Penentuan Posisi Interfering WiFi Access Point di Dalam Ruangan dengan Implementasi Model Klasifikasi Pembelajaran Mesin = Position Detection of Interfering WiFi Indoor Access Points with Machine Learning Classification Models

Ghulam Izzul Fuad, author

Abstrak

Teknologi lokalisasi dalam ruangan berkembang pesat karena keterbatasan GPS di lingkungan tertutup. WiFi fingerprinting menjadi solusi menjanjikan karena ketersediaannya yang luas dan biaya rendah. Penelitian ini bertujuan menentukan posisi access point ilegal di dalam ruangan menggunakan infrastruktur WiFi Aruba dan klasifikasi berbasis machine learning. Pendekatan ini melibatkan dua fase utama. Pertama, fase konstruksi fingerprint database di mana data kekuatan sinyal WiFi dikumpulkan dari berbagai lokasi di dalam ruangan dan disimpan dalam database. Kedua, fase klasifikasi berbasis machine learning yang menggunakan algoritma seperti K-Nearest Neighbor (KNN), Random Forest (RF), Extreme Gradient Boosting (XGBoost), dan Artificial Neural Network (ANN) untuk mengklasifikasikan lokasi access point ilegal berdasarkan fingerprint received strength signal (RSS). Model dievaluasi menggunakan metric accuracy dan f1-score. Hasil eksperimen menunjukkan bahwa untuk dataset NTUST, model yang paling sesuai adalah model dengan algoritma XGBoost dengan label jenis satu, tanpa augmentasi, dan dengan hyperparameter tuning yang memiliki skor accuracy sebesar 0.793 dan skor weighted average f1-score sebesar 0.792. Untuk dataset UI, model yang paling sesuai adalah model dengan algoritma XGBoost dengan label jenis satu, dengan augmentasi, dan tanpa hyperparameter tuning yang memiliki skor accuracy sebesar 0.591 dan skor weighted average f1-score sebesar 0.582.
.....Indoor localization technology is rapidly developing due to the limitations of GPS in enclosed environments. WiFi fingerprinting has become a promising solution due to its wide availability and low cost. This study aims to determine the position of illegal access points indoors using Aruba WiFi infrastructure and machine learning-based classification. This approach involves two main phases. First, the fingerprint database construction phase, where WiFi signal strength data is collected from various locations indoors and stored in a database. Second, the machine learning-based classification phase, which uses algorithms such as K-Nearest Neighbor (KNN), Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Artificial Neural Network (ANN) to classify the location of illegal access points based on received strength signal (RSS) fingerprints. The model is evaluated using accuracy and f1-score metrics. Experimental results show that for the NTUST dataset, the most suitable model is the one using the XGBoost algorithm with label type one, without augmentation, and with hyperparameter tuning, achieving an accuracy score of 0.793 and a weighted average f1-score of 0.792. For the UI dataset, the most suitable model is the one using the XGBoost algorithm with label type one, with augmentation, and without hyperparameter tuning, achieving an accuracy score of 0.591 and a weighted average f1-score of 0.582.