EVALUASI KINERJA PROTOKOL AOMDV TERHADAP SERANGAN *MALICIOUS NODE* DAN DDOS PADA MANET DENGAN MENGGUNAKAN *NETWORK SIMULATOR 2* (NS-2)

Mellia Aisyah Aristyorini[*)], Sukiswo, and Ajub Ajulian Zahra

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

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

Abstrak

Tujuan utama perangkat bergerak adalah untuk memudahkan pengguna dalam berkomunikasi dan betukar data. Sekarang ini berkembang teknologi Mobile Ad Hoc Network (MANET) yang merupakan jaringan yang terdiri dari node-node yang bergerak dan berkumpul secara tiba-tiba berkomunikasi menggunakan antarmuka nirkabel tanpa memerlukan infrastruktur yang tetap. Kelemahan utama jaringan ini adalah masalah keamanannya karena lebih rentan terhadap serangan yang dapat merugikan pengguna jaringan. Tugas akhir ini akan menganalisis evaluasi kinerja protokol routing yakni protokol routing AOMDV pada sebuah jaringan MANET terhadap serangan malicious node, DdoS, dan gabungan dari keduanya. Beberapa parameter yang digunakan untuk mengukur kinerjanya antara lain throughput, delay total dan PDR (*Packet Delivery Ratio*). Perancangan jaringan mobile ad hoc akan dilakukan menggunakan software NS2. Hasil simulasi dengan kondisi jaringan yang terkena serangan malicious node dengan jumlah node malicious sebanyak 9 node menunjukkan penurunan nilai PDR terbesar yaitu sebesar 5,08 % dari kondisi jaringan normalnya. Sementara untuk penurunan nilai throughput terbesar pada kondisi jaringan yang terkena serangan malicious dan DDoS dengan jumlah node malicious dan DDoS sebanyak 8 node yaitu sebesar 146 Kbps dari kondisi normalnya. Sementara serangan yang memberikan efek paling besar untuk nilai delay total adalah pada serangan serangan DDoS dengan jumlah node DDoS sebanyak 15 node yaitu sebesar 22,771 ms dari kondisi normalnya.

Kata kunci :MANET, AOMDV, Serangan Malicious Node, Serangan DDoS

Abstract

Main purpose of mobile device is to make it easy for users to communicate and exchange data. Now it develope Mobile Ad Hoc Network (MANET) technology where a network consisting of nodes that are mobile and assemble then suddenly communicate using wireless interface without any fixed infrastructure. Main weakness of this network is security problem where it is more susceptible toward attack that could harm sers. This research will analyze performance evaluation of routing protocol AOMDV on a network node MANET against malicious attacks, DDoS, and a combination of both. Some of parameters are used to measure performance are throughput, total delay and PDR (Packet Delivery Ratio). Design of mobile ad hoc networks is using software NS2.. Simulation results with condition of the affected network by the number of malicious node attacks with 9 malicious node showed the biggest decrease in PDR value that is equal to 5,08 % of normal network conditions. The biggest value of the decrease on network affected by the number 8 nodes of malicious and DDoS attacks is equal to 146 Kbps of normal conditions. While an attack that gives the greatest effect on the value of the total delay with 15 nodes of DDoS as much as node node is equal to 22,771 ms from the normal condition.

Keyword : MANET, AOMDV, Malicious Node Attack, DDoS Attack

1. Pendahuluan

Masalah keamana merupakan kelemahan dalam *wireless network.* Hal ini sangat masuk akal, sebab media untuk pertukaran data atau informasi pada jaringan *Wireless* adalah dengan menggunakan transmisi radio.Dengan keterbukaan media transmisi WLAN dan hampir selalu ada orang yang mengutak - atik sinyal jaringan *wireless*, maka akan selalu ada kesempatan untuk menyerang.Sehingga mengancam keamanan penggunaan jaringan.

