ANALISIS IMPLEMENTASI METODE PENAMBAHAN *DATA RATE* SEBAGAI TEKNIK MITIGASI SERANGAN *BLACKHOLE* PADA JARINGAN VANET

SKRIPSI

untuk memenuhi salah satu persyaratan
mencapai derajat Sarjana S1

Disusun oleh:

Afif Abiyyuna

16524136

Jurusan Teknik Elektro

Fakultas Teknologi Industri

Universitas Islam Indonesia

Yogyakarta

2020

LEMBAR PENGESAHAN

ANALISIS IMPLEMENTASI METODE PENAMBAHAN *DATA RATE* SEBAGAI TEKNIK MITIGASI SERANGAN *BLACKHOLE* PADA JARINGAN VANET

TUGAS AKHIR

Diajukan sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik
pada Program Studi Teknik Elektro
Fakultas Teknologi Industri
Universitas Islam Indonesia

Disusun oleh:

Afif Abiyyuna
16524136

Yogyakarta, 25 Juli 2020

Menyetujui,

Pembimbing 1

Ida Nurcahyani, S.T., M.Eng
155240104

LEMBAR PENGESAHAN

SKRIPSI

ANALISIS IMPLEMENTASI METODE PENAMBAHAN *DATA RATE* SEBAGAI TEKNIK MITIGASI SERANGAN *BLACKHOLE* PADA JARINGAN VANET

Dipersiapkan dan disusun oleh:

Afif Abiyyuna

16524136

Telah dipertahankan di depan dewan penguji

Pada tanggal: 3 September 2020

Susunan dewan penguji

Ketua Penguji**:**

Ida Nurcahyani, S.T., M.Eng : _____

Anggota Penguji 1**:**

Dzata Farahiyah, S.T., M.Sc. : _____

Anggota Penguji 2**:**

Elvira Sukma Wahyuni. S.Pd., M.Eng. : _____

Skripsi ini telah diterima sebagai salah satu persyaratan untuk memperoleh gelar Sarjana

Tanggal: tanggal bulan tahun

Ketua Program Studi Teknik Elektro

Yusuf Aziz Amrullah, S.T., M.Sc., Ph.D

045240101

PERNYATAAN

Dengan ini Saya menyatakan bahwa:

1. Skripsi ini tidak mengandung karya yang diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan Saya juga tidak mengandung karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.
2. Informasi dan materi Skripsi yang terkait hak milik, hak intelektual, dan paten merupakan milik bersama antara tiga pihak yaitu penulis, dosen pembimbing, dan Universitas Islam Indonesia. Dalam hal penggunaan informasi dan materi Skripsi terkait paten maka akan diskusikan lebih lanjut untuk mendapatkan persetujuan dari ketiga pihak tersebut diatas.

Yogyakarta, 25 Juli 2020

Afif Abiyyuna

KATA PENGANTAR

Assalamual'aikum Warrahmatullahi Wabarakatuh,

Segala puji dan rasa syukur penulis panjatkan kepada Allah SWT yang maha pengasih lagi maha penyayang, karena rahmat dan hidayahnya penulis bisa menyelesaikan laporan tugas akhir yang berjudul "Analisis Kinerja Teknik Mitigasi Pada Jaringan Vanet" sebagai salah satu syarat untuk menyelesaikan proses pembelajaran Program Sarjana (S1) pada Program Studi Teknik Elektro Fakultas Teknologi Industri Universitas Islam Indonesia. Sholawat serta salam tidak lupa penulis lantunkan kepada nabi besar umat islam Muhammad SAW sebagai tauladan bagi kita semua. Penelitian ini tentunya tidak mudah untuk dilakukan karena banyaknya hambatan dan masalah yang terjadi saat proses penelitian, namun hambatan dan masalah tersebut dapat teratasi atas bantuan banyak pihak. Oleh karena itu penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Kedua orang tua beserta seluruh keluarga besar di Yogyakarta yang telah mendukung secara material, emosional, dan spiritual selama menimba ilmu di Universitas Islam Indonesia.
2. Bapak Yusuf Aziz Amrullah, S.T., M.Sc., Ph.D. selaku ketua Program Studi Teknik Elektro Universitas Islam Indonesia.
3. Ibu Ida Nurcahyani, S.T., M.Eng. selaku dosen pembimbing yang telah memberikan arahan, masukan, dan nasihat dalam proses kegiatan penelitian ini.
4. Seluruh rekan Teknik Elektro Universitas Islam Indonesia angkatan 2016 khususnya rekan Jurusan Telekomunikasi yang telah membantu dalam proses kegiatan penelitian ini.
5. Bang Afif Fairuzqi, Mba Chintya Maharani, Mba Sulandari, Bang Fathullah, Bang Helmi Hartadi, dan masih banyak kakak tingkat lain yang telah memberikan ilmunya sehingga penulis bisa menyelesaikan penelitian ini
6. M. Tri Nur Pamungkas dan Annisa Christyanti selaku teman satu bimbingan yang selalu memberikan dukungan dan motivasi selama proses kegiatan penelitian berlangsung
7. Seluruh pihak yang telah membantu yang namanya tidak penulis cantumkan

Penulis meminta maaf sebesar-besarnya apabila dalam laporan ini ditemukan berbagai kekurangan, oleh karena itu penulis sangat senang bila diberikan kritik dan saran untuk menjadikan penelitian ini semakin baik. Semoga tulisan ini dapat bermanfaat bagi siapapun yang membacanya

Wassalamu'alaikum Warrahmatullahi Wabarakatuh

ARTI LAMBANG DAN SINGKATAN

AODV	: *Ad Hoc On-Demand Distance Vector Routing Protocol*
DSR	: *Dynamic Source Routing*
GPS	: *Global Positioning System*
IDS	: *Intrusion Detection System*
MANET	: *Mobile Ad-hoc Network*
OBU	: *On Board Unit*
OLSR	: *Optimized Link State Routing*
PDR	: *Packet Delivery Ratio*
QoS	: *Quality of Service*
RSU	: *Road Side Unit*
RREP	: *Route Replay*
RREQ	: *Route Request*
RRER	: *Route Error*
TORA	: *Temporally Ordered Routing Algorithm*
V2I	: *Vehicle to Infrastructure*
V2V	: *Vehicle to Vehicle*
VANET	: *Vehicle Ad-hoc Network*
WLAN	: *Wireless Local Area Network*

ABSTRAK

Vehicular Ad-hoc Network (VANET) adalah teknologi terbaru yang dihasilkan dari perkembangan teknologi *Mobile Ad-hoc Network* (MANET) yang dirancang untuk membuat routing data menjadi lebih efisien, sehingga dapat digunakan untuk komunikasi antar kendaraan yang memiliki kecepatan tinggi dan mobilitas yang acak secara nirkabel. Tujuan dari teknologi VANET adalah untuk mengurangi resiko kecelakaan di jalanan sehingga pengendara memiliki keamanan dan kenyaman yang tinggi saat berkendara, kemudian teknologi ini juga memungkinkan untuk digunakan sebagai media informasi dan hiburan seperti informasi keadaan jalan terkini dan mendengarkan music secara *online*. Jaringan VANET merupakan salah satu jaringan *Ad-hoc* yang mana jaringan ini memiliki topologi yang selalu berubah dengan cepat. Hal ini mengakibatkan komunikasi antar *node* sering terputus saat proses komunikasi data berlangsung. Sebuah serangan dapat terjadi saat sebuah jaringan tidak memiliki infrastruktur tetap dan topologi yang sering berubah-ubah, salah satu serangan yang kerap kali terjadi adalah serangan *blackhole*. Serangan *blackhole* adalah sebuah serangan yang dapat menjatuhkan paket data yang dikirimkan dari *node* sumber ke *node* tujuan dengan cara menyatakan dirinya sebagai rute terpendek dan tercepat untuk sampai tujuan. Penelitian ini dilakukan untuk mengetahui dan meminimalisir dampak dari serangan *blackhole*. Metode mitigasi yang digunakan dalam penelitian adalah dengan menambahkan *data rate* pada *node* yang terkena serangan *blackhole*. Skenario yang digunakan adalah membuat serangan *blackhole* pada jaringan VANET dan menambahkan nilai *data rate* pada *node* yang terkena serangan *blackhole* sebagai teknik mitigasinya. Penelitian ini menggunakan simulasi yang dibantu oleh aplikasi OPNET Modeler 14.5. Parameter yang digunakan oleh penulis adalah parameter *Quality of Service* (QoS) yaitu *data dropped*, *delay*, dan *throughput*. Hasil menunjukkan saat jaringan VANET mengalami serangan, kinerja *data dropped* menurun sebesar 0,29 kbit/sec, kinerja *delay* menurun sebesar 0,81 ms, dan kinerja *throughput* menurun sebesar 33,95 kbit/sec, hal ini ditunjukkan dengan adanya perubahan nilai rata-rata pada setiap parameter. Setelah dilakukan metode penambahan data rate sebagai mitigasi, hasil menunjukkan adanya kenaikan kinerja pada setiap parameter. Kinerja *data dropped* meningkat menjadi 0,2 kbit/sec, kinerja *delay* meningkat menjadi 0,74 ms, dan kinerja *throughput* meningkat menjadi 35,84 kbit/sec. Dari semua hasil tersebut dapat disimpulkan bahwa metode penambahan *data rate* berhasil untuk meminimalisir serangan *blackhole* pada jaringan VANET.

Kata kunci: AODV, *Blackhole*, QoS, VANET

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi saat ini berkembang pesat, dengan begitu teknologi menjadi salah satu kebutuhan yang paling penting untuk membantu pekerjaan kehidupan manusia, teknologi telekomunikasi merupakan salah satu teknologi yang memiliki kemajuan terbesar demi membantu perkerjaan manusia sehari-hari. Kemajuan teknologi telekomunikasi ini memberikan banyak pilihan demi membangun sebuah sistem jaringan nirkabel yang dapat membangun dan mengelola suatu jaringan tersendiri dalam luas area tertentu sehingga seseorang mampu untuk saling terkoneksi antara satu sama lain, kelebihan lain dari teknologi ini adalah kemungkinan untuk membuat sebuah jaringan yang bersifat sementara *(AD-Hoc)*. Jaringan atau infrastruktur dari teknologi tersebut adalah *Mobile AD-Hoc Network* (MANET) [1]. Jenis *routing protocol* yang digunakan akan berperan penting dalam sebuah jaringan tertentu dan akan sangat mempengaruhi kinerja jaringan MANET.

Jaringan *Ad-hoc* terdiri dari beberapa jenis, salah satu jaringan *ad-hoc* yang memiliki kecepatan dan mobilitas yang tinggi adalah *Vehicular AD-Hoc Network* (VANET). VANET adalah teknologi terbaru yang dirancang untuk membuat *routing data* yang lebih efisien antara kendaraaan (V2V) maupun antara kendaraan dengan bangunan infrastruktur (V2I) [2]. Perbedaan antara VANET dan MANET berada pada letak pergerakan dan kecepatan *node*nya. *Node* dalam MANET diwakili oleh perankat nirkabel seluler seperti handphone, komputer, dan barang nirkabel lain, dengan demikian *node* pada MANET memiliki kecepatan yang relatif rendah dan pergerakan nodenya masih bisa diprediksi. *Node* pada VANET diwakili oleh kendaraan dan bangunan infrastruktur yang ada di jalanan, hal ini membuat kecepatan *node* pada VANET sangat lah tinggi dikarenakan pergerakan *node* pada kendaraan mempunyai kecepatan yang tidak menentu, selain itu pergerakan dari *node* tersebut pun sulit untuk diprediksi [3].

