SIMULASI DAN ANALISIS PERBANDINGAN KINERJA TEKNIK MITIGASI SERANGAN *BLACK HOLE* PADA JARINGAN MANET

SKRIPSI

untuk memenuhi salah satu persyaratan
mencapai derajat Sarjana S1

Disusun oleh:

Fathullah

14524135

Jurusan Teknik Elektro

Fakultas Teknologi Industri

Universitas Islam Indonesia

Yogyakarta

2018

LEMBAR PENGESAHAN

SIMULASI DAN ANALISIS PERBANDINGAN TEKNIK MITIGASI SERANGAN *BLACK HOLE* PADA JARINGAN MANET

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:

Fathullah
14524135

Yogyakarta, 16 Agustus 2018

Menyetujui,

Pembimbing 1

Ida Nurcahayani ST., M.Eng
155240104

LEMBAR PENGESAHAN

SKRIPSI

SIMULASI DAN ANALISIS PERBANDINGAN KINERJA TEKNIK MITIGASI SERANGAN *BLACK HOLE* PADA JARINGAN MANET

Dipersiapkan dan disusun oleh:

Fathullah

14524135

Telah dipertahankan di depan dewan penguji

Pada tanggal: 20 Agustus 2018

Susunan dewan penguji

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

Anggota Penguji 1: Dr. Eng. Hendra Setiawan S.T., M.T , _____

Anggota Penguji 2: Tito Yuwono S.T M.Sc, _____

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

Tanggal: 20 Agustus 2018

Ketua Program Studi Teknik Elektro

UNIVERSITAS ISLAM INDONESIA ★ YOGYAKARTA ★ FAKULTAS TEKNOLOGI INDUSTRI

Yusuf Aziz Amrulloh S.T., M.Eng., 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, 16 Agustus 2018

Fathullah

KATA PENGANTAR

Assalamu'alaykum warahmatullahi wabarakatuh

Alhamdulillahirabbil'alamin, puji dan syukur penulis panjatkan kepada Allah SWT yang Maha Pengasih dan Maha Penyayang, yang telah memberikan rahmat serta karunia-NYA sehingga Tugas Akhir yang berjudul: "Analisis Perbandingan Teknik Mitigasi Black hole Pada Jaringan MANET"**,** ini dapat diselesaikan dengan baik dan lancar. Tak lupa pula Shalawat dan Salam tercurahkan kepada Rasulullah Muhammad SAW. Yang menjadi teladan bagi kita.

Penelitian ini dilakukan dengan metode simulasi. Tujuan penulisan laporan Tugas Akhir ini sebagai salah satu syarat kelulusan pada pada Pendidikan Strata Satu (S1) Fakultas Teknologi Industri Jurusan Teknik Elektro Universitas Islam Indonesia selain itu agar dapat bermanfaat bagi para pembaca.

Dalam penulisan laporan tugas akhir ini penulis mendapatkan bantuan dari berbagai pihak untuk itu penulis mengucapkan banyak terima kasih atas bantuan dan dukungannya. Penulis mengucapkan terima kasih antara lain kepada:

1. Kedua orang tua penulis atas semua dukungan, semangat, fasilitas, motivasi, serta doa yang telah mereka berikan.
2. Bapak Dr.Eng. Hendra Setiawan, S.T., M.T selaku Ketua Jurusan Teknik Elektro Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Ibu Ida Nurcahyani, S.T., M, Eng. selaku Dosen Pembimbing Tugas Akhir yang telah mendampingi dan memberikan berbagai masukan, arahan, motivasi, serta doa dalam penulisan laporan ini.
4. Segenap Dosen dan staff Jurusan Teknik Elektro Fakultas Teknologi Industri Universitas Islam Indonesia yang telah membimbing dan memberikan ilmunya selama penulis duduk di bangku kuliah.
5. Aa dan Teteh yang memberikan semangat dalam penulisan laporan ini
6. Abiyu Ahmad yang menjadi teman diskusi dalam penyelesaian Tugas Akhir ini.
7. Helmi, Ghonim, Faritz, Ramadhan, Fakhroni, Ariefka, dan Astrid yang juga memberikan dukungan serta teman seperjuangan dalam pengerjaan Tugas Akhir ini.

8. Teman – teman Teknik Elektro UII pada umumnya dan khususnya angkatan 2014 atas doa dan dukungannya.
9. Teman – teman Dai Hijrah yang juga memberikan semangat dan motivasi dalam pengerjaan tugas akhir ini.
10. Teman – teman Majelis Ta Alim yang memberikan support serta motivasi dalam mengerjakan tugas akhir ini
11. Pihak – pihak lain yang tidak dapat disebutkan satu persatu, baik secara langsung maupun tidak langsung telah membantu penulis dalam penyelesaian laporan ini yang telah membantu dalam penyelesaian skripsi ini.

Dalam penulisan laporan ini penulis menyadari masih terdapat kekurangan untuk itu penulis memohon maaf dikarenakan keterbatasan yang dimiliki penulis baik dalam segi pengalaman maupun segi pengetahuan, sehingga penulisan laporan tugas akhir ini masih jauh dari kata sempurna. Semoga skripsi ini bisa bermanfaat bagi pembaca dan penggunanya.

Wassalamu'alaykum Warahmatullahi Wabarakatuh.

ARTI LAMBANG DAN SINGKATAN

AODV	=	*Ad-hoc on-demand Distance Vector*
MANET	=	*Mobile Ad-hoc Network*
RREQ	=	*Route Request*
RREP	=	*Route Reply*
QOS	=	*Quality Of Service*
RRER	=	*Route Request Error*
PDR	=	*Packet Delivery Ratio*

ABSTRAK

Jaringan MANET adalah suatu jaringan yang terdiri dari sekumpulan *node* atau perangkat yang membentuk sebuah jaringan. MANET dapat berkomunikasi secara nirkabel sehingga tidak memerlukan jaringan tetap serta dapat mengatur dirinya sendiri pada jaringan yang dinamis dan sementara. Namun, jaringan MANET sangat rentan terhadap serangan, salah satunya adalah serangan *black hole.* Serangan *black hole* adalah serangan yang menyebabkan paket–paket yang dikirimkan itu hilang dan mengirimkan pesan palsu bahwa paket sudah sampai pada *node* tujuan. Protokol routing adalah standarisasi yang melakukan kontrol bagaimana sebuah *node* dapat meneruskan paket diantara perangkat komputasi dalam jaringan MANET. Protokol routing AODV adalah merupakan salah satu dari protocol routing reaktif. AODV bekerja hanya jika adanya permintaan dengan mengirimkan pesan RREQ kepada *node* disekitarnya. Penelitian ini dibuat untuk memperbaiki kinerja jaringan MANET dari serangan *black hole.* Metode yang digunakan untuk memperbaiki kinerja adalah jumlah *bit rate* yang digunakan, jumlah *node* yang digunakan dan jarak antar *node* . Hasil dari penelitian ini menunjukan bahwa dengan mengubah jarak antar *node* yang digunakan mampu memperbaiki parameter–parameter yang digunakan, seperti *delay, packet delivery ratio (PDR),* dan *throughput.* Pada *delay*, mengalami percepatan menjadi 88,56 ms dengan mengubah jarak antar *node* . Untuk *PDR*, meningkat menjadi 93, 63% pada saat jarak antar *node* di dekatkan. sedangkan untuk *throughput* sendiri meningkat menjadi 487,3 kbps saat kondisi *data rate* 550 kbps. Dari semua hasil yang didapat, beberapa metode yang digunakan berhasil memperbaiki kinerja dari jaringan MANET saat terkena *black hole.*

Kata kunci : MANET, AODV, QOS, *blackhole.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Jaringan *Mobile Ad-Hoc* terdiri dari *node* bergerak yang dapat berkomunikasi dengan *node* lain melalui koneksi nirkabel tanpa infrastruktur tetap. Jaringan *Mobile Ad-Hoc* adalah sistem *node mobile* nirkabel yang mengatur dirinya sendiri dalam topologi jaringan dinamis dan sementara [1]. *Node -node* ini bertugas menghubungkan setiap *node* untuk membentuk sebuah jaringan agar dapat berkomunikasi.

Jaringan (MANET) memiliki beberapa karakteristik yaitu, *multiple wireless link, dynamic topology, limited resources*. *Multiple wireless link* merupakan sifat dimana setiap *node* dapat memiliki interface yang terhubung ke *node* lainnya. Sedangkan *dynamic* topologi adalah sifat MANET yang *mobile*, sehingga topologi jaringan yang dapat berubah secara acak. *Limited resources* sudah menjadi sifat pada jaringan nirkabel, terbatasnya sumber daya serta kapasitas penyimpanan [2].

Dalam penerapannya, jaringan MANET bisa dibangun diberbagai tempat sekalipun tanpa adanya infrastruktur jaringan sebelumnya. Dalam keadaan darurat, jaringan ini dapat dengan mudah dibangun. Misalnya saja saat bencana alam, pencarian dan penyelamatan korban. Selain itu juga dapat digunakan untuk kebutuhan militer, pendidikan, *entertainment*,robot, dan *sensor network* dan masih banyak lagi [3].

Pada jaringan MANET terdapat dua macam protokol *routing*, yaitu *routing* proaktif,*routing* reaktif. *Routing* proaktif adalah protokol *routing* dimana masing-masing *node* mempertahankan rutenya ke semua jaringan lainnya *node* . Dalam protokol *routing* reaktif, rute antara dua *node* hanya ditemukan bila yang dicari dianggap sebagai keuntungan penting yaitu, karena pesan berkurang, jumlah total transmisi paket kontrol berkurang [1].

