Chris Bird, Blake Tacklind

997337048, 997051049

ECS 152A/EEC 173A – Computer Networks

Due: 12th March, 2015

Ad Hoc Network – Project Phase 2

Taken directly from the project description, the above graphs have throughput as the number of bytes sent per millisecond, and the average network delay as the number of total delay divided by throughput. However, these numbers did not seem to be useful, so we got a few others to include with the report.

In these graphs, average network delay is instead calculated by total delay divided by bytes sent total. This results in more realistic units of measure, rather than (time^2)/bytes, this is time/bytes. This is *not* what the project asked for, but it seems more logical to include it.

Since our other two simulations did not have much collision, we decided to make the lambda values large enough to show collisions happening. Our lambda values were the values given in the project specifications multiplied by one thousand. We used the same average network delay calculations as the second set, which is total delay divided by bytes sent.

Phase I Write up – Description and Logic

Discrete Event Simulation

Discrete event simulation is the simulating based on distinct events. Those events and only those events are what affect the state of the simulation. Other properties such as time and stacks only exist as a byproduct of the events occurring.

Description of Phase I

In Phase I, we simulated a single server as it receives and distributes response packets. Packets are received and handled in a negative exponentially distributed time (a decent approximation of real networks). Our simulated server therefore had to deal with any number of incoming packets and occasionally had to drop the packets due to insufficient incoming buffer size.

Logic of Phase I

Our phase I simulation ran until an arbitrary time was passed. Each cycle handled one event advancing time to the time of the next events occurrence. The next event would always be either an incoming event or a departure event (if the buffer was not empty). On incoming event we would check if we had room in our buffer and if so add a departure event to our buffer. Then decide when the next incoming event would occur. If a departure was the next event we would pop an event off the departure queue and decide when the next departure event is to occur. We would repeat this process with different lambda and buffer sizes for all conditions in the simulation.

Phase II Write up – Description and Logic

Description of Phase II

In phase II, the goal was to use our phase I code along with some modifications to make an Ad Hoc network. This means that there is no central hub or router for the network, but that each host communicates directly with all other hosts. In order to make sure that this is successful, there can only be one packet being broadcast at any given time. This is to ensure that the data doesn’t get incorrectly read by the destination host. To secure this, CSMA/CA protocol is used with DCF to detect possible collisions and stop them from happening. If at any given moment in time, the network has been idle for more than DFIS time, and an ACK has been sent acknowledging the most recently sent packet (also greater than SIFS time), the network opens up again to have another packet sent. If more than one host wants to send a packet at that exact time, they both get told to ‘back off’ and have to defer their packet by a randomly generated amount of time. This back off time is increased by a factor of 100%, then 200% etcetera for each time it is told to back-off. If at a given time the network is idle and only one wants to send, it gets to send and all others must wait until the network is idle again.

As far as our implementation goes, a few assumptions have been made, the most notable of which is that all packets that get sent are guaranteed to be received by their intended host. This is important to note as once a packet is sent, it will certainly get an ACK back after SIFS plus time to send 64 bytes has expired. Other assumptions include that there are no hidden hosts, hosts that are out of range of any other host, and that the max packet size is 1544 bytes long.

Description of Phase II Logic

Unlike our implementation of phase I, we used a for loop that counted through time in single steps at a time. In phase I we ‘jumped’ the clock to the next time value when an arrival or departure happened and ignored all the ones in between. However, since so many different things needed to be done on each clock cycle, we found it fitting to step through the clock on step at a time rather than skipping to the next appropriate time. Before this clock loop, some initializations needed to be done to prepare for smooth operation. First, using the number of networks given by the simulation, a list of hosts called ‘network’ was made that contained pointers to each of the hosts created. Using this list, each host could be accessed and worked with without needing to give it its own name. When each host is created, it generates a time until it will attempt to send its first packet, which will also be assigned a size based on a negative exponential distribution. From here, the clock can proceed as normal until a packet wants to be sent.

On each clock cycle, which increments in hundredths of a millisecond, if the channel is not busy, each the DIFS counter is decremented, letting the hosts know how long until they can attempt to send again. Also, if the channel isn’t busy but a packet was recently received by a host, a SIFS amount of time is waited, and then the receiver of the packet sends an ACK back to the sender. Due to SIFS being less than DIFS, the ACK will always be sent *before* the channel opens up to new traffic, ensuring proper acknowledgment of packets.

Once SIFS and DIFS are zero, and the channel is idle, each host is then polled for whether it wants to send a packet at this very moment or not. If it does, it is added onto a list called ‘sending’. This list is used to determine if there is a collision or not, and if so, to handle that collision. If the size of sending is exactly one, that packet is removed from the outgoing queue on that host and sent to the received after the amount of time it takes to send a packet of that size. If the number of items in sending is greater than one, a collision notice is sent to both, and they both set backoff counters before retrying to send that packet. Since these backoff counters are negatively exponentially generated, there is a low chance that they will try to send again at the exact same time. However, each time a packet collides with any other packet, it will wait a longer period of time before trying again. This makes it harder and harder for the backoff counters to be the same, allowing for traffic to flow once again.

After the clock has run its course, and is now equal to the total amount of time set to run the network, throughput and average delay is calculated using basic equations. A description of how we got our numbers can be found in the next section.

Phase II – Data Analysis



There are three data sets listed above, these data sets were used to create the graphs you can see on pages one through three of this report. Data set one is the exact data as requested by the project specification sheet. Using the given lambda values and number of networks, we determined throughput by calculating the total number of bytes sent through the network, and then dividing by the total amount of time that the network was running. Next, the average delay was calculated by taking the total amount of delay both in time the packet was spent sending and the time from creation to sending of the packet, and then dividing by the throughput. This yielded some somewhat unexpected results.

In data set two, we modified the calculation of average delay to use number of bytes sent as the denominator rather than the throughput. This put our units of measurement at milliseconds per byte rather than the milliseconds squared over bytes that was calculated in the first data set. We created this data set, along with data set three, to expand on the project and determine some new information. In data set three, we multiplied lambda by one thousand in order to force collision to happen. We also used our new average network delay calculation rather than the project defined one in this section as well. As can be seen from the data, the through put has multiplied exponentially as the packets are being sent much faster, but the delay has also increased dramatically as the number of collisions and need for back-off counters is much greater than in previous data sets.

Final Thoughts and Conclusions

Looking back over our code, we are very proud of how it turned out. We have made many tweaks, many changes, and many deletions of code, and as a result have a very short and optimized run time. However, there are still some things that could be made more efficient, which we may work on after finals. Running our code with the number of networks set at two thousand, regardless of lambda value, produced very predictable results. There were a ton of collisions, throughput was still relatively high, but the average wait time for a packet was very high as well. Since we have a counter for number of packets sent from each host, it was interesting to see how long it would take before a second packet was sent from a server.

In closing, our main function is very neat, and laid out in a very easy to understand fashion, and the packet and host classes both are very easy to understand their function and practicality. There are very few things that could be made more optimized and the code itself works beautifully. Running many simulations on this code would take very little time and almost no edits. It should also be noted that upon completion of each run, all the data is written to a .csv file that can be easily opened and edited in Microsoft Excel. This allows for easy creation of graphs, data sheets, and trend lines.