S.ID.1605062

Computer Networks Sessional
Network Simulator 2.0 Assignment Report

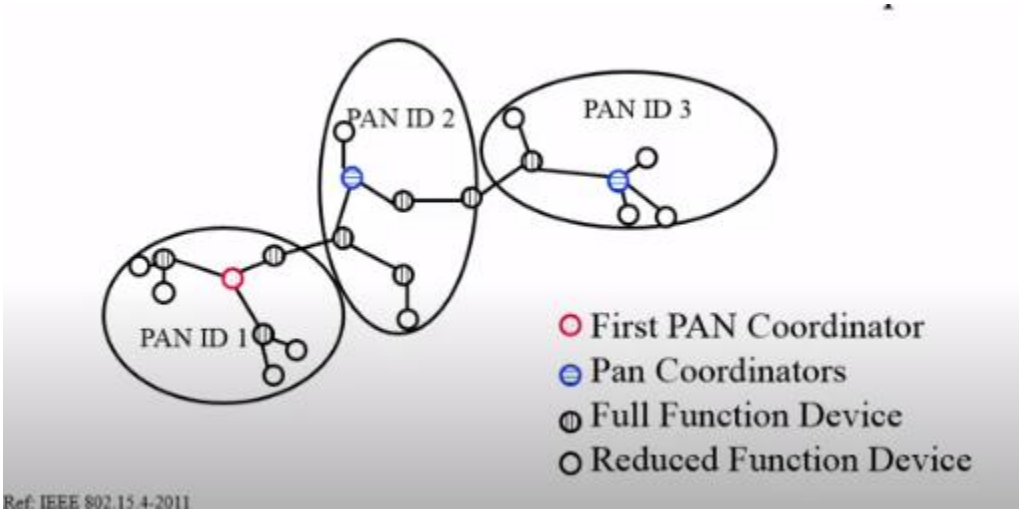
Wireless 802.15.4

This MAC protocol is also known as wireless personal area networks. This is underlying architecture of many famous IOT protocols such as ZigBee, 6LowPAN, Wireless Hart, MiWi etc. This has very low power consumption and very low bandwidth speed (around 50kbps application data rate). As it consumes very less power that's why this is very suitable for establishing communication between IOT devices. Every 802.15.4 supported IOT device has a unique EUI-64 address like our NIC has unique MAC address.

In this protocol a network can has two kind of nodes. We can call them Full Function Device (FFD) and Reduced Function Device (RFD). FFDs can forward packet on the other hand RFD only can receive or sent its own packet throughout the network.

In the beginning, out of all the FFDs, the network selects one coordinator. RFDs can not forward packets hence they can not the network coordinator. Any FFDs can become a coordinator, and the coordinator might change in various circumstances. Nodes join a cluster by sending association request to the coordinator and coordinator assigns a 16-bit short address to the device. This 16-bit address can be used to communicate between this cluster. To communicate with outside network complete EUI-64-bit address is needed.

One or more clusters can form a network where each cluster has one PAN coordinator connecting one or more FFDs and RFDs. Each cluster is connected with other clusters by FFDs which are not necessarily PAN coordinators. The network than looks like the figure shown below.



Ad Hoc On-Demand Distance Vector Routing Protocol (AODV) :

This is an on demand reactive routing protocol which means the route is decided when we want to send a packet from source to destination at first. Route is discovered by broadcasting Route Request Packet (RREQ) to all the other nodes in the network. When the destination router receives this packet, it sends unicast Route Reply Packet (RREP) to the RREQ initiator and thus nodes in between updates their routing table and knows how to send a packet from source to destination. This information is cached until any node finds out their neighbour is not available or new neighbour has emerged. If these things happen the network maintained it routes by notify the source node about the link failure and then again source sends RREQ like before to establish a connection to the destination.

Here Ad Hoc means no infrastructure hence the network is resilient. Quite useful in military and emergency. This protocol helps in multi-hop wireless communication as the

intermediate nodes changes far to often and route is discovered when needed not when the network changes state (which is far too often when wireless network is concerned).

