CHAPTER 7
CONCLUSION AND FUTURE WORK

In this thesis, a ticket based handoff authentication, homomorphic encryption and weight trusted routing (using SITO optimizer) mechanism have been exploited to detect and eliminate the malicious nodes involved during the handoff, message transmission and routing path formation. The proposed ticket based handoff authentication is an efficient technique in terms of authentication delay and secures authentication protocol which is centralized during handoff. The mesh client authenticates itself with its new mesh router by verifying its tickets generated by the Authentication Server. The experimental analysis and empirical study confirm that the proposed protocol outperforms ticket based handoff under different probabilistic scenarios of authentication delay and request delay and is resilient against various attacks. Further, for ensuring the data security during transmission, an algebraic encryption technique is proposed which ensures the security with reduced encryption/decryption time, processing delay and increased throughput. The key idea of the proposed technique is to generate the cipher text message using OR/XOR operations and transmit it with the private key generated by NTRU algorithm. In comparison with existing approaches, the proposed technique reduces the processing delay and encryption/decryption time for different file sizes. Further, the proposed technique is compared in terms of throughput. According to the experimental results, the proposed technique performs better in terms of throughput and processing delay with an efficient level of security. Moreover, the weight trusted routing mechanism for hierarchical mesh networks using Social Impact Theory Optimizer mechanism has been proposed. The proposed mechanism has significantly reduced the packet loss ratio in the presence of black hole and wormhole attacks. Hence, the weight trusted routing mechanism has enhanced the packet delivery ratio and reduced the route discovery, end-to-end delay and packet loss ratio in comparison of reported secure routing mechanism protocol.

The proposed mechanisms have significantly reduced the authentication delay, encryption/decryption time, packet loss ratio and end-to-end delay and have increased the packet delivery ratio and throughput percentage in presence of black hole, worm hole and falsification attacks over small and large network sizes under fixed and dynamic environments.
In order to validate the proposed mechanisms, a commercial NS2 simulator is used consisting of small and large network sizes. Further, the proposed mechanisms are validated by considering a smart home application that is based on mesh architecture. The provided results depict that the proposed mechanisms reaches up to a constant level of values against end-to-end delay, message delivery ratio and throughput percentage in comparison of reported protocols.

In further studies, the proposed algorithm will be tested under high packet flow and large number of attackers (by considering black hole and wormhole attacks) and then their results will be compared on various performances. However, the energy consumption in the large number of network sizes during the packet transmission/reception is a potential issue which will be reported in future communication. Moreover, each MC joining the network must be provided with a unique key by the AS in order to identify the MC for authentication.