Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 6, No. 8, Agustus 2022, hlm. 4072-4081 http://j-ptiik.ub.ac.id

Kinerja Protocol *Location Aided Routing* (LAR) terhadap serangan *Wormhole* pada Jaringan *Mobile Ad-Hoc Network* (MANET)

Hasan Sabiq[1], Primantara Hari Trisnawan[2], Reza Andria Siregar[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]asansabiq@student.ub.ac.id, [2]prima@ub.ac.id, [3]reza.jalin@ub.ac.id

Abstrak

Mobile ad-hoc network (MANET) adalah suatu jaringan yang dapat berfungsi tanpa adanya suatu infrastruktur tetap. Pada MANET, proses komunikasi diatur menggunakan suatu mekanisme yang disebut *protocol routing*. Dalam hal ini, muncul suatu permasalahan yang umumnya dapat terjadi pada MANET yaitu permasalahan kemanan jaringan. *Wormhole* sendiri merupakan serangan jaringan yang tidak dapat dilakukan oleh satu *node*, karena pada dasarnya serangan *wormhole* membentuk suatu *tunnel* yang menghubungkan satu *node wormhole* dengan *node wormhole* lainya. Maka dari itu penelitian ini melakukan evaluasi dampak dari serangan *wormhole* pada jaringan MANET yang mengunakan *protocol routing Location Aided Routing* (LAR). Dari hasil pengujian yang dilakukan, pengaruh pertambahan jumlah *node* dalam jaringan sebelum terjadi serangan *wormhole* mendapatkan nilai terbaik dari parameter *packet delivery ratio* sebesar 97,13% pada variasi 40 *node*. Untuk parameter *average end to end delay* nilai terbaik didapatkan dengan penggunaan 20 *node* dengan nilai 57,06ms. Dan parameter *routin overhead* nilai terbaik didapatkan pada variasi 40 *node* dengan nilai 0,73. Sedangkan pada skema setelah terjadi serangan *wormhole*, nilai dari parameter *packet delivery ratio* meningkat secara signifikan diraih pada variasi 30 *node* dengan nilai 99,92%. Untuk parameter *average end to end delay*, nilai terbaik didapatkan dengan penggunaan 30 *node* dengan nilai 41,62ms. Dan untuk parameter *routin overhead*, nilai terbaik didapatkan pada variasi 30 *node* dengan nilai 0,18.

Kata kunci: *Mobile Ad-Hoc Network, Location Aided Routin, Wormole.*

Abstract

Mobile ad-hoc network (MANET) is a network that can function without a fixed infrastructure. In MANET, the communication process is managed using a mechanism called a routing protocol. In this case, a problem arises that generally can occur in MANET, namely network security problems. Wormhole itself is a network attack that cannot be carried out by one node, because basically a wormhole attack forms a tunnel that connects one wormhole node with other wormhole nodes. Therefore, this study evaluates the impact of wormhole attacks on the MANET network using the Location Aided Routing (LAR) routing protocol. From the results of the tests carried out, the effect of increasing the number of nodes in the network before the wormhole attack occurred to get the best value from the packet delivery ratio parameter of 97.13% for a variation of 40 nodes. For the average end to end delay parameter, the best value is obtained at a variation of 20 nodes with a value of 57.06ms. And the best value of the routine overhead parameter is obtained at a variation of 40 nodes with a value of 0.73. While in the scheme after the wormhole attack, the value of the packet delivery ratio parameter increased significantly, achieved at a variation of 30 nodes with a value of 99.92%. For the average end to end delay parameter, the best value is obtained at a variation of 30 nodes with a value of 41.62ms. And for the routine overhead parameter, the best value is obtained at a variation of 30 nodes with a value of 0.18..

Keywords: *Mobile Ad-Hoc Network, Location Aided Routin, Wormole.*

1. PENDAHULUAN

Sejalan dengan berjalannya waktu, perkembangan teknologi pada saat ini sudah pada jaman di mana pertukaran informasi dituntut untuk dapat dilakukan dengan sangat

cepat dan tidak terikat dengan hanya satu infrastruktur suatu jaringan saja. Sehingga jika suatu saat terjadi kondisi di mana infrastruktur tersebut tidak dapat diakses karena rusak, dalam masa perbaikan, atau kondisi geografis yang tidak memungkinkan, pertukaran informasi antar *node* masih dapat dilakukan.

Teknologi yang dibutuhkan dalam kasus tersebut adalah teknologi khusus yang berbentuk jaringan *Ad-hoc*, konektifitas *Ad-hoc* sendiri adalah salah satu jaringan dimana tidak terkait dengan suatu infrastruktur tunggal, melainkan jaringan yang terbentuk dari sekumpulan node yang saling bertukar data dan informasi melalui antar muka nirkabel. Dalam implementasinya jaringan Ad-hoc memiliki beberapa contoh seperti Wireless Ad-hoc Network (WANET), Vehicular Ad-hoc Network (VANET), Self Powered Ad-hoc Network (SPAN), dan Mobile Ad-hoc Network (MANET) (Septian,2014).

MANET memiliki beberapa keunggulan daripada dengan jaringan yang menggunakan jenis lainnya. Keunggulan tersebut merupakan jaringan MANET bisa tetap berjalan walaupun tidak terhubung pada satu infrastruktur permanen yang hasilnya dapat lebih cepat beradaptasi dengan pergerakan pengguna atau mobilitas tanpa memerlukan penyesuaian ulang terhadap perangkat yang digunakan. Jenis konektifitas jaringan terdapat dalam MANET memiliki sifat sementara atau dapat diartikan bahwa topologi jaringan pada MANET akan selalu berubah sesuai dengan tingkat pergerakan dari pengguna dalam jaringan MANET tersebut.