TCP Tahoe:

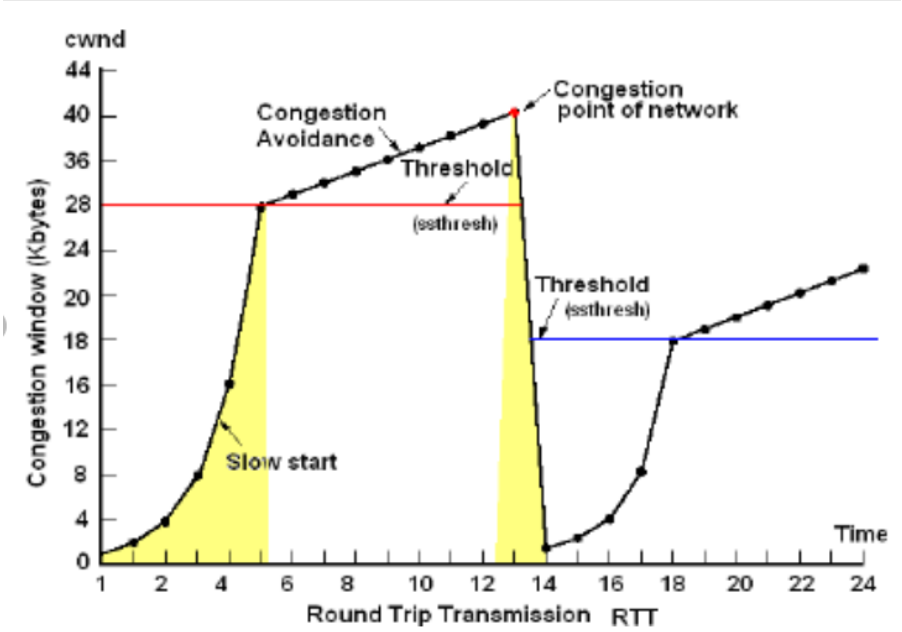
TCP Tahoe basically implements basic go-back-N with slow start and congestion avoidance. It uses two variables cwnd(congestion window) and ssthresh(slow-start threshold).

At the beginning, slow start phase occurs where we initialize cwnd with 1 and when new data is acked we increment cwnd by 1. Eventually as the value of cwnd gets incremented the communication line faces congestion.

When congestion occurs in order to avoid congestion, we change the ssthresh hold value to the half of cwnd and initialize cwnd to 1 so that again we can initiate slow start until cwnd matches the value of ssthresh. This is how TCP Tahoe manages to avoid congestion. This congestion is detected and value of ssthresh is set when time out occurs.

When cwnd passes the value ssthresh hold then we increment cwnd by value less than 1 so that we get additive increase in total packet sent. As total packet sent in sliding window is 2^{cwnd}. This way we try to increase throughput until we again face congestion. Then we follow the congestion avoidance protocol again.

The graph below sums up the whole discussion.