Berdasarkan penelitian yang dilakukan oleh Mohzin Ahmed dan Dr. Md. Anwar Hussain[2]dengan judul "*Understanding Vulnerability of Adhoc Networks Under Malicious Node Attack"*, Penelitian ini menjelaskan tentang analisis kerentanan performansi MANET dibawah serangan Malicious Node Attack pada tiga kondisi yang berbeda dengan protokol *routing* MANET AODV. Penelitian selanjutnya yang dilakukan oleh Sachin Garg [3]dengan judul "*Performance Analysis of AODV and TORA under DDoS Attack in MANETs*", Penelitian ini menjelaskan tentang analisis performansi Quality of Service (QoS) protokol AODV dan TORA terhadap serangan DdoS dengan memvariasikan jumlah node-node malicious yang disimulasikan pada NS 2.

Berdasarkan teori pendukung diatas, penulis berinisiatif dianalisis performansi protokol routing AOMDV (*Ad hoc On-Demand Multipath Distance Vector*) pada jaringan MANET ketika terkena serangan *Malicious Node*, DdoS, dan gabungan keduanya . Pemilihan Protokol Routing AOMDV dalam penelitian ini dikarenakan protokol ini merupakan protokol pengembangan dari AODV (*Ad hoc On-Demand Distance Vector*) dengan perbedaan berbasis multipath. Analisis yang dibahas meliputi beberapa parameter kinerja protokol routing dalam MANET (Mobile Adhoc Network) seperti *Throughput*, *Delay*total dan PDR

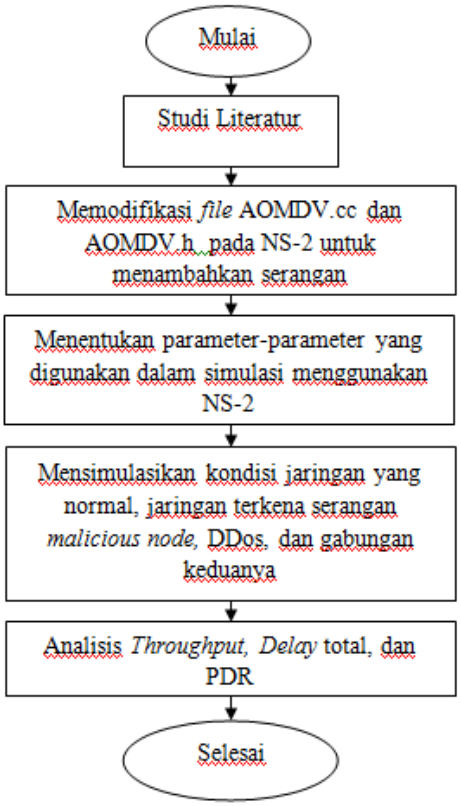
Maksud dan tujuan pembuatan pembuatan tugas akhir ini adalah :

1. Menganalisiskehandalan Protokol AOMDV pada kondisi terkena serangan Malicious Node.
2. Menganalisiskehandalan Protokol AOMDV pada kondisi terkena serangan DDoS.
3. Menganalisis kehandalan Protokol AOMDV pada kondisi terkena serangan *Malicious Node* dan *DDoS*.

2. Metode

2.1. Langkah Penelitian

Metode penelitian tugas akhir ini menjelaskan mengenai proses penelitian evaluasi kinerja protokol AOMDV dengan serangan *malicious node* dan DDoS pada MANET menggunakan NS-2
Gambar 1 berikut adalah langkah penelitian yang dilakukan pada tugas akhir ini:



