Prosiding Nasional Rekayasa Teknologi Industri dan Informasi XIII Tahun 2018 (ReTII)
November 2018, pp. 81~87
ISSN: 1907-5995

Simulasi Dan Analisis Perbandingan Kinerja Teknik Mitigasi Serangan Black Hole Pada Jaringan Manet

Fathullah, Ida Nurcahyani
Jurusan Teknik Elektro, Universitas Islam Indonesia
Korespondensi : 14524135@students.uii.ac.id

ABSTRAK

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

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

ABSTRACT

MANET network is a network which consist of a set of nodes or devices that form a network. MANET is able to communicate wirelessly so that it does not need a fixed network and able to regulate automatically on dynamic and temporary networks. However, MANET network is very vulnerable to attacks, one of which is a black hole attack. A black hole attack is an attack that causes the packets that are sent to disappear. Meanwhile, the black hole node sends a false message to sender node that the packet has arrived at the destination node. Routing protocol is a standard that controls how a node can forward packets between nodes in MANET network. AODV routing protocol is one of the reactive routing protocols. AODV works only if there is a request from a node by sending RREQ messages to the surrounding nodes. This research was made to improve the performances of MANET network when attacked by black hole attacks. The methods that are used to improve the performances are the modification of the bit rates, the number of nodes, and the distance between nodes in the network. The results of this study indicate that by changing the distance between nodes used was able to improve the QoS parameters such as delay, packet delivery ratio (PDR), and throughput. In delay value, it accelerates to 88.56 ms by changing the distance between nodes. For PDR value, it increases to 93.63% when the distance between nodes is closer. While for the throughput value increased to 487.3 kbps when the data rate used was 550 kbps. All of the results obtained show that several methods implemented are proven in improving the performance of the MANET network when exposed to black holes attack.

Keywords: *MANET, AODV, QOS, blackhole.*

1. PENDAHULUAN

Jaringan *Mobile Ad-Hoc* terdiri dari *node* bergerak yang dapat berkomunikasi dengan node lain melalui koneksi nirkabel tanpa infrastruktur tetap. Jaringan *Mobile Ad-Hoc* adalah sistem *node mobile* nirkabel yang mengatur dirinya sendiri dalam topologi jaringan dinamis dan sementara [1]. *Node-node* ini membentuk sebuah jaringan yang berfungsi sebagai jaringan yang bertugas menghubungkan setiap *node*. Setiap *node* yang akan berkomunikasi dengan *fixed host* diwajibkan dahulu melewati gerbang. Metode *gateway discovery* memberikan kemudahan *node* untuk menemukan dan saling berhubung antar *node*.

