Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 3, Maret 2019, hlm. 2853-2861 http://j-ptiik.ub.ac.id

Analisis Pengaruh *Blackhole Attack* Terhadap Kinerja Protokol *Routing* BATMAN *(Better Approach To Mobile Ad Hoc Network*) Pada *Mobile Ad Hoc Network*

Imam Nurhidayat[1], Primantara Hari Trisnawan[2], Reza Andria Siregar[3]

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

Abstrak

Mobile Ad-hoc Network (MANET) merupakan sebuah arsitektur jaringan yang terdiri dari beberapa *node* yang bergerak secara bebas dan saling berkomunikasi satu sama lain. Setiap *node* dapat berfungsi sebagai *router* maupun *client* bagi *node* lainnya. MANET memiliki 3 jenis protokol *routing* yaitu protokol *routing proaktif*, *reaktif*, dan *hybrid*. BATMAN (*Better Approach to Mobile Adhoc Network*) merupakan salah satu protokol *routing* pada MANET. Dalam segi keamanan, MANET masih rentan terhadap berbagai bentuk serangan, terutama terhadap serangan aktif yang dapat menghancurkan, memodifikasi, dan menghapus data serta informasi di dalamnya. Salah satu jenis serangan aktif yang dapat terjadi pada MANET adalah *blackhole attack*. *Blackhole Attack* adalah serangan yang dapat menyebabkan hilangnya paket data yang dikirimkan. Berdasarkan permasalahan di atas, maka penulis membuat penelitian yang berjudul Analisis Pengaruh *Blackhole Attack* terhadap Kinerja Protokol Routing BATMAN (*Better Approach To Mobile Ad Hoc Network*) pada *Mobile Ad Hoc Network.* Hasil yang didapatkan dalam penelitian ini adalah serangan *blackhole* mempengaruhi kinerja dari protokol *routing* BATMAN. Pengujian dilakukan menggunakan OMNET++ dengan skenario pengujian berupa variasi jumlah *node*, jumlah *node* penyerang, dan luas area simulasi. Parameter pengujian meliputi *packet delivery ratio* (PDR) dan *packet loss*. Perhitungan *packet loss* hanya dilakukan pada paket yang di-*drop* oleh *node* penyerang saja. Hasil pengujian menunjukkan rata – rata *packet delivery ratio* paling rendah terdapat pada skenario 30 *node* dengan luas area 1200x1200 m2 yaitu sebesar 14,24%. Sedangkan nilai rata – rata *packet loss* tertinggi terdapat pada skenario 30 *node* dengan luas area 1000x1000 m2 yaitu sebesar 56,62%.

Kata kunci: MANET, BATMAN, *blackhole*, OMNET++

Abstract

Mobile Ad-hoc Network (MANET) is a network architecture consisting of several nodes that move freely and communicate with each other. Each node can function as a router or client for other nodes. MANET has 3 types of routing protocols, namely proactive, reactive and hybrid routing protocols. BATMAN (Better Approach to Mobile Adhoc Network) is one of the routing protocols on MANET. In terms of security, MANET is still vulnerable to various forms of attacks, especially against active attacks that can destroy, modify, and delete data and information. One type of active attack that can occurs in MANET is blackhole attack. Blackhole Attack is an attack that can cause loss of data packets. Based on the above problems, the authors made a study entitled Analysis the Effect of Blackhole Attack on the Performance of the BATMAN (Better Approach To Mobile Adhoc Network) Routing Protocol on Mobile Adhoc Network. The results obtained in this study are blackhole attacks affect the performance of the BATMAN routing protocol. Testing is done using OMNET ++ with a test scenario in the form of variations in number of nodes, number of attacking nodes, and area of the simulation. Test parameters used are packet delivery ratio (PDR) and packet loss. The packet loss calculation is only done on packets dropped by the attacker node. The test results show that the lowest packet delivery ratio is 14,24% in the 30 node scenario with an area of 1200x1200 m^2*. While the highest average packet loss is 56.62% in the 30 node scenario with an area of 1000x1000* m^2*.*

Keywords: *MANET, BATMAN, blackhole, OMNET++*

1. PENDAHULUAN

Mobile Ad-hoc Network atau biasa disingkat MANET merupakan sebuah arsitektur jaringan yang terdiri dari beberapa *node* yang bergerak secara bebas dan saling berkomunikasi satu sama lain. MANET tidak membutuhkan backbone infrastruktur sehingga sangat cocok diterapkan pada daerah – daerah yang tidak memiliki infrastruktur jaringan. Pada jaringan MANET, setiap *node* dapat berfungsi sebagai *router* maupun *client* bagi *node* lainnya (Sarika, 2016).

Dalam mengirimkan paket data sampai ke tujuan, suatu *node* harus mengetahui jalur yang harus dilewati agar sampai pada *node* tujuan paket. Metode yang digunakan untuk penentuan jalur hingga pengiriman paket data ini disebut protokol *routing*. MANET memiliki 3 jenis protokol *routing* yaitu protokol *routing proaktif, reaktif*, dan *hybrid*. BATMAN (*Better Approach to Mobile Ad-hoc Network*) adalah salah satu protokol *routing proaktif* yang terdapat pada jaringan MANET. Konsep *routing* pada BATMAN adalah dengan meminimalisir penggunaan informasi *routing*, yaitu setiap *node* hanya mengetahui *nexthop* untusk dapat sampai pada *node* tujuan. Protokol BATMAN tidak mencoba untuk mencari jalur *routing* secara keseluruhan, melainkan hanya mencari tahu link-local mana yang merupakan *gateway* terbaik untuk setiap *node* tujuan. (Neuman, 2008).