Pada proses pengiriman paketnya, jaringan MANET akan memenafaatkan kemampuan setiap *node* untuk melakukan proses *routing* atau proses pencarian rute terbaik untuk pengiriman data dari *node source* kepada *node destination*, sehingga komunikasi antara *node* dalam lingkup koneksititas MANET dapat terjadi. Komunikasi yang dilakukan oleh *node* dalam jaringan MANET juga diatur menggunakan sebuah *protocol* sehingga dapat disebut juga sebagai *protocol routing* (Rachman, 2019).

Setiap *protocol routing* dalam MANET memiliki karakteristik yang berbeda-beda sehingga terdapat kelebihan dan kekurangan pada setiap jenis *protocol*nya. *Location Aided Routing* (LAR) adalah satu dari *protocol routing* berjenis reaktif dimana proses penentuan jalur hanya terjadi apabila diperlukan, *protocol routing* LAR sendiri merupakan *protocol routing* lanjutan dari *protocol* AODV dimana *protocol routing* LAR mempunyai karakteristik dasar yang mirip dengan *protocol routing* AODV dan DSR yaitu sama-sama menggunakan teknik dasar *flooding* dalam proses pencarian rutenya, namun pada *protocol routing* LAR terdapat penambahan informasi lokasi pada *packet header* yang digunakan dalam proses pencarian rute atau RREQ sehingga dapat mengurangi tingkat *routing overhead* dalam jaringan. Informasi lokasi dari setiap *node* dalam jaringan ini didapatkan dengan cara menggunakan *Global Positioning Sistem* (GPS) (Pucanganom, 2019).

Penggunaan *protocol routing* LAR dan MANET sangat berguna dalam kondisi pasca bencana dimana peran MANET yang berbentuk jaringan nirkabel dan penggunaan *protocol routing* LAR dapat menjadikan proses pertukaran informasi lebih cepat dan efisien. Hal tersebut didukung dengan salah satu keunggulan *protocol routing* LAR yang menggunakan lokasi dari *node* pengirim dan *node* penerima untuk memperkecil area pencarian rute dalam proses pengiriman paket.

Namun pada MANET sendiri masih banyak kekurangan yang salah satunya merupakan kelemahan dalam bidang kemanan. Pada MANET, kemanan jaringan merupakan salah satu aspek yang rentan terkena serangan. Contoh dari serangan jaringan di MANET tersebut merupakan *wormhole*, serangan *wormhole* adalah salah satu dari jenis serangan yang dapat menghambat komunikasi antar *node* dalam jaringan *ad-hoc* atau bahkan sampai membuat komunikasi dalam jaringan tersebut mati atau proses komunikasi natar *node* dalam jaringan tidak dapat berjalan sama sekali. Pada dasarnya komunikasi dalam jaringan *ad-hoc* antara *node* S (*sender*) kepada *node* D (*destination*) harus melalui beberapa *node* tetangganya agar terbentuk sebuah *tunnel* atau jalur yang terdekat yang bisa dimanfaatkan dalam proses pengantaran paket.

Serangan jaringan *wormhole* pada umumnya terdiri dari setidaknya dua *wormhole node* sehingga dapat membuat *tunnel* atau jalur terdekata untuk mengantarkan data dari *node* S kepada *node* D. sehingga data yang dikirimkan kemungkinan akan mengambil *tunnel wormhole* tersebut. Masalah ini juga dapat terjadi dalam *protocol* LAR karena pada dasarnya serangan jaringan *wormhole* memiliki kemampuan untuk berpura-pura menjadi *node* normal dalam jaringan yang memungkinkan serangan *wormhole* terjadi.

Pada *protocol routing* LAR, proses

perutean akan menggunakan 2 buah proses yang berbeda yaitu *expected zone* dan *request zone*. Jika *node wormhole* berada pada *expected zone* atau *request zone* sedangkan pasangan *node wormhole* tersebut berada di luar kedua zona tersebut. Maka hal ini dapat menyebabkan perubahan rute yang telah dipilih oleh *protocol* LAR sebelumnya.

Berdasarkan penjelasan mengenai kekurangan MANET dalam segi keamanan jaringan, penelitian ini akan dikerjakan dalam tujuan agar mendapatkan informasi kinerja *protocol Location Aided Routing* (LAR) yang memiliki *wormhole node* pada jaringannya pada MANET. Penelitian ini nantinya dapat diimplementasikan pada *Network Simulator-2.34* dengan jenis proses menguji perbedaan pengunaan *node* pada jaringan simulasi yang akan dibangun, sedangkan untuk *node wormhole* yang akan digunakan berjumlah 0 pasang atau tidak ada sama sekali untuk skenario sebelum terjadi serangan *wormhole* dan 1 pasang *node wormhole*.

Untuk skenario setelah terjadi serangan jaringan *wormhole*, untuk memastikan hasil dari penelitian yang dilakukan, akan digunakan beberapa parameter menguji diantaranya *Packet Delivery Ratio* (PDR), *Average End to End Delay*, dan *Routing Overhead*. Hasil untuk proses menguji menggunakan parameter yang telah disebutkan akan dibandingkan kinerja oleh *protocol* LAR sebelum terjadi serangan *wormhole* dengan kinerja LAR setelah terjadi serangan *wormhole*. Sehingga nantinya dapat digunakan dalam proses pengembangan atau pertimbangan dalam penelitian selanjutnya.