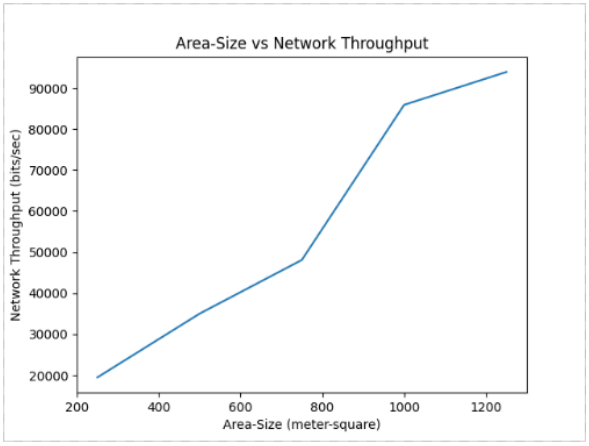


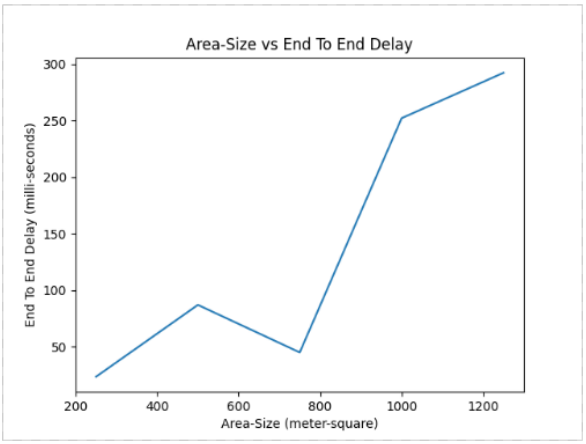
Telnet:

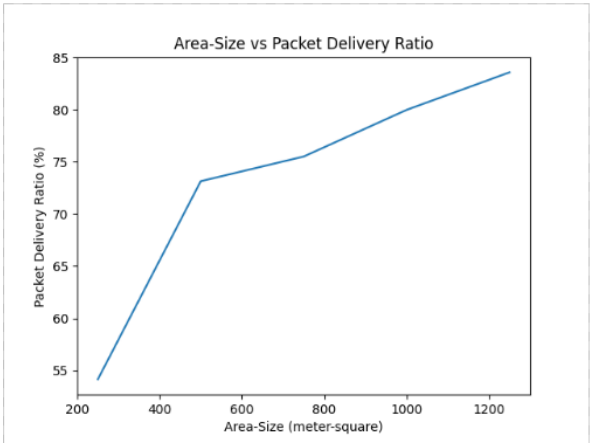
This is a terminal emulation program that is used to access and configure remote servers, routers, switches etc. It is a command line tool that helps us to access another device through network and control that device from the device we are currently working on. As it is a command line tool, it doesn't send any graphics so it is extremely fast.

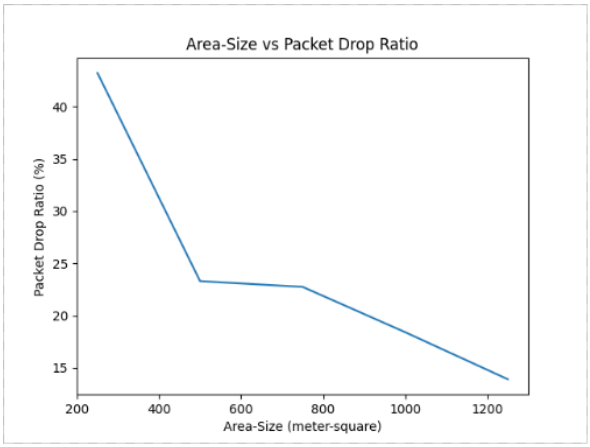
Telnet was used to configure servers. But as Telnet doesn't support encryption protocol, it is not safe to use it to access databases over public network. These days it is mainly used in personal area network. Instead of Telnet, SSH is now used globally as it supports encryption.

Discussion with Plots:





