CHAPTER 6

CONCLUSIONS AND FUTURE ENHANCEMENTS

6.1 CONCLUSIONS

In this thesis work, we have proposed three different approaches for optimal secure routing in WMNs. The first approach provides privacy protection and better security for optimal routing using security card model, combination of group signature and ID based encryption schemes and enhanced routing metrics. Under this approach, two routing protocols namely PBOR and UPSRM have been proposed. PBOR protocol provides anonymity and authentication by introducing security card model. It also provides better security against packet dropping and misdirecting attacks by incorporating neighbors passive acknowledgement mechanism during route discovery. PBOR also finds an optimal path for efficient data transmission using cross layer information exchange. The simulation results show that PBOR provides better packet delivery ratio and end to end delay than existing SIBR protocol.

However, none of the existing schemes including PBOR offers complete unobservability and unlinkability in infrastructure based WMNs. Hence, UPSRM has been designed to incorporate these properties in WMNs by applying group signature and ID based encryption schemes during route discovery. The analysis demonstrates that UPSRM not only provides strong privacy protection but also defends against attacks caused by packet dropping and misdirecting attacks. Similar to PBOR, UPSRM also finds an optimal path for efficient data transmission using cross layer information exchange.

The simulation results show that UPSRM has better performance in terms of packet delivery ratio in both malicious and non malicious environments than USOR.

The second approach is reputation maintenance for optimal secure routing. It has been designed using extended local monitoring mechanism and a new CLSL-DR mechanism along with security tag model. This approach is able to detect packet dropping and misdirecting attacks during route discovery. Under this approach two routing protocols namely SERPDA and TSRR have been proposed. Secure Efficient Routing scheme against Packet Dropping Attacks (SERPDA) has been designed to address two severe packet dropping attacks namely misrouting attack and power control attack by implementing the extended local monitoring mechanism. Moreover it improves the performance by implementing enhanced routing metrics during route discovery. A comparison of SERPDA with AODV and SADEC protocols is done using NS2 simulator. SERPDA provides better performance than AODV by choosing the optimal path and it gives slight increase in delay compared to SADEC due to the routing metrics enhancement.

Trust based Secured Reliable Routing (TSRR) protocol has been proposed to provide complete reliable routing path and to have more security against adversaries. This protocol discovers reliable routing paths by considering trusted nodes with forwarding reliability during route discovery. The proposed protocol protects the network against packet dropping and misdirecting attacks by implementing a new Cross Layer and Subject Logic based Dynamic Reputation mechanism (CLSL-DR) and security tag model in mesh routers. Comparison shows that the proposed protocol provides better performance in terms of PDR, routing overhead and end-to-end delay than SAODV. Performance and security analysis show that the proposed protocol

is efficient and is able to defend various packet dropping attacks such as Sybil, sink hole and hello flood attacks.

The third mechanism is effective QoS provisioning for optimal routing. This mechanism provides better reconfiguration plans to support QoS demands and also provides better solution for local link failures in WMN. Under this approach, Efficient Routing with QoS Aware Reconfiguration (ER-QAR) protocol has been proposed to support QoS for real time applications. The proposed scheme ER-QAR combines Self Reconfiguration System (SRS) with an enhanced AODV to autonomously reconfigure local network settings for recovery from link failures. SRS helps to perform localized configuration changes by providing better reconfiguration plans that satisfy the applications' QoS requirements. This protocol determines an optimal route by making use of the hybrid routing metrics, WCETT, ETT, ETX, Path cost and hop count. The simulation results show that the proposed scheme performs better than AODV in terms of throughput, PDR and end-to-end delay.

Thus we have provided holistic approaches for optimal secure routing in infrastructure based wireless mesh networks by considering privacy, security and performance metrics.

6.2 FUTURE ENHANCEMENTS

The work can further be enhanced in the following ways. Firstly, the mechanisms of this work can be tested in WMN test bed environments so that the pros and cons of the mechanisms are identified clearly. Based on those observations, it is possible to enhance the mechanisms further. Secondly the mechanisms may be applied to hybrid and mobile WMN environment which will pose the need for additional functionalities and challenges. Our future work also goes in the direction of providing an anonymous

authentication mechanism and designing secured key distribution mechanism within the backbone of hybrid WMN environments. Also, we are planning to test the proposed approaches when number of mesh clients is increased. The proposed thesis work has addressed packet dropping and misdirecting attacks by means of enhanced routing metrics and reputation mechanisms. The work can be extended and analyzed further to address other DoS attacks like packet modification attacks, resource consumption attacks in infrastructure based WMNs. Hence, further enhancements can be incorporated in the proposed mechanisms to suit hybrid and mobile WMN environment based applications. Another possible enhancement is designing a novel reputation mechanism with different concepts such as Fuzzy logic, Bayesian theorem, etc. to well isolate the malicious nodes in WMNs.