e-XXXX-XXXX

Original Article

Pengujian Keamanan Jaringan Wireless terhadap Serangan Rogue Access Point

Musdalifah Hasan [1]✉, Muh. Raihan [2], Rakhmadi Rahman[3]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: musdalifahhasan891@gmail.com, rhnt123.id@gmail.com , rakhmadi.rahman@ith.ac.id

Abstrak:

Keamanan Wireless Local Area Network (WLAN) menghadapi ancaman serius dari Rogue Access Point (RAP), yang memungkinkan serangan Man-in-the-Middle (MITM) untuk mencuri data sensitif. Penelitian ini mengintegrasikan berbagai metodologi untuk mendeteksi dan memitigasi RAP. Metode yang digunakan meliputi sistem deteksi berbasis mikrokontroler Wemos D1, penerapan arsitektur Multi-Agent (Master dan Slave Agent), serta vulnerability assessment menggunakan tool open-source seperti Kismet dan Airodump-ng. Hasil analisis menunjukkan bahwa penggunaan metode Multi-Agent mampu memperluas jangkauan deteksi melalui titik-titik staf, sementara vulnerability assessment dengan skor CVSS (rata-rata 7,58) membantu memprioritaskan penanganan pada titik akses yang kritis. Mitigasi otomatis berupa paket deauthentication terbukti efektif memutus hubungan klien dari AP ilegal secara real-time.

Keywords: Rogue Access Point, Multi-Agent, Vulnerability Assessment, CVSS, Keamanan Wi-Fi.

Pendahuluan

Tingginya ketergantungan terhadap jaringan Wi-Fi, baik di area publik maupun lingkungan institusi pendidikan, membawa risiko keamanan yang signifikan akibat sifat media transmisinya yang terbuka. Sebagaimana dijelaskan oleh Wofford (2020), protokol keamanan standar seperti Wired Equivalent Privacy (WEP) dan Wi-Fi Protected Access (WPA) masih memiliki celah keamanan yang dapat dieksploitasi oleh penyerang untuk membangun Rogue Access Point (RAP). Ancaman ini tidak hanya muncul dalam bentuk perangkat keras ilegal yang dipasang secara fisik, tetapi juga dapat berupa software-based access point yang meniru identitas Service Set Identifier (SSID) resmi. Teknik ini dikenal sebagai serangan Evil Twin, yang bertujuan memancing pengguna agar terhubung ke jaringan palsu sehingga data yang dikirimkan dapat disadap atau dimanipulasi oleh penyerang.

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026

Risiko tersebut menjadi semakin nyata di lingkungan pendidikan yang memiliki tingkat mobilitas dan jumlah pengguna aktif yang tinggi. Studi kasus yang dilakukan di SMKN 1 Kota Jantho menunjukkan bahwa kelemahan konfigurasi jaringan, seperti penggunaan metode enkripsi yang lemah serta layanan manajemen jaringan yang tidak aman, dapat meningkatkan tingkat risiko keamanan secara signifikan. Kondisi ini memperbesar peluang terjadinya serangan RAP yang berdampak pada kebocoran data, penyalahgunaan jaringan, dan gangguan layanan. Oleh karena itu, penerapan Vulnerability Assessment menjadi langkah penting untuk mengidentifikasi celah keamanan yang ada serta mengukur tingkat keparahan risiko menggunakan standar Common Vulnerability Scoring System (CVSS) sebelum serangan benar-benar terjadi (Farhan & Aziz, 2025).

Selain itu, penggunaan metode deteksi tunggal sering kali memiliki keterbatasan dalam jangkauan pemantauan dan efektivitas deteksi. Untuk mengatasi keterbatasan tersebut, pendekatan arsitektur Multi-Agent yang diusulkan oleh Utama et al. (2020) menawarkan solusi deteksi yang lebih komprehensif dan adaptif. Pendekatan ini membagi tugas pemantauan antara Master Agent dan Slave Agent, sehingga proses pemindaian jaringan dapat dilakukan secara terdistribusi di berbagai titik. Mekanisme ini memungkinkan validasi MAC Address serta karakteristik perangkat jaringan yang mencurigakan secara lebih akurat dan berkelanjutan.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk mengintegrasikan pendekatan deteksi berbasis perangkat keras, analisis kerentanan jaringan, serta arsitektur multi-agent dalam rangka membangun sistem pertahanan jaringan Wi-Fi yang tangguh, otomatis, dan proaktif terhadap serangan Rogue Access Point. Pendekatan terintegrasi ini diharapkan mampu meningkatkan keamanan jaringan nirkabel, khususnya di lingkungan pendidikan, serta meminimalkan risiko penyalahgunaan jaringan oleh pihak yang tidak berwenang.