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

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

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

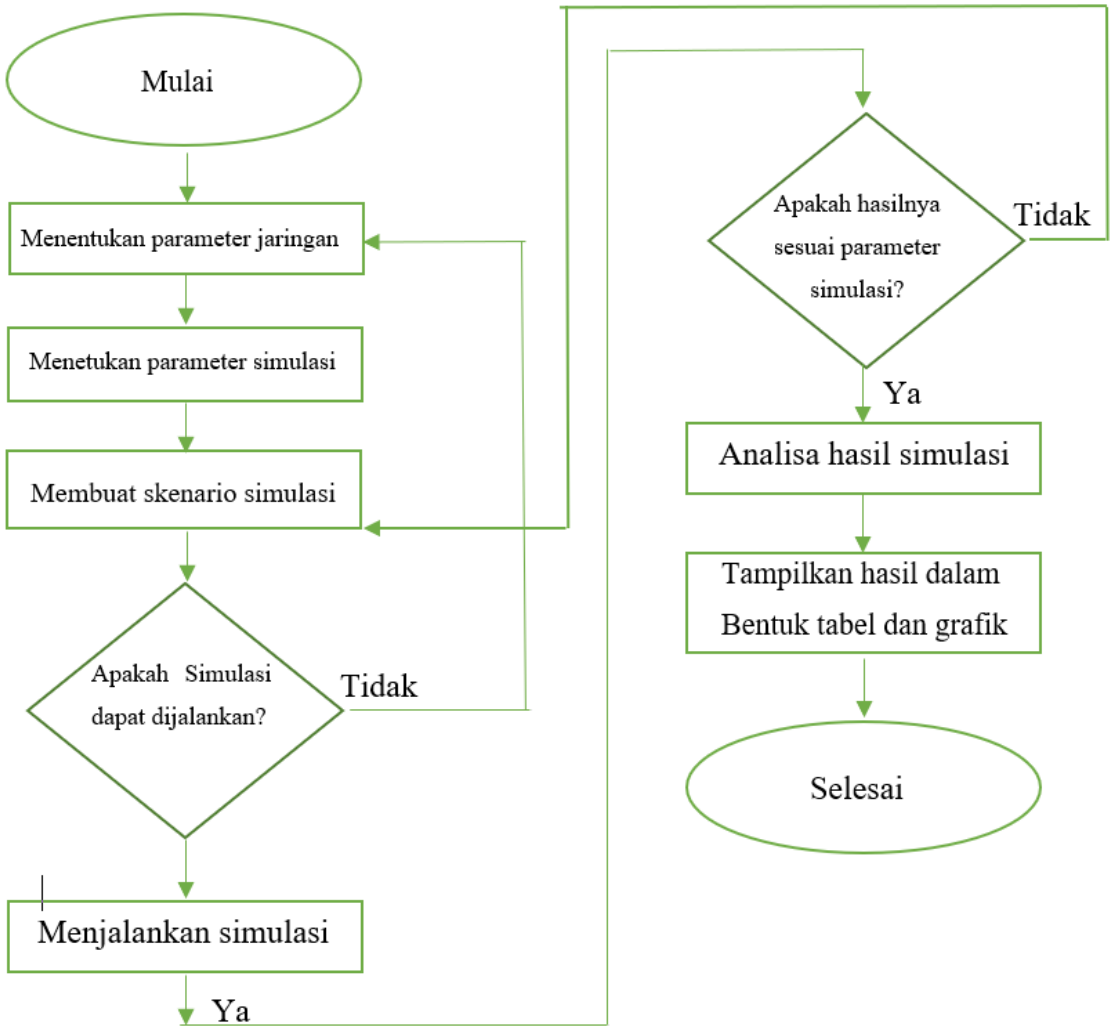
Protokol routing reaktif terbagi menjadi beberapa bagian, salah satunya routing ad hoc On Demand Distance Vector (AODV). AODV adalah protokol routing yang dirancang untuk jaringan bergerak ad hoc. AODV membangun jalur menggunakan rute permintaan atau rute siklus permintaan jawaban. Bila node sumber menginginkan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

2. METODE PENELITIAN

Pada gambar 2.1 dapat dilihat alur pembahasan simulasi yang dilakukan oleh penulis. Pada penelitian ini dilakukan untuk mengetahui parameter apa saja yang dapat memperbaiki kinerja jaringan MANET setelah terkena serangan *Blackhole*. Penulis membagi beberapa percobaan, yaitu tanpa serangan, terkena serangan *blackhole* dan perbaikan dengan jumlah *node* [5], *data rate* [5] dan jarak antar *node* [6]. Pada percobaan yang pertama yaitu tanpa adanya serangan serta parameter dibiarkan *default*. Percobaan selanjutnya, dengan adanya serangan *black hole* serta lainnya dibiarkan *default.* Lalu untuk yang terakhir, percobaan dilakukan dengan merubah beberapa parameter seperti jumlah *node* (30 *node* , 35 *node* , 40 *node*), data rate (350 kbps,400 kbps, 450 kbps, 550 kbps dan 600 kbps) dan jarak antar *node* (30 meter dan 40 meter). Secara *default* parameter pada percobaan ini ditunjukan pada Tabel 2.1 yang terlampir.