Protokol *routing* reaktif terbagi menjadi beberapa bagian, salah satunya *routing ad hoc On Demand Distance Vector* (AODV). AODV adalah protokol *routing* yang dirancang untuk jaringan bergerak *ad hoc*. AODV membangun jalur menggunakan rute permintaan atau rute siklus permintaan jawaban. Bila *node* sumber menginginkan rute ke tujuan yang belum memiliki rute, ia akan mengirim paket permintaan rute (*route request*) ke seluruh jaringan. *Node* yang menerima paket ini memperbarui informasinya untuk *node* sumber dan mengatur pointer ke *node* sumber dalam tabel rute [4].

Jaringan MANET bersifat *dynamic topology* menjadikannya sangat mudah terkena serangan, salah satunya adalah serangan *black hole.* Serangan *black hole* adalah serangan yang menyatakan memiliki rute terpendek untuk sampai tujuan. Setelah menerima RREQ dari sumber, *node* serangan tersebut akan mengirimkan RREP palsu ke *node* sumber tanpa melihat informasi mengenai *node* tujuan. Serangan *Black hole* dapat dibagi menjadi dua kategori, serangan berkelompok yang dilakukan oleh lebih dari satu *node* penyerang yang saling berkerja sama dan serangan sendiri yang hanya dilakukan oleh satu *node* penyerang [5]. Terdapat beberapa metode untuk meminimalisir dampak dari serangan *black hole*, antara lain mengubah jarak antar *node* [5], mengubah *data rate* [6], mengubah jumlah *node* [7].

Tujuan dari penelitian ini dilakukan adalah untuk mencari metode yang paling tepat untuk meminimalkan dampak yang diakibatkan serangan *black hole*, agar kinerjanya tidak berbeda jauh dari kondisi tanpa adanya serangan *black hole* yang menjadi perbandingan. Metode yang digunakan untuk mengurangi dampak serangan *black hole* yaitu jarak antar *node* , variasi *node* , dan variasi *data rate.* Penelitian ini dilakukan dengan cara membuat simulasi dan untuk analisa menggunakan parameter QOS, yaitu *packet delivery ratio, delay, throughput.*

1.2 Rumusan Masalah

Perumusan masalah pada penelitian ini adalah :

1. Bagaiman kinerja MANET setelah terkena serangan *black hole*?
2. Bagaimana kinerja masing-masing metode saat terkena serangan *black hole*?
3. Metode mana yang paling baik dari 3 metode yang digunakan?

1.3 Batasan Masalah

1. Penelitian ini hanya membahas bagaimana memperbaiki kinerja jaringan MANET saat terkena *black hole.*
2. Pada penelitian ini tidak membahas bagaimana mendeteksi serangan *black hole* terjadi.
3. Penelitian ini hanya menggunakan *routing* protokol AODV.
4. Penelitian ini hanya menggunakan *software* NS 2.
5. Parameter QOS yang dianalsis meliputi *packet delivery ratio*, *delay*, dan *throughput*

1.4 Tujuan Penelitian

Tujuan dari penelitian ini yaitu :

1. Mengetahui bagaimana kinerja dari MANET dengan *routing* AODV saat sebelum terkena serangan dan sesudah terkena serangan.
2. Mengetahui cara mengurangi dampak dari serangan *black hole* terhadap jaringan MANET.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini :

1. Mencari metode yang paling tepat untuk memperbaiki kinerja jaringan MANET saat terkena serangan *black hole.*
2. Meminimalkan dampak pada sisi kinerja jaringan saat terjadi serangan *black hole.*

BAB 2
TINJAUAN PUSTAKA

2.1 Studi Literatur

Tinjuan pustaka ini berisi survei yang dilakukan terhadap perbaikan kinerja untuk jaringan MANET saat tidak terjadi serangan atau terjadi serangan *black hole* pada beberapa jurnal. Perbedaan yang ada pada masing-masing penelitian adalah terletak pada metode yang digunakan dalam mengatur *node -node* yang digunakan dalam MANET tersebut, selain itu juga perbedaan yang mendasar lainnya adalah metode *routing* yang digunakan. Karena adanya perbedaan tersebut, penulis menguraikan beberapa penelitian yang dilakukan dan juga desain *algoritma* untuk mempertahankan perfoma pada *routing* AODV.

Salah satu penelitian pada jaringan MANET yaitu pada penelitian [7] melakukan perbaikan jaringan MANET saat terkena serangan *black hole.* Penelitian dilakukan menggunakan *software* NS-2. Penelitian memiliki 4 skenario berbeda dengan aplikasi yang digunakan sama, yaitu CBR (*Constant Bit Rate)*. Untuk analisis, masing-masing skenario memiliki beberapa metode perbaikan. Pada bagian hasil, penelitian ini menggunakan beberapa parameter QOS, yaitu *packet delivery fraction, throughput, normalize routing* dan *dropped packet.* Pada *packet delivery fracktion*, hasil menurun pada skenario variasi *pause time* dan variasi jumlah *node* sekitar 60%,namun meningkat saat skenario variasi kecepatan *node* dan variasi jumlah *node* serangan. Untuk *throughput*, rata-rata mengalami penurunan disetiap skenario. Hasil NRL (*normalize route load*) pada skenario variasi *pause time* dan variasi jumlah *node* meningkat mengikut jumlah yang digunakan, sedangkan pada variasi kecapatan *node* , hasilnya tidak stabil. Pada skenario jumlah *node* serangan, hasilnya terus menurun. Terakhir, untuk *dropped packet*, sama halnya seperti pada hasil NRL, namun pada *dropped packet* tidak mengalami kenaikan dan penurunan yang signifikan.

Selanjutnya pada penelitian melakukan penelitian pencegahan dan pendeteksian *black hole* dan *grey hole* [8]. Penelitian ini menggunakan beberapa metode pendeteksian, yaitu pengumpulan data *node* tetangga, pendeteksian local, pendeteksian global, dan peringatan global. Untuk pencegahannya, penelitian ini menggunakan metode peningkatan ukuran jaringan saja. Pada analisis, penelitian ini menggunakan parameter *throughput, delay* serta energi yang digunakan. Untuk hasil *throughput,* mengalami penurunan dengan bertambahnya ukuran jaringan. Selanjutnya, untuk *delay* hasilnya meningkat berbanding lurus dengan ukuran jaringan yang digunakan. Serta untuk daya yang digunakan, hasilnya meningkat mengikuti ukuran jaringan yang digunakan.

Penelitian mengenai studi evaluasi kinerja AODV saat serangan *black hole*. Dengan menggunakan software NS-2 sebagai simulator [9]. Penelitian ini dibuat dengan mengubah jumlah *node* pada jaringan 50, 100, dan 150. Untuk aplikasi yang digunakan adalah CBR. Untuk analisis, parameter yang digunakan yaitu PDR, *delay, throughput,* dan *packet drop.* Pada skenario posisi penyerang, *throughput,* PDR, dan *packet drop* hasilnya membaik saat *node* penyerang menjauhi sumber, sedangkan untuk *delay* meningkat. Untuk scenario jumlah *node* penyerang, *throughput* dan PDR hasilnya berbanding terbalik dengan banyaknya jumlah *node* penyerang.

Pada studi literatur, dijelaskan bahwa serangan *black hole* mampu mengurangi kinerja dari jaringan MANET. Dari penelitian [8], [7], dan [9] telah dilakukan percobaan dengan banyak skenario perbaikan serta pendeteksian yang mempengaruhi kinerja jaringan MANET. Oleh karena itu, peneliti mencoba untuk melakukan penelitian mengenai perbandingan dalam hal memperbaiki kinerja jaringan MANET untuk mencari metode terbaik dalam meminimalisir dampak serangan *black hole.*

2.2 Tinjauan Teori

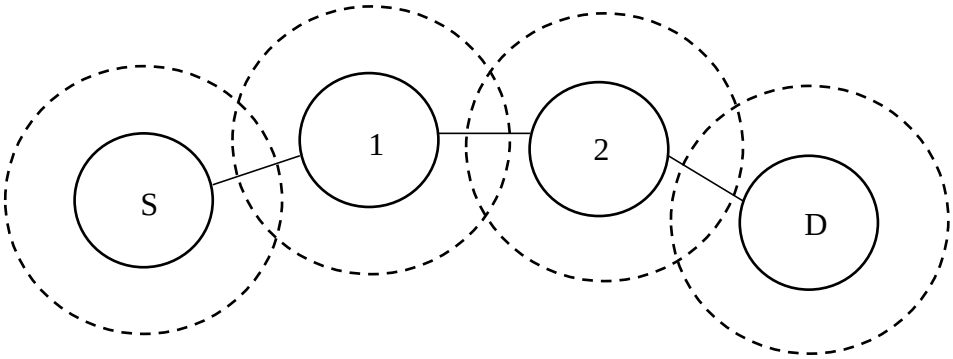
Jaringan MANET merupakan jaringan yang terdiri dari beberapa *node* yang saling berkoordinasi dan berkomunikasi satu sama lain. Setiap *node* memiliki keterbatasan jangkauan sehingga digunakan konsep *multi–hop forwarding* dimana setiap *node* beroperasi seperti sebuah router yang dapat meneruskan paket *node* lain pada jaringan. MANET banyak diaplikasikan pada komunikasi militer, peralatan perang otomatis, tim penolong saat bencana, polisi, pemadam kebakaran, dan sebagai alat komunikasi saat infrastruktur komunikasi rusak akibat bencana alam.