2. LANDASAN KEPUSTAKAAN

2.1 Penelitian Terdahulu

Pada penelitian sebelumnya dari Safitri Dkk. (2019) tentang permasalahan kemanan jaringan terhadap serangan *wormhole* pada jaringan MANET menggunakan *Protocol* AOMDV sebagai *Protocol* komunikasi di dalamnya. Penelitian ini bertujuan untuk pencegahan atau peningkatan dalam sisi kemanan pada MANET menggunakan dua metode yaitu *Delay Per Hop Indicator* (Delphi), serta *Roud Trip Time and Topologilac Comparison* (RTT-TC) untuk mencegah serangan jaringan *wormhole*. hasil dari penelitian yang dilakukan oleh Safitri dkk adalah gabungan dari metode Delphi dan RTT-TC bisa mengetahi serta menangkal serangan jaringan *wormhole* terjadi. Penggunaan dua teknik ini juga bisa mengurangi tingkat *delay* dan menaikan tingkat PDR serta *troughput* pada *protocol routing* AOMDV yang digunakan.

Penelitian selanjutnya dilakukan oleh Suryadilaga (2016). Penelitian tersebut dilakukan analisis dari kinerja *Protocol Routing Greedy Parimeter Stateless Routing* (GPSR) serta *Protocol Routing Location Aided Routing* (LAR) pada lingkup konektifitas VANET. Metodologi yang digunakan dalam penelitian tersebut adalah perbandigan efisiensi kinerja kedua *Protocol Routing* tersebut yang nantinya akan diukur menggunakan parameter *Average End-to-end delay, Normalized Routing Load, Average throughput, Packet Delivery Ratio* (PDR), serta *Routing Overhead*. Hasil untuk penelitian tersebut adalah dengan penggunaan skenario perbedaan jumlah *node* serta perbedaan kecepatan *node*, *protocol routing* GPSR mendapatkan nilai yang lebih baik untuk VANET pada skenario ruang lingkup perkotaan dibandingkan oleh *protocol routing* LAR.

Penelitian lainya dilakukan oleh Yulianto, dkk. (2020). Pada penelitian tersebut dilakukan analisis mengenai unjuk kerja *Protocol* DREAM yang ditambahkan *wormhole attack* di MANET, metode anailisis yang diterapkan adalah skenario menguji dengan menggunakan perbedaan jumlah *node*, serta perbedaan penggunaan *node wormhole* serta parameter menguji yang digunakan adalah *packet delivery ratio* (PDR), *end-to-end delay, routing overhead* serta waktu *convergence*. Nilai dari penelitian tersebut adalah serangan *Wormhole* dapat mempengaruhi kinja *Protocol Routing* DREAM dimana perbedaan penggunaan *node* dapat sangat mempengaruhi untuk kerja *Protocol Routing* DREAM.

2.2 *Mobile Ad-hoc Network* (MANET)

Mobile Ad Hoc Network (MANET) merupakan sekumpulan oleh sejumlah *wireless node* yang bisa dikonfigurasi dengan *dynamic* tanpa perlu terikat oleh teknologi konektifitas tetap yang tersedia. MANET bisa dikatakan sebagai konektifitas sementara yang bisa dibuat dengan sejumlah *mobile node* tanpa memerlukan suatu bentuk pusat administrasi serta teknologi berkabel. MANET, *mobile host* yang terkoneksi oleh *wireless* bisa bergerak secara leluasa serta bisa menjadi *router* (Pucanganom, 2019).

Pada implementasinya, Jaringan MANET biasanya digunakan dalam kondisi tertentu seperti di daerah-daerah yang belum memiliki perangkat *wireless* dengan infrastruktur yang

tetap sampai daerah yang terkena suatu bencana sehingga infrastruktur jaringan pada daerah tersebut terganggu atau putus

Dalam perkembangannya MANET diharapkan dapat diimplementasikan dalam berbagai skenario dan skala network yang beragam. Hal ini disebabkan karena MANET lebih fleksible dalam hal scalability dan mobilitas.

2.3 *Location Aided Routing* (LAR)

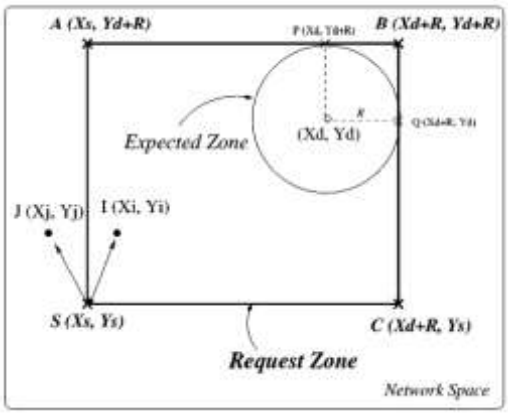
Location aided routing (LAR) merupakan *protocol routing* berjenis reaktif, *protocol* LAR sendiri merupakan salah satu turunan dari *protocol routing* AODV sehingga memiliki kesamaan dalam proses pencarian rutenya yang menggunakan algoritma *flooding* yang membanjiri jaringan dengan paket RREQ.

Namun, *protocol routing* LAR memiliki kemampuan untuk menggunakan informasi lokasi untuk mengetahui lokasi tepat atau lokasi perkiraan dari setiap *node* yang ada sehingga dapat mengurangi tingkat *routing overhead* dalam jaringan. Informasi lokasi tersebut didapatkan dari penggunaan *Global Positioning System* (GPS) (Suryadilaga, 2016).

