Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 3, No. 3, Maret 2019, hlm. 2693-2701 http://j-ptiik.ub.ac.id

Dampak Serangan *Black Hole* Terhadap Protokol *Routing Destination-Sequenced Distance Vector* (DSDV) Dengan Model Mobilitas *Random* Pada MANET

Asroful Khusna Arifianto[1], Rakhmadhany Primananda[2], Reza Andria Siregar[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]asrofulkhusna11@gmail.com, [2]rakhmadhany@ub.ac.id, [3]rezaandria.s@gmail.com

Abstrak

Mobile ad hoc network (MANET) merupakan jaringan *nirkabel* yang terdiri dari *mobile node* dan memiliki infrastruktur tidak tetap. Dengan tidak adanya infrastruktur tetap pada MANET menyebabkan *node* memiliki pergerakan yang berubah-ubah. *Node* pada MANET dapat masuk dan keluar dalam jaringan secara bebas, hal ini menyebabkan MANET rentan terhadap serangan. Salah satu serangan yang ada pada MANET adalah serangan *black hole*. Pada penelitian ini menggunakan protokol *routing destination-sequenced distance vector* (DSDV) serta model mobilitas *random waypoint* dan *random direction*. Parameter simulasi pada penelitian ini adalah luas area 1000x1000m^2, 700x700m^2, 500x500m^2, jumlah *node* 40, 50, 60 *node* dengan *node black hole* 5, 10, 15 dan 20 *node black hole*. Penelitian ini bertujuan untuk mengetahui dampak serangan *black hole* terhadap protokol *routing* DSDV pada jenis mobilitas model *random*. Parameter uji yang digunakan adalah *paket delivery ratio, average end-to-end delay* dan *normalized routing load*. Berdasarkan hasil pengujian yang dilakukan didapatkan kesimpulan bahwa pada luas area 1000x1000m^2 dan 700x700m^2 protokol *routing* DSDV pada *random waypoint* memiliki dampak lebih besar daripada protokol *routing* DSDV pada *random direction*. Pada luas area 500x500m^2 protokol *routing* DSDV pada *random direction* memiliki dampak lebih besar dibanding protokol *routing* DSDV pada *random waypoint*.

Kata kunci: *Mobile Ad-Hoc Network*, DSDV, *Black Hole*, Model Mobilitas *Random*

Abstract

Mobile ad hoc network (MANET) is a wireless network that consists of a mobile node and has a non-fixed infrastructure. In the absence of a fixed infrastructure in MANET causes the node has an arbitrary movement. The MANET node can enter and exit the network freely, this causes MANET to be vulnerable to attacks. One of the attacks on MANET was a black hole attack. In this study using destination-sequenced distance vector (DSDV) routing as well as random waypoint mobility models and random direction models. The simulation parameters in this study are the area of 1000x1000m^2, 700x700m^2, 500x500m^2, number of nodes 40, 50, 60 nodes with 5, 10, 15 and 20 black hole nodes. This study aims to determine the impact of black hole attacks on the DSDV routing protocol on random model mobility. The test parameters used are delivery ratio packages, average end-to-end delay, and normalized routing load. Based on the results of tests conducted, it was concluded that in the area of 1000x1000m^2 and 700x700m^2 the DSDV routing protocol on random waypoints had a greater impact than the DSDV routing protocol in a random direction. In the area of 500x500m^2, the DSDV routing protocol in random direction has a greater impact than the DSDV routing protocol at random waypoints.

Keywords: *Mobile Ad-Hoc Network, DSDV, Black Hole, Random Mobility Model*

1. PENDAHULUAN

Mobile ad hoc network (MANET) merupakan jaringan *nirkabel* yang terdiri dari *mobile node* dan memiliki infrastruktur tidak tetap. Tidak adanya infrastruktur yang tetap, *node* pada MANET memiliki pergerakan yang berubah-ubah.(Natarajan & Mahadevan, 2017).

Untuk mengatasi pergerakan *node* yang berubah-ubah diperlukan sebuah protokol *routing* untuk mengatur pengiriman paket pada jaringan MANET. Ada tiga jenis protokol *routing* pada MANET yaitu reaktif *routing* (*on*

demand), proaktif *routing* (Tabel *routing*) dan Hybrid *routing*. Salah satu protokol *routing* proaktif yang ada pada MANET adalah *destination-sequenced distance vector* (DSDV), protokol tersebut merupakan pengembangan dari algoritme *bellman-ford*. Protokol DSDV melakukan *broadcast message* ke seluruh *node* terdekat untuk mendapatkan informasi jalur pengiriman paket serta memanfaatkan *sequence number* agar tidak terjadi *routing loop* pada jaringan (Aji, et al., 2015).

Salah satu tantangan yang ada pada MANET adalah masalah keamanan. *Node* pada MANET dapat masuk dan keluar dalam jaringan secara bebas, yang menyebabkan MANET rentan terhadap serangan. Salah satu jenis serangan aktif yang ada pada MANET adalah serangan *black hole*. Serangan *black hole* adalah serangan yang menyerang *layer network* dan bekerja dengan melakukan *drop* pada paket data yang diterima (Puray & Palod, 2016).

