SIMULASI DAN ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV (*AD-HOC ON DEMAND DISTANCE VECTOR*) DAN OLSR (*OPTIMIZED LINK STATE ROUTING)* TERHADAP SERANGAN *WORMHOLE* PADA JARINGAN MANET

SKRIPSI

untuk memenuhi salah satu persyaratan

mencapai derajat Sarjana S1

Disusun oleh:

MUHAMMAD RAMADHAN

14524022

Jurusan Teknik Elektro

Fakultas Teknologi Industri

Universitas Islam Indonesia

Yogyakarta

2018

LEMBAR PENGESAHAN

SIMULASI DAN ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV (*AD-HOC ON DEMAND DISTANCE VECTOR*) DAN OLSR (*OPTIMIZED LINK STATE ROUTING*) TERHADAP SERANGAN *WORMHOLE* 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:

Muhammad Ramadhan
14524022

Yogyakarta, 16 Agustus 2018

Menyetujui,

Pembimbing 1

Ida Nurcahyani, ST., M.Eng.
155240104

LEMBAR PENGESAHAN

SIMULASI DAN ANALISIS PERBANDINGAN KINERJA *ROUTING PROTOCOL* AODV (*AD-HOC ON DEMAND DISTANCE VECTOR*) DAN OLSR (*OPTIMIZED LINK STATE ROUTING*) TERHADAP SERANGAN *WORMHOLE* PADA JARINGAN MANET

Dipersiapkan dan disusun oleh:

Muhammad Ramadhan

14524022

Telah dipertahankan di depan dewan penguji

Pada tanggal: 23 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: Elvira Wahyuni, S.Pd.T.,M.Eng _____

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

Tanggal: 23 Agustus 2018

Ketua Program Studi Teknik Elektro

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

Muhammad Ramadhan

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah subhanahu wa ta'ala yang telah memberikan rahmat serta karunia-Nya 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 Shallallahu 'alaihi Wa Sallam. Didalam pekerjaan skripsi ini banyak 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 Syarifuddin dan Ibu Soeharti,** yang selalu mendoa'kan dan mendukung penulis tehadap 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 ahir ini.
3. **Bapak Dr. Eng. Hendra Setiawan, ST., M.Eng**. Selaku Ketua Jurusan Teknik Elektro, Fakultas Teknologi Industri, Universitas Islam Indonesia.
4. **Keluarga** penulis yang sudah memberikan dukungan terkait proses pengerjaan skripsi hingga akhir.
5. **Teman-teman Kontrakan, MTA, Angkatan 2014 Jurusan Teknik Elektro** dan **PASTEL 14 UII** karena telah menemani dan mendukung kegiatan kuliah dari awal.

Yogyakarta, 16 Agustus 2018

Muhammad Ramadhan

ARTI LAMBANG DAN SINGKATAN

AODV	:	*Ad-Hoc On Demand Distance Vector*
MANET	:	*Mobile Ad-hoc Network*
OLSR	:	*Optimized Link State Routing*
QoS	:	*Quality of Service*
DSR	:	*Dynamic Source Routing*
GRP	:	*Geographic Routing Protocol*
DSDV	:	*Destination-Squenced Distance Vector*
RREQ	:	*Route Request*
RREP	:	*Route Repley*
RRER	:	*Route Error*
MPR	:	*Multi Point Relay*
TC	:	*Topology Control*
FTP	:	*File Transfer Protocol*
LAN	:	*Local Area Network*
IEEE	:	*Institute of Electrical and Electronics Engineers*
TIPHON	:	*Telecommunications and Internet Protocol Harmonization Over Networks*
m	:	*Meter*
ms	:	*Milisecond*
Mbps	:	*Megabit per second*
GHz	:	*Gigahertz*

ABSTRAK

MANET (*Mobile Ad Hoc Network*) merupakan jaringan yang teridiri atas kumpulan *node* dan sifatnya dinamis, karena setiap *node* bergerak secara bebas. Jaringan ini biasa digunakan saat kondisi darurat seperti bencana alam, militer, dan lain-lain. Selain itu, MANET juga dapat dibuat dengan mudah tanpa menggunakan infrastruktur jaringan yang tetap seperti *base station,* sehingga MANET menjadi rentan terkena serangan. Salah satu serangan yang mungkin terjadi adalah *wormhole attack*. Serangan *wormhole* merupakan serangan yang sangat jahat dapat merusak jaringan MANET efeknya dapat merubah topologi jaringan, dapat merubah aliran pesan yang normal, dan menyebabkan salah dalam pengiriman informasi routing. Pemilihan *routing protocol* yang tepat dapat meminimalkan dampak dari serangan *wormhole*. Penelitian ini dibuat untuk membandingkan manakah yang lebih baik kinerjanya diantara *routing protocol* AODV dan OLSR dalam meminimalkan dampak dari serangan *wormhole*. Hasil dari penelitian ini menunjukan bahwa OLSR lebih baik kinerjanya dibandingkan dengan AODV dari beberapa nilai QoS seperti *throughput*, *delay*, dan *packet loss*. Pada nilai *throughput*, ketika terkena serangan *wormhole* AODV mengalami penurunan sebesar 25,1%, sedangkan OLSR mengalami penurunan sebesar 9%. Untuk nilai *delay*, OLSR lebih baik dibandingkan dengan AODV, namun ketika terkena serangan *wormhole,* AODV dan OLSR mengalami kenaikan sebesar 7,1% dan 2,5%. Untuk *packet loss*, OLSR lebih baik kinerjanya dibandingkan dengan AODV karena paket yang terbuang lebih kecil pada saat jaringan MANET terkena serangan *wormhole*. Dimana AODV nilainya sebesar 2880% dan OLSR 659%. Dari kesuluruhan penelitian ini, hasil yang diperoleh memperlihatkan bahwa protokol OLSR memberikan nilai QoS yang lebih baik pada saat jaringan tidak terkena serangan maupun pada saat terkena serangan *wormhole*.

Kata Kunci : MANET, AODV, OLSR, *Wormhole Attack*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi nirkabel yang sangatlah pesat dapat memenuhi kebutuhan masyarakat akan akses informasi yang *real time*, dapat diandalkan, dan fleksibel [1]. Dengan melakukan transformasi pada sistem transmisi, muncullah teknologi baru yang bisa disebut dengan MANET (*Mobile Ad hoc Network*). MANET tidak memiliki *base station* untuk mengirimkan paket data sehingga mudah untuk diaplikasikan. Jaringan ini biasa digunakan saat kondisi darurat seperti bencana alam, militer, dan lain-lain [2].

Kehadiran MANET sendiri merupakan sebuah jaringan nirkabel yang menghubungkan *node* satu ke *node* lainnya dan bersifat hanya sementara sehingga dapat dikatakan tidak tetap. Adanya pergerakan pada *node* yang membuat jaringan menjadi rentan terhadap serangan. Serangan yang mungkin terjadi adalah *wormhole attack*. Serangan ini dapat merusak jaringan pada MANET dimana pada umumnya ada dua penyerang yang saling terhubung dengan kecepatan tinggi [3].

Routing protokol merupakan pengaturan *node* untuk meneruskan paket dari *node* satu ke *node* lainnya. Pada jaringan MANET setiap *node* bersifat sebagai *router* yang berfungsi menentukan pencarian *rute* tersingkat untuk mengirimkan paket data yang akan dituju, sehingga pada jaringan MANET dibutuhkan *routing protocol* yang tepat untuk membantu *node* mengirimkan paket data secara cepat dan efisien [1].

Pada jaringan MANET ada beberapa macam *routing protocol* yaitu reaktif, proaktif, dan *hybrid*. Protokol yang akan dibahas adalah protokol *proaktive* dan protokol *reactive*. Protokol proaktif berfungsi *meng-update rute* secara berkala, sedangkan protokol reaktif berfungsi untuk mencari *rute* apabila ada permintaan. Ada beberapa protokol dari kelas reaktif dan proaktif, salah satunya adalah AODV dan OLSR. AODV dan OLSR dipilih, karena kinerja keduanya yang terbaik dikelasnya [4]. Cara kerja protokol AODV memperbolehkan *node* melewatkan *node* lainnya ke *node* tujuan, sedangkan protokol OLSR bekerja dengan cara *update routing table*.

Wormhole attack merupakan serangan yang sangat jahat pada jaringan MANET dimana ada dua penyerang yang saling terhubung dengan kecepatan tinggi [5]. Efek serangan *wormhole* adalah dapat merubah topologi jaringan, dapat merubah aliran pesan yang normal, dan menyebabkan salah dalam pengiriman informasi *routing* [6]. Serangan *wormhole* dapat

dilakukan dengan satu *node*, tetapi pada umumnya dilakukan untuk dua atau lebih penyerang [7].