2.3.1 Proses Route Discovery Pada LAR

Pada proses pencarian rutenya, *protocol routing* LAR akan membentuk lokasi perkiraan atau *expected zone* yang berbentuk lingkaran dimana titik tengahnya merupakan lokasi dari *node* destinasi atau *node* d pada waktu sebelumnya atau lokasi *node* d yang diketahui oleh *node* sumber atau *node* s (X_d,Y_d). Radius dari lingkaran *Expected Zone* sendiri dibentuk dari rata-rata kecepatan pergerakan *node* D sehingga dapat disimbolkan dengan $v(t_1-t_0)$.

Setelah *Expected Zone* diketahui, *node* S akan membentuk *Request Zone* yang berbentuk persegi. *Request Zone* sendiri merupakan zona yang diperbolehkan untuk tiap *node* tetangga untuk mengirimkan paket RREQ sampai ke *node* D. pada *Request Zone* juga berisi *Expected Zone* di dalamnya, *Request Zone* memiliki bentuk persegi yang dibatasi oleh titik S, A, B, dan C. titik S merupakan titik lokasi dari *node* S berada (X_s,Y_s), sedangkan titik A merupakan batas kiri atas (X_s,Y_d+R), titik B kanan atas (X_d+R,Y_d+R), dan titik C (X_d+R,Y_d). Agar penjelasan lebih lengkap bisa ditunjukan oleh Gambar 1 berikut.



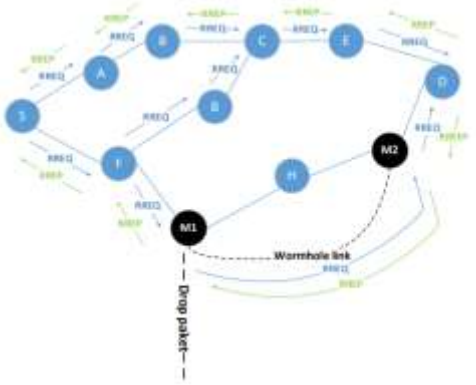
Gambar 1. Skema *Expected Zone* dan *Request Zone*

Sumber : (Ko & Vaidya, 2000)

2.4 *Serangan Wormhole*

Wormhole attack atau serangan jaringan *wormhole* adalah suatu gangguan jaringan di konektifitas MANET, serangan *Wormhole* sendiri terdiri dari setidaknya 2 *Wormhole node* namun juga bisa lebih dari itu dan saling terkoneksi dengan suatu *link* yang dapat dikatakan juga sebagai *Wormhole tunnel.*

Pada proses serangannya, *Wormhole node* mendapatkan paket serta meneruskannya kepada *wormhole node* lain menggunakan *wormhole tunnel* untuk selanjutkan dikirimkan kembali kepada *node* biasa didekatnya sehingga diterima oleh *node destination*. Setelah jalur pengiriman telah ditentukan, data bisa diteruskan menggunakan jalur yang telah dibuat sehingga *Wormhole node* yang ada bisa dengan leluasa melakukan tindakan yang merugikan jaringan seperti melakukan *drop* paket yang akan menyebabkan terjadinya gangguan jaringan.



Gambar 2 Ilustrasi Serangan *Wormhole*

Sumber: (Safitri, andy,dkk 2019).

Gambar 2. menjelaskan tentang proses pencarian rute pada jaringan ketika serangan

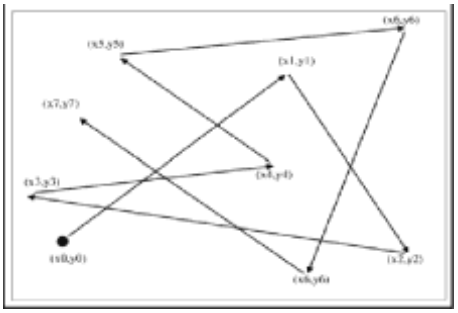
wormhole terjadi. Saat *node* S mengerjakan *Broadcast* data RREQ kepada *node* didekatnya agar menentukan jalur kepada *node* D, *node* M1 yang juga menerima *broadcast* paket RREQ ini langsung meneruskan data RREQ tersebut kepada *node* M2 menggunakan *Wormhole link* atau *wormhole tunnel* yang sudah terbentuk sebelumnya sehingga paket RREQ dari *node* S bisa sangat cepat diterima kepada *node* D yang merupakan *node* tetangga dari *node* M2. Selanjutnya, *node* D bisa membalas data RREQ dari *node* S dengan mengirimkan paket RREP menggunakan *reverse path* ayang melalui *node* M2 serta M1. Oleh karena itu jalur dipilih yang bisa digunakan untuk mengirimkan paket merupakan *node* S-F-M1-M2-D.

2.5 *Random Waypoint* (RWP)

Random waypoint (RWP) merupakan salah satu tipe pergerakan *node* dalam jaringan MANET. Dalam *network simulator* (ns-2), tipe pergerakan *random waypoint* dapat diimplementasikan melalu beberapa tahapan berikut:

1. Saat simulasi dalam *network* simulator (ns-2) dimulai, semua *node* yang terdapat pada konektifitas memilih satu lokasi yang dituju dan selanjutnya melaju menuju lokasi tersebut dengan kecepatan konstan yang dapat diatur seragam maupun random dengan skema pengaturan [0, V_{max}]. skema yang dimaksud merupakan keterangan kecepatan pergerakan *node* yang dapat bergerak mulai dari 0 sampai dengan V_{max} yang sudah ditentukan.
2. Saat *node* dalam jaringan sudah sampai pada tujuan yang dipilih saat awal mula simulasi dijalankan. Terdapat parameter "*pause time*" atau (T_{pause}). Jika parameter *pause time* diset 0 maka node yang sudah sampai pada titik tujuanya akan kembali memilih lokasi tujuan baru untuk bergerak kearah itu.

