ABSTRACT

Wireless Sensor Networks (WSN) are widely used in various industries but are vulnerable to cyber-attacks, especially virtual jamming. This attack disrupts communication between sensor nodes, causing data exchange issues. Machine learning algorithms, specifically K-Nearest Neighbors (KNN), can help overcome this attack. KNN can detect suspicious data patterns and adapt to environmental changes and various types of attacks. To evaluate the performance of the KNN model in detecting virtual jamming, this research applies the KNN model through simulation on NS-2, a network simulation application. The resulting dataset is then classified using a confusion matrix as an evaluation tool. KNN's simple reliability and high accuracy make it an effective choice for detecting and reducing the impact of virtual jamming attacks in WSNs.

Keywords: *wireless sensor network, virtual jamming, K-Nearest Neighbors (KNN), Network Simulator-2*