Jaringan VANET membutuhkan *routing protocol* yang berfungsi untuk membantu proses routing setiap node, karena pada jaringan *ad-hoc* setiap *node*nya dapat difungsikan sebagai *router* yang artinya *node* tersebut dapat berkomunikasi dengan sesama *node* lain untuk menyebarkan sebuah informasi. *Routing protocol topology based* adalah *routing* yang dilakukan berdasarkan topologi *node*nya, routing ini masih dibagi menjadi 2 bagian yaitu proaktif dan reaktif. *Routing protocol* proaktif merupakan *routing* dimana setiap *node*nya mempertahankan posisinya pada jalur yang telah ditentukan ke seluruh jaringan, sedangkan *routing protocol* reaktif merupakan proses *routing* dimana jalur antar *node* yang berbeda akan dipertemukan jika ada suatu kepentingan

tertentu [4]. *Routing protocol* reaktif dapat dibagi menjadi 3 jenis yaitu *Ad Hoc On-Demand Distance Vector Routing Protocol* (AODV), *Dynamic Source Routing* (DSR), dan *Temporally Ordered Routing Protocol* (TORA). AODV memungkinkan sebuah *node* untuk menanggapi kerusakan yang ada pada suatu link dan perubahan topologi jaringan secara cepat dan tepat waktu. Karena itu AODV dipilih sebagai *routing protocol* yang difungsikan untuk mengirim data lalu lintas antar kendaraan maupun antara kendaraan dan bangunan infrastruktur. AODV adalah *routing protocol* yang menetapkan sebuah jalur ketika sebuah *node* membutuhkan pengiriman paket data. AODV memungkinkan *node* untuk menemukan tujuan yang baru dengan cepat dan tidak memerlukan *node* untuk mempertahankan jalur ke tujuan yang komunikasinya tidak diaktifkan [5].

Proses pengiriman data dengan *node* yang bergerak sangat cepat menyebabkan topologi berubah selama proses komunikasi berlangsung. Keadaan tersebut dapat menyebabkan adanya *node* jahat yang dengan mudah memperkenalkan identitasnya untuk mengambil semua paket data saat proses komunikasi berlangsung. Setelah menerima paket data, *node* tersebut akan membuang datanya tanpa memberitahu sumber dan tujuannya [6]. Pada jaringan VANET sangat penting untuk menjaga keamanan saat poses pengiriman data karena data yang diberikan merupakan data yang bertujuan untuk keselamatan banyak orang di jalanan, namun karena jaringan VANET merupakan jaringan yang nirkabel maka akan sangat banyak serangan yang kerap terjadi salah satu serangan tersebut adalah serangan *blackhole* [7]. Serangan *blackhole* adalah sebuah serangan dimana sebuah *node* mengklaim memiliki tujuan yang telah ditentukan dengan jalur terpendek, selanjutnya *node* tersebut akan menjatuhkan semua paket data yang memiliki tujuan yang telah ditentukan sebelumnya. Dalam kasus yang lebih lanjut, sebuah *node* bahkan bisa menurunkan persentase paket pengiriman walaupun tidak semua paket dijatuhkan [8]. Berbagai cara telah dilakukan untuk mencegah serangan *blackhole* yang terjadi pada jaringan nirkabel, sampai saat ini belum ada metode yang benar-benar bisa mencegah serangan tersebut. Namun demikian ada beberapa cara yang bisa dilakukan untuk mengurangi dampak dari serangan *blackhole* yaitu penambahan jumlah *node* [9], penambahahn jarak antar *node* [10], dan penambahan *data rate* [11].

Penelitian ini dilakukan untuk melakukan mitigasi dari serangan *blackhole* pada jaringan VANET. Jaringan VANET memiliki kecepatan antar *node* yang sangat cepat dan berubah-ubah sehingga metode mitigasi penambahan jumlah *node* dan penambahan jarak antar *node* tidak bisa dilakukan. Metode yang penulis gunakan adalah dengan cara melakukan perubahan data rate pada *node* yang terkena serangan. Penelitian ini dilakukan dengan cara membuat simulasi pada OPNET modeler 14.5, selanjutnya analisa akan menggunakan parameter *Quality of Service* (QoS) yaitu, *data dropped*, *delay*, dan *throughput*.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah:

1. Bagaimana kinerja jaringan VANET sebelum dan sesudah terkena serangan *blackhole*?
2. Bagaimana kinerja metode mitigasi penambahan *data rate* pada jaringan VANET yang telah terkena serangan *blackhole*?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Pada penelitian ini tidak membahas cara mendeteksi serangan *blackhole*.
2. Penelitian ini hanya membahas bagaimana cara meminimalisir kinerja jaringan VANET saat terkena serangan *blackhole*.
3. Penelitian ini hanya menggunakan *routing protocol* AODV.
4. Penelitian ini hanya menggunakan simulator OPNET 14.5.
5. Parameter yang digunakan adalah bagian dari parameter QoS yaitu, *data dropped*, *delay*, dan *throughput*.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengetahui kinerja jaringan VANET sebelum dan sesudah terkena serangan *blackhole*.
2. Mengetahui kinerja jaringan VANET yang telah terkena serangan *blackhole* setelah dilakukan metode mitigasi penambahan *data rate*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Menambah referensi bagi peneliti lain yang ingin memperbaiki kinerja jaringan VANET setelah terkena serangan *blackhole*.
2. Mengetahui hasil data dari skenario yang telah dilakukan oleh peneliti.
3. Meminimalisir dampak serangan *blackhole* pada kinerja jaringan VANET

BAB 2
TINJAUAN PUSTAKA

2.1 Studi Literatur

Bagian ini merupakan survei yang telah dilakukan dari beberapa penelitian sebelumnya mengenai pengaruh serangan *blackhole* terhadap kinerja jaringan VANET dan berbagai macam metode yang telah dilakukan untuk meminimalisir dampak dari serangan *blackhole*. Perbedaan menonjol yang terlihat pada setiap penelitian terletak pada parameter jaringan yang digunakan dan metode yang digunakan dalam meminimalisir dampak dari serangan *blackhole* pada jaringan VANET. Selain itu perbedaan lain yang paling mendasar ada pada jenis *routing protocol* yang digunakan oleh para peneliti. Dengan adanya perbedaan parameter dari setiap penelitian tersebut, penulis akan mencoba untuk melakukan pembahasan dari beberapa hasil penelitian yang telah dilakukan untuk mengurangi dampak serangan *blackhole* pada jaringan VANET menggunakan *routing protocol* AODV.

Salah satu penelitian tentang kinerja VANET yaitu pada penelitian [12] mengungkapkan bahwa peneliti telah melakukan analisis terhadap performa jaringan VANET yang telah mengalami serangan *blackhole*. Peneliti memanfaatkan *routing protocol* AODV dan OLSR untuk menegtahui kinerja jaringan VANET setelah mendapatkan serangan *blackhole*. Parameter yang digunakan oleh peneliti adalah nilai *end-to-end delay* dan nilai *throughput*. Hasilnya didapatkan bahwa nilai *delay* pada *routing protocol* OLSR naik sebanyak 2 sampai 5 persen sedangkan pada *routing protocol* AODV nilai *delay* lebih parah lagi yaitu naik sebanyak 5 sampai 10 persen. Kesimpulan selanjutnya dari penelitian ini menyatakan bahwa *routing protocol* AODV lebih rentang terkena serangan *blackhole* dibandingkan dengan *routing protocol* OLSR.

Penelitian selanjutnya membahas terkait pengaruh blackhole pada *routing protocol* AODV [13]. Dalam penelitian ini penulis melakukan uji coba untuk mencegah dampak serangan *blackhole* secara keseluruhan dengan cara menambahkan algoritma IDS. Hal ini berguna untuk meningkatkan kinerja yang dapat dilihat melalui parameter QoS seperti PDR, *end-to-end delay*, dan *throughput*. Dalam penelitian ini peneliti melakukan 2 skenario yaitu skenario penambahan jumlah *node* dan skenario penambahan kecepatan node. Hasil yang diperoleh dalam penelitian yang meminimalisir dampak dari serangan *blackhole* ini adalah nilai rata-rata PDR meningkat menjadi 53,34%, nilai *throughput* juga meningkat 61,24% sehingga kecepatannya menjadi 22,20 kbps, dan nilai *delay end-to-end* meningkat sebesar 6,53% sehingga kecepatan *delay*nya adalah 6,41 ms.

Dalam penelitian yang dilakukan John Tobin, Christina Thorpe, dan Lian Murphy [14] penulis melakukan pendekatan untuk memitigasi serangan *blackhole* pada jaringan VANET. Penulis memberikan solusi dengan cara berfokus pada *node* yang terkena serangan *blackhole*, kemudian melakukan tiga tahapan yaitu deteksi serangan, penetapan *node* yang terkena serangan, dan melakukan pendataan kepada *node* yang terkena serangan *blackhole*. Serangan blackhole adalah serangan yang dapat secara signifikan mengurangi ketersediaan jaringan VANET dan mencegah komunikasi antara kendaraan sepenuhnya. Penulis menggunakan NS3 untuk melakukan simulasi dari skenario yang telah dibuat. Parameter jaringan yang digunakan oleh penulis adalah nilai PDR, nilai rata-rata *throughput*, dan nilai *packet loss*. Hasil penelitian ini membuktikan bahwa serangan blackhole dapat dicegah dan diatasi dengan cara membuang node yang terkena serangan dari jaringan VANET yang sedang berjalan. Waktu yang dibutuhkan untuk melakukan metode yang penulis ajukan adalah sebanayak 5,48 detik. Dengan demikian nilai parameter jaringan yang dilihat akan tetap sama seperti pada jaringan VANET dalam kondisi normal.

Penelitian lain tentang mitigasi serangan *blackhole* dilakukan oleh Agostino martorana, Giuseppe Primiero, Jacopo Tagliabue [15] penulis menyatakan bahwa dari segi keamanan, jaringan VANET memang sangat rentan terhadap serangan *blackhole* dikarenakan sifat system nirkabel yang terdesentralisasi dan terbuka, sehingga pendeteksian hampir tidak mungkin untuk dilakukan. Selanjutnya penulis melakukan mitigasi dengan cara mengidentifikasi jenis topologi dan banyaknya *node* yang ada pada suatu jaringan VANET. Simulasi dilakukan dengan menggunakan aplikasi NetLogo dengan fokus pada parameter topologi jaringan, ukuran jaringan, pemeringkatan pesan data, proporsi penemu, proporsi penyerang, dan jangkauan jaringan untuk serangan. Hasilnya menunjukan bahwa dengan melakukan indentifikasi dan konfigurasi ulang sesuai dengan parameter yang telah disebutkan akan berdampak pada protokol kerja yang sangat efisien dengan jaringan yang bersifat total maupun yang bersifat acak. Hal ini bisa lebih dirasakan dampaknya saat pada awal proses *routing* dengan memiliki konektifitas yang berkapasitas besar ke sumber informasi eksternal.

