6.033 Computer System Engineering

Spring 2009

Preparation for Recitation 14

Read *TCP Congestion Control with a Misbehaving Receiver* by Stefan Savage et al.

Underlying the design of TCP is an assumption that senders and receivers will abide by TCP's congestion control algorithm. A sender or a receiver may want to cheat and deactivate congestion control however. In particular, honest TCP senders back off in response to drops, reducing their transmission rates. In contrast, a cheating sender may increase its rate and grab the capacity that the honest senders release. This will cause more drops and thus the honest sender will reduce their rates further, letting the cheater grab an even bigger share of the bottleneck capacity.

A receiver also may be interested in cheating to make its FTP or Web download go faster. It is not immediately clear that a receiver can force an honest TCP sender to transmit more than its fair share, if the latter abides by TCP congestion control. This paper was the first to point out that a misbehaving receiver can actually fool an honest sender to send faster than it should.

Note that the paper refers to packets as segments. Also note that, in lectures, we simplified the TCP ACK scheme by saying that each data packet has a sequence number. In reality, each data packet is identified by the sequence of bytes it contains. For example packet 1:1460 contains the byte sequence 1 up to 1460. ACKs ask for the next byte that the receiver expect to receive, e.g., ACK 1460, means that the receiver has received all bytes up to byte 1460. Also, note that TCP has more components than the two we talked about in lectures (congestion avoidance (AIMD) and fast retransmit (use 3 duplicate ACKs as a sign of loss)). In particular, the paper mentions the slow-start and fast-recovery components. Check RFC 2581 for more information on these algorithms.

After reading the paper, try to answer the following questions:

- Attacks that change TCP as described in this paper are not common. Can you think why this is the case?
- Why it is wiser for a misbehaving receiver to use Attack 1 or 2 instead of Attack 3?