**ANALISA SERANGAN *BLACKHOLE*   
PADA JARINGAN VANET**

SKRIPSI



Disusun oleh :

**Indra Setyo Wibowo**

**20190140077**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH YOGYAKARTA**

**2024**

# HALAMAN PENGESAHAN I

**SKRIPSI**

**ANALISA SERANGAN *BLACKHOLE*   
PADA JARINGAN VANET** 

Disusun oleh :

Indra Setyo Wibowo

20190140077

Telah disetujui oleh :

|  |  |
| --- | --- |
| **Dosen Pembimbing 1** | **Dosen Pembimbing 2** |
|  |
|  |  |  |
|  |  |  |
| **Ir. Asroni, S.T., M.Eng.** | **Dr. Ronald Adrian, S.T., M.Eng.** |  |
| **NIDN : 0516047401** | **NIDN : -** |  |
|  |  |  |

# HALAMAN PENGESAHAN II

**SKRIPSI**

**ANALISA SERANGAN *BLACKHOLE*   
PADA JARINGAN VANET **

Disusun oleh :

Indra Setyo Wibowo

20190140077

Telah dipertahankan di Depan Tim Penguji

Pada Tanggal

Selasa, 20 Agustus 2024

Susunan Tim Penguji :

|  |  |
| --- | --- |
| **Dosen Pembimbing 1** | **Dosen Pembimbing 2** |
|  | |
|  |  |  | |
|  |  |  | |
| **Ir. Asroni, S.T., M.Eng.** | **Dr. Ronald Adrian, S.T., M.Eng.** |  | |
| **NIDN : 0516047401** | **NIDN :** |  | |
|  |  |  | |
| **Dosen Penguji** | | |  | |
|  | |
|  |  |  | |
|  |  |  | |
| **-** | | |  | |
| **NIDN : -** | | |  | |

Skripsi ini telah dinyatakan sah sebagai salah satu persyaratan

Untuk memperoleh gelar Sarjana Komputer

Tanggal, 20 Agustus 2024

|  |
| --- |
| Mengesahkan, |
| Kepala Program Studi Teknologi Informasi |
|  |
|  |
| **Dr. Reza Giga Isnanda, S.T., M.Sc.** |
| **NIDN : 0503068601** |

# DAFTAR ISI

[HALAMAN PENGESAHAN I i](#_Toc174553297)

[HALAMAN PENGESAHAN II ii](#_Toc174553298)

[DAFTAR ISI iii](#_Toc174553299)

[DAFTAR TABEL v](#_Toc174553300)

[DAFTAR GAMBAR vi](#_Toc174553301)

[DAFTAR SINGKATAN vii](#_Toc174553302)

[INTISARI viii](#_Toc174553303)

[ABSTRACT ix](#_Toc174553304)

[BAB I. PENDAHULUAN 1](#_Toc174553305)

[**1.1.** **Latar Belakang** 1](#_Toc174553306)

[**1.2.** **Rumusan Masalah** 4](#_Toc174553307)

[**1.3.** **Batasan Masalah** 4](#_Toc174553308)

[**5.1.** **Tujuan Tugas Akhir** 4](#_Toc174553309)

[**5.2.** **Manfaat Tugas Akhir** 5](#_Toc174553310)

[**5.3.** **Sistematika Penulisan** 5](#_Toc174553311)

[Bab I Pendahaluan 5](#_Toc174553319)

[Bab II TINJAUAN PUSTAKA DAN LANDASAN TEORI 5](#_Toc174553320)

[Bab III METODOLOGI PENELITIAN 5](#_Toc174553321)

[Bab IV HASIL DAN PEMBAHASAN 6](#_Toc174553322)

[Bab IV KESIMPULAN DAN SARAN 6](#_Toc174553323)

[BAB II TINJAUAN PUSTAKA DAN DASAR TEORI 7](#_Toc174553324)

[**2.1** **Tinjauan Pustaka** 7](#_Toc174553328)

[**2.2** **Dasar Teori** 9](#_Toc174553329)

[**2.3** **Analisis perbandingan metode** 12](#_Toc174553330)

[**BAB III. METODE TUGAS AKHIR** 13](#_Toc174553331)

[**3.1** **Metode Penelitian** 13](#_Toc174553337)

[**3.2** **Alat dan Bahan Tugas akhir** 13](#_Toc174553338)

[**3.1.** **Alat Tugas akhir** 13](#_Toc174553343)

[**3.3** **Alat dan Bahan Tugas akhir** 13](#_Toc174553344)

[**3.4** **Alur Tugas akhir** 14](#_Toc174553348)

[**3.5** **Alur Tugas akhir** 18](#_Toc174553349)

[**BAB IV. HASIL DAN PEMBAHASAN** 25](#_Toc174553350)

[**4.1** **Pembahasan Hasil RO-1 (Ubah Sesuai dengan Hal Yang hendak dibahas)** 25](#_Toc174553355)

[**8.1.1.** **Data 1** 25](#_Toc174553360)

[**8.1.2.** **Data 2** 25](#_Toc174553361)

[**4.2** **Pembahasan Hasil RO-2 (Ubah sesuai dengan Hal yang hendak dibahas)** 25](#_Toc174553362)

[**4.3** **Tinjauan Hasil Tugas akhir dibanding dengan Tugas akhir Terdahulu** 25](#_Toc174553363)

[**BAB V. KESIMPULAN DAN SARAN** 26](#_Toc174553364)

[**5.1** **Kesimpulan** 26](#_Toc174553366)

[**5.2** **Saran** 26](#_Toc174553367)

[**DAFTAR PUSTAKA** 27](#_Toc174553368)

[**LAMPIRAN** 30](#_Toc174553369)

# DAFTAR TABEL

[Table 1. 1 Contoh Tabel 6](#_Toc46401127)

# DAFTAR GAMBAR

[Gambar 1.1 Contoh Gambar Diambil Dari Website (Tashia, 2017) 2](#_Toc46401152)

# DAFTAR SINGKATAN

|  |  |
| --- | --- |
| **C** |  |
| *Challenge* | Bagian *gameplay* yang menjelaskan tantangan atau halangan apa saja yang terdapat didalam *game* yang dimainkan |
| Construct2 | *Tools* pembuat *game* yang dibuat oleh Scirra berbasis HTML5 untuk *platform* 2D |
| **G** |  |
| *Game* | Aktifitas bermain yang dilakukan dalam konteks berpura-pura namun terlihat seperti realitas, yang mana pemainnya memiliki tujuan untuk mendapatkan satu kemenangan serta dilakukan sesuai dengan aturan permainan yang telah dibuat |
| *Game Asset* | Elemen-elemen penyusun *game* seperti *art* (gambar), *sound* (musik), *program (behavior)* |
| *Game Design* | Proses mengimajinasikan suatu ide *game*, mendefinisikan bagaimana suatu *game* bekerja, mendeskripsikan elemen-elemen yang membangun *game* |

Note : Jika Ada

# INTISARI

Intisari ditulis menggunakan bahasa Indonesia dengan jarak antar baris 1 spasi dan maksimal 1 halaman. Intisari sekurang-kurangnya berisi penjelasan apa masalah atau fenomena yang hendak dikaji, mengapa masalah atau tugas akhir penting dilakukan, tujuan tugas akhir, metode tugas akhir yang digunakan, dan hasil penting tugas akhir. Intisari dapat ditulis dalam beberapa paragraf. Baris pertama paragraph harus menjorok ke dalam sekitar 1 cm.

Kata Kunci ditulis maksimal 5 kata dan minimal 3 kata yang paling berhubungan dengan isi tugas akhir. untuk pembuatan referensi, silahkan mengacu pada APA Style Journal Article Reporting Standards (APA Style JARS) <https://apastyle.apa.org/jars>. Semua kata dalam bahasa asing harus cetak miring.

