CHAPTER 7
CONCLUSION AND FUTURE ENHANCEMENT

7.1 CONCLUSION

In a mobile ad hoc network, energy and security are the important factors to evaluate the performance of the network. The protocol named as cooperative communication performs efficient broadcasting, and it provides full coverage of a network. Efficient Power Aware Routing (EPAR) produces less energy consumption than COSPNCR and CCSPR in $24 \times 10^{-3}J$. The energy saving is compared to 50% and also the delay value is 15%. An efficient medium access protocol to optimize spectral reuse and maximize channel utilization has been developed. Throughput can be increased by 15% more than the other method. Packet transmission rate and detection rate can be increased. The proposed relay selection schemes for a network consist of an ST, an SD and multiple SRs communicating in the presence of an eavesdropper. It examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and the reliability of secondary transmissions are characterized in terms of their IP and OP respectively.

Moreover, the SRT performance of MRS is better than that of SRS. Additionally, as the number of SRs increases, the SRTs of both the SRS and of the MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and the reliability of secondary transmissions. An opportunistic relay node is adopted for forwarding the
confidential information and the other relay nodes to send the artificial jamming for confusing the eavesdroppers. The impact of outdated CSIs to the relay selection and the achievable ESR is investigated. Incremental relay selection provides continuous transmission. Jammers can protect the data efficiently even when the eavesdroppers are more than relay nodes. Packet-dropping attack has always been a major threat to the security in MANETs. A novel IDS named EASACK protocol especially for MANETs is proposed and compared against the existing system in different scenarios through simulation. This scheme prevents the attackers from initiating forged acknowledgement attacks. Hence to prevent the attackers, digital signature technique is adopted in this scheme. DSA is chosen because it always produces slightly less network overhead than RSA. Although digital signature generates more routing overheads in some cases, it can vastly improve the network’s PDR when the attackers forget acknowledgment packets.

7.2 FUTURE ENHANCEMENT OF THE RESEARCH

- Energy consumption of every node should be monitored by other techniques.
- Full coverage can be done by using other methods.
- This security framework can also be extended to other kinds of security attack based on different applications.
- Noise detection and deduction, interference reduction with different traffic loads.