Namun seperti halnya arsitektur jaringan yang lain, MANET juga memiliki beberapa kelemahan. Salah satu kelemahan yang paling utama pada MANET adalah mengenai masalah keamanan. Pada MANET, *node – node* dapat secara bebas keluar masuk ke dalam jaringan. Hal ini lah yang menyebabkan MANET menjadi rentan terhadap serangan dari luar. BATMAN sebagai salah satu protokol *routing* pada MANET juga sangat rentan terhadap serangan yang dapat mengganggu kinerja dari *routing* protokol tersebut. MANET rentan terhadap dua jenis serangan yaitu serangan aktif dan serangan pasif. Pada serangan pasif, penyerang melakukan pemantauan terhadap koneksi tertentu dengan tujuan mencuri informasi lalu lintas tanpa menambahkan informasi palsu, mempengaruhi *resource* dari suatu sistem, dan mengganggu fungsi dari suatu jaringan. Contoh serangan pasif yaitu *eavesdropping*, *snooping*, dan lain - lain. Sedangkan pada serangan aktif, penyerang mencoba untuk memodifikasi atau menghancurkan sumber daya sistem dan data yang dipertukarkan dalam jaringan (Verma, 2016). Salah satu jenis serangan aktif yang sering terjadi pada MANET adalah *blackhole attack*. *Blackhole Attack* adalah serangan yang dapat menyebabkan hilangnya paket data yang dikirimkan. *Node* dengan serangan *blackhole* akan membuat dirinya tampak seperti layaknya *node* normal, sehingga akan diperlakukan seperti halnya *node* normal. Namun, paket yang dikirimkan melalui *node* tersebut akan hilang dan tidak akan sampai pada tujuan (Rajaram, 2010).

Penelitian sebelumnya yang membahas mengenai pengaruh *blackhole* pada jaringan MANET dilakukan oleh Patel(2017) mengenai Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26. Penelitian ini membahas mengenai pengaruh *blackhole* attack terhadap parameter packet delivery ratio, delay, dan throughput pada AODV (*Ad Hoc on Demand Distance Vector*). Pada penelitian ini membandingkan kinerja dari protokol *routing* AODV sebelum dan sesudah terkena serangan *blackhole*. Penelitian lain dilakukan oleh Virgi(2017) tentang Analisis Perbandingan Dampak Serangan *Blackhole* pada Performansi Protokol *Routing* OLSR (*Optimized Link State Routing*) dan AODV (*Ad Hoc on Demand Distance Vector*) di Jaringan *Wireless Mesh Network*. Pada penelitian ini membandingkan kinerja dari protokol AODV dan OLSR terhadap serangan *blackhole* pada MANET. Penelitian dilakukan untuk menentukan protokol *routing* mana yang lebih rentan terhadap serangan *blackhole*. Parameter pengujian meliputi *throughput*, *delay*, *packet loss*, dan *packet delivery ratio*. Penelitian selanjutnya dilakukan oleh Elguzka(2017) mengenai Analisis Pengaruh Serangan *Blackhole* Terhadap Protokol AODV Pada Mobile Ad Hoc Network Dengan Lingkungan Dinamis. Penelitian ini dilakukan untuk mengetahui kinerja protokol *routing* AODV ketika terjadi serangan *blackhole* dengan lingkungan yang dinamis.

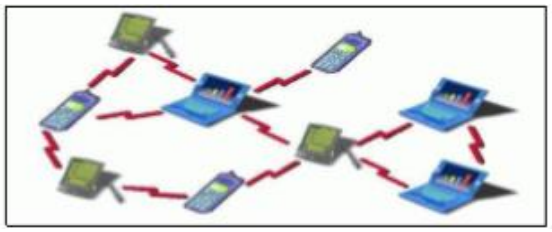
Berdasarkan permasalahan yang telah dijelaskan sebelumnya, diperlukan sebuah analisis serangan *blackhole* untuk mengetahui seberapa besar pengaruh serangan *blackhole* terhadap kinerja dari protokol BATMAN. Pada penelitian ini akan dilakukan analisis perbandingan kinerja dari protokol BATMAN sebelum dan sesudah terkena *blackhole attack*. Pengujian dilakukan dengan variasi jumlah node

penyerang dan variasi luas area. Parameter pengujian yang digunakan adalah dengan cara menghitung nilai *packet loss* yang dihasilkan oleh *node* serangan *blackhole* dan *packet delivery ratio*. Penelitian ini akan dilakukan dengan membuat simulasi jaringan MANET dengan protokol *routing* BATMAN sesuai parameter simulasi. Simulasi dibuat dengan menggunakan *simulator* OMNET++.

