Perbandingan Algoritma Machine Learning untuk Deteksi Routing Attack pada Wireless Sensor Network

Azriel Farasfauzan Sepvira[1], Vera Suryani[2,] Aulia Arif Wardana[3]

[1,2,3,]Fakultas Informatika, Universitas Telkom, Bandung
[1]azrielsepvira@students.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]aulia.wardana@telkomuniversity.ac.id

Abstrak

Tujuan dari penelitian ini adalah untuk menentukan model machine learning mana yang terbaik untuk mengidentifikasi Routing Attack berdasarkan nilai akurasi dan nilai false alarm yang dihasilkan oleh masing-masing model. Dataset yang digunakan dalam penelitian ini bernama WSN-DS, yang diperoleh dari website Kaggle. Dataset tersebut merupakan hasil simulasi serangan pada Wireless Sensor Network (WSN) meliputi Denial of Service Attack dengan jenis Routing Attack, antara lain Grayhole Attack, Blackhole Attack, Flooding Attack, dan Scheduling Attack. Routing attack sering digunakan oleh penyerang untuk tujuan pribadinya. Tujuan dari serangan ini adalah untuk menyebabkan mekanisme sistem jaringan menjadi rusak dan terhambat sehingga sistem jaringan tidak dapat diakses oleh pengguna. Model machine learning yang digunakan dalam penelitian ini adalah Decision Tree (DT), Naive Bayes (NB), Support Vector Machine (SVM), dan K-Nearest Neighbor (KNN). Oleh karena itu, penelitian ini menggunakan berbagai model machine learning untuk mengidentifikasi nilai akurasi dan nilai false alarm rate dengan membagi dataset menjadi 3 bagian (data training, data testing, dan data validasi). Hasil dari penelitian ini menyimpulkan bahwa model machine learning Decision Tree (DT) mendapatkan hasil yang paling baik dilihat dari nilai akurasi yang paling tinggi (0.994), dan nilai false alarm rate yang paling rendah (0.002) dibandingkan dengan model machine learning yang lain.

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