Review of TCP Congestion Control

- Connection-oriented, reliable, ordered, byte-stream protocol with explicit flow control.
- Divides data into Sender Maximum Segment Size (SMSS), and labels with sequence numbers to guarantee ordering and reliability.
- When a host receives in-sequence segment, it sends an ACK, if an out-of-sequence segment is received, it send next expected sequence numbers.
- If no ACK received within a timeout, sender transmits again.

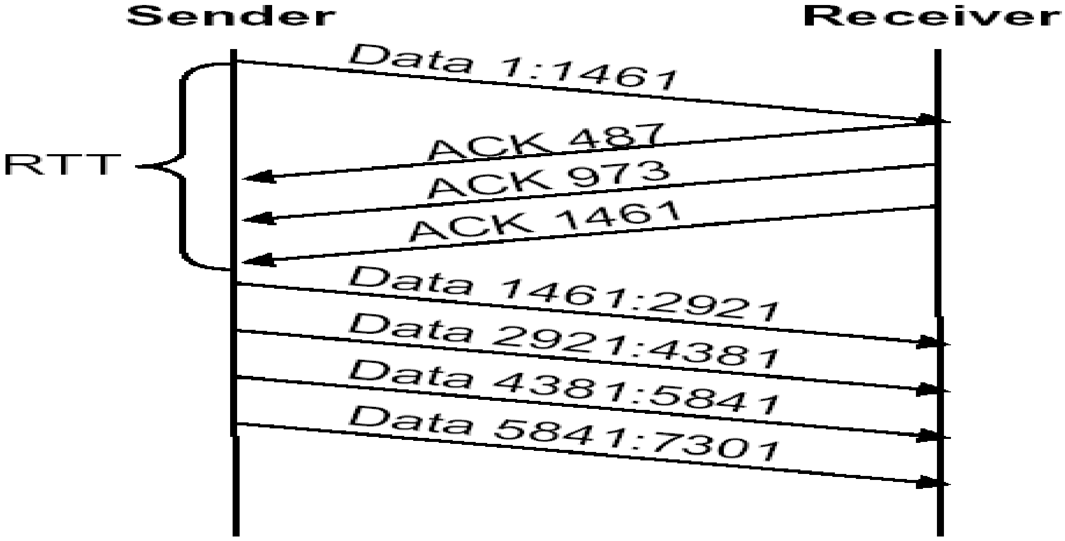
TCP Congestion Control Algorithm

- The **Slow Start and Congestion Avoidance** which is mentioned in **RFC 2581** algorithm **MUST** be used by TCP sender to control the amount of outstanding data being injected into the network.
- Transmission over network for the very first time or after repairing loss detected by the retransmission timer, TCP implements Slow Start.
- Slow Start is implemented with conjunction to Congestion Avoidance.
- During **Slow Start**, a TCP increments **congestion window** (cnwd) by at most SMSS bytes for each ACK received that cumulatively acknowledges new data.
- During **Congestion Avoidance**, cwnd is incremented by roughly 1 full-sized segment per round-trip time (RTT). Congestion avoidance continues until congestion is detected.

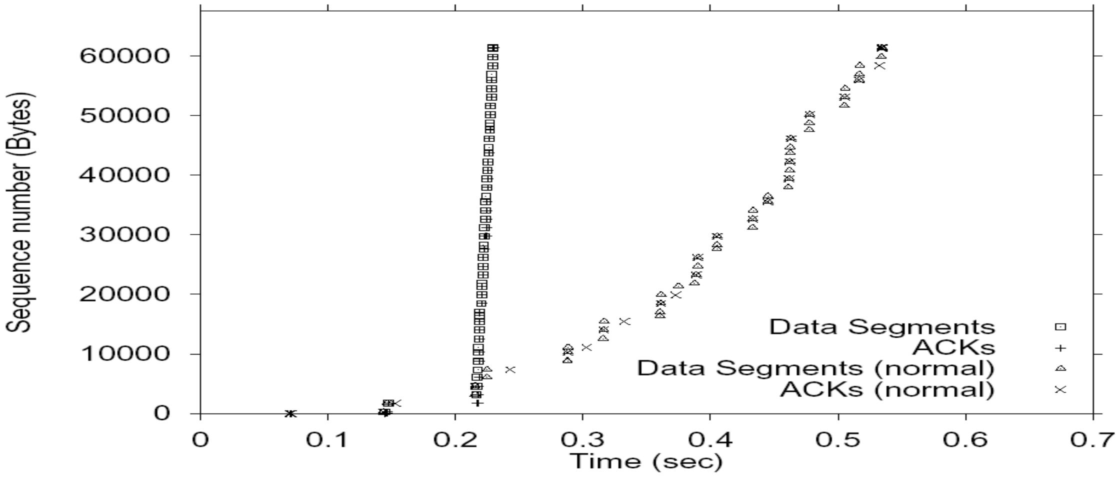
ACK Division Attack

- **Savage, Cardwell, Wetherall, and Anderson [SCWA99]** analysed the effect of sending spurious acknowledge. **They developed ACK Division Attack.**
- The discord between the byte granularity of error control and the segment granularity of congestion control leads to vulnerability.
- **The Attack :** When receiving N bytes of data, divide the data into M distinct segment (M<=N) and send acknowledgements for each segment.

- Each ACK is valid since it covers data that was sent and previously unacknowledged. And this leads the sender to grow CWND M times faster than usual.
- In this attack malicious receiver over exploit resources by tricking sender by sending more and more acknowledgements.



- As seen in the example , after one RTT **cwnd**=4, instead of expected value of2.



- This attack can convince a TCP sender to send all of its data in send buffer in a single burst.