2. DASAR TEORI

2.1 *Mobile Adhoc Network*

Mobile Ad-hoc Network (MANET) adalah jaringan nirkabel yang dibentuk secara dinamis oleh sekumpulan *node* yang saling terhubung tanpa menggunakan infrastruktur jaringan yang ada atau administrasi terpusat. Setiap *node* dapat bergerak bebas dan mengatur diri mereka sendiri. Dengan demikian, topologi jaringan MANET dapat berubah secara cepat dan tidak terduga. Pada jaringan MANET, tidak membutuhkan *backbone* infrastruktur karena setiap *node* dapat berfungsi sebagai *router* maupun *client* bagi *node* lainnya (Sarika, 2016). Secara teori, dua *node* yang bergerak dan berada dalam jangkauan transmisi masing-masing dapat berkomunikasi secara langsung, jika tidak, *node* yang berada di antara keduanya harus dapat meneruskan paket agar berhasil berkomunikasi. Arsitektur dari MANET dapat dilihat pada Gambar 1.



Gambar 1 Arsitektur MANET

2.1.1 Karakteristik MANET

Karakteristik utama dari MANET adalah sebagai berikut (Verma, 2016) :

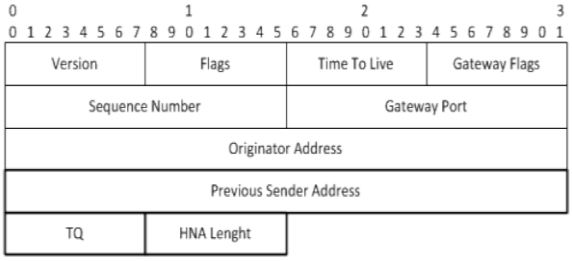
1. MANET bersifat autonomous, artinya tidak ada administrasi terpusat yang bertugas mengelola operasi dari semua *node* yang ada
2. Setiap *node* pada MANET bersifat self organizing dan self managing.
3. MANET tidak membutuhkan backbone infrastruktur atau access point karena setiap *node* nya berkomunikasi dengan metode peer-to-peer.
4. Setiap *node* pada MANET bertindak sebagai *host* dan *router*.
5. Topologi jaringan pada MANET bersifat dinamis dan dapat berubah kapan saja karena setiap *node* dapat bergerak dan keluar masuk kedalam jaringan secara bebas.
6. *Node - node* pada MANET memiliki sumber daya dan kapasitas penyimpanan yang terbatas.
7. MANET rentan terhadap berbagai macam serangan jaringan.

2.2 *Better Approach to Mobile Adhoc Network (*BATMAN*)*

Better Approach to Mobile Ad Hoc Network (BATMAN) adalah suatu protokol *routing proaktif* yang dikembangkan oleh *Freifunk Mesh Community*. Protokol ini merupakan pengembangan dari protokol *routing Optimized Link State Routing* (OLSR). Protokol *routing* BATMAN dikembangkan untuk digunakan pada *Wireless AdHoc Network* termasuk diantaranya adalah *Mobile Adhoc Network* (MANET). Konsep *routing* pada BATMAN adalah menentukan *node* tetangga mana yang merupakan *gateway* terbaik untuk berkomunikasi dengan *node* tujuan. Algoritme *routing* BATMAN hanya melakukan pencarian *best next-hop* untuk setiap *node* yang terdapat pada topologi jaringan tanpa perlu mengetahui jalur keseluruhan untuk mencapai tiap *node* tersebut. Hal ini menjadikan protokol *routing* BATMAN lebih cepat dan efisien (Neumann, 2008).

2.2.1 Format Paket BATMAN

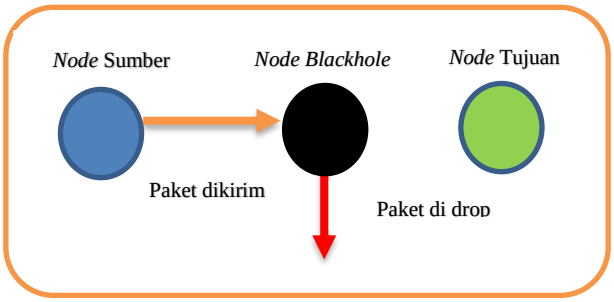
Paket pada BATMAN merupakan paket UDP yang terdiri dari *Originator Message* (OGM) dan bisa juga ditambahkan *Host Network Announcement* (HNA) *message*. HNA *message* digunakan ketika suatu originator ingin mengumumkan bahwa ia terhubung ke jaringan lain atau host lain. Ketika paket OGM di *broadcast* dalam jaringan, paket tersebut akan di enkapsulasi didalam UDP (User Datagram Protocol) datagram. OGM berisi informasi paling penting yang digunakan oleh algoritme *routing* BATMAN dalam proses pembentukkan jalur. OGM memiliki besar paket yang tetap, yaitu 12 oktet. Format paket OGM digambarkan dalam Gambar 2.



