Programming Assignment Five

CMSC 417 Spring 2014

1 Deadline

May 13.

2 Procedure

Analyze the packet trace at `http://www.cs.umd.edu/class/spring2014/cmsc417/trace.tcpd`. It comprises 40 minutes of intermittent SSH traffic between my home machine and campus. If you have access, you may collect your own controlled trace as well, in order to debug or test.

1. Choose your favorite language that has a binding for libpcap. (Most do.) Do not parse the text output of tcpdump or tshark. That would make me sad.
2. Use that library to write code to determine:
   - How many losses (retransmissions) occurred? What's the loss rate of this set of connections? What's the loss rate in the forward direction? In the reverse?
   - What TCP options are active?
   - What the RTO appears to be, if ever there's a retransmission by timeout.
3. Find one additional thing that's interesting about the trace. "Interesting" may include violations of the protocol rules as I've described them in class, or pathological behavior that should not exist.
4. Turn in your trace analyzer program, executable name "tracey" on submit. It should output results including lines having the following format:

```
Loss count: %u
Packet count: %u
Loss rate: %5.3f%%
```

   In addition to anything else you need to output.

You may use Wireshark to confirm.

to the extent you can tell. (you should be able to tell). in interesting.txt or output.txt

interesting.txt

(which ones, named…)

(unless there never is…. you could say that.)

interesting.txt

loss or rxmit as defined by you.

output.txt.

but wireshark is often wrong.