ECE-6610 Programming Assignement 1

Teammate: Ching-Kai Liang (cliang30@gatech.edu)
Huangwei Fang (hfang@gatech.edu)
Wan-Chen Yeh (wyeh7@gatech.edu)
Yash Shah (shah_yash10@gatech.edu)
Yiling Yin (yyin60@gatech.edu)

In this assignment, we have four cases for 802.11 mac protocols:

	ACK is enabled	ACK is disabled
RTS/CTS is enabled	CSMA/CA	CSMA+RTS/CTS
RTS/CTS is disabled	CSMA+ACK	CSMA

PART 0:

How to disable ACK and disable RTS/CTS?

Disabling ACK:

1) Disabling sending ACK for received data by commenting out line 1927 and 1938 in mac-802_11.cc
2) Change tx retransmit data to considere every packet as successfully transmitted after timeout by modifying line 1327-1338 in mac-802_11.cc
3) Change timeout period to only wait for transmit latency and propagation latency by commenting out all the other waiting time in line 1042 in mac-802_11.cc

Disabling RTS/CTS:

1) Add a line in the *.tcl :

```
Mac/802_11 set RTSThreshold_    3000
```

2) The default value of RTS threshold is 0 which means that any packet with size greater than 0 has the RTS/CTS mechanism. Therefore, if we want to disable RTS/CTS, we just set this value greater than the maximum packet size (1500 bytes).

PART 1:

1. **Obtain the total throughput achieved with four MAC protocols (CSMA/CA,CSMA+RTS/CTS, CSMA+ACK, and CSMA) under zero packet loss in both topologies. Plot the results as a bar chart.**

Ans:

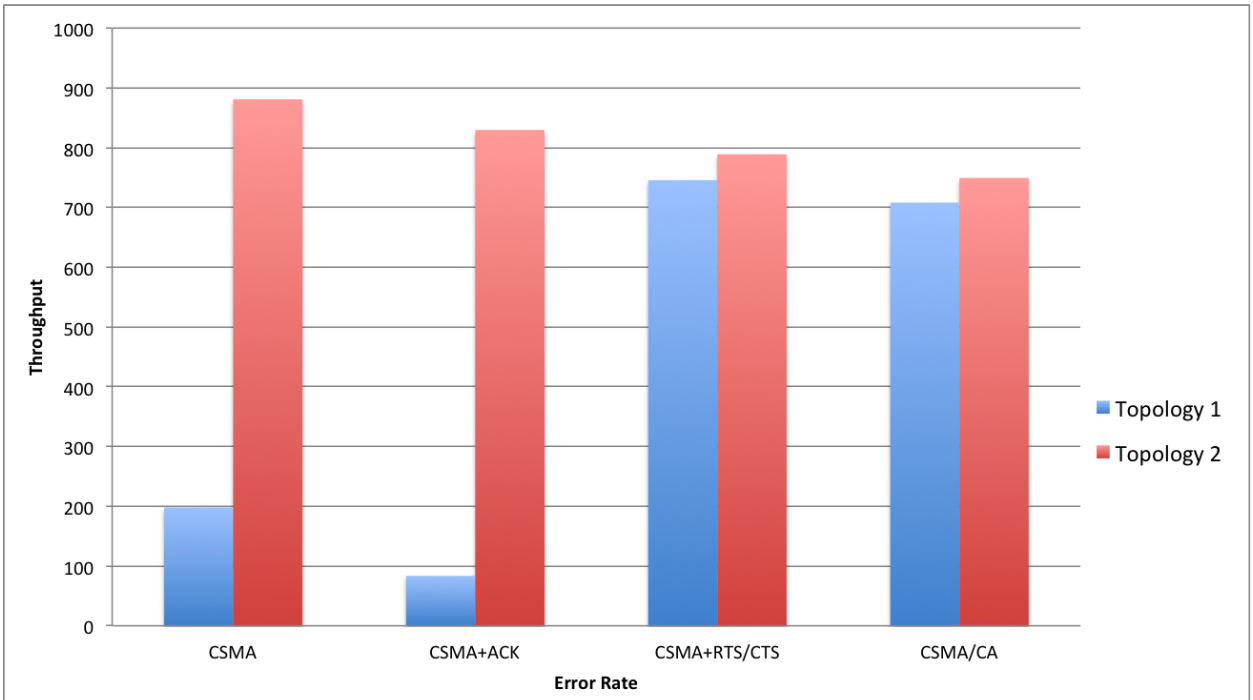

Figure 1: Throughput of Topology 1&2 with Zero Packet Loss

2. **What is the difference between topologies T1 and T2 that leads to different performance?**

Ans: Compare with topology 1 and topology 2, the main difference is the hidden terminal problem. From figure 1, we can see the throughput is much better when the RTS/CTS is enabled for topology 1. This is because RTS/CTS can mitigate the hidden terminal problem. In topology 2, since the two senders are close to each other, they can hear each others transmitted signal so there is no hidden terminal problem.