Siklus pergerakan ini akan terus berjalan sampai waktu simulasi yang digunakan selesai. Dalam tipe pergerakan *random waypoint* ini, dua parameter yang disebutkan di atas yaitu V_{max} dan T_{pause} sangat berpengaruh dalam perilaku mobilitas *node* dalam jaringan (Bai & Helmy, 2014).



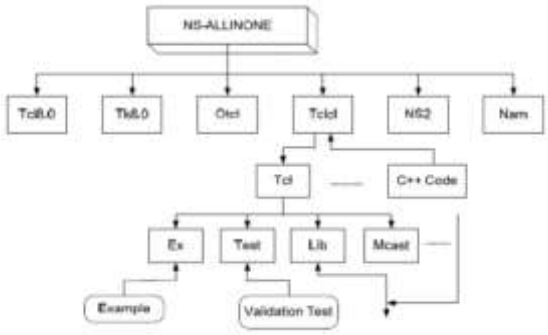
Gambar 3 Pergerakan *Node Tipe Random Waypoint*

Sumber: (Bai & Helmy, 2014)

2.6 *Network Simulator* (NS)

NS merupakan aplikasi simulasi konektifitas yang pertama kali dibuat oleh *University of California Berkeley* serta USC ISI pada salah satu projek *Virtual INternet Testbed* (VINT). NS juga merupakan *tool* yang bisa digunakan sebagai simulasi untuk konektifitas nirkabel (*wireless*) serta konektifitas *ad-hoc*.

Pemrogrraman NS mengaplikasikan dua Bahasa pemrograman, yaitu C++ serta Otcl. Bahasa C++ diperuntukan untuk *library* lantaran C++ bisa mendapatkan *runtime* simulator yang lebih andal, Otcl juga dipakai oleh *script* simulator yang diimplementasikan dari NS user dan bertindak menjadi interpreter. Bagian pembentuk NS-2 serta penempatanya dapat sangat berpengaruh pada proses pembuatan simulator. Bagian pembentuk NS-2 bisa digambarkan pada Gambar 4 berikut.



Gambar 4 Komponen pembangun NS

Sumber : (Suladria, 2014)

3. METODE PENELITIAN

Bagian metode penelitian bisa menjelaskan tentang proses yang dilakukan pada penelitian dari mulai sampai selesai seperti yang digambarkan pada Gambar 5.

3.1 Kerangka Penelitian

Kerangka penelitian menjelaskan mengenai metode serta proses yang digunakan pada pengerjaan penelitian ini. Berikut adalah proses yang akan dilakukan dalam penelitian.

Gambar 5 Metodologi Penelitian

3.2 Studi Literatur

Tahapan studi literatur adalah tahapan untuk mencari mengenai dasar serta landasan mengenai perancangan serta implementasi. Beberapa dari studi literatur yang dibuat tentang dasar dari MANET seperti kelebihan serta kekurangannya. Setelah itu, proses studi literatur mengenai *routing protocol* LAR, simulator pengujian yang bisa digunakan, dan serangan *wormhole*.

3.3 Analisis Kebutuhan

Tahapan analisis kebutuhan dilakukan untuk mendeskripsikan kebutuhan yang diperlukan mengenai analisis dampak serangan *Wormhole* pada jaringan MANET dengan *protocol routing Location Aided Routing* (LAR). Kebutuhan yang akan dibahas pada tahapan ini merupakan kebutuhan mengenai *hardware* serta *software* yang bisa dipakai untuk proses penelitian.

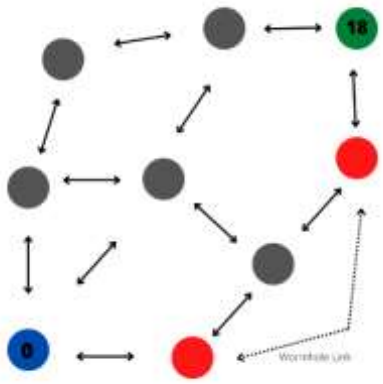
3.4 Perancangan Sistem

Tahapan mengenai perancangan system adalah proses untuk melakukan gambaran dari system yang akan dibuat dan memcukupi kebutuhan untuk penelitian yang akan dilakukan. Perancangan dilakukan dengan proses perancangan simulasi yang akan digunakan, perancangan serangan *Wormhole* yang dilakukan, serta penggambaran parameter pengujian yang bisa diterapkan untuk menguji hasil simulasi. Untuk lebih jelasnya, tahapan perancangan akan dilakukan menggunakan parameter yang dapat ditunjukan dalam Tabel 1 sebagai berikut.

Tabel 1. Perancangan Sistem

Parameter	Spesifikasi
Network Simulator	Network Simulator-2.34
Routing Protocol	*Location Aided Routing* (LAR)
Parameter Pengujian	*packet delivery ratio, End to End Delay, Routing Overhead*
Waktu Simulasi	1000s
Area Simulasi	1000 x 1000
Jumlah Node	20,30,40
Jumlah Node *Wormhole*	0, dan 1 pasang.
Model Pergerakan Node	*Random Way Point*
Tipe Koneksi	CBR (*constant bit rate*)
Kecepatan Pergerakan Node	0,5 – 1,5 m/s
Source/Destination	Statik (Node 0 / Node 18)
Besar Paket Data	512 byte
Set *Rate*	512 kbps

Penelitian ini akan menggunakan parameter penelitian dimana simulator yang akan digunakan adalah NS-2.34 dan *routing protocol* LAR pada jaringan MANET. Adapun variasi *node* yang bisa di aplikasikan dalam proses simulasi berjumlah 20, 30, serta 40 *node* dengan luas dari area simulasi mencapai 1000x1000m^2. Pergerakan *node* yang digunakan dalam simulasi merupakan pergerakan *node* dengan tipe *random way point* menggunakan kemampuan pergerakan *node* sekitar 0.5 - 1.5 m/s. Paket data yang akan dikirimkan antara *node* pengirim dan *node* penerima memiliki besaran sebesar 512 bytes dengan tipe konektifitas CBR (*constant bit rate*) dengan set *rate* 512 kbps. Waktu simulasi yang akan dilakukan adalah 1000s dimana *node* 0 berperan sebagai pengirim dan *node* 18 berperan sebagai penerima.