Penelitian ini menginvestigasi dampak dari serangan *wormhole* terhadap kinerja *routing protocol* AODV dan OLSR pada jaringan MANET. Analisis dilakukan untuk melihat efek serangan *wormhole* terhadap nilai QoS pada parameter *throughput*, *delay*, dan *packet loss*. Dengan penelitian ini, diharapkan dapat diketahui jenis *routing protocol* mana yang lebih tahan terhadap serangan *wormhole*.

1.2 Rumusan Masalah

Perumusan masalah pada penelitian ini adalah :

1. Bagaimana kinerja protocol AODV dan OLSR pada saat sebelum dan sesudah serangan *wormhole* pada jaringan MANET ?
2. Bagaimana dampak serangan *wormhole* bagi *routing protocol* AODV dan OLSR pada jaringan MANET ?
3. Manakah yang lebih baik kinerjanya diantara *routing protocol* AODV dan OLSR saat sebelum dan sesudah terkena serangan *wormhole* ?

1.3 Batasan Masalah

Adapun dalam penelitian ini batasan masalah pada tugas akhir ini adalah:

1. Penelitian ini menggunakan OPNET MODELER 14.5 untuk simulasinya.
2. Penelitian ini hanya berfokus pada analisis perbandingan kinerja *routing protocol* AODV dan OLSR dengan dan tanpa serangan *wormhole.*
3. Parameter QOS yang dianalsis adalah *packet loss*, *delay*, dan *throughput*.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Mengetahui bagaimana kinerja protocol AODV dan OLSR saat sebelum dan sesudah terkena *wormhole attack* pada jaringan MANET.
2. Mengetahui dampak serangan *wormhole* bagi *routing protocol* AODV dan OLSR pada jaringan MANET.
3. Mencari yang lebih baik kinerjanya antar *routing protocol* AODV dan OLSR saat sebelum dan sesudah terkena serangan *wormhole.*

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah :

1. Memberikan informasi tentang protokol mana yang lebih baik kinerjanya khususnya terhadap *routing protocol* yang diteliti.
2. Membuat rancangan jaringan yang dapat dijadikan referensi saat akan dikembangkan dalam infrastruktur jaringan yang sebenarnya.
3. Memberikan data informasi kepada peniliti lain untuk mengembangkan serta memperbaiki sistem pada jaringan MANET.

BAB 2
TINJAUAN PUSTAKA

2.1 Studi Literatur

Penelitian dari Wahyu Edy Seputra, Sukiswo, dan Ajub Ajulian Zahra melakukan perbandingan kinerja protokol AODV dengan OLSR pada MANET [4]. Perbandingan ini menggunakan *software* OPNET MODELER 14.5. Penelitian ini dibagi menjadi 4 skenario, skenario pertama AODV dengan jumlah node 50, kedua OLSR dengan jumlah node 50, ketiga AODV dengan jumlah node 100, dan Keempat OLSR dengan jumlah node 100. Skenario yang dirancang luas areanya 2000 m x 2000 m. Parameter yang digunakan adalah *throughput*, *delay*, *load*, dan *packet delivery ratio.* Pada parameter *delay* OLSR lebih rendah daripada AODV. Selisih yang didapat dari node 50 masing-masing routing yaitu 0,256 detik dan pada node 100 selisihnya sebesar 0,852 detik. Pada *load* dan *throughput* OLSR lebih besar daripada AODV, sedangkan pada parameter *Packet delivery ratio* OLSR memiliki nilai terbaik dari semua skenario, karena OSLR bersifat proaktif sedangkan AODV bersifat reaktif. Bahwa kesimpulan dari penelitian ini adalah OLSR memiliki kinerja terbaik dibandingkan AODV dari semua skenario.

Selanjutnya penelitian dari Fitri Amillia, Marzuki, dan Agustina melakukan analisis perbandingan kinerja protokol DSR dan GRP pada MANET [8]. Penelitian ini menggunakan *software* OPNET MODELER 14.0. Subjek menggunakan dua buah skenario yaitu skenario yang pertama menggunakan 25 *node* dan kedua 50 *node.* Skenario yang dirancang luas areanya 3000 m x 3000 m, parameter yang digunakan adalah *throughput*, *delay*, *load*, *media access delay*, *data dropped*, dan *network load*. Protokol GRP nilai *throughput* lebih besar daripada DSR, untuk *delay* lebih rendah GRP daripada DSR semakin rendah *delay* semakin bagus hasilnya, untuk *load* protokol DSR lebih baik kinerjanya dibandingkan dengan GRP, untuk *media access load* protokol lebih besar dibandingakan dengan GRP, untuk *data dropped* protokol GRP lebih baik kinerjanya dibandingakan dengan DSR, sedangkan untuk *network load* protokol DSR lebih besar daripada GRP. Bahwa kesimpulan dari penelitian ini adalah hasil dari simulasi protokol GRP dan DSR, lebih baik GRP dibandingakn dengan DSR.

Debora Valentina Silaban, Sofia Naning Hertiana, Asep Mualana melakukan simulasi dan analisis perbandingan kinerja pada jaringan MANET untuk aplikasi video menggunakan routing protocol AODV dan OLSR [9]. Penelitian ini menggunakan *software NS-2* dan *Evalvid.* Pada kedua protocol tersebut, parameter yang dianalisis adalah *delay and to end, delay jitter, throughput, packet loss* dan *PSNR.* Dengan skenario menambahkan *node* dan pengaruh perpindahan keccepatan *node* pada dua video yang disimulasikan secara terpisah. Protocol AODV

nilai *delay and to end* 49 ms dibandingkan dengan OLSR sebesar 70 ms lebih baik AODV, untuk *delay jitter* AODV lebih baik daripada OLSR, untuk throughput AODV lebih baik daripada OLSR. Dari keseluruhan parameter yang dianalisis dapat diambil kesimpulan bahwa routing protocol AODV lebih bagus dibandingkan dengan routing protocol OLSR.

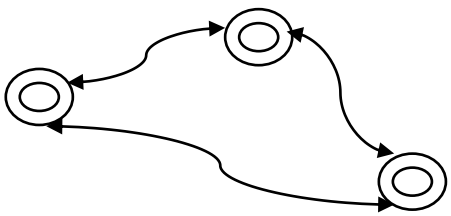
H.Ghayvat, S.Pandya, S.V.Shah, & M.H.Yap melakukan penelitian pendekatan AODV tidak lanjut untuk deteksi efisien dan mitigasi serangan *wormhole* di MANET [10]. Penelitian ini menggunakan software NS-2.35. Skenario yang digunakan 25 *node* dengan luas area sebesar 1000 m x 1000 m. Parameter yang digunakan adalah *end-to-end delay, PDR,* dan *throughput*. Dimana pada penelitian ini peneliti meningkatkan *lifetime, throughput,* dan meminimalkan penundaan jaringan dari jaringan seluler dibandingkan sistem yang ada. Dapat disimpulkan dari penelitian ini adalah hanya meningkatkan dan meminimalkan penundaan pada jaringan.

Pada studi literatur, dapat dijelaskan dari beberapa penelitian para penulis mengklaim routing protocol AODV dan OLSR sama-sama memiliki kelebihan dan kekurangan. Pada penelitian AODV dan OLSR pernah dilakukan bahwa OLSR lebih baik daripada AODV menggunakan beberapa parameter QoS untuk menilai. Namun pada jaringan lain, protokol AODV mengalami penurunan apabila terkena serangan *wormhole*. Oleh sebab ini peneliti mencoba melakukan penelitian tentang dampak dari *wormhole attack* terhadap *routing protocol* yang ada pada jaringan MANET.

2.2 Tinjauan Teori

2.2.1 *Mobile Ad-Hoc Network* (MANET)

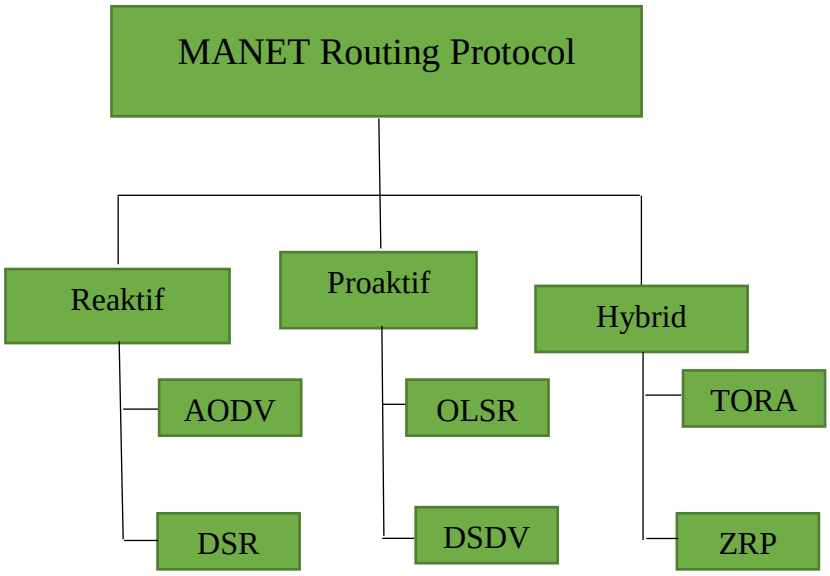
MANET merupakan sebuah jaringan nirkabel yang dibentuk dari banyak *node* yang tidak memiliki *router* tetap [11]. *Node* berfungsi juga sebagai *router* yang dapat berkontribusi dalam memberikan informasi ke setiap *node* pada jaringan. Topologi jaringan yang bersifat dinamis dapat berubah ubah sesuai perpindahan posisi dalam jaringan yang akan digunakan untuk mengirimkan pesan ke *node* tujuan. Oleh karena itu, *node* pada jaringan MANET dapat berfungsi maksimal harus diberikan *routing* agar *node* dapat menjalankan proses pencarian *rute* dan data bisa efisien dan dinamis. Gambar 2.1 Menunjukkan jaringan MANET.



