**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 JUDUL i](#_Toc46400993)

[HALAMAN PENGESAHAN I i](#_Toc46400994)

[HALAMAN PENGESAHAN II ii](#_Toc46400995)

[DAFTAR ISI iii](#_Toc46400996)

[DAFTAR TABEL v](#_Toc46400997)

[DAFTAR GAMBAR vi](#_Toc46400998)

[DAFTAR SINGKATAN vii](#_Toc46400999)

[INTISARI viii](#_Toc46401000)

[ABSTRACT ix](#_Toc46401001)

[BAB I. PENDAHULUAN 1](#_Toc46401002)

[1.1. Latar Belakang 1](#_Toc46401003)

[1.2. Rumusan Masalah 3](#_Toc46401004)

[1.3. Batasan Masalah 4](#_Toc46401005)

[1.4. Tujuan Tugas Akhir 5](#_Toc46401006)

[1.5. Manfaat Tugas Akhir 5](#_Toc46401007)

[1.6. Sistematika Penulisan 5](#_Toc46401008)

[1.6.1. Bab I 5](#_Toc46401016)

[1.6.2. Bab II 5](#_Toc46401017)

[BAB II. TINJAUAN PUSTAKA DAN DASAR TEORI 6](#_Toc46401018)

[2.1 Tinjauan Pustaka 6](#_Toc46401022)

[2.2 Dasar Teori 7](#_Toc46401023)

[2.3 Analisis perbandingan metode 7](#_Toc46401024)

[2.4 Pertanyaan Tugas akhir (jika perlu) 7](#_Toc46401025)

[BAB III. METODE TUGAS AKHIR 8](#_Toc46401026)

[3.1 Metode Penelitian 8](#_Toc46401032)

[3.2 Alat dan Bahan Tugas akhir 8](#_Toc46401033)

[3.1.1. Alat Tugas akhir 8](#_Toc46401038)

[3.1.2. Bahan Tugas akhir 9](#_Toc46401039)

[3.3 Alur Tugas akhir 9](#_Toc46401043)

[BAB IV. HASIL DAN PEMBAHASAN 10](#_Toc46401044)

[4.1 Pembahasan Hasil RO-1 (Ubah Sesuai dengan Hal Yang hendak dibahas) 10](#_Toc46401049)

[4.1.1. Data 1 10](#_Toc46401054)

[4.1.2. Data 2 10](#_Toc46401055)

[4.2 Pembahasan Hasil RO-2 (Ubah sesuai dengan Hal yang hendak dibahas) 10](#_Toc46401056)

[4.3 Tinjauan Hasil Tugas akhir dibanding dengan Tugas akhir Terdahulu 10](#_Toc46401057)

[BAB V. KESIMPULAN DAN SARAN 11](#_Toc46401058)

[5.1 Kesimpulan 11](#_Toc46401060)

[5.2 Saran 11](#_Toc46401061)

[DAFTAR PUSTAKA 11](#_Toc46401062)

[LAMPIRAN 12](#_Toc46401063)

# 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 *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 *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 *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 *routing* dalam menghadapi serangan *Blackhole*.(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 *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 *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 AODV 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 AODV
   1. **Batasan Masalah**

Batasan masalah pada analisis:

1. Analisis ini dilakukan menggunakan *Matrix Laboratory* (MATLAB)
2. Simulasi *software* dilakukan menggunakan *operating system Windows* *11*
3. Penelitian ini hanya akan menganalisis dampak serangan *Blackhole* terhadap kinerja jaringan AODV dalam lingkungan VANET.
4. Analisis akan difokuskan pada modifikasi protokol AODV untuk mendeteksi dan mengatasi serangan *Blackhole*.
5. Evaluasi kinerja jaringan akan dilakukan berdasarkan dua metrik utama: *delay* (latensi) dan *throughput*.
6. Penelitian ini akan mengimplementasikan fungsi threshold sebagai bagian dari modifikasi protokol AODV untuk mendeteksi *node* jahat.
7. Fokus penelitian adalah pada pengaruh serangan *Blackhole* terhadap performa jaringan dalam hal *delay* dan *throughput*.
   1. **Tujuan Tugas Akhir**

Tujuan analisis ini yaitu:

1. Untuk mengevaluasi kinerja protokol AODV dalam konteks *Vehicular Ad-Hoc Network* (VANET) ketika terjadi serangan *Blackhole*, dengan fokus pada metrik seperti *delay* dan *throughput*.
2. Untuk memahami dan mengukur dampak serangan *Blackhole* terhadap performa jaringan VANET, termasuk bagaimana serangan ini mempengaruhi *delay* dan *throughput* jaringan.
3. 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