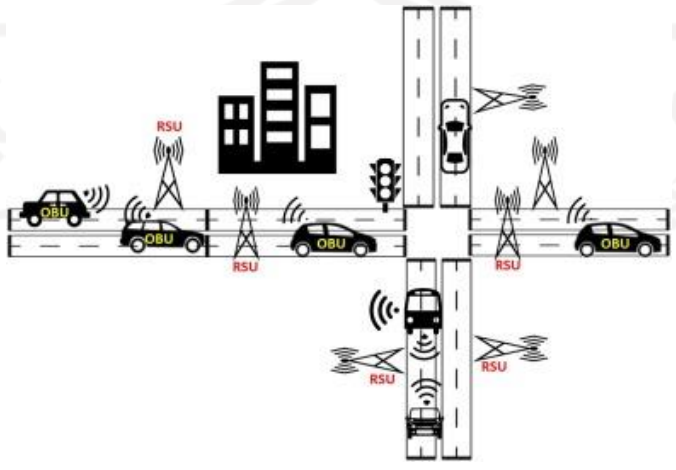
Pada studi literatur, para penulis menjelaskan bahwa jaringan VANET yang mengalami serangan *blackhole* kinerja jaringannya akan menurun. Penelitian tentang jaringan VANET yang mengalami serangan *blackhole* beserta mitigasinya sudah banyak dilakukan. Pada penelitian ini penulis mencoba untuk mengusulkan metode mitigasi baru dengan cara penambahan nilai *data rate* pada *node* yang terkena serangan *blackhole*, parameter yang digunakan oleh penulis adalah parameter QoS yaitu *data dropped, delay,* dan *throughput*

2.2 Tinjauan Teori

Jaringan *Ad-hoc* adalah jaringan yang meruapakan bagian dari jenis jaringan *Wireless Local Area Network* (WLAN) yang mana jaringan ini terdiri atas sekelompok *node* yang dapat berkomunikasi antara satu sama lain secara langsung tanpa harus menggunakan *node* perantara seperti *access point*. Sifat dari *node* pada jaringan *Ad-hoc* adalah dinamis dan dapat dengan mudah unuk berubah-ubah. *Node* yang ada pada jaringan ini juga bisa digunakan sebagai pendukung jaringan seperti *router*. Karena itu lah jaringan *Ad-hoc* ini memerlukan suatu *routing protocol* untuk menunjang proses pengiriman dan penerimaan data antar *node*nya.

2.2.1 *Vehicular Ad-hoc Network* (VANET)

VANET adalah teknologi baru yang berbasis dari teknologi sebelumnya yaitu MANET, dengan demikian jaringan VANET ini masih merupakan jaringan *Ad-hoc* tidak memiliki topologi jaringan untuk berkomunikasi antar *node* disekitarnya. Komunikasi antar *node* dilakukan dengan cara mengumumkan keberadaan sebuah *node,* sehingga *node* tetangga akan menyadari keberadaan dari *node* yang ingin melakukan komunikasi, hal ini dapat dilakukan secara otomatis dengan menggunakan *broadcasting packet*. Oleh karena itu jaringan ini perlu sebuah *routing protocol* agar komunikasi antar *node* bisa dilakukan dengan baik dan juga bisa menemukan *node* tetangga terdekat dengan cepat. Komunikasi VANET dapat dibagi menjadi dua kategori yaitu komunikasi antara kendaraan dengan kendaraan (V2V) dan komunikasi antara kendaraan dengan bangunan infrastruktur (V2I). *Node* yang mewakili infrastruktur jalan biasa disebut sebagai *Road Side Unit* (RSU) sedangkan *node* yang mewakili kendaraan yang bergerak biasa disebut *On Board Unit* (OBU) [16]. Gambar 2.1 dibawah ini menunjukan proses komunikasi jaringan VANET [7]



Gambar 2.1 Komunikasi Jaringan VANET

Tujuan akhir dari jaringan VANET adalah menyediakan informasi keselamatan jalan diantara *node-node* yang berada di area tertentu sehingga pertukaran informasi yang dilakukan secara terus menerus akan menandakan tingkat keamanan dan keselamatan yang tinggi bagi para pengguna jalan. Untuk itu jaringan VANET terdiri dari kendaraan yang telah dilengkapi oleh beberapa sensor *wireless* dan GPS. Karakteristik yang dimiliki oleh jaringan VANET adalah mobilitas node yang sangat yang tinggi, perubahan topologi jaringan yang berlangsung dengan cepat, ketersediaan media transmisi, pertukaran informasi yang selalu terjadi, *bandwidth* yang terbatas, dan perlindungan fisik yang baik [17].

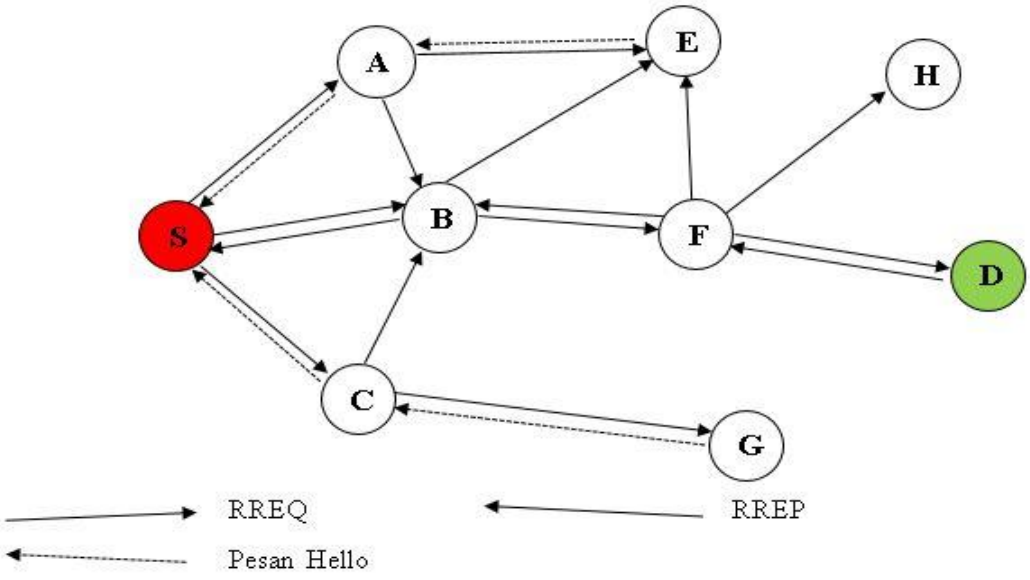
2.2.2 Routing Protocol

Ruoting protocol adalah suatu standarisasi yang mengontrol sebuah *node* agar dapat mengirimkan sebuah paket kepada *node* tujuan dalam suatu jaringan. *Routing protocol* dapat diibaratkan sebagai *router* yang dapat melakukan komunikasi kepada seluruh perangkat lain untuk menyebarkan sebuah informasi ataupun data, kemudian *router* ini akan memperkenankan pemilihan jalur antara dua *node* yaitu *node* sumber dan *node* tujuan dalam jaringan tersebut. Keistimewaan jaringan *Ad-hoc* terletak pada karakteristik *node*nya, dimana setiap *node* nya dapat difungsikan sebagai *router* yang dapat menjalankan data yang dikirimkan *antar node* disekitarnya, oleh karena itu perlu sebuah *routing protocol* untuk mendukung proses *routing* pada setiap *node* [18]. Jaringan *Ad-hoc* memiliki *node* yang bersifat *mobile* sehingga pada jaringan ini tidak memiliki topologi yang tetap, hal ini menyebabkan kejadian kehilangan jalur sering terjadi. Maka dari itu, jaringan *Ad-hoc* memerlukan *routing protocol* yang dinamis karena protokol ini dapat bekerja jika *node* sumber memerlukan jalur untuk mentransmisikan sebuah data menuju *node* tujuan. Salah satu *routing protocol* yang memiliki sifat dinamis adalah AODV [19].

2.2.3 *Ad-hoc On Demand Vector* (AODV)

Routing protocol AODV adalah salah satu jenis protokol yang termasuk pada jenis *routing protocol* reaktif. AODV menentukan sebuah jalur apabila sebuah *node* membutuhkan proses pengiriman data. Pada jaringan *Ad-hoc routing* ini sangat lah diperlukan karena mobilitasnya yang sangat tinggi dan pergerakan yang tidak beraturan, sehingga saat sebuah *node* memerlukan sebuah jalur ke tujuan yang belum mempunyai jalur maka *node* tersebut akan mengirim sebuah paket permintaan rute ke seluruh jaringan. *Node* yang menerima paket ini akan melakukan pembaharuan informasi kepada *node* sumber serta akan mengatur penunjuk rute ke *node* sumber tersebut, selain itu node tersebut juga akan menuliskan penunjuk rute tersebut pada sebuah tabel rute. Hal ini lah yang membuat *routing protocol* AODV berbeda dibandingkan dengan *routing protocol* lain [20].

Ketika *node* sumber memiliki paket permintaan, *routing protocol* AODV akan menjalankan tugasnya sebagai pencari jalur terbaik dan akan mengarahkan kepada *node* tujuan. Kemudian AODV akan melakukan *route discovery*, dalam hal ini AODV akan mengirimkan *route request* (RREQ) kepada seluruh *node* yang ada disekitar *node* sumber dalam jaringan tertentu. Selain itu *ID Broadcast* dan *Sequence number* juga turut dikirimkan kepada *node* tersebut untuk mencegah terjadinya pengiriman pesan secara bersamaan saat menyebarkan RREQ. Penyebaran akan terus dilakukan hingga *node* tujuan berhasil dicapai. Setelah *node* tujuan mendapatkan RREQ, *node* tersebut akan mengirimkan balasan berupa *Route Replay* (RREP). Jalur yang dipilih oleh AODV merupakan jalur yang meiliki jarak terpendek dan biaya yang lebih rendah dibandingkan dengan jalur lainnya. Demi mencegah terjadinya perubahan topologi dan pemutusan rute ke *node* tujuan, AODV akan mengirimkan pesan HELLO saat proses *routing* berlangsung, selanjutnya sebuah pesan *route error* (RRER) akan dikirimkan oleh *node* tersebut menuju *node* sumber. Setelah RRER diterima oleh *node* sumber maka proses pencarian rute akan terus dilakukan lagi demi menemukan *node* tujuan asli [21]. Gambar *routing protocol* AODV ditunjukkan pada Gambar 2.2

