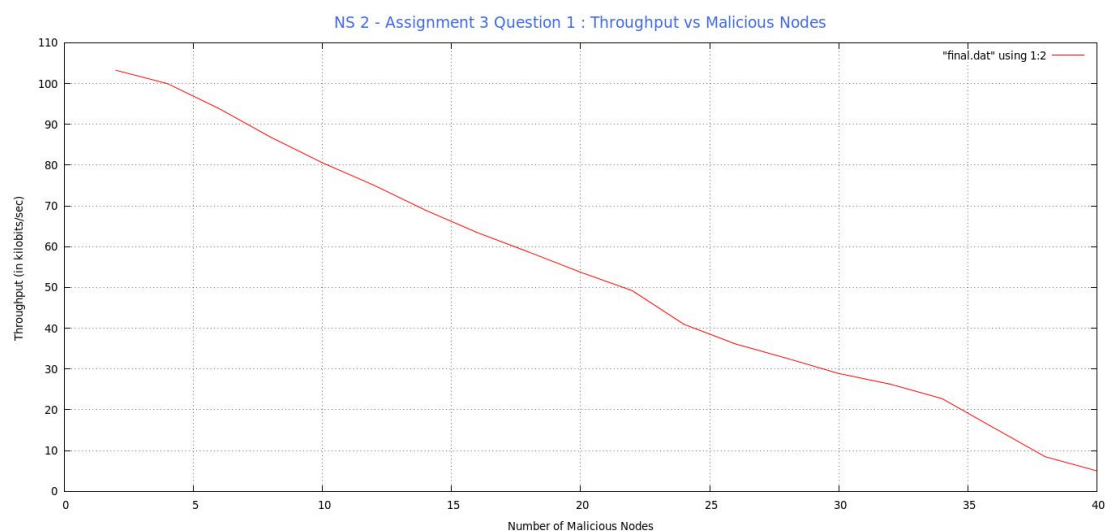


Question a)

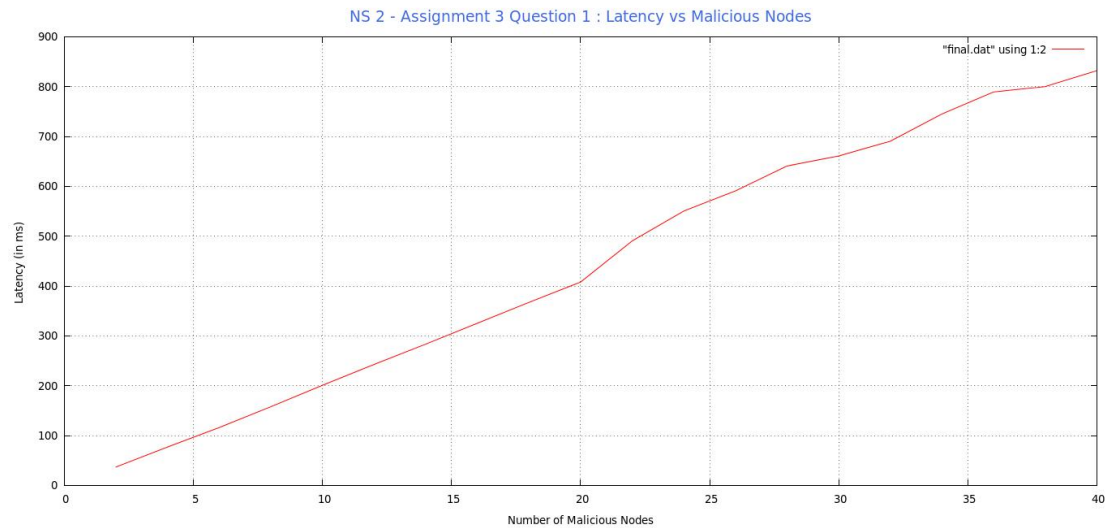
Implement the Packet Dropping Attack for AODV routing protocol and analyze the impact of the attack on overall performance for varying percentage of malicious nodes. Run the simulation for varying number of seeds (typically 1-100) and average the results obtained from simulations.

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. Once again the simulation was run for 20 times and the average for each iteration is calculated and is plotted against time. As one can observe, from the above graph it is clear that as the number of malicious nodes increase, the latency of the network goes up owing to the massive delay caused due to packet dropping of the malicious nodes. The higher the number of malicious nodes, the more the latency involved in packet transfer in the network.