EVALUASI KINERJA PROTOKOL *ROUTING* DSDV TERHADAP PENGARUH *MALICIOUS NODE* PADA MANET MENGGUNAKAN *NETWORK SIMULATOR* 2 (NS-2)

Muhammad Arif Bayu Aji[*)], Sukiswo, and Ajub Ajulian Zahra

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)] *Email: bayuindi2134@gmail.com*

Abstrak

MANET merupakan teknologi telekomunikasi yang dikembangkan untuk memberikan kemudahan bagi pengguna dalam berkomunikasi. MANET terbentuk dari beberapa node yang bergerak bebas dan tidak bergantung pada infrastruktur tetap. Kelemahan utama MANET adalah masalah keamanannya. Node-node secara bebas masuk dan keluar dalam jaringan hal ini lah yang menyebabkan MANET rentan terhadap serangan. Salah satu contoh serangan dalam MANET adalah serangan malicious node. Pada penelitian menganalisis evaluasi kinerja DSDV pada MANET terhadap serangan malicious node. Beberapa parameter yang digunakan untuk mengukur kinerjanya antara lain throughput, delay total dan PDR. Perancangan MANET dilakukan menggunakan software NS2. Hasil simulasi menunjukkan serangan malicious node mengakibatkan penurunan nilai throughput, delay, dan PDR disetiap kondisi. Penurunan nilai throughput terbesar terjadi pada kondisi jaringan yang mengalami perubahan luas dimensi, yaitu jaringan 100 node dimensi 1000x1000 m^2 turun 100 Kbps dari kondisi normalnya. Sementara penurunan nilai delay total terbesar terjadi pada kondisi jaringan yang mengalamai perubahan kecepatan gerak node, yaitu pada jaringan 75 node saat kecepatan gerak node-nya 1,75 m/s turun 30,53 ms dari kondisi normalnya. Serangan malicious node memberikan efek paling besar untuk nilai PDR pada kondisi jaringan yang mengalami perubahan luas dimensi, yaitu jaringan 50 node dimensi 1000x1000 m^2 turun 0,76% dari kondisi normalnya.

Kata kunci : MANET, DSDV, Serangan Malicious Node, NS2

Abstract

MANET is telecommunication technology developed to make it easy for users to communicate. MANET formed from multiple nodes to move freely and not rely on fixed infrastructure. Main weakness of MANET is security problem. Nodes can freely join and leave the network, which cause MANET vurnerable. Malicious node attack is the example of attack in MANET. This research analyze performance evaluation of DSDV on MANET against malicious node attacks. Some of parameters used to measure performance of throughput, total delay and PDR. Design of MANET using software NS2. Simulation results indicate malicious node attacks resulted decrease of throughput, delay, and PDR in every condition. The greatest decrease in throughput happens on network conditions that experienced changes dimensions wide , at 100 nodes network with dimension 1000x1000 m^2 decreased by 100 Kbps of normal conditions. While the greatest decrease in total delay happens on network conditions that experienced changes movement speed of node, at 75 nodes network when the speed of node at 1,75 m/s decreased by 30,53 ms of normal conditions. Malicious node attack gives the greatest effect to PDR happens on network conditions that experienced changes dimensions wide, at 50 nodes network with dimension 1000x1000 m^2 decreased by 0,76% of normal conditions.

Kata kunci : MANET, DSDV, Serangan Malicious Node, NS2

1. Pendahuluan

Kelemahan utama pada MANET adalah masalah keamanannya. Node-node secara bebas dapat masuk dan keluar dalam jaringan hal ini lah yang menyebabkan MANET rentan terhadap serangan. Hal ini dikarenakan media pertukaran data atau informasi pada MANET menggunakan transmisi radio ditambah tidak adanya administrator yang mengawasi perangkat komunikasi yang terhubung. Sehingga memungkinkan setiap orang dapat terhubung pada jaringan dan mengakses informasi didalam jaringan tersebut. Dengan keterbukaan media

