ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV DAN DSR TERHADAP SERANGAN *BLACK HOLE* PADA JARINGAN MANET

SKRIPSI

untuk memenuhi salah satu persyaratan

mencapai derajat Sarjana S1

Disusun oleh:

HELMI HARTADI

14524082

Jurusan Teknik Elektro

Fakultas Teknologi Industri

Universitas Islam Indonesia

Yogyakarta

2018

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV DAN DSR TERHADAP 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:

Helmi Hartadi
14524082

Yogyakarta, 13 April 2018

Menyetujui,

Pembimbing 1

Ida Nurcahyani, ST., M.Eng.
155240104

LEMBAR PENGESAHAN PENGUJI

LEMBAR PENGESAHAN PENGUJI

ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV DAN DSR TERHADAP SERANGAN *BLACK HOLE* PADA JARINGAN MANET

TUGAS AKHIR

Disusun Oleh :

Helmi Hartadi

14524082

Telah dipertahankan di depan Sidang Penguji syarat untuk memperoleh Gelar Sarjana Konsentrasi Telekomunikasi Jurusan Teknik Elektro Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 27 April 2018

Tim Penguji,

Tito Yuwono, S.T., M.Sc. .....

Penguji 1

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

Penguji 2

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

Penguji 3

Mengetahui,

Ketua Jurusan Teknik Elektro

Universitas Islam Indonesia

Dr. Eng. Hendra Setiawan, S.T., M.T.

ii

PERNYATAAN

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, 13 April 2018

Helmi Hartadi

iii

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Puji dan syukur penulis panjatkan ke hadirat Allah Subhanahu wa ta'ala yang telah melimpahkan kasih dan sayang-Nya kepada kita, sehingga penulis bisa menyelesaikan skripsi ini guna memenuhi salah satu syarat untuk bisa menempuh ujian sarjana teknik pada Fakultas Teknologi Industri (FTI) Program Studi Teknik Elektro di Universitas Islam Indonesia. Shalawat serta salam semoga selalu tercurahkan kepada Baginda Besar Nabi Muhammad SAW. Didalam pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu, disini penulis sampaikan rasa terima kasih sedalam-dalamnya kepada :

1. **Orang Tua tercinta Bapak Mardi dan Ibu Hartini** yang selalu mendoa'kan dan mendukung penulis terhadap hal yang berkaitan dengan tugas akhir maupun tidak.
2. **Ibu Ida Nurcahyani, ST., M.Eng**. Selaku Dosen Pembimbing tugas akhir ini yang telah membantu, mendampingi, serta memberikan banyak masukan di tugas akhir ini.
3. **Bapak Dr. Eng. Hendra Setiawan, ST., M.Eng.** selaku Ketua Jurusan Teknik Elektro, Fakultas Teknik Industri, Universitas Islam Indonesia.
4. **Keluarga** penulis yang sudah memberikan dukungan terkait proses pengerjaan skripsi hingga akhir.
5. **Teman-teman Kos, MTA, Angkatan 2014 Jurusan Teknik Elektro** dan **PASTEL 14 UII** karena telah menemani dan mendukung kegiatan kuliah dari awal hingga kuliah.

Yogyakarta, 13 April 2018

Penulis

Helmi Hartadi

ARTI LAMBANG DAN SINGKATAN

MANET	:	*Mobile Ad-hoc Network*
AODV	:	*Ad-Hoc On Demand Distance Vector*
DSR	:	*Dynamic Source Routing*
GRP	:	*Geographic Routing protocol*
DSDV	:	*Destination-Sequenced Distance Vector*
QoS	:	*Quality of Services*
RREQ	:	*Route Request*
RREP	:	*Route Reply*
RRER	:	*Route Error*
FTP	:	*File Transfer Protocol*
m	:	*Meter*
ms	:	*Milisecond*
Mbps	:	*Megabit per second*

ABSTRAK

Jaringan MANET adalah jaringan yang terdiri atas kumpulan *node* dan sifatnya dinamis serta dapat dibuat dimana saja tanpa menggunakan infrastruktur jaringan yang tetap seperti *base station*, sehingga MANET menjadi rentan terkena serangan. Salah satu dari beberapa serangan yang terjadi dalam jaringan MANET adalah serangan *black hole*. Serangan *black hole* adalah serangan yang menyebabkan paket-paket disekitar *node* penyerang hilang sehingga jaringan mengalami kerugian. Pemilihan *routing protocol* yang tepat adalah salah satu upaya untuk meminimalkan dampak dari serangan *black hole*. Penelitian ini dibuat untuk membandingkan manakah yang lebih baik diantara *routing protocol* AODV dan DSR dalam meminimalkan dampak dari serangan *black hole*. Hasil dari penelitian ini menunjukkan bahwa AODV lebih baik dibandingkan dengan DSR dari beberapa nilai QoS seperti *throughput, delay* dan *packet loss*. Pada *throughput*, ketika terkena serangan *collaborative black hole*, DSR menunjukkan penurunan *throughput* yang signifikan yaitu 13,38% sedangkan AODV hanya 9,21%. Untuk *delay*, AODV juga lebih baik dari DSR, namun ketika terkena serangan *black hole*, AODV dan DSR menunjukkan kinerja tidak stabil yang hampir sama. Untuk *packet loss*, AODV juga lebih baik dari DSR karena AODV memiliki nilai *packet loss* yang lebih sedikit. Dari keseluruhan penelitian ini, diperoleh hasil bahwa protokol AODV memberikan nilai QoS yang lebih baik pada saat jaringan tidak terkena serangan maupu pada saat terkena serangan *black hole*.

Kata Kunci : MANET, AODV, DSR , *Black Hole*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi jaringan nirkabel semakin berkembang sejak jaringan nirkabel pertama kali ditemukan. *Mobile Ad Hoc Network* (MANET) adalah salah satu teknologi pada bidang telekomunikasi yang saat ini masih diteliti dan dikembangkan. MANET terdiri dari sekumpulan titik perangkat nirkabel (*node*) yang bersifat dinamis dan sementara tanpa menggunakan infrastruktur jaringan yang sudah ada seperti *base station*. Jaringan MANET tidak membutuhkan prasarana yang menggunakan biaya besar, sehingga tidak perlu membangun jaringan komunikasi fisik di tempat yang sulit dibuat infrastrukturnya [1]. Salah satu contoh penerapan MANET adalah pada saat terjadi bencana alam dan infrastruktur telekomunikasi terjadi kerusakan yang menyebabkan komunikasi jaringan selular melalui BTS tidak dapat digunakan, disinilah MANET dapat diterapakan sebagai komunikasi jaringan nirkabel alternatif untuk berkomunikasi dengan memanfaatkan perangkat *mobile* yang ada disekitarnya.

Setiap *node* pada jaringan MANET tidak hanya berfungsi sebagai *host,* tetapi juga dapat berfungsi sebagai *router* untuk meneruskan paket data dari satu perangkat ke perangkat lainnya. Pada jaringan *ad hoc,* rute diantara *node* pada jaringan *ad hoc* bersifat *multihop*, sehingga komunikasi antar *node* memanfaatkan *node* lain sebagai perantara apabila jangkauan komunikasi langsung berada di luar *node* tujuan komunikasi tersebut. *Ad hoc* merupakan mode jaringan *Wireless Local Area Network* yang cukup sederhana, karena pada jaringan *ad hoc* tidak memerlukan *access point*, setiap *host* memiliki *transmitter* dan *receiver* untuk berkomunikasi secara langsung [2].

Routing protocol adalah standarisasi tentang pengaturan sebuah *node* untuk meneruskan paket dari *node* satu ke *node* lainnya. Pada jaringan MANET setiap *node* bersifat sebagai *router* yang berfungsi untuk menentukan rute yang akan dituju. Tiap *node* pada jaringan MANET bersifat *ad hoc* yang selalu bergerak, sehingga berdampak pada jaringan MANET karena sifatnya yang berubah ubah seiring dengan pergerakan *node* tersebut. Karena setiap *node* bersifat sebagai *router* yang bergerak bebas, maka pada jaringan MANET dibutuhkan *routing protocol* yang tepat untuk membantu *node* agar dapat mengirimkan data secara cepat dan lebih efisien.

Pada jaringan MANET, *routing protocol* diklasifikasikan menjadi tiga bagian yaitu reaktif, proaktif dan *hybrid*. Protokol yang akan dibahas adalah protokol yang berada dari kelas reaktif. Potokol reaktif bekerja dengan cara mencari rute apabila ada permintaan. Ada beberapa macam

protokol dari kelas reaktif, salah satunya yaitu adalah AODV dan DSR. Cara kerja pencarian rute dari protokol AODV dan DSR ini memiliki kesamaan, karena berasal dari kelas yang sama. Meskipun memiliki kesamaan, namun protokol AODV dan DSR ini adalah protokol yang memiliki cara kerja yang berbeda. Hal ini yang membuat AODV dan DSR menjadi bahan penelitian penulis.

Jaringan MANET yang bersifat dinamis menjadikan MANET sangat rentan terhadap serangan-serangan yang terjadi dari dalam maupun dari luar jaringan. Ada beberapa macam serangan yang ada pada jaringan MANET, salah satunya adalah serangan *Black Hole*. Serangan *Black hole* ini bekerja dengan cara yaitu mengambil paket yang lewat pada *node* sekitar node *black hole*, lalu kemudian paket akan dibuang. *Node Black hole* menempatkan dirinya di tengah-tengah pengiriman paket antara *node* pengirim dengan *node* penerima. Serangan *black hole* dapat dengan mudah masuk ke jaringan karena mekanisme penyerangannya yang sederhana dan dapat memberikan dampak yang buruk bagi jaringan.

