Integrasi Sistem untuk Deteksi Peniruan Router Nirkabel Berbasis Machine Learning dengan Optimasi QoS

1st Nizar Rizqi Bachtiar
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
nizarrizqib@student.telkomuniversity.ac.id

2nd Ida Wahidah
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
wahidah@.telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanfnn@.telkomuniversity.ac.id

***Abstrak* — Peniruan router nirkabel merupakan ancaman keamanan yang signifikan dalam jaringan, yang dapat menyebabkan akses tidak sah dan pencurian data. Untuk mengatasi masalah ini, penelitian ini mengembangkan sebuah sistem deteksi berbasis Machine Learning yang terintegrasi untuk mendeteksi upaya peniruan router secara real-time. Selain itu, sistem ini dirancang untuk mengoptimalkan kualitas layanan (QoS) jaringan, sehingga tidak hanya mampu mendeteksi ancaman dengan akurasi tinggi tetapi juga mempertahankan kinerja jaringan yang stabil dan efisien. Hasil uji menunjukkan bahwa sistem ini efektif dalam mendeteksi peniruan sekaligus menjaga QoS pada tingkat yang optimal, menjadikannya solusi yang andal untuk meningkatkan keamanan jaringan tanpa mengorbankan kinerja. Pengujian lebih lanjut menunjukkan bahwa model ini berhasil mendeteksi peniruan dengan akurasi hingga 98.85%, sambil menjaga performa jaringan dengan throughput rata-rata 10240.78 bits/detik, delay 0.22 detik, dan tanpa packet loss. Sistem ini membuktikan bahwa integrasi pembelajaran mesin dengan optimasi QoS dapat meningkatkan keamanan jaringan nirkabel secara efektif.**

***Kata kunci:* Peniruan router nirkabel, Machine Learning, deteksi ancaman, optimasi QoS, keamanan jaringan.**

I. PENDAHULUAN

Dalam era konektivitas yang semakin meningkat, jaringan nirkabel telah menjadi tulang punggung utama komunikasi, baik di rumah, kantor, maupun di ruang publik. Namun, seiring dengan meluasnya penggunaan jaringan ini, ancaman terhadap keamanannya juga terus berkembang. Salah satu ancaman yang paling signifikan adalah peniruan *router* nirkabel (*wireless router impersonation*), di mana penyerang menyamar sebagai router yang sah untuk mendapatkan akses ke data sensitif pengguna. Serangan semacam ini tidak hanya berpotensi merugikan privasi pengguna, tetapi juga dapat mengancam keamanan data di seluruh jaringan[1].

Peniruan *router* nirkabel memungkinkan penyerang melakukan berbagai serangan berbahaya, termasuk pembajakan koneksi dengan teknik *man-in-the-middle* (MITM), pengalihan pengguna ke situs web phishing, dan penyebaran malware. Serangan ini menjadi lebih berbahaya dalam konteks jaringan Wi-Fi publik, di mana pengguna sering kali tidak dapat membedakan antara jaringan yang sah dan yang palsu, seperti pada serangan *Evil Twin Attack* (ETA)[2]. Ancaman ini menuntut adanya solusi deteksi yang efektif dan *real-time* untuk melindungi pengguna dari serangan yang semakin canggih.

Penelitian ini mengusulkan pengembangan sistem deteksi peniruan *router* nirkabel berbasis *Machine Learning* (ML) yang dirancang untuk beroperasi secara real-time, sekaligus mengoptimalkan kualitas layanan (QoS) jaringan. Dengan menggunakan ML, sistem ini mampu mengenali pola lalu lintas jaringan yang kompleks dan sulit terdeteksi oleh metode konvensional, serta memberikan respons yang tepat terhadap serangan. Selain fokus pada deteksi ancaman, sistem ini juga dirancang untuk mempertahankan performa jaringan yang optimal, memastikan bahwa pengguna tetap mendapatkan pengalaman koneksi yang cepat dan stabil meskipun ada ancaman yang terjadi.

