# ICSI 525 Mobile Wireless Networks, Spring 2018 – Homework 1
# Due February 21st, 2018 11:59PM via Blackboard

## 1 Requirements and policies

Students should complete this assignment individually. Your turn-in is due on Blackboard. Note that there is a fair amount of software installation to be completed before you can answer the questions below. This will take time and will raise questions, so start early and come to office hours to discuss any issues.
**Late submissions will not be accepted.**

## 2 Assignment overview

The purpose of this assignment is to familiarize you with ns-3[1] network simulator and remind you of how to use Wireshark[2]. To complete this assignment you must install ns-3. Note that ns-3 runs only under Linux, so if you don't have access to a Linux machine, you can do one of the following: (i) create a dual-boot machine, (ii) install Linux in a virtual machine or (iii) use a Linux environment like Cygwin. The directions for installing ns-3 can be found on the following URL https://www.nsnam.org/docs/tutorial/html/getting-started.html. The assignment consists of two parts. In the first part you will get familiar with the simulator and the modules it includes. In the second part you will run some basic simulations and analyze the results.

## 3 Part 1: Getting familiar with ns-3

At this point you should have successfully installed the ns-3 simulator on your computer. Navigate in your installation to answer the following questions.

1. What wireless network modules are available in ns-3? Consider Data Link Layer (i.e. MAC protocol modules) and Network Layer (i.e. routing protocol modules). In what directories are they located?

2. OLSR and DSR are two mobile network routing protocols. Refer to [1] and briefly (in one paragraph) describe their similarities and differences.

3. What mobility models are included in ns-3? In what directory are they located? Lookup online and briefly describe what is the *random waypoint* mobility model. Go on GoogleScholar and find one highly-cited paper on random waypoint mobility. List the paper title, authors, venue and year of publication.

4. In part 2 of the assignment we will run a ns-3 example called `csma-ping` provided through the ns-3 code base. The example code can be found in `ns-3.25/src/csma/examples/csma-ping.cc`. Following our in-class discussion of `ns-3.25/examples/tutorial/third.cc` draw the network architecture that `csma-ping` creates and also draw the block-diagram of the `csma-ping.cc` implementation. Who pings whom in this example?

## 4 Part 2: Running a simulation and analyzing the results

In this part you will learn how to run a simulation and analyze the results. We will work with an example called `csma-ping` provided through the ns-3 code base. Run the `csma-ping` example using waf[3] and note where the program stores the output .pcap files. Once you fully understand how to run the example and where to find the output you can proceed to the actual measurements.

[1] `https://www.nsnam.org/`
[2] `https://www.wireshark.org/`
[3] If you are unsure how to do this, follow the "Running a script" instructions on the Getting Started page `https://www.nsnam.org/docs/tutorial/html/getting-started.html`

For your measurements, you will execute `csma-ping` five times using the default parameters and saving the .pcap files for each execution. Note that when running simulations, you should never draw conclusions based on a single execution of an experiment. In order to obtain statistically-significant results, you need to run an experiment multiple times and then present results across these runs.

Once you have the pcap files saved, you will analyze them using Wireshark and its command-line equivalent Tshark[4]. (If you haven't already) you will need to install Wireshark and Tshark on your computer. For more information and installation instructions visit `https://www.wireshark.org/` and the Wireshark User's Guide `https://www.wireshark.org/docs/wsug_html_chunked/`.

After running the five simulations, use Wireshark or Tshark to examine the packet traces and answer the following questions.

1. How many of ICMP requests/replies were sent in each ping session?
2. Did you notice any protocols that were not ICMP-related? Why were they necessary?
3. Were there any packet losses?
4. Compare and contrast RTTs achieved in simulation to these from real-world measurements. To answer this question, follow the instructions below.

Compute the average round-trip time (RTT) across all runs for each pair of hosts. This is where you can use `tshark` to convert your .pcap file to a textual file and automate your computations. In order to do this you can issue the following `tshark` command:

```
tshark -r <ping-output.pcap> -T fields -e frame.number -e frame.time_epoch -e eth.src -e
eth.dst -e ip.src -e ip.dst -e icmp.type -E separator=, > <ping-output.csv>
```

substituting the .pcap and .csv file names as appropriate. This command reads the already collected .pcap file and applies filters to it in order to extract the frame number (frame.number), frame unix timestamp (frame.time epoch), source and destination MAC and IP addresses and ICMP packet type (icmp.type)[5]. You can learn more about all the filters you can apply to a .pcap file here `https://www.wireshark.org/docs/dfref/`. The information produced by the above tshark command is saved in a .csv file, which you can post-process (e.g. using `awk`[6]) to calculate the RTT.

Your calculations should produce three values of average RTT – one for each node pair. Note these values in your submission. Now let's compare the results from simulated ping measurements with these from a real Internet ping. Execute `ping` from your machine to a server on the University at Albany network (say our web server at `www.albany.edu`). Here is how it looks like if I send 3 ping requests from my PC to the university web server:

```
 mariya@shasta  $ ping www.albany.edu -c 3
PING www.albany.edu (169.226.1.110) 56(84) bytes of data.
64 bytes from www.albany.edu (169.226.1.110):  icmp seq=1 ttl=254 time=0.742 ms
64 bytes from www.albany.edu (169.226.1.110):  icmp seq=2 ttl=254 time=0.768 ms
64 bytes from www.albany.edu (169.226.1.110):  icmp seq=3 ttl=254 time=0.755 ms
--- www.albany.edu ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.742/0.755/0.768/0.010 ms
```

Do you see a difference in the average RTT from your simulation and in a real Internet scenario? Comment on your findings.

# 5 Turn in

This homework is due by 11:59PM on Wednesday, February 21st, 2018. The turn-in consists of the answers to the questions in part 1 and 2 (in a single PDF) and the script(s) you wrote to compute the average RTT in part 2. Turn in your work through Blackboard as two files – the first file is your PDF with answers and the second file is a zip archive with your script(s).

[4] `https://www.wireshark.org/docs/man-pages/tshark.html`
[5] ICMP type 8 is the code for ICMP request and ICMP type 0 is the code for ICMP reply.
[6] `https://www.gnu.org/software/gawk/manual/gawk.html`

# References

[1] C. E. Perkins, E. M. Royer, S. R. Das, and M. K. Marina. Performance comparison of two on-demand routing protocols for ad hoc networks. *IEEE Personal Communications*, 8(1):16–28, Feb 2001.