Another interesting thing is that the performance is better for topology 2 when RTS/CTS is disabled. This is because using carrier sensing is sufficient to detect the collision. Therefore enabling RTS/CTS only introduce additional overhead but does not provide any additional performance benefit.

3. Compare the performance of the MAC protocols in T1. Explain the reasons.

Ans: The slope of CSMA+RTS/CTS and CSMA/CA is steeper than that of CSMA and CSMA+ACK. The former cases have RTS/CTS mechanism which overcomes the hidden terminal problem. Therefore, it is obvious that the throughput will decrease as the error rates increase. For the latter cases, the hidden terminal problem dominates the performance, so the variations in error rates will not greatly affect the throughput. Besides, the protocols with ACK (CSMA+ACK and CSMA/CA) has smaller throughputs than those without ACK. This is because we shorten the timeout period when we disable ACK. Thus the transmitter can send more data in a time period which results in increased throughputs.

An interesting thing is that we observe a relatively flat trend in throughputs versus error rates for CSMA and CSMA+ACK. This is because with hidden terminal problem and without RTS/CTS, collisions at the receiver already introduce more than 80% of the packet loss when the channel has a 0% error rate (The maximum throughput is 1000 kbps). Therefore, when we introduce a 10% channel error rate, we are only actually adding a 10% error rate on the packets that did not collide. That's why we see that for CSMA, a 0% error rate has around 200 kbps, whereas a 10% error rate ends with 185 kbps.