Kata kunci : Kata kunci 1, Kata kunci 2, Kata kunci 3, Kata kunci 4, Kata kunci 5

# ABSTRACT

*Abstract ditulis italic (miring) menggunakan bahasa Inggris dengan jarak antar baris 1 spasi dan maksimal 1 halaman. Abstract sekurang-kurangnya berisi research background (penjelasan mengapa tugas akhir penting dilakukan), objective (tujuan tugas akhir), method (cara tugas akhir), dan important results (hasil penting tugas akhir). Abstract dapat ditulis dalam beberapa paragraf. Baris pertama paragraph harus menjorok ke dalam sekitar 1 cm. Tidak disarankan menggunakan mesin penerjemah melainkan tulis ulang.*

*Kata Kunci ditulis maksimal 5 kata dan minimal 3 kata yang paling berhubungan dengan isi tugas akhir. untuk pembuatan referensi, silahkan mengacu pada APA Style Journal Article Reporting Standards (APA Style JARS)* [*https://apastyle.apa.org/jars*](https://apastyle.apa.org/jars)*.*

*Kata kunci : Kata kunci 1, Kata kunci 2, Kata kunci 3, Kata kunci 4, Kata kunci 5*

# BAB I. PENDAHULUAN

* 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 Networks (*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 Networks* (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)

Sedangakan, untuk *Vehicular Ad hoc Networks* (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 Networks* (MANET) dan *Vehicular Ad hoc Networks* (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. **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. **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. **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. **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. **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.

# BAB II TINJAUAN PUSTAKA DAN DASAR TEORI

3. 1. **Tinjauan Pustaka**

Pada penelitian yang sudah dilakukan oleh beberapa peneliti tentang serangan *Blackhole* menjadikan menjadi salah satu bahan yang digunakan sebagai referensi dan Alasan dilakukannya penelitian ini. Pada bagian ini peneliti menggambarkan bagaimana peneliti melakukan penelitian di tempat yang berbeda dan dalam kasus yang berbeda.

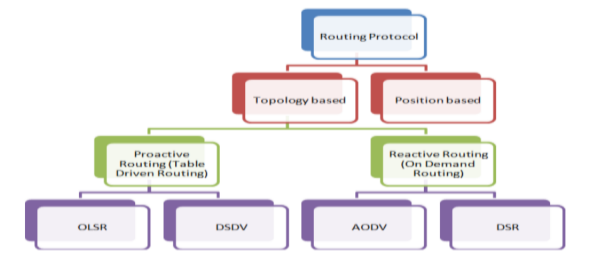
Dalam penelitian yang dilakukan oleh (Singh et al., 2019) dengan judul “*A tutorial survey on vehicular communication state of the art, and future research directions*”. Disebutkan bahwa komunikasi antar kendaraan dilakukan melalui metode Vehicle-to-Vehicle (V2V). Komunikasi V2V ini bersifat sepenuhnya ad hoc, memungkinkan kendaraan untuk berinteraksi tanpa infrastruktur tetap. Mode komunikasi tersebut dikenal sebagai Vehicular Ad-hoc Network (VANET) atau Inter-vehicle Communication (IVC). Ketika dua kendaraan berada dalam jangkauan komunikasi satu sama lain, mereka dapat berkomunikasi langsung tanpa perantara. Namun, jika kendaraan-kendaraan tersebut berada di luar jangkauan satu sama lain, mereka menggunakan metode komunikasi multi-hop. Dalam komunikasi multi-hop, data diteruskan melalui satu atau lebih kendaraan lain hingga mencapai tujuan. Pendekatan ini memastikan kontinuitas dan efisiensi dalam transfer data di antara kendaraan. Penelitian ini menyoroti pentingnya V2V dalam mendukung komunikasi yang efektif dalam lingkungan VANET. Sistem ini memainkan peran kunci dalam jaringan ad-hoc, khususnya dalam skenario mobilitas tinggi. Dengan ini dapat memungkin menggunakan komunikasi antar kendaraan menggunakan Vehicle-to-Vehicle pada penelitian ini.

Penelitian yang dilakukan oleh peneliti (Sindhwani et al., 2022) dengan judul penelitian “*Improvisation of optimization technique and AODV routing protocol in VANET*”. Peneliti ini menggunakan Vehicular Adhoc Network (VANET) untuk merancang sebuah jaringan protokol Ad Hoc On-Demand Distance Vector (AODV). Pada penelitian ini VANET digunakan untuk membantu dalam menyebarkan informasi dari satu *node* ke *node* kendaraan lainnya. Terdapat perbedaan antara jaringan ad-hoc tradisional dan *node routing* di VANET karena topologi yang digunakan sangat dinamis dibandingkan dengan yang digunakan pada jaringan ad-hoc tradisional. Pada jurnal ini peneliti menjelaskan tentang struktur VANET. Penelitian ini memiliki konteks yang serupa dalam menentukan protokol jaringan. Pada penelitian ini menggunakan node routing node ke node yang lain pada jaringan vanet.

Penelitian yang dilakukan oleh(Naim & Hossain, 2019). memanfaatkan VANET sebagai basis karena kemampuannya mendukung berbagai protokol jaringan. Beberapa protokol yang didukung oleh VANET antara lain AODV, DSDV, TORA, dan DSR. Selain itu, protokol lain seperti VADD, GEOpps, GEOcast, GPSR, dan GRANTS juga dapat diimplementasikan dalam jaringan ini. Pemilihan VANET sebagai platform utama memungkinkan fleksibilitas dalam eksperimen dan simulasi jaringan. Dalam konteks penelitian ini, peneliti memfokuskan penggunaan pada protokol AODV. AODV, atau Ad-hoc On-Demand Distance Vector, dipilih karena karakteristiknya yang sesuai untuk jaringan ad-hoc. Penggunaan protokol ini diharapkan dapat memberikan hasil yang optimal dalam skenario yang diteliti. Penelitian ini digunakan untuk memilih VANET dikarena dapat mendukung protokol jaringan yang akan digunakan pada penelitian ini. Pada penelitian ini protokol jaringan yang digunakan yaitu AODV.

Referensi yang digunakan dalam penelitian ini termasuk judul "*AODV-DSR Hybrid Reactive Routing Protocol and its Generalization for Mobile Ad-Hoc Networks*". (Biswas & Dasgupta, 2019) Artikel ini membahas penggabungan protokol routing AODV dan DSR dalam jaringan ad-hoc bergerak, serta generalisasinya untuk berbagai skenario jaringan. Dalam artikel tersebut, dijelaskan bahwa protokol AODV memperkenalkan paket baru yang dikenal sebagai RREQ untuk mentransfer data secara efisien. Penggunaan Probabilitas Bayesian dalam protokol ini memungkinkan perhitungan jumlah node yang terlibat antara sumber dan tujuan dengan akurat. Dengan cara ini, kebutuhan untuk mentransmisikan ulang paket dapat dikurangi secara signifikan. Selain itu, metode ini membantu menurunkan volume lalu lintas secara keseluruhan, mengurangi beban jaringan. Pengurangan kebutuhan transmisi ulang paket juga berkontribusi pada penurunan konsumsi energi dalam jaringan. Artikel ini menjelaskan bagaimana pendekatan ini mengoptimalkan perutean, mengurangi biaya perutean hingga tingkat minimum. Generalisasi protokol ini untuk berbagai skenario jaringan memastikan fleksibilitas dan efisiensi dalam aplikasi jaringan ad-hoc yang berbeda. Ini memberikan wawasan berharga tentang cara meningkatkan performa dan efisiensi routing dalam konteks mobilitas tinggi.

Pada penelitian yang dilakukan oleh peniliti (Upadhyaya & Shah, 2019) pada penelitian dengan judul *attack vanet* pada peneltian ini untuk efisiensi dari *node routing* protokol terdapat beberapa yang diusulkan oleh penulis, penulis menyertakan topology *node routing protocol* untuk menginformasikan tentang penulisannya. *Node routing* protocol berbasis topologi ini dapat dikategorikan menjadi 2 sub kategori, *Poractive Node routing* dan *Reactive Node routing*.



Gambar 2 topology *node routing* protocol

Pada penelitian ini penulis menggunakan AODV protocol *node routing*. AODV protocol *node routing* merupakan *reactive node routing protocol*. pada implementasi nya AODV digunakan untuk memanajemen *route* dengan menggunakan mekanisme <RREQ>RREP>.