Penelitian ini dilakukan untuk mengetahui kinerja dari *routing protocol* AODV dan DSR pada saat keduanya tidak terkena serangan maupun pada saat terkena serangan *black hole* di jaringan MANET. Penelitian ini dilakukan dengan cara simulasi dan dianalisis menggunakan parameter QoS yang sudah ditentukan seperti *throughput*, *delay*, dan *packet loss*.

1.2 Rumusan Masalah

Perumusan masalah pada peneltian ini adalah:

1. Bagaimana kinerja *routing protocol* AODV dibandingkan dengan protokol DSR pada jaringan MANET.
2. Apa dampak serangan *black hole* bagi *routing protocol* AODV dan DSR pada jaringan MANET.
3. Protokol manakah yang lebih baik antara AODV dan DSR apabila diberikan serangan *single black hole* ataupun *collaborative black hole* pada jaringan MANET.

1.3 Batasan Masalah

Adapun beberapa batasan masalah yang ada pada tugas akhir ini adalah :

1. Penelitian ini berupa simulasi menggunakan perangkat lunak OPNET Modeler 14.5.
2. Penelitian ini berfokus pada analisis perbandingan kinerja *routing protocol* AODV dan DSR dengan dan tanpa serangan *black hole*.
3. Parameter QoS yang diamati adalah *throughput*, *delay*, dan *packet loss*.

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini yaitu :

1. Mengetahui kinerja dari *routing protocol* AODV dan DSR pada jaringan MANET.
2. Mengetahui dampak serangan *black hole* pada *routing protocol* AODV dan DSR di jaringan MANET.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah :

1. Menambah data dan informasi yang ditujukan kepada peneliti lain yang juga ingin mengembangkan serta memperbaiki sistem jaringan MANET.
2. Memberikan informasi tentang protokol mana yang lebih baik khususnya terhadap *routing protocol* yang diteliti.
3. Mengetahui kinerja dari *routing protocol* AODV dan DSR pada jaringan MANET
4. Mengetahui kinerja dari *routing protocol* AODV dan DSR apabila terkena serangan *black hole* pada jaringan MANET.

BAB 2
TINJAUAN PUSTAKA

2.1 Studi Literatur

Salah satu penelitian pada MANET yaitu penelitian yang dilakukan oleh Sarah Devi Anggraini, Kukuh Nugroho, dan Eko Fajar Cahyadi [3] yang membandingkan kinerja protokol AODV dan DSR pada MANET. Pengambilan data dilakukan dengan menggunakan *software* OPNET MODELER 14.5. Penelitian ini dibagi menjadi 6 skenario yang berbeda yaitu masing-masing protokol diberikan aplikasi FTP *low load*, FTP *high load*, dan *video conferencing*. Masing-masing skenario dibuat setara agar menghasilkan keluaran yamg setara. Untuk analisis, ada beberapa parameter yang digunakan untuk menilai yaitu *latency, throughput, jitter,*dan *packet loss*. Untuk hasilnya, pada layanan FTP dan *video conferencing* menghasilkan nilai yang masih dapat diterima dalam standar TIPHON. Namun untuk latency, kedua layanan menghasilkan latency yang sangat tinggi. Pada parameter *throughput,* AODV menghasilkan *throughput* yang lebih besar dari DSR pada percobaan FTP dan *video conferencing*. Pada parameter delay dan jitter untuk hasilnya didapatkan bahwa AODV lebih baik daripada DSR karena mempunyai nilai *delay* dan *jitter* yang lebih kecil. Sedangkan pada *packet loss,* DSR mempunyai kinerja yang lebih baik dari DSR pada skenario FTP dan *video*. Kesimpulan untuk keseluruhannya adalah protokol AODV lebih baik dari DSR dari semua parameter yang diteliti kecuali *packet loss*.

Selanjutnya ada penelitian yang dilakukan oleh Fitri Amillia, Marzuki, dan Agustina mengenai studi perbandingan kinerja antara protokol DSR dan GRP pada MANET [2]. Penelitian ini dilakukan dengan cara simulasi menggunakan *software* OPNET MODELER 14.0. Penelitian ini dibuat dengan mensimulasikan dua skenario yang berbeda dengan masing-masing jumlah *Node* sebanyak 25 dan 50 *Node*. Penyusunan jaringannya dibuat sama untuk kedua protokol yang dibandingkan. Untuk parameter pengujian yang digunakan untuk analisis adalah *thorughput, delay, load, media access delay, data dropped, dan network load*. Pada parameter *throughput* protokol GRP menghasilkan throughput yang lebih besar dari DSR. Protokol GRP juga lebih baik dari protokol DSR dalam hal perbandingan *delay*. Untuk *load* keseluruhan, DSR lebih baik dari GRP. Dari hasil keseluruhanya penulis mendapatkan kesimpulan bahwa protokol GRP lebih baik dibandingkan dengan *protocol* DSR berdasarkan dari analisis dari parameter-parameter tersebut.

Yulia Dhamayanti dan Gamantyo Hendrantoro [4] membuat penelitian tentang studi perbandingan dari *routing protocol* DSR dan AODV untuk sistem komunikasi taktis di kapal perang. Metode penelitian yang dilakukan mengenai beberapa hal yaitu tentang spesifikasi dari

sistem yang digunakan, variabel dari penelitian, perancangan topologi dan membuat simulasi menggunakan *routing protocol* DSR dan AODV pada MANET. Pembutan topologi di jaringan menggunakan simulasi menggunakan *software* NS2. *Node* yang digunakan bervariasi yaitu terdiri dari 5, 13 dan 21 *node*. Pada masing-masing dari *node* tersebut di atur sedemikian rupa agar membentuk formasi yang ada pada kapal perang dan juga formasi *random*. Sedangkan parameter yang digunakan sebagai indikator perbandingan yaitu *packet deliver ratio, end to end delay,* dan *routing overhead.* DSR termasuk dalam *routing protocol* yang reaktif, begitu juga AODV. Dari keseluruhan percobaannya, penulis menyatakan bahwa *routing protocol* AODV lebih baik daripada *routing* protokol DSR dilihat dari beberapa aspek penilaian QoS. Penulis menemukan bahwa pada *routing* DSR ada kendala saat berada di jaringan yang jumlah *node*nya semakin banyak kinerjanya semakin menurun. Penulis lebih memilih *routing protocol* AODV untuk diimplementasikan pada komunikasi taktis pada kapal perang.

Istas Pratomo dan M. Hizrian Hizburrahman [5] pada tahun 2015 melakukan penelitian tentang Pendeteksian Dan Pencegahan Serangan *black hole* dan *grey hole* pada MANET. Penulis menjelaskan bagaimana caranya untuk mengetahui serta menangani serangan *black hole* dan *grey hole* pada *routing protocol* AODV. metode yang digunakan yaitu dengan cara *node* yang berbahaya dideteksi, lalu algoritma yang sudah dirancang akan melawan *node* berbahaya tersebut dengan cara menjauhkan *node* berbahaya dari jaringan dengan cara memanfaatkan paket *routing* yang sebelumnya hanya membawa tentang informasi *routing* dan akan ditambahkan informasi tentang lokasi *node* berbahaya yang sudah dideteksi sebelumnya. Kesimpulan paper ini adalah *black hole* dan *grey hole* ini menurunkan kinerja jaringan, khususnya pada QoS seperti *throughput, delay* dan penggunaan daya. Untuk memperbaiki hal tersebut maka ada beberapa hal yang harus diperbesar seperti *injection rate, buffer size* dan lainnya.

Pada studi literatur, dijelaskan bahwa dari beberapa penelitian yang dilakukan, para penulis mengklaim bahwa protokol AODV memiliki keunggulan. Penelitian AODV dan DSR sudah pernah dilakukan dan diambil kesimpulan bahwa AODV lebih baik dari DSR dengan menggunakan beberapa parameter yang digunakan untuk menilai. Sedangkan pada serangan *black hole,* protokol AODV mengalami penurunan apabila terkena serangan *black hole*. Namun pada jaringan lain selain AODV belum dilakukan perbandingkan tentang dampak serangan *black hole*. Oleh sebab itu, maka peneliti mencoba untuk melakukan penelitian yang menyangkut tentang dampak dari serangan *black hole* terhadap *routing protocol* yang ada pada jaringan MANET.