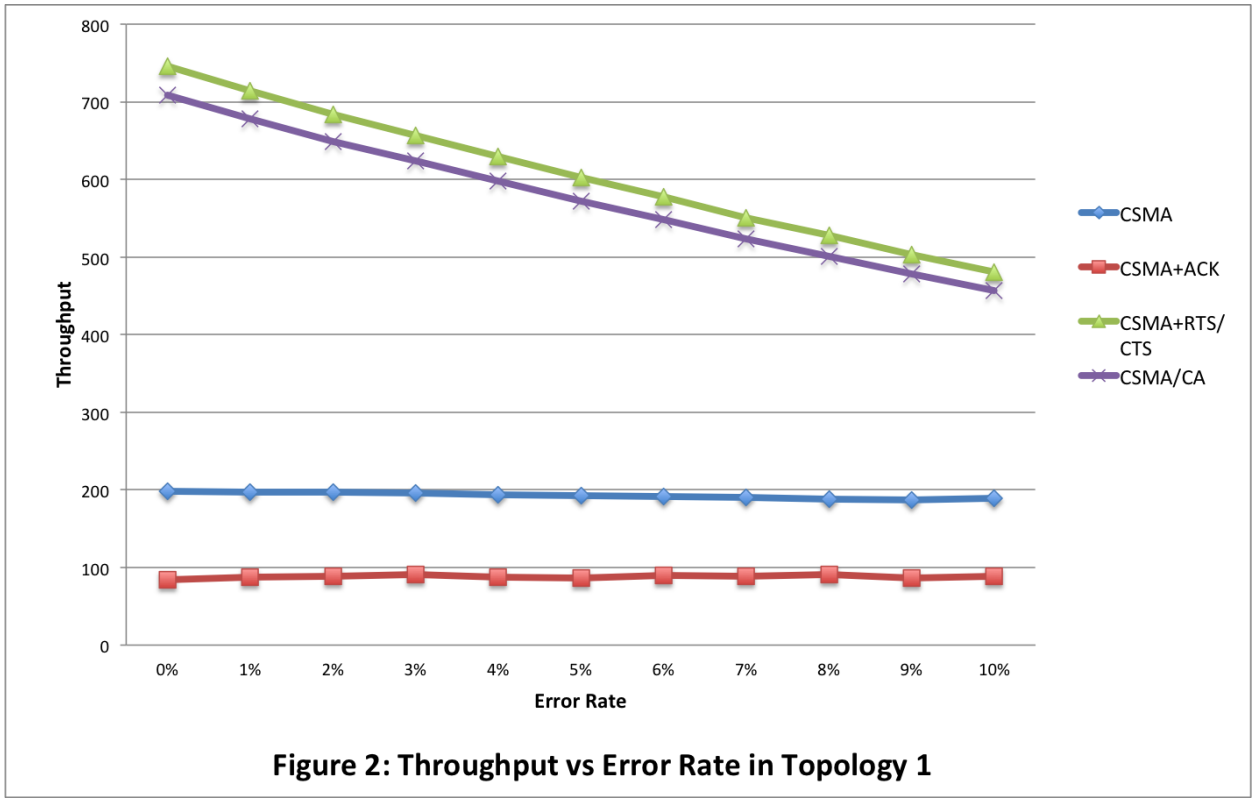

Figure 2: Throughput vs Error Rate in Topology 1

4. Compare the performance of the MAC protocols in T2. Explain the reasons.

Ans: In topology 2, since the distance between the two transmitter nodes N1 and N3 is 50m, which is within their range of reception, they could effectively hear each other, as opposed with the case in topology 1. The results shows that the throughputs of all the four protocols

decrease as the error rates increase. Since RTS/CTS has almost no use in this scenario, the two protocols with RTS/CTS have the lowest throughputs among the four. And particularly, CSMA/CA has the lowest throughputs, since with both RTS/CTS and ACK, the amounts of effective data it could send within a time period is comparatively lower than the others. For the other two protocols without RTS/CTS, CSMA has a higher throughput than CSMA+ACK because without ACKs, the transmitter is able to send more data within a time period since it has a shorter timeout period, which effectively increases its overall throughput.