Gambar 6 Perancangan topologi simulasi dengan serangan

3.5 Implementasi

Pada tahapan ini, dilakukan implentasi untuk menjalankan simulasi yang akan digunakan berupa proses pengimplementasian *protocol routing* yang diteliti, waktu simulasi, luas area, jumlah *node*, model pergerakan, dan ukuran data yang akan diteruskan serta parameter menguji yang akan digunakan.

3.5.1 *Packet Delivery Ratio*

Proses menguji ini dikerjakan melalui parameter *packet delivery ratio*. Proses pengujian ini berupa membandingkan data yang berhasil diperoleh oleh *node destination* dengan jumlah keseluruhan data yang diteruskan oleh *node source*.

3.5.2 *Average End to End Delay*

Proses menguji ini dikerjkan melalui parameter *average end to end delay*. Proses pengujian ini berupa menghitung waktu rata-rata yang ditempuh oleh data dari *node source* dapat diterima pada *node destination*.

3.5.3 *Routing Overhead*

Pengujian ini dilakukan dengan menggunakan parameter *routing overhead*. Proses pengujian ini berupa menghitung banyaknya paket yang dikirimkan dalam jaringan oleh *routing protocol*. Hal ini juga dapat menunjukan dampak serangan *wormhole* terhadap kinerja *protocol routing* LAR.

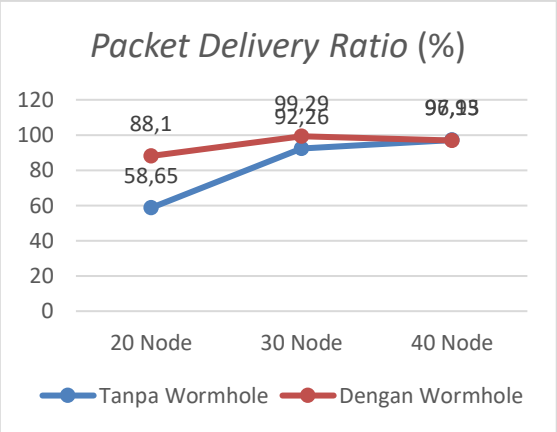
4. PENGUJIAN DAN ANALISIS

Pada pengujian dan analisis bisa menjelaskan tentang hasil menguji dari implementasi simulasi serangan *wormhole* pada *protocol Location Aided Routing* (LAR) di jaringan *Mobile Adhoc Network* (MANET). Pengujian yang dilakukan memiliki 2 skenario dimana pada skenario pertama ini, simulasi akan dilakukan tanpa adanya serangan *Wormhole*, namun pada skenario ini tetap dijalankan simulasi dengan perbedaan jumlah *node* dalam jaringan yaitu 20,30, dan 40 *node*. skenario ini dijalankan dengan tujuan untuk mengetahui kinerja awal dari *protocol* LAR yang berjalan di jaringan MANET.

Pada skenario kedua, simulasi akan dijalankan dengan adanya sarangan *wormhole* dalam jaringan MANET yang menggunakan *routing protocol* LAR. Skenario ini juga menggunakan perbedaan jumlah *node* untuk masing-masing simulasi yang dijalankan. Harapan awal dijalankannya skenario ini adalah untuk mengetahui perbedaan atau dampak dari serangan *wormhole* terhadap *protocol routing* LAR pada jaringan MANET. Selanjutnya, hasil simulasi yang sudah dijalankan akan dianalisis dengan parameter menguji seperti *Packet Delivery Ratio, Average End to End Delay,* dan *Routing Overhead* serta dibandingkan kinerja dari *protocol routing* LAR berdasarkan dua skenario tersebut.

4.1 Pengujian dan Analisis *Packet Delivery Ratio*

Analisis mengenai proses menguji dengan skema perbedaan penggunaan jumlah *node* yaitu 20, 30, dan 40 *node* tanpa menggunakan serangan *wormhole* dan dengan menggunakan serangan *wormhole* terhadap parameter pengujian *packet delivery ratio* yang menggunakan luas simulasi 1000x1000m_2 dengan pergerakan *random way point* (RWP) dan kecepatan *node* antara 0,5 sampai 1,5m/s. Besar paket data yang digunakan dalam simulasi ayaitu 512 bytes dan menggunakan tipe konektifitas *constant bit rate* (CBR). Waktu simulasi yang digunakan adalah 1000 s bisa digambarkan pada Gambar 6 sebagai berikut.