Gambar 1. Langkah Penelitian

2.2. Studi Literatur

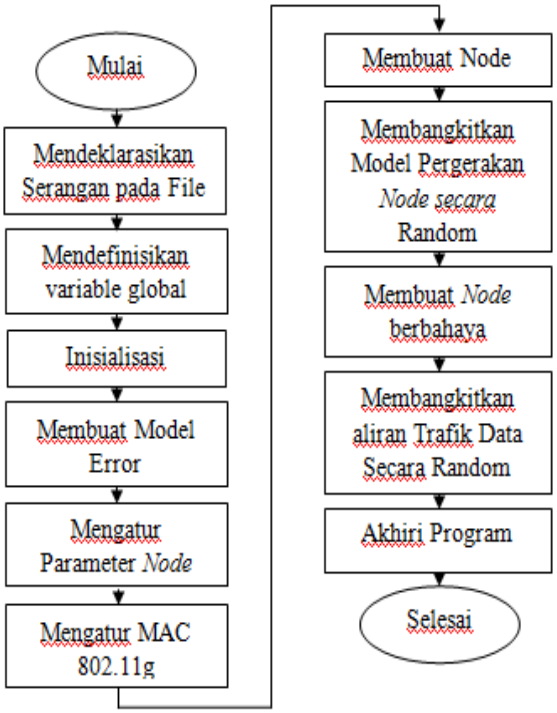
Langkah pertama yang perlu dilakukan dalam suatu penelitian yaitu melakukan studi literatur. Studi literatur merupakan proses pembelajaran terhadap objek yang akan diteliti, dalam hal ini tentang kinerja protokol *routing* MANET AOMDV serta serangan *malicious node* dan DDoS. Tujuan dari studi literatur yaitu untuk mendapatkan landasan teori mengenai kinerja protokol *routing* MANET AOMDV serta serangan *malicious node* dan DDoS.. Selain itu, objek studi literatur diarahkan ke perangkat lunak atau *software* simulasi jaringan yang dalam penelitian ini menggunakan *software* NS-2

2.3. Pengumpulan Data

Pada penelitian ini, dilakukan pengulangan pengambilan data sebanyak 5 kali lalu diambil data rata-rata dan deviasinya. Pada simulasi ini, pengambilan data pengujian dilakukan dengan cara parsing menggunakan awk. Senarai awk dibentuk untuk mengambil data yang diperlukan dari file trace. File awk digunakan untuk menghitung parameter kinerja jaringan, yaitu packet delivery ratio, throughput, dan delay total. Pada simulasi ini terdapat file awk untuk masing-masing parameter kinerja jaringan

2.4. Simulasi *Software* NS-2

Diagram alir simulasi dengan menggunakan software NS-2 dapat dilihat pada Gambar 2.



Gambar 2. Simulasi *Software* NS-2

Langkah pertama dalam menjalankan simulasi jaringan yaitu mendeklarasikan serangan pada file protokol AOMDV.cc dan AOMDV.h. Selanjutnya, Mendefinisikan Variable global pada file tcl. .Kemudian setelah itu, inisialisasi variable umum yang digunakan pada simulasi. Lalu membuat model error. Setelah itu mengatur parameter-parameter *node.* Selanjutnya mengatur parameter penggunaan MAC 802.11g. Setelah melakukan pengaturan pada parameter-parameter node selanjutnya adalah membuat node. Pembangkitan model pergerakan node dilakukan dengan bantuan program generator yang telah ada dalam NS-2. Lalu pembangkitan attack node dilakukan agar serangan dapat aktif dalam jaringan yaitu untuk *node malicious* dan DDoS.Pada simulasi ini, model trafik dibangkitkan secara random dengan menggunakan generator CMU yang ada di dalam NS-2. Untuk mengakhiri program simulasi, waktu henti yang menandakan simulasi telah selesai perlu ditetapkan dan juga node harus diatur ulang (reset). Skenario yang digunakan pada Tugas Akhir ini ada tiga yaitu kondisi jaringan saat terkena serangan malicious node, DDoS, dan saat terkena serangan malicious node dan DDoS secara bersamaan. Pada skenario saat jaringan terkena serangan malicious node, digunakan 3 sampai 15 node penyerang. Sedangkan pada skenario saat jaringan terkena serangan DDoS dilakukan tiga kali variasi node penyerang, yaitu dari 3 *node* sampai 15 *node*. Skenario yang terakhir adalah ketika jaringan terkena serangan malicious node dan DDoS secara bersamaan dengan jumlah node penyerang yaitu masing-masing 3 sampai 8 node penyerang. Serangan diberikan kepada jenis paket FTP. Tujuan dari pembagian skenario ini adalah untuk menguji kinerja protokol AOMDV pada jaringan dengan paket yang berbeda-beda saat terkena serangan sehingga didapatkan hasil kinerja yang efektif dari protokol tersebut.Dari hasil simulasi jaringan eksisting, kemudian dilakukan analisis pada nilai kinerjanya yaitu PDR, *throughput*, dan *delay* total.