Gambar 2 Format paket OGM
Sumber : (Bowitz, 2011)

2.3 *Blackhole Attack*

Serangan *blackhole* atau *blackhole attack* adalah salah satu ancaman atau gangguan pada jaringan MANET yang bersifat menghilangkan atau men-*drop* packet dan data sebelum paket dan data tersebut sampai di tujuan, karena paket di *drop* di *node blackhole* tersebut. *Node* dengan serangan *blackhole* bisa masuk ke dalam jaringan karena sifat dari *node* ini yang menyerupai bahkan sama seperti *node* normal pada umumnya. *Blackhole attack* dibagi menjadi dua jenis yaitu *internal blackhole attack* dan *external blackhole attack. Internal blackhole attack* merupakan jenis serangan *blackhole* dimana *node* penyerang tidak mengganggu proses pencarian jalur pengiriman paket. Namun apabila *node* penyerang dipilih menjadi salah satu *node* perantara pengiriman paket, maka paket tersebut akan langsung di *drop* oleh *node* penyerang. Sedangan *external blackhole attack* merupakan jenis serangan *blackhole* dimana *node* penyerang berusaha untuk mengganggu proses *routing* dengan memaksakan *node* penyerang untuk menjadi salah satu *node* perantara pengiriman paket data (Puray, 2016). Gambar 3 merupakan gambaran dari mekanisme serangan *blackhole.*



Gambar 3. Mekanisme serangan *blackhole*

2.4 *Random Waypoint*

Pergerakan *random way point* memungkinkan *node* bergerak secara acak pada seluruh area simulasi. Setiap *node* adalah independen tanpa terikat satu sama lain. Pemilihan tujuan, kecepatan dan arah akan dilakukan secara acak. Saat mencapai tujuan, setiap *node* akan berhenti sebentar untuk periode waktu yang tetap sebelum mulai bergerak kembali. Waktu berhenti sementara ini disebut pause time. Setelah berada di lokasi untuk durasi waktu selama pause time, mobile *node* akan memilih kembali arah tujuan dan kecepatan secara acak dan bergerak ke arah tujuan baru yang dipilih dengan kecepatan yang ditentukan. Kecepatan pergerakan *node* dan lama waktu *pause time* dapat digunakan untuk mendefinisikan perilaku mobilitas *node*. Kecepatan rendah dan *pause time* yang panjang menghasilkan topologi jaringan yang stabil, sedangkan kecepatan tinggi dan *pause time* yang singkat mengarah ke topologi dinamis (Pandey, 2014)

2.4 *Packet loss*

Packet loss adalah presentase nilai perbandingan jumlah paket yang hilang selama pengiriman dan tidak sampai pada tujuan dengan jumlah paket yang dikirimkan oleh pengirim. *Packet loss* dapat digunakan sebagai parameter untuk menguji kinerja dari suatu jaringan karena memperhitungkan tingkat kegagalan dalam pengiriman data. Secara matematika *packet loss* dapat dihitung dengan rumus berikut (Rohal, 2013) :

$$Packet\ loss = \frac{Packet\ send - Packet\ received}{Packet\ send} \times 100\%$$

2.5 *Packet Delivery Ratio* (PDR)

Packet delivery ratio (PDR) adalah perbandingan jumlah paket yang berhasil sampai pada tujuan dengan jumlah paket yang dikirimkan oleh pengirim. *Packet delivery ratio* dapat digunakan sebagai parameter untuk menguji kinerja dari suatu jaringan karena memperhitungkan tingkat keberhasilan dalam pengiriman data. Secara matematika PDR dapat dihitung dengan rumus berikut (Rohal, 2013):

$$PDR = \frac{Packet\ received}{Packet\ send} \times 100\%$$

3. PERANCANGAN SISTEM

3.1 Perancangan Parameter Simulasi

Pada tahap ini akan dilakukan perancangan parameter – parameter yang akan digunakan dalam simulasi. Parameter simulasi dapat dilihat

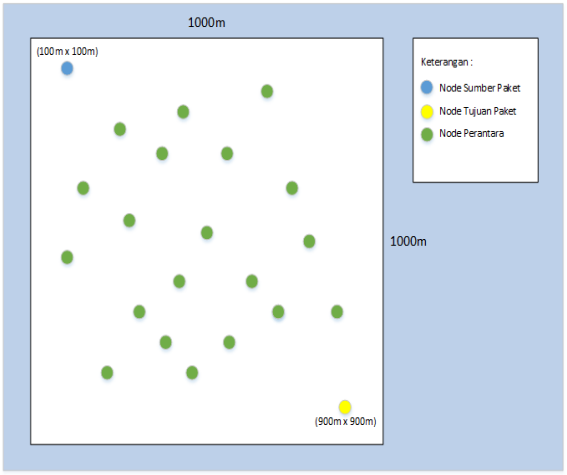
pada Tabel 4.1. Selanjutnya akan dari paramater simulasi yang telah dibuat akan dilakukan perancangan protokol *routing*, perancangan area dan waktu simulasi, perancangan posisi dan pergerakan *node*, perancangan pengiriman data, perancangan posisi *node*, dan perancangan untuk konfigurasi WLAN.

Tabel 3 Parameter simulasi

No	Parameter	Spesifikasi
1.	Network Simulator	OMNET++
2.	*Routing* Protocol	BATMAN
3.	Waktu Simulasi	1000s
4.	Area Simulasi	800x800 m^2, 1000x1000 m^2, 1200x1200 m^2
5.	Jumlah *Node*	30, 40, 50
6.	Jumlah *Malicious node*	5, 15, 20, 25
7.	Model Pergerakan *Node*	*Random Way Point*
8.	Kecepatan Pergerakan *Node*	1 ms
9.	*Pause Time*	15s
10.	Tipe Koneksi	UDP
11.	Besar Paket Data	512 bytes
12.	Sumber/Destination	*Node* 0 / *Node* 1
13.	Protokol WLAN	IEEE 802.11
14.	Bitrate	54 Mbps