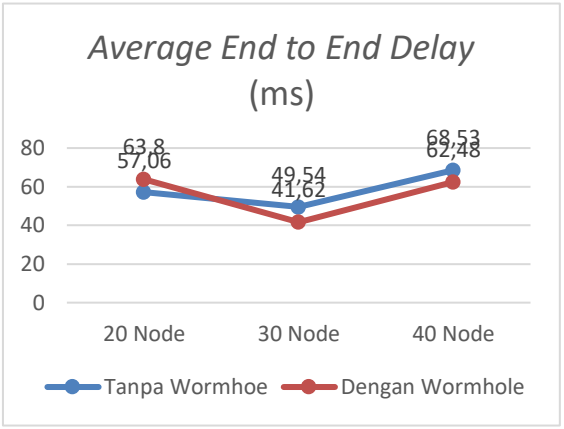
Gambar 6. Pengujian *Packet Delivery Ratio*

Pada Gambar 6, bisa menggambarkan mengenai grafik dari hasil parameter *packet delivery ratio* menunjukan peningkatan yang lumayan signifikan hanya berdasarkan perbedaan penggunaan *node*. Dalam hal ini, hasil dari parameter *packet delivery ratio* yang paling bagus berada pada variasi penggunaan 40 *node* 97,13% sebelum terjadi serangan *wormhole*. Hal ini dapat terjadi karena perbedaan jumlah node dapat berpengaruh pada batas jarak komunikasi yang bisa dicapat oleh setiap *node*nya. Sehingga semakin rapat posisi dari tiap node, akan membuat hasil dari *packet delivery ratio* juga membaik.

Sedangkan pada skema setelah terjadinya serangan *wormhole*, hasil mengenai parameter *packet delivery ratio* bisa bertambah secara signifikan. Hal ini dapat dilihat pada penggunaan variasi 20 *node*, dimana posisi *node* pada skema ini memiliki jarak antar node yang cukup jauh. Namun serangan *wormhole* yang pada dasarnya menghubungkan 2 *node* atau lebih yang berjauhan sehingga membentuk *tunnel* agar dapat terhubung satu sama lain, membuat jarak yang tadinya memiliki dampak negative untuk *packet delivery ratio* menjadi tidak terlalu berarti. Sehingga pada penggunaan variasi 20 *node* ini, dapat terjadi peningkatan yang signifikan dari 58,65% menjadi 88,10%. Walaupun nilai PDR tertinggi dimiliki oleh variasi penggunaan 30 *node* dengan nilai 99,29%.

4.2 Pengujian dan Analisis *Average End to End Delay*

Analisis dari proses menguji melalui skema menggunakan variasi jumlah *node* yaitu 20, 30, dan 40 *node* tanpa menggunakan serangan *wormhole* dan dengan menggunakan serangan *wormhole* terhadap parameter menguji *average end to nd delay* yang menggunakan luas simulasi 1000x1000m$_2$ dengan pergerakan *random way point* (RWP) dan kecepatan *node* antara 0,5 sampai 1,5m/s. Besar paket data yang dipakai dalam simulasi ayaitu 512 bytes dan dengan tipe konektifitas *constant bit rate* (CBR). Waktu simulasi yang dipakai adalah 1000 s dapat dilihat dari grafik di bawah ini.



Gambar 7. Pengujian *Average End to End Delay*

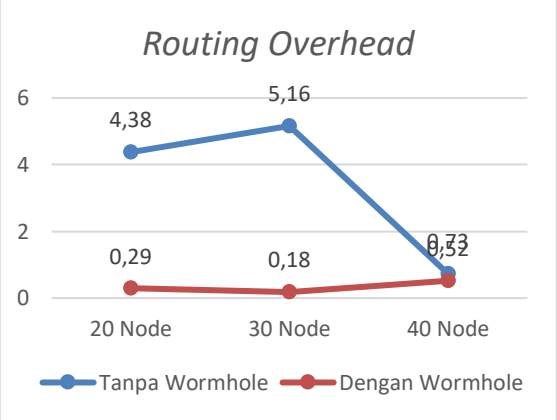
Gambar 7, bisa menggambarkan grafik yang menggambarkan perbedaan nilai dari parameter *average end to end delay*. Pada grafik tersebut, dapat dikatakan hasil dari parameter *average end to end delay* mengalami peningkatan dalam skema tanpa serangan *wormhole* terutama pada variasi 40 *node* dengan nilai mencapai 68,53ms. Hal ini bisa timbul disebabkan oleh penambahan jumlah *node* bisa membuat hampir keseluruhan proses *routing* mulai dari *route discovery* hinga paket dapat sampai pada *destination node* menjadi lebih lama.

Sedangkan pada skema setelah terjadi serangan *wormhole*, hasil dari parameter *average end to end delay* mendapatkan dampak penurunan yang tidak terlalu signifikan. Titik terendahnya ada pada variasi 30 *node* dengan nilai 41.62ms. penurunan tingkat *average end to end delay* ini bisa diakibatkan karena pembentukan *tunnel* yang dilakukan oleh *node wormhole* membuat data yang dikirimkan oleh *node source* dapat lebih cepat diterima pada *node destination*.

4.3 Pengujian dan Analisis *Routing Overhead*

Analisis dari pengujian dengan skema menggunakan variasi jumlah *node* yaitu 20, 30,

dan 40 *node* tanpa menggunakan serangan *wormhole* dan dengan menggunakan serangan *wormhole* terhadap parameter pengujian *routing overhead* yang menggunakan luas simulasi 1000x1000m_2 dengan pergerakan *random way point* (RWP) dan kecepatan *node* antara 0,5 sampai 1,5m/s. Ukuran paket data yang dipakai dalam simulasi ayaitu 512 bytes dan dengan tipe konektifitas *constant bit rate* (CBR). Waktu simulasi yang dipakai adalah 1000 s dapat dilihat dari grafik di bawah ini.