Tabel 2.1 Parameter Jaringan

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



Gambar 2. 1 Alur penelitian

Quality Of Service adalah standar untuk mengukur tingkat kualitas jaringan yang digunakan dengan parameter–parameter kualitas dengan metode pengukuran[7]. Pada percobaan ini menggunakan beberapa parameter QOS untuk menguji simulasi jaringan yang dibuat, seperti Packet Delivery Ratio, Delay dan throughput.

a. *Packet Delivery Ratio*

Packet delivery ratio adalah rasio antara jumlah data yang dikirimkan dengan data yang diterima. Untuk menghitung jumlah PDR, dapat menggunakan rumus yang ditunjukan pada persamaan 2.1.

$$PDR = \frac{jumlah\ data\ yang\ diterima}{jumlah\ data\ yang\ dikirim} \times\ 100\% \quad (2.1)$$

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

b. *Delay*

Delay adalah waktu yang digunakan untuk mengirimkan data dari pengirim menuju penerima dihitung dalam satuan waktu. *Delay* mudah dipengaruhi banyak hal, seperti jarak, media yang digunakan, gangguan pada jaringan, atau proses yang membutuhkan waktu lama. Menurut versi TIPHON [8], besarnya delay dapat diklasifikasikan pada Tabel 2.2 berikut ini :

Tabel 2. 2 Klasifikasi *Delay*

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

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

c. *Throughput*

Throughput adalah kecepatan suatu jaringan dalam mentrasmisikan data yang diukur dalam satuan *bit per second. Throughput* merupakan jumlah total paket yang diterima dengan sukses dan dibagi pada interval waktu tertentu [8]. Untuk parameter *throughput* yang digunakan pada penelitian ini adalah sama atau lebih besar dari hasil terkena serangan *black hole*.

Penilitian ini terdapat beberapa skenario simulasi yang diujikan, yaitu

1. Skenario Jumlah *node*

Pada skenario ini, penulis melakukan percobaan untuk memperbaiki kinerja jaringan MANET dengan jumlah node. Percobaan ini, penulis hanya merubah pada sisi jumlah *node* saja sehingga parameter lainnya adalah *default*. Jumlah node yang digunakan yaitu 35 *node,* 40 *node*, dan 25 *node*. Pada tabel 2.3 menunjukan spesifikasi dari jaringan MANET yang digunakan.

Tabel 2. 3 Skenario Jumlah *Node*

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

2. Skenario *data rate*

Pada skenario ini, sama seperti percobaan sebelumnya namun yang berubah adalah parameter data rate dan untuk parameter lainnya *default*. Berikut speksifikasi yang digunakan pada jaringan MANET yang ditunjukan pada tabel 2.4 terlampir.

Tabel 2. 4 Skenario *Data Rate*

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

3. Skenario Jarak Antar *node*

Pada skenario ini, sama seperti percobaan sebelumnya namun yang berubah adalah parameter jarak antar *node*, sedangkan yang lainnya menjadi *default.* Berikut adalah spesifikasi jaringan MANET yang ditunjukan pada Tabel 2.5 yang terlampir.