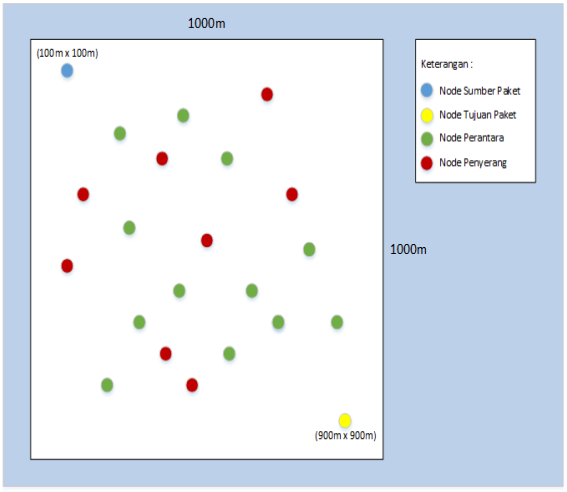
3.2 Perancangan Topologi Jaringan

Perancangan topologi jaringan dilakukan untuk menggambarkan topologi yang akan digunakan pada saat simulasi. Topologi yang digunakan pada simulasi ini dibedakan menjadi dua yaitu topologi tanpa serangan dan topologi dengan serangan *blackhole*. Gambar 4 merupakan perancangan topologi jaringan tanpa serangan dengan luas area simulasi diatur sebesar 1000m x 1000 m^2 sesuai dengan parameter simulasi. *Node* yang berwarna biru merupakan *node* sumber paket sedangkan *node* kuning merupakan *node* tujuan pengiriman paket. *Node* berwarna hijau merupakan *node* perantara untuk meneruskan paket. Posisi awal dari *node* perantara diatur secara acak pada area simulasi. *Node* sumber dan *node* tujuan diatur seperti gambar agar pengujian kinerja protokol *routing* dapat lebih optimal. Apabila *node* sumber dan *node* tujuan diatur berdekatan, maka paket data akan dapat dikirim secara langsung sehingga menjadikan pengujian kinerja protokol *routing* menjadi tidak optimal.



Gambar 4 Topologi tanpa serangan

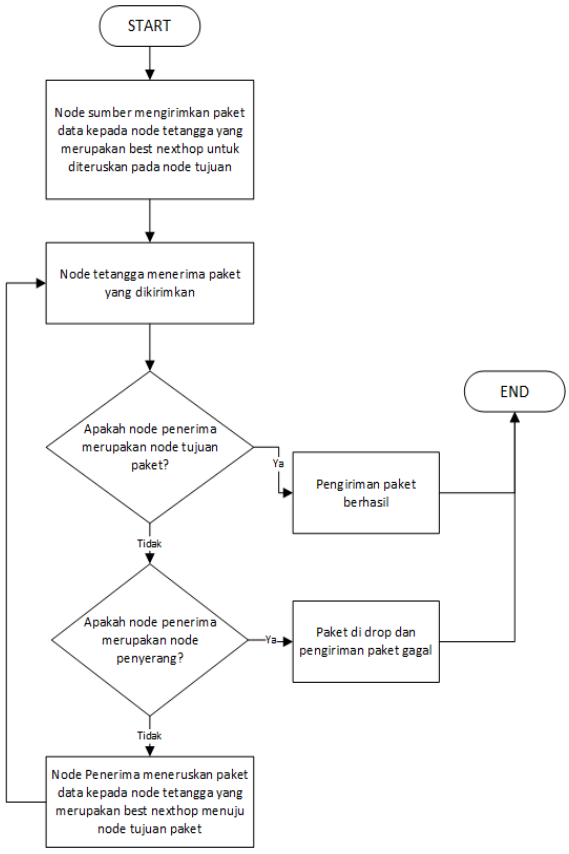
Gambar 5 merupakan perancangan topologi jaringan dengan serangan dengan luas area simulasi diatur sebesar 1000 x 1000 m^2 sesuai dengan parameter simulasi. *Node* yang berwarna biru merupakan *node* sumber paket sedangkan *node* kuning merupakan *node* tujuan pengiriman paket. *Node* berwarna hijau merupakan *node* perantara untuk meneruskan paket dan *node* berwarna merah merupakan *node* penyerang. Posisi awal dari *node* perantara dan *node* penyerang diatur secara acak pada area simulasi. *Node* sumber dan *node* tujuan diatur seperti Gambar agar pengujian kinerja protokol *routing* dapat lebih optimal. Apabila *node* sumber dan *node* tujuan diatur berdekatan, maka paket data akan dapat dikirim secara langsung sehingga menjadikan pengujian kinerja protokol *routing* menjadi tidak optimal.



