ABSTRACT

The main objective of the research is to design a security model to protect MANETs from single node and colluding node Byzantine attacks with minimal energy utilization. Mobile ad hoc networks are autonomous spontaneous networks of mobile nodes communicate with radio system. MANETs are used in applications ranging from crucial to commercial and military to medical. Few applications of MANETs are in medical field, military field, and disaster recovery, wild life study, predicting natural calamities, education systems, health care, transportation systems and robotics. Most of the applications using MANETs are security sensitive applications.

MANETS are vulnerable to attackers and Byzantine attacks are the most harmful and hazardous one among the active attacks. Byzantine attacks are the major potential threats that shatter the proper functioning of the system. Byzantine attacks are active insider multilayer attacks and they are carried out by the authenticated nodes aware of system functions. The malicious nodes can execute attacks as single handed or by colluding with other attackers. In network layer, these attackers destruct the data transmission phase and in MAC layer it affects distributed coordination function DCF and jams the RTS, CTS and ACK signals. These nodes also reduce its normal back off time and access the channel frequently to prevent the bandwidth usage of benign nodes.

In spite of tremendous research carried out in the security domain of networks, still it exists as an ever green field for new findings. The security needs in certain area remains unsatisfied. One such area is Byzantine Attacks.
The intensity of damage caused is high and necessary detection and preventive measures should be carried out to retain the reliability of system. Lot of research is done in this area of security but all of them deal with securing at any one part or specific layer especially the routing and communication protocols of networks. No work has been carried out so far to secure the system from Byzantine attackers at the other layers of network.

This work presents a triple layered protection and detection mechanism with cross layer feedback to block the Byzantine attacks. Nodes behavior from the point of joining into the network is monitored and measured against a trust factor at each layer. Aggregate performance in the form of weighted Laplacian or Kirchhoff matrix resembling reliability of nodes is transferred between the layers as a feedback. The affected system can be recovered quickly even if the attackers partition the network into many components. Prediction is done well in advance before the attackers succeed in their intention and proactive remedial actions are taken to retain the system performance and reliability. Reliable detection, recovery and routing scheme based on cryptosystems, message dispersion with forward error recovery along with cross layer feedback protect the system completely from Byzantine attacks.

Simulated results depict an improved performance with high number of successful delivery of message with normal delay. Numerical analysis of mathematical model proves the accuracy of predicting the network condition. The simple interaction between MAC, network and transport layer enriches all network activities. This cross layer feedback model results in improved security, less consumption of energy, reduced delay, efficient routing, reliable message transmission and better network management. The proposed design also suits for distributed systems.