ABSTRACT

The adoption of information technology is the main key, Wireless Sensor Network (WSN) has emerged as a promising technology, especially in the context of the Internet of Things (IoT). This research explains that the use of WSN is an important element in supporting IoT development, providing energy efficiency benefits, and overcoming emerging obstacles. However, the use of wireless channels makes WSNs vulnerable to Denial of Service (DoS) attacks, especially virtual jamming attacks. These attacks can cause significant reductions in network throughput and capacity. Therefore, this research proposes an approach by combining machine learning and wireless networks, specifically using the Support Vector Machine (SVM) algorithm to detect and prevent virtual jamming attacks. SVM was chosen because it shows a high level of accuracy in classification. This research has a limited problem with a focus on the use of the SVM algorithm. The dataset generated using NS-2, which has been filtered and classified, is used to evaluate SVM performance. The SVM model in SVM scenario (2) shows the best performance with an accuracy of 76.60%, recall of 75.19%, precision of 81.06%, and F1 Score of 78.02%. These results confirm that the SVM method is effective in detecting virtual jamming attacks, with a random spatial distribution of nodes and a dataset that supports the validity of the analysis.

Keywords: *wireless sensor network, virtual jamming, support vector machine* (SVM)*, Network Simulator*-2.