Gambar 5 Topologi dengan serangan

3.3 Perancangan Serangan *Blackhole*

Perancangan serangan *blackhole* dilakukan untuk mengatur parameter – parameter yang dibutuhkan dalam implementasi serangan *blackhole*. Serangan dilakukan dengan menggunakan NETA *Framework.* Jenis serangan yang digunakan adalah dropping *attack* dengan waktu serangan akan dibuat sesuai waktu simulasi yaitu 1000 detik. Probablitas serangan akan diberi nilai 1 yang berarti semua paket data yang diteruskan melalui *node* penyerang akan di *drop*. Serangan *blackhole* yang digunakan pada simulasi ini adalah serangan dengan jenis internal *blackhole attack*. Pada internal *blackhole attack*, *node* penyerang tidak berusaha untuk masuk kedalam rute pengiriman paket pada jaringan. Namun apabila ada kesempatan di mana paket data diteruskan pada *node* penyerang maka paket tersebut akan di *drop* sehingga tidak sampai pada *node* tujuan. Gambar 6 merupakan flowchart pengiriman data yang akan digunakan pada simulasi ini. Penyerangan hanya dapat terjadi apabila *node* penyerang merupakan salah satu rute pengiriman paket dari *node* sumber paket menuju *node* tujuan paket.



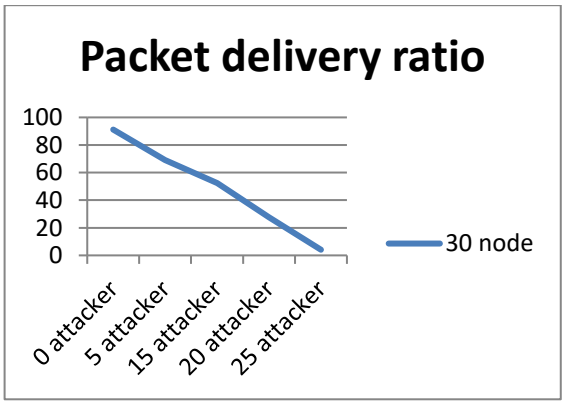
Gambar 6 Alur pengiriman data

4. ANALISIS HASIL PENGUJIAN

Secara umum hasil pengujian menunjukkan serangan *blackhole* dapat menyebabkan penurunan nilai PDR yang cukup signifikan hingga mencapai 0% dengan *packet loss* yang dihasilkan oleh serangan *blackhole* sebesar 92%. Protokol BATMAN menentukan jalur pengiriman paket data dengan cara menentukan *node* tetangga mana yang merupakan *gateway* terbaik untuk menuju *node* tujuan. Apabila *node* dengan serangan *blackhole* dipilih menjadi salah satu *node* perantara untuk mengirimkan paket, maka paket akan di *drop* sehingga tidak akan sampai pada *node* tujuan

4.1 Analisis Penambahan Jumlah Node Penyerang

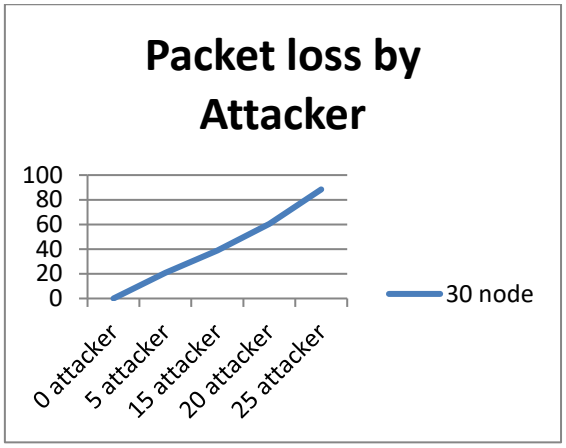
Hasil pengujian PDR dengan jumlah *node* dan luas area yang tetap serta penambahan jumlah *node* penyerang menunjukkan bahwa banyak *node* penyerang berbanding terbalik dengan nilai PDR yang dihasilkan. Jumlah *node* dan luas area simulasi yang tetap menyebabkan posisi *node* sama pada setiap skenario. Semakin banyak jumlah *node* penyerang maka probablitas *node* penyerang dipilih menjadi *node* perantara dalam pengiriman paket akan semakin tinggi. Hal ini menyebabkan nilai PDR yang dihasilkan akan semakin rendah. Gambar 7 menunjukkan grafik perbandingan PDR dengan penambahan jumlah *node* pada skenario 30 *node* dengan luas area 800x800 m.



Gambar 7 PDR 30 *node* 800x800m

Hasil pengujian *packet loss by attacker* dengan jumlah *node* dan luas area yang tetap serta penambahan jumlah *node* penyerang menunjukkan bahwa banyak *node* penyerang berbanding lurus dengan nilai *packet loss* yang dihasilkan. Jumlah *node* dan luas area simulasi yang tetap menyebabkan posisi *node* sama pada setiap skenario. Semakin banyak jumlah *node*

penyerang maka probablitas *node* penyerang dipilih menjadi *node* perantara dalam pengiriman paket akan semakin tinggi. Hal ini menyebabkan nilai *packet loss* yang dihasilkan oleh serangan *blackhole* akan semakin tinggi. Gambar 10 menunjukkan grafik perbandingan *packet loss* yang disebabkan oleh serangan *blackhole* dengan penambahan jumlah *node* penyerang pada skenario 30 *node* dengan luas area 800x800 m.

