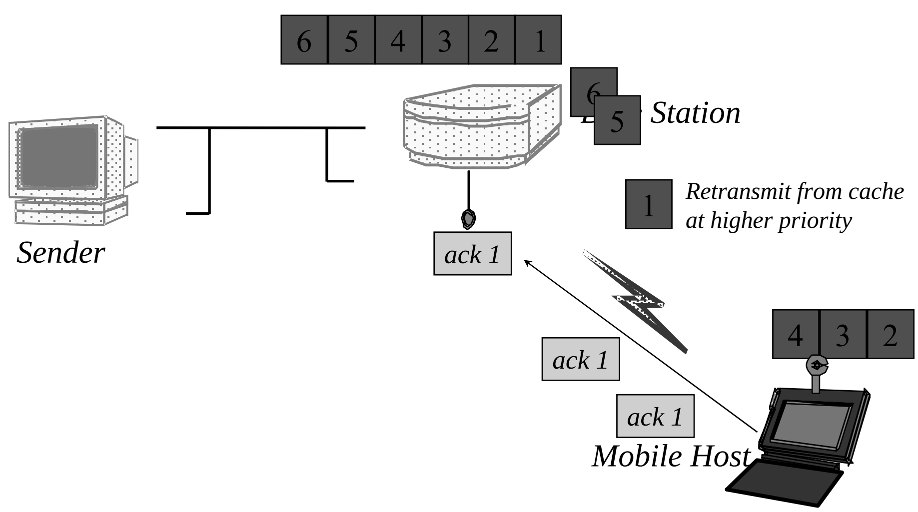
Snoop Protocol: FH to MH



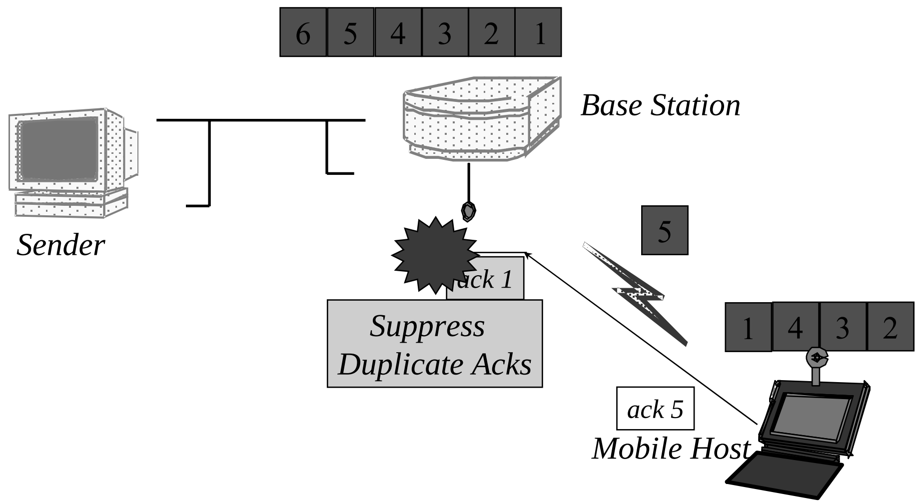
Snoop Protocol: FH to MH



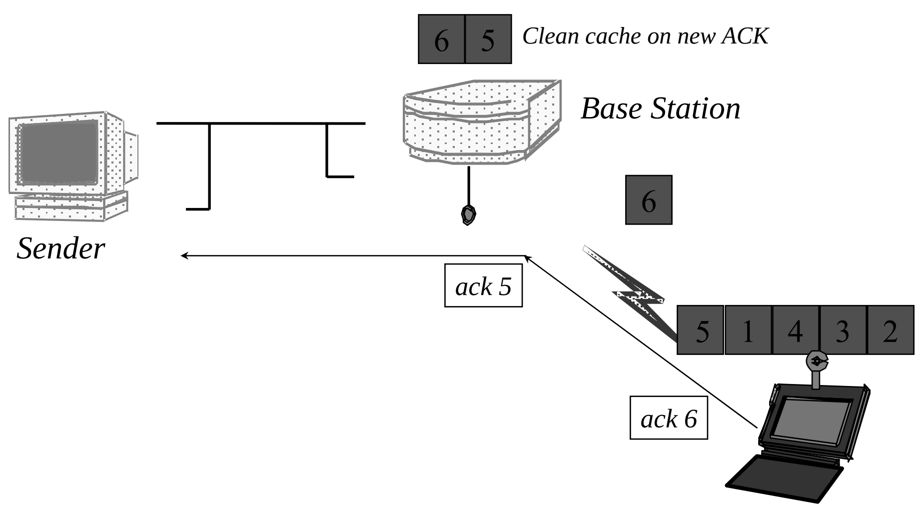
Snoop Protocol: FH to MH



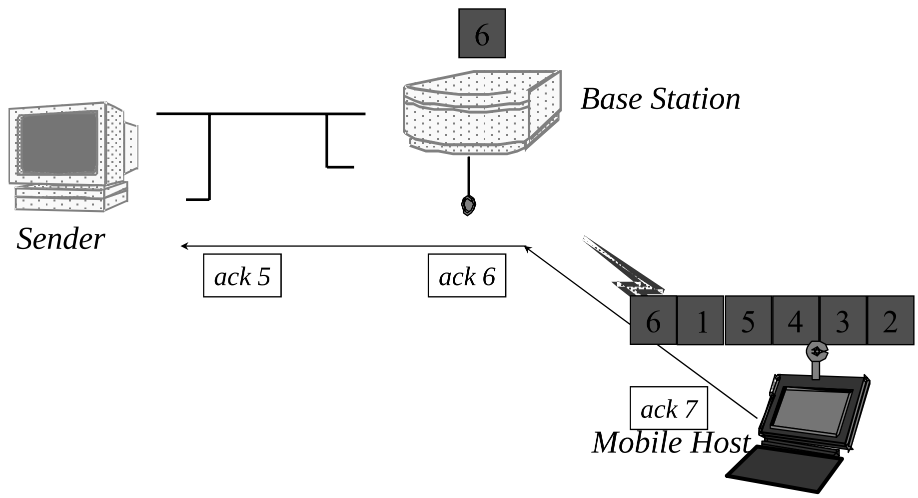
Snoop Protocol: FH to MH



