CMSC 417 Computer Networks **Spring 2010**

Programming Assignment 4 — Understanding Network's Behavior

Assigned: Mar. 13, 2010 *Due: Mar. 25. 2010, 11:59:59 PM*

1 Description

In this assignment you will analyze a web transaction using a trace of network packets captured by a packet sniffer. You will observe the sniffed packets to look for TCP retransmissions, congestion control behavior, flow control behavior, and estimate round trip times.

We ran the packet sniffer on a web server in the department and we instructed 40 nodes to simultaneously download a file from the web server. You will analyze only one of these connections. We will provide you the connection to student assignment mapping.

You can find background information about packet sniffing in the Sniffer FAQ [1]. There are tools that help you with the analysis of pcap files. The most popular and widely used is tcpdump [4]. Tcpdump is installed on linux-lab nodes. In order to use it, type /usr/sbin/tcpdump. You may find the manual pages for pcap(3) and tcpdump(3) useful. The are programming interfaces to process network trace files. For this assignment you will use the C interface [3]. This interface will allow you to extract one packet at a time for processing.

1.1 Programming with libPcap

You will need to develop a tool in order to complete this assignment. You should get an idea which attributes are important from an initial inspection of the questions in section 1.2. Your program will take the name of the trace file as an argument while its output will be text files with (time, attribute) pairs, space separated. You will use this files afterwards to produce the plots in order to answer the questions in section 1.2. You can create plots by using jgraph [2] or gnuplot [5]. Using these plotting tools is not mandatory; you can use any other tool you like. You program should be invoked as follows:

```
pcapReader -r  <trace_file>  -h <IP address>
```

1.2 Write-up

You should also submit a short write-up, preferably formatted using two-column, single spaced, 10 point Times Roman fonts. I expect at least two pages; if it takes more paper to display legible graphs and explain them, so be it. Do not attach your code as an appendix, though you may append additional, possibly zoomed-in graphs. Do not prepend a cover page. The write up should answer the following questions for your assigned trace:

- What was the overall performance of the connection: how long did it take to download, how many bytes were transferred, and what is the resulting throughput? You should be able to infer these numbers from the sequence number plot.
- Was the connection's performance limited by the receiver's window? Graph the remaining space in the window left unfilled by the sender.

- Graph the size of the congestion window (the amount of unacknowledged data in the network at a time) over time . What you can infer from the graph? How the congestion control policy affects the performance of this transaction ?
- If there is unfilled space in the receivers buffer, perhaps the senders window is the limit. What is the size of the senders buffer?
- Did packets experience delay due to queuing? Graph the round trip time as a function of time. It is not necessary to implement Karn's algorithm to ignore samples during retransmission events. Compare the round trip delay graph to the window graph above.
- Can you tell what the senders initial cwnd is? You have to look at the raw tcpdump output here: it can be more accurate than looking at graphs output by of your program.
- Did the connection experience losses? Did these losses slow down the connection or were there enough packets in the queue to absorb the losses? Were there any timeouts? You should be able to answer these questions by interpreting the sequence number plot, looking for periods of slow start, idle periods, etc.
- If there were any losses, did they occur when the window was large or did the size of the window have little effect? I don't expect a statistical analysis, particularly since I don't expect you to see very many losses: a visual, qualitative guess is sufficient.

Use your judgement in how much text you need to explain the graphs and answer the questions listed above. Make sure you answer all (appropriate) questions, but please do not list them in your write up.

Graphs that you should generate are:

- Sequence number plot
- Unused receiver buffer space plot
- Congestion or actual window plot
- Round trip time plot
- Actual transmission rate plot

Metrics that you should calculate or estimate include:

- *overall performance*: time, bytes, throughput
- losses, detection, correlation with window size
- send buffer size if appropriate

References

[1] Robert Graham, *Sniffing faq*, `http://newdata.box.sk/2001/jan/sniffing-faq.htm`.

[2] J.Plank, *Jgraph*, `http://www.cs.utk.edu/~plank/plank/jgraph/jgraph.html`.

[3] TcpDump, *Programing with pcap*, `http://www.tcpdump.org/pcap.htm`.

[4] Tcpdump, *Tcpdump, repository page*, `http://www.tcpdump.org/`.

[5] Thomas Williams, *gnuplot*, `http://www.gnuplot.info`.