transmisi MANET, maka akan selalu ada kesempatan untuk menyerang MANET. Beberapa motif serangan MANET diantaranya adalah ingin mendapatkan akses internet gratis, mencuri data, memata - matai kegiatan seseorang atau perusahaan, sampai merusak sistem sebuah perusahaan. Serangan pada MANET yang akan dibahas di penelitian ini adalah serangan *malicious node.* Pemilihan jenis serangan *malicious node* memiliki alasan tersendiri. Serangan *malicious node* menjatuhkan paket melalui *node malicious.* Karena saat *node malicious* aktif maka paket yang melaluinya akan dijatuhkan (*drop*). Tujuan dari serangan ini adalah supaya paket yang dikirim tidak sampai ke penerimaan. Efek dari *node malicious* sangat merugikan sehingga menarik untuk diteliti.

2. Metode

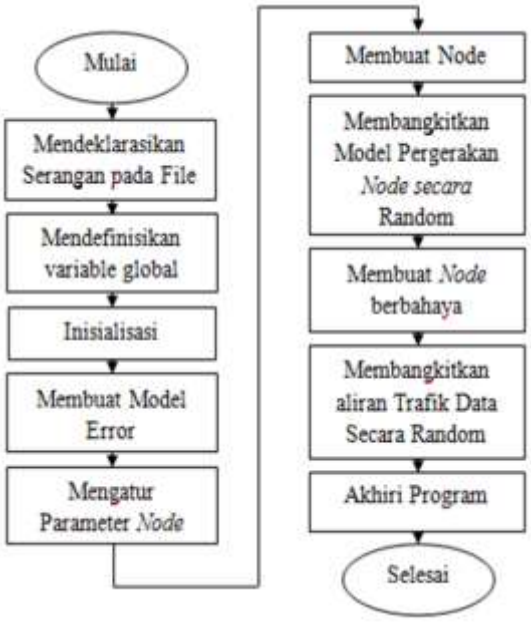
2.1. Simulasi Jaringan MANET

Pada penelitian ini terdapat 3 buah skenario yang digunakan yaitu kondisi jaringan terhadap perubahan luas dimensi jaringan, kondisi jaringan terhadap pertumbuhan *malicious node*, dan kondisi jaringan terhadap kecepatan gerak *node*. Jumlah *node* yang digunakan untuk setiap skenario adalah 50, 75, dan 100 *node*. Pada skenario pertama luas dimensi jaringan yang digunakan 100 x 100 m^2, 200 x 200 m^2, 300 x 300 m^2 sampai dengan 1000 x 1000 m^2. Pada skenario kedua, jumlah *malicious node* yang digunakan mengalami pertumbuhan dari 1 *node* hingga 50% dari jumlah *intermediate node* yang ada. Kemudian pada skenario ketiga variasi kecepatan gerak *node* dalam jaringan adalah 1.45 m/s, 1.6 m/s, 1.75 m/s, dan 1.9 m/s. Serangan *malicious node* diberikan kepada jaringan dengan jenis trafik TCP. Pengambilan data dilakukan sebanyak 5 kali secara acak dan diambil nilai rata-rata untuk dianalisis. Tujuan dari skenario ini adalah untuk menguji kinerja protokol DSDV pada kondisi jaringan yang berbeda-beda saat terkena serangan *malicious node* sehingga didapatkan hasil kinerja yang efektif dari protokol tersebut.

2.2. Perancangan Sistem

Pada penelitian ini dibuat suatu jaringan *Zigbee* dengan menggunakan *Network Simulator* 2. Secara keseluruhan, tahapan pembuatan simulasi ditunjukkan pada Gambar 1berikut.

Pada simulasi ini, terdapat parameter yang digunakan untuk menjalankan simulasi. Parameter tersebut ditunjukkan pada **tabel 1**.