Dalam penelitian berjudul "*Design and Implementation of VANET in Ad Hoc Network using MATLAB*,"(Kuthe et al., 2022) penulis memanfaatkan bahasa pemrograman MATLAB serta lingkungan komputasi numerik *multiparadigma* untuk membangun dan menganalisis sistem VANET. MATLAB menyediakan kemampuan untuk membuat antarmuka pengguna kustom dan mengintegrasikan dengan program lain, sambil mendukung kalkulasi matriks dan implementasi algoritme. Dengan MATLAB, peneliti dapat mengembangkan model mobilitas VANET dan memperbarui posisi kendaraan (*node*) setiap detik. Penelitian ini menekankan bahwa penggunaan MATLAB dalam simulasi dapat meningkatkan akurasi dan efektivitas sistem, khususnya dalam konteks protokol AODV dan penanganan serangan *blackhole*. Studi ini relevan dengan kebutuhan penelitian ini karena kabutuhan yang peneliti ini memanfaatkan MATLAB sebagai bahasa pemograman dan lingkungan komputasi numerik yang sangat sesuai dengan kebutuhan analisis dan pengembangan sistem VANET.

Dalam penelitian yang dilakukan oleh (Oberoi, 2020) dengan judul “Enhancement of QoS in Security Algorithm for Blackhole Attack in VANET” di jelaskan bahwa Serangan lubang hitam adalah salah satu bentuk dari serangan Denial of Service yang bertujuan untuk merusak komunikasi antar node atau kendaraan dalam jaringan VANET. Dalam konteks protokol routing AODV, serangan ini bekerja dengan cara mengganggu proses pencarian jalur. Ketika sebuah node sumber atau kendaraan menginisiasi pencarian jalur dengan mengirimkan pesan Route Request (RREQ), node jahat memanipulasi sistem dengan memberikan informasi jalur yang salah. Node jahat ini secara curang mengiklankan bahwa mereka memiliki jalur tercepat atau paling optimal ke tujuan dengan mengirimkan Route Reply (RREP) palsu yang menunjukkan jumlah hop yang paling sedikit atau nomor urut (sequence number) tertinggi. Hal ini membuat node sumber percaya bahwa jalur yang diberikan oleh node jahat adalah yang terbaik, sehingga data yang dikirimkan akan diarahkan melalui node tersebut. Akibatnya, komunikasi terganggu karena data yang masuk ke node jahat tidak akan diteruskan, melainkan dihancurkan, sehingga layanan jaringan terputus. Penelitian ini secara mendalam menganalisis ancaman serangan blackhole dalam jaringan VANET, yang merupakan fokus penting dalam penelitian Anda. Serangan blackhole merupakan salah satu bentuk serangan Denial of Service (DoS) yang sangat merusak, terutama dalam konteks protokol routing AODV yang Anda teliti. Penelitian ini menjelaskan mekanisme serangan blackhole, di mana node jahat memberikan informasi jalur yang salah untuk mengelabui node sumber, sehingga data dikirimkan melalui jalur yang dikuasai oleh penyerang. Hal ini menyebabkan data tidak diteruskan ke tujuan dan malah dihancurkan, mengakibatkan gangguan serius pada komunikasi jaringan.

Dalam penelitian berjudul “Comparative Analysis of Routing Algorithms in SUMO for VANET” yang dilakukan oleh (nama peneliti), SUMO digunakan sebagai alat simulasi untuk jaringan kendaraan VANET. SUMO mendukung berbagai algoritma pencarian rute yang penting untuk memodelkan skenario jalan raya dan perkotaan dengan presisi, sehingga memudahkan peneliti dalam mengevaluasi kinerja berbagai strategi routing. Karena VANET memiliki karakteristik unik, seperti topologi yang cepat berubah, komunikasi yang sering terputus, serta kemampuan komputasi dan penyimpanan yang luas, SUMO memungkinkan simulasi yang realistis dan sesuai dengan situasi nyata. Selain itu, biaya menjadi pertimbangan penting dalam penerapan sistem transportasi cerdas, dan SUMO menyediakan platform yang efisien dan ekonomis untuk penelitian ini, menjadikannya pilihan yang menarik bagi peneliti yang ingin menguji dan mengoptimalkan strategi routing dalam konteks VANET.

* 1. **Dasar Teori**
     1. ***VANET***

Vehicular Ad-hoc Network (VANET) merupakan jenis jaringan yang memungkinkan kendaraan berkomunikasi antara satu dengan yang lainnya, serta dengan infrastruktur jalan. Jaringan ini dibentuk dengan menggagas konsep suatu jaringan kendaraan untuk keperluan tertentu atau dalam situasi khusus. Sebagai hasilnya, VANET telah terbukti sebagai jaringan yang dapat diandalkan yang digunakan oleh kendaraan untuk berkomunikasi di jalan raya atau di lingkungan perkotaan.(Kugali & Kadadevar, n.d.)

Dalam vanet terdapat berbagai model komunikasi data telah dikembangkan yang mengusulkan integrasi beragam jenis infrastruktur kendaraan. Bentuk komunikasi ini mencakup Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), serta kombinasi dari keduanya, V2V dan V2I.

1. *Vehicle-to-Vehicle (V2V):* V2V adalah jenis komunikasi langsung antar kendaraan yang memungkinkan mereka bertukar informasi secara real-time. Misalnya, kendaraan dapat saling berbagi data mengenai kondisi jalan, kecepatan, atau bahaya di depan, yang dapat meningkatkan keselamatan dan efisiensi lalu lintas.
2. *Vehicle-to-Infrastructure (V2I):* V2I melibatkan komunikasi antara kendaraan dan infrastruktur jalan raya, seperti lampu lalu lintas, rambu-rambu, atau pusat pengendalian lalu lintas. Komunikasi ini memungkinkan kendaraan menerima informasi yang dapat membantu dalam navigasi dan pengambilan keputusan, seperti perubahan lampu lalu lintas atau kemacetan di depan.
   * 1. ***AODV***

Protokol *node routing* Ad Hoc On-Demand Distance Vector (AODV) merupakan hasil kombinasi dari dua protokol *node routing* lainnya, yaitu Dynamic Source *Node routing* (DSR) dan Destination Sequenced Distance Vector (DSDV). AODV adalah jenis protokol *node routing* on demand yang memanfaatkan mekanisme dari DSR, termasuk Route Discovery dan Route Maintenance, serta melibatkan hop-by-hop *node routing*, periodic beacon, dan menggunakan sequenced numbers yang juga ditemukan pada DSDV.(Assidiq & Nurcahyani, n.d.).

Penelitian ini berfokus pada bagaimana kinerja protokol *node routing* AODV mempengaruhi konsumsi energi dalam jaringan VANET, dengan menggunakan perangkat lunak MATLAB sebagai alat analisis. Dalam konteks ini, AODV digunakan untuk mengatur rute komunikasi antar kendaraan dalam VANET, yang memungkinkan pertukaran informasi secara efisien. Namun, penelitian ini juga mempertimbangkan skenario di mana jaringan AODV terpapar oleh serangan Blackhole, di mana *node* jahat mengelabui *node* sumber dengan memberikan informasi rute yang salah, sehingga menyebabkan data hilang. Penelitian ini bertujuan untuk menganalisis dan membandingkan perbedaan kinerja antara AODV yang beroperasi dalam kondisi normal dan saat mengalami serangan Blackhole. Perbandingan ini mencakup evaluasi terhadap konsumsi energi, yang menjadi salah satu indikator penting dalam menilai efisiensi jaringan VANET. Hasil dari penelitian ini diharapkan dapat memberikan wawasan mengenai dampak serangan Blackhole terhadap performa jaringan, khususnya dalam hal penggunaan energi.

A diagram of a diagram

Description automatically generated

Pada gambar () dijelaskan Terdapat beberapa langkah dalam proses pencarian rute pada protokol komunikasi AODV. Langkah pertama adalah node sumber mengirimkan paket RouteRequest (RREQ) ke node tetangganya. Selanjutnya, jika sebuah node memiliki informasi tentang rute menuju node tujuan, node tersebut akan mengirimkan paket RREP kembali ke node sumber melalui jalur yang terbentuk oleh RREQ. Apabila terdeteksi adanya kerusakan pada rute komunikasi, mekanisme perbaikan rute akan mengirimkan paket routeerror (RERR) ke salah satu node di sepanjang jalur, dan node sumber akan mengirimkan kembali paket RREQ. Node yang menerima RREQ akan memberikan informasi tentang masa aktif rute. Informasi perutean antara node sumber dan node di jalur akan dihapus jika masa aktif rute telah berakhir. Pada gambar 1, merupakan gambar struktur AODV. Penelitian ini digunakan sebagai referensi protokol routing AODV untuk mentransmisikan paket-paket paket RREQ dan RREP.