2.5. Perhitungan PDR

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

Pada penelitian ini, untuk menghitung *Packet Delivery Ratio* (PDR) dapat menggunakan persamaan

$$PDR = \left(\frac{\sum_{i=T_t}^{i=T_t+1} R_i}{\sum_{i=T_t}^{i=T_t+1} S_i} \right) \times 100 \quad ; \; 0 \le t \le T \quad (1)$$

Keterangan :
Ri = Jumlah paket yang diterima oleh nodepenerima (paket)
Si = Jumlah paket yang dikirim oleh node pengirim (paket)
Tt = Waktu pengambilan sample (detik)

2.6. Perhitungan *Throughput*

Throughput adalah jumlah paket data yang diterima per detik. Throughput bisa disebut sebagai bandwidth dalam kondisi yang sebenarnya. bandwidth lebih bersifat tetap, sementara throughput sifatnya dinamis tergantung trafik yang sedang terjadi. Throughput mempunyai satuan bps (bit per second) berikut rumus untuk menghitung throughput pada sebuah jaringan

$$Throughput = \sum_{i=T_t}^{i=T_t+1} Pi \quad ; \; 0 \le t \le T \; (2)$$

Keterangan :
P_i = Paket data yang diterima (byte)
T_t = Waktu pengambilan *sample* (detik)
T = Waktu pengamatan (detik)

2.7. Perhitungan *Delay Total*

Delay adalah total waktu tunda suatu paket yang diakibatkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya.

$$Delay = \frac{\sum_{i=T_t}^{i=T_{t+1}} RT_i - \sum_{i=T_t}^{i=T_t+1} ST_i}{\sum_{i=T_t}^{i=T_t+1} R_i} \quad ; \quad 0 \le t \le T \quad (3)$$

Keterangan :

RT_i = Waktu penerimaan paket (detik)

ST_i = Waktu pengiriman paket (detik)

R_i = Paket yang diterima selama (paket)

2.8. Teorema Little

Teorema Little berfungsi untuk mengetahui jumlah paket rata-rata yang berada pada sistem dalam suatu waktu.

$$N = \lambda T \quad (4)$$

Keterangan :

N = Jumlah paket rata-rata dalam sistem (paket)

λ = Laju kedatangan paket (paket/detik)

T = Delay Total (detik)

3. Analisis Hasil Simulasi

3.1. Kondisi Jaringan Terkena Serangan *Malicious Node*

Berdasarkan simulasi didapatkan data statistika kondisi jaringan dengan protokol AOMDV yang terkena serangan *Malicious Node* seperti ditunjukkan pada tabel 1.

Tabel 1. Statistika Jaringan pada Kondisi Jaringan Terkena Serangan *Malicious Node*

Jumlah *Node Malicious* (*Node*)	Total paket informasi yang dikirim (Paket)	Total Paket Informasi yang hilang (Paket)	Total Paket yang Hilang Karena Serangan (Paket)
3	29.176	1.682	17
4	28.308	1.808	19
5	27.351	1.768	21
6	28.099	3.420	22

Tabel 1. Lanjutan

Jumlah *Node Malicious* (*Node*)	Total paket informasi yang dikirim (Paket)	Total Paket Informasi yang hilang (Paket)	Total Paket yang Hilang Karena Serangan (Paket)
7	30.045	1.868	25
8	29.183	1.619	28
9	27.867	1.714	30
10	27.251	1.696	29
11	26.601	1.414	29
12	25.326	1.682	17
13	26.099	1.414	29
14	26.099	1.414	29
15	27.055	1.477	39

Dari tabel 1 penurunan terbesar untuk jumlah paket informasi yang dikirim pada jaringan yang terkena serangan malicious node dengan node malicious sebanyak 12 node. Paket informasi yang dikirim pada kondisi normal sebesar 38.304 paket namun menurun jumlahnya menjadi 25.326 paket, sehingga penurunan jumlah paket informasi yang dikirim sebesar 12.978 paket atau sebesar 33,88 %. Yang dapat menandakan serangan ini aktif adalah dengan melihat bahwa semakin banyak total paket yang hilang karena serangan. Pada saat node malicious berjumlah 12 dan 15 node dapat menunjukkan total paket yang hilang karena serangan terbesar yaitu sebanyak 29 paket sementara pada kondisi normal tidak ada.

