

PREFACE

MANET is an infrastructure less network that offers unrestricted mobility and quick deployability. Furthermore, it is an autonomous multi-hop network in which set of self organizing mobile nodes connected by an open access radio channel is free to move randomly and performs the dual role as a host and a router as well. The MANETs are finding more likely importance due to the flexibility, ease and speed with which these networks can be deployed as well as reconfigured. However the security sensitive applications of MANETs require a high degree of security, but on the flip side, they are inherently vulnerable 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 is necessary to pay utmost attention to the security issues of the MANETs. In view of the fact and factors as mentioned earlier the three secure routing protocols, namely GTASA, SEA and ECCEA are proposed as an extension to the traditional one that is on demand AODV protocol to compete with blackhole attacks which are more likely to occur in the MANETs.

The work related to the new protocol GTASA has been published in International Journal of Advances in Engineering & Technology (IJAET) entitled, "Defending blackhole attacks in mobile ad hoc networks using non-zero game theory" bearing Vol. 6, Issue 4, pp. 1653-1663, Sept. 2013, ISSN: 22311963. Pertaining to the proposed SEA protocol the relevant details can be further referred by way of the

source, i.e. International Journal of Research in Computer and Communication Technology, Vol 2, Issue 8, August -2013, ISSN 2278-5841 under the title “Intrusion Detection Enabled Mobile Ad hoc Networks to counter Blackhole and Grayhole Attacks”. As far as the proposed protocol ECCEA is concerned, further detail can be accessed from the source, i.e. International Journal of Research in Computer and Communication Technology, Vol 3, Issue 3, March- 2014, ISSN 2278- 5841 under the title “Efficient Lightweight Hybrid Cryptography Solution to Secure Mobile Ad hoc Networks”.

On the overall the experimental results of the investigation indicate that the newly proposed protocols GTASA, SEA and ECCEA outperform the conventional AODV routing protocol in terms of all QoS parameters under different network scenarios in the wake of blackhole attacks. For detailed analytical report one can go through the simulation results and respective graphs.