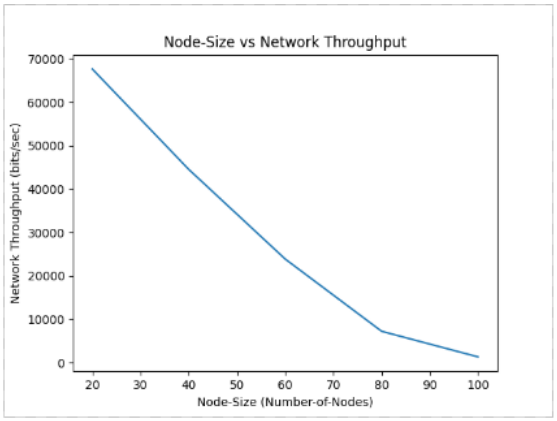


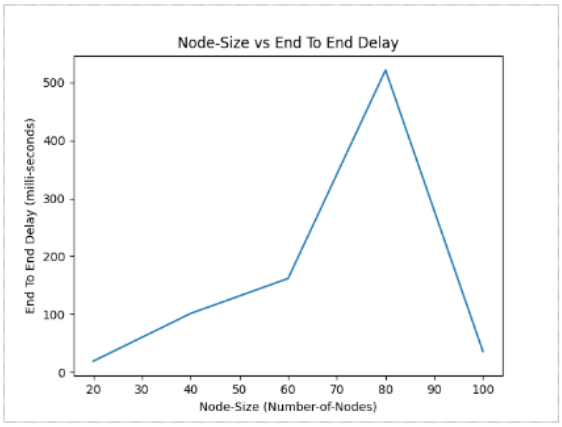


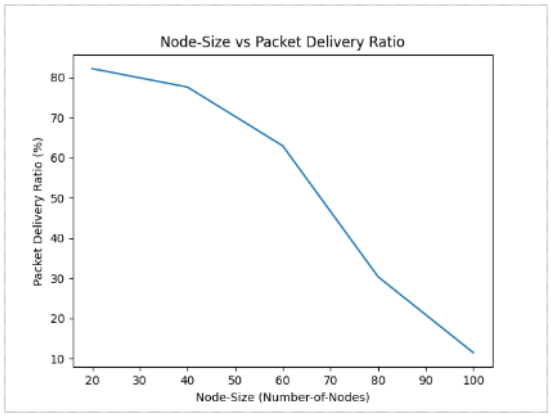
Observation on the change of Area Size:

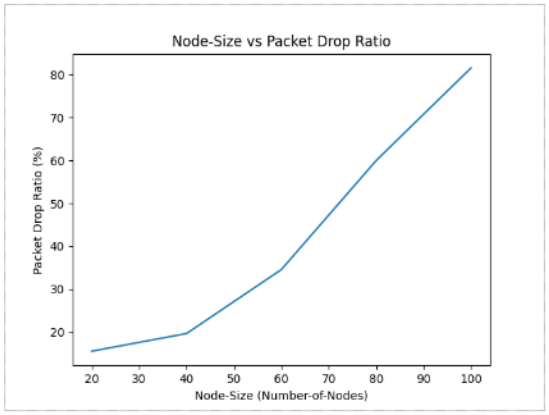
As we know AODV use broadcast RREQ to find out its route if source node has a lot of neighbors then broadcast packet grows exponentialy with the number of neighbors which wastes a lot of bandwidth. As area size increases nearby neighbor number decreases hence network bandwidht is less wasted on route request packet instead it is used to delivar data packet. That's why increasing in area size increases throughtput and packet delivary rate and decreases packet drop rate.

As area size increases the the distance between each node increases hence average delay also increases as area size increases.