Tabel 2.5 Skenario Jarak Antar *Node*

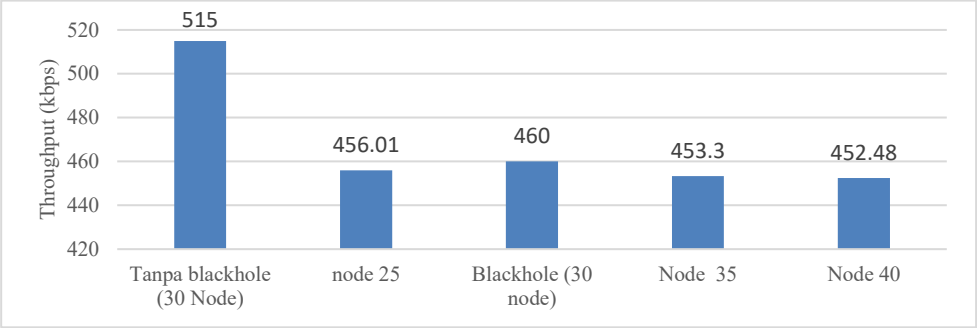
No	Parameter	Nilai
1	Luas Area	1000x1000 meter
2	Perubahan jarak antar *node*	30 meter 40 meter
3	Jumlah *node* normal	26 *node* + 1 *Server*
4	Jumlah *node black hole*	3 *node*
5	D*ata rate*	500 kbps
6	Ukuran paket	512 bit
7	Aplikasi jaringan	CBR

3. HASIL DAN ANALISIS

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

3.1. Variasi Jumlah *Node*

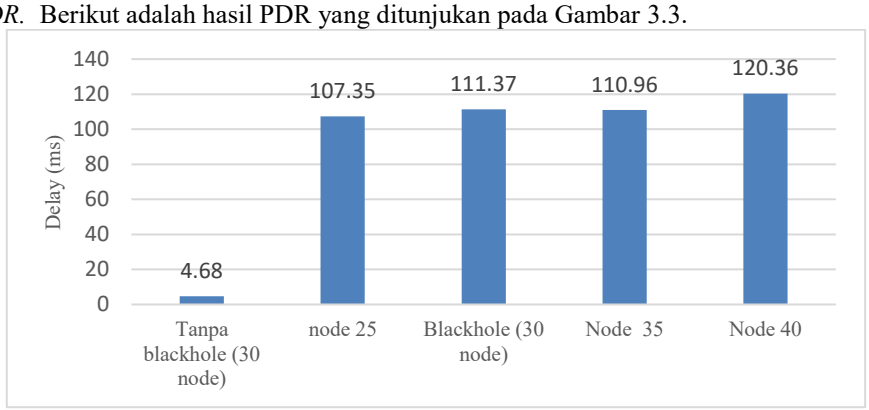
Hasil dari pengamatan *Throughput* yang dihasilkan simulator terlihat pada Gambar 3.1.



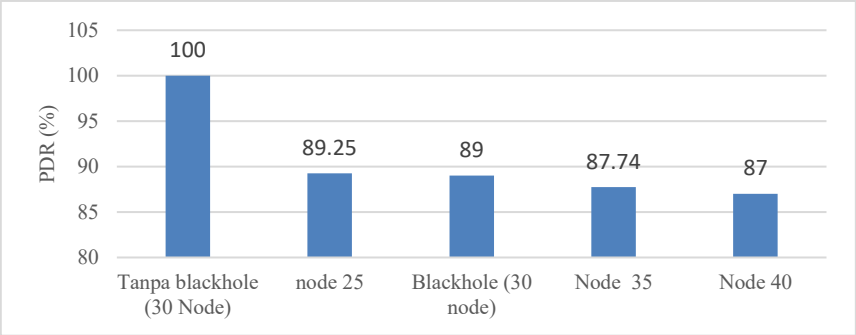
Gambar 3. 1 *Throughput* Jumlah *Node*

Hasil dari pengamatan *Throughput* yang dihasilkan simulator terlihat pada Gambar 4.1. Hasil keluaran *Throughput* dari masing-masing skenario ini memiliki hasil yang berbeda-beda. Pada kondisi normal menghasilkan throughput sebesar 515 kbps, sedangkan pada saat terkena serangan black hole turun menjadi 460,01 kbps. Hal ini terjadi karena node Black hole membuat dropping setiap ada paket yang melewatinya [9]. Selanjutnya, penulis mengganti jumlah node yang digunakan. Terlihat bahwa penambahan jumlah node mengakibatkan penurunan throughput. Menambah jumlah node mengakibatkan kongesti pada jaringan MANET, sehingga throughput menjadi turun [5], namun saat jumlah node diturunkan menjadi 25 node , terjadi peningkatan dibandingkan penambahan node , tapi tidak lebih baik dari kondisi normal terkena serangan black hole.

