BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam perkembangan teknologi yang pesat, keamanan komunikasi antar kendaraan menjadi fokus utama dalam pengembangan sistem transportasi cerdas. Teknologi penting yang mendukung komunikasi ini adalah *Vehicular Ad hoc Network (*VANET), yang memungkinkan kendaraan untuk saling berkomunikasi langsung tanpa memerlukan infrastruktur tetap. Protokol *Node Routing* seperti *Ad hoc On-Demand Distance Vector* (AODV) digunakan untuk mengatur komunikasi dalam VANET. Meskipun AODV berperan krusial dalam menjaga kelancaran pertukaran informasi, protokol ini tetap rentan terhadap serangan yang dapat mengancam stabilitas dan keamanan jaringan, yang menjadi tantangan serius dalam penerapan sistem transportasi cerdas.

Mobile Ad hoc Network (MANET) adalah jaringan nirkabel yang terdiri dari *Node* -*Node* yang dapat diatur secara dinamis tanpa memerlukan infrastruktur jaringan tetap. Setiap perangkat dalam MANET berfungsi sebagai *Node* dan router, memungkinkan komunikasi langsung antar perangkat tanpa perlu pusat administrasi. Keunggulan MANET adalah kemampuannya untuk beradaptasi dengan perubahan topologi jaringan secara *real-time*, sehingga perangkat dapat bergerak bebas sambil tetap mempertahankan konektivitas. MANET digunakan dalam berbagai situasi seperti operasi militer dan bantuan bencana, di mana jaringan yang fleksibel dan tangguh sangat dibutuhkan.(Manapa et al., 2020)

Sedangkan, untuk *Vehicular Ad hoc Network* (VANET) sering disebut sebagai "jaringan di atas roda," yang dirancang untuk memungkinkan komunikasi antar *Node* kendaraan. Jaringan ini memungkinkan kendaraan untuk saling bertukar informasi penting saat berada di jalan, tanpa memerlukan infrastruktur tetap. Dalam VANET, setiap kendaraan berfungsi sebagai *Node* yang dapat mengirim dan menerima data dengan kendaraan lain di sekitarnya. Komunikasi ini bertujuan untuk meningkatkan keselamatan, efisiensi, dan pengalaman berkendara dengan memungkinkan kendaraan berbagi informasi secara *real-time*. Sebagai

salah satu elemen kunci dalam pengembangan sistem transportasi cerdas, VANET memainkan peran penting dalam menghubungkan kendaraan dan mendukung berbagai aplikasi terkait lalu lintas.(Günay et al., 2021)

Perbedaan mendasar antara *MANET* dan *VANET* yaitu, *Mobile Ad hoc Network* (MANET) dan *Vehicular Ad hoc Network* (VANET) adalah jaringan nirkabel yang tidak memerlukan infrastruktur tetap, namun keduanya memiliki perbedaan dalam hal penggunaan dan mobilitas. MANET terdiri dari perangkat bergerak yang dapat berfungsi sebagai *Node* dan router, dan digunakan dalam situasi seperti operasi militer dan bantuan darurat yang membutuhkan jaringan yang sangat fleksibel. Sebaliknya, VANET dirancang khusus untuk kendaraan, memungkinkan mereka berkomunikasi saat berada di jalan untuk meningkatkan keselamatan dan efisiensi lalu lintas. MANET beradaptasi dengan topologi jaringan yang acak dan tidak terstruktur, sementara VANET menghadapi perubahan topologi yang cepat tetapi lebih teratur sesuai dengan pola pergerakan kendaraan. Selain itu, VANET berfokus pada pertukaran informasi *real-time* antar kendaraan, yang menjadikannya krusial dalam pengembangan sistem transportasi cerdas.

Penelitian ini berfokus pada analisis performa jaringan dalam *Vehicular Ad hoc Network* (VANET) dengan menggunakan protokol AODV. AODV adalah salah satu protokol *Node Routing* reaktif yang bekerja dengan cara memulai pencarian rute hanya ketika diperlukan. Ketika sebuah *Node* sumber membutuhkan rute ke *Node* tujuan, ia mengirimkan paket permintaan rute (*Request*) ke seluruh jaringan. *Node* yang berada di dekat tujuan akan merespons permintaan ini dengan mengirimkan paket balasan rute (*Reply*) kembali ke *Node* sumber.(Sindhwani et al., 2022)

Matrix Laboratory (MATLAB) merupakan sebuah program komputer interaktif yang berperan sebagai alat bantu yang efisien untuk berbagai jenis perhitungan. Program ini menyediakan lingkungan kerja yang nyaman, memungkinkan pengguna untuk melakukan kalkulasi yang kompleks. Salah satu fitur utama MATLAB adalah kemampuannya dalam menangani operasi yang melibatkan matriks. Dengan demikian, MATLAB sering digunakan sebagai

“laboratorium” virtual untuk menyelesaikan berbagai masalah matematis dan teknik yang melibatkan matriks.(Moler & Little, 2020)

Penelitian ini memfokuskan pada analisis serangan *Blackhole*, di mana serangan tersebut menyebabkan semua paket data di VANET dibuang, sehingga mengurangi kinerja jaringan secara keseluruhan. Untuk mendeteksi serangan *Blackhole* pada protokol *Node Routing* AODV, dikembangkan solusi berupa modifikasi protokol tersebut. Inovasi ini melibatkan perubahan pada paket *route request packet* (RREQ*)* dan *route Reply packet* (RREP) dalam AODV untuk meningkatkan kinerja jaringan. *Node* akan memverifikasi *Node* tujuan sebelum meneruskan paket dengan menggunakan fitur keamanan baru yang memeriksa nomor urut paket kendaraan. Modifikasi ini bertujuan untuk memperkuat keamanan dan efektivitas protokol *Node Routing* dalam menghadapi serangan *Blackhole*.(A. Kumar et al., 2021)