Node –node pada MANET berkomunikasi secara nirkabel dan memilki pergerakan dengan kecepatan tertentu yang menyebabkan topologi jaringan yang selalu berubah. MANET memiliki karakteristik lain seperti keterbatasan bandwidth, kapasitas baterai dan daya komputasi yang rendah. Meskipun karakteristik–karakteristik yang dimiliki oleh MANET tersebut diperlukan untuk fleksibilitas jaringan, tetapi juga menjadi faktor permasalah pada MANET seperti masalah pengalamatan IP, interferensi radio, protokol routing, keterbatasan daya, perlunya manajemen pergerakan, QoS dan keamanan jaringan. Dimana masalah keamanan pada MANET merupakan hal yang harus diperhatikan karena MANET cukup rentan terhadap berbagai jenis serangan seperti penyadapan, interferensi, peniruan, dan *Denial of Service* [9].

2.2.1 MANET (Mobile Ad-Hoc Network)

MANET merupakan jaringan nirkabel yang terdiri dari kumpulan *mobile node* yang bersifat dinamis. Sistem yang digunakan pada MANET bersifat yaitu mampu mengatur diri sendiri serta dibentuk oleh sekumpulan *node* atau terminal yang dihubungkan oleh jalur-jalur nirkabel. Dalam suatu jaringan, konektivitas beberapa *node* dapat menghilang karena jarak yang terlalu jauh dan muncul *node* baru dalam satu waktu dikarenakan pergerakan *node -node* tersebut. Berikut adalah gambaran dari jaringan MANET yang ditunjukan pada Gambar 2.1.

Node pada MANET tidak hanya berperan sebagai pengirim atau penerima data saja, namun dapat juga difungsikan sebagai penghubung *node* yang lain. Untuk mengatur seluruh proses *routing* pada topologi MANET tidak memerlukan *router*, karena setiap device berfungsi sebagai *router* untuk menentukan arah yang akan di tentukan. Sehingga pada proses komunikasi pada jaringan MANET sangat memerlukan protokol yang tepat dan cepat agar *node* dapat mengirimkan paket data yang dibutuhkan oleh jaringan MANET tersebut [10].



Gambar 2.1 Jaringan MANET

2.2.2 Protokol Routing

Protokol routing adalah standarisasi yang melakukan kontrol bagaimana sebuah *node* dapat meneruskan paket diantara perangkat komputasi dalam jaringan MANET. Protokol routing layaknya sebuah router yang berkomunikasi dengan perangkat lain untuk menyebarkan informasi dan mengijinkan pemilihan rute diantara dua *node* dalam jaringan, pada jaringan *ad hoc* setiap *node* akan memiliki kemampuan layaknya router yang meneruskan pesan antar *node* di sekitarnya untuk itu dibutuhkan protokol routing untuk membantu tiap-tiap *node* [11].

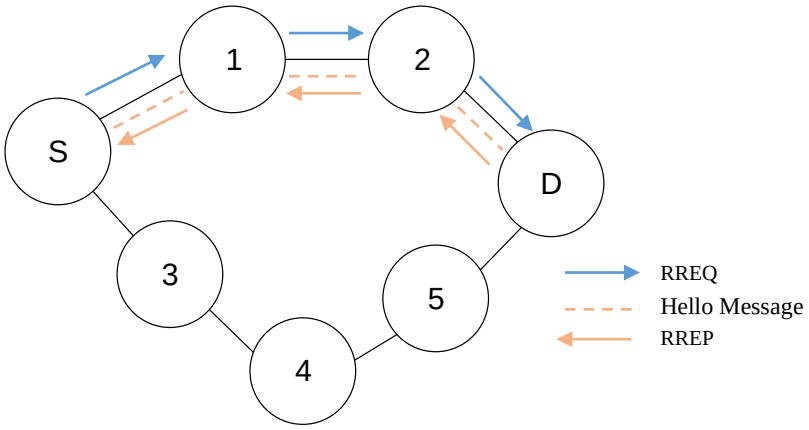
2.2.3 Routing Reaktif

Protokol *routing* reaktif hanya akan bekerja jika *node* sumber membutuhkan rute menuju *node* tujuan. Protokol routing reaktif meliputi *Ad hoc On-Demand Distance Vector* (AODV) dan *Dynamic Source Routing* (DSR). *Route Request* (RREQ) umumnya disiarkan ke seluruh jaringan oleh *node* sumber selama penetapan rute ke *node* tujuan.

2.2.4 Ad-Hoc On Demand Vector (AODV)

Routing AODV termasuk dalam kelompok routing protokol reaktif pada jaringan MANET. Routing AODV akan bekerja saat adanya permintaan dari *node* sumber untuk mencari jalur-jalur yang akan digunakan untuk mengirim pesan menuju *node* penerima. AODV akan berusaha mencari jalur yang terpendek menuju *node* tujuan [12].

Saat adanya permintaan dari *node* sumber, AODV akan mulai bekerja. Untuk menemukan jalur yang terbaik menuju *node* tujuan, AODV akan melakukan *route discovery* yang mana akan menyebarkan *Route Request* (RREQ) kepada semua *node* yang ada disekitar *node* sumber. Untuk menghindari pengiriman pesan yang sama, maka saat menyebarkan RREQ, dikirimkan juga *ID Broadcast* dan *Sequence number*. Penyebaran RREQ ini terus berlanjut sampai menuju *node* tujuan. Setelah RREQ sampai pada tujuan, maka tugas *node* tujuan adalah memberikan balasan *Route Reply* (RREP). Jalur yang dipilih adalah jalur yang paling pendek serta biaya yang lebih rendah dari jalur lainnya. Berikut adalah mekanisme AODV ditunjukan oleh Gambar 2.2.



Gambar 2.2 Mekanisme AODV

Selama proses pengiriman, routing AODV akan mengirimkan pesan HELLO untuk menghindari perubahan topologi secara berkala. Jika selama proses pengiriman terjadi perubahan topologi dan menyebabkan jalur yang menuju *node* tujuan terputus, maka suatu *node* akan mengirimkan pesan *Route Error* (RRER) menuju *node* sumber. Setelah *node* sumber menerima

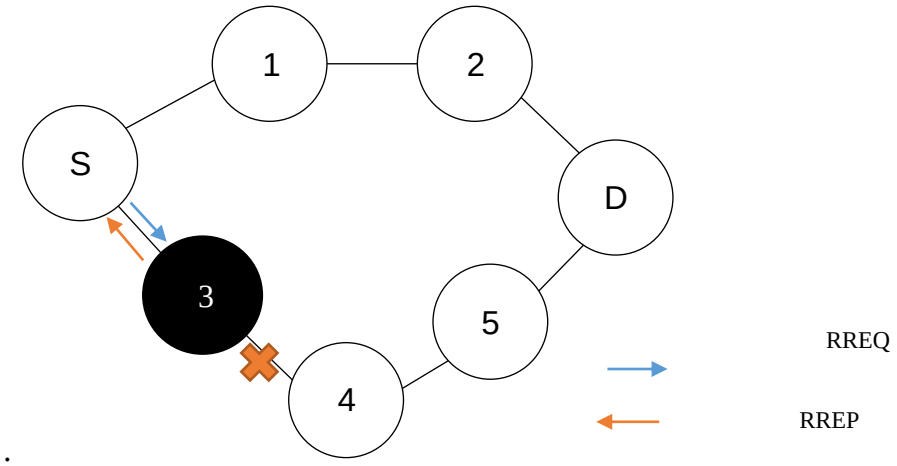
RRER, maka *node* sumber akan melakukan *Route Discovery* kembali untuk mencari jalur lainnya menuju *node* tujuan [13].

2.2.5 Black hole Attack

Serangan Blackhole dapat dibagi menjadi dua kateogri, serangan berkelompok yang dilakukan oleh lebih dari satu *node* penyerang yang saling berkerja sama dan serangan sendiri yang hanya dilakukan oleh satu *node* penyerang [9].

Pada serangan blackhole, *node* penyerang memperoleh rute yang diinginkan dengan menyatakan pada *node* sumber bahwa ia memiliki rute terpendek untuk mencapai *node* tujuan. Setelah menerima paket RREQ, *node* penyerang langsung mengirimkan paket RREP palsu ke *node* sumber tanpa melihat informasi mengenai *node* tujuan. *Node* penyerang memanipulasi RREP dengan memberikan sequence number dan hop count palsu yang menyatakan *node* penyerang memiliki rute terpendek dan terbaru.

Dengan nilai sequence number *node* tujuan yang tinggi dan paket RREP yang pertama kali diterima oleh *node* sumber. *Node* sumber akan menolak paket RREP yang dikirimkan oleh *node* lain meskipun memiliki rute yang benar. Sehingga rute antara *node* sumber dan *node* penyerang akan terbentuk dan *node* sumber mulai mengirimkan paket ke *node* penyerang. *Node* penyerang kemudian mulai membuang paket yang diterima.



Gambar 2.3 Mekanisme *Blackhole Attack*

2.2.6 Metode Perbaikan Kinerja Jaringan yang Digunakan

Kelemahan utama pada MANET adalah masalah keamanannya. *Node -node* secara bebas dapat masuk dan keluar dalam jaringan hal inilah yang menyebabkan MANET rentan terhadap serangan. Hal ini dikarenakan media pertukaran data atau informasi pada MANET menggunakan transmisi radio ditambah tidak adanya administrator yang mengawasi perangkat komunikasi yang terhubung. Sehingga memungkinkan setiap orang dapat terhubung pada jaringan dan mengakses informasi.

Untuk mengurangi dampak dari kelemahannya pada perfoma, perlu adanya evaluasi kinerja. Terdapat 3 cara untuk mengurangi dampak tersebut, yaitu jarak antar *node* , variasi jumlah *node* , dan variasi *data rate* yang digunakan. Pada jarak antar *node* , jika jarak terlalu dekat maka terjadi kemacetan, jika terlalu jauh, memungkinkan *node* serangan lebih dekat dari *node* normal. Maka dari itu perlu adanya jarak yang ideal antar masing-masing *node* [5].