Gambar 1. Diagram Alir Simulasi

Tabel 1. Parameter simulasi

Parameter	Nilai
MAC	IEEE 802.11g
Model antenna	Omnidirectional
Model propagasi	Two Ray Ground
Protokol routing	DSDV
Model antrian	Droptail
Maksimum paket dalam antrian	50 paket
Durasi simulasi	200 detik
Model pergerakan node	Random Way Point
Jumlah node	50, 75, 100
Kecepatan node	1,45 , 1,60 , 1,75 , 1,90 (m/s)
Dimensi topografi	100 x 100, 200 x 200, 300 x 300, 400 x 400, 500 x 500, 600 x 600, 700 x 700, 800 x 800, 900 x 900, 1000 x 1000 (m2)
Jenis serangan	Malicious node

2.3 Metode Pengambilan Data

Data hasil simulasi tersedia dalam bentuk *trace file. Trace file* berisi semua kejadian yang terjadi pada saat simulasi berlangsung. Dari *trace file* dapat diambil data yang diinginkan. Penilaian performansi jaringan terdiri dari beberapa parameter yaitu :

1. *Throughput*

Throughput merupakan laju rata-rata dari paket informasi yang berhasil diterima. Laju rata-rata paket diwakili dengan jumlah paket informasi yang diterima setiap detik. *Throughput* mempunyai satuan bps (*bit per second*).

$$Throughput = \sum_{i=T_t}^{i=T_{t+1}} R_i ; 0 \leq t \leq T \quad (1)$$

Keterangan :
P_i = Ukuran paket yang diterima (bit)
T = Waktu pengamatan (detik)
t = Waktu pengambilan sampel (detik)

2. Waktu Tunda (*Delay*)
Waktu tunda (*Delay*) merupakan selang waktu yang dibutuhkan oleh suatu paket informasi saat data mulai dikirim dan keluar dari proses antrian sampai mencapai titik tujuan.

$$Delay = \frac{\sum_{i=T_t}^{i=T_{t+1}} RT_i - \sum_{i=T_t}^{i=T_{t+1}} ST_i}{\sum_{i=T_t}^{i=T_{t+1}} R_i} ; 0 \leq t \leq T \quad (2)$$

Keterangan :
RT_i = Waktu penerimaan paket (detik)
ST_i = Waktu pengiriman paket (detik)
R_i = Paket yang diterima (paket)

Nilai delay dapat divalidasi dengan menggunakan teorema little yang ditunjukkan pada persamaan 3.

$$N = \lambda T \quad (3)$$

Keterangan :
N = Jumlah paket rata-rata dalam sistem
λ = Laju kedatangan
T = waktu rata-rata dalam system

3. PDR
Packet Delivery Ratio (PDR) merupakan perbandingan banyaknya jumlah paket yang diterima oleh node penerima dengan total paket yang dikirimkan dalam suatu periode waktu tertentu.

$$PDR = \frac{\sum_{i=T_t}^{i=T_{t+1}} R_i}{\sum_{i=T_t}^{i=T_{t+1}} S_i} \times 100\ \% ; 0 \leq t \leq T \quad (4)$$

Keterangan :
R_i = Paket yang diterima (paket)
S_i = Paket yang dikirim (paket)
T = Waktu pengamatan (detik)
t = Waktu pengambilan sampel (detik)

3. Hasil dan Analisis

3.1. Analisis *Throughput*

3.1.1. Kondisi Jaringan Terhadap Perubahan Luas Dimensi

Dari hasil simulasi didapatkan nilai *throughput* kinerja DSDV kondisi jaringan terhadap perubahan luas dimensi yang ditunjukkan pada tabel 2.