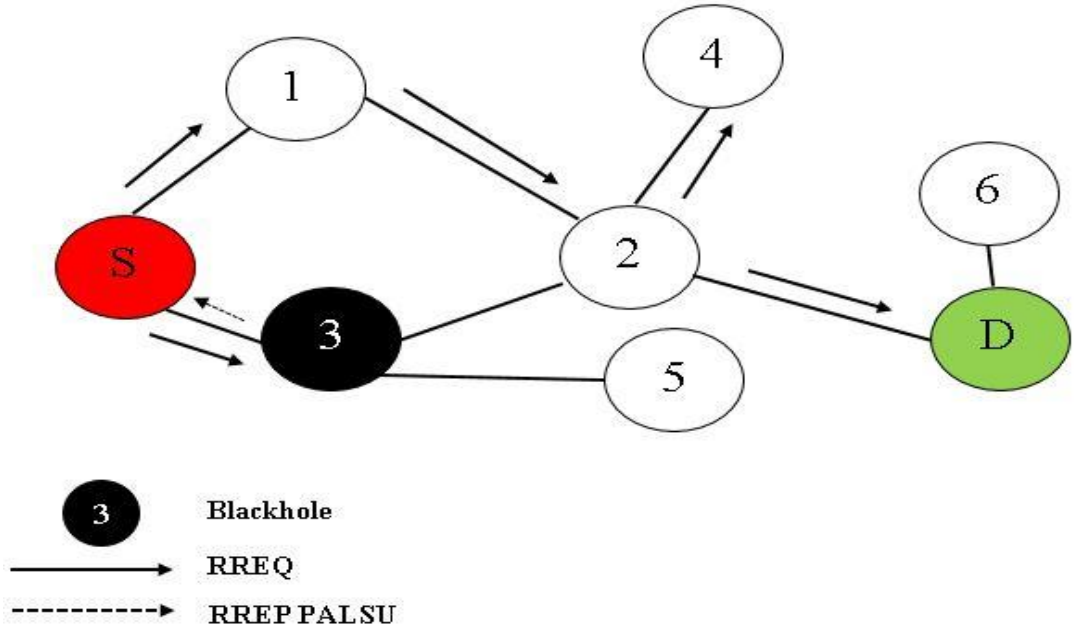


Gambar 2.2 Proses *routing* AODV

Keuntungan dari *routing protocol* AODV antara lain mendapatkan jalur terbaru karena nomor urut tujuan (*routing table*), mengurangi kebutuhan memori yang berlebihan serta meredudansi rute, dan dapat diterapkan pada jaringan *Ad-hoc* berskala besar. Kekurangan dari AODV adalah membutuhkan waktu yang lebih lama dalam pengaturan koneksi dan membangun rute awal untuk berkomunikasi, saat *node* berisi entri lama dapat menyebabkan inkonsistensi dalam rute, jika ada beberapa paket balasan bersamaan maka akan menyebabkan *overhead control* yang berat [20].

2.2.4 Serangan *Blackhole* (*Blackhole Attack*)

Serangan *blackhole* adalah sebuah serangan dimana node penyerang akan mengenalkan diri sebagai node tujuan yang palsu kepada node sumber untuk memperoleh rute yang diinginkan sebagai pemilik rute terpendek untuk mencapai *node* tujuan. Selanjutnya setelah *node* tujuan palsu mendapatkan RREQ, *node* penyerang akan mengirimkan paket RREP palsu kepada *node* sumber tanpa melihat informasi mengenai *node* tujuan. *Node* penyerang memberikan *sequence number* palsu untuk memanipulasi RREP, selanjutnya *node* penyerang akan menyatakan bahwa *node* ini memiliki rute dengan jalur yang paling pendek dan baru. Serangan *blackhole* ini dapat dibagi menjadi dua kategori yaitu serangan secara kelompok yaitu yang dilakukan lebih dari satu *node* dan serangan secara individual yang dilakukan oleh satu *node* [22]. Gambar 2.3 menunjukkan proses terjadinya *blackhole*



Gambar 2.3 *Node* penyerang mengirimkan RREP palsu

Dengan nilai *sequence number node* tujuan yang tinggi dan paket RREP yang pertama kali diterima oleh *node* sumber, maka *node* lain akan menolak semua paket RREP walaupun *node* tersebut adalah jalur yang sebenarnnya. Sehingga rute antara *node* sumber dan *node* penyerang akan tercipta yang mengakibatkan proses pengiriman paket dari *node* sumber ke *node* tujuan terputus. *Node* peneyerang kemudian akan membuang seluruh paket yang diterima dari *node* sumber [23].

2.2.5 *Quality of Service* (QoS)

QoS adalah sebuah metode pengukuran yang digunakan untuk mengetahui seberapa baik jaringan yang telah dibuat, selain itu juga dapat digunakan untuk mengetahui bahwa para pengguna sudah mendapatkan performansi yang baik dari suatu aplikasi berbasis jaringan. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah memiliki spesifikasi tertentu [24]. Tujuan dari QoS adalah menyempurnakan kebutuhan layanan yang berbeda-beda dengan menggunakan infrastruktur yang sama. Performansi QoS digunakan untuk meningkatkan kecepatan dan keketepatan penyampaian berbagai jenis data dalam sebuah jaringan komunikasi. Performansi ini memiliki banyak parameter salah satunya adalah *data dropped*, *delay*, dan *throughput* [18].

a. *Data dropped* adalah banyaknya data yang hilang selama proses transmisi berlangsung. Besarnya data yang hilang dapat berupa satuan *bits/second* [25].
b. *Throughput* adalah jumlah *bit* yang diterima oleh *nod*e tujuan dengan sukses perdetik melalui sebuah sistem ataupun media komunikasi dalam rentang waktu tertentu, pada umumnya keberhasilan ini ditunjukkan dalam satuan *bits/second*.
c. *Delay* adalah waktu tunda atau latensi yang terjadi pada sebuah data saat pengiriman berlangsung dari *node* sumber menuju *node* tujuan.

2.2.6 Metode Mitigasi Serangan *Blackhole*

Jaringan VANET memiliki mobilitas yang tinggi dan juga perubahan tempat pada *node* yang tidak beraturan. Hal ini lah yang menyebabkan jaringan VANET rentan terhadap serangan *blackhole*. Untuk meminimalisisir dampak dari kelemahan jaringan VANET perlu dilakukan langkah mitigasi yang tepat. Beberapa penelitian telah mencoba untuk mencegah serangan blackhole dengan parameter dan skenario yang berbeda, salah satu mitigasi yang dilakukan adalah dengan cara menggunakan penambahan jumlah *node*, perubahan jarak antar *node,* dan penambahan *data rate* [26]. Pada penelitian tersebut mitigasi diimplementasikan pada jaringan MANET, sehingga disini peneneliti menggunakan mitigasi penambahan *data rate* untuk diimplimentasikan pada jaringan VANET. Metode penambahan *data rate* dipilih karena jaringan VANET memiliki kecepatan dan mobilitas yang sangat tinggi, selain itu pada jalan raya, jumlah dan kecepatan kendaraan tidak dapat diprediksi dengan akurat. Hal ini mengartikan bahwa melakukan perubahan untuk jumlah dan jarak *node* sangat tidak mungkin untuk dilakukan. Selanjutnya akan dilakukan evaluasi dan perbandingan dengan cara melihat parameter QoS.

BAB 3
METODOLOGI

3.1 Alat dan Bahan

Penelitian ini dilakukan dengan cara membuat simulasi pada software simulator yang ada di perangkat computer. Perangkat-perangkat yang dibutuhkan akan dijelaskan pada sub bab berikut

3.1.1 Perangkat Keras

Pada penenlitian ini dibutuhkan sebuah laptop untuk menjalankan proses simulasi, adapun laptop yang digunakan oleh penulis adalah sebagai berikut:

a. Intel® Core™ i7-7500U CPU @ 2.70 GHz
b. RAM 8 GB (DDR4)
c. Harddisk 1 TB
d. Nvidia GeForce 940 MX (2 GB, GDDR5)

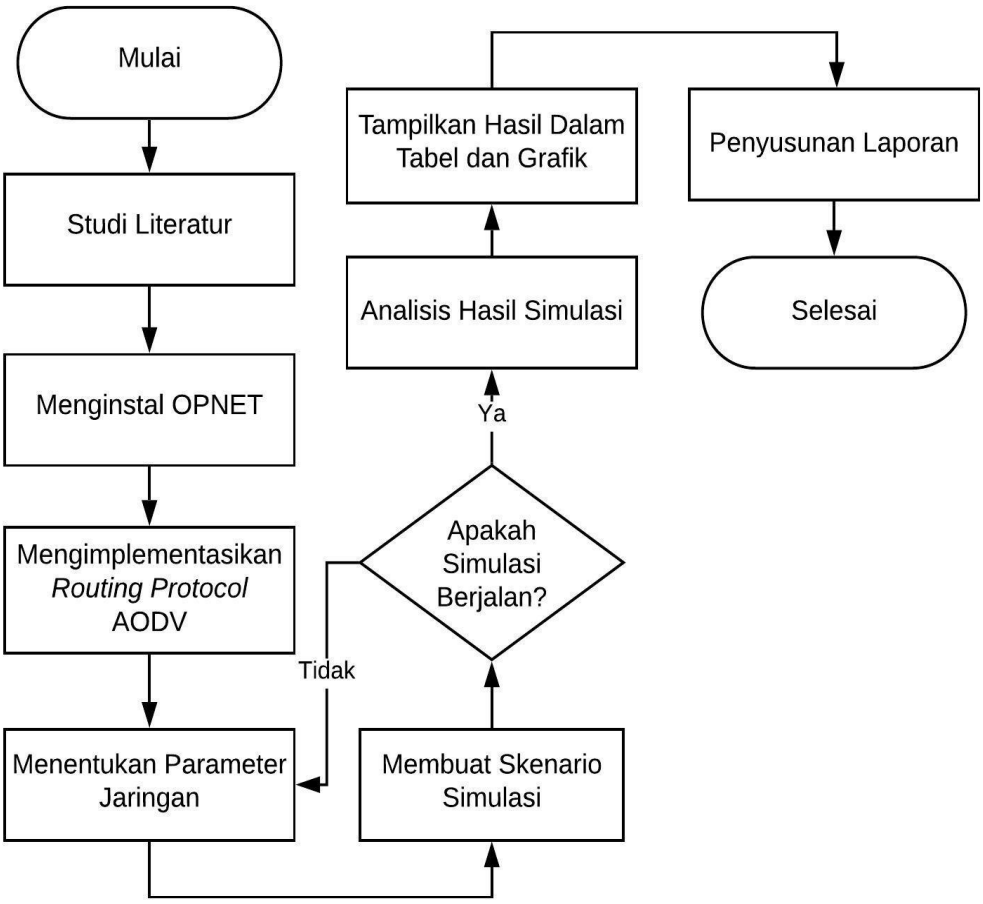
3.1.2 Perangkat Lunak

Penelitian ini juga membutuhkan beberapa perangkat lunak pendukung yang digunakan untuk menjalankan simulasi dan mencatat hasil yang didapatkan. Perangkat lunak yang digunakan adalah sebagai berikut:

a. Windows 10 Education
b. Microsoft Silver Light 2008
c. OPNET Modeler 14.5
d. Microsoft Word 2016
e. Microsoft Excel 2016

3.2 Alur Penelitian

Bagian ini menjelaskan tentang alur yang dilakukan oleh penulis untuk meneyelesaikan penelitian ini. Gambar 3.1 menunjukkan alur pembahasan simulasi yang telah dilakukan oleh penulis melalui beberapa langkah yaitu



Gambar 3.1 Alur Penelitian

3.2.1 Studi Literatur

Proses ini dilakukan oleh penulis dengan mencari dan mempelajari beberapa referensi dari penelitian yang telah dilakukan sebelumnya. Penelitian tersebut dijadikan sebagai acuan dan referensi oleh penulis, sehingga skenario dan parameter bisa didapatkan dengan baik dengan berlandaskan dari penelitian yang telah dilakukan sebelumnya. Dalam hal ini peneliti mendapatkan beberapa parameter melalui *jurnal*, *paper* dan skripsi yang telah dilakukan oleh para peneliti lain.