Gambar 2.1 Jaringan MANET

2.2.2 Klasifikasi *Routing Protocol Pada MANET*

Klasifikasi routing protocol yang digunakan ada 3 yaitu reaktif, proaktif, dan *hybrid.* Dimana *routing protocol* merupakan pengaturan *node* untuk pencarian *rute* tersingkat untuk mengirimkan paket data menuju alamat yang dituju. Pada penelitian ini, protokol yang digunakan untuk perbandingan adalah protokol reaktif dan proaktif, yaitu AODV dan OLSR. Gambar 2.2. Pada MANET memperlihatkan klasifikasi *routing protocol.*



Gambar 2.2 Klasifikasi *Routing Protocol*

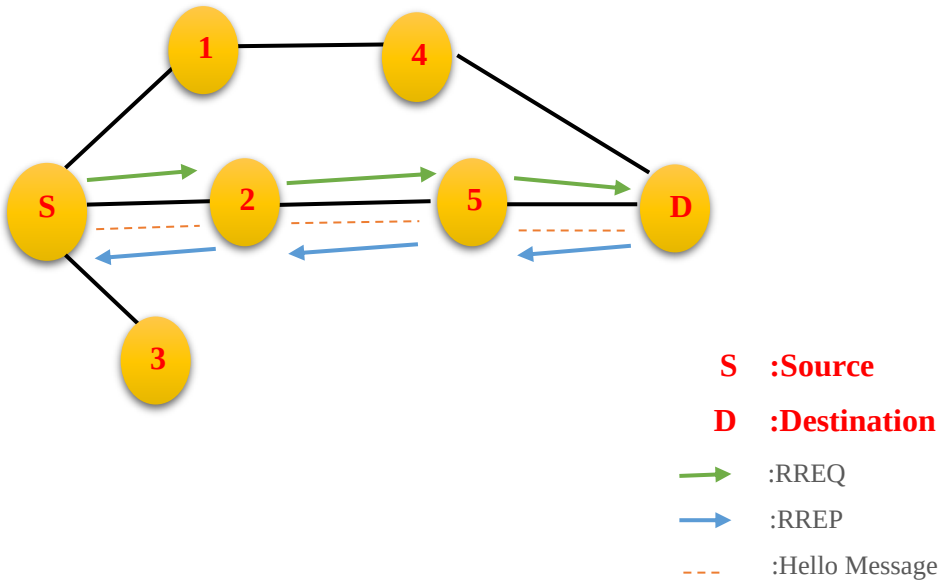
Routing protocol reaktif merupakan *routing* yang berfungsi untuk membentuk rute jika suatu saat n*ode* meminta dibuatkan rute untuk pengiriman pesan, contoh protokol reaktif yaitu AODV, DSR, dll. Sedangkan *routing protocol* proaktif merupakan *routing* yang berfungsi *meng-update* secara berkala, contoh protokol proaktif yaitu OLSR, DSDV, dll [12]. Sedangkan untuk protokol *hybrid,* cara kerjanya adalah dengan menggabungkan keuntungan antara kelas reaktif dan proaktif. Pada penelitian ini yang digunakan adalah protokol AODV dan OLSR. Karena pada kelas reaktif AODV lebih baik kinerjanya, sedangkan pada kelas proaktif OLSR lebih baik kinerjanya.

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

Ad-Hoc on Demand Distance Vector (AODV) adalah sebagian protokol *routing* yang bersifat reaktif. Protokol AODV, *rute* dari *node* satu ke *node* lain akan dibuat jika *source node* menginginkan adanya permintaan pengiriman paket ke *node* tujuan yang dipilih. Untuk menemukan jalur yang terbaik bagi *source node*, protokol *routing* AODV akan melakukan *Route discovery* dengan menyebarkan *Route Request* (RREQ) ke semua *node* yang bertetanggan dengan

node sumber. Setelah itu n*ode* tetangga mengirimkan RREQ ke *node* tetangga lagi hingga berakhir di *node* tujuan. *Node* tujuan akan membalas pesan RREQ dengan *Route Reply* (RREP) [13].

Cara kerja AODV adalah pada saat ada permintaan dari *source node* untuk mencari tahu jalur-jalur yang digunakan untuk mengirimkan pesan ke *node* tujuan. Selain itu AODV juga dapat mencegah terjadinya *routing loop* dan topologinya dinamis. *Routing loop* artinya adalah kondisi saat sebuah paket ditransmisikan dalam *route* tidak pernah sampai tujuan. Jalur yang dipilih yaitu jalur yang terpendek lebih rendah dari jalur lainnya. Dalam protokol AODV menggunakan nilai *squence number* dalam membangun *rute*. Sehingga dapat dipastikan bahwa jalur yang dihasilkan pada saat proses *route discovery* merupakan jalur yang bebas dari *looping* dan jalur yang paling *update*. Proses pencarian rute AODV dapat dilihat pada Gambar 2.3.



Gambar 2.3 Proses Pencarian *rute* AODV

Jika rute sudah terbentuk, maka yang bertanggung jawab dalam menjaga *rute* adalah *node* sumber. AODV mengirimkan pesan HELLO secara berkala. Apabila selama proses pengiriman pesan terjadi kerusakan yang menyebabkan *rute* menuju *node* tujuan terputus, maka suatu *node* akan mengirimkan *Route Error* (RRER) ke *node* tetangga hingga sampai ke *source node*. Routing protokol AODV memiliki kelebihan dan kekurangan yang ditampilkan pada Tabel 2.1.

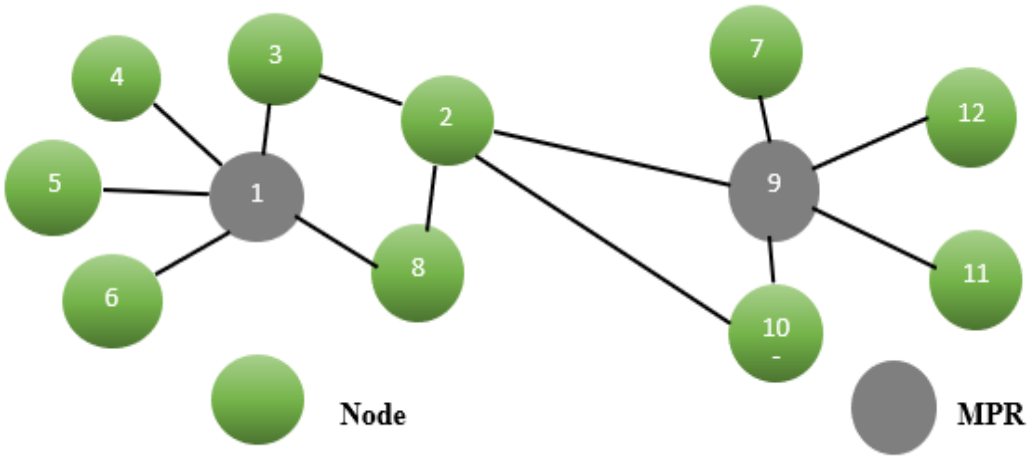
Tabel 2.1 Kelebihan dan Kekurangan AODV [13].

KELEBIHAN	KEKURANGAN
1. Bebas *loop* dan topologi dinamis 2. Rute yang diperoleh sesuai tujuan 3. Effisiensi dalam menggunakan *bandwidth* memiliki *overhead* yang kecil	1. Pencarian rute yang cukup lama 2. Memiliki ukuran *routing* tabel yang besar

2.2.4 *Optimized Link State Routing (OLSR)*

Optimized Link State Routing (OLSR) merupakan protokol *routing* yang bersifat *proaktif.* Keunggulan OLSR dapat menemukan jalur di antara dua *node* yang berada di dalam jaringan dengan waktu yang sangat singkat. Hal ini dikarenakan pola *proaktif,* namun OLSR juga dapat menghabiskan sumber daya dalam proses pemilihan *node Multi Point Relay* (MPR) [14]. MPR merupakan *node* yang dipilih oleh satu *node* dengan spesifikasi tertentu.