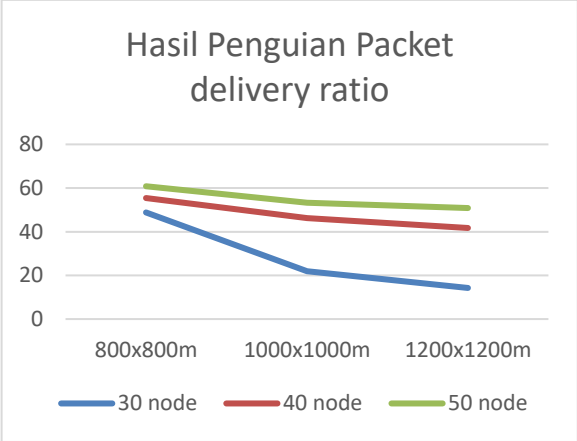


Gambar 8 *Packet loss by attacker* 30 *node* 800x800m

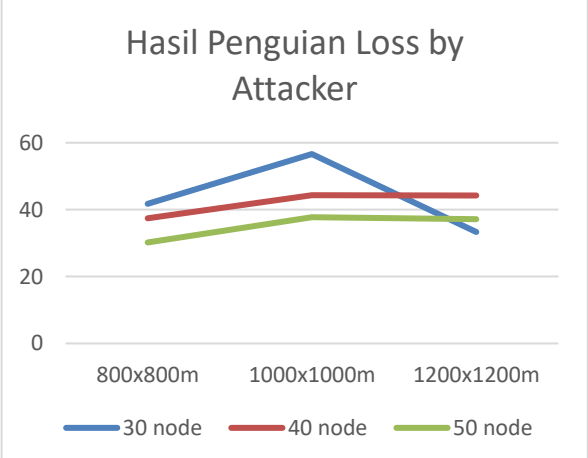
4.2 Analisis Penambahan Luas Area Simulasi

Gambar 9 merupakan grafik perbandingan rata – rata PDR dengan penambahan luas area simulasi. Hasil pengujian menunjukkan bahwa penambahan luas area dapat menurunkan nilai rata - rata *packet delivery ratio* yang dihasilkan. Penurunan nilai PDR disebabkan oleh *node* penyerang, kepadatan *node* dan luas area simulasi. Penambahan luas area dengan jumlah *node* tetap menyebabkan ruang lingkup pergerakan *node* pada simulasi menjadi lebih luas. Luas area simulasi yang bertambah menyebabkan jarak antara *node* menjadi semakin jauh sehingga menyebabkan komunikasi antara *node* terputus. Hal inilah yang menyebabkan banyak paket yang hilang dan nilai PDR menurun.

Penurunan nilai rata - rata PDR tidak membuat nilai rata - rata *packet loss* yang dihasilkan oleh serangan *blackhole* meningkat pada setiap penambahan luas area simulasi. Gambar 6.10 merupakan grafik perbandingan rata – rata *packet loss* yang dihasilkan oleh serangan *blackhole* dengan penambahan luas area simulasi. Hasil pengujian menunjukkan bahwa penambahan luas area simulasi menyebabkan fluktuasi pada nilai *packet loss* yang dihasilkan oleh serangan *blackhole*. Hal ini terjadi karena penambahan luas area mengakibatkan perubahan pada posisi dan ruang lingkup pergerakan *node*, sehingga mempengaruhi dalam pemilihan jalur oleh protokol *routing* BATMAN. Posisi *node* penyerang dalam jaringan sangat mempengaruhi dalam terpilihnya *node* penyerang menjadi salah satu *node* perantara pengiriman data. Semakin dekat posisi *node* penyerang dengan *node* sumber atau *node* tujuan paket, maka semakin besar peluang *node* penyerang untuk terpilih menjadi *node* perantara pengiriman paket data. Hal ini terjadi karena protokol BATMAN menentukkan jalur pengiriman dengan memilih *node* tetangga yang merupakan *best nexthop* menuju *node* tujuan paket. Secara umum dapat disimpulkan bahwa penambahan luas area tidak menjamin peningkatan nilai *packet loss* akibat serangan *blackhole*. Posisi dari *node* penyerang dalam jaringan adalah hal yang paling mempengaruhi keberhasilan serangan yang dilakukan.



Gambar 9 Grafik perbandingan rata - rata PDR



Gambar 10 Grafik perbandingan rata - rata *packet loss*

5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis dari pengaruh serangan *blackhole* terhadap kinerja protokol *routing* pada MANET dapat disimpulkan bahwa :