Jumlah *node* dalam suatu jaringan MANET perlu diperhatikan. Jumlah *node* yang terlalu banyak dalam wilayah yang kecil akan terjadinya kemacetan pada jaringan. Namun sebaliknya, jika *node* terlalu sedikit, akan membuat jarak semakin jauh serta memudahkan *node* penyerang berada paling dekat dengan *node* normal [7]. Sedangkan pada sisi *bit rate,* penggunaan *data rate* yang rendah akan memperlama *delay* yang dihasilkan. Namun, jika menggunakan *data rate* yang tinggi akan mengakibatkan topologi akan berubah. [6].

BAB 3
METODOLOGI

3.1 Alat dan Bahan (jika dibutuhkan)

Penelitian ini dilakukan dengan mengambil data dari hasil simulasi pada software simulasi. Adapun perangkat yang digunakan akan dijelaskan pada sub bab berikut

3.1.1 Perangkat Keras

Pada penelitian ini diperlukan perangkat keras berupa sebuah laptop untuk menjalankan simulasi, dengan spesifikasi sebagai berikut :

1. Intel® Core i5 8250U (6 MB *Cache*, 1.6 GHz)
2. RAM 8 GB (DDR4 2400 MHz)
3. Harddisk 1 TB
4. Nvidia GeForce GT 940MX (2 GB, GDDR5)

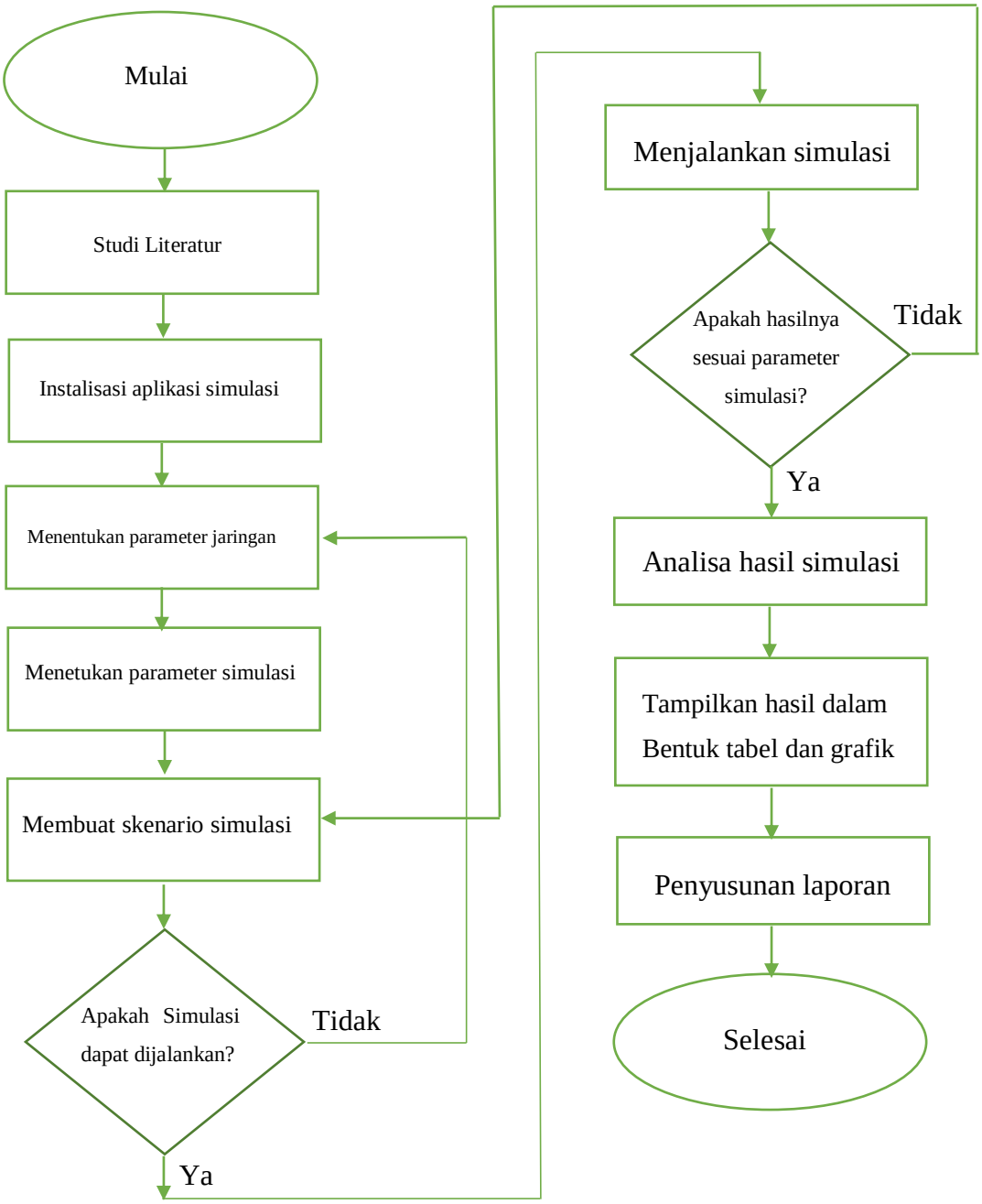
3.1.2 Perangkat Lunak

Pada penelitian ini juga diperlukan perangkat lunak untuk menjalankan dan mencatat hasil simulasi, adalah sebegai berikut :

1. Windows 10 SL
2. Oracle VM Virtual Box
3. Linux 16.04 LTs
4. Network Simulator 2
5. Microsoft Word 2016
6. Microsoft Excel 2016

3.2 Alur Penelitian

Pada Gambar 3.1 dapat dilihat alur pembahasan simulasi yang dilakukan oleh penulis melalui beberapa tahapan, yaitu



Gambar 3.1 Alur penelitian

3.3 Studi Literatur

Dalam proses ini penulis mencari dan mempelajari jurnal-jurnal untuk dijadikan sumber acuan dan referensi dalam melakukan penelitian ini. Dalam penelitian ini parameter-parameter yang diterapkan banyak didapatkan dari jurnal, *paper* ataupun skripsi yang telah dilakukan.

3.4 Instalasi Aplikasi Simulasi

Penelitian ini membutuhkan Operating System (OS) Linux berjenis ubuntu untuk proses simulasi dengan menggunakan software Network Simulator-2 (NS-2) yang sudah terinstall didalamnya. Versi Ubuntu yang digunakan adalah versi 16.04 dan untuk NS-2 sendiri menggunakan versi NS-2.2

3.5 Parameter Jaringan

Pada penelitian ini dilakukan untuk mengetahui parameter apa saja yang dapat memperbaiki kinerja jaringan MANET setelah terkena serangan *Blackhole*. Penulis membagi beberapa percobaan, yaitu tanpa serangan, terkena serangan *blackhole* dan perbaikan dengan jumlah *node* [7], *data rate* [7] dan jarak antar *node* [5]. Pada percobaan yang pertama yaitu tanpa adanya serangan serta parameter dibiarkan *default*. Percobaan selanjutnya, dengan adanya serangan *black hole* serta lainnya dibiarkan *default.* Lalu untuk yang terakhir, percobaan dilakukan dengan merubah beberapa parameter seperti jumlah *node* (30 *node* , 35 *node* , 40 *node*), data rate (350 kbps,400 kbps, 450 kbps, 550 kbps dan 600 kbps) dan jarak antar *node* (30 meter dan 40 meter). Secara *default* parameter pada percobaan ini ditunjukan pada Tabel 3.1 yang terlampir.

Tabel 3.1 Parameter Jaringan

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Jarak antar *node*	50 meter
3	Jumlah *node* normal	26 *node* + 1 *Server*
4	Jumlah *node black hole*	3 *node*
5	Ukuran paket	512 bit
6	Aplikasi Jaringan	CBR
7	Bit rate	500 kbps

3.6 Parameter Simulasi

Quality Of Service adalah standar untuk mengukur tingkat kualitas jaringan yang digunakan dengan parameter–parameter kualitas dengan metode pengukuran[14]. Pada percobaan ini menggunakan beberapa parameter QOS untuk menguji simulasi jaringan yang dibuat, seperti *Packet Delivery Ratio*, *Delay* dan *throughput*.

a. *Packet delivery ratio*

   Packet delivery ratio adalah rasio antara jumlah data yang dikirimkan dengan data yang diterima. Untuk menghitung jumlah PDR, dapat menggunakan rumus yang ditunjukan pada persamaan 3.1.

$$PDR = \frac{jumlah\ data\ yang\ diterima}{jumlah\ data\ yang\ dikirim} \times 100\% \qquad (3.1)$$

Untuk parameter PDR yang digunakan pada penelitian ini adalah sama atau lebih besar dari hasil terkena serangan *black hole*.

b. Delay (Latency)

Delay adalah waktu yang digunakan untuk mengirimkan data dari pengirim menuju penerima dihitung dalam satuan waktu. *Delay* mudah dipengaruhi banyak hal, seperti jarak, media yang digunakan, gangguan pada jaringan, atau proses yang membutuhkan waktu lama. Menurut versi TIPHON [15], besarnya delay dapat diklasifikasikan pada Tabel 3.2 berikut ini :

Tabel 3.2 Klasifikasi *Delay*

Katagori	Delay	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Buruk	>450 ms	1

Untuk parameter *delay* yang digunakan pada penelitian ini adalah sama atau lebih kecil dari hasil terkena serangan *black hole*.

c. *Throughput*

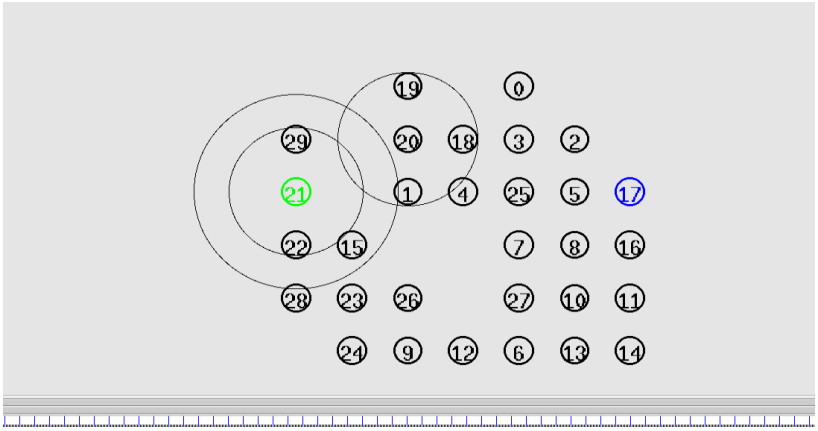
Throughput adalah kecepatan suatu jaringan dalam mentrasmisikan data yang diukur dalam satuan *bit per second. Throughput* merupakan jumlah total paket yang diterima dengan sukses dan dibagi pada interval waktu tertentu [15]. Untuk parameter *throughput* yang digunakan pada penelitian ini adalah sama atau lebih besar dari hasil terkena serangan *black hole*.