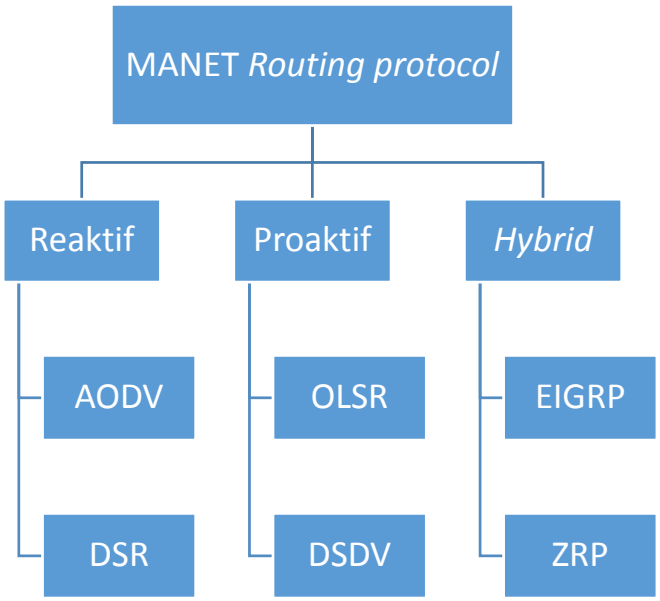
2.2 Tinjauan Teori

2.2.1 *Mobile Ad-Hoc Network* (MANET)

Mobile ad hoc network (MANET) adalah sekumpulan titik perangkat nirkabel (*node*) yang bersifat dinamis dan sementara tanpa menggunakan infrastruktur yang sudah dibangun seperti *base station* [1]. Pada MANET, setiap *node* yang aktif tidak hanya berperan sebagai penerima, tetapi berperan juga sebagai *router* untuk meneruskan paket ke tujuan. Setiap *node* pada MANET bergerak secara bebas dan saling berkomunikasi dengan cara saling meneruskan paket dari satu *node* ke *node* lainnya. Topologi jaringan MANET bersifat dinamis yang membuat jaringan MANET menjadi tidak terduga. Pada jaringan MANET, aktivitas jaringan dilakukan oleh *node* itu sendiri. termasuk pembuatan topologi dan penyampaian pesan. Karena hal itu, *node* pada MANET harus diberikan fungsi *routing* agar *node* pada jaringan dapat menjalankan proses pencarian rute dan pengiriman data secara cepat dan efisien.

2.2.2 Klasifikasi *Routing protocol*

Routing protocol merupakan standarisasi mengenai pengaturan *node* untuk pencarian rute. Umumnya *routing protocol* pada MANET diklasifikasikan menjadi tiga yaitu reaktif, proaktif dan *hybrid* seperti yang ditampilkan pada Gambar 2.1. Pada penelitian ini, protokol yang digunakan untuk perbandingan adalah protokol dari kelas reaktif, yaitu AODV dan DSR.



Gambar 2.1 Klasifikasi *Routing protocol*

Routing protocol proaktif adalah *routing* yang bekerja dengan cara membanjiri *node* yang terhubung dengan informasi tentang tetangganya. *Routing protocol* proaktif menyimpan informasi *routing* dan memeliharanya secara *up to date*, dengan menukarkan paket ke tetangganya. Contoh protokol proaktif adalah DSDV, OLSR, WRP dan lainnya [6]. Sedangkan untuk *routing protocol* reaktif bekerja hanya pada saat jika ada *node* yang melakukan permintaan untuk menemukan rute ke tujuan. Hal ini mengurangi *overhead* yang terjadi pada protokol proaktif. Contoh protokol reaktif adalah AODV, DSR, dan lainnya [7]. Sedangkan untuk protokol kelas *hybrid*, cara kerjanya yaitu dengan menggabungkan keuntungan antara kelas reaktif dan proaktif [8].

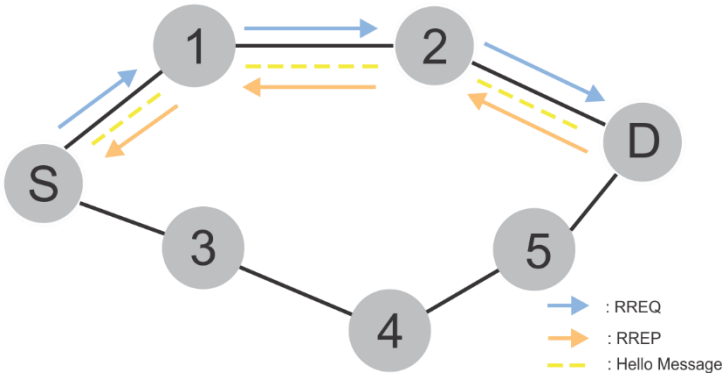
2.2.3 *Ad-Hoc On Demand Distance Vector* (AODV)

AODV adalah salah satu dari beberapa protokol reaktif pada MANET yang cara kerjanya berdasarkan pada permintaan. Pada AODV, rute dari *node* satu ke *node* lain akan dibuat jika *node* sumber menginginkan adanya pengiriman paket ke *node* tujuan yang dipilih. Node pada AODV akan menyimpan tabel *routing* hanya satu *node* tujuan untuk satu rute [9]. Pada *routing* AODV, jika rute tidak digunakan pada waktu yang sudah ditentukan maka rute akan dihapus dari tabel *routing*. Proses pencarian rute pada AODV terbagi menjadi dua macam, yaitu *route discovery* dan *route maintenance*. *Route discovery* ini menggunakan dua paket yaitu *Route Request* (RREQ) dan *Route Reply* (RREP). Sedangkan untuk *Route Maintenance* menggunakan paket *Route Error* (RERR). Untuk menghasilkan rute yang bebas *routing loop*, AODV menggunakan fitur *destination sequence number*. *Routing loop* di sini artinya yaitu kondisi saat sebuah paket yang ditransmisikan dalam *route* tidak pernah sampai ke tujuan.

Cara kerja AODV yaitu apabila ada permintaan pengiriman paket ke suatu *node*, maka paket RREQ akan disebar ke *node* disekitarnya. Apabila *node* yang menerima paket RREQ mempunyai informasi tentang rute ke *node* tujuan, maka *node* itu akan membalas dengan mengirimkan paket RREP ke *source node* seperti pada Gambar 2.2. Namun apabila jika *node* tersebut tidak mengetahuinya, pesan RREQ akan di-*broadcast* ulang oleh *node* tersebut ke *node* sekitarnya setelah nilai *hop counter*nya ditambahkan.

Pada AODV, *node* menggunakan *destination sequence number* untuk menjaga informasi yang benar mengenai *reverse path* yang mengarah ke *source node*. *Reverse Path* terbentuk saat RREQ menempuh *node* yang dituju, dimana setiap RREQ akan diidentifikasi dari *node* sekitar yang mengirimkan RREQ tadi. Saat *node* yang dituju mempunyai informasi rute menuju *node* tujuan menerima paket RREQ, maka nilai *destination sequence number* yang ada pada RREQ akan dibandingkan. Apabila nilai *sequence number* pada RREQ lebih besar dari nilai yang ada pada *node* yang menerima, maka paket RREQ akan diteruskan lagi ke *node* sekitarnya, dan sebaliknya

apabila nilai *destination sequence number* pada *node* penerima sama atau lebih besar dengan nilai di RREQ maka paket RREP akan dikirimkan oleh *node* tersebut kembali ke *source node* dengan memakai *reverse path* yang telah dibuat sebelumnya. Inilah fungsi dari *Reverse Path* ini yaitu agar *node* tujuan dapat mencapai *node* sumber yang nantinya akan dijadikan rute untuk pengiriman paket data [10].



Gambar 2.2 Proses pencarian rute AODV

Selanjutnya jika rute sudah terbentuk, maka yang akan bertanggungjawab untuk menjaga rutenya adalah *node* sumber. Jika nantinya ada kerusakan, maka *Route Maintenance* disini yang akan bekerja dengan cara mengirimkan paket RERR ke *node* yang mengalami kerusakan ke semua *node* yang ada di jaringan sampai ke sumbernya lagi. Protokol routing AODV ini memiliki beberapa kekurangan dan kelebihan yang diringkas dalam Tabel 2.1 [7].

Tabel 2.1 Kelebihan dan Kekurangan AODV

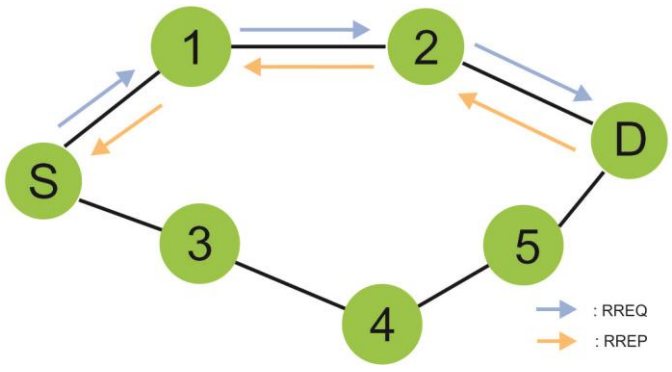
Kelebihan	Kekurangan
1. Beradaptasi ke topologi yang sangat dinamis 2. Bebas *Loop* 3. Memiliki *bandwidth* yang efisien karena *routing overhead* yang kecil	1. Tidak dapat menampung penambahan beban berat 2. AODV membutuhkan waktu untuk membangun tabel *routing*

2.2.4 *Dynamic Source Routing* (DSR)

DSR juga merupakan salah satu dari beberapa *routing protocol* reaktif yang ada, karena DSR berada dikategori *routing protocol* reaktif seperti AODV. Meskipun demikian AODV dan DSR memiliki cara kerja yang memiliki beberapa kesamaan dengan AODV. DSR menggunakan dua mekanisme juga untuk menghubungkan rute. Mekanisme tersebut yaitu dengan cara *Route Discovery* & *Route Maintenance* menggunakan paket RREP, RREQ dan RRER.

