CHAPTER VII

CONCLUSION AND FURTHER SCOPE OF RESEARCH

CHAPTER VII

CONCLUSION AND FURTHER SCOPE OF RESEARCH

MANET routing protocol is vulnerable to a variety of attacks that can allow attackers to influence routes selected by a victim and launch denial-of-service attacks. In this thesis we have presented various security threats to reactive and proactive routing protocols. We have identified how vulnerabilities in the protocols can be exploited to launch attacks in the nework environment**.**

We have investigated the performance of the evaluating mobile ad-hoc network routing protocols on various scenarios. The metrics used for the inspection of these routing protocols are picked in such a manner so that they can take all the possible changes in the routing protocols and provide their uses on different varieties of scenarios. The result for stimulation shows that reactive routing protocols are better in most of the scenarios and situations in the MANETs in comparison to the proactive and hybrid routing protocols. The results also prove that the AODV routing protocols are considered as the best suited routing protocols for MANETs as they can adapt their phase according to the dynamic condition of network.

We have analyzed different types of security attacks on MANETs. Here we have considered the attacks like Wormhole attack, Black hole attack, Sybil attack and Gray hole attack with respect to AODV reactive routing protocol and OLSR proactive routing protocol. We have made a conclusion that the effect of the Black hole attack, Wormhole attack and Gray hole attack on AODV protocol is high as compared to OLSR protocol. We have also analyzed that when Sybil attack is present, the throughput of OLSR protocol gets more reduced in comparison to AODV protocol. So for using efficient routing, we have to consider all the security parameters for applying routing in MANET.

Our first proposal is WPT based on AODV for wormhole detection method, where AODV avoid overheads due to overhearing. This approach works equally well with the defined three classifications of a Wormhole attack. Two key points of this algorithm are 1) The Timer approach and 2) The Queue implementation. The working of the timer approach results in number of overheads which is the basic con in every approach. The queues work in FIFO manner. Thus, we store the node appearing order in it. This result in the identification of these Wormhole attacks and the illusion created by the wormhole nodes can easily be broken. A Threshold value, i.e., Wormhole Prevention Timer value is done in accordance to the mentioned formula. Thus, this algorithm works better with less number of overheads and also the time taken in the checking of a wormhole attack.

Our second proposed solution is a novel blackhole attack resistant method named as TBBM-AODV. We have presented an algorithm which deals specifically with the detection, prevention and reaction mechanisms of a black hole attack. This is a purely timer based algorithm whose time limit is also described. Another feature of this algorithm is buffer mechanism which is used here to store the data packets before they are transmitted. Further, we have categorized the detection of malicious node into three phases according to their occurrence in any network and the specific strategies they can encounter. A comparative study between attacking the network using which the minimum processing time will be consumed by the algorithm to detect illegitimate nodes using which the minimum processing time will be less dense then this algorithm can be used to find the optimum path from all possible ways to route data.

The countermeasures are light weight as they do not rely on the expensive cryptographic solutions. The methods discussed are resource efficient and well suited for use in MANET.

We also observed from previously proposed attacks when a Malicious node receives a packet from the source node by generating the route reply of high sequence number and a large amount of route request is generated which increases the amount of traffic in the network which alarms the network that a packet has been hijacked by the attacker, also when a malicious node tunnel the packet to other malicious node then the broadcast occurs which helps in identification of the malicious node and the attack.

We have proposed a novel attack model Collusion BW Hole Attack as each node sends the route reply to the source node so there is very less time gap between the reply of the Malicious node and the legitimate node and also the packet is not dropped by the malicious node at the beginning, after tunneling of the packet to other malicious node the unicast occurs which also keeps the malicious node safe from being detected and the packet is dropped somewhere near the destination node which assures the network that the packet transmission was going in the legitimate route so no detection technique works to detect this attack.

The presented research in this thesis can be taken further in many directions. Proposed countermeasures WPT-AODV and TBBM-AODV can be analyzed for their resistance to other attacks on AODV like on Gray hole attack and Sybil attacks. More work should be carried out on the detection and countermeasures for collusion BW hole attack so after colluding nature on any of malicious node researchers may be able to detect the effect of attacks on network. Additionally relation between Network mobility, threshold values and network size or Network density can be formalized so that the countermeasures can be fine tuned to accommodate different scenarios.