OLSR menggunakan 2 jenis pesan kontrol, yaitu pesan *hello* dan *Topology Control* (TC). Fungsi pesan *hello* adalah untuk menemukan informasi tentang kondisi *link* dan *node* tetangga. Selain itu pesan *hello* juga digunakan untuk memilih *multi point relay* (MPR) *selector set.* MPR *Selector set* ditugaskan untuk memilih *node* tetangga bertindak sebagai *node* MPR. Pesan *hello* hanya mengirimkan sejauh 1 *hop,* sedangkan pesan TC dikirim secara *broadcast* ke seluruh jaringan. Pesan TC kegunaannya adalah menyebarkan informasi tentang *node* tetangga yang ditetapkan oleh MPR tidak terkecuali MPR *selector,* pesan TC disebarkan secara periodik [4]. Gambar 2.4 memperlihatkan *packet transmission using* MPR [14]. Tabel 2.2 menunjukan kelebihan dan kekurangan OLSR.



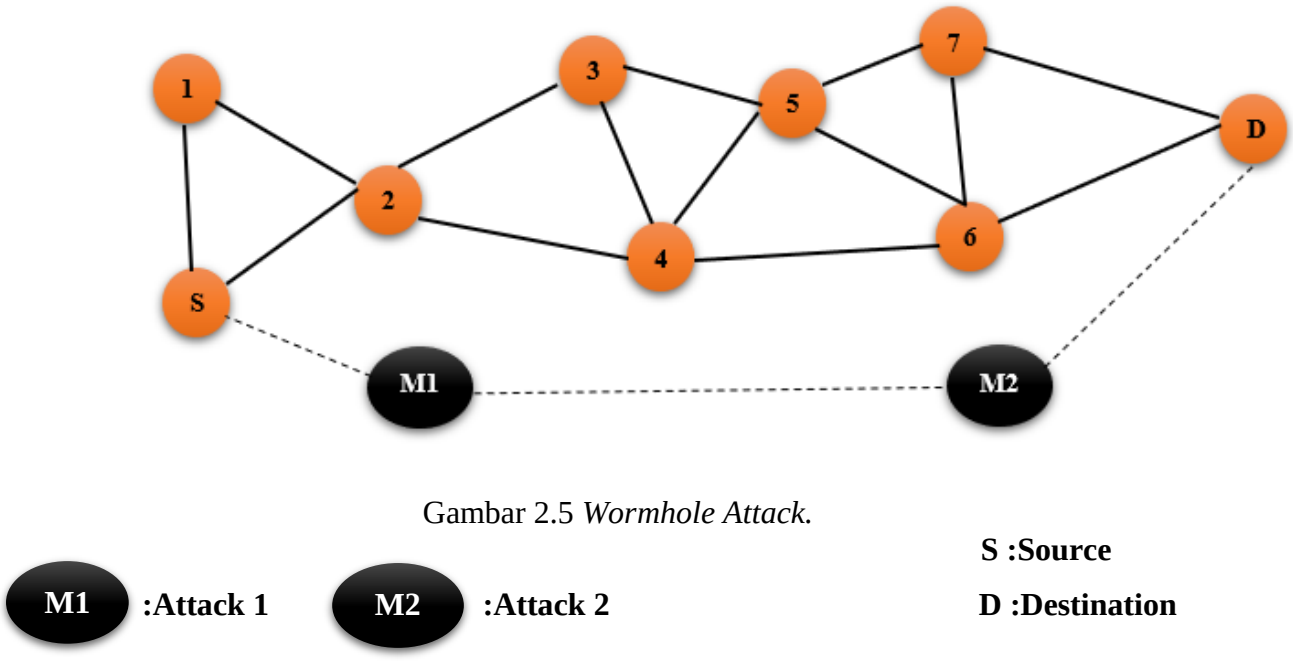
Gambar 2.4 *Packet Transmission Using* MPR.

Tabel 2.2 Kelebihan dan Kekurangan OLSR [14].

KELEBIHAN	KEKURANGAN
1. Dapat menemukan jalur diantara dua buah *node* 2. Terus *up-date* dalam waktu berkala	1. Boros dalam sumber daya dalam proses pemilihan *node* 2. Penggunaan *bandwidth* yang tinggi

2.2.5 *Wormhole Attack*

Wormhole attack adalah serangan yang sangat jahat pada jaringan MANET dimana ada dua penyerang yang saling terhubung dengan kecepatan tinggi. Serangan *wormhole* menciptakan terowongan antara dua titik di jaringan dan membuat koneksi secara langsung sehingga saling terhubung langsung [3]. Serangan ini dapat membuat kerusakan besar pada *ad-hoc network* yang telah terbentuk. Serangan *wormhole* dapat dilakukan dengan satu node, tetapi pada umumnya dilakukan untuk dua atau lebih penyerang. Efek serangan *wormhole* adalah dapat merubah topologi jaringan, dapat merubah aliran pesan yang normal, dan menyebabkan salah dalam pengiriman informasi *routing*. Berikut ini adalah bentuk dari serangan *wormhole* dapat dilihat pada Gambar 2.5 [3].



Gambar 2.5 *Wormhole Attack.*

BAB 3
METODOLOGI

3.1 Alat dan Bahan

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

3.1.1 Perangkat Keras

Perangkat keras yang digunakan adalah satu buah laptop dengan spesifikasi sebagai berikut:

1. RAM : 4GB DDR4
2. *Processor* : *Intel® Core™i3-6006U (2.0 GHz, 3MB L3 Cache)*
3. *Harddisk* : 128GB

3.1.2 Perangkat Lunak

Perangkat Lunak yang digunakan untuk melakukan simulasi adalah sebagai berikut :

1. OPNET MODELER 14.5
2. *Microsoft Excel*
3. *Microsoft Word*
4. *Operating System Microsoft Windows 10* Pro 64 bit

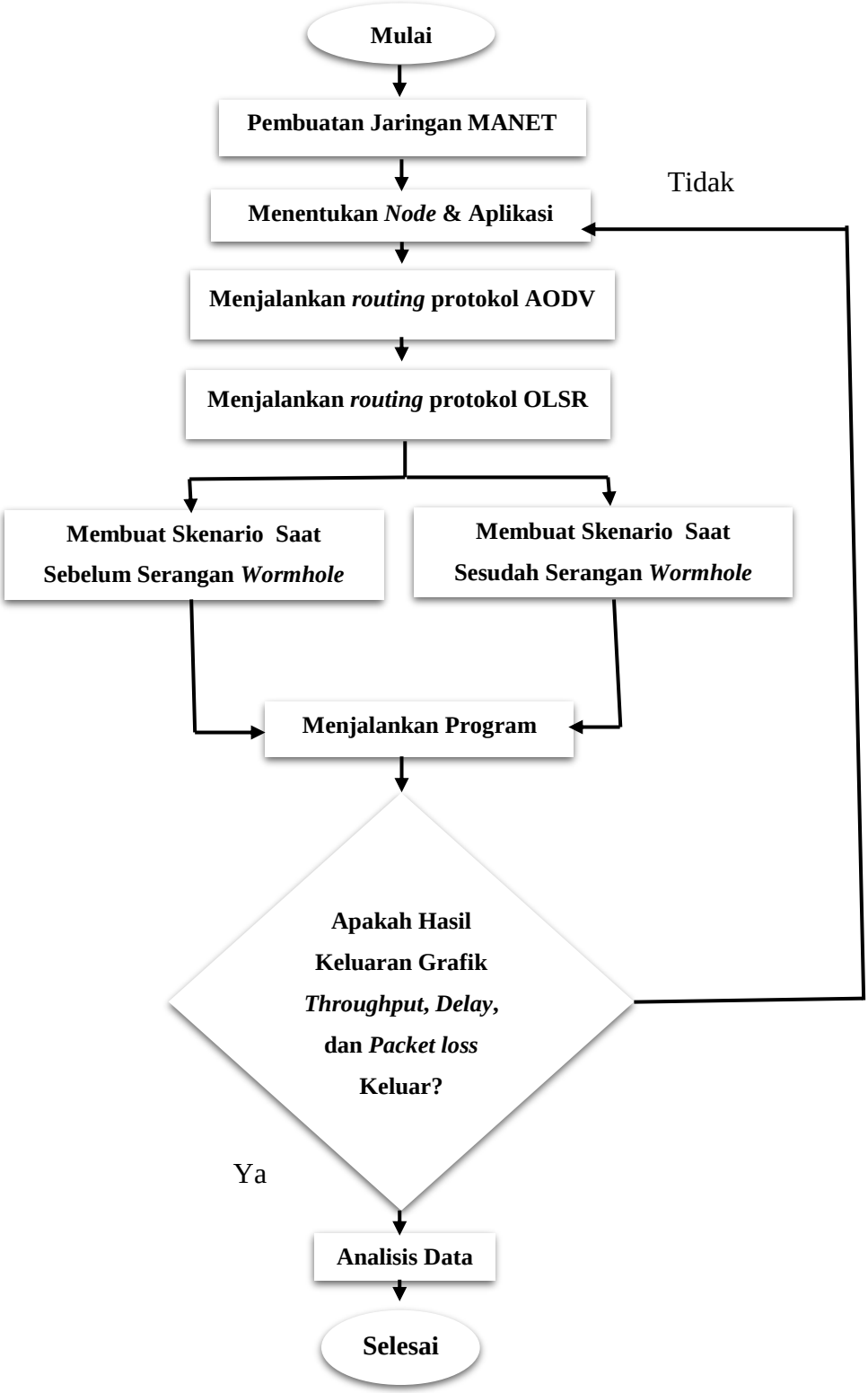
3.2 Perancangan Program

Perancangan simulasi yang dilakukan penulis ada beberapa tahapan yaitu :