1. Implementasi serangan *blackhole* pada protokol *routing* BATMAN di jaringan MANET bekerja sesuai dengan mekanisme dan memberikan dampak yang cukup signifikan pada percobaaan yang telah dilakukan. Hasil pengujian menunjukkan rata – rata *packet delivery ratio* paling rendah terdapat pada skenario 30 *node* dengan luas area 1200x1200 m^2 yaitu sebesar 14,24%. Sedangkan nilai rata – rata *packet loss* yang dihasilkan oleh serangan *blackhole* tertinggi terdapat pada skenario 30 *node* dengan luas area 1000x1000 m^2 yaitu sebesar 56,62%.
2. Hasil pengujian dengan jumlah *node* dan luas area yang tetap serta penambahan jumlah *node* penyerang menunjukkan bahwa penambahan jumlah *node* penyerang menyebabkan penurunan pada *packet delivery ratio*. Sementara pada parameter *packet loss*, penambahan jumlah *node* penyerang mampu meningkatkan nilai *packet loss* yang dihasilkan oleh serangan *blackhole*. Protokol BATMAN menentukan jalur pengiriman paket data dengan cara menentukan *node* tetangga mana yang merupakan *gateway* terbaik untuk menuju *node* tujuan. Apabila *node* dengan serangan *blackhole* dipilih menjadi salah satu *node* perantara untuk mengirimkan paket, maka paket akan di *drop* sehingga tidak akan sampai pada *node* tujuan. Semakin banyak jumlah *node* penyerang akan meningkatkan peluang *node* penyerang untuk menjadi salah satu *node* perantara dalam pengiriman paket.
3. Hasil pengujian dengan variasi luas area menunjukkan bahwa penambahan luas area simulasi dapat menurunkan nilai rata - rata *packet delivery ratio* yang dihasilkan. Penambahan luas area dengan jumlah *node* tetap menyebabkan ruang lingkup pergerakan *node* pada simulasi menjadi lebih luas. Luas area simulasi yang bertambah menyebabkan jarak antara *node* menjadi semakin jauh sehingga menyebabkan komunikasi antara *node* terputus. Hal inilah yang menyebabkan banyak paket yang hilang dan nilai PDR menurun. Penurunan nilai rata - rata PDR tidak membuat nilai rata - rata *packet loss* yang dihasilkan oleh serangan *blackhole* meningkat pada setiap penambahan luas area simulasi. Hasil pengujian menunjukkan bahwa penambahan luas area simulasi menyebabkan fluktuasi pada nilai *packet loss* yang dihasilkan oleh serangan *blackhole*. Hal ini terjadi karena penambahan luas area mengakibatkan perubahan pada posisi dan ruang lingkup pergerakan *node*. Posisi *node* penyerang dalam jaringan sangat mempengaruhi dalam terpilihnya *node* penyerang menjadi salah satu *node* perantara pengiriman data. Secara umum dapat disimpulkan bahwa penambahan luas area tidak menjamin peningkatan nilai *packet loss* akibat serangan *blackhole*. Posisi dari *node* penyerang dalam jaringan adalah hal yang paling mempengaruhi keberhasilan serangan yang dilakukan.

5.2 Saran

Saran yang disampaikan untuk penelitian lebih lanjut adalah sebagai berikut :

1. Perlu dilakukan penelitian lebih lanjut dengan model pergerakan yang berbeda dan juga penambahan jumlah *node*.
2. Perlu dilakukan pengujian terhadap terhadap jenis serangan malicious *node* yang berbeda seperti *wormhole, sinkhole,* dan lain-lain.

6. DAFTAR PUSTAKA

Balador, A., 2015. *Network Simulation Using OMNET++*. Department of Computer Systems and Informatics, Halmstad University.

Bowitz, A.G., 2011. Simulation of a Secure Ad Hoc Network Routing Protocol. Norwegian University of Science and Technology Department of Telematics.

Elguzka, D., 2017. Analisis Pengaruh Serangan Blackhole Terhadap Protokol AODV Pada Mobile Ad Hoc Network. Fakultas Ilmu Komputer Universitas Brawijaya

Casado, L.S., Gomez, R.R., Carrion, R.M., Fernandez, G.M., 2013. *NETA: Evaluating the Effects of Network Attacks MANETs as a Case Study*. Dpt. Signal Theory, Telematic and Communications, CITIC, Univ. of Granada.

INET Framework, 2016. *INET Framework for OMNeT++*. Tersedia di: <https://doc.omnetpp.org/inet/api-

3.4.0/inet-manual-draft.pdf>. [Diakses 15 Februari 2018].

Jayanti, V.N., 2014. *Routing Protocols in MANET: Comparative Study*. International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 7, July 2014, pg.119 – 125.

Neumann, A., Aichele, C., Lindner, M. & Wunderlich, B., 2008. *Internet Draft: Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N)*.

Pandey, M.K., Kandari, S., 2014. *Random WayPoint Mobility Model based Performance Estimation of MANET in terms of Average End to End Delay, Jitter and Throughput for CBR Application.* International Journal of Computer Applications (0975 – 8887) Volume 106 – No.3.

Patel, N.J.K., Tripathi, K., 2017. *Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26.* International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169.

Prakash, S., Saini, J.P, Gupta, S.C., 2012. *Methodologies and Applications of Wireless Mobile Ad-hoc Networks Routing Protocols*. International Journal of Applied Information Systems (IJAIS) : Foundation of Computer Science FCS, New York, USA.

Rajaram, A., Palaniswami, S., 2010. *Malicious Node Detection System for Mobile Adhoc Network*. International Journal of Computer Science and Information Technologies, Vol. 1 (2).

Sarika, S., Pravin, A., Vijaykumar, A., Selvamani, K., 2016. *Security Issues in Mobile Ad Hoc Network*. 2nd International Conference on Intelligent Computing, Communication & Convergence

Varga, A., Hornig, R., 2015. *An Overview Of The OMNET++ Simulation Environment*. Budapest: OpenSim Ltd.

Verma, S., 2016. *A Study of Active and Passive Attacks In Manet. IJSRD - International Journal for Scientific Research & Development| Vol. 4, Issue 09, 2016 | ISSN (online): 2321-0613*

Virgi, W. 2107. *Analisis Perbandingan Dampak Serangan Blackhole pada Performansi Protokol Routing OLSR (Optimized Link State Routing) dan AODV (Ad Hoc on Demand Distance Vector) di Jaringan Wireless Mesh Network.* Fakultas Ilmu Komputer Universitas Brawijaya.