* + 1. ***Modified sequence number***

Modified sequence number (MSN) adalah konsep yang berhubungan dengan perubahan atau penyesuaian dalam protokol *node routing* AODV. MSN digunakan untuk mendeteksi *node* blackhole yang berbahaya dengan mempertimbangkan nomor urut yang diterima dari *node* berikutnya. Ketika *node* sumber menerima pesan balasan rute (RREP) dengan nomor urut yang mencurigakan, *node* tersebut akan mengirim ulang permintaan rute (RREQ) dengan nomor urut yang telah dimodifikasi untuk mencocokkan nomor urut dari RREP yang diterima sebelumnya. Jika *node* yang menjawab adalah *node* blackhole, ia akan mengirim RREP dengan nomor urut yang lebih tinggi lagi. Penerimaan RREP dengan nomor urut yang lebih tinggi setelah siaran ulang akan mengonfirmasi bahwa *node* tersebut berbahaya, dan rute melalui *node* tersebut harus dihindari. Dengan cara ini, risiko paket yang hilang dapat dikurangi, yang pada akhirnya meningkatkan kinerja jaringan.(Shrestha et al., 2020)

* + 1. ***Blackhole***

*Blackhole* merupakan manipulasi *node* kendaraan untuk memblokir semua paket yang diterimanya, sehingga tidak diteruskan ke *node* kendaraan berikutnya menuju tujuan. Serangan ini memiliki dampak yang signifikan terhadap stabilitas dan kinerja jaringan. Tiga konsekuensi utama dari serangan ini adalah:

1. gangguan pada penerusan paket antar *node* kendaraan,
2. hambatan dalam penerimaan pesan oleh *node* tujuan
3. potensi pembuangan semua paket yang diterima oleh *node* penerima.

Dalam protokol AODV, serangan *blackhole* dapat menyebabkan pemutusan komunikasi dalam jaringan karena paket data tidak pernah mencapai tujuan yang diinginkan. Ini mengurangi keandalan dan efisiensi komunikasi antar kendaraan, yang merupakan salah satu fungsi utama VANET. Untuk mengatasi atau mendeteksi serangan ini, diperlukan modifikasi atau penguatan pada protokol *node routing* yang digunakan, seperti AODV, sehingga dapat mengenali dan menghindari *node* jahat yang terlibat dalam serangan *blackhole*.

Serangan Blackhole dalam jaringan VANET yang menggunakan protokol AODV dapat dijelaskan melalui beberapa langkah berikut:

* *Proses Penemuan Rute:* Ketika sebuah node sumber ingin mengirimkan data ke tujuan, ia memulai proses penemuan rute dengan mengirimkan Route Request (RREQ) ke seluruh jaringan. RREQ ini akan diteruskan oleh node-node yang menerima permintaan tersebut hingga mencapai node tujuan atau node yang dapat memberikan rute ke tujuan.
* *Penawaran Jalur Palsu:* Node Blackhole, yang terletak di jalur yang dilalui RREQ, mengirimkan Route Reply (RREP) palsu ke node sumber. Node Blackhole ini berpura-pura memiliki jalur yang lebih pendek atau lebih baik menuju tujuan dengan menunjukkan nomor urut yang tinggi atau jumlah hop yang sedikit.
* *Pengalihan dan Pemblokiran Data***:** Node sumber, yang menerima RREP palsu, akan memilih jalur yang diklaim sebagai yang terbaik dan mulai mengirimkan data melalui jalur tersebut. Data yang dikirimkan ke node Blackhole tidak diteruskan tetapi dibuang, menyebabkan kehilangan data dan gangguan dalam komunikasi.

Serangan Blackhole memiliki beberapa dampak signifikan pada jaringan, antara lain:

1. Gangguan pada Penerusan Paket: Paket data yang dikirimkan melalui jalur yang mengandung node Blackhole tidak diteruskan ke node berikutnya. Hal ini menyebabkan gangguan pada aliran paket dan mengakibatkan data yang dikirim tidak sampai ke tujuan.
2. Hambatan dalam Penerimaan Pesan oleh Node Tujuan: Node tujuan tidak menerima data yang dikirimkan karena paket-paket tersebut terhenti di node Blackhole. Ini mengakibatkan kegagalan dalam pengiriman pesan yang seharusnya diterima oleh node tujuan.
3. Potensi Pembuangan Paket: Node Blackhole membuang semua paket yang diterimanya tanpa meneruskannya. Hal ini mengurangi efisiensi dan keandalan jaringan, karena data yang penting tidak sampai ke node tujuan yang diinginkan.

Dalam protokol AODV, serangan Blackhole dapat mengakibatkan:

* Pemutusan Komunikasi: Karena paket data tidak pernah mencapai tujuan yang diinginkan, komunikasi antar node terganggu. Ini mengurangi keandalan dan efisiensi jaringan VANET, yang seharusnya memungkinkan pertukaran informasi antar kendaraan dengan lancar.
* Penurunan Kinerja Jaringan: Kehilangan paket dan gangguan komunikasi dapat menyebabkan penurunan keseluruhan kinerja jaringan, meningkatkan latensi, dan mengurangi throughput.

Untuk mengatasi atau mendeteksi serangan Blackhole dalam jaringan VANET yang menggunakan AODV, beberapa strategi dapat diterapkan, seperti:

* **Modifikasi Protokol Routing:** Melakukan perubahan pada mekanisme deteksi dan pengelolaan rute dalam AODV untuk mengenali dan menghindari node jahat.
* **Penguatan Keamanan:** Mengimplementasikan teknik keamanan tambahan seperti otentikasi dan enkripsi untuk memastikan keaslian informasi rute.
* **Metode Deteksi Anomali:** Menggunakan algoritma untuk mendeteksi perilaku yang tidak biasa atau tidak konsisten dalam rute dan mengidentifikasi potensi node Blackhole.

Proses terjadinya serangan *Blackhole* digambarkan sebagai berikut :

A diagram of a flowchart

Description automatically generated

Gambar 4 Proses serangan *Blackhole*

Pada gambar 4 merupakan ilustrasi *blackhole attack* pada jaringan VANET. Serangan blackhole dapat diilustrasikan dengan menunjukkan bahwa node jahat merupakan indikasi utama dari serangan ini. Node jahat cenderung menarik pengirim dengan meyakinkan pengirim tentang adanya jalur yang baru dan lebih pendek. Ada dua metode yang dapat digunakan oleh node jahat untuk melakukan tugas ini: pertama, dengan mengirimkan nomor urut tujuan yang tetap, dan kedua, dengan mengirimkan nomor urut tujuan yang berubah-ubah.(M. Kumar et al., 2019)

* + 1. ***Delay***
    2. Delay adalah waktu yang dibutuhkan untuk mentransfer data dari satu komputer ke komputer lain dalam suatu jaringan. Penyebab utama delay dalam transmisi paket termasuk antrean yang panjang sepanjang rute. Delay juga dapat terjadi ketika paket memilih rute alternatif untuk menghindari kemacetan di jalur utama. Jarak antara pengirim dan penerima turut berkontribusi pada peningkatan delay. Jenis media fisik yang digunakan, seperti kabel atau gelombang radio, dapat mempengaruhi kecepatan dan stabilitas transmisi, yang kemudian menambah delay. Selain itu, delay bisa meningkat karena kongesti atau kepadatan lalu lintas data dalam jaringan. Jika banyak data yang dikirimkan secara bersamaan, paket-paket data mungkin perlu menunggu lebih lama sebelum diproses dan dikirim. Waktu pemrosesan di setiap node juga dapat memperpanjang delay, terutama jika perangkat keras atau perangkat lunak yang digunakan kurang optimal. Semua faktor ini berkontribusi pada total waktu yang dibutuhkan untuk mengirimkan paket data. Dalam beberapa kasus, delay yang tinggi bisa menurunkan kinerja jaringan secara keseluruhan, terutama pada aplikasi yang memerlukan transmisi data secara real-time. Untuk menghitung delay pada paket yang ditransmisikan, dapat dilakukan dengan membagi panjang paket (dalam bit) dengan link bandwidth (dalam bit/s). Sedangkan untuk menghitung rata-rata delay, digunakan rumus tertentu sebagaimana yang tertuang dalam Persamaan (Nazif et al., n.d.).