3.7 Skenario Simulasi

Pada penelitian digunakan 5 skenario simulasi, yaitu:

3.7.1. Skenario Tanpa Serangan

Pada skenario ini, percobaan dilakukan tanpa adanya serangan *blackhole* pada jaringan MANET. Untuk parameter yang digunakan, diset pada kondisi *default*. Berikut adalah spesifikasi jaringan MANET pada Gambar 3.2 dan Tabel 3.3.



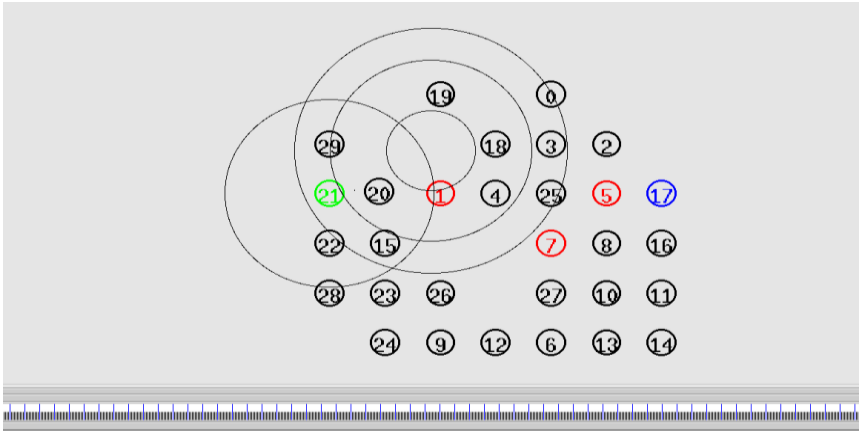
Gambar 3.2 Topologi tanpa serangan

Tabel 3.3 Parameter tanpa serangan

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Jarak antar *node*	50 meter
3	Jumlah *node* normal	26 *node* + 1 *Server*
4	Jumlah *node black hole*	3 *node*
5	D*ata rate*	500 kbps
6	Ukuran paket	512 bit
7	Aplikasi Jaringan	CBR

3.7.2. Skenario Serangan *Blackhole*

Pada skenario ini, parameter yang digunakan sama dengan tanpa serangan, hanya saja 3 *node* menjadi *blackhole*. Berikut speksifikasi jaringan MANET yang ditunjukan pada Gambar 3.3 dan Tabel 3.4



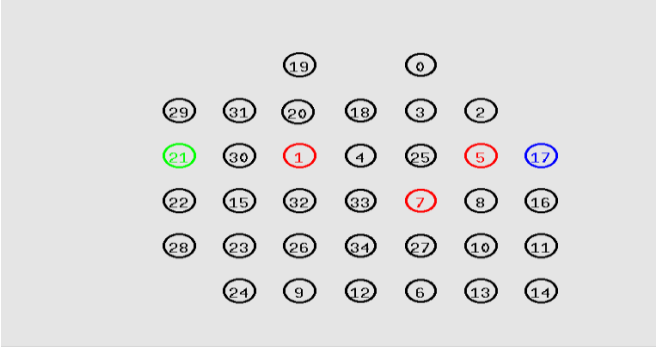
Gambar 3.3 Topologi *Black Hole*

Tabel 3.4 Parameter Serangan *black hole*

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Jarak antar *node*	50 meter
3	Jumlah *node* normal	26 *node* + 1 *Server*
4	Jumlah *node black hole*	3 *node*
5	D*ata rate*	500 kbps
6	Ukuran paket	512 bit
7	Aplikasi jaringan	CBR

3.7.3. Skenario penambahan Jumlah *Node*

Pada skenario ini, penulis melakukan percobaan untuk memperbaiki kinerja jaringan MANET dengan jumlah *node* . Percobaan ini, penulis hanya merubah pada sisi jumlah *node* saja sehingga parameter lainnya adalah *default*. Jumlah *node* yang digunakan yaitu 35 *node* , 40 *node* , dan 25 *node* . Pada Gambar 3.4 dan Tabel 3.5 menunjukan spesifikasi dari jaringan MANET yang digunakan.



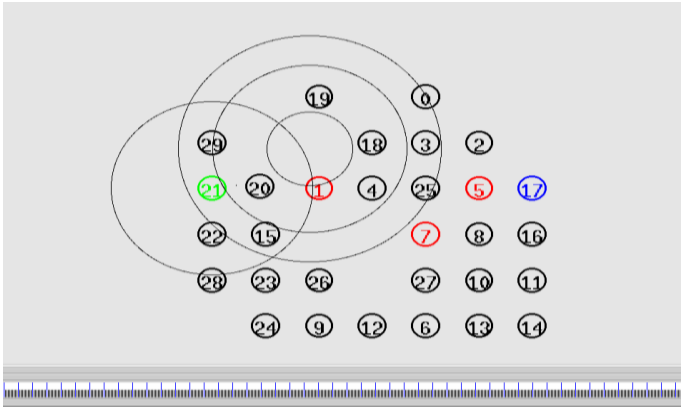
Gambar 3.4 Topologi mengubah jumlah *node*

Tabel 3.5 Parameter mengubah jumlah *node*

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Jarak antar *node*	50 meter
3	Perubahan *node* normal	21 *node* + 1 *server* 31 *node* + 1 *server* 36 *node* + 1 server
4	Jumlah *node black hole*	3 *node*
5	D*ata rate*	500 kbps
6	Ukuran paket	512 bit
7	Aplikasi Jaringan	CBR

3.7.4. Skenario penambahan data rate

Pada skenario ini, sama seperti percobaan sebelumnya namun yang berubah adalah parameter bit rate dan untuk parameter lainnya *default*. Berikut speksifikasi yang digunakan pada jaringan MANET yang ditunjukan pada Gambar 3.5 dan Tabel 3.6



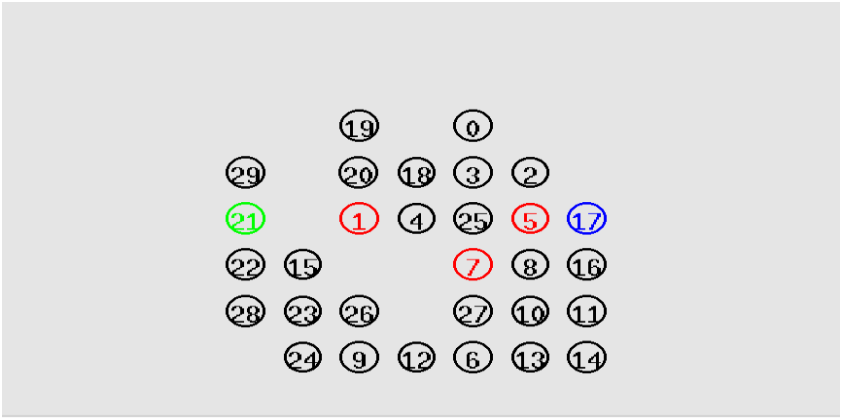
Gambar 3.5 Topologi mengubah *data rate*

Tabel 3.6 Parameter mengubah *data rate*

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Jarak antar *node*	50 meter
3	Jumlah *node* normal	26 *node* + 1 *server*
4	Jumlah *node black hole*	3 *node*
5	Perubahan d*ata rate* yang digunakan	350 kbps 400 kbps 450 kbps 550 kbps 600 kbps
6	Ukuran paket	512 bit
7	Aplikasi jaringan	CBR

3.7.5. Skenario Jarak antar *node*

Pada skenario ini, sama seperti percobaan sebelumnya namun yang berubah adalah parameter jarak antar *node* , sedangkan yang lainnya menjadi parameter awal. Berikut adalah spesifikasi jaringan MANET yang ditunjukan pada Gambar 3.6 dan Tabel 3.7 yang terlampir.