Salah satu perbedaannya yaitu DSR pemilihan rutenya berdasarkan dari *node* sumber. DSR tidak memiliki fitur pengiriman pesan secara periodik seperti AODV. DSR memiliki fitur *Cache Memory* yang berfungsi sebagai penyimpanan semua informasi tentang *routing* yang tersedia di jaringan. *Cache memory* ini membuat proses pemulihan jaringan lebih mudah jika seandainya topologi jaringan berubah secara tiba-tiba. DSR tidak perlu lagi melakukan *route discovery* lagi jika ada perubahan topologi. DSR hanya perlu mencari lagi rute yang tersedia pada *Cache memory* tadi yang telah menyimpan informasi-informasi *routing*.

Mekanisme pencarian rute pada DSR hampir sama dengan AODV, yaitu apabila *node* sumber menginginkan untuk melakukan pengiriman data namun tidak memiliki informasi mengenai rute yang akan dilalui, DSR akan memulai proses pencarian rute dengan cara menyebarkan paket RREQ ke *node* terdekatnya. Paket RREQ yang dikirimkan berisikan tentang alamat pengirim serta tujuannya. Node-*node* yang menerima paket RREQ akan menyimpan informasi mengenai jalur tersebut kedalam *cache memory* tadi. Jika rute telah ditemukan, *node* akan mengirimkan paket RREP untuk membalas ke rute asalnya. Paket RREP dikirimkan dengan menggunakan jalur *Reverse Path* yang terbentuk pada saat pengiriman paket RREQ tadi. Proses pencarian rute pada DSR dapat dilihat pada Gambar 2.3.



Gambar 2.3 Proses pencarian rute DSR

Routing protocol DSR memiliki beberapa kelebihan dan kekurangan yang ditunjukkan pada Tabel 2.2 [7] yang terlampir.

Tabel 2.2 Kelebihan dan Kekurangn DSR

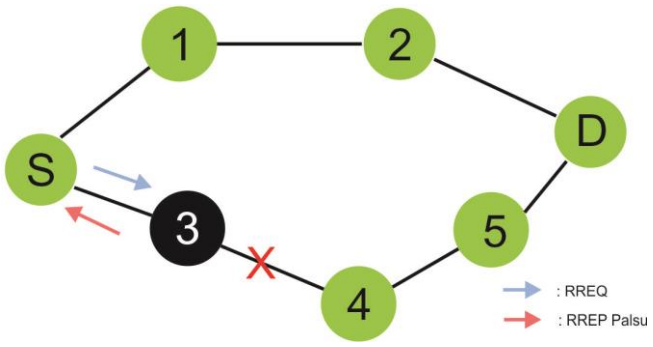
Kelebihan	Kekurangan
1. Mendukung pengrutean banyak jalur 2. Tidak perlu memelihara rute secara *update*	1. Tidak dapat menahan beban penambahan jaringan yang besar yang diakibatkan oleh pencarian rute dan *flooding*. 2. Latensi penemuan rute tinggi

2.2.5 *Black hole Attack*

Black hole attack adalah salah satu serangan yang bisa terjadi pada jaringan. *Black hole* bekerja dengan cara menyerap paket disekitar *node* penyerang, setelah itu membalas dengan paket RREP palsu lalu membuangnya. *Black hole attack* terbagi menjadi dua macam yaitu serangan yang hanya dilakukan oleh satu *node* penyerang dan serangan *collaborative black hole* yang dilakukan oleh lebih dari satu *node* yang saling bekerja sama [11].

Black hole melakukan penyerangan dengan cara *node* penyerang menyatakan kepada *node* sumber bahwa *node* penyerang ini mempunyai jarak rute terpendek ke arah *node* tujuan. Saat *node* penyerang menerima paket RREQ, maka selanjutnya *node* penyerang seketika mengirim paket RREP yang palsu kepada *node* sumber. *Node* penyerang tidak memeriksa informasi mengenai *node* tujuan. Node penyerang juga menyatakan bahwa ia adalah *node* dengan rute terpendek dan terbaru dengan cara memanipulasi RREP dan mengirimkan *hop count* yang salah [5].

Dengan cara tersebut *node* sumber akan menolak paket RREP dari *node* lain yang telah membalas paket RREQ tersebut meskipun rute yang dibalas tersebut adalah rute yang benar. Sehingga rute antara sumber dan penyerang akan terbentuk dan kemudian paket akan dibuang oleh *node* penyerang [10]. Berikut adalah gambaran dari serangan *black hole* yang ditunjukkan pada Gambar 2.4.



Gambar 2.4 Mekanisme *Black hole Attack*

BAB 3
METODOLOGI

3.1 Alat dan Bahan

Penelitian ini dilakukan dengan cara mengambil data dari suatu *software* simulasi. Adapun perangkat – perangkat yang digunakan untuk mendukung penelitian ini akan dijelaskan pada sub bab berikut.

3.1.1 Perangkat Keras

Penelitian ini menggunakan perangkat keras berupa satu buah laptop untuk menjalankan simulasi dengan spesifikasi :

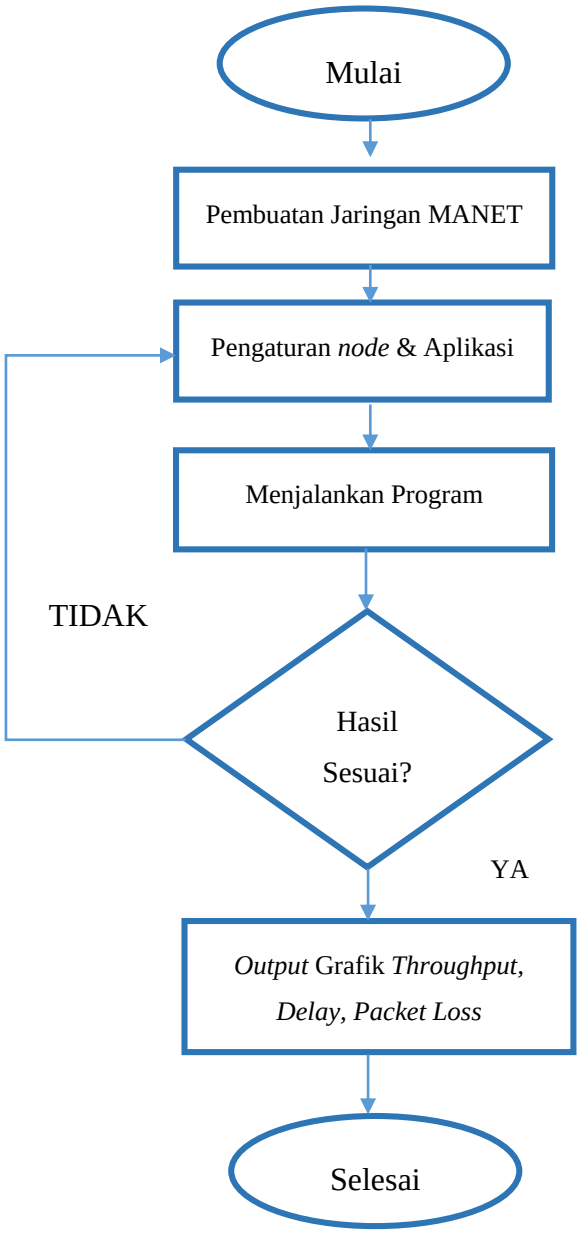
1. *Processor* : *Intel® Core™ i3-5005U Processor (3M Cache, 2.00 GHz)*
2. RAM : 8GB DDR3
3. VGA : Nvidia Geforce GT 920M 2GB
4. *Harddisk* : 500GB

3.1.2 Perangkat Lunak

Adapun beberapa perangkat lunak yang digunakan untuk melakukan simulasi adalah sebagai berikut :

1. *Operating System Microsoft Windows 8.1 Pro 64 bit*
2. OPNET MODELER 14.5
3. *Microsoft Excel 2013*
4. *Microsoft Visual Studio 2008*

3.2 Perancangan Program



Gambar 3.1 *Flowchart* perancangan program

Dari Gambar 3.1 dapat dilihat alur pembuatan simulasi yang dilakukan oleh penulis melalui beberapa tahapan yaitu :

1. Pembuatan Jaringan MANET untuk menentukan berapa *node*, server ataupun aplikasi apa yang akan dipakai di jaringan.
2. Pengaturan *node* & Aplikasi ini adalah proses pada saat mengatur apa saja yang akan berpengaruh pada jaringan, seperti protokol, jenis *traffic* yang digunakan, ukuran paket, kecepatan *node* dan pengaturan aplikasi lainnya.