Untuk melakukan simulasi pada MANET diperlukan sebuah model mobilitas atau pola pergerakan yang merepresentasikan setiap *node*. Salah satu model mobilitas yang ada pada MANET adalah model mobilitas *random*. Beberapa pergerakan yang ada pada model mobilitas *random* adalah model mobilitas *random waypoint* dan model mobilitas *random direction*. Kedua model mobilitas *random* tersebut memiliki perbedaan pergerakan *node* selama simulasi berjalan, mobilitas *random waypoint* memiliki pola pergerakan yang cenderung berkumpul di satu area simulasi sehingga dapat menyebabkan penumpukan *node* pada suatu area simulasi. Lalu model mobilitas *random direction* memiliki pola yang cenderung bergerak ke tepi area simulasi untuk menghindari permasalahan penumpukan *node* pada suatu area simulasi yang dihasilkan oleh mobilitas *random waypoint* (Das, et al., 2014).

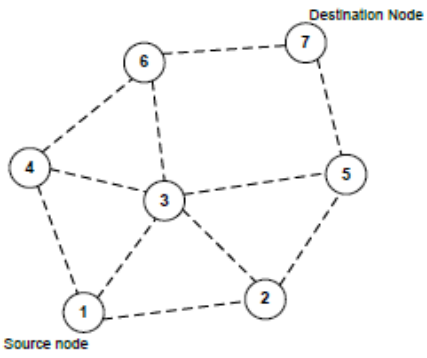
Pada penelitian sebelumnya yang berjudul "*Performance Analysis of DSDV, AODV and ZRP under Blackhole attack*" membahas tentang perbandingan performa protokol *routing* DSDV, AODV dan ZRP saat terdapat serangan *black hole* (Arora & Barwar, 2014). Penelitian yang berjudul "*Evaluation of Performance of AODV over DSDV Protocol using Blackhole attack in MANET*" yang membahas tentang perbandingan protokol *routing* AODV dan DSDV pada saat terkena serangan *black hole* (Sharma & Renu, 2013). Penelitian yang berjudul "*Evaluasi Kinerja Protokol Routing DSDV Terhadap Pengaruh Malicious Node Pada MANET Menggunakan Network simulator 2 (NS-2)*" membahas tentang pengaruh kinerja protokol *routing* DSDV terhadap *malicious node* (Aji, et al., 2015). Dari ketiga penelitian diatas dapat disimpulkan bahwa terdapat penurunan performa protokol *routing* pada saat terjadi serangan.

Berdasarkan permasalahan tersebut maka dilakukan penelitian untuk mengetahui dampak serangan blackhole pada kinerja protokol *routing* DSDV. Pada penelitian terdapat dua jenis model mobilitas *random* yang digunakan, yaitu model *random waypoint* dan model *random direction*. Variasi *node* yang dipakai adalah 40, 50, 60 *node* dan variasi *node black hole* 5, 10, 15, 20 *node black hole* serta variasi luas area simulasi 500x500m^2, 700x700m^2, 1000x1000m^2. Parameter yang diuji adalah *paket delivery ratio*, *average end-to-end delay* , *normalized routing load*. Diharapkan dengan adanya penelitian yang dilakukan ini dapat mengetahui dampak serangan *black hole* terhadap protokol *routing* DSDV pada jenis mobilitas *random waypoint* dan *random direction.*

2. DASAR TEORI

2.1 *Destination-sequenced distance vector* (DSDV)

DSDV merupakan algoritma protokol *routing ad hoc* proaktif yang didasari pada Bellman – Ford. Pada DSDV, digunakan *sequence number* untuk mengirimkan pesan pada jaringan. *Sequence number* dihasilkan juga saat ada perubahan dalam jaringan. (Sunita & Makkar, 2014).



Gambar 1. Skenario protokol DSDV
Sumber: (Arora & Barwar, 2014).

Setiap *node* pada *routing* protokol DSDV mengelola tabel *routing* secara individu. Dimana setiap *node* memiliki informasi berupa *destination*, next *hop*, *matric* dan *Sequence number* pada tabel *routing* tersebut. Dengan perincian tabel *routing* tersebut, tabel *routing* juga melacak next *hop* untuk mendapatkan tujuan dari *node* tersebut. (Arora & Barwar, 2014).

Tabel 1. *Routing* tabel *node* 1

Destination	*Next Hop*	*Matric*	*Sequence number*
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

Sumber: (Arora & Barwar, 2014).

Pada protokol routing DSDV, setiap node memelihara tabel routing ke node tetangganya. Tabel routing setiap node berisi informasi: alamat tujuan *node*, jumlah *hop* ke tujuan, serta sequenced number. Jika tabel *routing* dalam satu *node* telah diupdate, maka dipilih rute untuk mencapai *node* tujuan dengan beberapa pertimbangan sebagai berikut :

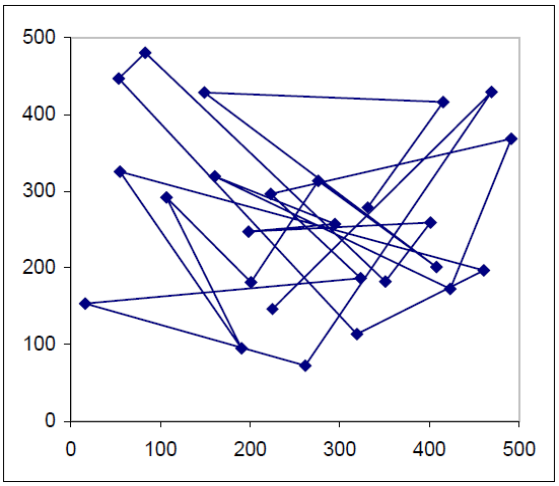
a. Memiliki *sequence number* yang terbaru, hal ini dapat dilihat dari nilai *sequenced number* yang paling besar.

b. Jika nilai *sequence number* sama, maka dilihat nilai *metric*-nya, nilai *metric* yang lebih kecil akan dipilih.

