ELEC-E7130 Assignment 4. Traffic with probe packets

Markus Peuhkuri Tran Thien Thi Weixuan Jiang
César Iván Olvera Espinosa Yu Fu

Prerequisites

1. To complete this assignment, a certain amount of network capture knowledge is required.

   If you are not very familiar with network capture skills (TCPdump, Wireshark or tshark), you can refer to previous assignment instructions on packet capture.

Learning outcomes

At the end of this assignment, students should be able to

1. Capture internet traffic with test traffic into the network.
2. Collect basic statistics about the traffic generated using counters.
3. Analyze the traffic captured in the network from different aspects.
4. Filter captured traffic based on criteria.
5. Differentiate between active and passive measurements.

Introduction

The present assignment contains two tasks to introduce the active measurements and compare them with the passive measurements. Please read all instructions before starting because it is helpful to identify common work.

- Task 1: Packet capture with probe packets
- Task 2: Compare active and passive measurements

In this assignment, **capture the traffic data from your computer**. In the case of using a virtual machine (VM), generate traffic within that virtual computer instead of the usual host because it acts as a separate computer.

Task 1: Packet capture with probe packets

Choose one of the packet-capturing tools available such as *dumpcap*, *Wireshark*, *tcpdump*, etc.

1. **Set up active measurements** by running scripts based on the table provided for selecting servers related to the "*Basic measurements*" assignment 2 but use shorter interval such that you will have multiple measurements within measurement period in step

Servers	Tool
3 research servers	`ping`
2 iperf servers	`ping`, `iperf3`

2.

2. **Capture for a duration of minimum 15 minutes**, which includes regular activities such as web browsing, checking emails, watching videos, listening to music, and completing assignments, as well as the active measurements at background.

> **Note:** Record *interface counters and overall statistics* at the **beginning** and **end** of the packet capture as well as **store *the result of these active measurements (the command outputs)* for the next task**.

Once the packet capture is complete, **do the first sanity checks on captured data** for

1. Size of trace file.
2. Number of packets in trace file.
3. Total size of packets.
4. Compare values from interface counters to capture file. Is there any difference?

Answer the next questions based on the obtained pcap file using one of the mass analysis tools to use such as shown in the Table 1. Mass analysis tools or another suitable tool.

1. Plot the traffic volume over time by considering all captured packets within the most appropriate time interval.

2. Plot the traffic volume without the `ping` packets and `iperf3` packets over time (select the same interval selected in the previous plot).

3. Plot the traffic volume comparing the `ping` packets with the `iperf3` packets over time (keeping the same interval).

Hint: You can use filters to check specific protocols (`ping` traffic using ICMP protocol and `iperf3` traffic using TCP protocol and ports defined) and/or IP addresses (target server's addresses).

4. Provide the average throughput.
5. Do you have any observations from the above plot of network traffic?

   Hint: One of the tools that can be useful is Wireshark to plot and apply filters easily, or another way is converting the pcap file into a CSV file through `tshark` or another similar tool to process, plot, and filter the data using Python or R.

   Hint: In terms of recording counters to see overall statistics (only capturing sent and received packet counts are sufficient) for all network interfaces, you can use the command `ip -s link` on Linux.

Report, task 1

- Describe your measurement setup (tools and workflow).
- Summary of capture data.
- Were there differences between capture file statistics and counters?
- Plot traffic volume with different filters.
- What observations can be made from the captured data?

Task 2: Compare active and passive measurements

In this task, use the captured data from the previous task to **compare the results obtained by the active measurements (what you get from `ping` and `iperf3` log files) and by the passive measurements (what you get from packet capture)**. Some helpful guides can be found in the supporting material.

Extract information appropriately from the `iperf3` and `ping` sessions

- For the `iperf3` sessions, **calculate throughput** where there are two different options:
  1. You can use flow tools as the previous assignment (converting packet capture into flows) because most likely, each `iperf3` run will result in a different flow.
  2. Another option is to use `tcptrace` to extract information on TCP connections.
- In the case of the `ping` results, extract ICMP messages from traces or flows, correlate requests to responses and **calculate delay and identify possible packet loss**.

Hint: You can use filters to check protocol (`ping` traffic using ICMP protocol and `iperf3` traffic using TCP protocol) and/or IP addresses (target server's addresses). Besides, there are different ways to obtain the filtered data set using Wireshark, tshark, CoralReef, pyshark, tcptrace.

Analyze the captured data and answer the following questions:

1. How much traffic was there that was not `iperf` or `ping` traffic?
2. Compare `iperf` results from active and passive measurements. Provide a table and plot a time series.
3. Compare `ping` results from active and passive measurements. Provide a table and plot a time series.

Make a table comparing the active and passive measurements according to the following points:

1. Which additional active measurement tools can be beneficial, and what specific characteristics can they measure? (e.g. `ping` for the latency and packet loss)
2. Mention some passive measurement tools that can be useful in terms of availability, bandwidth utilization, errors, and discards? (e.g. *CoralReef* for description of traffic flows)
3. Describe some problems and limitations for both measurements.

Report, task 2

- Describe your analysis setup. Include code snippets.
- Answers to questions above.
- Were there any systematic bias on active and passive measurements?
- Make a table with the main differences between active and passive measurements.

Grading standard

To pass this course, you need to achieve at least 15 points in this assignment. And if you submit the assignment late, you can get a maximum of 15 points.

You can get up to 30 points for this assignment:

Task 1

- Use the correct method for traffic capture. (1p)
- Do the first sanity checks. (2p)
- Make a basic summary based on the first sanity checks. (3p)
- Plot time series to compare the traffic data in different conditions. (4p)

- Draw appropriate conclusions about the differences (2p)

Task 2

- Extract the throughput and latency data from the packet captured. (4p)
- Accurately answer the 3 questions raised in the data analysis (plot and table). (8p)
- Summarize based on the answers to the questions you answered. (3p)
- Compare active and passive measurements using a table (3p)

The quality of the report (bonus 2p)

The instruction of assignment

For the assignment, your submission must contain (Please don't contain original data in your submission):

- A zip file that includes your codes and scripts.
- A PDF file as your report.

Regarding the report, your report must have:

- A cover page indicating your name, student ID and your e-mail address.
- The report should include a description of measurements, a summary of the results and conclusions based on the results.
- An explanation of each problem, explain how you solved it and why you did it.