II. KAJIAN TEORI

A. *Wireless Router Impersonation*

Peniruan router nirkabel adalah salah satu bentuk serangan siber di mana penyerang membuat titik akses nirkabel (*wireless access point*) yang meniru *router* asli. Tujuannya adalah untuk menipu pengguna agar terhubung ke jaringan palsu, memungkinkan penyerang untuk memantau dan mencuri data sensitif seperti kredensial login, informasi keuangan, dan data pribadi lainnya. Peniruan router sering digunakan dalam serangan *man-in-the-middle* (MITM) atau serangan *Evil Twin*, di mana penyerang memposisikan dirinya di antara pengguna dan jaringan yang sah untuk menyadap komunikasi atau menyebarkan malware. Peniruan *router* nirkabel menjadi semakin berbahaya di lingkungan dengan banyak pengguna yang tidak dapat membedakan antara jaringan yang sah dan palsu, seperti di tempat-tempat umum yang menyediakan Wi-Fi gratis.

B. *Machine Learning*

Pembelajaran mesin (*Machine Learning*) adalah subbidang kecerdasan buatan yang memungkinkan sistem untuk belajar dari data dan membuat keputusan atau prediksi

tanpa diprogram secara eksplisit. Dalam konteks keamanan jaringan, algoritma pembelajaran mesin seperti *Feedforward Neural Network* (FNN) digunakan untuk mendeteksi ancaman dengan mengklasifikasikan sinyal yang berasal dari *Rogue Access Point* (RAP) dan *Access Point* (AP) yang sah. FNN dilatih menggunakan data yang dikumpulkan dari alat seperti airodump-ng, yang mencakup karakteristik sinyal Wi-Fi seperti kekuatan sinyal dan jenis enkripsi. Melalui proses pembelajaran ini, FNN dapat mengenali pola yang membedakan antara RAP dan AP yang sah, memungkinkan deteksi ancaman yang akurat dan responsif terhadap berbagai jenis serangan, termasuk yang baru dan belum terdeteksi oleh metode konvensional[3].

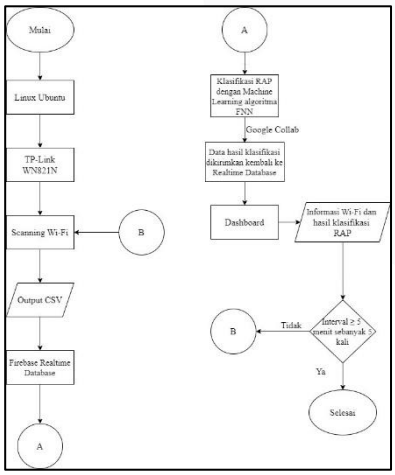
C. *Quality of Service* (QoS)

Kualitas Layanan (QoS) adalah metode yang digunakan untuk mengukur dan menganalisis kinerja jaringan, khususnya dalam konteks memberikan informasi mengenai kualitas jaringan secara numerik. QoS mengevaluasi berbagai parameter penting seperti throughput, delay dan packet loss yang semuanya berperan dalam menentukan seberapa baik sebuah jaringan mampu mengatasi beban dan gangguan. Dengan memprioritaskan jenis data tertentu dalam jaringan, QoS memungkinkan pengelolaan dan pengendalian sumber daya jaringan secara lebih efektif. Optimasi QoS sangat penting dalam jaringan nirkabel, terutama dalam sistem deteksi ancaman, untuk memastikan bahwa ancaman dapat dideteksi dengan akurat tanpa mengorbankan stabilitas dan kinerja jaringan. Integrasi QoS dengan pembelajaran mesin dalam deteksi ancaman membantu menjaga keseimbangan antara keamanan dan efisiensi jaringan, sehingga pengguna dapat tetap menikmati pengalaman yang cepat dan aman.

III. METODE

Strategi perencanaan ini dapat dirancang dengan Metode sebagai berikut :

A. Integrasi Sistem



GAMBAR 3.1
DIAGRAM INTEGRASI SYSTEM.

