CHAPTER 6
SUMMARY OF THE RESULT FINDINGS

6.1 SUMMARY

In this research, different IDS mechanisms are proposed to mitigate the Blackhole attack. In the first method, a modified routing protocol called Enhanced OLSR (E-OLSR) is proposed, and it uses ABHA algorithm to detect and isolate the Blackhole node from the routing process. Once the Blackhole nodes are removed from the path between source and destination, the path becomes reliable as it contains only reliable nodes in it. Here thereby, the reliability of the network is maintained uptime throughout is maintained during the process of data transmission. As seen from the results the PDR is enhanced by 7%. Throughput is also improved by a value of 3%. End to End delay, considered a major factor of QoS secured a better performance. This scheme also improves the overall quality of service as the route is made optimal. The results infers that PDR, Throughput and End to End delay are improved in E-OLSR compared to normal OLSR.

In the second approach, sequence number based technique is used for the detection of Blackhole nodes. This method (Sn-BDM) provides improved results by isolating all the misbehaving nodes, using the comparison of sequence numbers, that is generated during transmission of data. The results obtained in MI table and Path detection table, clearly shows that the nodes with distinct sequence number are misbehaving, and need to be removed from the MANET environment. The results obtained in that Sn-BDM of PDR is 5% improvement compared with watchdog method, 7% better result compared with the 2hopAck.
approach. Throughput of the Sn-BDM approach is increased by 12% with the watchdog mechanism, and a 10% improvement with the 2hopAck approach.

Finally, the modified AODV protocol is implemented with the activation of promiscuous mode, since the misbehaving nodes are changed to normal ones with the activation of promiscuous mode. As, the normal AODV does not assure any mechanism to detect or isolate the misbehaving nodes from the network, the proposed mechanism is considered to be more efficient. The performance of this protocol is superior to normal AODV protocol. It completely outperforms all other existing schemes to isolate Blackhole attacks in MANET, by securing a 6% better result value for PDR with promiscuous mode than with non promiscuous mode by the AODV protocol. Also, Throughput shows a 10% improved performance with promiscuous mode than without the non promiscuous mode. End to End Delay also gives better performance with promiscuous mode than without the non promiscuous mode.

The contributions achieved by this thesis are

- During the literature review, this work discussed about the various Intrusion Detection system with attacks for Mobile Ad hoc Network environment.
- This work is investigated the Blackhole attack with single blackhole attack and also cooperative blackhole attack. The performance of the network is evaluated in the presence of Blackhole attack with the malicious nodes.
- This work carried out the detection of malicious nodes with some proposed mechanisms. Final proposed method isolates the malicious nodes in the network.
- Simulations are carried out to compare the performance of implemented routing protocol with the existing protocol and some mechanisms in the presence of malicious nodes.


6.2 FUTURE RESEARCH DIRECTIONS

In this thesis, effort has been made to improve the throughput and packet delivery ratio of the schemes employing the concept of intrusion detection system. There is scope for improvement in the following areas:

- As security is the core requirement for future commercial wireless network, steps may be taken to improve the security of current network scenario with cryptographic techniques and key management.
- There is a possibility to reduce the impact in the following attacks like gray hole attack, Sybil attack and worm hole attack in the mobile ad-hoc networks.