Chapter – 7

SUMMARY, CONCLUSION AND FUTURE SCOPE

CHAPTER -7

Chapter - 1. DISCUSSION OF RESULTS

CHAPTER -7

SUMMARY, CONCLUSION AND FUTURE SCOPE

7.1. BRIEF SUMMARY OF RESULTS

Based on the simulation results it can be analyzed that the performance of the AODV routing protocol is drastically reduced in the presence of blackhole nodes. Since the AODV routing protocol was designed primarily only to route the packets without considering the security aspects of the network. So the traditional AODV protocol is completely helpless to compete with blackhole attack. Taking this as the advantage the blackhole nodes tries to exploit the AODV routing protocol and reduces its performance to the maximum extent. The same thing one can witness from the simulation results. During this investigation, with an objective to overcome the limitations of AODV protocol, three security extensions for it with the names GTASA, SEA and ECCEA are proposed with different techniques to compete with blackhole attacks. The analysis of simulation results shows that the new protocols are successful to the different extents in defending the blackhole attack.

The IDS based GTASA and SEA provides almost the same performance and succeeds in improving PDR in different MANET environments from 15 to 35% and 20 to 40% and the elliptic curve cryptography based ECCEA betters it to 76 and 80% in the presence of 1 and 3 blackhole nodes respectively against the traditional AODV routing protocol. The throughput of the network also increases by around 100% with GTASA and SEA and 400% with ECCEA in the presence of both 1 and 3 blackhole nodes as compared to the AODV protocol. The simulation results also illustrate that the new protocols produce improved results when compared to the AODV protocol in terms of the QoS parameters normalized routing load and average end to end delay. But unfortunately the overall routing load increases with new protocols as compared to normal AODV protocol. However, it is worth enough to make a point here that the routing load per received packet, i.e. normalized routing load is decreased with the proposed routing protocols.

On the overall the simulation results proved that new protocols GTASA, SEA and ECCEA outperforms the conventional AODV protocol in terms of all QoS parameters under different network scenarios in the presence of blackhole attacks. For detailed report one can go through the simulation results and respective graphs. The proposed IDS security schemes overcome the problem of the cooperative blackhole effect as compared to the existing REAct security scheme.

The authentication based ECCEA combines the features of symmetric and asymmetric cryptography approaches, hence it reduces the computational overhead as compared to the existing cryptography based security schemes. For instance 256-bit key length of ECCEA provides a security level equivalent to a key length of 3072 bits of existing RSA public key based schemes. This feature is very important and much suitable for MANETs as it is comprised of mobile devices which are naturally limited in terms of their processing power, energy, and bandwidth. The ECCEA is also successful to produce a PDR of 80% by countering the blackhole attacks which is much more than the existing SAR protocol. The lower Normalized routing load is another advantage of the proposed GTASA, SEA and ECCEA protocol as compared to the existing security schemes.

7.2. CONCLUSION

The proposed security extensions GTASA, SEA and ECCEA are the security enhancements of AODV protocol. The first two are based on intrusion detection system and the last one was based on the elliptic curve cryptographic approach. The proposed protocols are simulated in NS2 and their results are analyzed using the QoS parameters PDR, Throughput, AEED and NRL and finally compared their performance with the traditional AODV protocol. The simulation results proved that the proposed protocols outperform the AODV protocol in all aspects in the attack scenarios. For in depth analysis one can go through the results analysis and discussion section.

7.3. FUTURE SCOPE

As the present work is limited to only the blackhole attacks, in the further investigation one shall consider other attacks such as wormholes, grayholes etc. The present investigation is carried out only based on the Random Way Point mobility model, so the investigation can be extended to other random mobility models. The present investigation can also be extended to other existing Mobile Ad hoc Network routing protocols such as Dynamic Source Routing, Optimized Link State Routing etc. While implementing ECCEA, the elliptic curves are defined over the finite field of prime numbers. The elliptic curves can also be defined over the fine field of binary numbers. As a future scope, the researchers shall consider the later in the implementation of new secure routing protocols.