Metode

Penelitian ini menerapkan pendekatan hibrida yang mengintegrasikan pengembangan perangkat keras, arsitektur sistem terdistribusi, serta standar penilaian keamanan siber untuk mendeteksi dan memitigasi serangan Rogue Access Point (RAP) secara komprehensif. Pendekatan ini dirancang agar mampu mendeteksi ancaman baik dari sisi fisik jaringan nirkabel maupun dari sisi logis dan konfigurasi sistem.

Perancangan Sistem Deteksi Berbasis Internet of Things (IoT)

Sebagai lapisan awal dalam deteksi fisik jaringan nirkabel, penelitian ini memanfaatkan mikrokontroler Wemos D1 ESP8266 yang berperan sebagai sensor IoT. Perangkat ini dikonfigurasikan untuk beroperasi dalam promiscuous mode, sehingga mampu memantau lalu lintas jaringan Wi-Fi secara real-time tanpa harus terhubung ke access point tertentu.

Mikrokontroler melakukan pemindaian spektrum Wi-Fi dengan menangkap parameter penting seperti Service Set Identifier (SSID), Media Access Control (MAC) Address, dan Received Signal Strength Indicator (RSSI). Data hasil pemindaian kemudian dikirimkan ke platform cloud ThingSpeak untuk keperluan visualisasi, pencatatan historis, dan pemantauan jarak jauh oleh administrator jaringan. Pendekatan ini memungkinkan proses deteksi dilakukan secara kontinu dan terpusat.

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026

Arsitektur Multi-Agent System

Untuk mengatasi keterbatasan jangkauan yang dimiliki oleh sensor tunggal, penelitian ini mengadopsi arsitektur Multi-Agent System sebagaimana diusulkan oleh Utama et al. (2020). Arsitektur ini membagi fungsi pemantauan jaringan ke dalam dua jenis agen, yaitu Slave Agent dan Master Agent.

Slave Agent ditempatkan pada perangkat klien atau stasiun kerja yang tersebar di berbagai lokasi jaringan. Agen ini bertugas melakukan pemindaian terhadap access point yang terdeteksi di lingkungannya masing-masing dan mengirimkan laporan hasil pemindaian ke pusat sistem.

Sementara itu, Master Agent berfungsi sebagai pusat analisis dan validasi. Agen ini membandingkan data yang diterima dari Slave Agent dengan whitelist, yaitu daftar access point resmi yang telah terdaftar sebelumnya. Apabila ditemukan anomali, seperti SSID resmi yang muncul dengan MAC Address yang tidak dikenal, maka sistem akan menandainya sebagai indikasi serangan Rogue Access Point.

Vulnerability Assessment Menggunakan Standar CVSS

Pendekatan deteksi diperkuat dengan penerapan Vulnerability Assessment (VA) untuk mengukur tingkat risiko keamanan jaringan secara menyeluruh. Mengacu pada penelitian Farhan dan Aziz (2025), proses ini dilakukan melalui dua tahap utama.

Tahap pertama adalah Scanning and Enumeration, yaitu pemetaan topologi jaringan dan identifikasi konfigurasi yang lemah menggunakan perangkat lunak audit jaringan seperti Airodump-ng dan Kismet. Tahap ini bertujuan untuk mendeteksi penggunaan enkripsi yang tidak aman, seperti WEP atau WPA-TKIP, yang sering dimanfaatkan oleh pelaku RAP.

Tahap kedua adalah Risk Scoring, di mana setiap kerentanan yang ditemukan dinilai menggunakan standar Common Vulnerability Scoring System (CVSS). Skor CVSS digunakan untuk mengklasifikasikan tingkat keparahan risiko ke dalam kategori rendah (Low), sedang (Medium), tinggi (High), hingga kritis (Critical), sehingga membantu administrator dalam menentukan prioritas mitigasi.

Klasifikasi dan Mitigasi Otomatis

Berdasarkan parameter teknis yang dikumpulkan dari sistem IoT, Multi-Agent, dan hasil Vulnerability Assessment, sistem melakukan klasifikasi access point ke dalam tiga kategori, yaitu Authorized (resmi), Unauthorized (ilegal), dan Unsecured (tidak aman). Klasifikasi ini mengacu pada taksonomi ancaman jaringan nirkabel yang umum digunakan dalam penelitian keamanan siber.

