ABSTRACT

The Wireless Sensor Network (WSN) has become an important field of research in Wireless Communication (WC). Nowadays, many real-time applications are using sensors due to their characteristics such as scalability, small size, lightweight, portable, etc. Several sensor nodes associated with WSNs are randomly dispersed in the surrounding environment with limited sensing, computing, and communication capabilities. All the units in the sensor nodes are low powered battery-operated devices. The energy associated with the batteries is finite and must be replaced when they run out, which raises the expense of maintenance. Self-organization and concurrent processing are the important characteristics of WSN. Once the transmission takes place, the energy gets depleted and the node replacement is impossible even if the single node dies which results in network failure. Energy consumption, network lifetime, and security are the major challenges faced by WSN. Maintaining a balance between energy consumption and network lifetime is always a challenging factor in WSN as both are inversely proportional to each other. Secured clustered routing techniques can be adopted to overcome this challenge.

The proposed work aims to provide a secured clustered routing protocol. This research work is divided into 3 stages namely clustering, routing, and security.

Clustering is the process of grouping sensor nodes and electing proper Cluster Heads (CHs) to avoid long distance communication to the base station, optimizing energy consumption and providing a better quality of service.

The first work is to form a proper cluster and select appropriate Cluster Heads (CHs) using a Genetic Algorithm (GA) and Algorithm for Cluster Establishment (ACE). Data transmission in WSN consumes more energy compared to processing. Long distance nodes consume more energy than nodes with short distance communication, so maintaining energy across the network is difficult due to limited energy resources. To prolong network lifetime and for energy efficient transmission, nodes with sufficient energy are required. In this work, an energy optimization algorithm based on GA overcomes this drawback and finds a suitable CH, which leads to cluster formation.

Routing is the process of finding the shortest distance between the nodes for transferring the data. Sometimes the data is lost during the transmission due to long

distance communication, node failure, and the presence of malicious nodes. Still, research is going on to overcome these challenges.

The second phase of work is to perform routing based on the demand and node behaviour. Routing protocols improve the network lifetime and establish the perfect communication between the nodes. Since node behaviour detection is important, this work mainly focuses on maintaining the connectivity between the nodes and increasing the network lifetime by incorporating two processes such as node behaviour analysis and on-demand secured data transmission. Detecting the node behaviour will monitor the transmission path for continuous message transmission to detect malicious nodes that block the path. Congestion occurs when selfish nodes interfere with overall communication. Nodal behaviour changes create network disruptions. Predicting node behaviour detects malicious nodes in the network. The main advantage in predicting node behaviour is to differentiate between malicious and selfish nodes. Since malicious node causes errors, they are removed from the network. The semi-Markov process predicts the node behaviour, which brings trust to the network, as this method can alter the node formation at the point of detecting malicious nodes and gain trust between the nodes.

In the third stage, a secured clustered-based routing protocol establishes a satisfactory path to transmit the data without any loss. An energy-efficient and secured routing protocol called Multi Criteria Based Secured Routing Protocol (MSRP) has been developed. Every node can interact with the server and other nodes. Every time, the control layer is responsible for performing additional processing and stops all network processes if a malicious node is suspected. Several methods have been put forward to increase security and energy efficiency. By the current system, if malicious nodes are engaged in the network, it consumes more energy and produces more unwanted data as well as threatening the data captured, thus increasing computational time and complexity. This MSRP model helps to reduce the unwanted communication and data loss. It also separates the malicious nodes from the network once they are identified.

In this research, clustering, routing, and security models have been implemented and compared with the existing protocols. In which, the proposed clustering algorithm based on ACE with GA performs better compared to LEACH protocol. The routing

technique based on node behaviour performs better than the existing Trust Management System (TMS) and Reliable Trustworthy Approach (RTA). The protocol for secured routing is based on the multiple criteria, and performed well compared with the ESMR (Energy Efficient and Secure Mobile node Re-authentication scheme), AODV (Ad-hoc On Demand Distance Vector Routing), and TSRF (Trust aware Secure Routing Framework) techniques.