INTISARI

Pengembangan Purwarupa Alat *Packet Capture* dan Analisis Untuk Deteksi *Rogue Access Point*

Aditya Fadlil Achmad
21/473196/SV/18814

Penelitian ini mengembangkan purwarupa alat penangkap dan analisis paket berbasis ESP32 untuk mendeteksi *Rogue Access Point* (RAP) menggunakan pendekatan *Wi-Fi fingerprinting* dan *machine learning*. Sistem yang dirancang mampu melakukan pemindaian jaringan nirkabel, merekam data RSSI, SSID, BSSID, serta koordinat GPS untuk membentuk dataset geospasial. Data tersebut kemudian diolah menggunakan kombinasi algoritma *Random Forest Regression* untuk pemetaan sinyal dan DBSCAN untuk deteksi anomali lokasi. Pengujian menunjukkan purwarupa bekerja dengan baik, menghasilkan akurasi posisi rata-rata 11–12 meter dan tingkat ketepatan deteksi anomali mencapai 97,4% dengan *false positive rate* sebesar 2,6%. Hasil ini menunjukkan metode yang dikembangkan efektif dalam membedakan perangkat normal dan mencurigakan berbasis lokasi. Penelitian ini memberikan kontribusi dalam pengembangan sistem keamanan jaringan Wi-Fi yang adaptif, berbiaya rendah, dan dapat digunakan untuk audit keamanan maupun survei cakupan sinyal.

Kata kunci: ESP32, Wi-Fi, *Fingerprinting*, *Machine Learning*, *Random Forest Regression*, DBSCAN.

ABSTRACT

Development of Prototype Tool for Packet Capture and Analysis for the Purpose of Rogue Access Point Detection

Aditya Fadlil Achmad
21/473196/SV/18814

This study developed a prototype packet capture and analysis device based on the ESP32 microcontroller for detecting Rogue Access Points (RAP) using a Wi-Fi fingerprinting and machine learning approach. The designed system scans wireless networks, records RSSI, SSID, BSSID, and GPS coordinates to construct a geospatial dataset. The collected data were processed using a combination of Random Forest Regression for signal mapping and DBSCAN for anomaly detection. Experimental results show that the prototype performed effectively, achieving an average positioning accuracy of 11–12 meters and an anomaly detection precision of 97.4% with a 2.6% false positive rate. These findings demonstrate that the proposed method can accurately distinguish between normal and suspicious access points based on location data. The research contributes to the development of adaptive, low-cost Wi-Fi security systems suitable for network auditing and signal coverage surveys.

Keywords: ESP32, Wi-Fi, Fingerprinting, Machine Learning, Random Forest Regression, DBSCAN