Kategori dan besar delay berdasarkan standar versi TIPHON.

|  |  |  |
| --- | --- | --- |
| Kategori | Besar Delay | Indeks |
| Sangat bagus | <150 ms | 4 |
| Bagus | 150 – 300 ms | 3 |
| Sedang | 300-450 ms | 2 |
| Buruk | >450 ms | 1 |

* + 1. ***Throughput***

Throughput adalah ukuran bandwidth aktual yang tercatat dalam jangka waktu tertentu selama proses transmisi data. Meskipun satuannya sama dengan bandwidth, yaitu bits per second (bps), throughput memberikan gambaran lebih realistis mengenai bandwidth yang sebenarnya tersedia pada waktu tertentu dan dalam kondisi jaringan tertentu yang digunakan untuk mengunduh file dengan ukuran tertentu. Throughput mencerminkan jumlah total paket yang berhasil diterima di tujuan dalam jangka waktu tertentu, dibagi dengan durasi interval waktu tersebut. Nilai Throughput dapat dihitung menggunakan rumus tertentu.

Ada juga kategori dan indeks throughput berdasarkan standar TIPHON yang dapat digunakan untuk mengukur kinerja jaringan.

|  |  |  |
| --- | --- | --- |
| Kategori | Besar Throghput | Indeks |
| Sangat bagus | 100 bps | 4 |
| Bagus | 75 bps | 3 |
| Sedang | 50 bps | 2 |
| Buruk | 25 bps | 1 |

\

* 1. **Analisis perbandingan metode**

Analisis yang akan dilakukan dalam tugas akhir ini adalah analisis kuantitatif. Metode kuantitatif dipilih untuk mendapatkan pemahaman yang lebih terukur mengenai dampak jumlah kendaraan terhadap kinerja jaringan, dengan menggunakan studi kasus di wilayah RS. PKU Muhammadiyah Yogyakarta. Pemilihan metode ini didasarkan pada kebutuhan untuk mengumpulkan dan menganalisis data numerik yang dapat memberikan informasi yang lebih objektif.

Pendekatan kuantitatif adalah metode penelitian yang mengandalkan data numerik dan prinsip-prinsip ilmiah untuk menjawab hipotesis. Dalam pendekatan ini, informasi yang dikumpulkan berupa angka dan statistik. Data-data tersebut digunakan untuk menganalisis fenomena secara objektif. Pendekatan ini memfokuskan pada pengukuran yang tepat dan analisis yang dapat menghasilkan temuan yang terukur.(Waruwu, 2023)

Metode pelaksanaan tugas akhir ini mencakup penggunaan dua alat utama: Simulation of Urban MObility (SUMO) dan Vehicular Ad-hoc NETworks (VANET). SUMO adalah simulator lalu lintas yang memungkinkan pemodelan dan analisis pergerakan kendaraan di area perkotaan. Di sisi lain, VANET adalah jaringan ad hoc yang memungkinkan kendaraan untuk saling berkomunikasi serta berinteraksi dengan infrastruktur jaringan.

Dengan menerapkan metode kuantitatif ini, diharapkan tugas akhir dapat memberikan pemahaman yang lebih mendalam mengenai dampak jumlah kendaraan terhadap kinerja jaringan di wilayah RS. PKU Muhammadiyah Yogyakarta. Metode kuantitatif menawarkan keuntungan berupa data yang dapat diukur dan dianalisis secara statistik, yang memungkinkan peneliti untuk memperoleh wawasan yang lebih objektif dan dapat dipertanggungjawabkan tentang hubungan antara jumlah kendaraan dan kinerja jaringan. Selain itu, penelitian ini juga mencakup analisis AODV dalam konteks VANET untuk menambah pemahaman tentang performa jaringan dalam situasi yang dinamis.

Berikut adalah kelebihan dan kekurangan metode kuantitatif dalam konteks penelitian, beserta penjelasan spesifik untuk penelitian ini:

Kelebihan metode kuantitatif

1. **Objektivitas**: Metode kuantitatif menghasilkan data yang objektif dan terukur karena menggunakan angka dan analisis statistik. Ini memungkinkan peneliti untuk menarik kesimpulan yang kuat berdasarkan fakta dan bukti yang dapat diperiksa dan diverifikasi.
2. **Replikasi**: Metode ini memudahkan peneliti lain untuk mengulang studi dengan metode yang sama untuk memverifikasi hasilnya. Dengan demikian, kevalidan dan kepercayaan terhadap temuan penelitian dapat ditingkatkan.
3. **Generalisasi**: Penelitian kuantitatif memungkinkan hasil penelitian untuk digeneralisasikan ke populasi yang lebih luas. Data yang dikumpulkan dapat mencerminkan kondisi yang lebih umum dan memberikan wawasan yang lebih luas tentang efek variabel yang diteliti, seperti jumlah kendaraan terhadap kinerja jaringan.

Kekurangan Metode Kuantitatif:

1. **Keterbatasan dalam Pengumpulan Data**: Metode kuantitatif bergantung pada data numerik yang dapat diukur. Terkadang, pengumpulan data yang diperlukan dapat sulit dilakukan, atau data yang tersedia mungkin tidak lengkap atau kurang akurat.
2. **Pengabaian Aspek Kualitatif**: Metode ini cenderung fokus pada angka dan hasil yang dapat diukur, yang mungkin mengabaikan aspek kualitatif yang penting. Informasi seperti preferensi pengguna, persepsi, atau faktor sosial mungkin tidak sepenuhnya tercakup dalam analisis kuantitatif.

Pengumpulan dan Analisis Data Numerik: Metode kuantitatif memungkinkan penelitian ini untuk mengumpulkan dan menganalisis data numerik mengenai jumlah kendaraan dan kinerja jaringan secara terukur.

Dalam tugas akhir penelitian ini yang menggunakan MATLAB untuk menganalisis VANET AODV dengan Blackhole Attack, metode kuantitatif dipilih karena:

* **Pengumpulan dan Analisis Data Numerik**: Metode kuantitatif memungkinkan penelitian untuk mengumpulkan dan menganalisis data numerik tentang jumlah kendaraan dan kinerja jaringan dengan cara yang terukur.
* **Simulasi Menggunakan SUMO dan VANET**: Dengan SUMO untuk simulasi lalu lintas dan VANET untuk model jaringan, penelitian dapat menghasilkan data yang dibutuhkan untuk analisis kuantitatif. Ini memungkinkan pemodelan kondisi lalu lintas secara spesifik dan analisis mendalam dari hasil simulasi.
* **Pemahaman yang Lebih Mendalam**: Metode kuantitatif diharapkan memberikan pemahaman yang lebih mendalam mengenai dampak jumlah kendaraan terhadap kinerja jaringan di wilayah RS. PKU Muhammadiyah Yogyakarta, serta efek AODV dan serangan Blackhole pada jaringan vehikular.

**BAB III.  
METODE TUGAS AKHIR**

5. 1. **Metode Penelitian**

Metode penelitian merupakan aspek fundamental dalam pelaksanaan sebuah studi, berfungsi sebagai dasar untuk mencapai tujuan penelitian secara efektif. Dalam tugas akhir ini, pendekatan yang digunakan adalah metode kuantitatif untuk mengevaluasi dampak jumlah kendaraan terhadap kinerja jaringan di Wilayah RS. PKU Muhammadiyah Yogyakarta. Penelitian ini memanfaatkan SUMO (Simulation of Urban MObility) dan VANET (Vehicular Ad-hoc Network) untuk mengembangkan model simulasi yang mencerminkan kondisi lalu lintas di area tersebut. Data yang diperoleh dari simulasi akan dianalisis secara kuantitatif untuk memberikan pemahaman yang terukur dan objektif tentang bagaimana variasi jumlah kendaraan mempengaruhi performa jaringan. Penjelasan berikut akan menguraikan dengan lebih rinci tentang alat dan bahan yang digunakan serta tahapan yang akan diikuti dalam penelitian ini.

* 1. **Alat dan Bahan Tugas akhir**

3. **Alat Tugas akhir**

Alat yang digunakan berupa perangkat keras (hardware) dan perangkat lunak (software).