3.2.2 Menginstal OPNET

Penelitian ini membutuhkan sebuah aplikasi yang digunakan sebagai simulator untuk membuat sebuah simulasi jaringan VANET. Simulator yang digunakan oleh penulis adalah OPNET Modeler 14.5. untuk melakukan proses instalasi diperlukan aplikasi pendukung yaitu Microsoft Silver Light.

3.2.3 Mengimplementasikan *Routing Protocol* AODV

Dalam tahap simulasi ini penulis menggunakan *routing protocol* yang AODV. Karena *routing protocol* ini dapat digunakan pada jaringan *Ad-hoc* dalam skala yang besar [20]. Saat node memerlukan proses pengiriman paket ke *node* tujuan yang belum memiliki rute, maka *node* ini akan mengirimkan RREQ ke seluruh jaringan. *Node* yang menerima paket akan memperbarui informasi dan menuliskan *routing table* untuk *node* sumber. Ketika *node* tujuan ditemukan maka *node* tujuan akan mengirmkan RREP, selanjutnya peran AODV akan bekerja sebagai penemu rute terpendek dan terbaik untuk proses komunikasi antara *node* sumber dan *node* tujuan.

3.2.4 Menentukan Paramater Jaringan

Pada penelitian ini penulis memilih parameter jaringan sesuai skenario yang diperlukan agar simulasi dapat berjalan dengan baik dan hasilnya bisa didapatkan secara maksimal. Tabel 3.1 memaparkan parameter jaringan yang digunakan oleh penulis

Tabel 3.1 Parameter Jaringan

No	Parameter	Jaringan	Keterangan Penggunaan
1	Panjang Jarak Area	7 Kilometer	Semua Skenario
2	Kecepatan *Node*	70 Kilometer/Jam	Semua Skenario
3	Jumlah *Node*	20	Semua Skenario
4	*Data rate* setiap *Node*	1 Mbps	Semua Skenario
5	Waktu simulasi	5 menit	Semua Skenario
6	Teknologi Jaringan	WLAN 802.11B	Semua Skenario
7	*Node Blackhole*	4	Skenario Serangan Blackhole
8	*Data rate Node Blackhole* Mitigasi Pertama	2 Mbps	Skenario Mitigasi Blackhole
9	*Data rate Node Blackhole* Mitgasi Kedua	3 Mbps	Skenario Mitigasi Blackhole

3.2.5 Menentukan Paramater Simulasi

Pada penelitian ini penulis menggunakan parameter QoS sebagai tolak ukur atas keberhasilan penelitian ini. QoS sendiri adalah sekumpulan parameter yang bertujuan untuk mengetahui kinerja dari suatu aplikasi jaringan [24]. Paramater QoS yang digunakan oleh penulis adalah *data dropped*, *delay*, dan *throughput*. Masing-masing parameter tersebut telah dijelaskan pada bagian tinjauan teori.

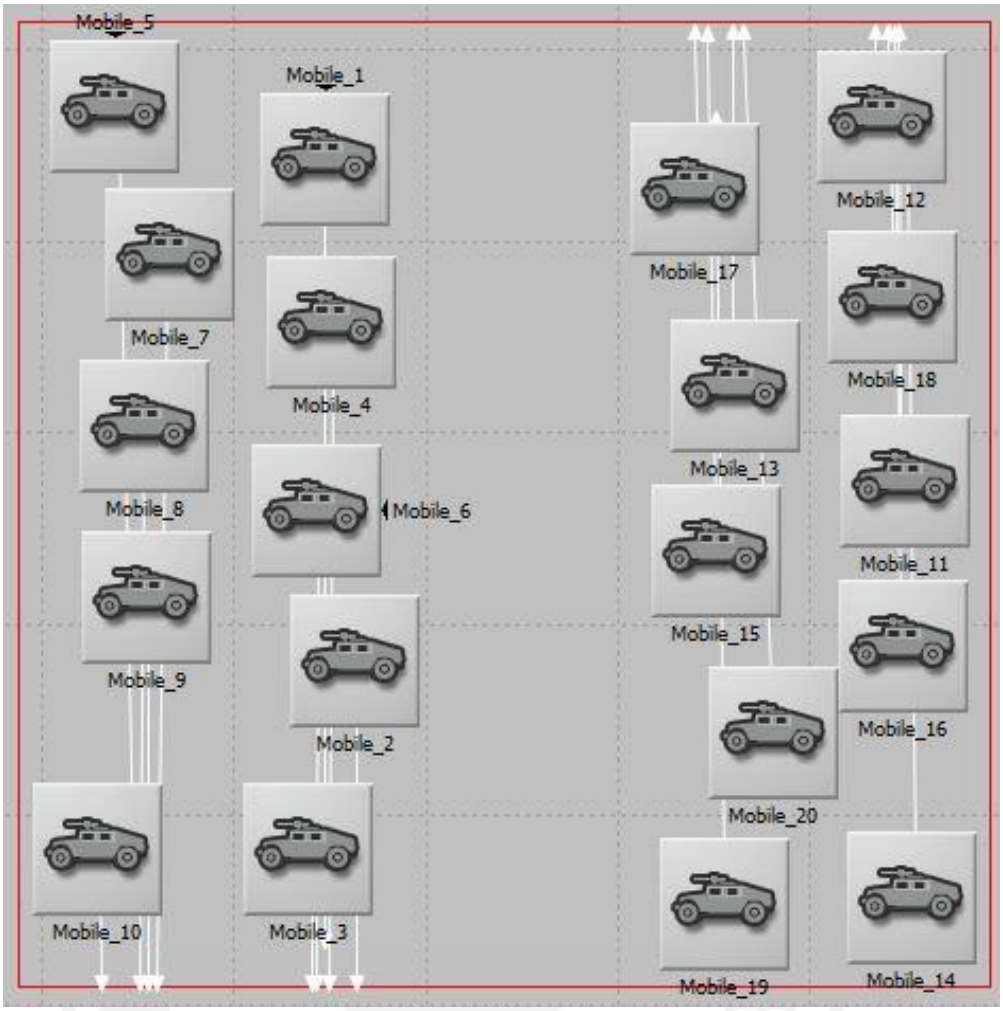
a. *Data dropped* yang digunakan oleh penulis memiliki ketentuan bahwa semakin besar nilai rata-rata *data dropped* pada suatu jaringan, maka jaringan tersebut semakin buruk. Hal ini dapat diartikan bahwa saat sebuah jaringan memiliki nilai *data dropped* yang tinggi maka semakin banyak pula paket yang dijatuhkan yang artina paket tersebut tidak berhasil dikirimkan dari node sumber ke node tujuan.
b. *Delay* yang digunakan pada penenlitian ini memiliki ketentuan bahwa semakin tinggi nilai rata-rata *delay* maka semakin buruk jaringan tersebut. Hal ini dapat diartikan bahwa saat sebuah jaringan memiliki nilai d*elay* yang tinggi, maka paket data akan dikirimkan dalam waktu yang lebih lama, sehingga proses pengiriman paket pun tidak berjalan dengan efisien.
c. *Throughput* yang digunakan pada penelitian ini memiliki ketentuan bahwa semakin rendah nilai rata-rata *throughput* maka semakin buruk jaringan tersebut. Hal ini dapat diartikan bahwa saat jaringan memiliki *throughput* yang rendah, maka pengiriman data akan sangat lambat dan menyebabkan sebuah paket terkirim dalam waktu yang lebih panjang.

3.3 Skenario Simulasi

Pada penelitian ini penulis melakukan simulasi sebanyak 3 skenario. Pada masing-masing skenario terdapat parameter yang berbeda-beda sesuai dengan kebutuhan jaringan yang akan dilakukan. Skenario tersebut adalah skenario tanpa serangan, skenario serangan *blackhol*e, dan skenario mitigasi *blackhole*. Skenario tersebut akan dilakukan beberapa kali demi mendapatkan hasil yang memuaskan, kemudian hasil-hasil tersebut akan dihitung rata-rata nya sehingga hasil yang ditampilkan dalam analisa adalah hasil rata-rata dari berbagai simulasi yang telah dilakukan. Berikut penjelasan masing-masing dari skenario tersebut:

3.3.1 Skenario Tanpa Serangan

Pada skenario ini, penulis melakukan simulasi jaringan VANET tanpa adanya serangan *blackhole*. Parameter yang digunakan diset dalam kondisi default seperti yang dituliskan pada bagian parameter jaringan. Skenario simulasi jaringan VANET dilampirkan pada Gambar 3.2