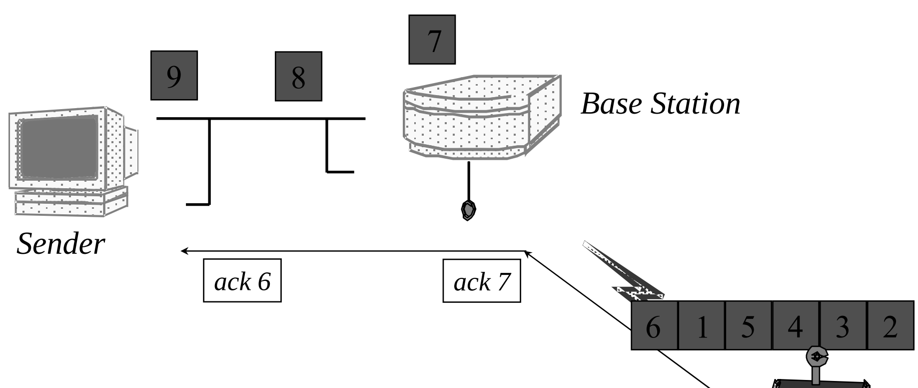
Snoop Protocol: FH to MH



Snoop Protocol: FH to MH

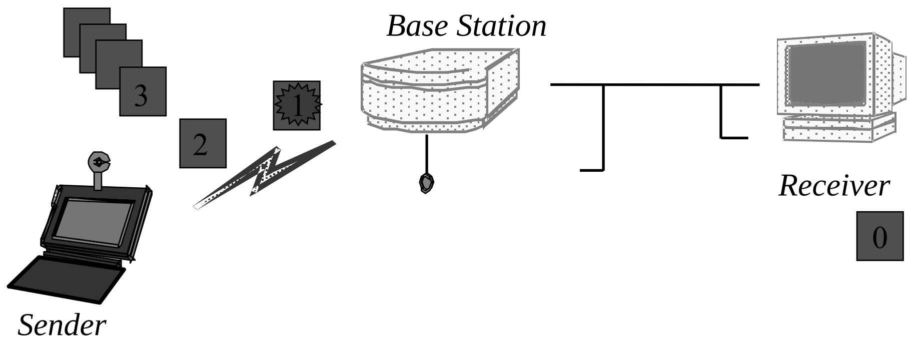


Snoop Protocol: FH to MH



Active soft state agent at base station
Transport-aware reliable link protocol
Preserves end-to-end semantics