Selanjutnya adalah delay. Saat kondisi normal, menghasilkan sebesar 4,6 ms, namun saat terkena serangan black hole, Delay meningkat menjadi 111,37 ms. Sedangkan saat penulis mengganti jumlah *node* menjadi 40 *node , delay* menjadi meningkat menjadi 120,36 ms, mengalami peningkatan sebesar 8,99 ms. Hal ini diakibatkan karena adanya *congestion* pada jaringan, namun ketika diturunkan menjadi 35 *node* dan 25 *node* hasil yang diperoleh juga ikut turun. Hasil ditunjukan pada Gambar 3.2 yang terlampir. Yang terakhir yaitu hasil *PDR.* Berikut adalah hasil PDR yang ditunjukan pada Gambar 3.3.



Gambar 3. 2 *Delay* Jumlah *node*

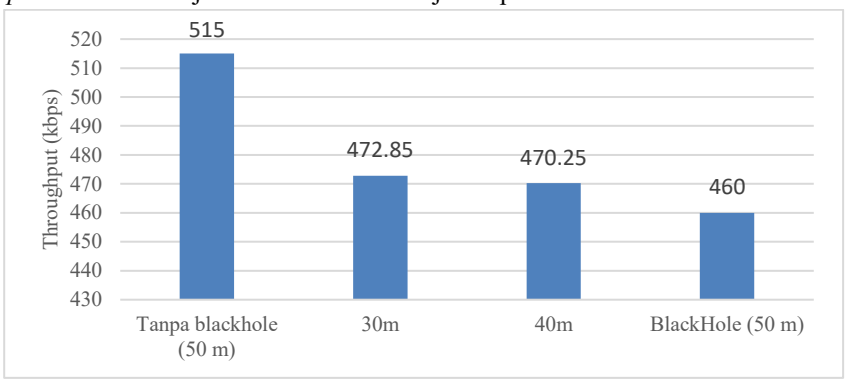


Gambar 3. 3 PDR Jumlah *Node*

Terlihat pada gambar, saat kondisi normal tanpa adanya serangan *PDR* sebesar 100%. Namun saat terkena serangan, drop 11% menjadi 89%. Akan tetap, saat jumlah *node* dikurangi, *PDR* meningkat menjadi 89,25%, lalu saat jumlah ditambahkan, PDR semakin turun menjadi 87% saat 40 *node* . Hal ini disebabkan karena serangan *black hole* menurunkan jumlah maksimum paket dari *node* yang dekat dengannya [10].

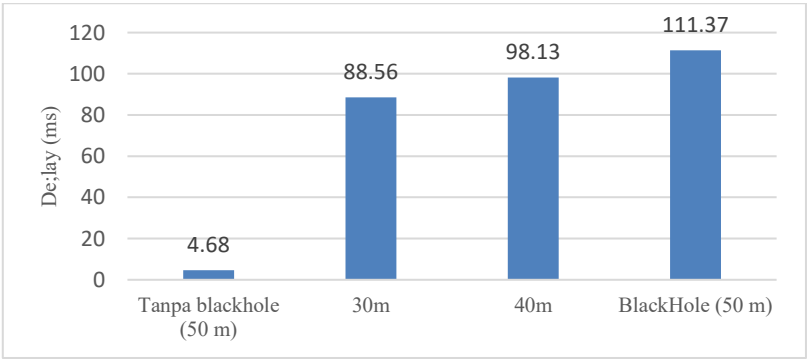
3.2. Variasi Jarak Antar *Node*

Data *throughput* dari skenario jarak antar *node* ditunjukan pada Gambar 3.4.