Tabel 2. Nilai *throughput* rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap perubahan luas dimensi

Jumlah *node* jaringan (*Node*)	Luas Dimensi Jaringan (m^2)	Kondisi normal		kondisi terserang *malicious*	
		Throughput (Kbps)	Deviasi	*Throughput* (Kbps)	Deviasi
50	600x600	602	48,932	563	62,187
	700x700	554	45,152	515	44,873
	800x800	555	64,895	458	137,490
	900x900	456	80,133	358	24,975
	1000x1000	345	109,535	313	195,629
75	600x600	570	56,782	527	30,847
	700x700	529	60,870	475	25,014
	800x800	510	49,605	481	27,318
	900x900	421	38,397	404	93,964
	1000x1000	341	96,423	261	86,125
100	600x600	547	50,911	488	39,084
	700x700	565	25,736	493	57,070
	800x800	519	64,287	500	29,383
	900x900	437	71,549	344	107,002
	1000x1000	354	36,216	254	84,575

Berdasarkan tabel 2, penurunan nilai *throughput* terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi pada luas dimensi 900 x 900 m^2 yang turun 99 Kbps atau 21,711 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi pada luas dimensi 1000 x 1000 m^2 yang turun 80 Kbps atau 23,460 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi pada luas dimensi 1000 x 1000 m^2 yang turun 100 Kbps atau 28,249 % dari kondisi normalnya

3.1.2. Kondisi jaringan Terhadap Pertumbuhan *Malicious Node*

Dari hasil simulasi didapatkan nilai *throughput* kinerja DSDV kondisi jaringan terhadap pertumbuhan *malicious node* yang ditunjukkan pada tabel 3.

Tabel 3. Nilai *throughput* rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap pertumbuhan *malicious node*

Jumlah *node* jaringan (*Node*)	Jumlah *malicious node* (*Node*)	*Throughput* (Kbps)	Deviasi
50	0	602	48,932

Tabel 3 Lanjutan

Jumlah *node* jaringan (*Node*)	Jumlah *malicious node* (*Node*)	*Throughput* (Kbps)	Deviasi
50	11	575	86,541
	12	575	86,517
	13	550	57,683
	14	543	27,747
	15	563	62,187
75	0	570	56,782
	18	526	50,494
	22	536	13,184
	24	530	14,437
	26	533	33,088
	28	527	30,847
100	0	565	25,736
	32	486	54,628
	34	506	29,836
	36	497	36,479
	38	499	62,395
	40	493	57,070

Berdasarkan tabel 3, penurunan nilai *throughput* terbesar pada jaringan 50 *node* terjadi saat terdapat 14 *malicious node* menyebabkan nilai *throughput* turun 59 Kbps atau 9,801 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat terdapat 18 *malicious node* menyebabkan nilai *throughput* turun 44 Kbps atau 7,719 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi saat terdapat 32 *malicious node* menyebabkan nilai *throughput* turun 79 Kbps atau 13,982 % dari kondisi normalnya.

3.1.3. Kondisi Jaringan Terhadap Kecepatan Gerak *Node*

Dari hasil simulasi didapatkan nilai *throughput* untuk kinerja DSDV kondisi jaringan terhadap perubahan kecepatan gerak *node* yang ditunjukkan pada tabel 4.

Tabel 4. Nilai *throughput* rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap kecepatan gerak *node*

Jumlah *node* jaringan (*node*)	Kecepatan gerak *node* (m/s)	Kondisi normal		kondisi terserang *malicious*	
		Throughput (Kbps)	Deviasi	*Throughput* (Kbps)	D eviasi
50	1,45	565	50,088	537	69,343
	1,60	570	41,025	530	28,968
	1,75	618	19,816	556	21,132
	1,90	592	38,054	562	42,728
75	1,45	581	33,001	587	64,552
	1,60	559	55,741	533	103,436
	1,75	572	29,122	523	62,342
	1,90	583	37,883	567	53,530

Tabel 4 Lanjutan

Jumlah *node* jaringan (*node*)	Kecepatan gerak *node* (m/s)	Kondisi normal		kondisi terserang *malicious*	
		Throughput (Kbps)	Deviasi	*Throughput* (Kbps)	D eviasi
100	1,45	536	67,969	492	118,444
	1,60	556	41,731	503	25,150
	1,75	557	33,458	517	27,502
	1,90	565	49,614	522	68,084

Berdasarkan tabel 4, penurunan nilai *throughput* terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi pada saat kecepatan gerak node-nya 1,75 m/s yang turun 62 Kbps atau 10,032 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat kecepatan gerak node-nya 1,75 m/s yang turun 49 Kbps atau 8,566 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi saat kecepatan gerak node-nya 1,60 m/s yang turun 53 Kbps atau 9,532 % dari kondisi normalnya.

