ABSTRACT

In the era of Wireless Sensor Networks (WSN) and Internet of Things (IoT) technology development, security is a crucial aspect of protecting the network from various attacks, one of which is virtual jamming. This attack jeopardizes the performance of sensor networks with limited energy and resources. This research proposes the use of the Naive Bayes (NB) method as a solution to overcome virtual jamming attacks in WSNs. Based on previous research, NB is proven to have high accuracy in the context of network security. The NB method will be implemented through simulation using NS-2, an application for network activity analysis. The experiment plan includes using a confusion matrix as an evaluation tool, enabling the measurement of virtual jamming attack detection performance. The experiment aims to identify how NB can distinguish between attacks and normal activities in a network environment. In this research, it is expected to contribute to the development of security, by applying calculation speed, simple algorithms, and high accuracy, to the advantages of the NB method.

Keywords: Naive Bayes, virtual jamming, Wireless Sensor Network, NS-2