Gambar 8. Pengujian *Routing Overhead*

Dari Gambar 8, dapat dilihat grafik yang menampilkan hasil pengaruh variasi jumlah *node* dengan sebelum dan sesudah terjadinya serangan *wormhole*. Pada skema penelitian sebelum terjadinya serangan *wormhole*, nilai terendah yang didapatkan ada pada variasi 40 *node* dengan nilai 0,73. Hal ini terjadi karena penambahan jumlah *node* dalam jaringan dapat mempengaruhi perilaku *node* dalam melakukan proses pencarian rute, sehinga paket RREQ yang tersebar dalam jaringan akan semakin bertambah. Namun pada variasi 40 *node*, jarak antar *node* yang berada dalam jaringan sudah sangat dekat dan pada dasarnya tipe pergerakan *random way point* (RPW) merupakan tipe pergerakan random yang lebih mengarah ke tengah area simulasi. Maka paket routing yang dikirimkan dalam jaringan dapat berkurang secara signifikan.

Pada skema setelah terjadi serangan *wormhole*. Nilai dari parameter *routing overhead* lebih cenderung stabil dan memiliki nilai terendah pada variasi 30 *node* dengan nilai 0,18. Hal ini menunjukan *tunneling* yang dibentuk oleh *node wormhole* berjalan sangat sukses sehinga proses perutean pasti akan melewati *tunnel wormhole* tersebut. Namun hal ini juga membuktikan bahwa attacker yang berada di balik *node wormhole* tersebut dapat secara leluasa mengakses data yang melalui *tunnel wormhole* dan jika diinginkan dapat dilakukan *drop* paket yang akan mengganggu jaringan MANET tersebut.

5. PENUTUP

5.1 Kesimpulan

Kesimpulan mengenai hasil menguji dan analisis dari perbedaan variasi jumlah *node* terhadap kinerja *routing protocol* LAR dengan atau tanpa serangan jaringan *wormhole* pada jaringan MANET yaitu:

1. Pengaruh dari perbedaan jumlah node 20, 30, dan 40 node terhadap protocol routing LAR dapat berdampak terhadap peningkatan nilai parameter pengujian. Peningkatan nilai yang paling signifikan dapat dilihat pada parameter packet delivery ratio (PDR) dimana terdapat peningkatan dari 58,65% pada penggunaan 20 node dan meningkat hingga 92,26% pada penggunaan 30 node atau dapat dikatakan terjadi peningkatan sebesar 33,61%.
2. Pada simulasi dengan menggunakan *wormhole*. *Protocol routing* LAR dapat berjalan dengan lebih baik dari segi parameter-parameter pengujian yang digunakan. Terbukti dari tingkat *packet delivery ratio* yang meningkat secara signifikan pada variasi 20 *node* yang meningkat dari 58,65% sebelum terjadi *wormhole* menjadi 88,10% pada skema setela terjadinya seranggan *wormhole*, penambahan *node wormhole* juga dapat membantu menurunkan tingkat *average end to end delay* dan menstabilkan tingkat *routing overhead* dalam jaringan. Namun hal positif yang didapatkan dari serangan *wormhole* ini terjadi karena implementasi *wormhole* pada penelitian ini hanya mengaplikasikan skema dasar *wormhole* yang melakukan *tunneling* antar *node wormhole*nya. Jika dilakukan modifikasi hingga *drop* paket pada paket yang melewati *tunnel wormhole*, hasil penelitian juga akan berubah.

5.2 Saran

Saran yang bisa diajukan mengenai hasil analisis serta pengujian yang telah dilakukan pada penelitian kali ini yaitu:

1. Melakukan penelitian yang akan membandingkan *protocol routing* LAR dengan *protocol routing* lain dalam skema serangan *wormhole*.
2. Melakukan penelitian *wormhole* menggunakan skema dan parameter pengujian yang berbeda.
3. Melakukan modifikasi atas perilaku *node wormhole* sehinga dapat membuat paket yang melewati *tunnel* wormhole dapat di *drop* atau dapat dilakukan skema serangan lain pada paket tersebut.

6. DAFTAR PUSTAKA

Nurusshobah, Muhammad. 2019. "Analisis Kinerja Protokol Routing Dynamic MANET On-Demand (DYMO) dan Cluster Based Routing Protocol (CBRP) pada Mobile Ad-Hoc Network (MANET)" Universitas Brawijaya. Malang. Indonesia.

Pucanganom, I Dewa Gede Ardhana. 2018. "Analisis Perbandingan Dampak Serangan Blackhole pada Kinerja Routing Protokol LAR (Location Aided Routing) dan DYMO (Dynamic MANET On-Demand) di Mobile Ad-Hoc Network (MANET)" Universitas Brawijaya. Malang. Indonesia.

Rachman, Wildan Aulia. 2019. "Analisis Konsumsi Energi Protokol Routing Fisheye State Routing (FSR) pada Mobile Adhoc Network (MANET). Universitas Brawijaya. Malang. Indonesia.

Safitri, dkk. 2019. “Deteksi dan Pencegahan Serangan wormhole pada Protokol Routing AOMDV Menggunakan Gabungan Metode Delphi dan RTT-TC pada Jaringan MANET”. Universitas Mataram. Indonesia.

Suryadilaga, M. A., Munadi, R. & Negara, R. M., 2016. “Analisis Kinerja Protokol Routing GPSR Dan LAR Pada Simulasi Jaringan Vehicular Ad Hoc Network (VANET)”. S.L.:S.N.

Yulianto, Prasetyo dkk. 2020. “Kinerja Protokol Distance Routing Effect Algorithm for Mobility (DREAM) Terhadap Serangan Wormhole pada Mobile Ad-hoc Network (MANET)”. Universitas Brawijaya. Indonesia.