2.2 Serangan *Black Hole*

Serangan *black hole* adalah serangan yang menyerang *layer network* dan bekerja dengan melakukan *drop* pada paket data yang diterima. Terdapat 2 jenis serangan *black hole* pada MANET, yaitu internal *black hole* dan eksternal *black hole*. Internal *black hole* merupakan jenis serangan *black hole* yang melakukan *drop* pada paket tanpa menggangu proses *routing*. *Node black hole* melakukan *drop* paket jika melalui node tersebut. Eksternal *black hole* merupakan jenis serangan *black hole* yang melakukan *drop* paket dengan memanipulasi *node* dalam jaringan, sehingga menggangu proses *routing* protokol. *Node black hole* mengirimkan *route reply* palsu yang menyatakan bahwa *node* tersebut merupakan jalur pengiriman tercepat ke tujuan (Puray & Palod, 2016).

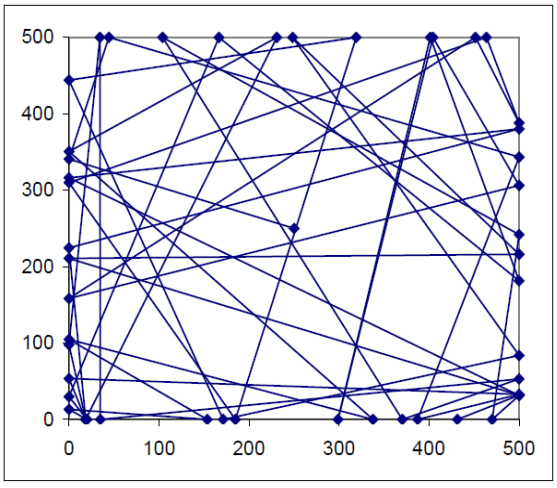
2.3 Random Waypoint Model



Gambar 2. *Random waypoint* model
Sumber: (Saad & Zukarnain, 2009).

Model mobilitas *random waypoint* dimulai dengan *mobile node* diam di satu lokasi untuk jangka waktu tertentu (yaitu, waktu jeda). Setelah waktu ini berakhir, *mobile node* memilih tujuan acak serta kecepatan yang terdistribusi secara merata antara [0, MAXSPEED]. Kemudian perjalanan menuju tujuan yang baru dipilih pada kecepatan yang dipilih. Setelah tiba, *mobile node* berhenti lagi sebelum memulai prosesnya lagi (Saad & Zukarnain, 2009). Mobilitas *random waypoint* memiliki pola pergerakan yang cenderung berkumpul di satu area simulasi sehingga dapat menyebabkan penumpukan *node* pada suatu area simulasi (Das, et al., 2014).

2.4 Random Direction Model



Gambar 3. *Random direction* model
Sumber: (Saad & Zukarnain, 2009).

Random direction model diciptakan untuk mengatasi kekurangan yang ditemukan pada model mobilitas *random waypoint*. Dalam

model ini, *Mobile Node* memilih arah acak untuk melakukan perjalanan dengan tujuan yang acak. Setelah memilih arah acak, sebuah *Mobile Node* melakukan perjalanan ke perbatasan area simulasi ke arah itu. Begitu mencapai batas area simulasi m*obile node* berhenti untuk jangka waktu tertentu, pilihlah arah sudut yang lain (antara 0 dan 180 derajat) dan melanjutkan prosesnya (Saad & Zukarnain, 2009). Sehingga tidak terjadi penumpukan node seperti yang terjadi pada *random waypoint*.

3. PERANCANGAN

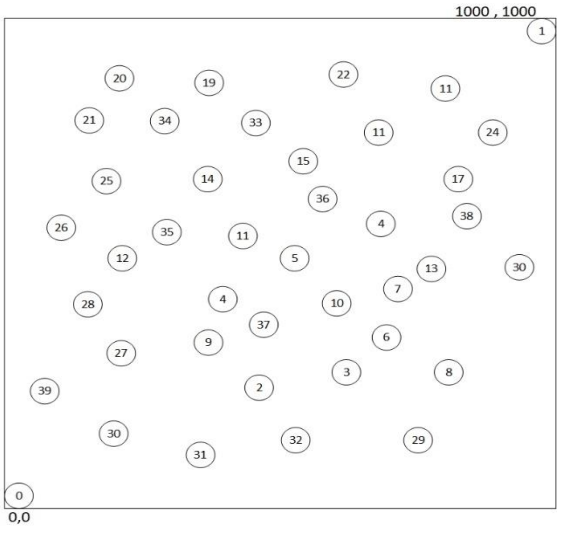
Perancangan pada penelitian dilakukan dengan menggunakan *network simulator* 2 yang terdapat pada sistem operasi berbasis *linux*.