3.2. Kondisi Jaringan Terkena Serangan DDoS

Berdasarkan simulasi didapatkan data statistika kondisi jaringan dengan protokol AOMDV yang terkena serangan *DDoS*seperti ditunjukkan pada tabel 2.

Tabel 2. Statistika Jaringan pada Kondisi Jaringan Terkena Serangan DDoS

Jumlah *Node* DDoS (*Node*)	Total paket informasi yang dikirim (Paket)	Total Paket *Request* yang dikirim (Paket)	Intensitas trafik (Erlang)
3	33.880	54.226	0,926
4	32.701	68.498	0,963
5	32.052	101.204	1,034
6	31.970	102.325	1,078
7	31.469	103.818	1,079
8	28.721	110.245	1,082
9	28.665	117.361	1,098
10	27.513	123.131	1,162
11	27.312	125.829	1,192
12	26.896	137.216	1,194
13	26.417	138.779	1,196

Tabel 2. Lanjutan

Jumlah *Node* DDoS (*Node*)	Total paket informasi yang dikirim (Paket)	Total Paket *Request* yang dikirim (Paket)	Intensitas trafik (Erlang)
14	26.360	182.127	1,216
15	25.684	216.532	1,203

Dari tabel 2 penurunan total paket yang dikirim adalah sebesar 12.620 paket atau sebesar 19,72 % saat 15 node DDoS aktif.. Selain itu, peningkatan total paket *request* yang dikirim adalah sebesar 210.850 paket atau sebesar 94,89 % saat 15*node* DDoS aktif. Perubahan yang lain pada saat serangan DDoS aktif adalah jumlah intensitas trafiknya. Intensitas trafik pada saat jaringan terkena serangan DDoSmeningkat hingga 0,285 erlang atau sebesar 13,43 % dari kondisi normalnya.

3.3. Kondisi Jaringan Terkena Serangan *Malicious Node* dan DDoS

Berdasarkan simulasi didapatkan data statistika kondisi jaringan dengan protokol AOMDV yang terkena serangan *DDoS* seperti ditunjukkan pada tabel 3.

Tabel 3. Statistika Jaringan pada Kondisi Jaringan Terkena Serangan DDoS

Jumlah *Node* DDoS (*Node*)	Total paket informasi yang dikirim (Paket)	Total Paket *Request* yang dikirim (Paket)	Total Paket Informasi hilang karena serangan (Paket)
3	26.881	53.255	11
4	26.788	65.718	14
5	26.463	89.326	22
6	26.164	89.488	22
7	25.944	100.118	26
8	25.370	109.281	21

Dari tabel 3 menunjukkan paket informasi yang dikirim pada kondisi normal sebesar 38.304 paket namun menurun jumlahnya menjadi 25.370 paket, sehingga penurunan jumlah paket informasi yang dikirim sebesar 7.873 paket atau sebesar 33,77 %.. Selain itu saat serangan DDoS aktif maka node DDoS akan membanjiri jaringan dengan RREQ sehingga menyebabkan peningkatan total paket request yang dikirim. Paket informasi yang dikirim pada kondisi normal sebesar 5.682 paket namun meningkat jumlahnya saat 8 node malicious dan DDoS aktif menjadi 109.281 paket, sehingga peningkatan jumlah paket informasi yang dikirim sebesar 103.599 paket atau sebesar 94,8 %. Yang dapat menandakan serangan ini aktif adalah dengan mengetahui bahwa total paket yang hilang disebabkan karena serangan ini aktif adalah jumlah total paket yang hilang karena serangan dengan keterangan 'LOOP' pada tracefile. Pada saat node malicious berjumlah 7 node dapat menunjukkan total paket yang hilang karena serangan terbesar yaitu sebanyak 26 paket sementara pada kondisi normal tidak ada.