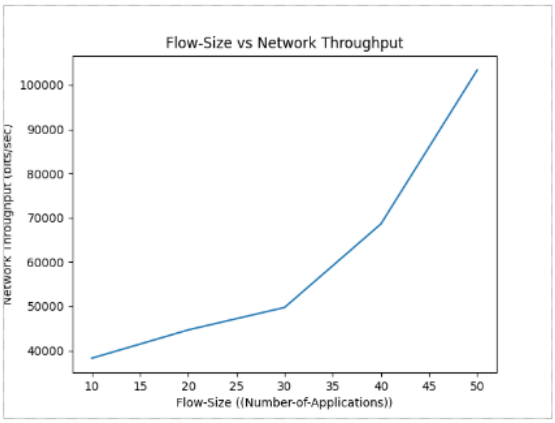


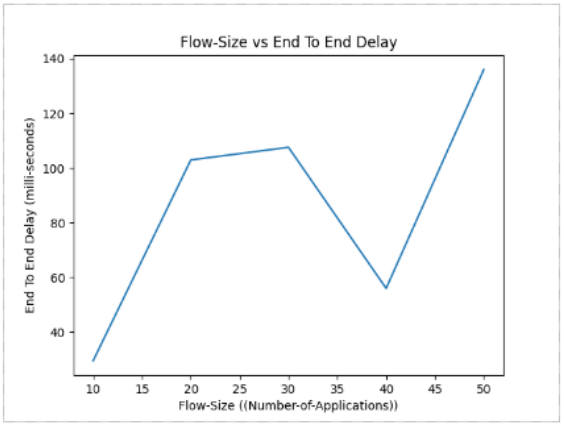


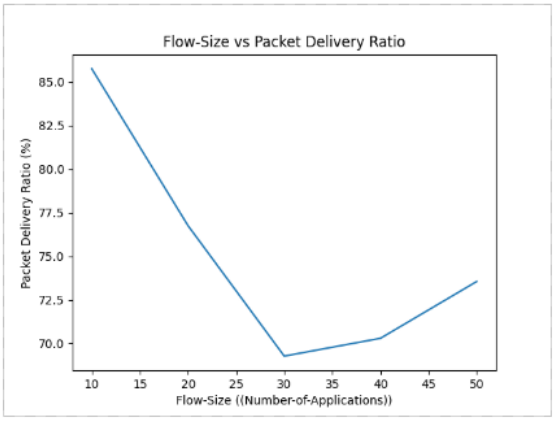
Observation on the change of Number of Nodes:

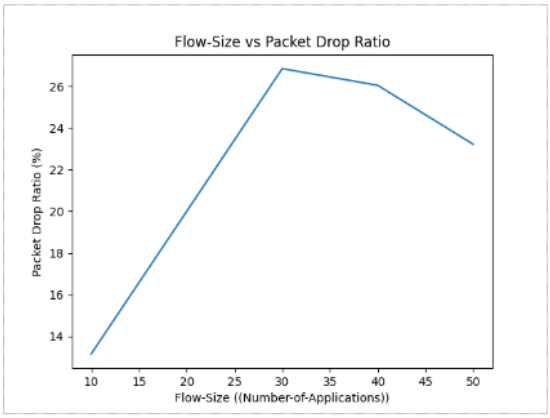
As area size remain fixed the increase of node in the network increases average number of neighbors for each node. If number of neighbors increases the network gets flooded exponentially more as new RREQ enters the network by AODV protocol. This fact is present in all 4 plots that we have got here. As number of nodes increases, throughtput decreases drasticlly because when node number are high network is mostly busy sending RREQ packets to each other which also causes high packet drop because TCP layer faces serious congestion due to so much RREQ packets on the network.

An interesting phenomena can be observed in case of end to end delay as the curve changes the direction which actually represents the exhaustion because after the peak total number of data packet sent decreases so much that only few packet can be transferred from source to destination which are very nearby. Any packet that needs more hop gets dropped hence delay is less but network wastes due to RREQ packets is nearly 95%.









Observation on the change of Number of Flows:

The main observation of this simulation is that with increasing flow the throughtput is increasing. Its because TCP layer is always ready with packet to send and AODV is capable of using cached route if route is unchanged. So with increase with packet and AODV cost remianing the same as it is, throughput is increasing. End to end delay is rising because with increasing flow average queue waiting time is increasing which results in high average end to end delay. Lastly delivary rate at first rise with the increasing of flow number as the network was under utilized but after a while when the network gets saturated after introducing more flow, the drop rate has no other option but to increase as system is saturated and not capable of meeting the high demand of TCP-Application layer.

Conclusion:

In this simulation assignment we assigned flow randomly which most of the time created result that doesn't reflect with usual scenario. We tried to generate more than one simulation result using same input parameters and picked the one that can be easily explained with our knowledge about the system. The plots were haviley influenced by AODV protocol as it has broadcast route request system which floods the network. But saddest part was I couldn't realize the impact of using 802.15.4 in the plots. The reason could be AODV was major bottleneck for the performance of the whole system, which is why we couldn't realize impact of other network layers and protocols much. Or I just failed to interpreate the right explaination behind the curve. Other than this case I think I now have a better understaing about different network layers and protocols.

Written by-
Raihan Rasheed Apurbo
S.ID: 1605062
Level 3 Term 2