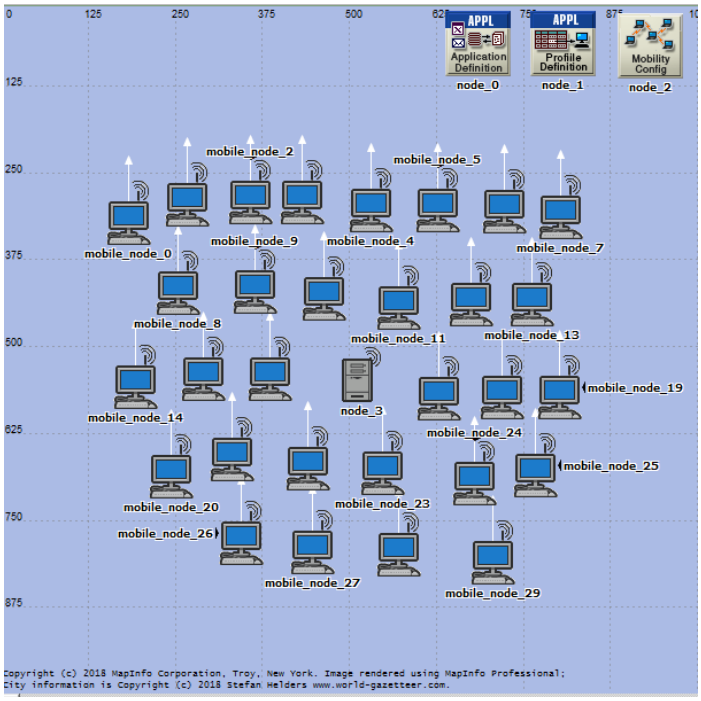
3. Menjalankan program untuk mengetahui hasil keluarannya.
4. Jika simulasi selesai dijalankan dan sesuai dengan yang diinginkan, maka akan menghasilkan keluaran *berupa throughput, delay,* dan *packet loss.*

3.3 Skenario Simulasi

Pada penelitian ini, untuk mengetahui kinerja dari masing-masing protokol yaitu dengan cara membuat beberapa skenario yang berbeda. skenario yang digunakan adalah yang pertama berupa pengaturan *default* pada saat *node* belum terkena serangan *black hole*. Lalu yang kedua yaitu skenario pada saat kedua *routing protocol* terkena serangan *black hole* dan yang terakhir adalah skenario pada saat jaringan MANET terkena serangan *black hole* dari kumpulan *attacker node* yang membentuk *collaborative black hole*. Simulasi dijalankan selama 1000 detik atau sekitar 16,6 menit untuk semua skenario. Berikut di bawah ini adalah detail dari masing-masing skenario yang akan di buat.

3.3.1 Skenario Tanpa Serangan

Pada skenario ini masing-masing *routing protocol* (AODV dan DSR) akan diuji dengan parameter-parameter yang sudah ditentukan. Skenario 1 ini menggunakan pengaturan biasa untuk kedua *routing protocol*. Masing-masing *routing protocol* akan diuji dengan *node* yang berjumlah sebanyak 30 *node + 1 Server*. Berikut adalah spesifikasi jaringan MANET pada Gambar 3.2 dan Tabel 3.1 yang terlampir.



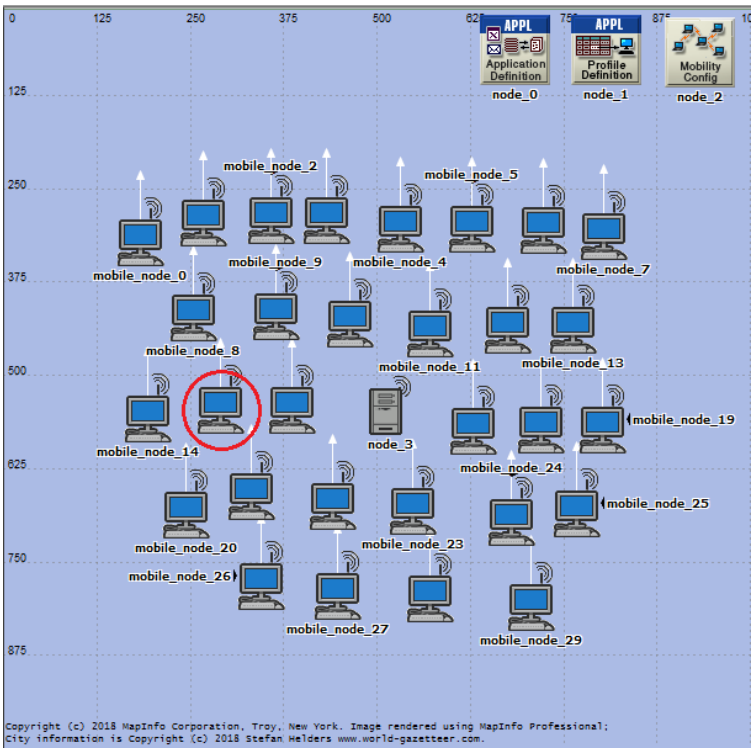
Gambar 3.2 Skenario Tanpa serangan

Tabel 3.1 Spesifikasi Skenario 1

No	Parameter	Nilai
1.	Luas Area	1000x1000 meter
2.	Jumlah *node* Normal	30 *node + 1 Server*
3.	Jumlah *node Black hole*	-
4.	*Data rate*	11 Mbps
5.	Jenis Pergerakan *node*	*Random Waypoint*
6.	Aplikasi Jaringan	FTP
7.	Jenis *Traffic* Aplikasi	*High load*

3.3.2 Skenario *Single Black Hole*

Untuk skenario kedua ini pengaturannya dibuat sama dengan skenario pertama, hanya saja ada penambahan satu *Black hole node* yang diberikan pada jaringan MANET AODV dan DSR untuk memberikan efek *Single Black hole node*. Berikut adalah spesifikasi dari jaringan MANET yang ditunjukkan pada Gambar 3.3 dan Tabel 3.2 yang terlampir.



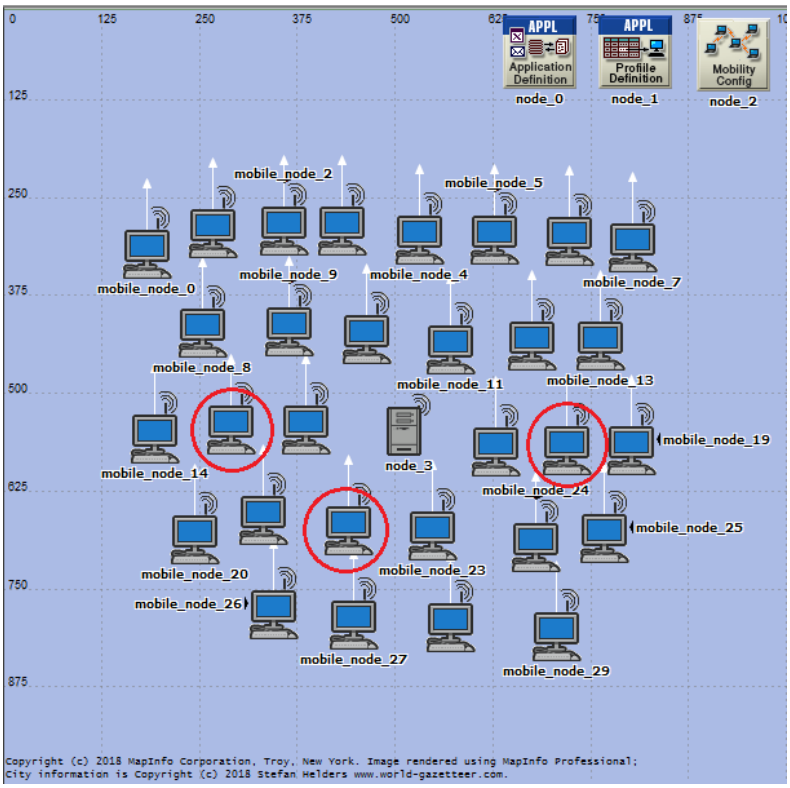
Gambar 3.3 Skenario *Black hole*

Tabel 3.2 Spesifikasi Skenario 2

No	Parameter	Nilai
1.	Luas Area	1000x1000 meter
2.	Jumlah *node* Biasa	29 *node* + 1 *Server*
3.	Jumlah *node Black hole*	1 *Attacker node*
4.	*Data rate*	11 Mbps
5.	Jenis Pergerakan *node*	*Random Waypoint*
6.	Aplikasi Jaringan	FTP
7.	Jenis *Traffic* Aplikasi	*High load*

3.3.3 Skenario *Collaborative Black Hole*

Skenario ketiga adalah skenario untuk jaringan MANET yang terkena serangan *collaborative black hole*. Serangan jenis ini menyerang jaringan MANET dengan menggunakan lebih dari satu *node* penyerang. Berikut spesifikasi dari skenario 3 ada pada Gambar 3.4 dan Tabel 3.3 yang terlampir.



Gambar 3.4 Skenario *Collaborative Black hole*

Tabel 3.3 Spesifikasi Skenario 3

No	Parameter	Nilai
1.	Luas Area	1000x1000 meter
2.	Jumlah *node* Normal	27 *node* + *1 Server*
3.	Jumlah *node Black hole*	3 *Attacker node*
4.	*Data rate*	11 Mbps
5.	Jenis Pergerakan *node*	*Random Waypoint*
6.	Aplikasi Jaringan	FTP
7.	Jenis *Traffic* Aplikasi	*High load*

3.3.4 Cara Analisis

Parameter QoS *routing* didalam jaringan *ad hoc* ad-hoc adalah suatu hal penting untuk mengetahui kinerja dari suatu jaringan. Pada skenario ini beberapa parameter QoS yang digunakan untuk menguji kinerja jaringan protokol secara keseluruhan yaitu *Throughput*, *Delay* dan *Packet loss* [12].

1. *Throughput*

   Throughput adalah kecepatan transfer data yang berjalan pada suatu jaringan yang diukur dengan satuan *bit per second*. *Throughput* merupakan jumlah total paket yang diterima dengan sukses dan dibagi pada interval waktu tertentu.