Tabel 2. Skenario simulasi

Parameter Simulasi	Nilai
Luas	500x500m^2, 700x700m^2, 1000x1000m^2
Kecepatan *Node*	0-2 m/s
Node Black hole	5 *node*, 10 *Node*, 15 *Node*, 20 *Node*
Jumlah *Node*	40 *node*, 50 *node*, 60 *Node*
Model Mobilitas	*Random waypoint* model, *Random direction* model
Waktu Simulasi	1000 detik
Tipe trafik	UDP
Simulator	*Network simulator* 2

Perancangan skenario simulasi ini bertujuan untuk memberikan gambaran secara garis besar tentang sistem yang akan dirancang pada penelitian. Sistem dirancang dan di implementasikan dengan *software Network simulator* 2.

3.1 Perancangan Topologi jaringan

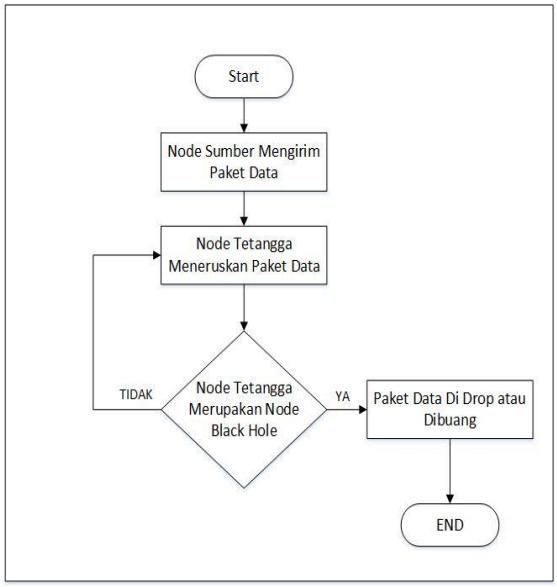


Gambar 4. Perancangan Topologi Jaringan

Pada perancangan topologi menggambarkan topologi yang dibuat pada penelitian ini. Dimana topologi jaringan terdiri dari variasi luas area 500x500m^2, 700x700m^2 dan 1000x1000m^2. Pada variasi luas area tersebut terdapat juga variasi jumlah *node* dalam simulasi yaitu 40 *node*, 50 *node* dan 60 *node* serta terdapat variasi *node black hole* pada variasi jumlah *node* tersebut. Variasi jumlah *node black hole* yaitu 5, 10, 15 dan 20 *node black hole*.

3.2 Perancangan Serangan *Black Hole*

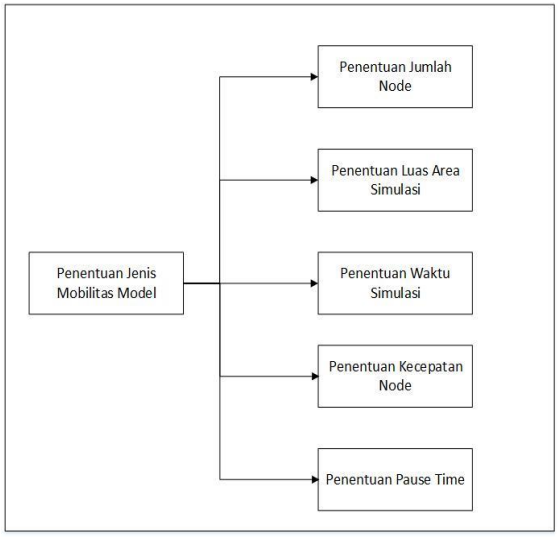
Pada penelitian ini tipe serangan *black hole* yang digunakan adalah internal *black hole* dimana *node black hole* berperilaku seperti *node* biasa pada proses pembentukan *routing*. Setalah proses *routing* selesai dan route atau jalur *routing* ke *node* tujuan terbentuk maka paket data dikirim. Paket data yang melalui *node black hole* di *drop* atau dibuang sehingga paket tidak sampai pada *node* tujuan.



Gambar 5. Perancangan serangan *black hole*

3.3 Perancangan Mobilitas *Node*

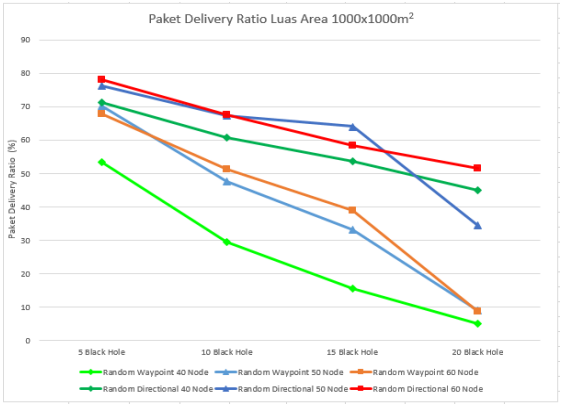
Pola pergerakan pada penelitian ini dibuat oleh suatu *software* yang bernama *bonnmotion*. Pada *boonmotion* diperlukan beberapa parameter untuk membuat pola pergerakan yang diinginkan seperti jumlah *node*, luas area, waktu simulasi, kecepatan *node*, dan pause time. Parameter yang dibutuhkan tergantung dari jenis mobilitas yang dibuat. Terdapat dua jenis mobilitas pada penelitian ini yaitu mobilitas *random waypoint* dan mobilitas *random direction*.