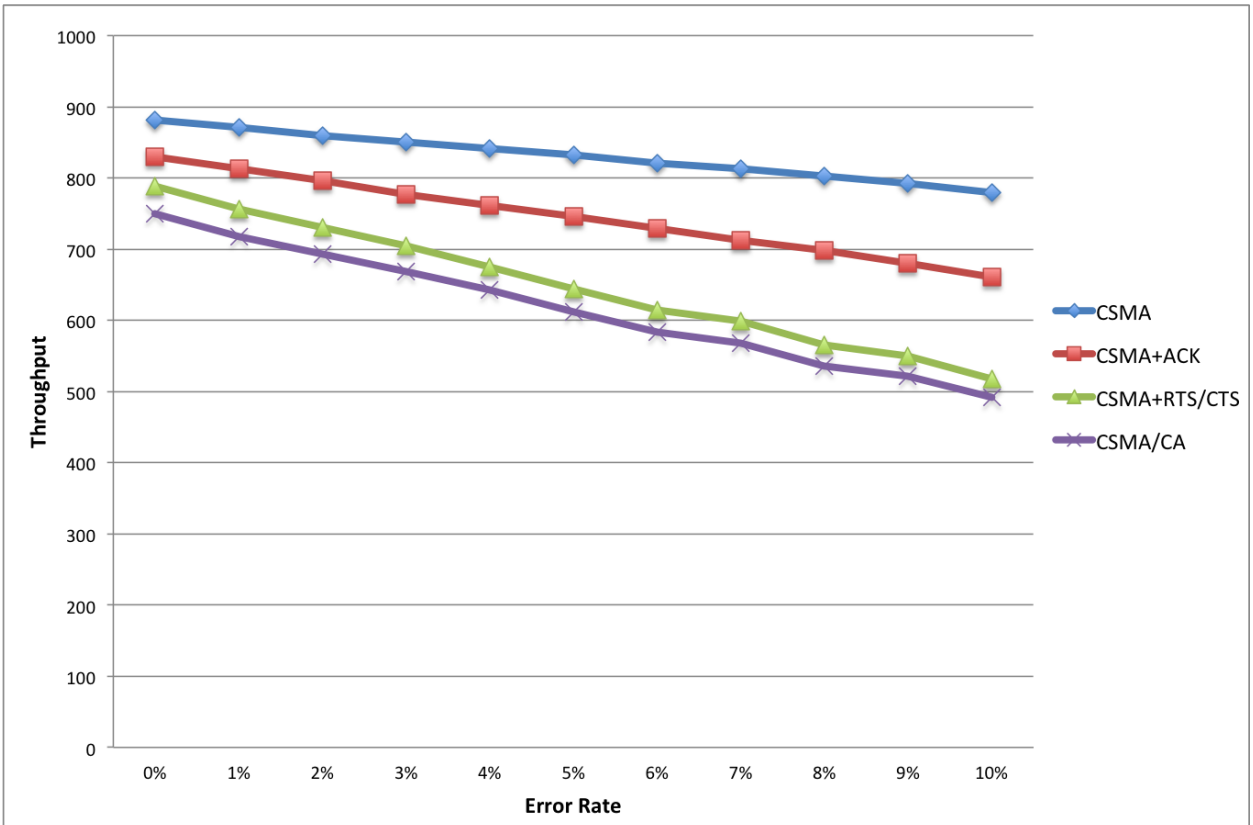

Figure 3: Throughput vs Error Rate in Topology 2

5. **Obtain the total throughput achieved with four MAC protocols (CSMA/CA, CSMA+RTS/CTS, CSMA+ACK, and CSMA) under different packet loss rates in both topologies. Compare the throughput performance among the medium access strategies. Explain the results.**

Ans: The major difference between the throughput for the same medium access strategies for the two topologies stems from the positioning of the Tx nodes. In topology-1 the two transmitting nodes are on opposites sides of the receiver and are not able to sense each other creating the conditions of the hidden terminal problem, while in topology-2 the Tx nodes are closer to each other allowing for inter-node sensing, this leads to lesser contention taking place between the Tx nodes removing the need for RTS/CTS contention management.

Another major difference between the protocols for the two topologies is the shift in the ordering of the best to worst protocol throughput. In topology-1 CSMA+RTS/CTS and CSMA/CA are positioned higher because they are modelled to reduce contentions leading to it being an effective protocol for the hidden terminal problem.
While in topology-2, CSMA and CSMA+ACK are positioned higher because the inter-node sensing removes the need for the overhead involved with RTS/CTS in the other two protocols results in a higher throughput.

PART 2:

1. **Connect your wireless card on the laptop to some Wi-Fi network (Ex: GTLawn). Find the following: the 802.11 standards supported by your Wi-Fi card (a/b/g/n), ESSID of the network connected, MAC ID of the access point, MAC ID of the Wi-Fi card, different bit-rates supported by the access point, whether RTS/CTS is enabled, whether security is enabled and if yes what kind of security is used.**

Ans: Machine: late-2011 MacBook Pro
Supported wifi: 802.11 a/b/g/n
ESSID: GTwifi
$MAC\_ID_{access\_point}$: 0C:D9:96:76:9C:2B
MAC_ID_{wifi}: B8:8D:12:44:CB:0E
Bit-rate supported: 6, 9, 12, 18, 24, 36, 48, 54
RTS/CTS: off
Security: WPA2 Enterprise

2. **Perform this experiment in a residential area (your house or apartment. Any sort of campus housing is not a valid location). Scan for all the Wi-Fi access points in the vicinity. If necessary, you might have to disassociate with your network to be able to scan all the networks. Find the following: number of APs, how many APs have security enabled, the different channels used by the APs, number of APs using each channel. Repeat the experiment in the Klaus building. Present the results in the form of a table. You might find that more than one AP has the same ESSID in Klaus. What is the reason for this? Qualitatively compare the two types of Wi-Fi deployments (distributed residential and centralized office).**

Ans:

	Klaus	Home
Number of APs	23	8
Number of APs with security	16	5
Number of channels used by APs	8	3

Number of APs in channel 1	1	1
Number of APs in channel 2	1	0
Number of APs in channel 6	2	0
Number of APs in channel 11	5	6
Number of APs in channel 36	4	0
Number of APs in channel 52	4	0
Number of APs in channel 132	4	1
Number of APs in channel 149	2	0

The reason to have APs with the same ESSID but on different channel is to increase the coverage but minimizing the interference. This is often done in network cell planning, where adjacent cells/APs will use different channels to limit interference.

On campus, the wifi are centralized managed, therefore we can see a certain degree of network planning. Such as the same ESSID will have multiple access points that utilizes different channels to avoid interference. And also, the channel used are also separated far apart, thus minimize signal leakage to adjacent channels.