2. *Delay (Latency)*

   Delay adalah selang waktu pengiriman data dari pengirim hingga ke penerima dihitung dengan menggunakan satuan waktu. Banyak hal yang mempengaruhi *delay* ini, seperti jarak, media yang digunakan, gangguan pada jaringan atau juga proses yang memakan waktu lama [13]. Pada standar TIPHON [14], *delay* diklasifikasikan dalam beberapa kategori yang ditunjukkan Tabel 3.4.

Tabel 3.4 Klasifikasi *Delay*

Kategori *Delay*	***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

3. *Packet loss*

Packet loss adalah jumlah banyaknya paket yang hilang pada saat pengiriman paket pada suatu jaringan. Pada TIPHON [14], Packet Loss diklasifikasikan dalam beberapa kategori yang ditunjukkan pada Tabel 3.5.

$$Packet\ Loss = \left(\frac{data\ dikirim - data\ yang\ diterima}{paket\ data\ yang\ dikirim} \right) \times 100\% \qquad (3.1)$$

Tabel 3.5 Klasifikasi *Packet Loss*

Kategori Packet Loss	***Packet Loss***	**Indeks**
Sangat Bagus	0%	4
Bagus	3%	3
Sedang	15%	2
Buruk	25%	1

BAB 4
HASIL DAN PEMBAHASAN

4.1 Hasil dan Analisis

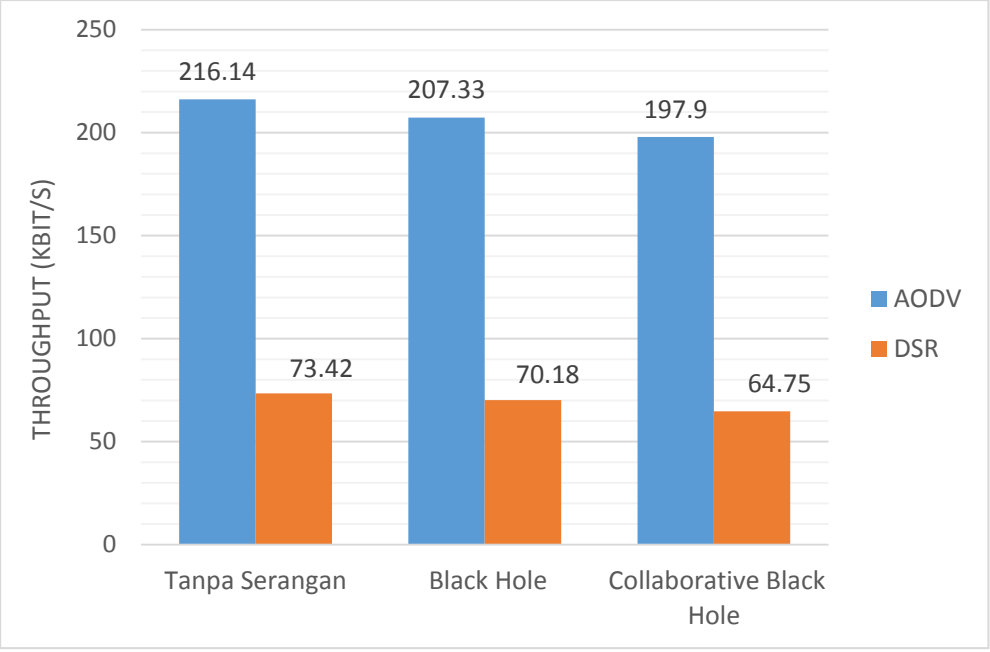
Pada bagian bab ini penulis akan membahas secara keseluruhan mengenai hasil yang didapatkan dari simulasi jaringan yang sudah dijalankan hingga selesai. Hasil ini akan diamati menggunakan parameter-parameter QoS yang sudah ditentukan sebelumnya yaitu *throughput*, *delay* dan *packet loss*. Layanan yang digunakan pada jaringan pada masing-masing skenario adalah FTP dengan beban *high load*.

4.2 *Throughput*

Data *Throughput* yang dihasilkan oleh keluaran simulator ditunjukkan pada Tabel 4.1 dan Gambar 4.1 yang terlampir.

Tabel 4.1 Nilai rata-rata *Throughput (kbit/s)*

Routing protocol	**Tanpa Serangan**	***Black hole***	***Collaborative Black hole***
AODV	216.14	207.33	197.90
DSR	73.42	70.18	64.75



Gambar 4.1 Grafik keluaran *Throughput (kbit/s)*

Hasil Keluaran *Throughput, routing protocol* AODV dan DSR masing-masing memiliki kemampuan untuk mengirimkan data yang berbeda. Pada AODV, percobaan tanpa serangan menghasilkan *throughput* sebesar 216,14 bit/s. Sedangkan untuk DSR hanya mempunyai *throughput* sebesar 73,42 bit/s. Hal ini disebabkan oleh beberapa faktor. Salah satu alasannya protokol DSR memiliki *throughput* lebih rendah adalah akrena protokol *routing* DSR menggunakan mekanisme *Source Routing* pada saat pencarian rutenya, yang membuat pencarian rute menjadi lebih lama dan berdampak kepada *throughput*nya [3]. Hal kedua yang membuat throughput AODV lebih tinggi daripada protokol DSR yaitu karena, AODV menggunakan pesan periodik terhadap *node* yang telah terbentuk rute untuk menjaga rutenya, sehingga AODV mengeluarkan throughput yang lebih besar daripada DSR.

Pada percobaan *single Black hole*, untuk protokol *routing* AODV, *throughput*nya mengalami penurunan sebesar 4,25% dari sebelumnya tanpa serangan. Sedangkan pada protokol DSR mengalami penurunan yang berbeda sedikit dengan AODV yaitu sebesar 4,62%. Hal ini dapat terjadi karena pengaruh Malicious *node Black hole* yang membuat jaringan MANET menjadi tidak stabil akibat proses penyerapan dan pembuangan paket yang dilakukan oleh *black hole node* tersebut dan mengakibatkan *throughput* turun.

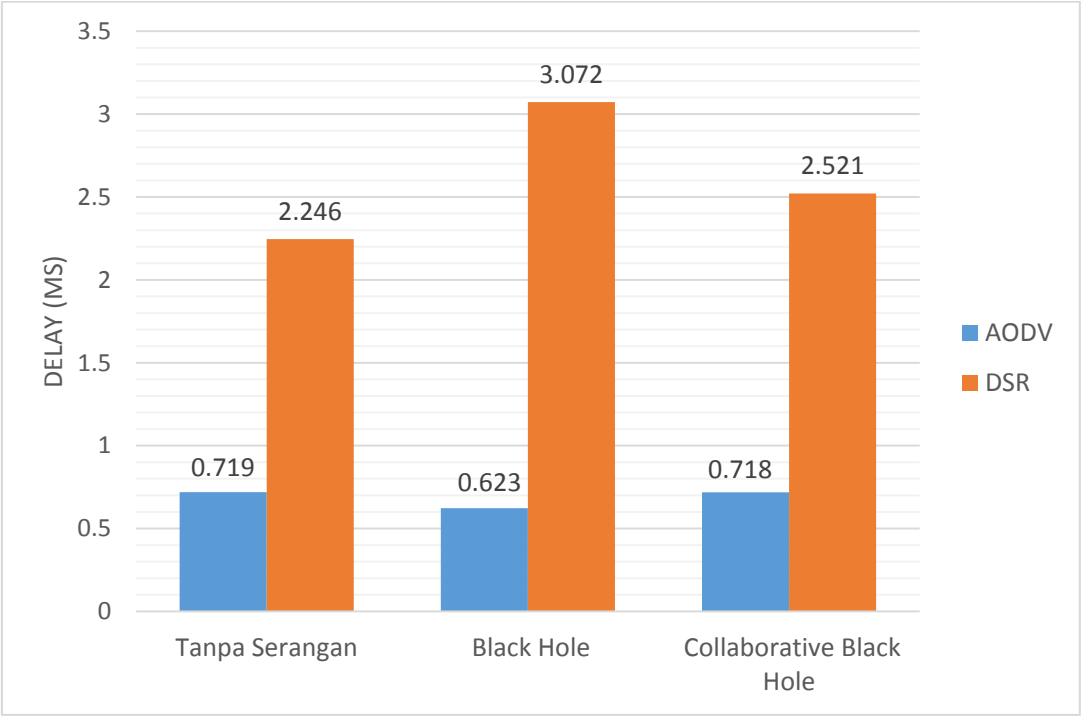
Sedangkan pada jaringan MANET yang terkena serangan *collaborative black hole* mengalami penurunan *throughput* yang cukup signifikan yaitu sebesar 9,21% protokol AODV dan untuk DSR mengalami penurunan yang cukup banyak yaitu 13,38% dibandingkan dari skenario pada saat jaringan MANET tidak terkena serangan apapun. Penurunan ini disebabkan oleh serangan black hole yang dilakukan secara berkelompok, yang mengakibatkan turunnya *throughput* secara signifikan.

4.3 *Delay*

Data *Delay* yang dihasilkan oleh keluaran simulator ditunjukkan pada Tabel 4.2 dan Gambar 4.2 yang terlampir.