Gambar 6. Perancangan mobilitas *node*

4. PENGUJIAN DAN ANALISIS

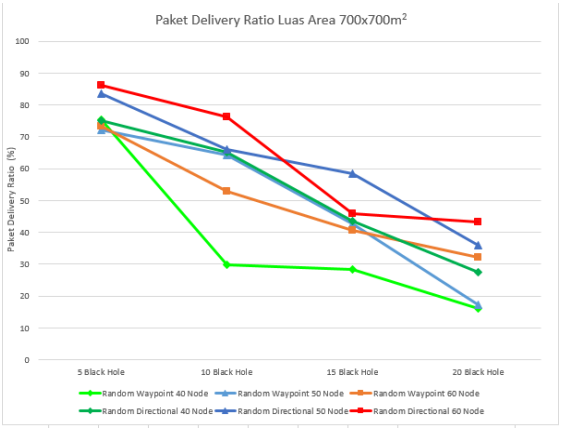
4.1 Analisis Pengujian *Paket delivery ratio* pada Luas Area 1000x1000m^2



Gambar 7. Pengujian *paket delivery ratio* pada luas area 1000x1000m^2

Gambar 7 menggambarkan nilai *paket delivery ratio* pada jenis mobilitas *random waypoint* dan *random direction* pada skenario jumlah *node* 40, 50, 60 *node* dan variasi serangan balck hole 5, 10, 15, 20 *node black hole* dengan luas area 1000x1000m^2. Secara umum terdapat penurunan nilai *paket delivery ratio* pada setiap penambahan *node black hole* pada jaringan. Hal ini dikarenakan semakin bayaknya jumlah *node black hole* semakin tinggi pula *ratio* paket di *drop* atau dibuang. Pada pergerakan *random waypoint* terdapat penurunan nilai *paket delivery ratio* cukup signifikan. Hal ini disebabkan karena *node* bergerakan ke suatu area simulasi sehingga menyebabkan penumpukan *node* pada area tersebut. Hal tersebut memungkinkan probabilitas terpilihnya *node black hole* sebagai *node* perantara pengiriman data semakin tinggi.

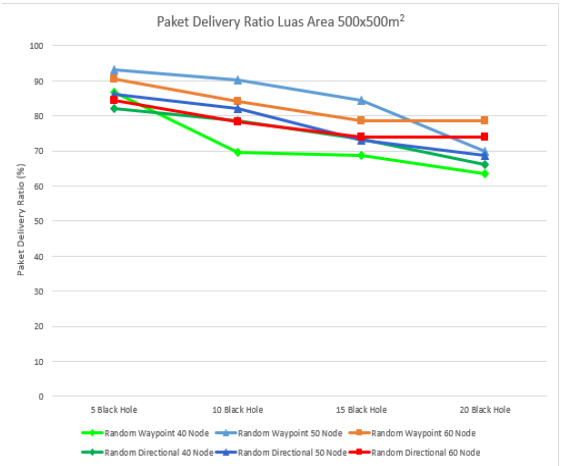
4.2 Analisis Pengujian *Paket delivery ratio* pada Luas Area 700x700m^2



Gambar 8. Pengujian *paket delivery ratio* pada luas area 700x700m^2

Gambar 8 menggambarkan nilai *paket delivery ratio* pada jenis mobilitas *random waypoint* dan *random direction* pada skenario jumlah *node* 40, 50, 60 *node* dan variasi serangan balck hole 5, 10, 15, 20 *node black hole* dengan luas area 700x700m^2. Secara umum terdapat penurunan nilai *paket delivery ratio* pada setiap penambahan *node black hole* pada jaringan. Hal ini dikarenakan semakin bayaknya jumlah *node black hole* semakin tinggi pula *ratio* paket di *drop* atau dibuang. Pada pergerakan *random waypoint* terdapat penurunan nilai *paket delivery ratio* cukup signifikan. Hal ini disebabkan karena *node* bergerakan ke suatu area simulasi sehingga menyebabkan penumpukan *node* pada area tersebut. Hal tersebut memungkinkan probabilitas terpilihnya *node black hole* sebagai *node* perantara pengiriman data semakin tinggi.

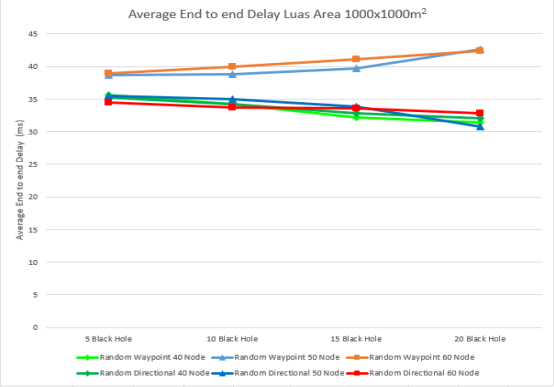
4.3 Analisis Pengujian *Paket delivery ratio* pada Luas Area 500x500m^2



