Extending Snoop to Handle IPSec Packets

Yan Yu
AT&T Research / USC, UCLA

Joint work with
S. Bellovin, R. Caceres, K. Fisher, A. Rogers

The problem of using TCP in wireless networks

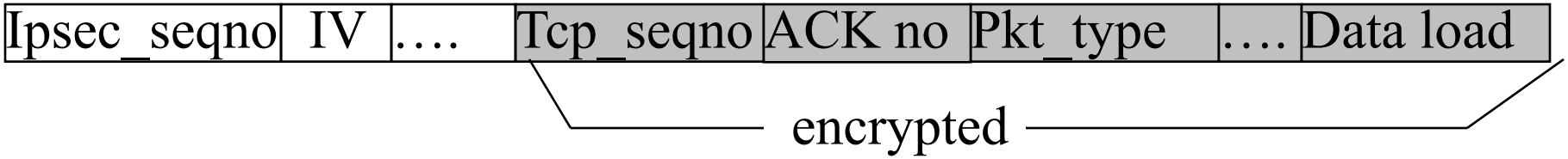
- Major causes for losses in wireless networks
  - lossy wireless links or hand-offs
- TCP can not distinguish between:
  - Congestion loss
  - Error loss
- When misunderstanding error loss as congestion loss, TCP sender back off => performance degradation.

Snoop

- A link layer protocol that snoops into the TCP header.
- Cache the TCP data packets that being sent across the wireless link
- Error detection
  - local timeout
  - a small number of duplicate ACKs.

IPSec: encrypted IP packet

- IPSec packet format:



- The problem of Snoop over IPSec:
  - Snoop needs to access the higher layer (TCP) packet header
    - ACK sequence number.
    - Packet sequence number.

Snoop layer over IPsec

- Network configuration:

At the Base Station:

- **Traffic from FH → MH**:
  - Cache TCP data packets.
  - Identify congestion loss if receiving out-of-order packets

Snoop layer over Ipsec (cont.)

At the Mobile Host:

- set IV in the ACK to hash(IV).
- the IPSEC seqno is assigned a new one at TCP sink.
- when need to generate duplicate ACK (the received packet is out of order):
  - TCP: dup tcp seqno, but new uid
  - In our snoop version (for security reason):

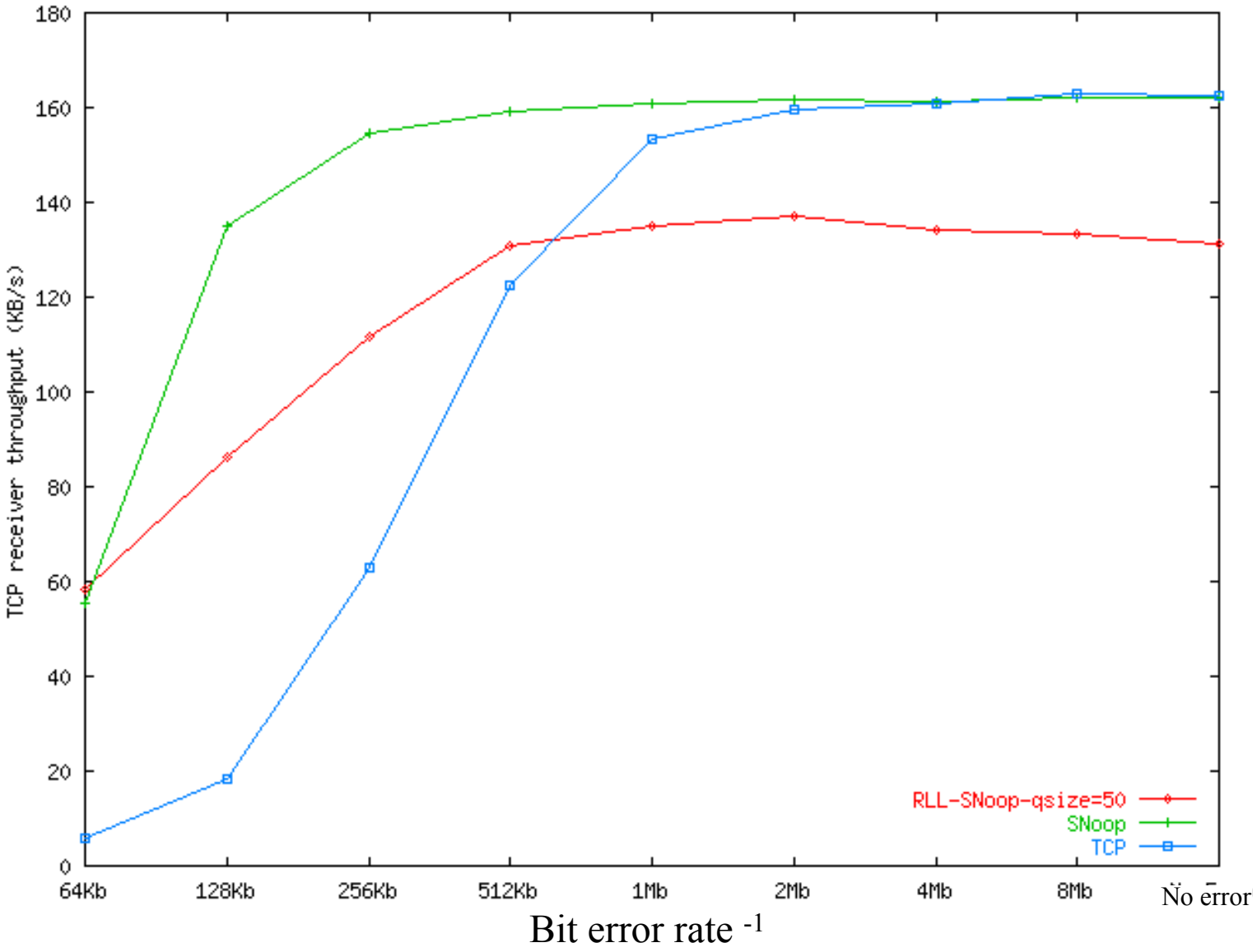
  Use the cached ACK for duplicate ACK, so exactly the same ACK as before.

Snoop layer over Ipsec (cont.)

At the Base Station:

- **Traffic from MH → FH:**
  - New ACK: propagate.
  - Dup ACK:
    - Congestion loss => propagate
    - o/w, Propagate one, then suppress the following duplicate ACKs.
  - Use IV to identify which packet is being ACKed.
  - Use IPSec sequence number to do cumulative ACK.

Simulation results:



Simulation results (cont.):