3.2. Analisis *Delay*

3.2.1. Kondisi Jaringan Terhadap Perubahan Luas Dimensi

Dari hasil simulasi didapatkan nilai *delay* untuk kinerja DSDV kondisi jaringan terhadap perubahan luas dimensi yang ditunjukkan pada tabel 5.

Tabel 5. Nilai *delay* total rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap perubahan luas dimensi

Jumlah node jaringan (*node*)	Luas dimensi (m^2)	Kondisi normal		Kondisi terserang *malicious node*	
		Delay Total (ms)	Deviasi	*Delay* Total (ms)	Deviasi
50	100x100	565,595	51,192	531,249	63,109
	200x200	557,705	43,612	509,795	30,772
	300x300	438,640	22,684	431,663	33,973
	400x400	293,949	84,499	305,091	48,901
	500x500	207,523	37,506	202,530	35,919
75	100x100	556,283	54,939	509,472	18,245
	200x200	559,559	34,382	507,827	17,208
	300x300	440,074	38,263	407,765	28,971
	400x400	291,930	79,603	268,566	41,624
	500x500	189,917	54,727	181,659	34,435
100	100x100	578,969	34,830	471,444	40,788
	200x200	562,366	47,742	536,286	49,097
	300x300	479,826	28,993	410,757	38,082
	400x400	271,451	66,201	250,359	109,375
	500x500	241,984	28,580	205,359	62,438

Berdasarkan tabel 5, penurunan nilai *delay* terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi pada luas dimensi 200 x 200 m^2 yang turun 47,9 ms atau 8,589 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi pada luas dimensi 200 x 200 m^2 yang turun 51,7 ms atau 9,257 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi pada luas dimensi 100 x 100 m^2

yang turun 107,5 ms atau 18,584 % dari kondisi normalnya.

3.2.2. Kondisi Jaringan Terhadap Pertumbuhan *Malicious Node*

Dari hasil simulasi didapatkan nilai *delay* untuk kinerja DSDV kondisi jaringan terhadap pertumbuhan *malicious node* yang ditunjukkan pada tabel 6.

Tabel 6. Nilai *delay* total rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap pertumbuhan *malicious node*

Jumlah *node* jaringan (*Node*)	Jumlah *malicious node* (*Node*)	*Delay* Total (ms)	Deviasi
50	0	138,915	36,906
	2	119,580	27,394
	6	133,888	7,458
	10	134,408	12,758
	14	128,604	29,721
	15	131,288	27,113
75	0	141,697	21,740
	22	137,874	16,619
	24	148,291	35,538
	26	140,111	16,679
	27	140,111	16,679
	28	138,161	17,700
100	0	127,804	22,183
	10	107,665	16,115
	11	104,434	15,310
	21	121,252	13,823
	31	140,065	17,074
	40	135,913	34,486

Berdasarkan tabel 6, Penurunan nilai *delay* terbesar karena serangan *malicious node* untuk jaringan 50 *node* terjadi saat terdapat 2 *malicious node* menyebabkan nilai *delay* turun 19,33 ms atau 13,915 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat terdapat 22 *malicious node* menyebabkan nilai *delay* turun 3,82 ms atau 2,696 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi saat terdapat 11 *malicious node* menyebabkan nilai *delay* turun 23,37 ms atau 18,286 % dari kondisi normalnya.

3.2.3. Kondisi Jaringan Terhadap Perubahan Kecepatan Gerak *Node*

Dari hasil simulasi didapatkan nilai *delay* untuk kinerja DSDV kondisi jaringan terhadap perubahan kecepatan gerak *node* yang ditunjukkan pada tabel 7.