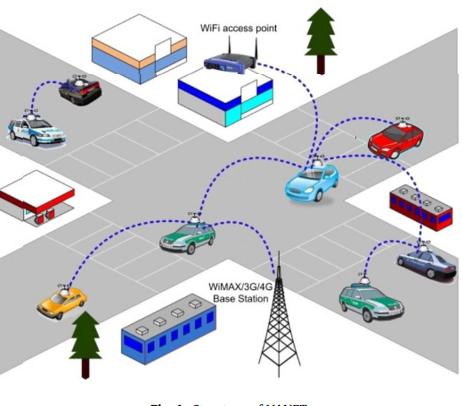
Pada bab ini akan dijelaskan kesimpulan dari sistem yang telah dibangun dan saran-saran yang diperoleh dari hasil penelitian. Saran-saran ini dapat digunakan sebagai panduan dalam pengembangan simulasi serangan *Blackhole* pada jaringan VANET.

# 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.

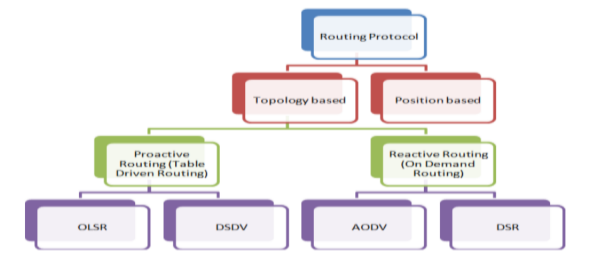
Penelitian yang dilakukan oleh peneliti (Sindhwani et al., 2022) peneliti ini menggunakan Vehicular Adhoc Network (VANET) untuk merancang sebuah jaringan protokol Ad Hoc On-Demand Distance Vector (AODV). Pada penelitian ini VANET digunakan untuk membantu dalam menyebarkan informasi dari satu *node* ke *node* kendaraan lainnya. Terdapat perbedaan antara jaringan ad-hoc tradisional dan *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.



Gambar 1 struktur VANET

Pada penelitian yang dilakukan oleh peneliti (Tanaya et al., 2019), peneliti ini melakukan penelitian dengan judul serangan *Blackhole* terhadap Kinerja Protokol AODV. Pada penelitian ini I Putu Krisna Yoga Tanaya menjelaskan dampak dari serangan *Blackhole* pada kinerja protokol AODV. Peneliti menggunakan NS 2 sebagai simulasi implementasi simulatornya. Paca penelitian ini peneliti menggunakan *random way point*  untuk pergerakan *node*-*node* dan penulis menggunakan warna *node* untuk menetapkan *node*-*node* tersebut. Penulis menggunakan DYMO dikarenakan protokol tersebut termasuk pada satu jenis protokol *routing* yaitu reaktif. DYMO juga merupakan protokol penerus dari AODV.

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



Gambar 2 topology *routing* protocol

Pada penelitian ini penulis menggunakan AODV protocol *routing*. AODV protocol *routing* merupakan *reactive 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*.

* 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.)

* + 1. ***AODV***

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

Penelitian ini berfokus pada bagaimana kinerja protokol 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.

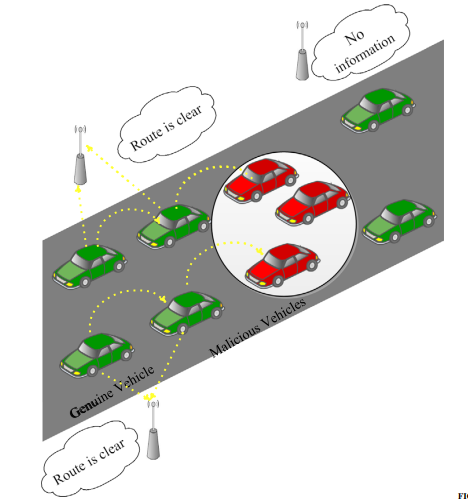
* + 1. ***Blackhole***

*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 routing yang digunakan, seperti AODV, sehingga dapat mengenali dan menghindari *node* jahat yang terlibat dalam serangan *blackhole*.

Proses terjadinya serangan *Blackhole* digambarkan sebagai berikut :



Gambar 4 Proses serangan *Blackhole*

Pada gambar 4 merupakan ilustrasi *blackhole attack* pada jaringan VANET. *Node* jahat berpura-pura menjadi *node* tujuan dengan mengirimkan pesan balasan rute palsu kepada *node* sumber saat proses penemuan rute berlangsung. Akibatnya, lalu lintas data dari *node* sumber diarahkan ke *node* jahat tersebut, yang kemudian menghentikan aliran data tersebut sehingga paket data tidak pernah mencapai tujuan yang sebenarnya.(Tanwar et al., 2018).

