Abstract

The purpose of this research is to determine which machine learning model is the best for identifying routing attack based on accuracy and false alarm rate generated by each model. The dataset used in this research named WSN-DS, obtained from the Kaggle website. The dataset is the result of simulated attacks on Wireless Sensor Network (WSN) includes a Denial of Service Attack with Routing Attack types, including Grayhole Attack, Blackhole Attack, Flooding Attack, and Scheduling Attack. Routing attacks are often used by attackers for their personal purposes. The purpose of this attack is to cause the network system mechanism to be damaged and blocked so that the network system cannot be accessed by users. The machine learning models used in this research are Decision Tree (DT), Naive Bayes (NB), Support Vector Machine (SVM), and K-Nearest Neighbor (KNN). Therefore, this research uses various machine learning models to identify the accuracy value and false alarm rate value by splitting the dataset into 3 parts (training data, testing data, and validation data). The results of this research conclude that the machine learning model Decision Tree (DT) got the best results seen from the highest accuracy value (0.994), and the lowest false alarm rate value (0.002) compared to other machine learning models.

Keywords: ***intrusion detection, routing attack, machine learning, wireless sensor network, performance evaluation***