Apabila sebuah Rogue Access Point teridentifikasi secara positif, sistem secara otomatis menjalankan mekanisme mitigasi berbasis live forensics. Mekanisme ini berupa skrip otomatis yang mengirimkan paket deauthentication secara berulang ke alamat MAC access point ilegal dan klien yang terhubung dengannya. Tindakan ini bertujuan untuk memutus koneksi jaringan ilegal secara efektif melalui mekanisme Denial of Service terhadap RAP, sehingga mencegah penyalahgunaan jaringan lebih lanjut.

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026

Hasil dan Pembahasan

Analisis Kerentanan dan Profil Risiko Jaringan

Berdasarkan hasil Vulnerability Assessment yang dilakukan menggunakan perangkat audit jaringan Kismet dan Airodump-ng pada lingkungan studi kasus di SMKN 1 Kota Jantho, ditemukan sejumlah celah keamanan yang tergolong kritis. Hasil pemindaian menunjukkan adanya penggunaan protokol manajemen jaringan yang tidak terenkripsi serta konfigurasi access point (AP) yang belum menerapkan standar keamanan yang memadai. Kondisi ini sejalan dengan temuan Farhan dan Aziz (2025) yang menyatakan bahwa lemahnya konfigurasi jaringan nirkabel meningkatkan potensi penyalahgunaan oleh pihak tidak berwenang.

Penilaian tingkat risiko dilakukan menggunakan standar Common Vulnerability Scoring System (CVSS). Berdasarkan hasil analisis, kerentanan yang teridentifikasi memiliki skor rata-rata sebesar 7,58, yang termasuk dalam kategori risiko tinggi (High). Tingginya nilai ini menunjukkan bahwa jaringan sangat rentan dieksploitasi, khususnya untuk penyisipan Rogue Access Point (RAP) tanpa terdeteksi oleh administrator jaringan. Risiko ini semakin meningkat pada area blind spot yang tidak terpantau secara fisik maupun administratif.

Kinerja Deteksi Menggunakan Arsitektur Multi-Agent

Implementasi arsitektur Multi-Agent System menunjukkan peningkatan yang signifikan dalam akurasi dan kecepatan deteksi dibandingkan metode pemindaian tunggal. Sistem ini mampu melakukan pemantauan jaringan secara terdistribusi melalui kerja sama antara Slave Agent dan Master Agent.

Mekanisme Validasi Access Point

Sistem berhasil membedakan antara Authorized Access Point dan Rogue Access Point melalui mekanisme pencocokan white list. Ketika Slave Agent mendeteksi SSID yang sah, misalnya “Kampus_WIFI”, namun memancarkan sinyal dari BSSID (MAC Address) yang tidak terdaftar pada basis data Master Agent, sistem secara otomatis mengklasifikasikan perangkat tersebut sebagai ancaman. Mekanisme ini efektif dalam mengidentifikasi serangan Evil Twin yang meniru identitas jaringan resmi.

Kecepatan Respons Deteksi

Hasil pengujian menunjukkan bahwa komunikasi antara Slave Agent dan Master Agent berjalan secara real-time dan stabil. Agen yang ditempatkan pada perangkat klien mampu melaporkan anomali jaringan segera setelah perangkat aktif. Dengan demikian, celah waktu yang biasanya dimanfaatkan penyerang saat tidak adanya pemantauan manual dapat diminimalkan secara signifikan.

Analisis Karakteristik Serangan Evil Twin

Dalam simulasi serangan yang mengacu pada taksonomi ancaman nirkabel yang dikemukakan oleh Wofford (2020), Rogue Access Point umumnya dikonfigurasi sebagai Evil Twin. Hasil pemantauan berbasis IoT menunjukkan bahwa RAP cenderung memancarkan sinyal dengan kekuatan lebih tinggi (Received Signal Strength Indicator / RSSI) dibandingkan AP resmi. Strategi ini digunakan untuk memancing perangkat korban agar berpindah koneksi secara otomatis melalui mekanisme aggressive roaming yang umum terdapat pada perangkat smartphone dan laptop.

Sistem deteksi berbasis Wemos D1 ESP8266 berhasil menangkap anomali

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026

lonjakan sinyal tersebut dan mengidentifikasi keberadaan perangkat mencurigakan. Temuan ini mengindikasikan adanya upaya serangan Man-in-the-Middle (MITM) yang berpotensi digunakan untuk mencuri kredensial dan data pengguna.