1. Pembuatan jaringan MANET, yang dimana untuk menentukan *node*, server dan aplikasi yang akan digunakan pada jaringan.
2. Menentukan *node* dan aplikasi, yang dimana proses mengatur apa saja yang berpengaruh pada jaringan, adapun seperti protokol, ukuran paket, kecepatan *node*, jenis traffic yang digunakan dan pengaturan aplikasi lainnya.
3. Membuat skenario saat sebelum dan sesudah terkena serangan *wormhole* menggunakan protokol AODV dan OLSR, adapun yang dilakukan yaitu mengubah parameter dan *wireless* LAN parameter.
4. Menjalankan program agar dapat mengetahui hasil keluaran dari simulasi

5. Jika simulasi selesai dijalankan, maka akan menghasilkan keluaran berupa *throughput*, *packet loss*, dan *delay*. Jika tidak sesuai akan kembali ke menentukan *node* dan aplikasi
6. Analisis hasil yang sudah disimulasikan dan selesai.

Pada Gambar 3.1 menunjukan diagram alir perancangan program



Gambar 3.1 Diagram Alir Perancangan Program

3.3 Simulasi Skenario

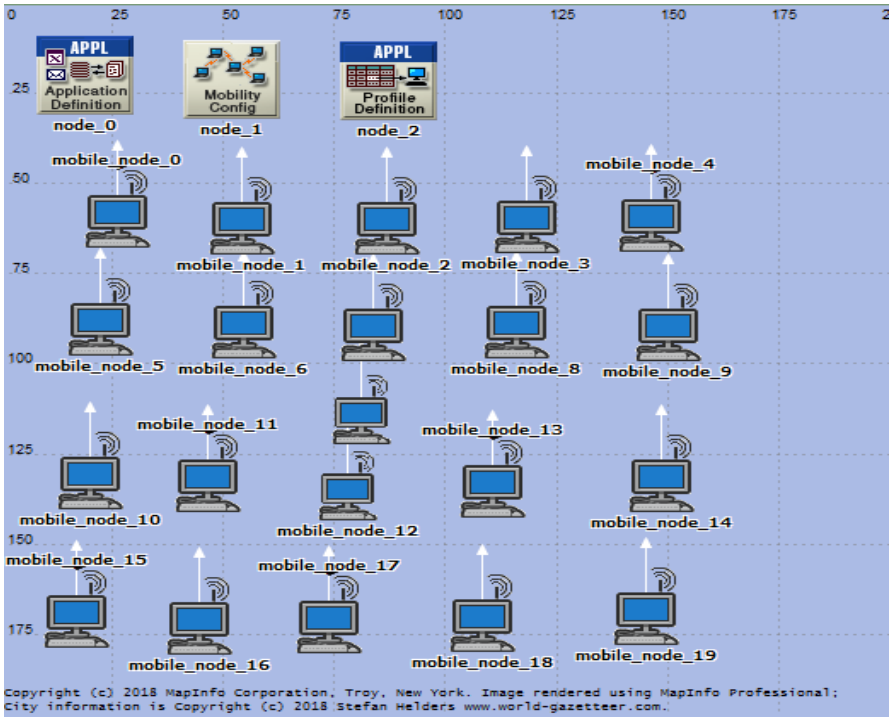
Penelitian ini memiliki beberapa skenario yang berbeda, sehingga dapat mengetahui kinerja dari masing-masing protokol. Dalam simulasi ini menggunakan *application definiton*, kegunaannya adalah menentukan aplikasi untuk parameter yang digunakan, *mobility config*, kegunaannya adalah menentukan parameter untuk berbagai model mobilitas MANET, *profile definition*, kegunaannya adalah menentukan berbagai karakteristik pemuatan untuk berbagai aplikasi, sedangkan *mobile node*, kegunaannya adalah menentukan nama simpul komunikasi seluler. Skenario yang dilakukan adalah skenario tanpa serangan, atau bisa dibilang *default* pada saat *node* tidak terkena *wormhole*. Setalah itu skenario pada saat kedua *routing protocol* terkena serangan *wormhole*. Pada simulasi ini waktu yang dibutuhkan selama 600 detik atau sekitar 10 menit untuk semua skenario. *Technology* jaringan yang digunakan adalah IEEE 802.11b, hanya memiliki kemampuan transmisi standard sebesar 11*Mbps* dengan menggunakan frekuensi 2.45 *GHz*. Aplikasi layanan yang digunakan adalah FTP dengan *type traffic* aplikasi *high load*. *High load* merupakan beban dari layanan yang digunakan *file size* sebesar 50000 *bytes*. Sub-bab berikut ini menjelaskan masing-masing skenario yang telah dibuat.

3.3.1 Skenario Tanpa Serangan

Pada skenario tanpa serangan ini masing-masing *routing protocol* (AODV dan OLSR) diuji kinerjanya sesuai dengan parameter yang sudah ditentukan. *Node* yang digunakan dalam skenario ini sebanyak 21 *node*. Dalam skenario ini menggunakan pengaturan *default* untuk kedua *routing protocol*. Berikut ini adalah spesifikasi jaringan MANET pada Gambar 3.2 dan Tabel 3.1 menunjukan parameter yang digunakan pada skenario tanpa serangan.

Tabel 3.1 Spesifikasi Skenario Tanpa Serangan

No	PARAMETER	NILAI
1.	*Technology* Jaringan	802.11b
2.	Luas Area	200X200 meter
3.	Jumlah *Node*	21 *Node*
4.	Jenis Pergerakan *Node*	*Random Waypoint*
5.	Data *Rate*	11 Mbps
6.	Aplikasi Layanan	FTP
7.	Jenis *Traffic* Aplikasi	*High load*



