6.1. CONCLUSIONS

The present study analyzes the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range). Two detection models are considered: single-sensing detection and multiple sensing detection models. The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios.

Moreover, we consider the network connectivity and the broadcast reach ability in a heterogeneous WSN. Our simulation results verify the correctness of the proposed analytical model. This work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application requirements.

We have seen that WSNs have special vulnerabilities that do not exist in wire-line networks. We cannot, therefore, simply transfer all our protocols for wire-line networks to WSNs. Protocols must be designed with low computational power and low energy requirements in mind. In this present study we have seen some of the protocols that are used, as well as some ways to determine
where to check packets, in which we saw that by allowing the attack to have some utility, we are able to increase ours through energy saving for sufficiently large, resource constrained networks.

We have dealt with the neighbor based intrusion detection technique. In order to design generic IDS capable of revealing several types of attacks at a time, symptoms and statistics have to be defined for these attacks. This work provides a study of several attacks which can be conducted in WSNs and describes possible statistics which can be used to reveal them. It is pointed out that only some of them are appropriate for the neighbor based detection technique.

A neighbor based IDS were designed implemented and evaluated in the thesis. It was programmed to detect different types of jammers, hello flood and selective forwarding attackers. It was shown that detection in aggregation protocol operating networks provides very good and stable detection results. The IDS was able to reveal all of the attackers in every single simulation producing no false positives or false negatives except for the case of the hello flood attack.

Furthermore, we were able to enhance the IDS to be able to detect mentioned attackers in networks with the CTP as well. We described how the clustering method can be used in order to achieve this. By employing it, we decreased the number of false positives and false negatives almost to 0 in case of the detection of
a deceptive jammer. The IDS was never able to reveal all of the random jammers deployed in the network.

The IDS comes in several modifications - stand-alone, 1-hop and 2-hop collaboration. Collaboration can be used in order to refine the statistics gathered by the IDS agent. It can also be used when the IDS is deployed in a sparse network where the number of monitored nodes by a single IDS agent is too low. IDS agents share their knowledge of their neighborhoods.

6.2. FUTURE SCOPE

Our Future enhancements are intrusion detections in internet application and parallel computer interconnection network.