Efektivitas Mitigasi Otomatis Menggunakan Deauthentication

Setelah Rogue Access Point teridentifikasi secara positif melalui validasi silang antara hasil Vulnerability Assessment dan laporan sistem Multi-Agent, sistem secara otomatis menjalankan prosedur mitigasi. Proses containment dilakukan dengan mengirimkan paket deauthentication secara terarah ke BSSID milik RAP.

Berdasarkan hasil pengujian di lingkungan laboratorium, teknik ini terbukti efektif dalam memutus koneksi klien dari RAP dalam waktu kurang dari lima detik setelah deteksi. Klien yang terputus akan mencoba melakukan koneksi ulang (re-association), namun karena RAP terus-menerus mengalami gangguan (jamming), perangkat klien akhirnya terhubung kembali ke access point resmi yang memiliki sinyal stabil dan terdaftar dalam white list. Hasil ini menunjukkan bahwa pendekatan live forensics dan respons aktif yang diterapkan mampu meminimalkan risiko pencurian data serta meningkatkan ketahanan jaringan terhadap serangan Rogue Access Point secara signifikan.

Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa pengamanan jaringan WLAN terhadap serangan Rogue Access Point memerlukan penerapan strategi pertahanan berlapis (defense in depth). Pelaksanaan Vulnerability Assessment secara berkala terbukti penting dalam memetakan profil risiko jaringan serta mengidentifikasi celah keamanan yang berpotensi dimanfaatkan oleh penyerang. Selain itu, penerapan arsitektur Multi-Agent System mampu meningkatkan cakupan dan akurasi deteksi Rogue Access Point, khususnya pada serangan yang menggunakan teknik Evil Twin dengan meniru identitas access point resmi.

Hasil penelitian juga menunjukkan bahwa mekanisme mitigasi otomatis berbasis deauthentication efektif dalam meminimalkan durasi paparan risiko terhadap pengguna jaringan. Dengan respons yang cepat dan terukur, sistem mampu memutus koneksi ilegal serta mengarahkan kembali pengguna ke access point resmi, sehingga potensi pencurian data dapat ditekan secara signifikan.

Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat dijadikan bahan pertimbangan untuk pengembangan dan penerapan sistem ke depan. Pertama, penelitian selanjutnya disarankan untuk mengintegrasikan sistem deteksi Rogue Access Point dengan platform Wireless Intrusion Detection and Prevention System (WIDPS) yang lebih komprehensif. Integrasi ini diharapkan mampu meningkatkan efektivitas deteksi dan mitigasi ancaman secara terpusat, adaptif, dan berkelanjutan.

Kedua, pengujian sistem sebaiknya diperluas pada lingkungan jaringan yang lebih kompleks, seperti area dengan kepadatan pengguna yang tinggi atau pada skala institusi yang lebih besar. Hal ini bertujuan untuk mengevaluasi kinerja sistem dalam menghadapi lalu lintas jaringan yang dinamis, heterogenitas perangkat, serta potensi gangguan yang lebih beragam.

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026

Terakhir, administrator jaringan disarankan untuk secara rutin melakukan pelatihan dan evaluasi keamanan jaringan. Upaya ini penting untuk meningkatkan kesadaran terhadap ancaman Rogue Access Point serta memastikan bahwa kebijakan dan mekanisme keamanan jaringan selalu diperbarui dan selaras dengan perkembangan teknik serangan siber yang semakin canggih.

Daftar Pustaka

Farhan, Y., & Aziz, A. S. (2025). Analisis keamanan jaringan Wi-Fi pada SMKN 1 Kota Jantho menggunakan metode Vulnerability Assessment. CyberSecurity dan Forensik Digital, 8(2), 55–62.

Hermaduanti, N. (2016). Pengembangan framework otomatisasi mitigasi kasus Rogue Access Point pada jaringan wireless IEEE 802.1X (Tesis Magister). Universitas Islam Indonesia, Yogyakarta.

Iman, W. (2020). Sistem deteksi serangan Rogue Access Point berbasis Internet of Things (IoT) (Tugas Akhir). Universitas Islam Indonesia, Yogyakarta.

Utama, D. S., & Oktavia, D. (2020). Implementasi metode multi-agent untuk mendeteksi Rogue Access Point (RAP). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 4(9), 2966–2973.

Wofford, P. (2020). Rogue access points: The threat to public wireless networks (Capstone Project). Utica College, New York.

Alotaibi, F., & Alshammari, R. (2021). Detection of rogue access point attacks in wireless networks: A survey. International Journal of Computer Networks & Communications, 13(2), 1–16.

IEEE. (2020). IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standards Association.

Received: November 18, 2025 – Revised: November 25, 2025 - Accepted: Desember 10, 2025 - Published online: January 10, 2026