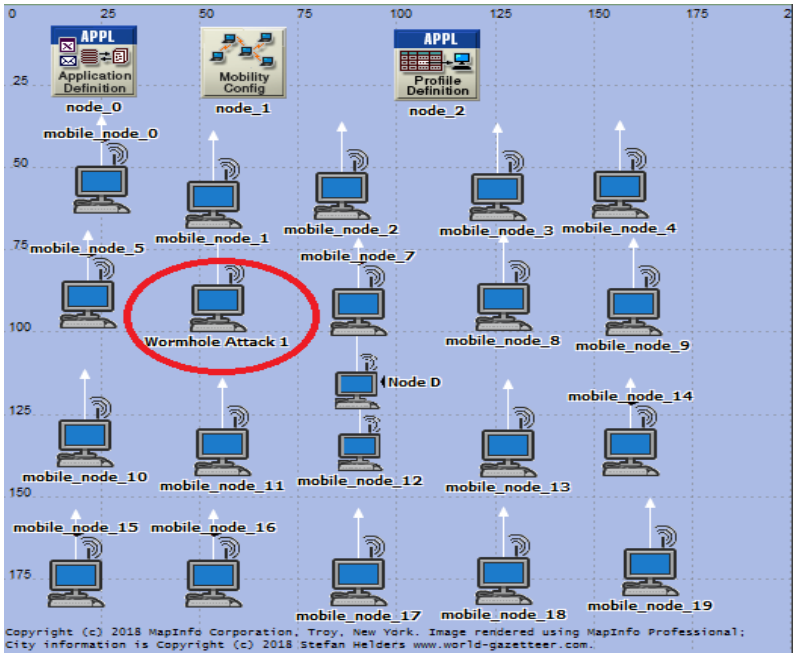
Gambar 3.2 Skenario Tanpa Serangan

3.3.2 Skenario Serangan *Wormhole*

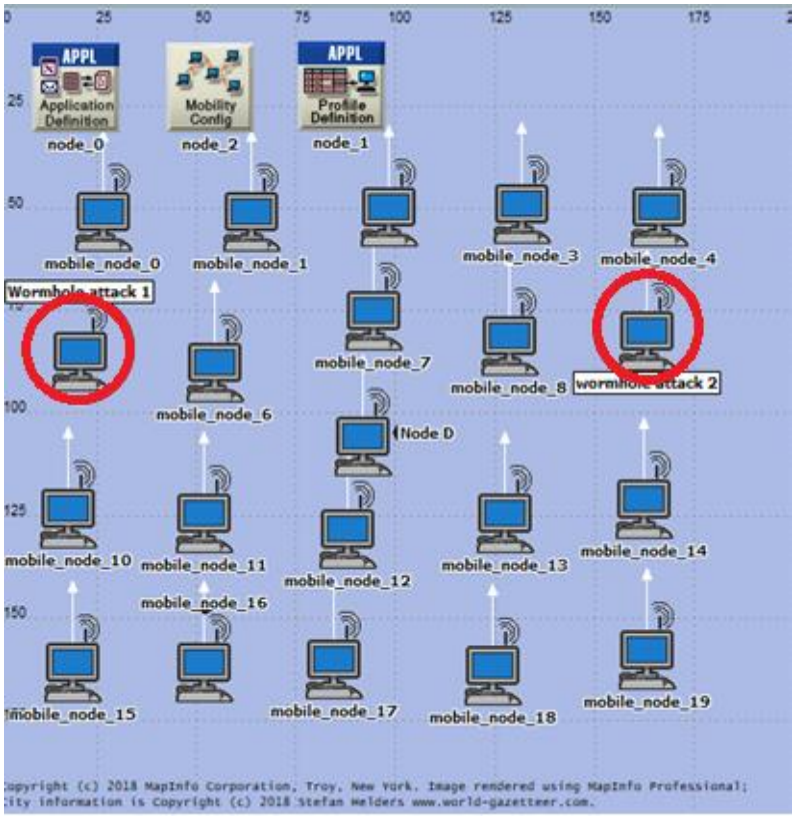
Skenario Serangan *Wormhole* ini pengaturannya sama seperti skenario tanpa serangan, hanya saja ini adanya serangan wormhole pada jaringan MANET AODV dan OLSR. Dimana ada 1, 2, dan 3 buah *attacker* dan 1 *node* D. Berikut ini adalah spesifikasi jaringan MANET pada Gambar 3.3 dan Tabel 3.2 menunjukan parameter yang digunakan.

Tabel 3.2 Spesifikasi Serangan *Wormhole*

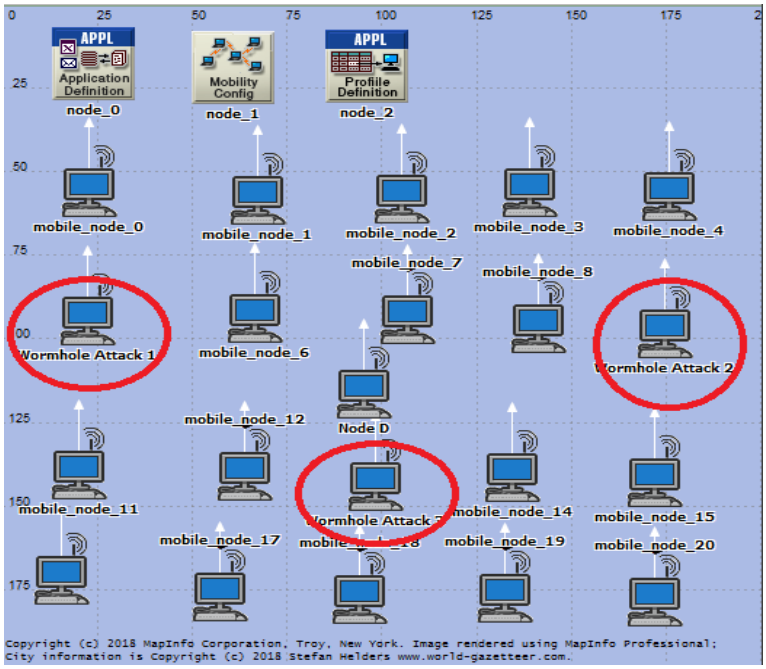
No	PARAMETER	NILAI
1.	*Technology* jaringan	802.11b
2.	Luas Area	200X200 meter
2.	Jumlah *Node*	18 *Node*
3.	Jenis Pergerakan *Node*	*Random Waypoint*
4.	Data *Rate*	11 Mbps
5.	Aplikasi Layanan	FTP
6.	Jenis *Traffic* Aplikasi	*High load*
7.	Jumlah *node Wormhole*	1, 2, dan 3 *Attacker node* + 1 *Node* D



Gambar 3.3 Skenario Serangan *Wormhole* 1



Gambar 3.4 Skenario Serangan *Wormhole* 2



Gambar 3.5 Skenario Serangan *Wormhole* 3

3.4 Cara analisis

Pada penelitian ini didalam *ad-hoc* ada parameter QoS yang dimana sangat penting untuk mengetahui kinerja dari suatu jaringan. Parameter QoS yang digunakan untuk menguji kinerja dari jaringan protokol yaitu *throughput*, *delay*, dan *packet loss*.

3.4.1 Packet loss

Packet loss merupakan banyaknya jumlah paket yang terbuang saat proses pengiriman paket didalam suatu jaringan. Pada TIPHON terdapat klasifikasi *packet loss* yang dimana terdapat beberapa kategori [15].

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

3.4.2 Throughput

Throughput merupakan kecepatan dalam mentransfer data yang terdapat pada jaringan, dikalkulasikan dalam *bit per second*. Semakin besar nilai *throughput* maka semakin baik nilainya.

$$Throughput = \frac{jumlah\ data\ yang\ dikirim}{waktu\ pengiriman\ data} \quad (3.2)$$

3.4.3 Delay

Delay merupakan rata-rata waktu yang dibutuhkan untuk mengirimkan paket dari pengirim ke tujuan. Klasifikasi *delay* beberapa kategori dapat dilihat pada Tabel 3.3 [15].

$$Delay = \frac{Total\ Delay}{Total\ packet\ received} \tag{3.3}$$

Tabel 3.3 Klasifikasi *delay dan packet loss*

Kategori *Delay*	*Delay*	*Packet loss*	Indeks
Sangat Baik	< 150 ms	0% s.d 3%	4
Baik	150 ms s/d 300 ms	3% s.d 15%	3
Sedang	300 ms s/d 450 ms	15% s.d 25%	2
Buruk	> 450 ms	>25%	1

BAB 4
HASIL DAN PEMBAHASAN

4.1 Hasil dan Analisis

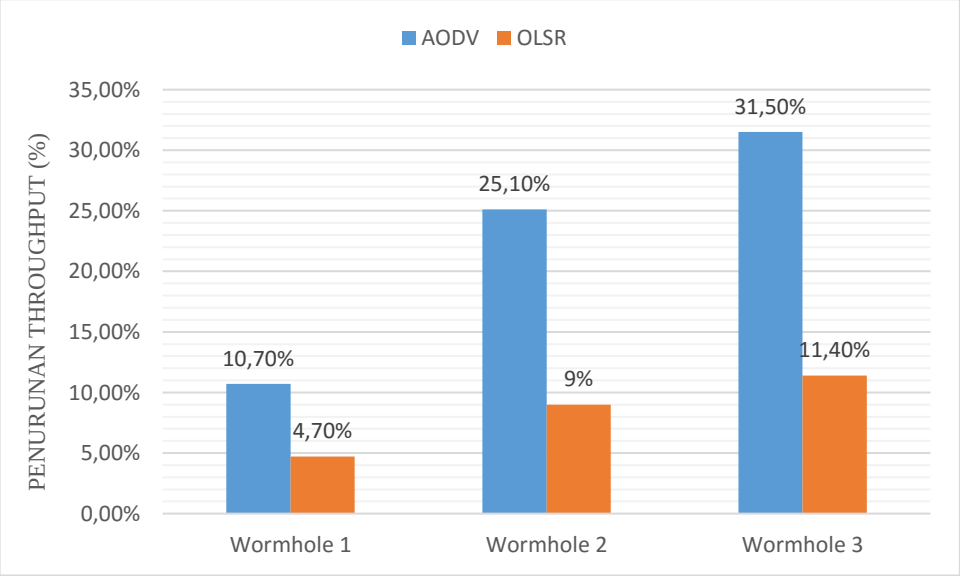
Pada hasil dan analisis pada simulasi ini penulis membahas secara keseluruhan semua yang didapatkan setelah simulasi sampa selesai. Nilai yang diamati menggunakan parameter-parameter QoS yang sudah ditentukan seperti *throughput*, *delay*, dan *packet loss*. Aplikasi layanan yang digunakan dalam skenario ini adalah FTP dengan beban *traffic high load.*

4.2 *Throughput*

Dari hasil keluaran nilai *Throughput*, *routing protocol* AODV dan OLSR memiliki kemampuan dalam mentransfer paket data yang berbeda. Semakin besar nilai *throughput* maka semakin baik nilainya. Nilai *Throughput* data yang dihasilkan dapat dilihat pada Gambar 4.1 dan Tabel 4.1 berikut ini.

