ABSTRACT

Mobile Ad-hoc Network (MANET) is a group of wireless dynamic nodes without any infrastructure and centralized administration. As the environment is dynamic here, the communication among the multiple paths is a critical task. The routing protocols in MANET are relatively vulnerable to the connection failure as well as susceptible to malicious node attacks. Some issues related to security may arise due to the self-organization, decentralization, dynamic changing topology, lack of sufficient information about each nodes, free interruption of malicious nodes, power limitation, channel or bandwidth availability, and no security considerations in routing protocols. Also, the problem related to QoS involves node mobility, limited battery life, hidden terminal problem, unpredictable link properties, security, and route maintenance.

In the existing works, various security and path maintenance techniques are developed for providing a better communication in MANET. Even though they have some advantages like low energy consumption, increased computational performance, reduced complexity, and overhead, they have some limitations such as link failures, malicious node attacks, throughput, inaccuracy, delay, and less packet delivery ratio.

In this research, in order to improve the network performance in MANET, an attempt is made to develop a Heuristic-based link quality preservation algorithm for reliable data delivery and a secure link aware fault detection algorithm for allowing a secured and reliable data transmission.

In the first contribution, a Tabu list and Heuristic-based fitness search algorithm–based Link Quality Factor (THLQF) estimation is proposed to create the routing path and to update the path for the link failure analysis.

Here, four measures such as received signal strength indicator, bandwidth, node mobility, and the number of connections are used to evaluate the link quality. The Link Quality Factor (LQF) measurement considers the signal and noise level in 5 operating conditions to permit the automatic finding of closest neighbors and their location. The estimation of LQF and the dynamic update helps to provide minimum number of iterations with efficient delivery of packets.

In the second contribution, the security and privacy of packet transmission is preserved by establishing a Secure Link Aware Fault Detection (SLFD) mechanism. This technique is useful for permitting the data transmission in secure manner and allows a fault free communication in MANET. First, it discovers the neighbor and route for performing the communication by sending the HELLO packets and RREQ to the neighboring nodes that are within the range of less than 200 meter. Then the attack detection operation is executed by analyzing the activities of malicious nodes. In this technique, the dangerous attacks like black hole and grayhole are identified earlier and blocked them before the communication process begins. After that, the routes are enabled between trusted nodes and the path links are analyzed with the help of Tabu list and Heuristic-based fitness search algorithm-based Link Quality Factor (THLQF) estimation. Additionally, the secured data transmission is performed by producing the bogus key and by validating the authenticity of the nodes. Here, jitter is estimated for the discovery of compromised nodes within the path. The performances of both the proposed algorithms are compared with the existing techniques and the results demonstrate the improvement of the packet delivery ratio, throughput, link fault detection, and reduced packet loss rate, and latency.