BLG433E: Computer Communications

Homework #2

Due Date: 22.04.2018, 23:00

Network protocol analyzers or ***sniffers*** are extensively used by network administrators (and unfortunately by hackers) to capture network traffic and inspect the packets to determine what is happening on the network.

Sniffers present the captured network traffic in a user-friendly manner. For example, they show arrival times, protocols, source/destination addresses, and sequence numbers of packets in an easy-to-follow tabular format. In addition, they let you analyze captured traffic by means of filters. Wireshark (https://www.wireshark.org/) is one of the mostly used network protocol analysers.

In this homework, you are asked to use Wireshark to capture network traffic on a moderate traffic network (e.g., in library or a coffe shop).

You are asked to capture network traffic via your computer's wireless interface and analyze the TCP traffic generated. You should create traffic for short flows (e.g., by requesting some web pages) and long flows (e.g., by downloading a file (e.g. a Linux distribution) or watching a long YouTube video).

First of all, identify your TCP connections by using TCP end-points (i.e., source/destination IP addresses and TCP ports). Then, show and analyze your TCP connection packets: How TCP data/ACK sequence numbers change with time? How many retransmissions occur? What are the round-trip times? What are TCP segment sizes used for data/ACK packets? ...

You have to submit **Wireshark *.pcap files and a report**.

The report should contain

1. The Wireshark filters used as well as their explanations.
2. Properties of the computer used in measurements.
3. Locations/Times where/when the experiments were run.
4. The graphs (along with your comments) for the TCP traffic measurements.