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

Routing protocol	**Tanpa Serangan**	***Black hole***	***Collaborative Black hole***
AODV	0.719	0.623	0.718
DSR	2.246	3.072	2.521



Gambar 4.2 Grafik Keluaran *Delay (ms)*

Pada perbandingan tanpa adanya serangan apapun, dapat dilihat pada tabel 4.2, rata-rata *delay* pada protokol AODV lebih kecil dibandingkan dengan DSR. Hal ini menunjukkan bahwa protokol DSR membutuhkan waktu yang lebih lama dalam penyampaian paket. Tingginya *delay* pada DSR berkaitan dengan pencarian rute DSR yang berdasarkan *Source Routing* membuat DSR memiliki *delay* yang lebih lama dibandingkan dengan protokol AODV. Meski begitu, DSR masih dikategorikan dalam kategori sangat baik menurut standar *delay* pada TIPHON.

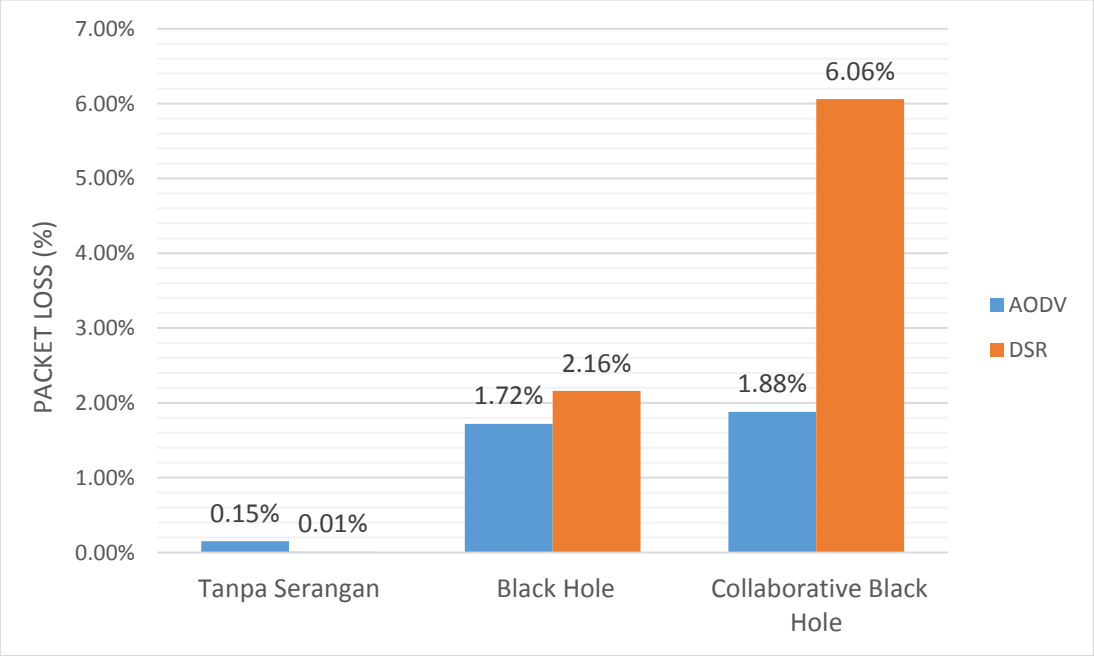
Ketika Jaringan MANET diberikan *single black hole* dan *collaborative black hole*, kedua protokol *routing* memberikan respon yang hampir sama, yaitu ketika penyerangan oleh *node black hole* terjadi, kinerja dari jaringan menjadi tidak stabil. Khususnya pada parameter *delay* menjadi tidak menentu. Hal ini dikarenakan oleh *black hole node* yang mencoba untuk menahan paket pada waktu tertentu lalu melepaskannya dalam waktu tertentu juga sehingga mempengaruhi *delay* dari kedua protokol *routing* menjadi naik turun dan tidak stabil.

4.4 *Packet loss*

Data *Packet loss* yang dihasilkan oleh keluaran simulator ditunjukkan pada Tabel 4.3 dan Gambar 4.3 yang terlampir.

Tabel 4.3 Nilai rata-rata *Packet loss (%)*

Routing protocol	**Tanpa Serangan**	***Black hole***	***Collaborative Black hole***
AODV	0.15%	1.72%	1.88%
DSR	0.01%	2.16%	6.06%



Gambar 4.3 Grafik Keluaran *Packet loss (%)*

Kedua *routing* protokol yaitu AODV maupun DSR pada saat dilakukan percobaan tanpa serangan keduanya mengalami *packet loss* yang sangat kecil. Namun pada saat protokol AODV dan DSR diberi serangan *single black hole* ataupun *collaborative black hole*, *packet loss* muncul pada kedua protokol tersebut. *Packet loss* pada protokol AODV mengalami kenaikan yang masih terbilang cukup kecil, yaitu ketika *single black hole* terjadi muncul *loss* sekitar 1,72%. Pada saat *collaborative black hole* terjadi, *loss* pada AODV terjadi peningkatan yang masih sangat kecil, yaitu nilainya naik menjadi 1,88%.

Nilai kenaikan yang terjadi pada AODV relatif kecil dibandingkan dengan *packet loss* yang terjadi pada jaringan diprotokol *routing* DSR. Pada DSR, *loss* mengalami kenaikan yang cukup signifikan yaitu saat *single black hole, loss* yang muncul sebanyak 2,16%. Pada saat *Collaborative black hole* terjadi *loss* mengalami kenaikan yang drastis ke 6,06%. Angka *packet loss* pada DSR ini cukup besar dibandingkan dengan *loss* yang terjadi pada protokol AODV. Meskipun AODV dan DSR mengalami *packet loss*, namun *packet loss* yang terjadi pada kedua protokol masih dikategorikan ke dalam kategori bagus. *Packet loss* yang terjadi pada kedua protokol ini diakibatkan oleh sifat dari *black hole node* yang menahan paket dan lalu membuangnya pada saat jaringan sedang aktif.

DSR mengalami penurunan yang cukup banyak dibandingkan dengan AODV karena mekanisme pencarian rute berdasarkan *node* sumber yang membuat DSR mengalami lebih banyak *packet loss* pada saat *black hole* terjadi. Mekanisme *source routing* yang dimiliki oleh DSR ini tidak efektif untuk menghadapi serangan *black hole* pada jaringan MANET.

4.5 Hasil Keseluruhan

Tabel 4.4 Hasil Keseluruhan

Parameter	Tanpa Serangan		*Black Hole*		*Collaborative Black Hole*	
	AODV	DSR	AODV	DSR	AODV	DSR
Throughput (kbit/s)	216,146	73,423	207,332	70,180	197,909	64,755
Delay (ms)	0.719	2.246	0.623	3.072	0.718	2.521
Packet Loss (%)	0.15%	0.01%	1.72%	2.16%	1.88%	6.06%

Dari hasil rekap keseluruhan penelitian pada Tabel 4.4, dapat dilihat bahwa kinerja pada *routing protocol* AODV lebih baik dibandingkan dengan protokol DSR dari beberapa aspek penelitian. Hal ini membuat AODV lebih dapat dipertimbangkan untuk pemilihan *routing protocol* untuk diimplementasikan pada jaringan MANET. Khususnya pada saat jaringan MANET terkena serangan *black hole*. AODV terbukti dapat lebih meminimalkan dampak dari serangan *black hole* pada jaringan MANET.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian yang sudah dilakukan, dapat diambil beberapa kesimpulan :

1. Pada parameter uji coba *throughput*, AODV mempunyai kinerja yang lebih baik dibandingkan dengan DSR. Terutama pada saat jaringan MANET terkena serangan *black hole*. AODV hanya mengalami penurunan sebesar 4,25% hingga 9.21%, sedangkan untuk DSR penurunannya mencapai 4,62% dan 13,38%
2. Untuk parameter *delay*, AODV lebih baik dari DSR karena memiliki waktu *delay* yang kecil yaitu 0,000719305 *second* dibandingkan dengan DSR. Namun ketika tekena serangan *black hole*, keduanya menunjukkan kinerja yang sama.
3. Pada parameter *Packet loss*, AODV juga lebih baik dari DSR. Hal ini ditunjukkan dari nilai persen DSR yang mengalami kenaikan yang cukup banyak dibandingkan dengan AODV ketika terkena *single* ataupun *collaborative black hole*.
4. Protokol *routing* AODV lebih baik daripada protokol DSR dari beberapa aspek penelitian. Terutama pada jaringan yang terkena *black hole*. Keduanya mengalami beberapa penurunan kinerja, namun AODV menunjukkan penurunan yang masih bisa diterima.

5.2 Saran

1. Melakukan perbandingan protokol lain selain protokol reaktif terhadap serangan *black hole* pada MANET.
2. Menguji coba atau mensimulasikan serangan *black hole* terhadap jaringan lain selain jaringan MANET, seperti *Wireless Mesh Network*, *Wireless Sensor Network* dan lainnya.
3. Melakukan penelitian tentang serangan lain yang memiliki kesamaan pada serangan *black hole* terhadap protokol atau jaringan MANET, seperti *gray hole*, *worm hole* dan serangan lainnya.

DAFTAR PUSTAKA

[1] Y. Sidharta and D. Widjaja, "Perbandingan Unjuk Kerja Protokol Routing Ad Hoc On-Demand Distance Vector (AODV) Dan Dynamic Source Routing (DSR) Pada Jaringan MANET," *J. Teknol.*, vol. 6, no. 274, pp. 83–89, 2013.