Gambar 3.6 Topologi mengubah jarak antar *node*

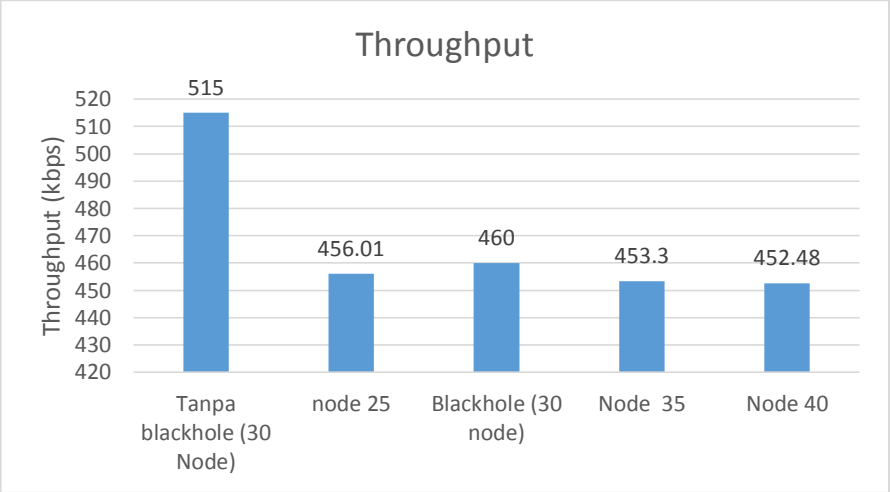
Tabel 3.7 Parameter mengubah jarak antar *node*

No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Perubahan jarak antar *node*	30 meter 40 meter
3	Jumlah *node* normal	26 *node* + 1 *Server*
4	Jumlah *node black hole*	3 *node*
5	D*ata rate*	500 kbps
6	Ukuran paket	512 bit
7	Aplikasi jaringan	CBR

BAB 4
HASIL DAN PEMBAHASAN

Pada bab ini, penulis membahas hasil didapatkan dari simulasi jaringan yang dijalankan hingga selesai. Hasil yang diamati adalah parameter-parameter QOS yang sudah ditentukan yaitu *PDR, delay,* dan *throughput.* Layanan yang digunakan pada setiap skenario adalah *Constant bit rate* (CBR). Pembahasan dibagi menjadi beberapa bagian yaitu Jumlah *node* , jarak antar *node* , dan variasi *data rate.*

4.1. Skenario Penambahan Jumlah *Node*

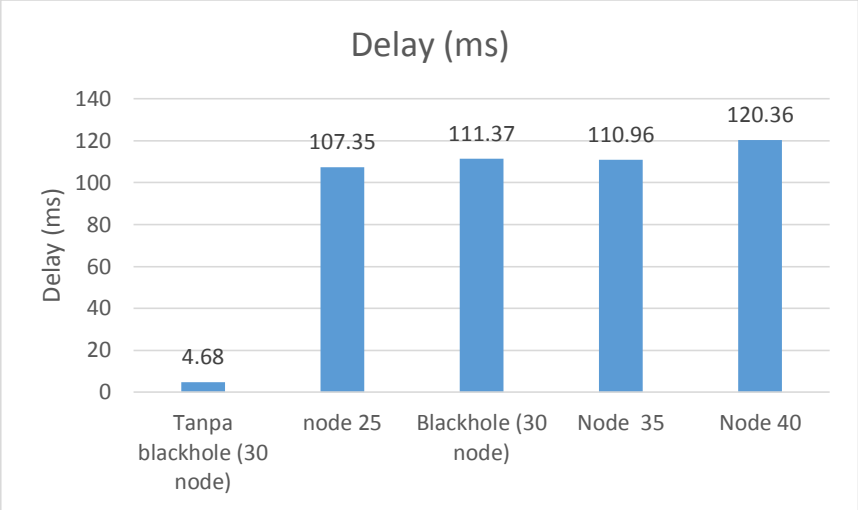


Gambar 4.1 *Throughput* jumlah *node*

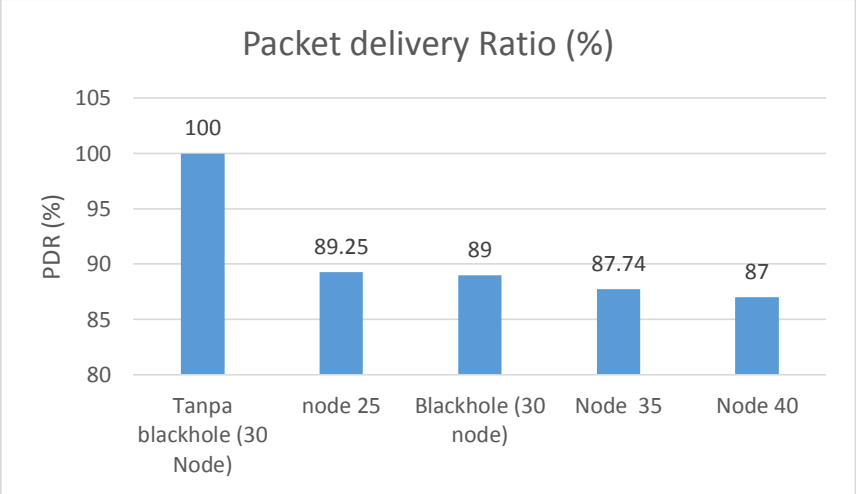
Hasil dari pengamatan *Throughput* yang dihasilkan simulator terlihat pada Gambar 4.1. Hasil keluaran *Throughput* dari masing-masing skenario ini memiliki hasil yang berbeda-beda. Pada kondisi normal menghasilkan *throughput* sebesar 515 kbps, sedangkan pada saat terkena serangan *black hole* turun menjadi 460,01 kbps. Hal ini terjadi karena *node Black hole* membuat *dropping* setiap ada paket yang melewatinya [16]. Selanjutnya, penulis mengganti jumlah *node* yang digunakan. Terlihat bahwa penambahan jumlah *node* mengakibatkan penurunan *throughput*. Menambah jumlah *node* mengakibatkan kongesti pada jaringan MANET, sehingga *throughput* menjadi turun [7], namun saat jumlah *node* diturunkan menjadi 25 *node* , terjadi peningkatan dibandingkan penambahan *node* , tapi tidak lebih baik dari kondisi normal terkena serangan *black hole.*

Selanjutnya adalah *delay.* Saat kondisi normal, menghasilkan sebesar 4,6 ms, namun saat terkena serangan *black hole, Delay* meningkat menjadi 111,37 ms. Sedangkan saat penulis mengganti jumlah *node* menjadi 40 *node* , *delay* menjadi meningkat menjadi 120,36 ms,

mengalami peningkatan sebesar 8,99 ms. Hal ini diakibatkan karena adanya *congestion* pada jaringan, namun ketika diturunkan menjadi 35 *node* dan 25 *node* hasil yang diperoleh juga ikut turun. Hasil ditunjukan pada Gambar 4.2 yang terlampir. Yang terakhir yaitu hasil *PDR*. Berikut adalah hasil PDR yang ditunjukan pada Gambar 4.3.



Gambar 4.2 *Delay* jumlah *node*

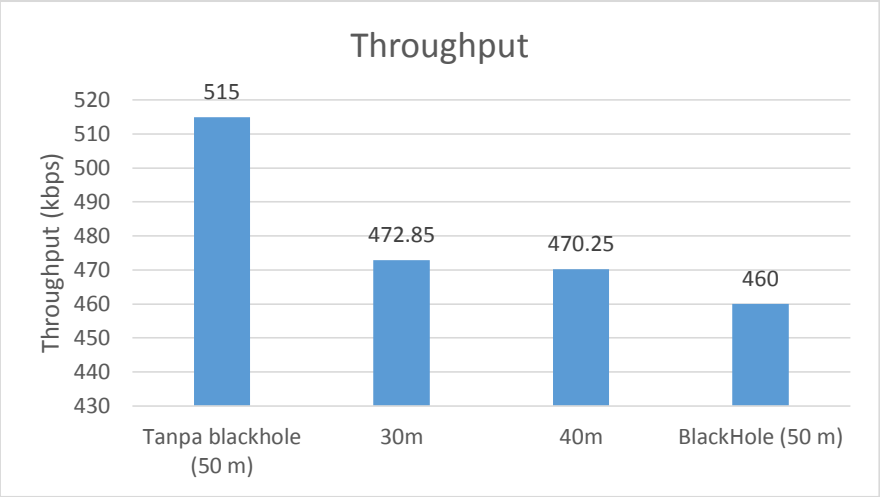


Gambar 4.3 *PDR* jumlah *node*

Terlihat pada gambar, saat kondisi normal tanpa adanya serangan *PDR* sebesar 100%. Namun saat terkena serangan, *drop* 11% menjadi 89%. Akan tetap, saat jumlah *node* dikurangi, *PDR* meningkat menjadi 89,25%, lalu saat jumlah ditambahkan, PDR semakin turun menjadi 87% saat 40 *node* . Hal ini disebabkan karena serangan *black hole* menurunkan jumlah maksimum paket dari *node* yang dekat dengannya [17].

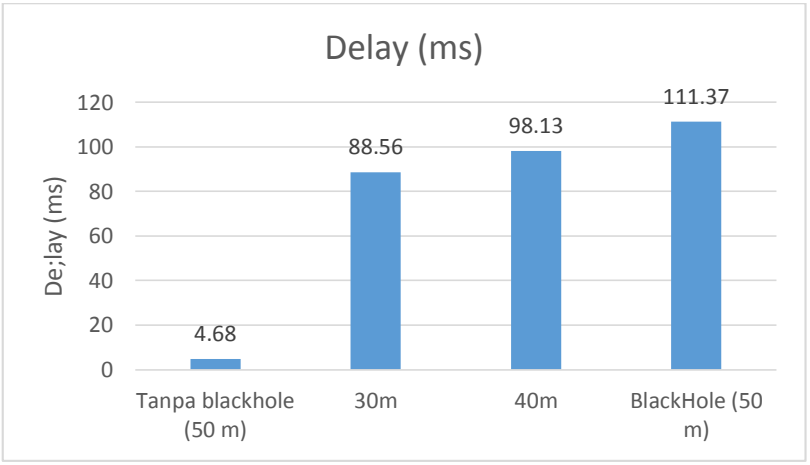
4.2. Jarak Antar *node*

Data *throughput* dari skenario jarak antar *node* ditunjukan pada Gambar 4.4.