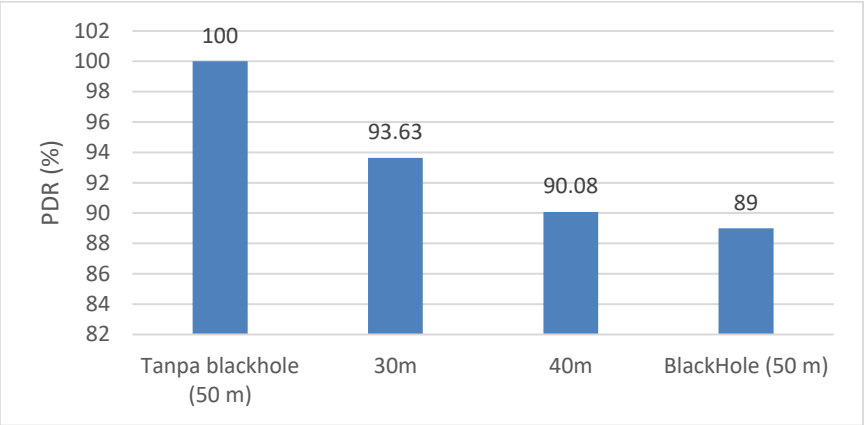
Gambar 3. 4 *Throughput* Jarak Antar *Node*

Saat kondisi normal tanpa serangan, *Throughput* sebesar 515 kbps. Terjadi penurunan ketika terkena serangan sebesar 56 kbps. Saat jarak antar *node* dikecilkan menjadi 30 meter, terjadi perningkatan menjadi 472,85 kbps. Namun, jika dibandingkan dengan 50 meter hasilnya terjadinya peningkatan. Hal ini dipengaruhi dengan semakin dekatnya jarak antar *node* Selanjutnya hasil *delay.* Berikut adalah *delay* jarak antar *node* yang ditunjukan pada Gambar 3.5.



Gambar 3. 5 *Delay* Jarak Antar *Node*

Terlihat pada gambar, saat kondisi normal tanpa serangan *delay* sebesar 4,68 ms. Pada saat terkena serangan, *delay* meningkat 107,06 ms. Sama seperti hasil *throughput*, saat jarak dikecilkan menjadi 30 meter, hasilnya *delay* turun sebesar 88,56 ms.Hal ini disebabkan semakin dekat sehingga *delay* semakin rendah. Selanjutnya hasil *PDR* jarak antar *node* . Berikut adalah hasil dari *PDR* yang ditunjukan pada Gambar 3.6.



Gambar 3. 6 PDR Jarak Antar *Node*

4. KESIMPULAN

Serangan black hole pada jaringan MANET mengakibatkan penurunan kinerja. Indikasi penurunan terlihat pada parameter QOS, yaitu PDR, delay, dan throughput. Pada PDR, menurun sekitar 11%; pada delay meningkat sekitar 95 ms, dan pada throughput menurun sekitar 56 kbps.

Pengubahan node, jarak antar node dan data rate mampu memperbaiki kinerja jaringan MANET yang terkena serangan black hole. Mengubah node mengakibatkan delay menurun menjadi 107 ms. Mengubah jarak antar node yang digunakan mampu meningkatkan throughput menjadi 472 kbps, packet delivery ratio 93,63% dan delay menjadi 88,56 ms.. Sedangakan mengubah data rate mampu meningkatkan throughput menjadi 487 kbps dan delay menjadi 87 ms. Metode pengubahan jarak antar node mempunyai kinerja terbaik.

DAFTAR PUSTAKA

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

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

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

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

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

[6] M. Arif, B. Aji, and A. A. Zahra, "Evaluasi Kinerja Protokol Routing DSDV Terhadap Pengaruh Malicious Node Pada Manet Menggunakan Network Simulator 2 (Ns-2)," vol. 2.

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

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

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

[10] D. Gaurav, "Performance Evaluation of AODV with and without Black hole Attack in MANETs," no. June, pp. 7–13, 2016.