3.4. Analisis *Packet Delivery Ratio* (PDR)

Berdasarkan simulasi dan perhitungan parameter kinerja protokol AOMDV pada jaringan dengan file awk, maka didapatkan data kinerja AOMDV yang ditunjukkan pada tabel 4.

Tabel 4. Nilai PDR rata-rata dan standar deviasi jaringan saat terkena serangan *Malicious Node, DdoS* dan keduanya secara bersamaan

Skenario	Jenis Trafik	Jumlah Node Penyerang (node)	PDR Rata-Rata (%)	Deviasi
Normal	FTP	-	95,09	0,01
Malicious Node	FTP	3	93,06	0,05
		4	92,57	0,03
		5	91,68	0,06
		6	92,33	0,05
		7	93,11	0,03
		8	93,76	0,03
		9	90,01	0,11
		10	91,95	0,06
		11	91,50	0,02
		12	94,12	0,02
		13	93,87	0,02
		14	93,87	0,02
		15	93,16	0,05
DdoS	FTP	3	94,22	0,02
		4	93,81	0,02
		5	93,81	0,01
		6	93,23	0,01
		7	93,18	0,01
		8	92,90	0,00
		9	92,78	0,01
		10	92,52	0,01
		11	92,49	0,01
		12	92,34	0,01
		13	92,24	0,01
		14	92,20	0,01
		15	91,92	0,02
Malicious node dan DdoS	FTP	3	93,90	0,02
		4	93,84	0,03
		5	93,36	0,04
		6	93,34	0,04
		7	92,23	0,08
		8	91,07	0,10

Dari tabel 4 dapat dilihat bahwa pada trafik FTP dengan protokol AOMDV, serangan yang dapat memberikan efek paling besar adalah serangan *malicious node*. Efek paling besar ini terjadi pada saat jumlah node malicious sebanyak 9 node, dimana nilai PDR yang didapatkan sebanyak 90,01 % , sehingga nilai penurunan PDR sebesar 5,08 % dari kondisi normalnya yaitu 95.10 %

3.5. Analisis *Throughput*

Dari hasil simulasi dan perhitungan parameter kinerja protokol AOMDV pada jaringan dengan file awk, maka didapatkan data kinerja AOMDV yang ditunjukkan pada tabel 5.

Tabel 5. Nilai *Throughput* rata-rata dan standar deviasi jaringan saat terkena serangan *Malicious Node, DdoS* dan keduanya secara bersamaan

Skenario	Jenis Trafik	Jumlah Node Penyerang (node)	*Throughput* Rata-Rata (Kbps)	Deviasi
Normal	FTP	-	434	112,32
Malicious Node	FTP	3	331	99,57
		4	321	116,09
		5	310	117,50
		6	299	97,12
		7	341	97,97
		8	331	95,28
		9	316	144,61
		10	309	140,69
		11	302	121,44
		12	288	115,39
		13	296	121,44
		14	296	121,44
		15	307	116,69
DDoS	FTP	3	381	98,95
		4	368	88,97
		5	357	59,74
		6	353	54,97
		7	347	43,77
		8	334	51,46
		9	333	54,92
		10	330	57,97

		11	329	52,89
		12	324	51,53
		13	321	50,68
		14	319	51,84
		15	317	51,16
		3	310	93,96
		4	306	122,50
Malicious node dan *DDoS*	FTP	5	305	107,71
		6	305	118,49
		7	294	112,68
		8	288	139,63

Dari tabel 5 dapat dilihat bahwa saat serangan pada trafik FTP, serangan yang memberikan efek paling besar adalah serangan *malicious node* dan DDoS. Efek paling besar ini terjadi pada saat masing-masing jumlah node malicious dan DDoS sebanyak 8 node, dimana nilai throughput yang didapatkan sebanyak 288 Kbps , sehingga nilai penurunan Throughput sebesar 146 Kbps atau sebesar 33,76 % dibandingkan dengan kondisi normalnya yaitu 434 Kbps.

