Chapter 8

CHAPTER 8

CONCLUSION AND SCOPE FOR FUTURE WORK

This chapter gives the conclusion and recommends the future enhancements of this thesis work toward to secure and protect hybrid routing to thwart sequential attacks in mobile ad-hoc networks. The review of entire work and conclusion with respect to the results and performance obtained for different protocols are given in this chapter.

8.1 CONCLUSION

The main objective of this research work is to is to protect the mobile ad-hoc network from distinct attacks. This work contains four phases: (i) Secure Route Discovery (ii)Attack Discovery based on Energy and Trust (iii) Distinct Attack Identification (iv) Protecting MANET's from distinct Attacks.

In the first phase of this work, developed a hybrid framework with secure neighbour discovery, node authentication using MECDHA and malicious node detection and isolation process. The hybrid framework is incorporated with the AODV protocol and changed as SRD-AODV. The proposed work achieves good attack detection rated and improves the packet delivery.

In the second phase of this work, black hole and grey hole attacks are identified and minimized energy consumption. Hence, the data packet dropping was mitigated and the routing overhead was reduced. To evaluate the effectiveness of the proposed protocol, it is compared to existing protocols through simulation for detecting black and gray-hole attacks. The evaluation is performed based on several performance metrics including end-to-end delay (EED), packet delivery ratio (PDR) and throughput.

In the third phase of this work, the SIIDAI protocol was developed to identify various types of attacks based on their SAP number. The proposed SIIDAI protocol offers protection against various types of malicious nodes in the network, resulting in reduced packet loss. As a result of the evaluation, it was found that the SIIDAI protocol outperforms the SRD-AODV and SRMAD-AODV protocols in terms of end-to-end delay, PDR and throughput, while providing better protection against malicious nodes.

In the fourth phase of this work the SIIDAI protocol with DPI used to prevent the packets from various attacks, the simulation results showed that the proposed SIIDAI protocol with DPI has an average end-to-end delay, PDR, and a highest throughput. In the final phase of this work, the proposed methodology protected packets from sequential attacks based on their DPI number. The SIIDAI protocol based on DPI number protected the MANET from six different attacks namely black-hole, grey-hole sink-hole, bogus, modification attacks and route fabrication.

8.2 SCOPE FOR FUTURE WORK

The work can be expanded in the future to examine the effectiveness of more intricate network scenarios. Under the influence of flooding attacks, more dense networks may be investigated, and learning-based algorithms can be used to carry out the detection of rogue nodes.

This plan can be altered as well to lessen the impact of outside attacks on the network. Future research may examine additional aspects of flooding attacks, such as hello flooding and data flooding, in order to create a comprehensive solution for protecting against all forms of flooding attack. For the purpose of evaluating devised methods to achieve robustness,

additional metrics such as routing overhead, packet drop rate, and the concept of energy efficiency may be investigated. Future developments could include expanding the suggested method to discover black holes in multihop and heterogeneous WSNs.