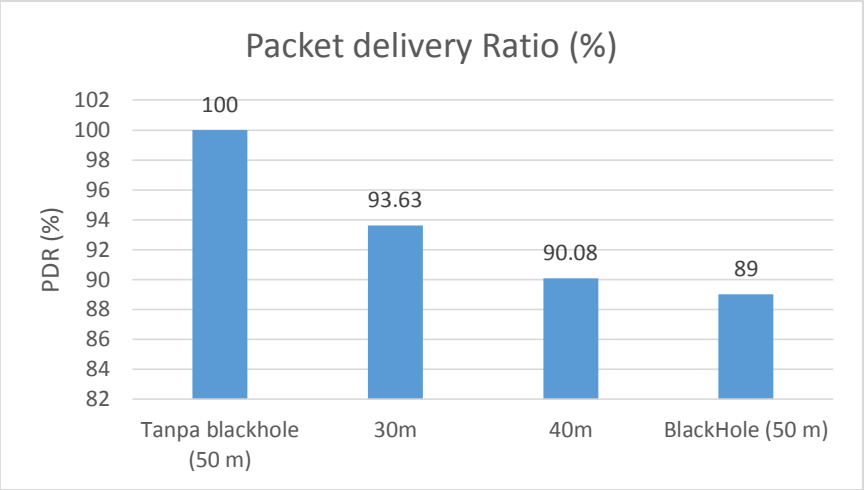
Gambar 4.4 *Throughput* jarak antar *node*

Saat kondisi normal tanpa serangan, *Throughput* sebesar 515 kbps. Terjadi penurunan ketika terkena serangan sebesar 56 kbps. Saat jarak antar *node* dikecilkan menjadi 30 meter, terjadi perningkatan menjadi 472,85 kbps. Namun, jika dibandingkan dengan 50 meter hasilnya terjadinya peningkatan. Hal ini dipengaruhi dengan semakin dekatnya jarak antar *node* Selanjutnya hasil *delay*. Berikut adalah *delay* jarak antar *node* yang ditunjukan pada Gambar 4.5.



Gambar 4.5 *Delay* jarak antar *node*

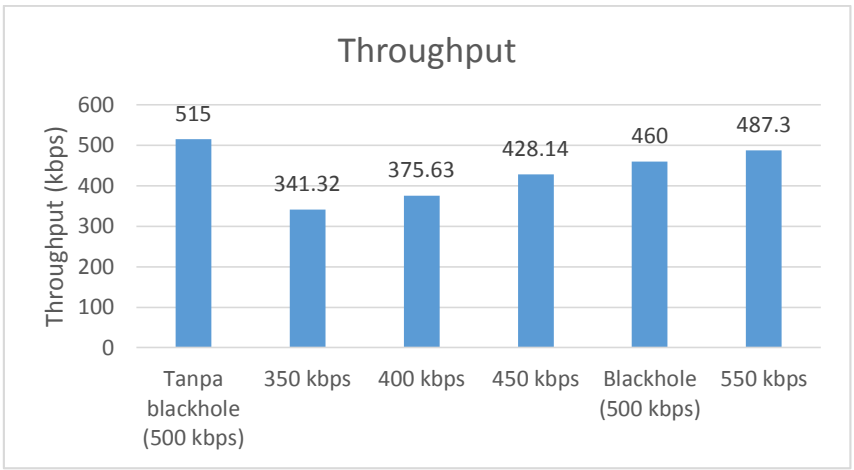
Terlihat pada gambar, saat kondisi normal tanpa serangan *delay* sebesar 4,68 ms. Pada saat terkena serangan, *delay* meningkat 107,06 ms. Sama seperti hasil *throughput*, saat jarak dikecilkan menjadi 30 meter, hasilnya *delay* turun sebesar 88,56 ms.Hal ini disebabkan semakin dekat sehingga *delay* semakin rendah. Selanjutnya hasil *PDR* jarak antar *node* . Berikut adalah hasil dari *PDR* yang ditunjukan pada Gambar 4.6.



Gambar 4.6 *PDR* jarak antar *node*

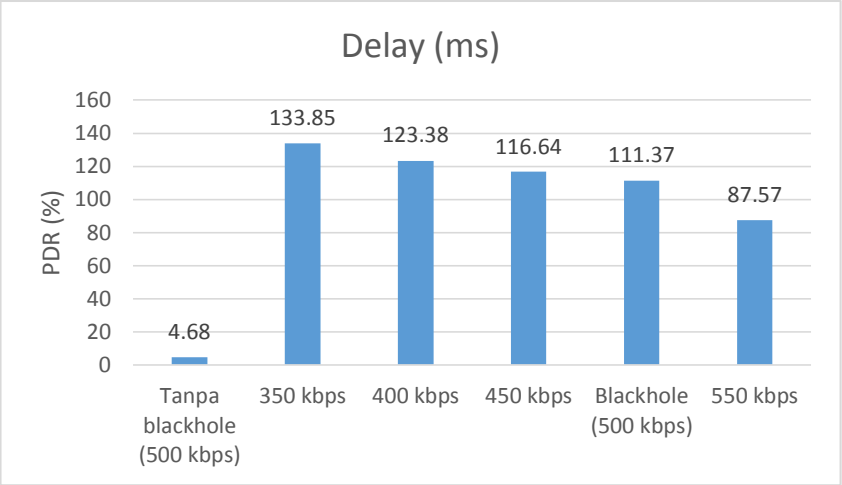
Sama seperti hasil sebelumnya, saat kondisi normal tanpa serangan sebesar 100%. Saat terkena serangan turun menjadi 89%. Hal ini disebabkan oleh *node* serangan yang membuang paket data yang melewati *node* tersebut. Saat jarak antar *node* dikecilkan, hasilnya menigkat saat jarak 40 meter maupun 30 meter. Hal ini terjadi karena jarak antar *node* semakin dekat sehingga mengurangi dampak dari *blackhole*.

4.3. Variasi *Data rate*



Gambar 4.7 *Throughput* variasi *data rate*

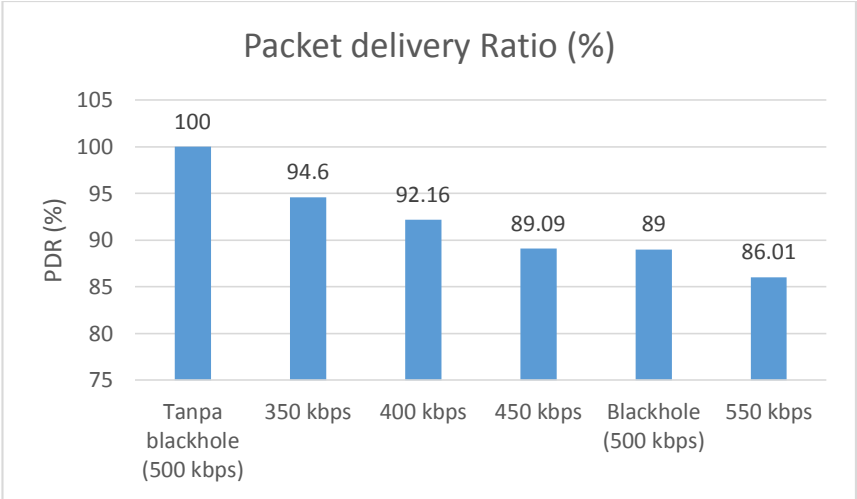
Berikut adalah hasil *troughput* dari variasi *data rate* yang ditunjukan pada Gambar 4.7 yang terlampir. Semakin besar data rate yang digunakan, nilai *throughput* yang dihasilkan lebih besar. Saat terkena serangan, mengalami *dropping* sebesar 56 kbps dari kondisi tanpa serangan. Saat adanya perubahan *data rate* terjadi peningkatan, hal ini karena berbanding lurus dengan meningkatnya *datat rate*. Selanjutnya, untuk hasil *delay* variasi *data rate*. Berikut adalah hasil *delay* yang ditunjukan pada Gambar 4.8.



Gambar 4.8 *Delay* variasi *data rate*

Terlihat saat kondisi tanpa serangan dengan terkena serangan mengalami peningkatan 107,06 ms. Saat *data rate* 350 kbps, meningkat menjadi 133,85ms, hal ini berbanding lurus *delay* dengan *data rate*. Begitupun saat terus ditingkatkan, *delay* terus mengalami penurunan. Walaupun adanya peningkatan saat kondisi 550 kbps, namun tetap lebih rendah saat kondisi normal terkena serangan.

Hasil tersebut jika dibandingkan dengan *PDR* yang berbanding terbalik dengan *data rate*. Hal ini ditunjukan pada Gambar 4.9 yang terlampir. Saat *data rate* kecil, data yang dikirimkan juga semakin mengecil, sehingga *PDR* meningkat. Dari kondisi terkena serangan dengan *data rate* 350 kbps mengalami peningkatan 5,6 %.