Snoop Protocol: MH to FH



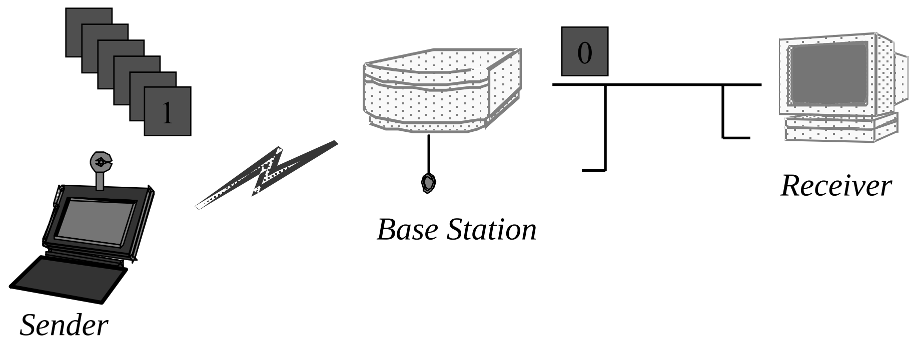
Caching and retransmission will not work

- Losses occur before packet reaches BS
- Losses should not be hidden

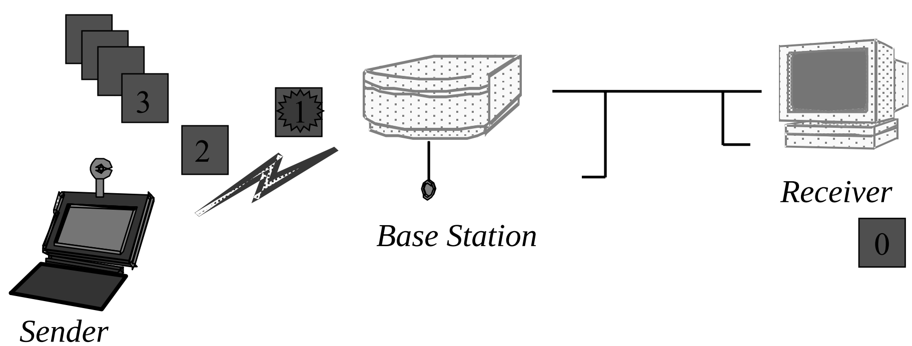
Snoop Protocol: MH to FH

- Solution #1: Negative ACKs (NACKs)
  - NACK from BS to MH on wireless loss
- Solution #2: *Explicit Loss Notifications (ELN)*
  - In-band message to TCP sender
  - General solution framework

