ABSTRACT

At present, Wireless Sensor Networks (WSN) plays several roles and applications in many fields such as health monitoring application, traffic signal monitoring, weather reporting and forest fire and land slide detection. The sensors in WSN network senses the surrounding information and transfer this information to the central unit or sensor. All sensors in WSN environment are otherwise called as node and each node is having individual properties to transfer or receive the data. The central node or sensor is called as cluster head and all cluster head are tagged with sink in WSN environment. The individual node in WSN network senses the data and these data are transferred to its corresponding cluster head. The cluster head receives the data from individual node and send this information to the sink in WSN network. The node in network may be failed due to its low connectivity between adjacent nodes, or due to the low energy value in sensor node. This node failure interrupts the entire network performance by stopping the data transfer or reception through this particular node. Further, link failure will be occurred due to this node failure. Hence, detection of this particular failed node is important in WSN network.

Security issues are the primary issues in WSN due to its large network coverage and number of nodes. The attackers in WSN attack the particular node which has low energy level and converts this node into malicious node. The formation of malicious node is the primary reason for link failures between nodes. This research work proposes an efficient methodology to detect the malicious nodes in WSN using feed forward back propagation neural network classifier. This classifier differentiates the malicious node from trusty node based on the extracted features of the test node. The performance of the proposed malicious node detection system is

analyzed in terms of detection rate, Packet Delivery Ratio (PDR) and latency. The experimental results are compared with state-of-art methods.

The attackers in WSN attack the particular node which has low energy level and converts this node into malicious node. The formation of malicious node is the primary reason for link failures between nodes. In this research work, accumulation factor based link failure detection algorithm is proposed to detect the failure links due to malicious nodes in WSN network. This proposed algorithm determines the link failure nodes in both static and dynamic network environment. The performance of the proposed link failure detection algorithm is analyzed in terms of packet delivery ratio and latency.

The transmission and reception of data between nodes in wireless sensor networks are effectively improved by analyzing their links between nodes in WSN environment. In this chapter, the strength of the links between nodes is analyzed into strong or weak based on the extracted features from each node in WSN. These features are further trained and classified using Adaptive Neuro Fuzzy Inference System (ANFIS) classifier. This proposed system for link failure detection has the following stages as features extraction, feature vector construction and classification of links using ANFIS classifier. This proposed work classifies the link between nodes in WSN into either strong or weak based on the extracted features. The performance of the proposed link failure detection system is analyzed in terms of PDR, latency and detection rate, by varying number of malicious nodes in WSN environment.