ABSTRACT

In the day-to-day life, the requirement for applying an Adhoc network contributes more when a crisis circumstance emerges. It is very useful for military application when there is confidential information to be shared among group of soldiers without any impediment. Hence, there is a need for secured and authenticated technique or system to disseminate the confidential information. Security is required in all the places where there is a request to deliver the information to the authenticated destination. A technique named as Fault Tolerant Petri Net (FTPN) using Hybrid Cluster Stable Link Routing (HCSLR) protocol is proposed to ensure the security and authentication compared to existing methods. Different Mobile Adhoc Network (MANET) routing protocols are examined to know the working strategy in Mobile Adhoc Network with their working nature, upsides and downsides together with the essential characteristics such as security, authentication and energy efficiency.

Hybrid Cluster Stable Link Routing (HCSLR) protocol is proposed to disseminate the secured messages to attain the correct balance between overhead and end to end delay. It is observed that overhead is decreased with the assistance of link expiration time and evacuating repetitive rebroadcast messages. In HCSLR arrangements, a better stability has been accomplished with less overhead towards a definitive objective of cluster routing scheme. Though the scheme is more desirable for enhancing the security by reducing the control overhead and delay, it does not maintain the fault tolerance level and authentication rate within the substantial limit. The limitation is overcome by introducing Cross Layer enhanced Secure Routing Scheme (CLSRS). In CLSRS, cross layer is deployed to increase the network lifetime and network performance using trust threshold value derived from signal strength and residual energy level. Computerized signature generation and verification

method is also incorporated to authenticate packets as well as mobile agents. Fault tolerant rate is verified during the route maintenance phase.

The proposed methods and protocols are evaluated using Petri Net, a powerful simulation and modelling tool. Petri Net, a graphical and mathematical tool defines fault tolerant framework to effectively handle the faulty nodes so as to enhance the performance of Adhoc network. Fault Tolerant Petri Net is implemented by using HCSLR protocol to make sure that it outperforms other existing approaches. Also, a secured and authenticated protocol for MANET is proposed to disseminate the confidential information among mobile nodes. So, simulation is carried out in Network Simulator -2 for HCSLR and CLSRS protocols by comparing various existing technique. Proposed methods are simulated with respect to various parameters such as packet delivery ratio, packet delay ratio, throughput, bandwidth consumption, utility ratio and response time. Results obtained show that the explained protocols performed better than existing protocols.