1. Perangkat keras (*Hardware*)
2. Interl® Core™ i7 9750-H *processor*,
3. 8.00 GB RAM,
4. 64 -bit *Operating System,*
5. Windows 11 pro.
6. Perangkat lunak (Soft*ware*)
   1. Matrix Lab (MATLAB),
   2. Windows Operating System,
   3. Microsoft .Excel
7. **Bahan**

Data survei lapangan merupakan informasi yang dikumpulkan secara langsung dari lapangan untuk memberikan gambaran akurat mengenai kondisi nyata di area penelitian. Dalam konteks tugas akhir ini, bahan survei lapangan meliputi:

* Data Jumlah Kendaraan:
  + Sumber Data

Data ini diperoleh dari pengamatan langsung di area sekitar RS. PKU Muhammadiyah Yogyakarta.

* + Rincian Data

Termasuk total jumlah kendaraan yang lewat, frekuensi kedatangan kendaraan, serta jam-jam sibuk dan sepi.

* + Tujuan  
    Memahami volume lalu lintas dan pola pergerakan kendaraan di wilayah tersebut, yang akan membantu dalam analisis bagaimana pergerakan kendaraan memengaruhi performa dan efisiensi jaringan VANET.
* Data sekunder

Data sekunder adalah informasi yang diperoleh dari sumber yang sudah ada sebelumnya dan relevan untuk analisis. Dalam konteks ini, data sekunder meliputi: Data Lalu Lintas: Jalur dan Rute: Informasi mengenai jalur-jalur utama dan alternatif di sekitar RS. PKU Muhammadiyah Yogyakarta, termasuk tata letak jalan, rute utama, dan area yang sering macet. Lama Waktu Lalu Lintas: Data mengenai durasi perjalanan rata-rata di berbagai jalur, waktu puncak, dan pergerakan lalu lintas yang mungkin menunjukkan pola atau masalah yang dapat mempengaruhi performa sistem VANET.

|  |  |
| --- | --- |
| **Parameter** | **Value** |
| Jumlah Kendaraan | 100 per *lane* |
| Jenis Kendaraan | Mobil, Taxi |
| Kecepatan Maksimum | 140 km/jam |
| *Traffic Light* | Ada |
| Protokol Komunikasi | V2I, V2V |
| Model Propagasi | *Free Space Path Loss* (FSPL) |
| *Path Loss Model* | *Free Space Path Loss* (FSPL) |
| Durasi Simulasi | 120 s |
| Frekuensi Operasi | 5.9 Ghz |
| Algoritma Pemilihan Jalur | *Ad Hoc On-Demand Distance Vector* (AODV), *Dynamic Source Routing* (DSR) |

2. 2. **Alur Tugas akhir**

Pada bagian ini, dijelaskan mengenai langkah-langkah yang diambil oleh penulis dalam menyelesaikan penelitian ini. Berikut pembahasan alur penelitian melalui beberapa alur.

A diagram of a program

Description automatically generated

Gambar 5 Alur Pembuatan Penelitian

* + 1. Tinjauan Pustaka

Pada tahap tinjauan pustaka, penulis melakukan observasi terkait penelitian sebelumnya dengan cara memperlajari dan memahami metode-metode pada *Ad hoc On-Demand Distance Vector Node routing* (AODV) dan serangan *Blackhole.* Penulis dapat mempelajari dengan mendalam tentang AODV dan serangan Blachole pada literatur penelitian sebelumnya.

* + 1. Pengumpulan Data

Pada tahap pengumpulan data, penulis melakukan pengumpulan data pada implementasi dari jalur jalanan yang berada di RS. PKU Yogyakarta. Data yang didapati menggunakan jalur dari citra *maps* yang diimplementasikan sebagai desain jalur AODV.



Gambar 6 peta jalur rute AODV

* + 1. Implementesi AODV *Node routing* Protocol

Pada tahap ini, merupakan tahap yang dilakukan ketika penulis sudah mengumpulkan data dengan valid. Penulis akan mengimplementasi kan simulasi menggunakan data yang sudah dikumpulkan sebelumnya.

* + 1. Membuat Program Simulasi

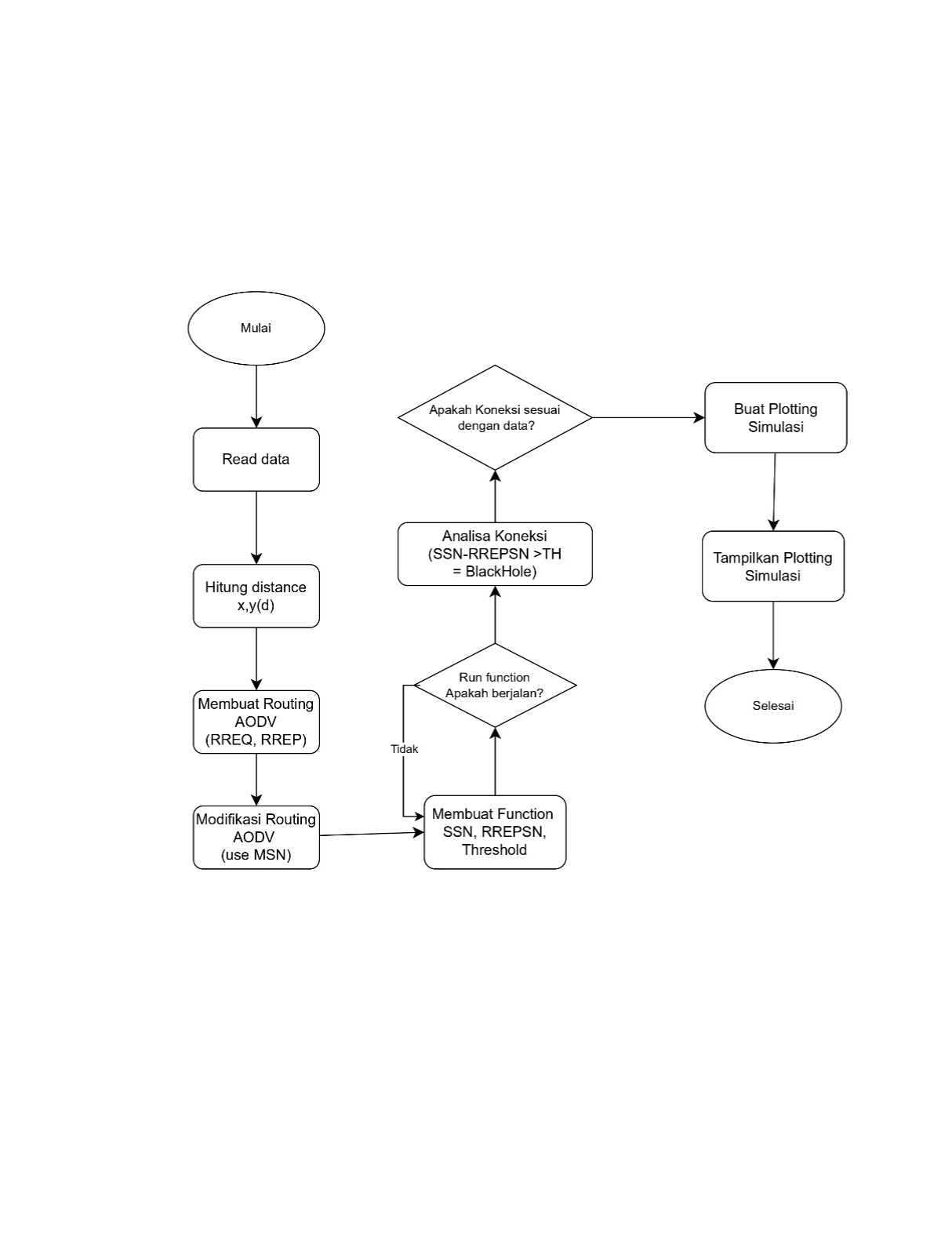
Tahap ini, merupakan tahap dari implementasi data yang sudah dikumpulkan untuk diterjemahkan menggunakan program simulasi AODV. Pada tahap ini penulis melakukan *run* pada program, apakah program sudah sesuai dengan data yang sudah ditentukan sebelumnya atau belum?. Pada simulasi ini data-data yang dikumpulkan di implementasikan dengan *node*-*node* kendaraan yang melintas pada jalur tersebut. Pada tahap ini peneliti membuat jaringan koneksi pada *node* berdasarkan data yang telah dikumpulkan

* + 1. Memberi Serangan

Pada tahap ini, setelah peneliti membuat program simulasi AODV dengan benar dan sesuai, selanjutnya peneliti memberikan serangan *Blackhole* pada *node* yang ditentukan oleh peneliti. pada program ini peneliti menentukan serangan AODV menggunakan perbandingan jumlah SSN (source sequence number) dan Reply Sequence Number. Dengan perbandingan ini peneliti menggunakan threshold untuk memberi ambang batas jumlah sequence

* + 1. Analisa Hasil Simulasi
    2. Menampilkan Hasil
    3. Menyusun Laporan
  1. **Alur Program Tugas akhir**

Bagian ini menguraikan langkah-langkah yang ditempuh oleh penulis dalam menyelesaikan penelitian ini. Berikut adalah pembahasan mengenai alur program penelitian yang disusun melalui beberapa tahapan.