Tabel 4.1 Nilai rata-rata Penurunan *Throughput*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	10,7%	25,1%	31,5%
OLSR	4,7%	9%	11,4%



Gambar 4.1 Grafik Penurunan *Throughput*

Pada protokol AODV percobaan tanpa serangan menghasilkan nilai sebesar 287,09 *kbit/s*. Sedangkan untuk protokol OLSR menghasilkan nilai sebesar 773,36 *kbit/s*. Nilai rata-rata

throughput pada OLSR lebih tinggi dibandingkan dengan AODV, hal ini disebabkan dari beberapa faktor yaitu OLSR menggunakan pesan *hello* dan pesan *topology control* (TC) dalam penyebaran paket, sedangkan protokol AODV hanya menggunakan pesan *hello* saja [4].

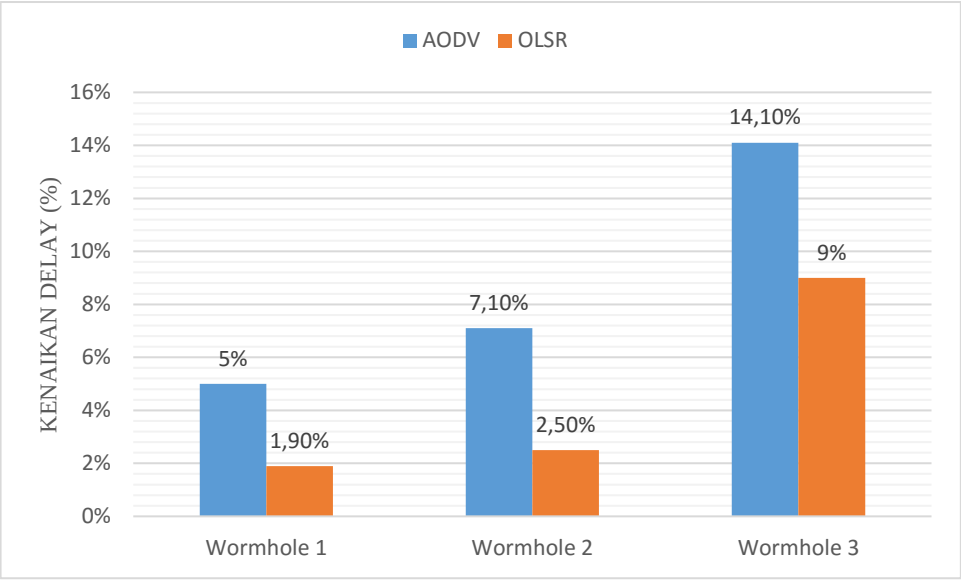
Selanjutnya pada percobaan serangan *wormhole throughput* mengalami penurunan, untuk skenario serangan *wormhole* 1 diperoleh penurunan *throughput* sebesar 10,7% untuk AODV dan untuk OLSR sebesar 4,7%. Sedangkan untuk skenario serangan *wormhole* 2 diperoleh penurunan *throughput* sebesar 25,1% untuk AODV dan untuk OLSR sebesar 9%. Sedangkan untuk skenario serangan *wormhole* 3 diperoleh penurunan *throughput* sebesar 31,5% untuk AODV dan untuk OLSR sebesar 11,4%. Dimana adanya serangan *wormhole* sangat berpengaruh bagi jaringan MANET yang membuat tidak stabil dan dapat mengakibatkan *throughput* turun.

4.3 *Delay*

Dari hasil keluaran nilai *Delay*, *routing protocol* AODV dan OLSR memiliki kemampuan dalam mengirim paket data yang berbeda hingga sampai ke tujuan. Nilai *Delay* yang dihasilkan dapat dilihat pada Gambar 4.2 dan Tabel 4.2 berikut ini.

Tabel 4.2 Nilai rata-rata Kenaikan *Delay*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	5%	7,1%	14,1%
OLSR	1,9%	2,5%	9%



Gambar 4.2 Grafik Kenaikan *Delay*

Dari hasil keluaran nilai *Delay*, protokol AODV percobaan tanpa serangan menghasilkan nilai *delay* sebesar 0.704 *ms.* Sedangkan protokol OLSR menghasilkan nilai *delay* sebesar 0,362

ms. Lebih besar protokol AODV dibandingkan dengan OLSR. Hal ini disebabkan dari beberapa faktor yaitu protokol AODV bekerja secara *on demand*, dimana pencarian *rute* sesuai dengan permintaan pengiriman paket secara *hop by hop* sehingga membutuhkan waktu yang ekstra untuk mencapai tujuan. Berbeda dengan protokol OLSR yang bekerja secara *link state*, dimana rute sudah tersedia sehingga tidak membutuhkan waktu yang lama untuk mencapai tujuan [4]. Meski begitu kedua protokol AODV dan OLSR dikategotikan sangat baik nilai *delay*nya yang terdapat pada standar TIPHON [15].

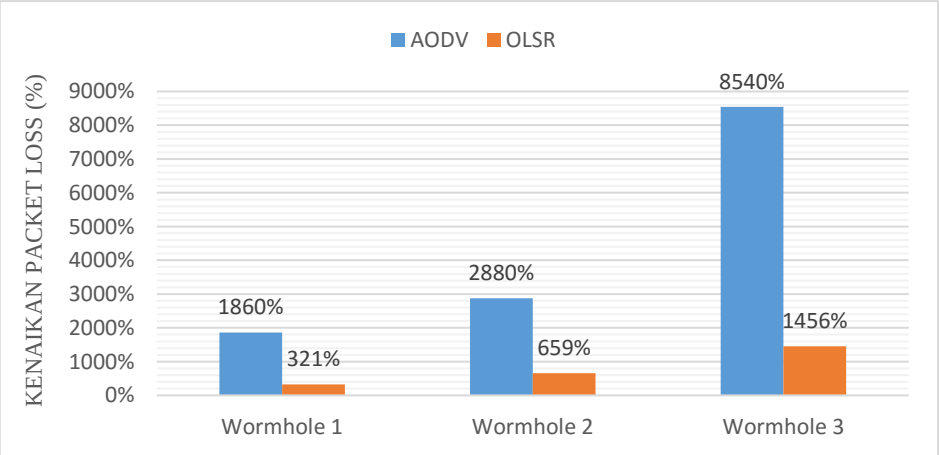
Selanjutnya pada percobaan serangan *wormhole delay* mengalami kenaikan, untuk skenario serangan *wormhole* 1 diperoleh kenaikan *delay* sebesar 5% untuk AODV dan untuk OLSR sebesar 1,9%. Sedangkan untuk skenario serangan *wormhole* 2 diperoleh kenaikan *delay* sebesar 7,1% untuk AODV dan untuk OLSR sebesar 2,5%. Untuk skenario serangan *wormhole* 3 diperoleh kenaikan *delay* sebesar 14,1% untuk AODV dan untuk OLSR sebesar 9%. Serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *delay*, sehingga menjadi naik.

4.4 *Packet Loss Ratio*

Dari hasil keluaran nilai *Packet loss*, *routing protocol* AODV dan OLSR saat terjadi serangan, paket banyak yang dibuang sehingga serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *packet loss.* Pada *packet loss* data yang dihasilkan dapat dilihat pada Gambar 4.3 dan Tabel 4.3 berikut ini.

Tabel 4.3 Nilai rata-rata Kenaikan *Packet loss*

Routing Protocol	*Wormhole* 1	*Wormhole* 2	*Wormhole* 3
AODV	1860 %	2880 %	8540 %
OLSR	321 %	659 %	1456 %



Gambar 4.3 Grafik Kenaikan *Packet loss*

Dari hasil keluaran *packet loss*, protokol AODV percobaan tanpa serangan menghasilkan *packet loss* sebesar 0,05%. Sedangkan protokol OLSR menghasilkan *packet loss* sebesar 0,37%. Hal ini disebabkan dari masing-masing protokol memiliki kinerja yang berbeda. Protokol AODV tanpa serangan lebih baik dibandingkan dengan protokol OLSR. Tetapi masih dikategorikan sangat baik menurut standar TIPHON.

Selanjutnya pada serangan *wormhole packet loss* mengalami kenaikan, untuk skenario serangan *wormhole* 1 diperoleh kenaikan *packet loss* sebesar 1860% untuk AODV dan untuk OLSR sebesar 321%. Sedangkan Untuk skenario serangan *wormhole* 2 diperoleh kenaikan *packet loss* sebesar 2880% untuk AODV dan untuk OLSR sebesar 659%. Sedangkan Untuk skenario serangan *wormhole* 3 diperoleh kenaikan *packet loss* sebesar 8540% untuk AODV dan untuk OLSR sebesar 1456%. Dimana saat terjadi serangan paket banyak yang dibuang, sehingga serangan *wormhole* dapat membuat jaringan tidak stabil yang dapat mempengaruhi nilai *packet loss*. Efek serangan *wormhole* adalah dapat membuat perubahan topologi jaringan, dapat merubah pengiriman pesan yang normal, dan menyebabkan salah dalam pengiriman informasi *routing*.

