Name of Student : Ashok A Kanthe

SUMMARY

Mobile ad-hoc networks (MANETs) have features like self organization, adaptation in changing enviornments and nodes in MANETs work as a router for routing packets. Each node has limited resources like bandwidth, battery power and storage capacity. MANETs are vulnerable to Denial of Service (DoS) attacks like black hole attack, gray hole attack, cooperative gray hole attack and packet drop attack. The goal of DoS attacks is to prevent the availability of network services from their legitimate users.

The black hole attack is a DoS attack where black hole node can attract all packets from neighboring nodes by pretending shortest route to the destination. The gray hole attack is a specialized variation of black hole attack where nodes switch their states from black hole to honest intermittently and vice versa. The cooperative gray hole attack has two phases. In first phase, the malicious node exploits the ad-hoc routing protocol to advertise itself as having valid route to a destination node, with the intention of intercepting packets. In the second phase, the attacker node drop the intercepted packets without forwarding them. These nodes are cooperating with each other. In a packet drop attack, packet dropper node drop the packets, but it is not attracting to the neighboring nodes to drop the packets.

This thesis investigates the mechanism against DoS attacks in MANETs and proposes different mechanisms against DoS attacks. Mechanism against gray hole attack is to detect gray hole node and to eliminate the normal nodes to enter in black list. The algorithm calculates peak value and checks whether the reply packet sequence number is lower than a threshold. The mechanism against gray hole attack improve the performance of MANET. The mechanism against cooperative gray hole is to detect two or more cooperative gray hole attacks and isolate them. The new packet has been introduced for the purpose of malicious announcing. Each node in the

path checks its next hop node for malicious activity. Channel overhearing technique is used to check the total packets send/forward by the next hop node. The mechanism against packet drop attack is to detect packet dropper, isolate it from the networks. Network performance is improved using mechanism against packet drop attack. In this mechanism, concept like trust list and direct reputation are used. Trusted list is local to every node maintained as a data structure in local RAM (Random Access Memory). Direct reputation method is using two counters, which present total forward packets and total dropped packets of the replying node.

The specific outcomes of this work are:

- Development of a mechanism against gray hole attack based on Ad-hoc On-demand Distance Vector (AODV) routing protocol and improves the performance of the network.
- Development of a mechanism against cooperative gray hole attack based on AODV and improves the performance of the network.
- Development of a mechanism against packet drop attack based on AODV which improves the performance of the network.
- Propagation models like two-ray ground, COST 231 and Okumura-Hata models are tested and compared based on AODV in different environment and scenario.

Keywords: Mobile ad-hoc networks, security, Denial of Service attacks, black hole attack, gray hole attack, cooperative gray hole attack, packet drop attack, AODV protocol, network layer