Tabel 7. Nilai *delay* total rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap kecepatan gerak *node*

Jumlah *node* jaringan (*node*)	Kecepatan gerak *node* (m/s)	Kondisi normal		Kondisi jaringan terserang	
		Delay Total (ms)	Deviasi	*Delay* Total (ms)	Deviasi
50	1,45	135,826	21,947	128,537	30,358
	1,60	143,773	19,746	136,294	19,815
	1,75	142,507	23,229	127,090	28,833
	1,90	143,817	19,835	140,069	17,990
75	1,45	147,043	18,824	134,035	26,109
	1,60	139,341	25,237	125,140	38,453
	1,75	145,618	20,783	115,083	29,177
	1,90	147,944	8,883	131,467	26,984
100	1,45	119,777	19,327	114,066	18,356
	1,60	128,053	40,002	125,956	43,058
	1,75	123,313	17,787	118,954	31,218
	1,90	126,943	35,664	108,723	14,394

Berdasarkan tabel 7, penurunan nilai *delay* terbesar karena serangan *malicious node* untuk jaringan 50 *node* terjadi saat kecepatan gerak node-nya 1,75 m/s menyebabkan nilai *delay* turun 15,42 ms atau 10,820 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat kecepatan gerak node-nya 1,75 m/s menyebabkan nilai *delay* turun 30,53 ms atau 20,966 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi saat kecepatan gerak node-nya 1,90 m/s menyebabkan nilai *delay* turun 18,22 ms atau 14,353 % dari kondisi normalnya.

3.3. Analisis *Packet Delivery Ratio* (PDR)

3.3.1. Kondisi Jaringan Terhadap Perubahan Luas Dimensi

Dari hasil simulasi didapatkan nilai PDR untuk kinerja DSDV kondisi jaringan terhadap perubahan luas dimensi yang ditunjukkan pada tabel 8.

Tabel 8. Nilai PDR rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap perubahan luas dimensi

Jumlah *node* jaringan (*node*)	Luas Dimensi (m^2)	Jaringan normal		Jaringan terserang *malicious*	
		PDR (%)	Deviasi	PDR (%)	Deviasi
50	100x100	98,952	0,003	98,728	0,004
	400x400	98,754	0,004	98,786	0,002
	700x700	99,266	0,002	99,110	0,002
	900x900	98,426	0,006	98,602	0,005
	1000x1000	98,020	0,009	97,264	0,021
75	100x100	99,072	0,001	98,566	0,004
	400x400	98,788	0,004	98,666	0,004
	700x700	98,920	0,002	98,842	0,004
	900x900	98,676	0,004	98,694	0,004
	1000x1000	97,700	0,014	97,800	0,015
100	100x100	98,674	0,003	98,144	0,004

Tabel 8. Lanjutan

Jumlah *node* jaringan (*node*)	Luas Dimensi (m^2)	Jaringan normal		Jaringan terserang *malicious*	
		PDR (%)	Deviasi	PDR (%)	Deviasi
100	400x400	98,622	0,005	98,518	0,005
	700x700	98,860	0,003	98,850	0,001
	900x900	98,094	0,004	98,514	0,004
	1000x1000	97,486	0,005	98,008	0,006

Berdasarkan tabel 8 Penurunan terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi pada luas dimensi 1000 x 1000 m^2 yang turun 0,756 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi pada luas dimensi 100 x 100 m^2 yang turun 0,506 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi pada luas dimensi 100 x 100 m^2 yang turun 0,530 % dari kondisi normalnya.

3.3.2. Kondisi Jaringan Terhadap Pertumbuhan *Malicious Node*

Dari hasil simulasi didapatkan nilai PDR untuk kinerja DSDV kondisi jaringan terhadap pertumbuhan *malicious node* yang ditunjukkan pada tabel 9.