[2] 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.

[3] S. D. Anggraini, K. Nugroho, and E. F. Cahyadi, "Analisis Perbandingan Performasi Protokol Routing AODV Dan DSR Pada Mobile Ad-Hoc Network (MANET)," *2nd Semin. Nas. IPTEk Terap.*, pp. 112–118, 2017.

[4] Y. Dhamayanti, "Analisis Perbandingan Kinerja Protokol Dynamic Source Routing dan Ad hoc On-demand Distance Vector pada Mobile Ad Hoc Network untuk Sistem Komunikasi Taktis Kapal Perang," *J. Ilm. Elit. Elektro*, vol. 4, no. 1, pp. 5–10, 2013.

[5] 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.

[6] A. Kumar B R, L. C. Reddy, and P. S. Hiremath, "Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols," *Eur. J. Sci. Res.*, vol. 8, no. 6, pp. 337–343, 2008.

[7] S. Lalar and A. K. Yadav, "Comparative Study of Routing Protocols in MANET," *Orient. J. Comput. Sci. Technol.*, vol. 10, no. 1, pp. 174–179, 2017.

[8] S. Puri and V. Arora, "Performance of MANET : A Review," vol. 9, no. 11, pp. 544–549, 2014.

[9] Usha and Bose, "Comparing the impact of black hole and gray hole attacks in mobile adhoc networks," *J. Comput. Sci.*, vol. 8, no. 11, pp. 1788–1802, 2012.

[10] C. Lohi, "A Survey of Mitigation Techniques to Black Hole Attack and Gray Hole Attack in MANET," vol. 5, no. April, pp. 560–566, 2014.

[11] M. Medadian, K. Fardad, and A. Mebadi, "Proposing a Method to Remove Gray Hole Attack in AODV Protocol in MANET," vol. 2, no. 6, pp. 512–518, 2013.

[12] I. Hyder, S. Malek, and F. Duani, "Modeling and Simulation Of Dynamic Intermediate Nodes And Performance Analysis in MANETS Reactive Routing protocols," vol. 4, no. 1,

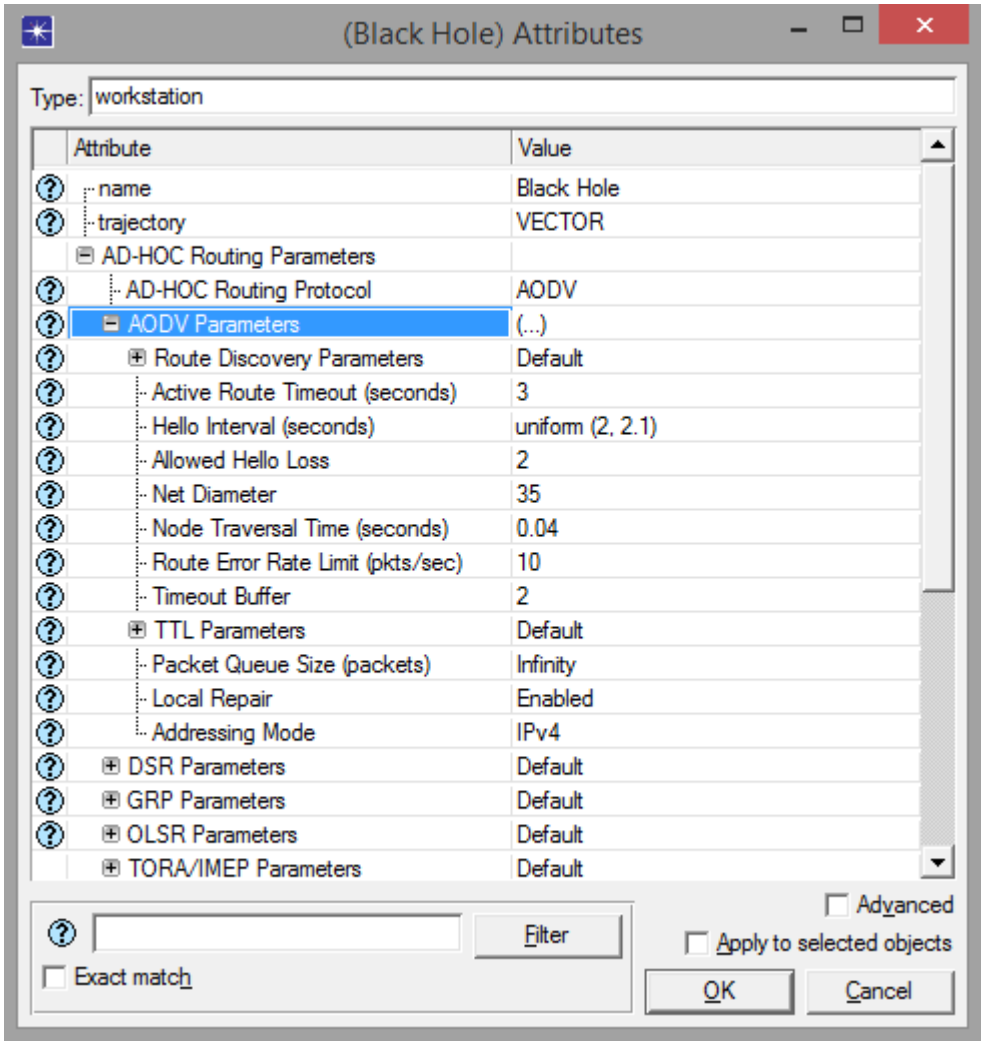
pp. 31–56, 2011.

[13] 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*, vol. 1, no. 1, p. 12, 2015.

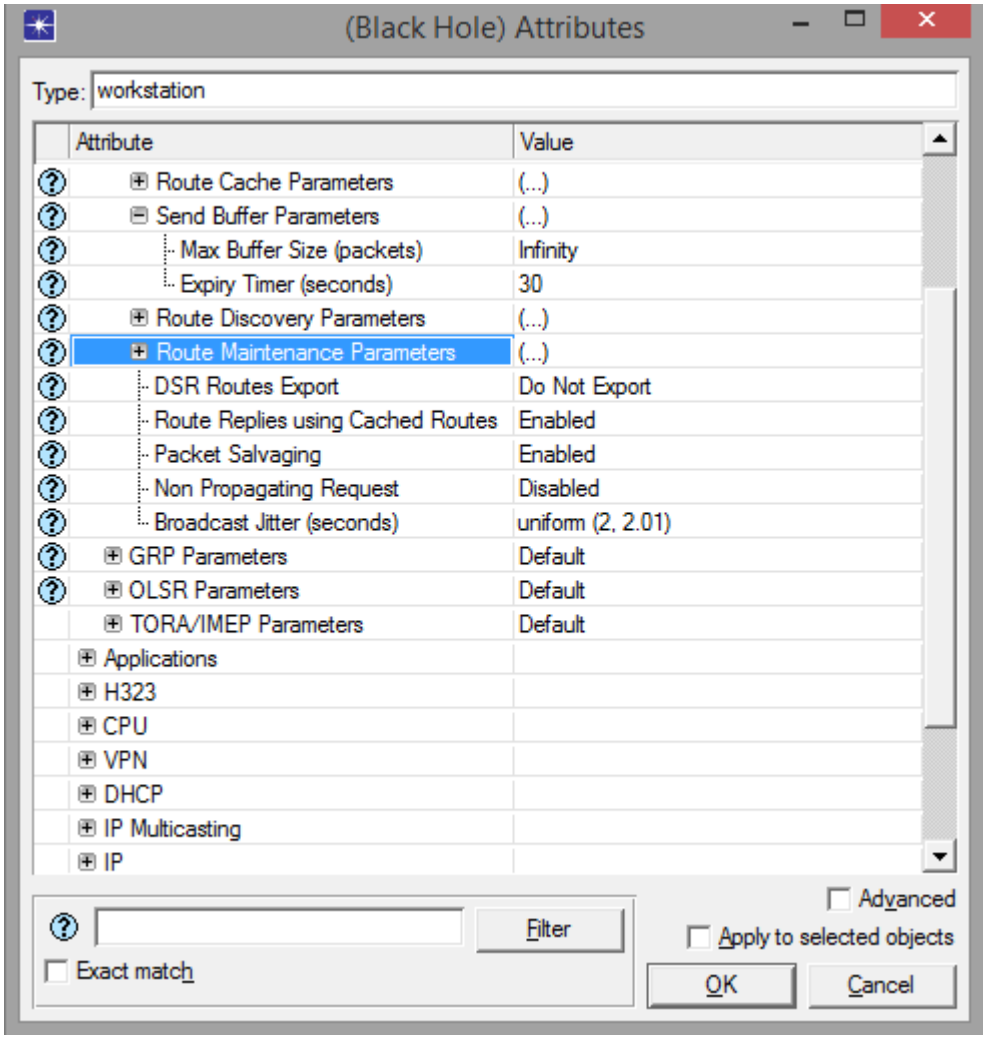
[14] ETSI, “Telecommunication and Internet Protocol Harmonization Over Network (TIPHON); General Aspects of Quality of Service (Qos),” *Etsi*, vol. 2.1.1, pp. 1–37, 1999.

LAMPIRAN

1. Setting Black Hole AODV



2. Setting Black Hole DSR



3. Setting parameter WLAN