Gambar 3.2 Skenario VANET

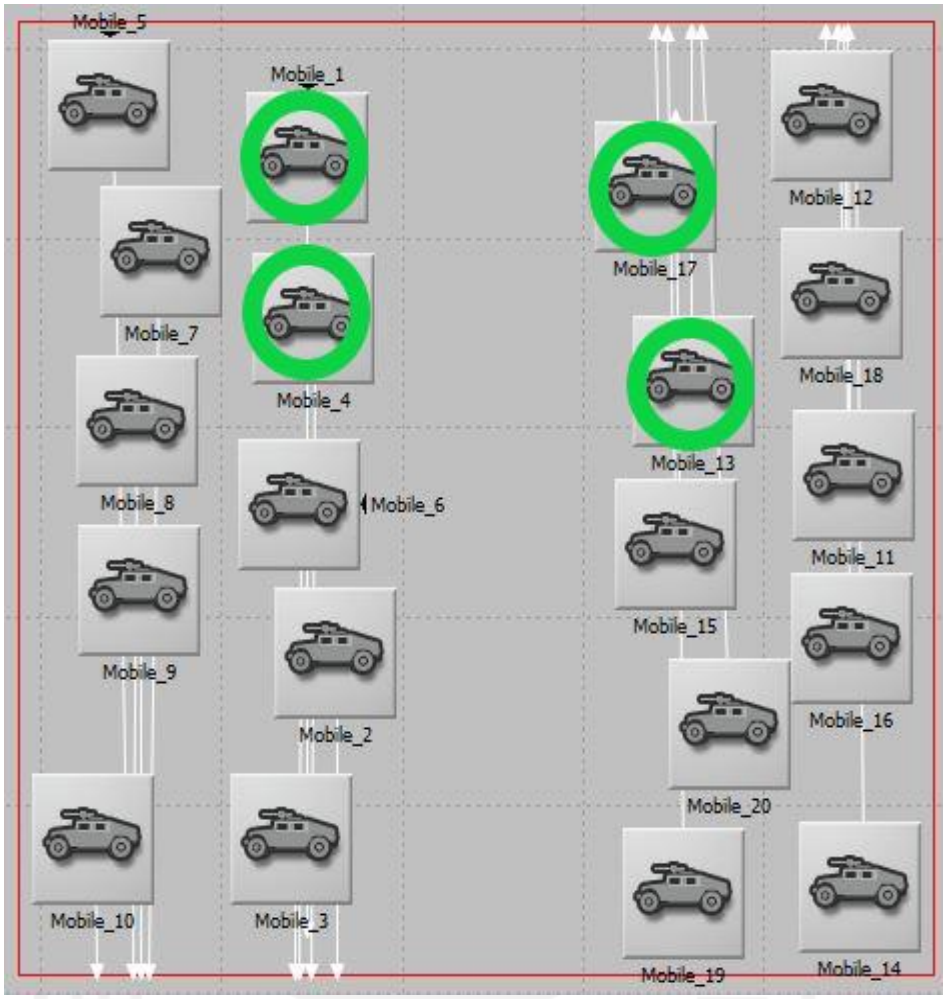
3.3.2 Skenario Serangan *Blackhole*

Pada skenario ini, penulis melakukan simulasi jaringan VANET yang terkena serangan *blackhole*, parameter yang digunakan sama seperti simulasi pada jaringan VANET hanya saja ada 4 *node* yang dijadikan sebagai *node blackhole*. Skenario dan spesifikasi simulasi serangan *blackhole* dilampirkan pada Gambar 3.3.

Gambar 3.3 Skenario Serangan *Blackhole*

3.3.3 Skenario Mitigasi *Blackhole*

Pada skenario ini, penulis melakukan simulasi untuk memitigasi jaringan VANET yang telah terkena serangan *blackhole*. Parameter yang digunakan masih sama seperti simulasi serangan *blackhole*, namun data rate pada node blackhole ditingkatkan menjadi 2 Mbps secara bertahap mulai dari memitigasi 1 node blackhole hingga keseleuruhan node blackhole. Selanjutnya akan diperlihatkan juga hasil untuk mitigasi jika data rate yang ditambahkan pada seluruh node blackhole menjadi sebesar 3 Mbps, untuk mengetahui keberhasilan metode penambahan data rate jika semakin besar yang ditambahkan pada sebuah node blackhole. Skenario dan spesifikasi simulasi mitigasi dilampirkan pada Gambar 3.4.



Gambar 3.4 Simulasi Mitigasi *Blackhole*

BAB 4
HASIL DAN PEMBAHASAN

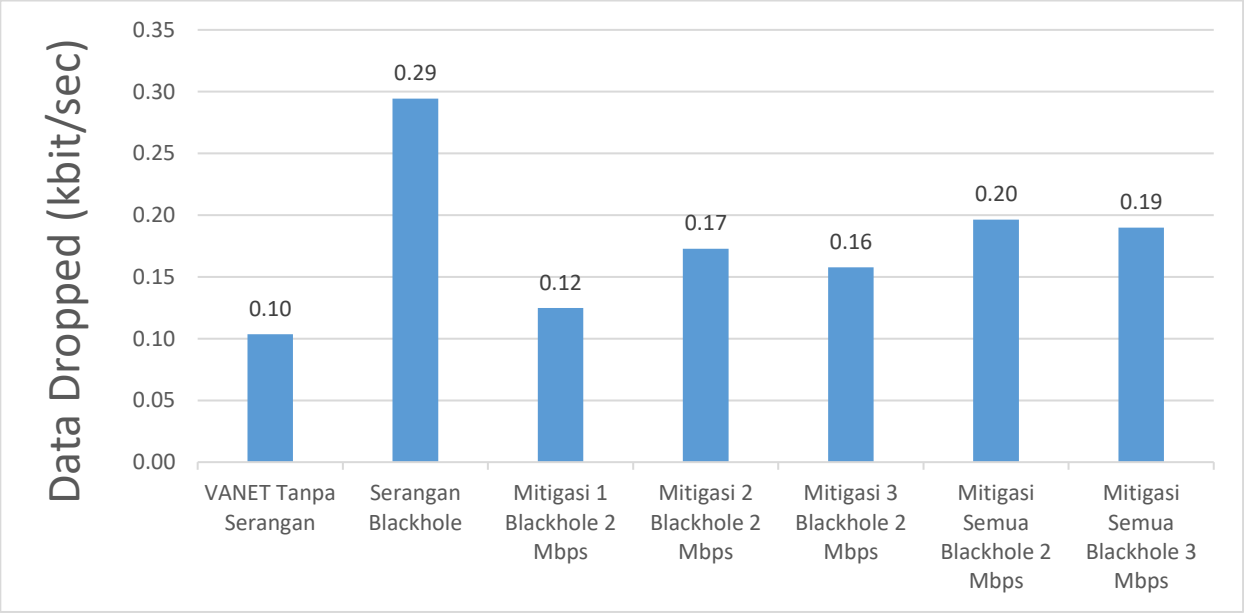
Pada Bagian ini penulis membahas keseluruhan hasil dari simulasi yang telah dilakukan hingga akhir menggunakan aplikasi OPNET Modeler 14.5. Hasil yang telah didapatkan akan diamati menggunakan parameter QoS yaitu *data dropped*, *delay*, dan *throughput*. Simulasi dilakukan sebanyak 3 skenario yang masing-masing memiliki parameter QoS. Hasil simulasi akan dipaparkan sesuai dengan parameter QoS melalui sub bab berikut:

4.1 Analisis *Data Dropped*

Pada setiap skenario nilai rata-rata *data dropped* mengalami perubahan. Data tersebut dapat dilihat pada tabel 4.1 dan gambar 4.1

Tabel 4.1 Nilai Rata-Rata *Data Dropped* (kbit/s)

No	Nama Skenario	Hasil (kbit/s)
1	VANET Tanpa Serangan	0.10
2	Serangan *Blackhole*	0.29
3	Mitigasi 1 *Blackhole* 2 Mbps	0.12
4	Mitigasi 2 *Blackhole* 2 Mbps	0.17
5	Mitigasi 3 *Blackhole* 2 Mbps	0.16
6	Mitigasi Semua *Blackhole* 2 Mbps	0.20
7	Mitigasi Semua *Blackhole* 3 Mbps	0.19



Gambar 4.1 Grafik Nilai Rata-Rata *Data Dropped* (kbit/s)

Hasil pengamatan nilai rata-rata *data dropped* yang didapatkan oleh simulator terlihat pada tabel 4.1 dan gambar 4.1. Hasil keluaran nilai rata-rata *data dropped* memiliki hasil yang berbeda-beda. Pada kondisi jaringan VANET tanpa serangan didapatkan nilai rata-rata sebesar 0,1 kbit/sec, kemudian saat terkena serangan *blackhole* nilai rata-*data dropped* memburuk menjadi 0,29 kbit/sec. Hal ini terjadi karena adanya serangan *blackhole* yang mengakibatkan banyaknya data yang dijatuhkan pada saat proses komunikasi sedang berlangsung, *node blackhole* menyebabkan komunikasi antar *node* menjadi tidak lancar sehingga akan menyebabkan antrian data yang berlebihan saat komunikasi berlangsung [18]. Selanjutnya saat dilakukan mitigasi dengan cara penambahan *data rate* secara bertahap, kinerja *data dropped* mulai naik kembali dengan hasil 0,12 kbit/sec saat memitigasi satu backhole saja hingga berakhir dengan nilai 0,20 kbit/sec saat node blackhole seluruhnya dilakukan mitigasi penambahan data rate. Hal ini berbanding lurus dengan meningkatnya data rate pada *node* yang terserang *blackhole*, sehingga *node* tersebut akan memperlancar kembali proses komunikasi antar *node* dan tidak akan menyebabkan antrian yang berlebihan saat proses komunikasi berlangsung. Saat *node blackhole* dimitigasi secara keseluruhan nilai *data dropped* kembali menurun walaupun masih meminimalisir dampak dari serangan blackhole, hal ini berbanding terbalik dengan meningkatnya kineja *delay* dan *throughput* yang meningkat saat semua *node blackhole* dimitigasi secara keseluruhan, maka dari itu penambahan *data rate* dilakukan secara keseluruhan karena melihat efektifitas dari segala parameter.saat mencoba menambahkan *data rate* yang lebih besar, yaitu menjadi 3 mbps pada *node blackhole*, hasilnya menunjukkan bahwa kinerja *data dropped* dapat ditingkatkan kembali, hal ini mengartikan bahwa semakin besar penambahan *data rate* yang dilakukan maka bisa memperbaiki jaringan yang telah terkena serangan *blackhole*. Dalam hal ini dapat dipastikan bahwa metode mitigasi berhasil untuk meminimalisir nilai *data dropped*.

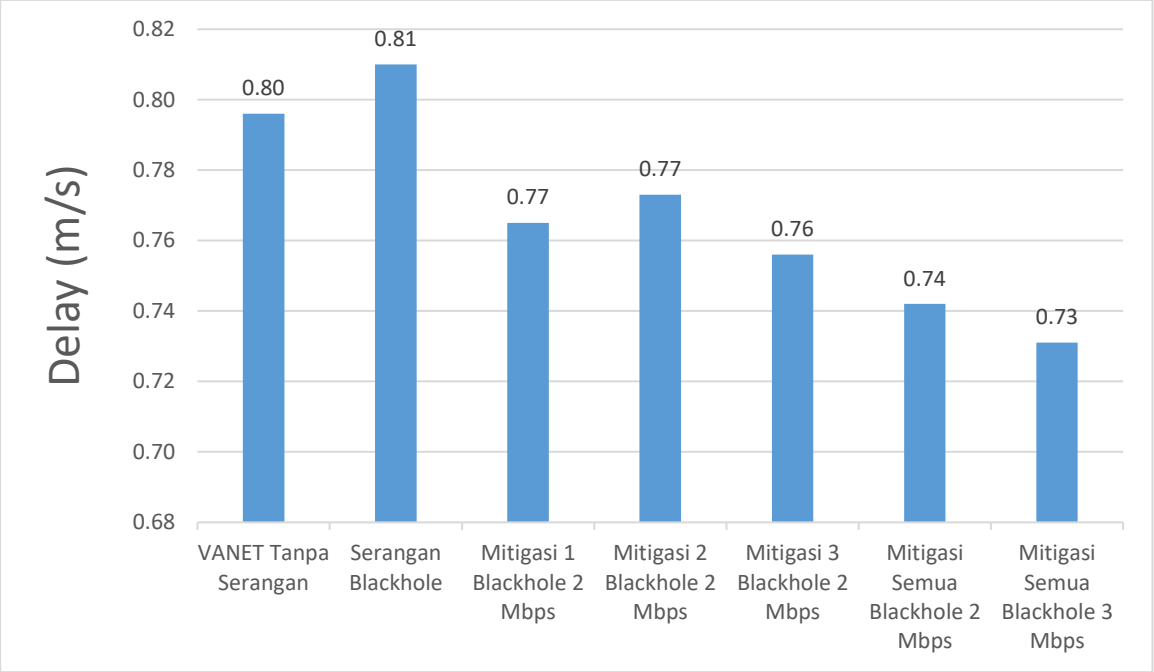
4.2 Analisis *Delay*

Hasil nilai rata-rata *delay* menunjukkan adanya perubahan pada setiap skenario. Data tersebut dapat dilihat pada tabel 4.2 dan gambar 4.2

