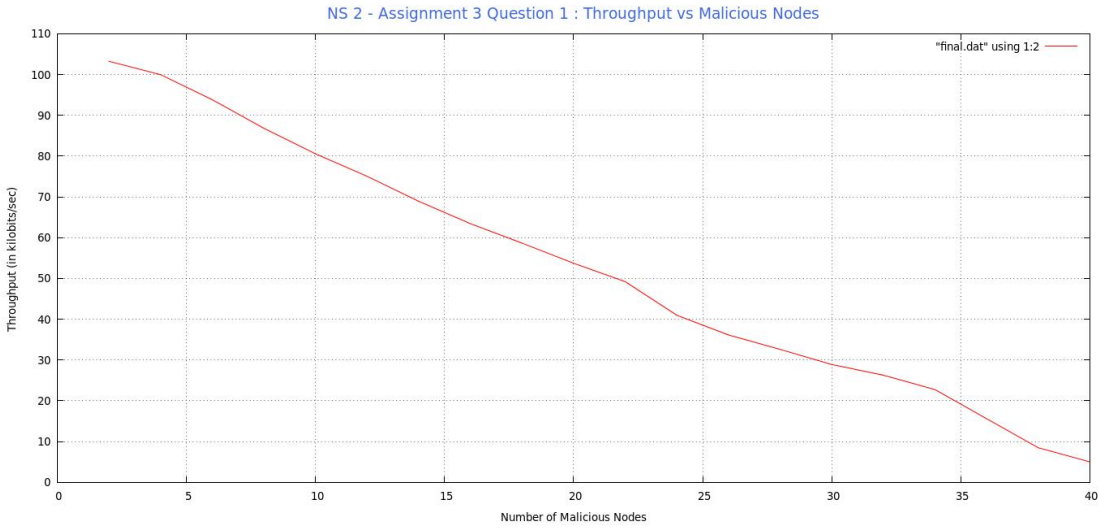
Question a)

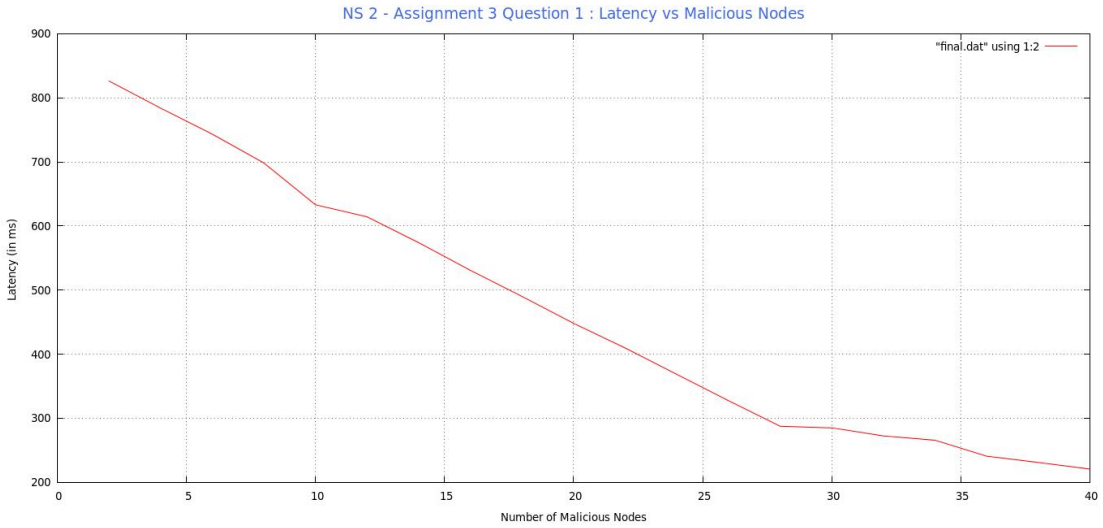
Implement the Packet Dropping Attack for AODV routing protocol and analyze the impact of the attack on overall performance for varying percentage of malicious nodes. Run the simulation for varying number of seeds (typically 1-100) and average the results obtained from simulations.

Answer :

Modifications were made to both the aodv.cc and aodv.h which included introducing an additional parameter called malicious make certain nodes malicious and thereby making the infected nodes drop packets as soon as they are routed to them. The screenshot of both throughput and latency vs the number of malicious nodes are shown below :



The simulation with varying number of malicious nodes and varying seed values (1-100) were run 20 times and are correspondingly plotted to obtain the given graph. As is observed and expected there is a sharp decline in the throughput as the number of malicious nodes increase. The malicious nodes act by dropping all packets when received thus fewer packets reach the destination. Thus the throughput decreases as the number of malicious nodes increase. As the malicious nodes increase the performance of the network drops.



This graph depicts Latency vs Number of malicious nodes. The simulation once again is run 20 times with varying seed values and varying number of malicious nodes. As we can observe, the latency is highest when the number of malicious nodes are minimal and the latency decreases as the number of malicious nodes increase.