CHAPTER 5. CONCLUSION

CONCLUSION AND FUTURE WORK

The concept of proposed engine in this thesis will work as system model on NIC and provide secure channel when node communicates to each other which is describe in chapter four. MANETs are susceptible to a variety of attacks which focuses on the protocols of the network layer (layer 3) & data-link layers (layer 2). In the forthcoming days, a large number of detection engines have been proposed for Mobile ad hoc networks however the majority of all present a number of boundary & weaknesses. So, the existing detection engines meant for MANETs have only focused on monitoring the (layer 3) i.e. network layer & capable of detecting routing attacks. The designed engine aims to deploy the range of attacks and address these limitations detected by FSM detection engines. So it introduces a number of significant advantages since it can effectively detect all attacks in real time and without any communication overhead, it is resilient to the dynamic topologies that are common in Mobile ad hoc networks & its deployment.

The design of the engine can be further expand in future with order to

- Detect & activate all the attacks that target the critical protocols employed at the data link layer, Network layer and transport layer of MANETs.
- Regarding hardware failures & different type of attacks, where the detection engine will be provided with a more resilient FSM design architecture in order to alleviate the need of operating a detection engine at each single network node. The design of FSM will evaluate in the contest of following steps.
  - To provide better detection accuracy.
  - Capability of detecting more attacks at Network & Data link layers.
  - False positives Rate.
MANETs present different threats due to difficult properties. These are open up very security risk from conventional wired network, and each of them how security is provided and maintained. Due to mobility and dynamic nature of mobile ad hoc network nodes, link breaks are likely to be common. So the network layer, in which routing take place, is vitally focused on MANET. The attacks other than these are beyond the scope of this model. In this paper, we have faced various attacks in mobile ad hoc network and working of routing protocols that can resist various attacks using advance secure routing model.

Our proposed model resist the malicious behavior by node in network and NBAC protocol protect the blocking of the multiple node at a time. The malicious behavior is identifying by finite state machine (FSM) and their function in proposed model which is explained in chapter 3. The other proposed model designed for protect a single node blocking if problem arise in network. So this model presented in thesis provide better solution for multi-hop network in mobile ad-hoc network