Pada gambar 3.1 adalah proses deteksi peniruan *router* nirkabel dimulai dengan menggunakan sistem operasi Linux Ubuntu, di mana kartu jaringan nirkabel TP-Link WN821N digunakan untuk menangkap sinyal Wi-Fi dalam mode monitor. Perangkat kemudian memindai jaringan Wi-Fi yang tersedia di lingkungan sekitar, dan hasil pemindaian ini diekspor dalam format CSV untuk memudahkan pemrosesan data lebih lanjut. Data yang telah disimpan dalam format CSV diunggah ke Firebase Realtime Database untuk penyimpanan dan akses oleh system lain. Selanjutnya, data tersebut diproses dan dianalisis menggunakan algoritma ML *Feedforward Neural Network* (FNN) di Google Colab untuk mengidentifikasi dan mengklasifikasikan *Rogue Access Point* (RAP). Hasil klasifikasi RAP dari model FNN kemudian dikirim kembali dan disimpan di Firebase Realtime Database. Informasi mengenai Wi-Fi dan hasil klasifikasi RAP ini ditampilkan di dashboard untuk memudahkan pemantauan. Proses ini diulang setiap 5 menit dan dilakukan hingga 5 kali, memberikan pembaruan berkala terkait status jaringan nirkabel.

B. Simulasi

Berikut merupakan cara kerja deteksi Wi-Fi menggunakan TP-Link WN821N untuk mendeteksi sinyal Wi-Fi menggunakan airodump-ng, yaitu:

- Persiapan alat TP-Link WN821N

  Perangkat keras TP-Link WN821N, yang merupakan USB *wireless adapter*, digunakan untuk mendeteksi sinyal Wi-Fi yang ada di sekitarnya. Koneksi dengan Ubuntu
- Koneksi dengan Ubuntu

  TP-Link WN821N dihubungkan ke komputer yang menjalankan sistem operasi Ubuntu melalui port USB. Ubuntu adalah sistem operasi yang sering digunakan untuk keperluan keamanan dan pengujian jaringan, termasuk pengujian Wi-Fi.
- Integrasi ke Airodump-ng

  Di dalam Ubuntu, menggunakan perangkat lunak bernama airodump-ng untuk me-monitor dan menangkap sinyal Wi-Fi yang dideteksi oleh TP-Link WN821N.
- Mode monitor

  Sebelum menggunakan airodump-ng, TP-Link WN821N perlu dikonfigurasi ke dalam mode monitor. Mode monitor memungkinkan perangkat untuk menangkap dan menganalisis semua paket yang dikirimkan melalui jaringan Wi-Fi, bukan hanya paket yang ditujukan untuk perangkat tersebut.
- Pengumpulan informasi

  Setelah TP-Link WN821N berada dalam mode monitor dan airodump-ng berjalan, perangkat akan mulai mengumpulkan informasi dari sinyal Wi-Fi yang terdeteksi. Informasi yang dikumpulkan meliputi alamat BSSID, daya sinyal (*power*), jumlah *beacon* (*beacons*), jumlah frame data (#data), rata-rata jumlah frame (#/s), saluran (*channel*), kecepatan maksimum AP (MB), jenis enkripsi (ENC), jenis *chipper* (*chiper*), metode autentikasi (*authentication*), dan nama SSID (essid).

C. Pengujian Sistem

a. *Quality of Service* (QoS)

Pada pengujian ini menggunakan laptop airdump-ng sebagai sensor yang di bantu oleh TL-WN821 untuk menangkap data-data yang dikirim ke firebase, juga menggunakan *software* Wireshark.

- *Throughput*

Throughput adalah jumlah dari total kedatangan suatu paket yang berhasil di kirim dari tujuan. Pada pengukuran ini jumlah data yang berhasil diproses atau ditransfer antara airdump-ng sebagai sensor ke firebase dalam jangka waktu tertentu. *throughput* yang tinggi menunjukkan bahwa sistem dapat menangani banyak permintaan dan mentransfer sejumlah besar data dengan cepat[4]. Rumus dapat ditunjukkan pada persamaan 5.1. Rumus *throughput* dapat ditunjukkan pada persamaan.

$$Throughput(\text{bps}) = \frac{\text{Jumlah paket yang dikirim (bytes)}}{\text{Lama waktu pengamatan } (s)} \text{x8} \quad (1)$$

- *Delay*

Delay atau waktu yang dibutuhkan sebuah paket dalam mengirim data atau jarak tempuh dari pengirim ke tujuan penerima. Dengan demikian waktu yang dibutuhkan untuk mentransfer data dari airodump-ng sebagai sensor ke dashboard [4]. Standar *delay* yang direkomendasikan adalah kurang dari 15 detik sebagai preferensi, dan kurang dari 60 detik sebagai nilai yang dapat diterima[5]. Rumus *delay* dapat ditunjukkan pada persamaan 5.2.

