ABSTRACT

Rogue Access Point (RAP) detection is very important to avoid Evil Twin Attack (ETA) attacks in the campus environment, as is done at Telkom University, especially in the TULT building. This research aims to develop and test a Machine Learning (ML) model that is able to detect RAP based on data collected using airodump-ng. The data obtained includes various network parameters, such as Channel, Speed, Privacy, Cipher, Authentication, Power, and beacons.

The testing process begins with data collection using a TP-Link WN821N device and a Linux Ubuntu airodump-ng. The collected data was then saved in CSV format and uploaded to Firebase Realtime Database. This data is then processed using encoding techniques with the one-hot encoding method on categorical features, such as Privacy, Cipher, and Authentication. After that, the processed data is used to train the ML model using the Feedforward Neural Network (FNN) algorithm with sequential architecture.

The test results showed that the model experienced a significant increase in accuracy and a decrease in loss values. At some epochs, the loss value jumped and the accuracy dropped dramatically, indicating potential problems such as overfitting and underfitting. The model achieved the highest accuracy of 99.72% with a loss value of 0.04296. Quality of Service (QoS) testing was also conducted to measure throughput, delay, and packet loss in accessing the Firebase database and dashboard. The test results show that the average throughput is 12416.03 bits/second. The average delay was recorded at 0.18 seconds, with a variation between 0.12 to 0.29 seconds. No packet loss was detected in this test, with an average of 0.000%. This research shows that the ML model is effective in detecting RAPs and can be reliably applied in a wider network environment. The QoS test results show good network performance. This provides a solid foundation for further development and practical implementation in improving the security of wireless networks in campus environments.

Keywords : Rogue Access Point (RAP), Evil Twin Attack (ETA), Machine Learning (ML), Feedforward Neural Network (FNN), Quality of Service (QoS).