1. Read data

Pada tahap ini, data yang dibutuhkan untuk simulasi diperoleh dari *file* sumber, seperti *file* Excel atau *file* sejenis yang menyimpan informasi mengenai *node* dalam jaringan. *File* tersebut menyediakan data penting yang digunakan dalam proses simulasi. Data ini mencakup berbagai informasi terkait karakteristik dan kondisi *node*. Informasi yang tersedia memastikan bahwa setiap aspek penting dari *node* dalam jaringan tercakup. Dengan data tersebut, simulasi dapat berjalan sesuai dengan skenario yang diinginkan. Data ini mencakup informasi penting seperti:

1. Posisi *node*

Posisi *node* adalah koordinat geografis atau posisi dalam ruang simulasi di mana *node* berada pada titik waktu tertentu. Dalam konteks jaringan ad-hoc atau VANET, posisi ini biasanya diberikan dalam bentuk koordinat *Cartesian* (x, y) dalam suatu area simulasi.

1. Waktu

Waktu mencatat kapan peristiwa tertentu terjadi dalam simulasi. Ini bisa berupa waktu simulasi yang sebenarnya atau waktu relatif dalam simulasi.

1. *Id* *node*

Ide *node* adalah identifikasi unik untuk setiap *node* dalam jaringan. Ini penting untuk membedakan *node* satu dengan yang lainnya, terutama dalam proses *node routing* dan manajemen jaringan.

1. Hitung distance

Pada tahap ini, dilakukan perhitungan jarak antara setiap pasangan *node* dalam jaringan. Perhitungan jarak menggunakan rumus Euclidean yang dinyatakan sebagai:

Jarak(d)=(x2​−x1​)2+(y2​−y1​)2

dengan menggunakan posisi (x, y) yang telah dibaca sebelumnya. Jarak ini penting untuk menentukan apakah dua *node* dapat berkomunikasi langsung satu sama lain. Berdasarkan hasil perhitungan, akan diketahui apakah *node*-*node* tersebut berada dalam jangkauan komunikasi langsung. Ini membantu dalam menentukan konektivitas dan pengaturan rute dalam simulasi jaringan. Perhitungan ini bertujuan untuk mendukung proses *node routing*.

1. Membuat *Node routing* AODV

Pada tahap ini, diimplementasikan protokol *node routing* AODV, yang merupakan protokol dinamis untuk jaringan ad-hoc. Proses utama yang dilakukan meliputi:

1. Permintaan Rute (RREQ): *Node* yang memerlukan rute mengirimkan permintaan ke seluruh jaringan untuk mencari jalur menuju *node* tujuan.
2. Respon Rute (RREP): Setelah rute ditemukan, *node* tujuan mengirimkan respons kembali ke *node* asal dengan informasi tentang rute terbaik yang tersedia.
3. Pemeliharaan Rute: Rute akan diperbarui atau dibatalkan jika terjadi perubahan dalam jaringan, seperti pergerakan *node* yang keluar dari jangkauan.

Hal ini membantu untuk mengatur komunikasi antara *node* dengan cara menemukan dan mempertahankan rute yang optimal.

1. Modifikasi *Node routing* AODV

Setelah implementasi dasar protokol *node routing* AODV selesai, berbagai modifikasi dapat dilakukan untuk meningkatkan kinerja atau menyesuaikan dengan kebutuhan spesifik. Misalnya:

1. Optimasi Rute: Mengurangi overhead dan mempercepat proses pencarian rute untuk efisiensi yang lebih baik.
2. Penambahan Fitur Keamanan: Menambahkan mekanisme untuk mendeteksi dan mencegah serangan Blackhole dalam jaringan.
3. Penanganan *Node* yang Bergerak Cepat: Menyesuaikan AODV untuk beroperasi secara efektif dalam kondisi jaringan dengan mobilitas tinggi, seperti dalam VANET.

Tujuan dari modifikasi ini adalah untuk meningkatkan efisiensi dan keamanan *node routing* AODV dalam berbagai situasi jaringan.

1. Membuat Function SSN, RREPSN, Threshold

1. SSN (*Source Sequence Number*)

* Definisi: SSN adalah angka urut yang digunakan dalam protokol *node routing* untuk melacak pesan dan memastikan urutan yang benar dalam transmisi data. SSN membantu untuk mengidentifikasi pesan yang lebih baru dan memastikan bahwa tidak ada pesan yang hilang atau duplikat.
* Penggunaan: Dalam *node routing* AODV (*Ad hoc On-Demand Distance Vector*), setiap pesan kontrol seperti *Route Request* (RREQ) dan *Route Reply* (RREP) memiliki SSN. *Node* yang menerima pesan dapat menggunakan SSN untuk menentukan apakah pesan tersebut adalah yang terbaru dan valid.

2. RREPSN (Route Reply Sequence Number)

* Definisi: RREPSN adalah angka urut yang digunakan dalam proses Route Reply untuk memvalidasi rute yang diterima. RREPSN memastikan bahwa *node* yang menerima RREP dapat memverifikasi dan memilih rute yang lebih baru dan lebih optimal.
* Penggunaan: RREPSN dalam pesan RREP membantu menentukan apakah rute yang diterima adalah yang terbaru. *Node* tujuan dalam AODV akan membandingkan RREPSN dari berbagai RREP yang diterimanya untuk memilih rute yang terbaik.

3. Threshold (Ambang Batas)

Definisi: Threshold adalah nilai ambang yang digunakan untuk memutuskan apakah sebuah rute atau *node* masih valid atau perlu diperbarui. Ini sering digunakan dalam perhitungan kinerja untuk memastikan bahwa *node* atau rute yang memiliki metrik atau nilai di bawah ambang batas dianggap tidak valid atau perlu diperbaiki.

* Penggunaan: Dalam analisis koneksi, threshold digunakan untuk menentukan apakah suatu rute atau *node* harus dianggap sebagai blackhole atau tidak. Jika perbedaan antara SSN dan RREPSN melebihi threshold, rute atau *node* dapat dianggap sebagai blackhole.

Rumus SSN - RREPSN > TH = blackhole

* Rumus: SSN - RREPSN > TH = blackhole
  + SSN: Sequence Sequence Number, angka urut dari pesan.
  + RREPSN: Route Reply Sequence Number, angka urut dari rute balasan.
  + TH: Threshold, nilai ambang batas.

1. Analisa koneksi

Pada tahap ini, konektivitas jaringan dianalisis menggunakan data yang dikumpulkan dari simulasi. Beberapa analisis yang dilakukan termasuk:

* Validasi Rute: Memeriksa apakah rute yang ditemukan masih valid berdasarkan SSN dan RREPSN.
* Deteksi *Node* yang Terputus: Menentukan apakah ada *node* yang keluar dari jangkauan atau tidak lagi dapat dihubungi.
* Evaluasi Kinerja Jaringan: Misalnya, berapa banyak rute yang valid, berapa banyak yang gagal, dan bagaimana kinerja jaringan secara keseluruhan.

Tujuan: Menilai stabilitas dan kinerja koneksi jaringan.