Gambar 9. Pengujian *paket delivery ratio* pada luas area 500x500m^2

Gambar 9 menggambarkan nilai *paket delivery ratio* pada jenis mobilitas *random waypoint* dan *random direction* pada skenario jumlah *node* 40, 50, 60 *node* dan variasi serangan balck hole 5, 10, 15, 20 *node black hole* dengan luas area 500x500m^2. Secara umum terdapat penurunan nilai *paket delivery ratio* pada setiap penambahan *node black hole* pada protokol routing DSDV. Hal ini dikarenakan semakin bayaknya jumlah *node black hole* semakin tinggi pula *ratio* paket di *drop* atau dibuang. Pada luas area 500x500m^2 nilai *paket delivery ratio* cenderung lebih stabil dibanding pada luas area 1000x1000m^2 dan 700x700m^2. Pada luas area 500x500m^2 penurunan tidak terlalu signifikan seperti pengujuan pada luas area 1000x1000m^2 dan 700x700m^2.

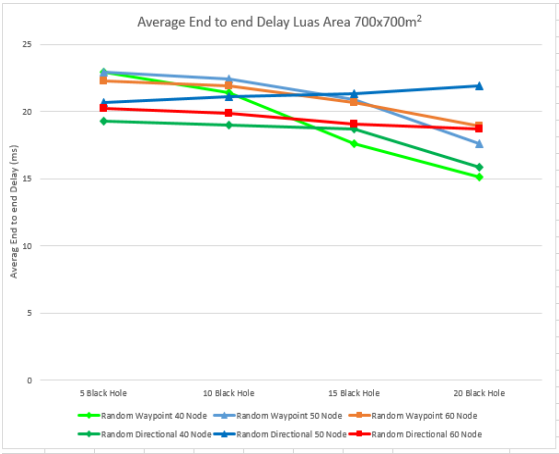
4.4 Analisis Pengujian *Average end-to-end delay* pada Luas Area 1000x1000m^2



Gambar 10. Pengujian *average end-to-end delay* pada luas area 1000x1000m^2

Gambar 10 menggambarkan nilai *average end-to-end delay* pada *random waypoint* dan *random direction* dengan scenario jumlah *node* 40, 50 dan 60 *node* dengan luas area 1000 x 1000 m^2 dan variasi 5, 10, 15 dan 20 *node black hole*. Nilai *average end-to-end delay* dipengaruhi oleh jumlah *hop* atau *node* yang dilewati saat pengiriman paket. Selain itu jarak antar *node* dan luas area simulasi mempengahi besar nya nilai *delay* dari tiap paketnya. Nilai *average end-to-end delay* dihitung dari *delay* jumlah paket yang sampai ke tujuan sehingga paket yang di *drop* oleh *node black hole* tidak dihitung. Pada *random waypoint* 50 *node* dan 60 *node* nilai *average end-to-end delay* mengalami kenaikan. Hal ini disebabkan karena nilai delay pada tiap paket yang dikirim berbeda. Selain itu jarak antar *node* dan juga banyaknya *node* yang dilewati juga mempengaruhi besarnya nilai delay tiap paket.

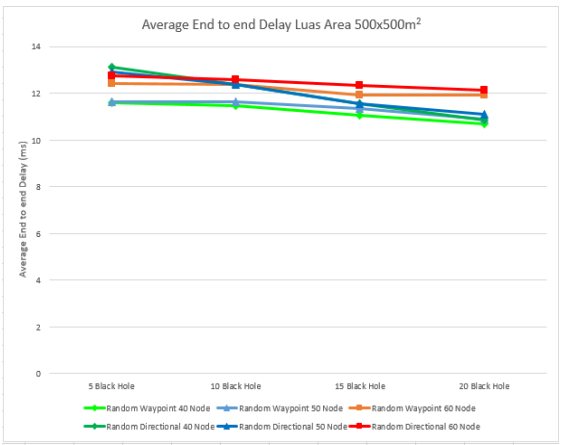
4.5 Analisis Pengujian *Average end-to-end delay* pada Luas Area 700x700m^2



Gambar 11. Pengujian *average end-to-end delay* pada luas area 700x700m^2

Gambar 11 menggambarkan nilai *average end-to-end delay* pada *random waypoint* dan *random direction* dengan scenario jumlah *node* 40, 50 dan 60 *node* dengan luas area 700x700m^2 dan variasi 5, 10, 15 dan 20 *node black hole*. Nilai *average end-to-end delay* dipengaruhi oleh jumlah *hop* atau *node* yang dilewati saat pengiriman paket. Selain itu jarak antar *node* dan luas area simulasi mempengahi besar nya nilai *delay* dari tiap paketnya. Nilai *average end-to-end delay* dihitung dari *delay* jumlah paket yang sampai ke tujuan sehingga paket yang di *drop* oleh *node black hole* tidak dihitung. Pada *random direction* 50 *node* nilai *average end-to-end delay* mengalami kenaikan. Hal ini disebabkan karena nilai delay pada tiap paket yang dikirim berbeda. Selain itu jarak antar *node* dan juga banyaknya *node* yang dilewati juga mempengaruhi besarnya nilai delay tiap paket.