$$Delay\ (\text{s}) = \frac{\text{Lama waktu pengamatan (s)}}{\text{Jumlah paket diterima}} \quad (2)$$

- *Packet Loss*

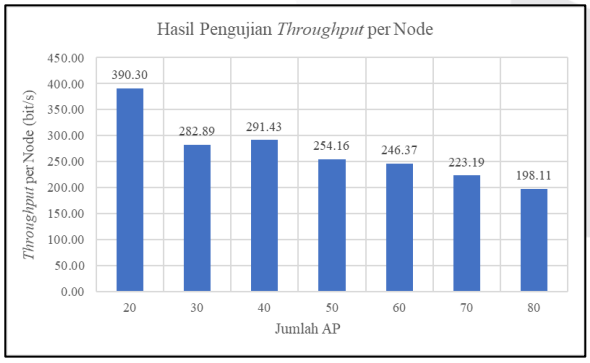
Packet loss adalah situasi di mana satu atau lebih paket data yang dikirim melalui jaringan tidak berhasil mencapai tujuan yang diinginkan. Bisa didefinisikan ketika paket data yang dikirim dari airodump-ng sebagai sensor ke *dashboard* atau sebaliknya hilang dalam perjalanan dan tidak sampai ke tujuan[4]. Rumus *packet loss* dapat ditunjukkan pada persamaan 5.3.

$$Packet\ Loss(\%) = \frac{\text{(Total paket dikirim-Total paket diterima)}}{\text{Total paket dikirim}} \text{x100} \quad (3)$$

IV. HASIL DAN PEMBAHASAN

A. *Quality of Service* (QoS)

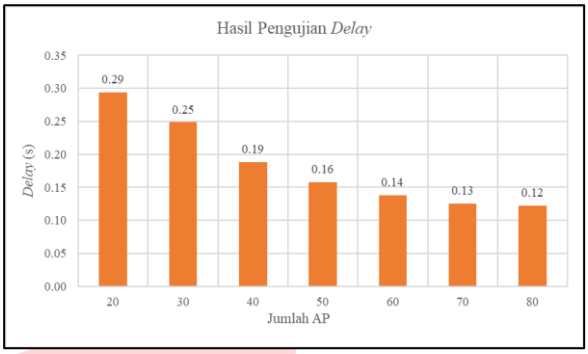
- *Throughput*



GAMBAR 4.1
THROUGHPUT DATASET KE *FIREBASE*

Berdasarkan Gambar 4.1 hasil pengujian throughput QoS yang diukur dalam satuan bit per second selama 70 kali pengujian, di mana setiap 10 sesi ditambahkan 10 jumlah data AP, terlihat adanya peningkatan *throughput* yang signifikan dan stabil seiring bertambahnya jumlah AP. Throughput meningkat dari 7805.99 bps pada 20 AP hingga mencapai 15848.53 bps pada 80 AP, dengan peningkatan yang konsisten pada setiap tahap, termasuk 8486.81 bps pada 30 AP, 11657.31 bps pada 40 AP, dan seterusnya, hingga 15848.53 bps pada 80 AP.

- *Delay*



GAMBAR 4.2
DELAY DATASET KE *FIREBASE*

Berdasarkan Gambar 4.2 hasil pengujian *delay* QoS yang diukur dalam detik selama 70 kali pengujian, di mana setiap 10 sesi ditambahkan 10 jumlah data AP, terlihat penurunan *delay* yang signifikan dan konsisten seiring bertambahnya jumlah AP. *Delay* menurun dari 0.29 detik pada 20 AP hingga 0.12 detik pada 80 AP, dengan penurunan bertahap di setiap tahap, termasuk 0.25 detik pada 30 AP, 0.19 detik pada 40 AP, dan seterusnya hingga mencapai 0.12 detik pada 80 AP. Hasil ini menunjukkan bahwa jaringan mampu beradaptasi dengan baik terhadap peningkatan jumlah data AP, mempertahankan kinerja yang stabil dan responsif.