Tabel 9. Nilai PDR rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap pertumbuhan *malicious node*

Jumlah *node* jaringan (*node*)	Jumlah *malicious node* (*node*)	PDR (%)	Deviasi
50	0	98,992	0,003
	8	99,086	0,002
	10	98,770	0,004
	12	98,970	0,001
	14	99,166	0,002
	15	99,222	0,002
75	0	98,924	0,002
	3	98,592	0,004
	9	98,748	0,005
	15	99,010	0,003
	21	98,760	0,005
	28	99,108	0,002
100	0	98,864	0,003
	33	98,542	0,008
	35	98,898	0,004
	37	99,006	0,003
	39	98,850	0,001
	40	98,850	0,001

Berdasarkan tabel 9, Penurunan terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi saat terdapat 10 *malicious node* menyebabkan nilai PDR turun 0,222 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat terdapat 3 *malicious node* menyebabkan nilai PDR turun 0,332 % dari kondisi normalnya, dan pada jaringan 100 *node* terjadi saat terdapat 33 *malicious node* menyebabkan nilai PDR turun 0,322 % dari kondisi normalnya.

3.3.3. Kondisi Jaringan Terhadap Perubahan Kecepatan Gerak *Node*

Dari hasil simulasi didapatkan nilai PDR untuk kinerja DSDV kondisi jaringan terhadap perubahan kecepatan gerak *node* yang ditunjukkan pada tabel 10.

Tabel 10. Nilai PDR rata-rata dan standar deviasi jaringan normal dan jaringan terkena serangan *malicious node* terhadap kecepatan gerak *node*

Jumlah *node* Jaringan (*node*)	Kecepatan gerak *node* (m/s)	Jaringan normal		Jaringan terserang *malicious*	
		PDR (%)	Deviasi	PDR (%)	Deviasi
50	1,45	98,936	0,004	99,114	0,002
	1,60	99,018	0,002	98,930	0,003
	1,75	99,068	0,001	98,974	0,004
	1,90	98,892	0,002	98,832	0,003
75	1,45	99,036	0,003	99,190	0,002
	1,60	98,916	0,002	98,884	0,003
	1,75	98,792	0,005	98,670	0,007
	1,90	99,014	0,002	98,956	0,005
100	1,45	98,866	0,006	99,090	0,008
	1,60	98,902	0,004	99,130	0,003
	1,75	99,070	0,003	99,140	0,002
	1,90	98,956	0,005	99,076	0,002

Berdasarkan tabel 10, penurunan terbesar akibat serangan *malicious node* pada jaringan 50 *node* terjadi saat kecepatan gerak *node*-nya 1,60 m/s menyebabkan nilai PDR turun 0,088 % dari kondisi normalnya, lalu pada jaringan 75 *node* terjadi saat kecepatan gerak *node*-nya 1,75 m/s menyebabkan nilai PDR turun 0,122 % dari kondisi normalnya, dan pada jaringan 100 *node* tidak terjadi penurunan nilai PDR.

4. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari simulasi dan evaluasi permasalahan dalam Penelitian ini adalah :

1. Penurunan nilai *throughput* terjadi pada jaringan yang terkena serangan untuk setiap kondisi seperti perubahan dimensi, pertumbuhan *malicious node*, dan perubahan kecepatan gerak *node*. Penurunan nilai *throughput* terbesar terjadi pada jaringan yang mengalami perubahan luas dimensi yaitu pada jaringan 100 *node* dengan dimensi 1000 x 1000 m^2. Nilai *throughput* turun menjadi 254 Kbps dari 354 Kbps, sehingga terjadi penurunan sebesar 100 Kbps atau 28,249 %.
2. Penurunan nilai *delay* total terjadi pada jaringan yang terkena serangan untuk setiap kondisi seperti perubahan dimensi, pertumbuhan *malicious node*, dan perubahan kecepatan gerak *node*. Penurunan nilai *delay* total terbesar terjadi pada jaringan yang mengalami perubahan kecepatan gerak *node* yang terjadi pada jaringan 75 *node* saat kecepatan gerak *node*-nya 1,75 m/s. Nilai *delay* total turun menjadi 115,08 ms dari 145,61 ms, sehingga terjadi penurunan sebesar 30,53 ms atau 20,967 %.