4.5 Hasil Keseluruhan

Tabel 4.4 Hasil Keseluruhan

Parameter	Tanpa Serangan		*Wormhole* 1		*Wormhole* 2		*Wormhole 3*	
	AODV	OLSR	AODV	OLSR	AODV	OLSR	AODV	OLSR
Throughput (*kbit/s*)	287,09	773,36	10,7%	4,7%	25,1%	9%	31,5%	11,4%
Delay (*ms*)	0,704	0,362	5%	1,9%	7,1%	2,5%	14,1%	9%
Packet loss (*%*)	0,05%	0,37%	1860%	321%	2880%	659%	8540%	1456%

Dari hasil semua percobaan pada Tabel 4.4, maka dapat dilihat kinerja *routing protocol* pada parameter QoS *throughput*, *delay*, dan *packet loss*, protokol OLSR lebih baik dibandingkan dengan AODV. Karena protokol OLSR bersifat proaktif, kemampuan OLSR dapat menemukan jalur di antara dua *node* yang berada di dalam jaringan dengan waktu yang sangat singkat.

Dimana pada saat dengan dan tanpa serangan *wormhole, routing* protokol OLSR lebih baik dalam meminimalkan dampak dari serangan *wormhole* pada jaringan MANET. Efek serangan *wormhole* adalah dapat membuat perubahan topologi jaringan, dapat merubah pengiriman pesan yang normal, dan menyebabkan salah dalam pengiriman informasi *routing*.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Bahwa dari penelitian yang sudah dilakukan, dapat diambil kesimpulan :

1. Pada percobaan ini parameter QoS yang digunakan yaitu *throughput*, *delay*, dan *packet loss*. OLSR lebih baik kinerjanya dibandingankan dengan AODV pada saat jaringan MANET sebelum dan sesudah terkena serangan *wormhole.* Keluaran *Throughput* dari kedua protokol, sebelum terkena serangan protokol AODV menghasilkan nilai sebesar 287,09 *kbit/s*. Sedangkan untuk protokol OLSR menghasilkan nilai sebesar 773,36 *kbit/s.* Untuk skenario serangan *wormhole* 1 diperoleh penurunan *throughput* sebesar 10,7% untuk AODV dan untuk OLSR sebesar 4,7%. Sedangkan Untuk skenario serangan *wormhole* 2 diperoleh penurunan *throughput* sebesar 25,1% untuk AODV dan untuk OLSR sebesar 9%. Sedangkan Untuk skenario serangan *wormhole* 3 diperoleh penurunan *throughput* sebesar 31,5% untuk AODV dan untuk OLSR sebesar 11,4%.
2. Pada parameter *delay*, OLSR lebih baik dibandingkan dengan protokol AODV karena memiliki waktu *delay* yang sangat kecil yaitu 0,000362 *second* dibandingkan dengan AODV sebesar 0,000704 *second.* Untuk skenario serangan *wormhole* 1 diperoleh kenaikan *delay* sebesar 5% untuk AODV dan untuk OLSR sebesar 1,9%. Sedangkan Untuk skenario serangan *wormhole* 2 diperoleh kenaikan *delay* sebesar 7,1% untuk AODV dan untuk OLSR sebesar 2,5%. Untuk skenario serangan *wormhole* 3 diperoleh kenaikan *delay* sebesar 14,1% untuk AODV dan untuk OLSR sebesar 9%.
3. Pada parameter *packet loss, routing* protokol OLSR Lebih baik dibandingkan dengan *routing* protokol AODV karena paket yang terbuang lebih kecil dalam hitungan *persen* pada saat jaringan MANET terkena serangan *wormhole.* Untuk skenario serangan *wormhole* 1 diperoleh kenaikan packet loss sebesar 1860% untuk AODV dan untuk OLSR sebesar 321%. Sedangkan Untuk skenario serangan *wormhole* 2 diperoleh kenaikan *packet loss* sebesar 2880% untuk AODV dan untuk OLSR sebesar 659%. Sedangkan Untuk skenario serangan *wormhole* 3 diperoleh kenaikan *packet loss* sebesar 8540% untuk AODV dan untuk OLSR sebesar 1456%.
4. Dari semua percobaan yang dilakukan pada parameter QoS yang digunakan yaitu *throughput*, *delay*, dan *packet loss*, bahwa protokol OLSR lebih baik dibandingkan dengan protokol AODV pada jaringan MANET yang terkena *wormhole*.

5. Dampak dari serangan *wormhole* dapat menyebabkan perubahan pada topologi jaringan, dan menyebabkan salah dalam pengiriman informasi *routing* pada jaringan MANET. sehingga kinerja dari kedua protokol terhambat dalam pengiriman paket data.

5.2 Saran

1. Melakukan perbandingan selain menggunakan protokol reaktif dan proaktif pada *wormhole attack* di jaringan MANET.
2. Mencoba melakukan penelitian selain serangan *wormhole* pada jaringan MANET, seperti serangan *black hole*, *gray hole*, *flooding attack* dan serangan lainnya.

DAFTAR PUSTAKA

[1] R. M. N. Muhammad Irfan Denatama, Doan Perdana, "Analisis Perbandingan Kinerja Protokol Routing DSDV dan OLSR untuk Perubahan Kecepatan Mobilitas pada Standar IEEE 802.11ah," Univ Telkom, 2016.

[2] D. Imawan, "Analisis Kinerja Pola-Pola Trafik pada Beberapa Protokol Routing dalam Jaringan Manet." Institut Teknologi Sepuluh Nopember, pp. 1–9, 2009.

[3] M. Susanto, "Evaluasi Protokol untuk Mendeteksi Wormhole Attack dengan Menggunakan Global Positioning System (GPS)," ITB, 2013.

[4] W. E. Seputra, Sukiswo, and A. A. Zahra, "Perbandingan Kinerja Protokol AODV dengan OLSR pada MANET," *J. Jur. Tek. Elektro, Fak. Tek. Univ. Diponegoro, Semarang, Indonesia*, pp. 1–7, 2011.

[5] A. P. Rai, V. Srivastava, and R. Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks," Institute Of Technology and Management, Gwalior (M.P), India, vol. 2, no. 2, pp. 174–179, 2012.

[6] P. M. and N. Chavhan, "A Survey on Security Issues to Detect Wormhole Attack in Wirelss Sensor Network," G.H. Raisoni College od Engineering, Nagpur, India, vol. 2, no. 4, pp. 37–50, 2012.

[7] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of Detection Features for Wormhole Attacks in MANETs," *Procedia Comput. Sci.*, vol. 56, no. 1, pp. 384–390, 2015.

[8] A. Fitri Amillia, Marzuki, "Analisis Perbandingan Kinerja Protokol Dynamic Source Routing (DSR) dan Geographic Routing Protocol (GRP) pada Mobile Ad Hoc Network (MANET)," UIN Sultan Syarif Kasim, Riau, vol. 12, no. 1, pp. 9–15, 2014.

[9] D. V. Silaban, S. N. Hertiana, and A. Mulyana, "Simulasi dan Analisis Perbandingan Performansi Jaringan MANET (Mobile Ad Hoc Network) untuk Aplikasi Video Menggunakan Routing Protocol AODV (Ad Hoc On-Demand Distance Vector) dan OLSR (Optimized Link State Routing)," Universitas Telkom, vol. 4, 2010.

[10] M. H. Y. H.Ghayvat, S.Pandya, S.V.Shah, "Advanced AODV Approach for Efficient Detection and Mitigation of Wormhole Attack in MANET," Science and Engineering,Manchester,Metropolitan University, UK. 2014.

[11] K. Purwoko, "Analisis Kinerja Routing Protocol AODV dan OLSR pada Jaringan Wireless," Mesh. Univ Mercu Buana,2012.

[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] R. F. Sari, A. Syarif, and B. Budiardjo, "Analisis Kinerja Protokol Routing Ad Hoc On-Demand Distance Vector (AODV) pada Jaringan Ad Hoc Hybrid Perbandingan Hasil Simulasi dengan NS-2 dan Implementasi pada Testbed dengan PDA," Universitas Indonesia, vol. 12, no. 1, pp. 7–18, 2008.

[14] A. Pradesh, "A Quantitative Study and Comparison of AODV , OLSR and TORA Routing

Protocols in MANET," Tamilarasan-Santhamurthy, LITAM, India, *J. Comput. Sci.*, vol. 9, no. 1, pp. 364–369, 2012.

[15] S. A. Cedex, "Telecommunication and Internet Protocol Harmonization Over Network (TIPHON); Ganeral Aspects of Quality of Service (QoS)," *ETSI*, vol. 2.1.1, pp. 1-37, 1999.