- *Packet Loss*

Berdasarkan hasil pengujian *packet loss* QoS yang diukur dalam persentase, jaringan menunjukkan kualitas yang sangat baik dengan tidak ada paket data yang hilang selama pengujian, meskipun jumlah data AP bertambah. Ini menandakan bahwa jaringan memiliki kapasitas yang cukup untuk menangani variasi beban tanpa degradasi kualitas transmisi data. Hasil ini juga menunjukkan bahwa optimasi jaringan dan infrastruktur yang digunakan efektif, mampu mengakomodasi peningkatan jumlah data AP tanpa mempengaruhi keandalan jaringan. Secara keseluruhan, performa jaringan yang diuji sangat baik dan stabil, dengan kemampuan untuk mengelola peningkatan data AP tanpa kehilangan paket data.

Berdasarkan hasil pengujian QoS terhadap jaringan yang dilakukan, parameter yang diukur meliputi *throughput*, *delay*, dan *packet loss*. *Throughput* meningkat secara signifikan dan stabil dari 7805,99 bps pada 20 AP hingga 15848,53 bps pada 80 AP, sementara *delay* menunjukkan penurunan konsisten dari 0,29 detik menjadi 0,12 detik pada jumlah AP yang sama. Selain itu, *packet loss* tercatat sebesar 0,00%, menunjukkan bahwa jaringan mampu menangani peningkatan jumlah data AP tanpa kehilangan paket data. Hasil ini menunjukkan bahwa jaringan memiliki performa yang sangat baik dan stabil, sesuai dengan standar sesuai dengan standar ITU-T G.1010[5].

V. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem deteksi peniruan router nirkabel berbasis *Machine Learning* yang efektif dan efisien. Hasil pengujian menunjukkan bahwa sistem ini mampu mendeteksi peniruan *router* dengan akurasi tinggi hingga 98.85%, sambil menjaga kualitas layanan (QoS) jaringan yang optimal. *Throughput* jaringan meningkat secara signifikan dan stabil dari 7805.99 bps pada 20 AP hingga 15848.53 bps pada 80 AP, menunjukkan bahwa sistem dapat menangani peningkatan jumlah *Access Point* (AP) tanpa penurunan kinerja. *Delay* juga menurun secara konsisten dari 0.29 detik menjadi 0.12 detik pada jumlah AP yang sama, menandakan bahwa jaringan mampu beradaptasi dengan baik terhadap peningkatan beban. Selain itu, tidak ada *packet loss* yang terjadi selama pengujian, yang menunjukkan bahwa jaringan mampu mentransmisikan data dengan andal meskipun jumlah AP meningkat.

Secara keseluruhan, integrasi pembelajaran mesin dengan optimasi QoS terbukti efektif dalam meningkatkan keamanan dan stabilitas jaringan nirkabel. Sistem yang dikembangkan tidak hanya mampu mendeteksi ancaman dengan akurasi tinggi, tetapi juga mempertahankan kinerja jaringan yang cepat dan stabil. Dengan kemampuan untuk mengelola peningkatan jumlah data AP tanpa kehilangan paket data, sistem ini menjadi solusi andal untuk meningkatkan keamanan jaringan nirkabel, terutama di lingkungan yang memiliki risiko tinggi terhadap serangan peniruan *router*.

VI. REFERENSI

[1] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, “Catch me if you can: Rogue access point detection using intentional channel interference,” IEEE Trans Mob Comput, vol. 19, no. 5, pp. 1056–1071, May 2020, doi: 10.1109/TMC.2019.2903052.

[2] Z. Zhang, H. Hasegawa, Y. Yamaguchi, and H. Shimada, “Rogue wireless AP detection using delay fluctuation in backbone network,” in Proceedings - International Computer Software and Applications Conference, IEEE Computer Society, Jul. 2019, pp. 936–937. doi: 10.1109/COMPSAC.2019.00149.

[3] J. Zou, Y. Han, and S.-S. So, “Overview of Artificial Neural Networks,” 2008. doi: 10.1007/978-1-60327-101-1_2.

[4] M. Ryan Kamil, F. Arzalega, and A. Sani, “JBPI-Jurnal Bidang Penelitian Informatika Ciptaan disebarluaskan di bawah Lisensi Creative Commons Atribusi 4.0 Internasional Analisis Kualitas Layanan Jaringan Internet Wifi PT.XYZ dengan Metode QoS (Quality of Service),” Feb. 2023. [Online]. Available: https://ejournal.kreatifcemerlang.id/index.php/jbpi

[5] INTERNATIONAL TELECOMMUNICATION UNION, “ITU-T End-user multimedia QoS categories,” 2001.