Tabel 4.2 Nilai Rata-Rata *Delay* (ms)

No	Nama Skenario	Hasil (ms)
1	VANET Tanpa Serangan	0.80
2	Serangan *Blackhole*	0.81
3	Mitigasi 1 *Blackhole* 2 Mbps	0.77
4	Mitigasi 2 *Blackhole* 2 Mbps	0.77
5	Mitigasi 3 *Blackhole* 2 Mbps	0.76

6	Mitigasi Semua *Blackhole* 2 Mbps	0.74
7	Mitigasi Semua *Blackhole* 3 Mbps	0.73



Gambar 4.2 Grafik Nilai Rata-Rata *Delay* (ms)

Hasil pengamatan nilai rata-rata *delay* yang diperoleh dari simulator menunjukkan adanya perbedaan data yang terjadi pada setiap skenario. Data ini dapat dilihat pada tabel 4.2 dan gambar 4.2. Hasil menyebutkan saat skenario jaringan VANET berlangsung delay yang diperoleh adalah sebesar 0,79 ms. Kemudian saat adanya serangan *blackhole* pada skenario serangan *blackhole*, parameter *delay* mengalami penurunan kinerja, sehingga nilai delaynya naik menjadi 0,81 ms. Hal ini menunjukkan bahwa adanya *node* penyerang bisa mengakibatkan *delay* menjadi bertambah, karena *node* penyerang akan menghalangi proses pencarian rute yang benar kepada *node* tujuan yang sesunggguhnya. Hal ini mengakibatkan proses pegiriman data akan memerlukan waktu yang lebih lama, sehingga membahayakan para pengendara dijalan yang memerlukan informasi secara *real time*. Saat dilakukan mitigasi, kinerja parameter *delay* dapat ditingkatkan kembali sesuai banyaknya *node blackhole* yang dilakukan penambahan *data rate*.Nilai rata-rata *delay* dapat diturunkan dari 0,77 ms saat hanya satu *node blackhole* yang dilakukan mitigasi, hingga bernilai 0,74 ms saat seluruh *node blackhole* dilakukan mitigasi dengan penambahan *data rate*. Selanjutnya saat nilai *data rate* menjadi lebih tinggi dan digunakan kepada seluruh *node blackhole* maka hasilnya bisa menurunkan nilai rata-rata *delay* menjadi 0,73 ms. Hal ini dikarenakan penambahan data rate pada *node* yang terserang *blackhole* mengakibatkan proses transmisi data pada *node* tersebut meningkat dibandingkan saat terserang dengan *data rate* yang sama seperti node lainnya,

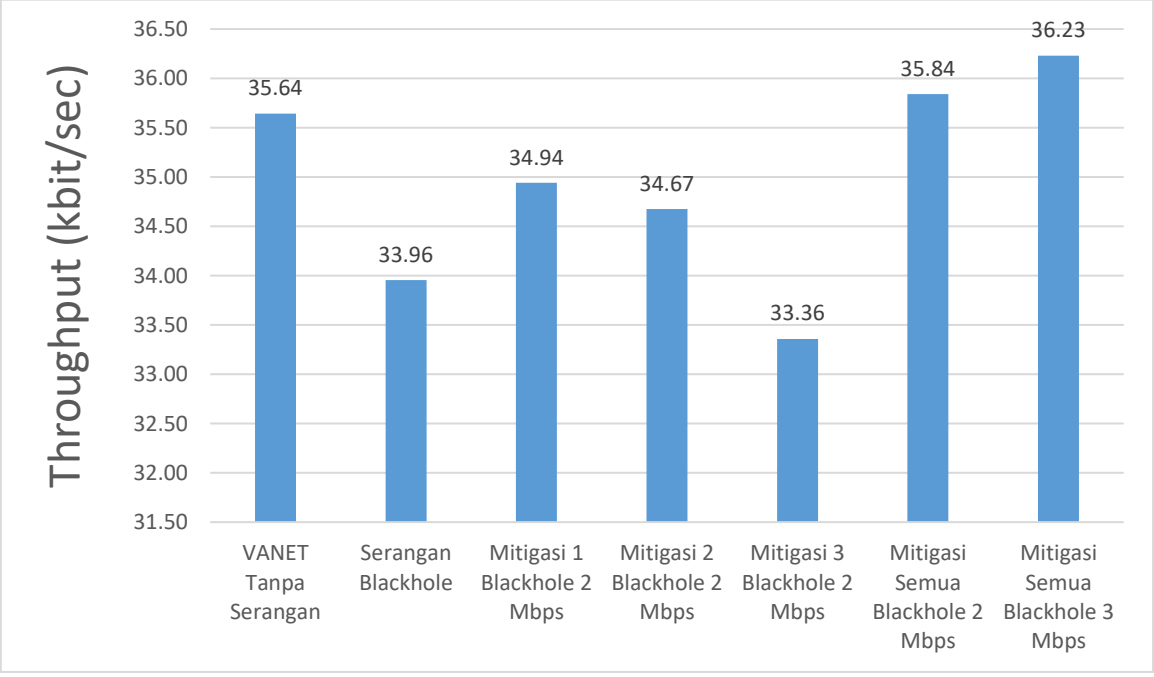
sehingga proses penemuan rute ke *node* tujuan asli juga ikut meningkat. Hasil membuktikan bahwa semakin besar penambahan *data rate* yang dilakukan pada sebuah jaringan *blackhole* maka jaringan tersebut bisa diperbaiki kembali bahkan nilainya lebih baik dari sebelum terserang *blackhole*. Panambahan *data rate* pada *node* yang terkena serangan *blackhole* dinyatakan berhasil diatasi, karena *delay* menjadi lebih baik sehingga menguntungkan para pengendara untuk mendapatkan informasi seputar jalanan secara *real time*.

4.3 Analisis *Throughput*

Hasil simulasi menunjukkan adanya perbedaan nilai rata-rata *throughput* pada setiap skenario. Data tersebut dapat dilihat pada tabel 4.3 dan gambar 4.3

Tabel 4.3 Nilai Rata-Rata *Throughput*

No	Nama Skenario	Hasil (kbit/sec)
1	VANET Tanpa Serangan	35.64
2	Serangan *Blackhole*	33.96
3	Mitigasi 1 *Blackhole* 2 Mbps	34.94
4	Mitigasi 2 *Blackhole* 2 Mbps	34.67
5	Mitigasi 3 *Blackhole* 2 Mbps	33.36
6	Mitigasi Semua *Blackhole* 2 Mbps	35.84
7	Mitigasi Semua *Blackhole* 3 Mbps	36.23



Gambar 4.3 Grafik Nilai Rata-Rata *Throughput* (kbit/s)

Hasil pengamatan nilai rata-rata *throughput* yang diperoleh dari simulator dapat dilihat pada tabel 4.3 dan gambar 4.3. Hasilnya menunjukkan pada saat kondisi tanpa serangan, nilai *throughput* diperoleh sebesar 35,64 kbit/sec. Kemudian saat terjadi serangan *blackhole* pada skenario serangan *blackhole* parameter *throughput* mengalami penurunan kinerja sehingga nilai throughput menurun menjadi 33,95 kbit/sec. Hal ini disebabkan oleh Node *blackhole* yang menyebabkan proses transfer data antar *node* terganggu [9]. Masalah tersebut selanjutkan akan menyebabkan kecepatan pengiriman data yang sedang berlangsung menurun sehingga pengiriman paket data akan mengalami keterlambatan. Kemudian saat proses mitigasi dilakukan maka parameter throughput akan mengalami kenaikan kinerja kembali secara bertahap dengan penambahan *data rate* dari satu *node* yang terkena *blackhole* hingga melakukan penambahan *data rate* keseluruh *node blackhole,* nilainya pun mengalami kenaikan secara bertahap dari 14.94 kbit/sec hingga 35.84 kbit/sec. Hal ini disebabkan oleh penambahan *data rate* pada *node blackhole,* sehingga *node blackhole* memiliki kecepatan transfer data yang lebih cepat dibandingkan dengan *node* lainnya dan banyaknya *bit* data yang terkirim ke *node* tujuan akan lebih banyak. Semakin banyak *node blackhole* yang dimitigasi dengan penambahan *data rate*, maka semakin cepat pula proses pengiriman dapat dilakukan sehingga hasilnya pun dapat dilihat sangat memuaskan saat *node blackhole* dilakukan penambahan *data rate* secara keseluruhan. Saat dilakukan penambahan *data rate* dengan nilai yang lebih tinggi, hasilnya kembali meningkat menjadi 36,23 kbit/sec, hal ini menunjukkan bahwa semakin besar nilai *data rate* yang ditambahkan pada *node blackhole* maka hasilnya dapat memperbaiki kinerja jaringan VANET yang telah terserang *blackhole*. Pada akhirnya hasil yang didapatkan sangat memuaskan dikarenakan nilai rata-rata *throughput* menjadi lebih baik dari sebelum terkena serangan, sehingga kecepatan pengiriman paket pun semakin meningkat dan akan berpengaruh pada pengendara untuk mendapatkan akses data yang lebih cepat dan akurat.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada penelitian ini didapatkan kesimpulan bahwa:

1. Serangan *blackhole* mengakibatkan kinerja pada jaringan VANET menurun. Hal ini dapat dilihat dari beberapa parameter QoS, yaitu data *dropped*, *delay*, dan *throughput* yang kinerjanya menurun saat ada serangan *blackhole*. Kinerja *data dropped* turun sebesar 0,29 kbit/sec, pada *delay* kinerja menurun sebesar 0,81 ms, dan *throughput* kinerjanya menurun sebesar 33,95 kbit/sec.
2. Untuk meminimalisir dampak serangan *blackhole* pada jaringan VANET perlu dilakukan sebuah metode, salah satunya adalah penambahan *data rate*. Kinerja jaringan VANET dapat ditingkatkan kembali dengan melihat beberapa parameter QoS. Kinerja *data dropped* meningkat sebesar 0,2 kbit/sec, pada *delay* dan *throughput* kinerjanya meningkat lebih baik dibandingkan dengan sebelum ada serangan yaitu sebesar 0,74 ms pada kinerja *delay* dan 35,84 kbit/sec pada kinerja *throughput*.
3. Metode mitigasi penambahan *data rate* dinyatakan berhasil karena mampu menaikkan performa jaringan VANET setelah terkena serangan *blackhole*, dengan parameter *data dropped*, *delay*, dan *throughput*.