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

Modified sequence number (MSN) adalah konsep yang berhubungan dengan perubahan atau penyesuaian dalam protokol 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. **Analisis perbandingan metode**

Di dalam tinjauan pustaka hasil akhirnya adalah analisis secara kualitatif atau pun secara kuantitatif kelebihan dan kekurangan metode jika dikaitkan dengan masalah, batasan-batasan masalah dan solusi yang dinginkan. Analisis kuantitatif ***tidak wajib*** tapi mempunyai nilai tambah di dalam tugas akhir saudara. Bagian ini menjelaskan kenapa metode tersebut dipilih dan uraikan dengan lebih jelas metode pelaksanaan tugas akhir yang ingin Anda lakukan.

* 1. **Pertanyaan Tugas akhir (jika perlu)**

Pertanyaan tugas akhir bersifat opsional dan dapat ditambahkan untuk menekankan hal-hal yang hendak diketahui dari tugas akhir berdasar pada tujuan tugas akhir. Pertanyaan tugas akhir dikenal dengan RQ (Research Question) dan harus memiliki keterkaitan dengan RO (Research Objective). Satu RO dapat memiliki satu atau lebih dari satu RQ.

**BAB III.  
METODE TUGAS AKHIR**

5. 1. **Metode Penelitian**

Kemukakan metode penelitian yang anda gunakan ketika anda membangun software, aplikasi, database ataupun pengembangan game. Jelaskan dengan detail tahapan mana saja yang anda lalukan maupun tidak anda lakukan dalam membangun sistem tersebut.

* 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
   4. **Alat dan Bahan Tugas akhir**

Data yang diperoleh merupakan implementasi dari jalanan pada RS.PKU Yogyakarta

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 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 *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. Pada program ini peneliti menggunakan :

1. *Routing* AODV

*Routng* AODV merupakan mekanisme penemuan rute ketika sebuah *node* mengirim data ke *node* tujuan yang tidak diketahui rutenya. *Node*-*node* tersebut didapati dengan menggunakan data yang sudah dikumpulkan. Pada tiap *node* diberi table *routing* yang berisi:

* IP Destination

Pemberian fungsi ini untuk mengindentifikasi tujuan dari paket data yang akan dikirim.

* Next Hop

Fungsi ini digunakan untuk Menentukan *node* berikutnya yang harus dilalui untuk mencapai tujuan akhir. *Node* ini berfungsi sebagai titik perantara dalam rute pengiriman.

* Sequence Number

Fungsi *sequence number* merupakan fungsi untuk Memastikan informasi rute tetap terbaru. Nomor urut yang lebih tinggi menandakan rute yang lebih baru dan lebih valid. Setiap kali rute diperbarui, nomor urut ini dinaikkan untuk menunjukkan adanya pembaruan.

* Hop Count

*Hop Count* merupakan fungsi untuk menyediakan informasi tentang jarak tujuan dari *node* saat ini berdasarkan jumlah hop. Semakin sedikit jumlah hop, semakin dekat tujuannya.

* Lifetime

*Lifetime* digunakan untuk menetapkan durasi validitas rute sebelum dihapus dari tabel *routing*. Jika rute tidak digunakan dalam periode waktu tertentu, rute tersebut dihapus untuk memastikan tabel *routing* tetap terbaru dan efisien.

1. RREQ

*Node* akan meminta permintaan rute ke tetangga *node* sampai diterima oleh *node* tujuan.

1. RREP

Setelah *node* tujuan yang mempunyai rute langsung ke tujuan menerima permintaan. *Node* akan mengerimkan pesan balasan rute (RREP) ke *node*

1. Reply Sequence Number

Fungsi ini bertujuan ketika pesan RREQ, RREP dikirimkan jumlah bertambah dengan urut. *Sequence number* digunakan untuk menentukan kesegaran sebuah rute.

Algorima AODV beserta serangan *Blackhole* seperti di

* + 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

**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*.

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

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

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

Tanaya, I. P. K. Y., Primananda, R., & Nurwarsito, H. (2019). Analisis Dampak Serangan Black Hole terhadap Kinerja Protokol AODV dan DYMO pada MANET (Mobile Ad-Hoc Network). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(4), Article 4.

Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *SECURITY AND PRIVACY*, *1*(5), e39. https://doi.org/10.1002/spy2.39

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

**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.