3.6. Analisis Delay

Dari hasil simulasi dan perhitungan parameter kinerja protokol AOMDV pada jaringan dengan file awk, maka didapatkan data kinerja AOMDV yang ditunjukkan pada tabel 6. Data tersebut didapat dengan melakukan pengulangan pengambilan data secara random sebanyak 5 kali. Kemudian diambil data rata-rata dan deviasinya

Tabel 6. Nilai *Delay* rata-rata dan standar deviasi jaringan saat terkena serangan *Malicious Node, DdoS,* dan keduanya secara bersamaan

Skenario	Jenis Trafik	Jumlah Node Penyerang (node)	*Delay* Total (ms)	Deviasi
Normal	FTP	-	156,10	14,28
		3	156,00	32,00
		4	155,72	32,89
		5	149,72	43,38
		6	153,47	32,41
		7	154,37	33,38
		8	155,67	30,17
Malicious Node	FTP	9	142,30	38,56
		10	154,60	46,64
		11	151,68	39,13
		12	155,98	42,22
		13	155,96	39,13
		14	155,96	39,13
		15	154,46	38,64
		3	161,77	16,13
		4	162,20	7,39
		5	164,58	15,08
		6	167,98	12,19
		7	166,33	12,78
		8	169,65	11,31
DDoS	FTP	9	169,76	13,80
		10	171,75	15,08
		11	171,95	26,46
		12	173,23	15,41
		13	176,47	27,06
		14	176,78	27,39
		15	178,80	123,68
		3	155,87	44,82
		4	156,50	37,10
Malicious node dan *DDoS*	FTP	5	157,39	42,68
		6	157,61	19,18
		7	161,29	43,90
		8	166,30	53,37

Dari tabel. 6 menunjukkan kondisi peningkatan delay pada saat serangan DDoS aktif pada trafik FTP, efek paling besar ini terjadi pada saat jumlah node DDoS sebanyak 15 node, dimana nilai Delay total meningkat sebanyak 22,71 ms atau sebesar 12,70 %. dibandingkan dengan kondisi normalnya yaitu 156,10 ms. Kondisi penurunan nilai delay pada saat serangan malicious node aktif, efek paling besar ini terjadi pada saat jumlah node malicious sebanyak 9 node, dimana nilai Delay total menurun menjadi 13,8 ms atau 8,84 % dari kondisi normalnya yaitu 156,10 ms.

3.7. Analisa Teorema Little

Dengan menerapkan teorema Little dan dengan data yang sudah didapatkan, maka dapat diketahui jumlah paket yang berada pada sistem yang ditunjukkan pada Tabel 7. Data tersebut didapat dengan melakukan pengulangan pengambilan data secara random sebanyak 5 kali. Kemudian Jumlah paket dalam sistem (N) hasil perhitungan akan dibandingkan dengan jumlah paket dalam sistem (N) hasil pengamatan.

Tabel 7. Nilai jumlah paket dalam sistem pada jaringan saat terkena serangan *Malicious Node, DdoS,* dan keduanya secara bersamaan

Skenario	Jenis Trafik	Jumlah node penyerang (*node*)	Jumlah Paket antrian dalam sistem (N) hasil Perhitungan (Paket)	Jumlah Paket antrian dalam sistem (N) hasil Pengamatan (Paket)
Normal	FTP	-	100	100
		3	85	85
		4	76	76
		5	73	73
		6	79	79
		7	85	85
		8	68	68
Malicious Node	FTP	9	85	85
		10	75	75
		11	73	73
		12	71	71
		13	67	67
		14	67	67
		15	71	71
		3	118	118
		4	121	121
		5	130	130
DDoS	FTP	6	135	135
		7	136	136
		8	139	139