5.2 Saran

Pada penelitian ini terdapat beberapa saran yaitu:

1. Melakukan perbaikan kinerja jaringan VANET menggunakan protokol lain terhadap serangan *blackhole*
2. Melakukan metode mitigasi serangan *blackhole* dengan cara lain.
3. Menguji kinerja jaringan VANET menggunakan parameter QoS yang lain.
4. Melakukan penelitian untuk meningkatkan kinerja jaringan VANET agar tidak terdampak serangan lain seperti *blackhole*, *wormhole*, dan *grayhole*.

DAFTAR PUSTAKA

[1] L. Raja and C. S. Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges," *International Journal of Computer Science and Mobile Computing*, vol. 3131, no. 1, pp. 408–417, 2014, [Online].

[2] A. Varga *et al.*, "Discrete Mathematics third edition," *WEIRD workshop on WiMax, wireless and mobility*, vol. 25, no. 3, pp. 2456–2460, 2011, doi: 10.1109/ICIT.2008.28.

[3] M. Sood and S. Kanwar, "Clustering in MANET and VANET: A survey," *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications, CSCITA 2014*, pp. 375–380, 2014, doi: 10.1109/CSCITA.2014.6839290.

[4] S. Sridhar, R. Baskaran, and P. Chandrasekar, "Energy Supported AODV (EN-AODV) for QoS Routing in MANET," *Procedia - Social and Behavioral Sciences*, vol. 73, pp. 294–301, 2013, doi: 10.1016/j.sbspro.2013.02.055.

[5] R. Sugumar and J. Hussain, "The Enhanced Network Architecture , Route discovery and Data Transmission of AODV," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 10, pp. 453–460, 2017.

[6] R. Baiad, O. Alhussein, H. Otrok, and S. Muhaidat, "Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET," *Vehicular Communications*, vol. 5, pp. 9–17, 2016, doi: 10.1016/j.vehcom.2016.09.001.

[7] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017, doi: 10.1016/j.vehcom.2017.01.002.

[8] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks*, vol. 113, pp. 94–110, 2017, doi: 10.1016/j.comnet.2016.12.006.

[9] T. Bhatia and A. K. Verma, "Performance Evaluation of AODV under Blackhole Attack," *International Journal of Computer Network and Information Security*, vol. 5, no. 12, pp. 35–44, 2013, doi: 10.5815/ijcnis.2013.12.05.

[10] M. Arif, B. Aji, and A. A. Zahra, "Evaluasi Kinerja Protokol Routing Dsdv Terhadap Pengaruh Malicious Node Pada Manet Menggunakan Network Simulator 2 (Ns-2)," *Transient*, vol. 4, no. 4, 2015.

[11] Rendra, "Analisis Perbandingan Unjuk Kerja Protokol Routing Reaktif (Dymo) Terhadap Protokol Routing Reaktif (Aodv) Di Jaringan Vanet," p. 112, 2016.

[12] V. Bibhu, K. Roshan, K. B. Singh, and D. K. Singh, "Performance Analysis of Black Hole Attack in Vanet," *International Journal of Computer Network and Information Security*, vol. 4, no. 11, pp. 47–54, 2012, doi: 10.5815/ijcnis.2012.11.06.

[13] E. Mustikawati, D. Perdana, and R. M. Negara, "Network Security Analysis in Vanet Against Black Hole and Jellyfish Attack with Intrusion Detection System Algorithm," *CommIT (Communication and Information Technology) Journal*, vol. 11, no. 2, p. 77, 2017, doi: 10.21512/commit.v11i2.3886.

[14] J. Tobin, C. Thorpe, and L. Murphy, “An Approach to Mitigate Black Hole Attacks on Vehicular Wireless Networks,” *IEEE Vehicular Technology Conference*, vol. 2017-June, 2017, doi: 10.1109/VTCSpring.2017.8108460.

[15] A. Martorana, G. Primero, and J. Tagliabue, “Simulation of a Trust Reputation Based Mitigation Protocol for a Blackhole Style Attack on VANET,” *Middlesex University Research Repository*, 2018.

[16] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” *Vehicular Communications*, vol. 9, pp. 19–30, 2017, doi: 10.1016/j.vehcom.2017.02.001.

[17] M. N. Rajkumar, M. Nithya, and P. Hemalatha, “Overview of Vanet With Its Features and Security Attacks,” *International Research Journal of Engineering and Technology*, vol. 03, no. 01, pp. 137–142, 2016, [Online].

[18] F. Amilia, Marzuki, and Agustina, “Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) Dan Geographic Routing Protocol (GRP) Pada Mobile Ad Hoc Network (MANET),” *Jurnal Sains, Teknologi dan Industri*, vol. 12, no. 1, pp. 9–15, 2014.

[19] A. A. Chavan, D. S. Kurule, and P. U. Dere, “Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack,” *Procedia Computer Science*, vol. 79, pp. 835–844, 2016, doi: 10.1016/j.procs.2016.03.108.

[20] B. Paul, “Survey over VANET Routing Protocols for Vehicle to Vehicle Communication,” *IOSR Journal of Computer Engineering*, vol. 7, no. 5, pp. 01–09, 2012, doi: 10.9790/0661-0750109.

[21] Sulandari, “Analisis Pengaruh Blackhole Attack Pada Jaringan VANET,” Universitas islam Indonesia, 2019.

[22] I. Pratomo and H. Hizburrahman, “Pendeteksian Dan Pencegahan Serangan Black Hole,” *JAVA Journal of Electrical and Electronics Engineering*, vol. 13, no. 1, pp. 47–53, 2015.

[23] M. K. S. Amanpreet Kaur, “Diminution of MANET Attacks by HOOSC Scheme,” *International Journal of Science and Research (IJSR)*, vol. 3, no. 10, p. —, 2014, [Online]. Available: https://www.ijsr.net/archive/v3i10/T0NUMTQ1Mg==.pdf.

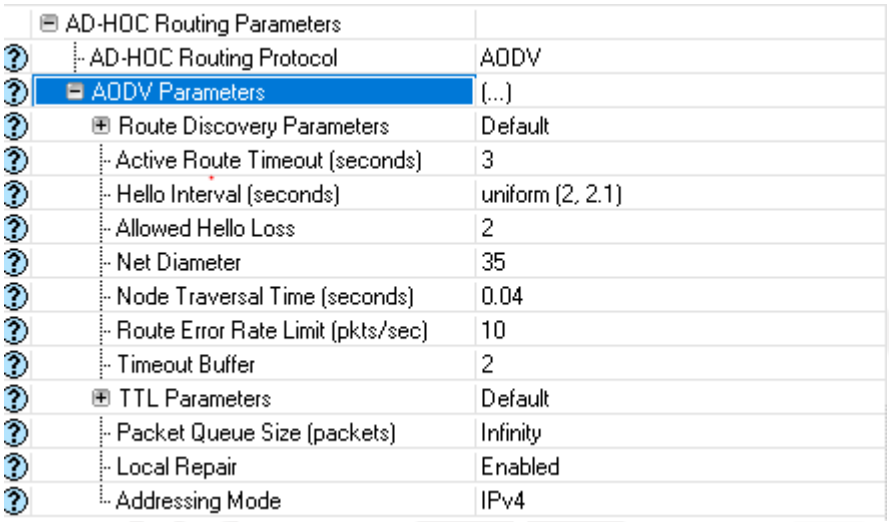
[24] R. Wulandari, “Analisis QoS (Quality of Service) Pada Jaringan Internet (Studi Kasus : UPT Loka Uji Teknik Penambangan Jampang Kulon – LIPI),” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 2, no. 2, pp. 162–172, 2016, doi: 10.28932/jutisi.v2i2.454.

[25] M. Alkhathami, L. Alazzawi, and A. Elkateeb, “Border surveillance and intrusion detection using wireless sensor networks,” *International Journal of Advances in Engineering & Technology*, vol. 8, no. 2, p. 17, 2015.

[26] Fathullah, “Simulasi Dan Analisis Perbandingan Kinerja Teknik Mitigasi Serangan Blackhole Pada Jaringan Manet,” vol. 2018, no. November, 2018.

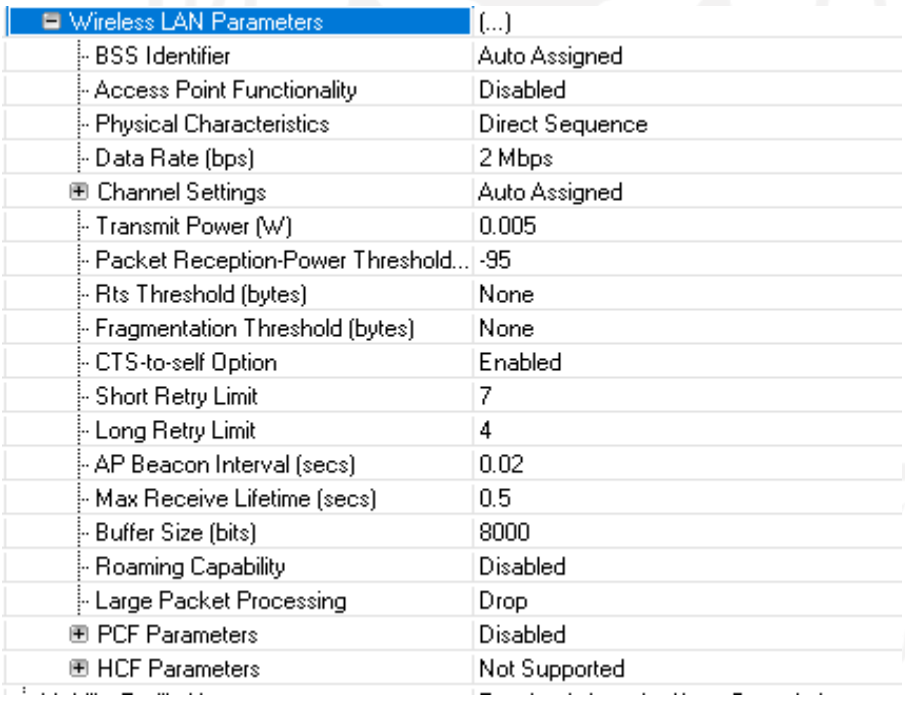
LAMPIRAN

1. Setting *node blackhole*



AD-HOC Routing Parameters	
AD-HOC Routing Protocol	AODV
AODV Parameters	(...)
Route Discovery Parameters	Default
Active Route Timeout (seconds)	3
Hello Interval (seconds)	uniform (2, 2.1)
Allowed Hello Loss	2
Net Diameter	35
Node Traversal Time (seconds)	0.04
Route Error Rate Limit (pkts/sec)	10
Timeout Buffer	2
TTL Parameters	Default
Packet Queue Size (packets)	Infinity
Local Repair	Enabled
Addressing Mode	IPv4

2. Setting mitigasi *blackhole*



Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	2 Mbps
Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	8000
Roaming Capability	Disabled
Large Packet Processing	Drop
PCF Parameters	Disabled
HCF Parameters	Not Supported