1. Buat plotting Simulasi

Setelah analisis selesai, hasil simulasi divisualisasikan. Plotting dapat mencakup:

* Jaringan *Node*: Representasi visual dari *node* dan rute yang terbentuk di antara mereka.
* Status *Node*: Warna atau simbol yang berbeda untuk menunjukkan status *node* (misalnya, hijau untuk terhubung, merah untuk terputus).
* Perubahan Jaringan: Bagaimana jaringan berubah dari waktu ke waktu, terutama jika *node* bergerak.

Tujuan: Menyediakan cara visual untuk memahami hasil simulasi dan dinamika jaringan.

1. Tampilkan Plotting simulasi

Tahap akhir adalah menampilkan hasil plotting kepada pengguna. Ini dapat dilakukan dalam bentuk grafik atau animasi yang menunjukkan perkembangan jaringan dari waktu ke waktu.

Hal ini bertujuan untuk menyampaikan hasil simulasi secara visual agar lebih mudah dipahami dan dianalisis.

**BAB IV.  
HASIL DAN PEMBAHASAN**

4. 1. **Pembahasan Hasil RO-1 (Ubah Sesuai dengan Hal Yang hendak dibahas)**

Poin pertama adalah membahas tujuan tugas akhir pertama (RO-1). Apabila RO menggunakan RQ maka dapat dibuatkan beberapa sub bab yang mendiskusikan masing-masing RQ

2. 1. 1. **Data 1**
      2. **Data 2**
   2. **Pembahasan Hasil RO-2 (Ubah sesuai dengan Hal yang hendak dibahas)**

Poin kedua adalah membahas tujuan tugas akhir pertama (RO-2). Apabila RO menggunakan RQ maka dapat dibuatkan beberapa sub bab yang mendiskusikan masing-masing RQ.

* 1. **Tinjauan Hasil Tugas akhir dibanding dengan Tugas akhir Terdahulu**

Pembahasan penutup dapat menjelaskan mengenai kelebihan hasil pengembangan atau tugas akhir dan kekurangan dibandingkan dengan tugas akhir atau produk lain. Penulis dapat menggunakan tabel untuk membandingkan secara gamblang dan menjelaskannya .

**BAB V.  
KESIMPULAN DAN SARAN**

1. 1. **Kesimpulan**

Kesimpulan dapat diawali dengan apa yang dilakukan dengan tugas akhir ini lalu dilanjutkan berisi poin-poin yang setiap poin membahas RO atau menjawab RQ. Cara termudah adalah dengan menjawab RQ. Apabila terdapat 5 RQ maka kesimpulan selayaknya berupa poin-poin menjawab masing-masing RQ. Dalam beberapa hal, kesimpulan dapat juga berisi tentang temuan/*findings* yang Anda dapatkan setelah melakukan pengamatan dana atau analisis terhadap hasil tugas akhir.

* 1. **Saran**

Saran berisi hal-hal yang bisa dilanjutkan dari tugas akhir ini yang belum dilakukan karena batasan permasalahan. Saran bukan berisi saran kepada sistem atau pengguna, tetapi saran diberikan kepada aspek tugas akhir yang dapat dikembangkan dan ditambahkan di tugas akhir selanjutnya.

**DAFTAR PUSTAKA**

Assidiq, N. F., & Nurcahyani, I. (n.d.). *ANALISIS PENGARUH KINERJA ROUTING PROTOCOL AODV DAN DSDV TERHADAP KONSUMSI ENERGI NODE PADA JARINGAN*.

Biswas, A. K., & Dasgupta, M. (2019). AODV-DSR Hybrid Reactive Routing Protocol and its Generalization for Mobile Ad-Hoc Networks. *2019 3rd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, 1–5. https://doi.org/10.1109/IEMENTech48150.2019.8981052

Günay, F. B., Öztürk, E., Çavdar, T., Hanay, Y. S., & Khan, A. U. R. (2021). Vehicular Ad Hoc Network (VANET) Localization Techniques: A Survey. *Archives of Computational Methods in Engineering*, *28*(4), 3001–3033. https://doi.org/10.1007/s11831-020-09487-1

Kugali, S. N., & Kadadevar, S. (n.d.). Vehicular ADHOC Network (VANET):-A Brief Knowledge. *International Journal of Engineering Research*, *9*(06).

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. D. A., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, *80*, 103352. https://doi.org/10.1016/j.micpro.2020.103352

Kumar, M., Jain, V., Jain, A., Bisht, U. S., & Gupta, N. (2019). Evaluation of black hole attack with avoidance scheme using AODV protocol in VANET. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(2), 277–291. https://doi.org/10.1080/09720529.2019.1585635

Kuthe, A., Chaudhari, T., Thakare, S., Dohtare, P., & Waghmare, D. (2022). Design and Implementation of VANET in Ad hoc Network using MATLAB. *International Journal of Computer Science and Mobile Computing*, *11*(3), 49–55. https://doi.org/10.47760/ijcsmc.2022.v11i03.007

Manapa, E. S., Sampetoding, E. A. M., & Lewakabessy, G. (2020). POTENSI PENGGUNAAN MOBILE AD-HOC NETWORK (MANET) SEBAGAI ALAT KOMUNIKASI DATA PADA TRANSPORTASI DI INDONESIA. *Journal Dynamic Saint*, *4*(2), 865–868. https://doi.org/10.47178/dynamicsaint.v4i2.889

Moler, C., & Little, J. (2020). A history of MATLAB. *Proceedings of the ACM on Programming Languages*, *4*(HOPL), 1–67. https://doi.org/10.1145/3386331

Naim, Z., & Hossain, Md. I. (2019). Performance Analysis of AODV, DSDV And DSR in Vehicular Adhoc Network (VANET). *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, 17–22. https://doi.org/10.1109/ICREST.2019.8644313

Nazif, F., Wibawa, I. P. D., & Rizal, A. (n.d.). *Pemantauan Dan Notifikasi Kondisi Tanah Pada Tanaman Menggunakan Platform Iot*.

Oberoi, V. (2020). Enhancement of QoS in Security Algorithm for Blackhole Attack in VANET. *2020 IEEE Pune Section International Conference (PuneCon)*, 33–37. https://doi.org/10.1109/PuneCon50868.2020.9362444

Shrestha, S., Baidya, R., Giri, B., & Thapa, A. (2020). Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol. *2020 8th International Electrical Engineering Congress (iEECON)*, 1–4. https://doi.org/10.1109/iEECON48109.2020.229555

Sindhwani, M., Singh, R., Sachdeva, A., & Singh, C. (2022). Improvisation of optimization technique and AODV routing protocol in VANET. *Materials Today: Proceedings*, *49*, 3457–3461. https://doi.org/10.1016/j.matpr.2021.03.727

Singh, P. K., Nandi, S. K., & Nandi, S. (2019). A tutorial survey on vehicular communication state of the art, and future research directions. *Vehicular Communications*, *18*, 100164. https://doi.org/10.1016/j.vehcom.2019.100164

Upadhyaya, A. N., & Shah, J. S. (2019). Effect on aodv routing protocol under blackhole attack in vanet. *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY*, *10*(3). https://doi.org/10.34218/IJCET.10.3.2019.019

Waruwu, M. (2023). *Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi*. *7*.

**LAMPIRAN**

Lampiran bersifat opsional bergantung hasil kesepakatan dengan pembimbing dapat berupa

* Bukti pelaksanaan Kuesioner seperti pertanyaan kuesioner, resume jawaban responden, dan dokumentasi kuesioner
* Spesifikasi Aplikasi atau Sistem yang dikembangkan meliputi spesifikasi teknis aplikasi, tautan unduh aplikasi, manual penggunaan aplikasi, hingga screenshot aplikasi
* Cuplikan kode yang sekiranya penting dan ditambahkan.
* Tabel yang terlalu panjang yang masih diperlukan tetapi tidak memungkinkan untuk ditayangkan di bagian utama skripsi.
* Gambar-gambar pendukung yang tidak terlalu penting untuk ditampilkan di bagian utama. Akan tetapi, mendukung argumentasi/pengamatan/analisis
* Penurunan rumus-rumus atau pembuktian suatu teorema yang terlalu panjang dan terlalu teknis sehingga Anda berasumsi bahwa pembaca biasa tidak akan menelaah lebih lanjut. Hal ini digunakan untuk memberikan kesempatan bagi pembaca tingkat lanjut untuk melihat proses penurunan rumus-rumus ini.