Gambar 4.9 *PDR* variasi *data rate*

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada percobaan ini, dapat ditarik beberapa kesimpulan :

1. Serangan *black hole* yang menyerang jaringan MANET mengakibatkan menurunnya kinerja dari jaringan MANET tersebut. Hal ini terlihat dari beberapa parameter QOS, yaitu PDR, *delay*, dan *throughput* memburuk. Pada PDR, menurun sekitar 11% dari tanpa serangan, pada *delay* meningkat sekitar 95 ms, dan juga *throughput* turun sekitar 56 kbps.
2. Untuk memperbaiki kinerja dari jaringan MANET yang terkena serangan *black hole*, dengan menggunakan beberapa metode, diantarnya mengubah jarak antar *node* , mengubah *node* yang digunakan, serta mengubah *data rate* yang digunakan pada jaringan tersebut. Pada jarak antar *node* mampu meningkatkan *throughput* menjadi 472 kbps, *delay* 88,56 *ms* dan *packet delivery ratio* 93,63%. Metode mengubah *node* yang digunakan, *delay* menurun menjadi 107 ms. Sedangakan mengubah *data rate* mampu meningkatkan *throughput* menjadi 487 kbps dan *delay* menjadi 87 ms.
3. Dari percobaan yang dilakukan, metode yang terbaik dari metode yang digunakan adalah metode mengubah jarak antar *node* . Dengan mengubah jarak antar *node* , *throughput* yang dihasilkan sebesar 472 kbps dan *delay* mengecil menjadi 88,56 ms, walaupun pada PDR hanya mengalami kenaikan sedikit yaitu 3%

5.2 Saran

Pada percobaan ini terdapat beberapa saran :

1. Melakukan perbaikan kinerja pada protokol routing reaktif ataupun selain protokol routing reaktif terhadap serangan *black hole*.
2. Melakukan perbaikan dengan metode yang lain dari yang sudah diujikan.
3. Melakukan perbaikan terhadap serangan *black hole* pada jaringan lain seperti *wireless sensor network, wireless mesh network* dan jaringan lainnya
4. Melakukan penelitian guna peningkatan kinerja MANET terhadap serangan lain seperti, *wormhole, gray hole* dan serangan lainnya

DAFTAR PUSTAKA

[1] S. Sridhar, R. Baskaran, and P. Chandrasekar, "Energy Supported AODV (EN-AODV) for QoS Routing in MANET," *Procedia - Soc. Behav. Sci.*, vol. 73, pp. 294–301, 2013.

[2] P. Ramachandran and M. Dinakaran, "Signal Strength and Residual Power Based Optimum Transmission Power Routing for Mobile Ad hoc Networks," *Procedia Comput. Sci.*, vol. 92, pp. 168–174, 2016.

[3] K. Sumathi and A. Priyadharshini, "Energy optimization in manets using on-demand routing protocol," *Procedia Comput. Sci.*, vol. 47, no. C, pp. 460–470, 2014.

[4] B. K. Saraswat, M. Bhardwaj, and A. Pathak, "Optimum Experimental Results of AODV, DSDV & DSR Routing Protocol in Grid Environment," *Procedia Comput. Sci.*, vol. 57, pp. 1359–1366, 2015.

[5] 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, PP: 1072 - 1078, 2016.

[6] D. Untuk, M. Salah, S. Syarat, M. Gelar, K. Program, and S. Teknik, "Analisis Perbandingan Unjuk Kerja Protokol Routing Reaktif (DYMO) Terhadap Routing Reaktif (AODV) Pada Jaringan MANET," 2016.

[7] T. Bhatia and A. K. Verma, "Performance Evaluation of AODV under Blackhole Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 12, pp. 35–44, 2013.

[8] I. Pratomo and M. H. Hizburrahman, "Pendeteksian Dan Pencegahan Serangan Black Hole & Grey Hole Pada Manet," *JAVA J. Electr. Electron. Eng.*, vol. 13, no. 4, pp. 47–53, 2015.

[9] C. Joseph, P. C. Kishoreraja, R. Baskar, and M. Reji, "Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios," *Indian J. Sci. Technol.*, vol. 8, no. 29, pp. 1–10, 2015.

[10] B. S. Kusuma, "Analisis Perbandingan Performansi Protokol Aodv Dan Zrp Pada Mobile Adhoc Network," *Kinetik*, vol. 2, no. 3, pp. 165–174, 2017.

[11] F. Amilia, Marzuki, and Agustina, "Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) Dan Geographic Routing Protocol (GRP) Pada Mobile Ad Hoc Network (MANET)," *J. Sains, Teknol. dan Ind.*, vol. 12, no. 1, pp. 9–15, 2014.

[12] E. H. Harahap, "Analisis Performansi Protokol AODV (Ad Hoc On Demand Distance

Vector) dan DSR (Dynamic Source Routing) Terhadap Active Attack Pada MANET (Mobile Ad Hoc Network) Ditinjau dari Qos (Quality Of Service),” *Tugas Akhir Telkom Univ.*, vol. 34, no. 1, p. 9, 2014.

[13] E. H. Harahap, “Analisis Performansi Protokol AODV (Ad Hoc On Demand Distance Vector) dan DSR (Dynamic Source Routing) Terhadap Active Attack Pada MANET (Mobile Ad Hoc Network) Ditinjau dari Qos (Quality Of Service),” *Tugas Akhir Telkom Univ.*, vol. 34, no. 1, p. 9, 2014.

[14] S. N. M. P. Simamora, “Analisis QOS Pada Layanan Jaringan dalam Mobile Ad-Hoc Network ISBN : 979-26-0280-1 ISBN : 979-26-0280-1,” SEMANTIK, pp. 305–310, 2015.

[15] T. Pratama, M. A. Irwansyah, and Yulianti, “Perbandingan Metode PCQ, SFQ, RED Dan FIFO Pada Mikrotik Sebagai Upaya Optimalisasi Layanan Jaringan Pada Fakultas Teknik Universitas Tanjungpura,” *J. Tek. Inform. Univ. Tanjungpura*, no. 1, p. 12, 2015.

[16] W. Virgi, A. Bhawiyuga, and R. Primananda, “Analisis Perbandingan Dampak Serangan Black Hole pada Peformansi Protokol Routing OLSR dan AODV di Jaringan Wireless Mesh Network,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 3, pp. 1017–1026, 2018.

[17] D. Gaurav, “Performance Evaluation of AODV with and without Black hole Attack in MANETs,” International Journal on Recent and Innovation Trends in Computing and Communication, vol 4.no 6, pp. 7–13, 2016.

[18] E. R. Widasari and A. Bhawiyuga, “Analisis Perbandingan Kinerja Protokol AOMDV , DSDV , Dan ZRP Sebagai Protokol Routing Pada Mobile Ad-Hoc Network (MANET),” vol. 2, no. 10, pp. 3671–3680, 2018.

LAMPIRAN

```
#====================================
#        Agents Definition
#====================================
#Setup a UDP connection
set udp0 [new Agent/UDP]
$ns attach-agent $n21 $udp0
set null1 [new Agent/Null]
$ns attach-agent $n20 $null1
$ns connect $udp0 $null1
$udp0 set packetSize_ 512

#Setup a CBR Application over UDP connection
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 512
$cbr0 set rate_ 0.5Mb
$cbr0 set random_ null
$ns at 1.0 "$cbr0 start"
$ns at 20.0 "$cbr0 stop"
#Setup a UDP connection
set udp1 [new Agent/UDP]
$ns attach-agent $n20 $udp1
set null2 [new Agent/Null]
$ns attach-agent $n4 $null2
$ns connect $udp1 $null1
$udp1 set packetSize_ 512

#Setup a CBR Application over UDP connection
set cbr1 [new Application/Traffic/CBR]
$cbr1 attach-agent $udp1
$cbr1 set packetSize_ 512
$cbr1 set rate_ 0.5Mb
$cbr1 set random_ null
$ns at 20.0 "$cbr1 start"
$ns at 40.0 "$cbr1 stop"
#Setup a UDP connection
set udp3 [new Agent/UDP]
$ns attach-agent $n4 $udp3
set null3 [new Agent/Null]
$ns attach-agent $n8 $null3
$ns connect $udp3 $null1
$udp3 set packetSize_ 512

#Setup a CBR Application over UDP connection
set cbr2 [new Application/Traffic/CBR]
$cbr2 attach-agent $udp3
$cbr2 set packetSize_ 512
$cbr2 set rate_ 0.5Mb
$cbr2 set random_ null
$ns at 40.0 "$cbr2 start"
$ns at 60.0 "$cbr2 stop"
set udp4 [new Agent/UDP]
$ns attach-agent $n8 $udp4
set null4 [new Agent/Null]
$ns attach-agent $n17 $null4
$ns connect $udp4 $null4
```

```
$n3 set Y_ 450
$n3 set Z_ 0.0
$ns initial_node_pos $n3 50
set n4 [$ns node]
$n4 set X_ 560
$n4 set Y_ 350
$n4 set Z_ 0.0
$ns initial_node_pos $n4 50
set n5 [$ns node]
$n5 set X_ 760
$n5 set Y_ 350
$n5 set Z_ 0.0
$ns initial_node_pos $n5 50
set n6 [$ns node]
$n6 set X_ 660
$n6 set Y_ 50
$n6 set Z_ 0.0
$ns initial_node_pos $n6 50
set n7 [$ns node]
$n7 set X_ 660
$n7 set Y_ 250
$n7 set Z_ 0.0
$ns initial_node_pos $n7 50
set n8 [$ns node]
$n8 set X_ 760
$n8 set Y_ 250
$n8 set Z_ 0.0
$ns initial_node_pos $n8 50
set n9 [$ns node]
$n9 set X_ 460
$n9 set Y_ 50
$n9 set Z_ 0.0
$ns initial_node_pos $n9 50
set n10 [$ns node]
$n10 set X_ 760
$n10 set Y_ 150
$n10 set Z_ 0.0
$ns initial_node_pos $n10 50
set n11 [$ns node]
$n11 set X_ 860
$n11 set Y_ 150
$n11 set Z_ 0.0
$ns initial_node_pos $n11 50
set n12 [$ns node]
$n12 set X_ 560
$n12 set Y_ 50
$n12 set Z_ 0.0
$ns initial_node_pos $n12 50
set n13 [$ns node]
$n13 set X_ 760
$n13 set Y_ 50
$n13 set Z_ 0.0
$ns initial_node_pos $n13 50
set n14 [$ns node]
$n14 set X_ 860
$n14 set Y_ 50
```