Snoop Protocol: MH to FH

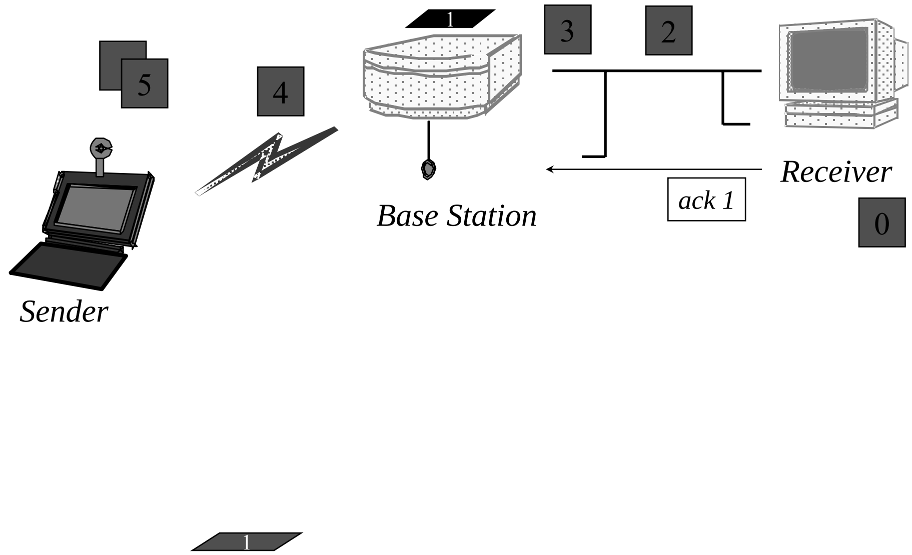


Snoop Protocol: MH to FH

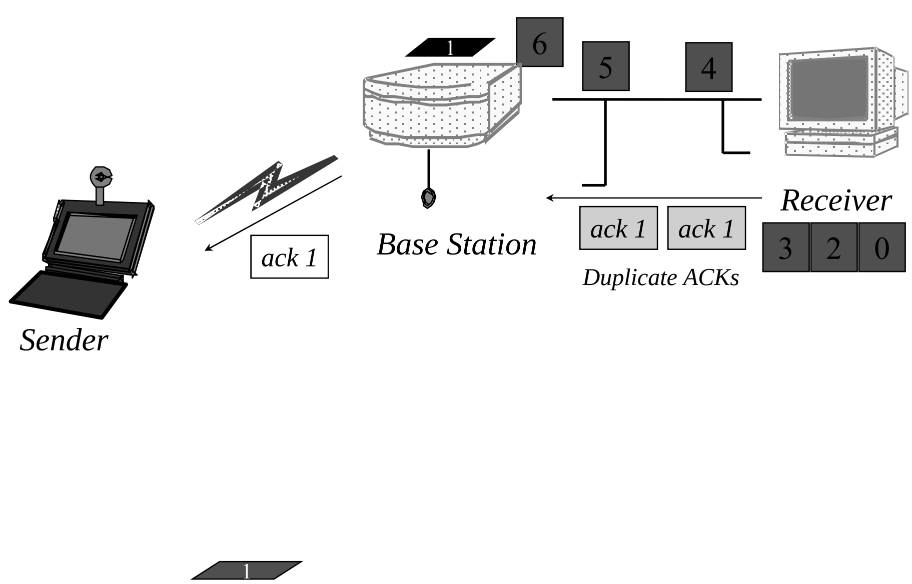


Snoop Protocol: MH to FH

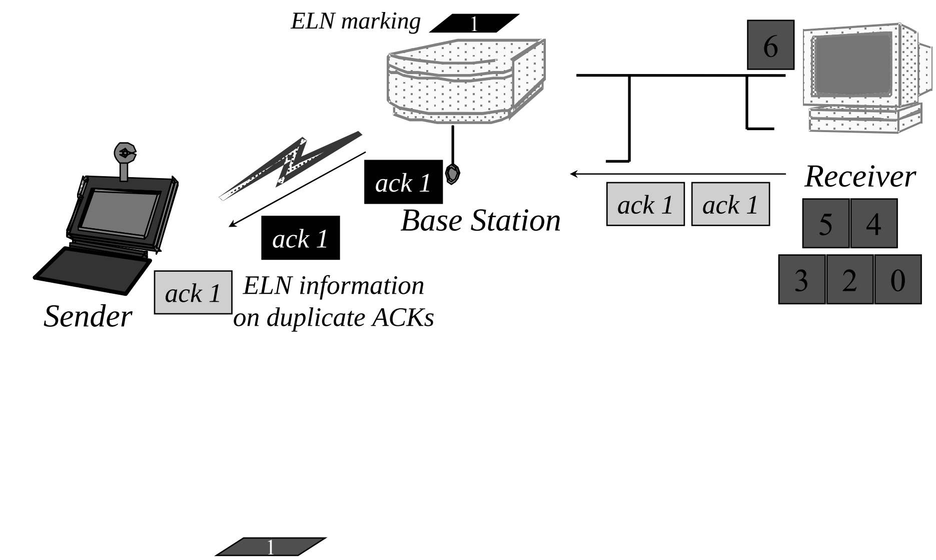
Add 1 to list of holes after checking for congestion



