ABSTRACT

Mobile Ad hoc Network (MANET) being a new paradigm of wireless networks offers an unrestricted mobility even in the absence of centralized infrastructure like mobile switching centers or base stations. In addition, it is an autonomous Multi-hop network that comprises a self organizing set of mobile nodes connected by an unreliable open access radio channels. Often the nodes perform a dual role as a host and a router as well. Owing to their flexibility, ease of application, ability of reconfiguration and speedy deployability, the MANETs are attracting more preferability and significance. Be it a war zone, recovery from a natural calamity or medical services of urgent nature, this type of network, enveloping all the aforesaid aspects, can be most suitably accessed.

However the security, responsive applications of MANET necessitates an extreme level of security, but on the flip side, they are inherently susceptible to multiple attacks, because of the factors like unreliable open access wireless links, dynamically changing topology, restricted battery power, lack of centralized control and the likes. Therefore, it becomes very much necessary to pay more attention to the security issues of the MANETs.

To date, most of the research has focused on performance and services with security being given a lower priority and in most of the cases, considered as an add-on afterthought technology rather than a design feature. Even though such type of approach may be suitable

for networks with predictable faults, but it is not appropriate for error prone and unpredictable Ad hoc Networks. The inbuilt characteristics of MANET give rise to a greater susceptibility to extensively varied attacks such as flooding, blackhole, spoofing, wormhole, eavesdropping etc.

Nevertheless a lot of research, as it is observed nowadays, is being focused on this field, the existing secure routing solutions such as Source Routing Protocol (SRP), Secure Efficient Ad hoc Distance Vector (SEAD), Secure Ad hoc On-demand Distance Vector (SAODV), Secure Ad hoc Routing (SAR), Authenticate Routing Ad hoc Network (ARAN) Routing Protocols etc have not reached the satisfactory level in respect of effective and precise routing security. In case of resource constrained MANETs these are ineffective, or they posses ability to deal with the single malicious node and remain ineffective in case of multiple attacks. In this thesis three secure routing protocols, namely GTASA, SEA and ECCEA are proposed as extensions to the traditional on demand AODV routing protocol to compete with blackhole attacks which are most likely to occur in MANETs. The former two new secure routing protocols are designed based on the anomaly intrusion detection system approach and the later is designed based on the elliptic curve digital signature approach. The new protocols are implemented using the most popular event driven NS2 network simulator in order to verify their performance in the presence of blackhole attacks in different MANET scenarios. The Quality of Service parameters like Packet Delivery Ratio, Throughput, Average End to

End Delay and Normalized Routing Load are used to analyze the simulation results thus making the comparison with conventional AODV routing protocol. Our simulation results indicate that the proposed protocols outperform the AODV protocol in MANETs in the wake of blackhole attacks.

Key words: Flooding, Blackhole, Spoofing, Wormhole, Eavesdropping, Quality of Service, Throughput.