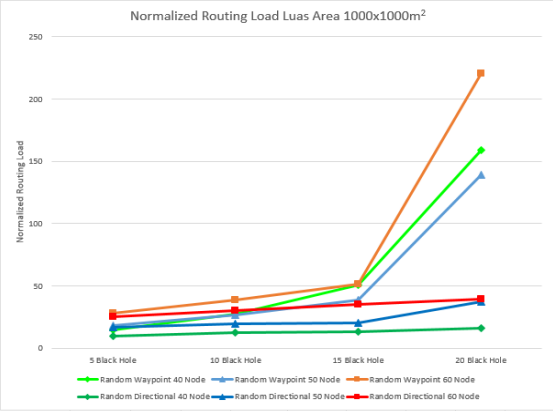
4.6 Analisis Pengujian *Average end-to-end delay* pada Luas Area 500x500m^2



Gambar 12. Pengujian *average end-to-end delay* pada luas area 500x500m^2

Gambar 12 menggambarkan nilai *average end-to-end delay* pada *random waypoint* dan *random direction* dengan scenario jumlah *node* 40, 50 dan 60 *node* dengan luas area 500x500m^2 dan variasi 5, 10, 15 dan 20 *node black hole*. Nilai *average end-to-end delay* dipengaruhi oleh jumlah *hop* atau *node* yang dilewati saat pengiriman paket. Selain itu jarak antar *node* dan luas area simulasi mempengahi besar nya nilai *delay* dari tiap paketnya. Nilai *average end-to-end delay* dihitung dari *delay* jumlah paket yang sampai ke tujuan sehingga paket yang di *drop* oleh *node black hole* tidak dihitung. Pada pengujian luas area 500x500m^2 pada kepadatan *node* 40, 50, dan 60 nilai average end-to-end delay cenderung mengalami penurunan dan lebih stabil.

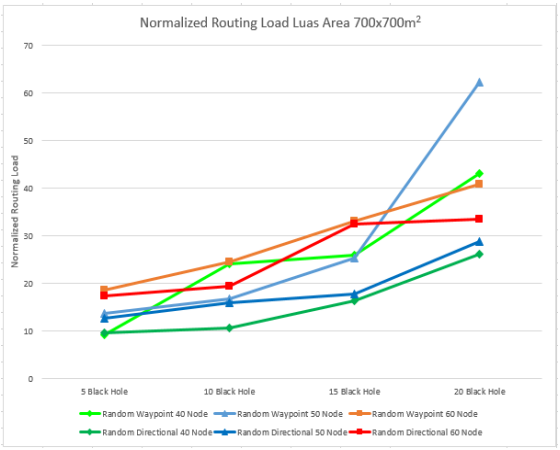
4.7 Analisis Pengujian Normalized Routing Load pada Luas Area 1000x1000m^2



Gambar 13. Pengujian normalized routing load pada luas area 1000x1000m^2

Gambar 13 menggambarkan perbandingan nilai *normalized routing load* pada *random waypoint* dan *random direction* dengan variasi *node* 40, 50, 60 dan variasi jumlah *node black hole* 5, 10, 15, 20 dengan luas area 1000x1000m^2. Gambar 5.7 secara keseluruhan nilai *normalized routing load* mengalami peningkatan seiring dengan penambahan jumlah *node black hole*. Nilai *normalized routing load* berbanding lurus dengan banyaknya jumlah *node black hole*. Hal ini disebabkan karena nilai dari *paket delivery ratio* digunkan sebagai pembagi dari banyak jumlah paket *routing* yang dikirimkan. Gambar 13 menunjukan pada *random waypoint* pada variasi serangan 20 *node black hole* terjadi kenaikan yang cukup signifikan. Hal ini disebabkan karena jumlah paket data yang diterima mengalami penurunan yang cukup signifikan pada variasi 20 serangan *black hole*.

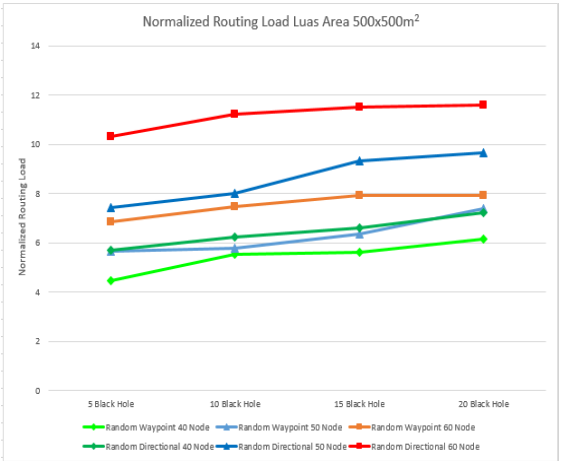
4.8 Analisis Pengujian Normalized Routing Load pada Luas Area 700x700m^2



Gambar 14. Pengujian *normalized routing load* pada luas area 700x700m^2

Gambar 14 menggambarkan perbandingan nilai *normalized routing load* pada *random waypoint* dan *random direction* dengan variasi *node* 40, 50, 60 dan variasi jumlah *node black hole* 5, 10, 15, 20 dengan luas area 700x700m^2. Gambar 14. secara keseluruhan nilai *normalized routing load* mengalami peningkatan seiring dengan penambahan jumlah *node black hole*. Nilai *normalized routing load* berbanding lurus dengan banyaknya jumlah *node black hole*. Hal ini disebabkan karena nilai dari *paket delivery ratio* digunkan sebagai pembagi dari banyak jumlah paket *routing* yang dikirimkan. Gambar 14 pada *random waypoint* 50 *node* pada variasi serangan 20 *node black hole* terjadi kenaikan yang cukup signifikan. Hal ini disebabkan karena jumlah paket data yang diterima mengalami penurunan yang cukup signifikan pada variasi 20 serangan *black hole*.