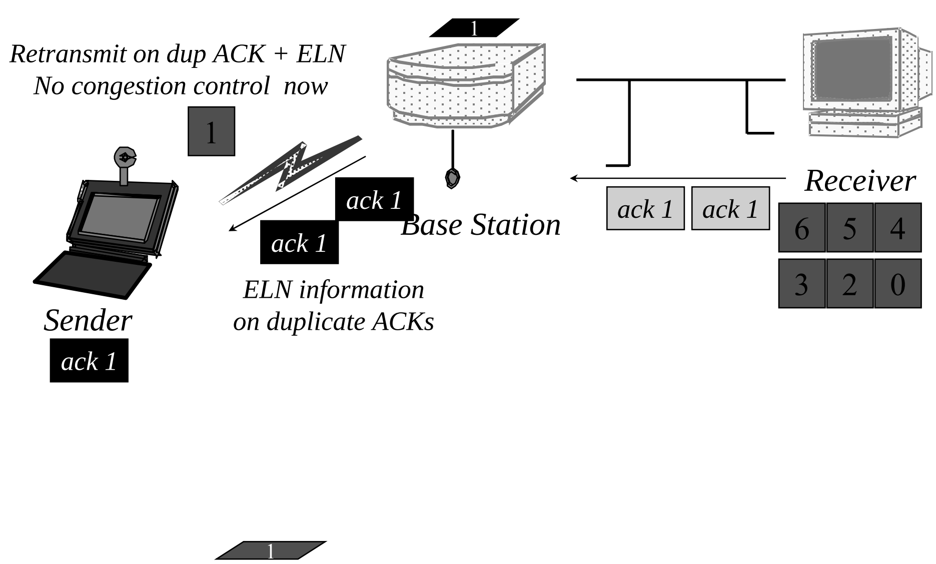
Snoop Protocol: MH to FH



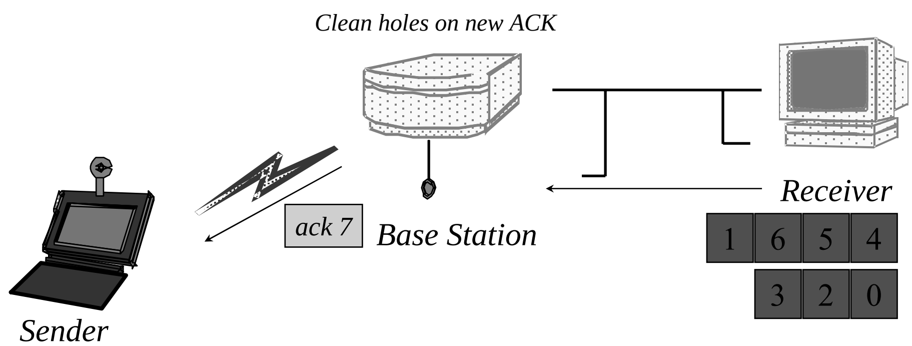
Snoop Protocol: MH to FH



Snoop Protocol: MH to FH

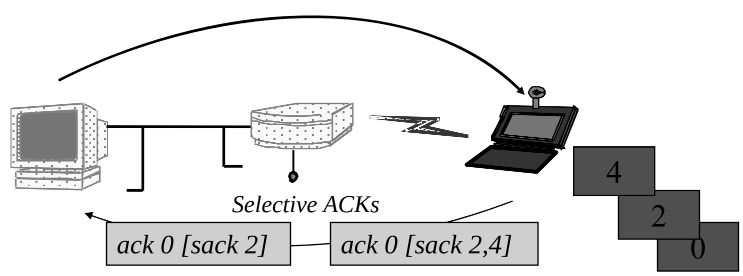


Snoop Protocol: MH to FH



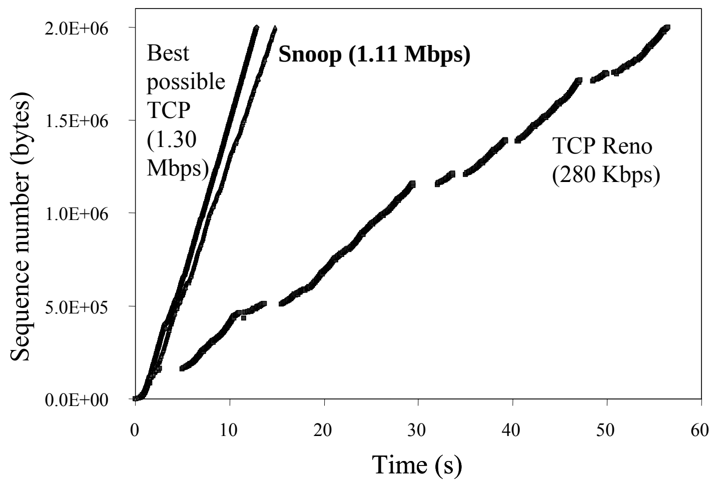
Link-aware transport decouples congestion control from loss recovery. Technique generalizes nicely to wireless transit links