Penelitian ini bertujuan untuk menganalisis kinerja jaringan AODV dalam VANET ketika mengalami serangan *Blackhole*. Uji coba dilakukan dengan memodifikasi jaringan AODV untuk mensimulasikan serangan *Blackhole*, sehingga memungkinkan pengamatan dampaknya secara mendalam. Pendeteksian serangan ini dilakukan dengan membandingkan *Source Sequence Number* dan *Route Reply Sequence Number* pada protokol *Node Routing* AODV. Untuk meningkatkan akurasi deteksi, ditambahkan fungsi *Threshold* (ambang batas) yang membantu dalam mengidentifikasi *Node* yang bersifat jahat (*malicious*). Dengan pendekatan ini, identifikasi serangan *Blackhole* pada jaringan AODV dapat dilakukan dengan lebih tepat. Penelitian ini juga mencakup evaluasi terhadap dampak serangan *Blackhole* pada *delay* dan *throughput* jaringan. Ditemukan bahwa kedua metrik ini cenderung menurun seiring dengan peningkatan jumlah serangan *Blackhole*. Penurunan tersebut terjadi karena serangan *Blackhole* dapat menyebabkan *timeout* atau pemutusan koneksi pada *Node Routing*, yang berdampak langsung pada kinerja jaringan. Selain itu, modifikasi protokol AODV yang dilakukan juga bertujuan untuk meningkatkan ketahanan jaringan terhadap serangan semacam ini. Hasil penelitian diharapkan dapat memberikan wawasan

tentang bagaimana meningkatkan keamanan dan efisiensi jaringan AODV dalam lingkungan VANET.

1.2. Rumusan Masalah

Rumusan masalah pada analisis ini yaitu:

1 Bagaimana kinerja jaringan dalam VANET terpengaruh oleh serangan *Blackhole*?
2 Bagaimana cara mendeteksi serangan *Blackhole* pada protokol AODV?
3 Apa pengaruh modifikasi protokol AODV terhadap kinerja jaringan ketika menghadapi serangan *Blackhole*?
4 Bagaimana perubahan *throughput* dan *delay* apabila terjadi serangan *Blackhole* pada jaringan VANET

1.3. Batasan Masalah

Batasan masalah pada analisis:

1. Analisis ini dilakukan menggunakan *Matrix Laboratory* (MATLAB)
2. Penelitian ini hanya akan menganalisis dampak serangan *Blackhole* terhadap kinerja jaringan AODV dalam lingkungan VANET.
3. Analisis akan difokuskan pada modifikasi protokol AODV untuk mendeteksi dan mengatasi serangan *Blackhole*.
4. Evaluasi kinerja jaringan akan dilakukan berdasarkan tiga metrik utama: simulasi, *delay* (latensi) dan *throughput*.
5. Penelitian ini akan mengimplementasikan fungsi *Threshold* sebagai bagian dari modifikasi protokol AODV untuk mendeteksi *Node* jahat.

1.4. Tujuan Tugas Akhir

Tujuan analisis ini yaitu:

1. Untuk memahami dan mengukur dampak serangan *Blackhole* terhadap performa jaringan VANET, termasuk bagaimana serangan ini mempengaruhi *delay* dan *throughput* jaringan.
2. Untuk mengevaluasi efektivitas modifikasi protokol AODV yang telah diterapkan untuk mengidentifikasi dan mendeteksi serangan *Blackhole*

1.4. Manfaat Tugas Akhir

Berdasarkan penjelasan di atas, berikut adalah manfaat penelitian:

1. Penelitian ini memberikan pemahaman mendalam tentang bagaimana protokol AODV beroperasi dalam lingkungan VANET, khususnya dalam situasi terjadinya serangan *Blackhole*.
2. Dengan menganalisis dampak serangan *Blackhole* terhadap *delay* dan *throughput* dalam jaringan AODV, penelitian ini memberikan wawasan tentang bagaimana serangan ini mempengaruhi kinerja jaringan.
3. Hasil penelitian dapat membantu dalam merancang strategi mitigasi yang lebih baik untuk meningkatkan performa jaringan dalam menghadapi serangan semacam ini.
4. penelitian ini memberikan kontribusi pada pengembangan sistem transportasi cerdas yang lebih baik.

1.5. Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun dengan beberapa bab yang teratur dan terstruktur sebagai berikut:

BAB I PENDAHALUAN

Bab ini mencakup penjelasan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, serta sistematika penulisan.

Bab II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab ini menyajikan ringkasan dan analisis dari berbagai literatur yang relevan dengan topik penelitian, mencakup teori dasar tentang VANET dan *Blackhole*, serta konsep-konsep yang digunakan dalam penelitian ini.

Bab III METODOLOGI PENELITIAN

Bab ini akan berfokus pada penjelasan tentang metode penelitian yang digunakan untuk melakukan analisis serangan *Blackhole* pada jaringan VANET.

Bab IV HASIL DAN PEMBAHASAN

Bab ini membahas pendekatan yang diterapkan dalam penelitian. Selain itu, bab ini menjelaskan langkah-langkah yang diambil untuk melaksanakan penelitian tersebut. Setiap tahapan penelitian diuraikan secara rinci. Bab ini bertujuan memberikan gambaran yang jelas tentang proses penelitian analisa serangan *Blackhole* yang dilakukan.

Bab IV KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan kesimpulan dari sistem yang telah dibangun dan saran-saran yang diperoleh dari hasil penelitian. Saran-saran ini dapat digunakan sebagai panduan dalam pengembangan simulasi serangan *Blackhole* pada jaringan VANET.