NOTIFICATION:NO: 555/2024

NOTIFICATION DATE: 20/03/2024

STUDENT NAME : SHALINI SHARMA

SUPERVISOR: NAME: PROF. SYRD ZEESHAN HUSSAIN

TOPIC :TRUST BASED MODEL FOR A MOBILE AD- HOC NETWORK

DEPARTMENT: DEPARTMENT OF COMPUTER SCIENCE

FINDING

In this era of communication, wireless communication is on the boom with its capabilities of cost-efficient setup and flexibility of movement. Wireless communication, particularly in Mobile Adhoc Network, the nodes form adhoc network where topology and routes dynamically change repeatedly and rapidly. On contrary part wireless network have certain pitfalls. The major issue and concern in infrastructure less wireless network is lack of security mechanism. Adhoc network are prone to severe attacks since sensitive data is being transmitted over open shared medium.Secure routing protocol in MANET discovers the multi hop secured path between source and destination nodes. A highly reliable secure route is significant for improving the data delivery over the network.

The research work has addressed the security concern in Mobile Adhoc Network. The research work is carried out to design Trust Based Model that will detect any malfunctioning within network and choose reliable communication path that is reliable, optimal and energy efficient.

The first contributioncovers the study and shortcomings associatedwith watchdog, which isthe most popular intrusion detection system.It covers different scenario where watchdog fails and review the approaches that resolve the problems associated with watchdog.In addition, it covers the gaps in lined with those approaches.

As the second contribution, the thesis possessesdifferent types of secure routing mechanisms such as optimization based routing, and key encryption-based routing used in the MANET. Various secure routing utilized in the MANET are examined with its advantages, disadvantages along with its performance measures.

In the third contribution, the WCFOA-SVM model is proposed to design the trust model for attack detection and secure optimized routing. SVM is used to classify the malicious

users based on the residual energy, bandwidth, entropy, Packet Loss Ratio (PLR) and End to End Delay (EED). After classifying the malicious users, the information about these malicious users is broadcasted to achieve the reliable transmission. The WCFOA model is applied for link reliability measures and path selection. The developed WCFOA-SVM is used to overcome the issues of local optima trap and over fitting. The SVM based malicious attack detection with unique cost metrics is used to overcome the issue of over fitting. The incorporation of weighted coefficient in WC-FOA is used to enhance the exploration and exploitation capabilities that used to overcome the issue of local optima trap. The malicious nodesidentified by the SVM are avoided while discovering the route using WC-FOA that used to enhance the packet delivery of the network. The WCFOA method has higher efficiency than existing methods in terms of attack detection, energy consumption, packet delivery ratio, and throughput. The WCFOA-SVM model has 27J energy consumption and model has 96% malicious user detection.

In fourth contribution, a safe energy-efficient routing protocol addresses both the energy crisis as well as the security concerns. A successful routing approach is employed using the multi objective African vulture optimization calculations. The effective leaps for innovative routing are performed in MANET using the proposed ETA-MAVO method. The selection of CH and generation of routing path using ETA-MAVO increasingly involves the utilization of parameters related to fitness such as trust value, energy ratio, communication cost, the total number of gateway hops, and network load. The trust value obtained from ETA-MAVO is utilized for mitigating malicious attacks during the stage of data transmission. The results obtained from the comparative analysis show that ETA-MAVO attained high performance when compared with other existing methods.