3. Penurunan nilai PDR terjadi pada jaringan yang terkena serangan untuk setiap kondisi seperti perubahan dimensi, pertumbuhan *malicious node*, dan perubahan kecepatan gerak *node*. Penurunan nilai PDR terbesar terjadi pada jaringan yang mengalami perubahan luas dimensi yaitu pada jaringan 50 *node* dengan dimensi 1000 x 1000 m^2. Nilai PDR turun menjadi 97,26 % dari 98,02 %, sehingga terjadi penurunan sebesar 0,760 %.

Referensi

[1]. Ahmed, Mohzin dan Hussain, Anwar, "Understanding Vulnerability of Adhoc Networks Under Malicious Node Attack," dalam IJCNWC, ISSN : 2250-3501, Vol.2, No.3, Juni, 2012.

[2]. M. Ahmed dan D. M. A. Hussain, "Effect of Malicious Node Attacks Under Practical Adhoc Network," dalam IJCNWC, vol. 2, no. Oktober, pp. 542–549, 2012.

[3]. K. Majumber, S. Ray, dan S. K. Sarkar, "Performance Analysis of DSDV and DSR Under Variable Node Speed In Hybrid Scenario," dalam IJWMN, vol. 4, no. 4, Agustus, 2012.

[4]. M. V. Khiavi, S. Jamali, dan S. J. Gudakhriz, "Performance Comparison of AODV, DSDV, DSR, and TORA Routing Protocols In MANETs," dalam IRJABS, vol. 3 (7), pp. 1429–1436, 2012.

[5]. Haqqi, Ma'ruf Nashrul., "Analisis Kinerja PUMA Pada MANET Menggunakan NS 2," Makalah Jaringan Nirkabel dan Komputasi Bergerak Universitas Muhamadiyah Gresik Prodi Teknik Informatika, Gresik, 2013.

[6]. S. Basagni dkk, "Review of Wireless Network Evolution," Mobile Ad Hoc Networking, New Jersey. USA : IEEE Press. 2004.

[7]. D. Harinath, "OSI Reference Model – A Seven Layered Architecture of OSI Model," dalam IJARCSSE, vol. 3, no. 8, hal. 338–346, Agustus, 2013.

[8]. Wang. Shao-Cheng, Chen. Yi-Ming, Lee. Tsern-Huei, Helmy, Ahmed "Performance Evaluations for Hybird IEEE 802.11b and 802.11g Wireless Network".

[9]. Medepalli. Kamesh, Gopalakhrisna. Praveen, Famolari. David, dan Kodamaru. Toshikazu "Voice Capacity of IEEE 802.11b, 802.11a, amd 802.11g Wireless LANs," dalam IEEE.

[10]. P. Ghosekar dkk, "Mobile Ad Hoc Networking: Imperatives and Challenges," IJCA Spec. Issue "Mobile Ad-Hoc Networks," hal 153-158, 2010.

[11]. S. A. Sasongko, "Analisis Performansi dan Simulasi Protokol ZRP (Zone Routing Protocol) Pada MANET (Mobile Ad Hoc Network) Dengan Menggunakan NS-2," Makalah Penelitian, dari Universitas Diponegoro, Semarang, Indonesia.

[12]. Mahesh. K. Marina and Samir R. Das, "Ad Hoc On-Demand Multipath Distance Vector Routing", dalam Wirel. Commun. Mob. Comput., vol. 6, no. 7, 2006.

[13]. Bhatt, Jaya dan Hemrajani, Naveen, "Effective Routing Protocol (DSDV) for Mobile Ad Hoc Network", dalam IJSCE, ISSN : 2231-2307. Vol.3, Issue.5, Nov., 2013.

[14]. N. F Mir, "Computer and Communication Network", 2006.

[15]. Fall. Kevin dan Varadhan Kannan,"The ns Manual (formely ns Notes and Documentation)", The Vint Project, 2011.