4.9 Analisis Pengujian *Average end-to-end delay* pada Luas Area 500x500m^2



Gambar 15. Pengujian *normalized routing load* pada luas area 500x500m^2

Gambar 15 menggambarkan perbandingan nilai *normalized routing load* pada *random waypoint* dan *random direction* dengan variasi *node* 40, 50, 60 dan variasi jumlah *node black hole* 5, 10, 15, 20 dengan luas area 500x500m^2. Gambar 14 secara keseluruhan nilai *normalized routing load* mengalami peningkatan seiring dengan penambahan jumlah *node black hole*. Nilai *normalized routing load* berbanding lurus dengan banyaknya jumlah *node black hole*. Hal ini disebabkan karena nilai dari *paket delivery ratio* digunkan sebagai pembagi dari banyak jumlah paket *routing* yang dikirimkan. Gambar 15 menunjukan kenaikan nilai *normalized routing load* lebih stabil dan tidak terjadi kenaikan yang signifikan.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis dari dampak serangan *black hole* pada *routing* protokol DSDV, dapat disimpulkan bahwa :

1. Implementasi serangan black hole pada protokol DSDV pada MANET bekerja sesuai dengan perancangan yang telah dibuat. Pada penelitian serangan *black hole* yang diterapkan adalah tipe serangan *black hole* internal. Pada penelitian serangan *black hole* tidak menggangu proses routing hanya melakukan drop paket pada paket yang melalui node tersebut.
2. Pengaruh serangan *black hole* pada model mobilitas *random* dapat dilihat pada hasil analisis pengujian yang ada. Secara keseluruhan terjadi penurunan performa protokol *routing* DSDV pada kedua jenis mobilitas *random*. Hal ini dibuktikan dari hasil pengujian pada nilai *paket delivery ratio*, *average end-to-end delay* dan *normalized routing load*. Sehingga dapat disimpulkan Pada luas area 1000x1000m^2 dan 700x700m^2 protokol *routing* DSDV pada *random waypoint* mengalami dampak serangan *black hole* yang lebih besar dibanding protokol *routing* DSDV pada *random direction*. Protokol *routing* DSDV pada *random waypoint paket delivery ratio* turun hingga angka 5 %. *Nilai average end-to-end delay* mencapai 42,659 ms. Pada *normalized routing load* kenaikannya mencapai angka 220,545. Pada luas area simulasi 500x500m^2 protokol *routing* DSDV pada *random direction* memiliki dampak serangan *black hole* lebih besar dibanding protokol *routing* DSDV pada *random waypoint*. Protokol *routing* DSDV pada *random direction* memiliki penurunan nilai *paket delivery ratio* tidak sampai 30%. Parameter *average end-to-end delay* nilai tertinggi mencapai 13,1095 ms. Pada parameter *normalized routing load* kenaikannya tidak terlalu besar, nilai tertinggi normalized routing load mencapai 11,6103.

5.2 Saran

Saran yang disampaikan untuk penelitian lebih lanjut adalah sebagai berikut:

1. Perlu dilakukan penelitian lebih lanjut dengan model pergerakan seperti model pergerkan manhattan mobilitas model, gaus markov mobilitas model dll.
2. Perlunya dilakukan penelitian teradap pencegahan *malicious node* pada protokol routing DSDV.
3. Perlu dilakukan pengujian terhadap jenis serangan *malicious node* yang berbeda seperti grayhole, wormhole dll.

6. DAFTAR PUSTAKA

Aji, M. A. B., Sukiswo & Zahra, A. A., 2015. Evaluasi Kinerja Protokol Routing Dsdv Terhadap Pengaruh Malicious *Node* Pada Manet Menggunakan Network Simulator 2 (NS-2). TRANSIENT, 4(4).

Arora, N. & Barwar, D. N. C., 2014. Performance Analysis of DSDV, AODV and ZRP under Blackhole attack. International Journal of Engineering Research & Technology (IJERT), 3(4), pp. 2000-2004.

Das, I., Lobiyal, D. & Katti, C., 2014. Effect Of *Node* Mobility On AOMDV Protocol In MANET. International Journal of Wireless & Mobile Networks (IJWMN), 6(3), pp. 91-99.

Natarajan, K. & Mahadevan, G., 2017. Mobility based Performance Analysis of MANET Routing Protocols. International Journal of Computer Applications (0975 –

Puray, M. & Palod, P., 2016. Black-Hole Attack in MANET: A Study. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(3), pp. 597-601.

Saad, M. I. M. & Zukarnain, Z. A., 2009. Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol. European Journal of Scientific Research, 32(4), pp. 444-454.

Sharma, A. & Renu, 2013. Evaluation of Performance of AODV over DSDV Protocol using Blackhole attack in MANET. *International Journal of software & Hardware Research in Engineering*, 1(1), pp. 67-72.