End-to-End Enhancements



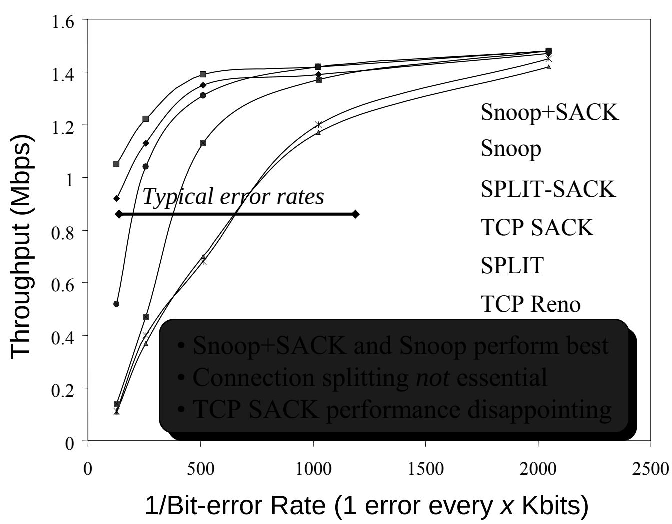
- Decouple congestion control from loss recovery
  - *Explicit Loss Notification (ELN)*
- Burst losses
  - *Selective ACKs (SACKs) [FF96,KM96,MMFR96,B96]*
- Snoop protocol: no changes to fixed hosts on the Internet

Snoop Performance Improvement



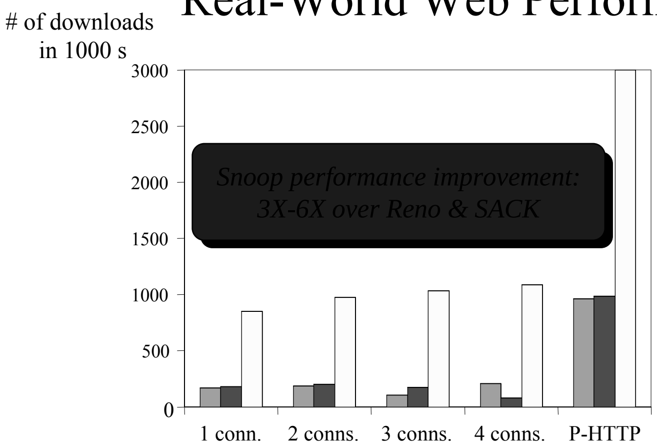
2 MB wide-area TCP transfer over 2 Mbps Lucent WaveLAN

Performance: FH to MH



2 MB local-area TCP transfer over 2 Mbps Lucent WaveLAN

Real-World Web Performance



	1 conn.	2 conns.	3 conns.	4 conns.	P-HTTP
Reno	170	186	102	206	966
SACK	179	203	177	76	985
Snoop	849	975	1033	1085	3000

Reno SACK Snoop

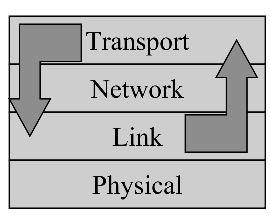
Empirical wireless error model from real traces of Reinas wireless network, UC Santa Cruz

Empirical Web workload model from real traces

Summary: Wireless Bit-Errors

- Problem: Wireless corruption mistaken for congestion
- Solution: Snoop Protocol
- General lessons
  - *Lightweight soft-state agent in network infrastructure*
    - Fully conforms to the IP service model
    - Automatic instantiation and cleanup
  - *Cross-layer protocol design & optimizations*

Transport-aware link (Snoop agent at BS)



Link-aware transport (ELN)

Snoop Protocol: Disadvantages

- Link layer at base station needs to be TCP-aware
- Not useful if TCP headers are encrypted (IPsec)
- Cannot be used if TCP data and TCP ACKs traverse different paths
  - Both do not go through the same base station, e.g., satellite links