		9	143	143
		10	152	152
		11	157	157

Tabel 7. Lanjutan

Skenario	Jenis Trafik	Jumlah node penyerang (*node*)	Jumlah Paket antrian dalam sistem (N) hasil Perhitungan (Paket)	Jumlah Paket antrian dalam sistem (N) hasil Pengamatan (Paket)
DDoS	FTP	12	158	158
		13	164	164
		14	170	170
		15	171	171
Malicious node dan *DDoS*	FTP	3	98	98
		4	103	103
		5	116	116
		6	117	117
		7	121	121
		8	128	128

Dari Tabel 7. diperoleh hasil nilai antrian dalam sistem hasil perhitungan dan hasil pengamatan. Adanya selisih hasil jumlah antrian dalam sistem hasil perhitungan dengan hasil pengamatan disebabkan oleh ketidak presisian pembulatan angka dalam menghitung pada perhitungan dikarenakan banyaknya data yang harus diolah.

4. Kesimpulan

1. Pada kondisi jaringan yang terkena serangan malicious node, penurunan jumlah paket yang dikirim pada jaringan yang terkena serangan malicious node terbesar saat 12 node malicious aktif yaitu sebesar 12.978 paket atau sebesar 33,88 % dari kondisi normal. Sementara peningkatan jumlah total paket informasi yang hilang karena serangan dari kondisi normal sebesar paket.
2. Pada kondisi jaringan yang terkena serangan DDoS Penurunan total paket yang dikirim adalah sebesar 12.620 paket atau sebesar 19,72% saat 15 node DDoS aktif. Sementara peningkatan total paket request yang dikirim adalah sebesar 210.850 paket atau sebesar 94,89 % saat 15 node DDoS aktif. Sementara itu, intensitas trafik pada saat jaringan terkena serangan DDoS meningkat hingga 0,285 erlang atau sebesar 13,43 % dari kondisi normalnya
3. Pada kondisi jaringan yang terkena serangan malicious node dan DDoS. Penurunan total paket yang dikirim adalah sebesar 7.873 paket atau sebesar 33,77 % saat 8 node malicious dan DDoS aktif Sementara peningkatan total paket request yang dikirim adalah sebesar 103.599 paket atau sebesar 94,8 % saat 8 node malicious dan DDoS aktif. Sementara peningkatan jumlah total paket informasi yang hilang karena serangan dari kondisi normal sebesar 26 paket saat 7 node malicious dan DDoS aktif
4. Untuk penurunan nilai PDR yang paling besar pada kondisi jaringan yang terkena serangan malicious node dengan jumlah node malicious sebesar 9 node, dimana nilai PDR yang didapatkan sebanyak 90,01 % , sehingga nilai penurunan PDR sebesar 5,08 % dari kondisi normalnya yaitu 95,10 %
5. Penurunan nilai Throughput yang paling besar terjadi pada kondisi jaringan yang terkena serangan gabungan maliciousnode dan DDoS dengan jumlah node malicious dan DDoS sebesar 8 node, dimana nilai throughput yang didapatkan sebesar 288 Kbps , sehingga nilai penurunan Throughput sebesar 146 Kbps atau sebesar 33,76 % dibandingkan dengan kondisi normalnya yaitu 434 Kbps
6. Pada kondisi jaringan dengan serangan DDoS memiliki efek paling besar dalam peningkatan nilai delay total, yaitu saat jumlah node DDoS sebanyak 15 node. Nilai Delay total yang didapatkan sebanyak 178,806 ms. Sehingga nilai peningkatan delay total nya sebesar sebesar 22,711 ms atau sebesar 6,78 % dibandingkan dengan kondisi normalnya yaitu 156,095 ms. Sementara pada kondisi jaringan dengan serangan malicious node memberikan efek paling besar dalam penurunan nilai delay total, yaitu saat jumlah node malicious sebesar 9 node. Nilai Delay total yang menurun 13,8 ms atau 8,84 % dari kondisi normalnya yaitu 156,10 ms.

Referensi

[1]. Kaur, Gaujinder dan Jain, V. K.," Distributed Denial Of Sevice Attack in Mobile Adhoc Network", dalam World Academy of Science, Engineering and Technology, Vol.55, Jan. 2011

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

[3]. Gang, Sachin, "Performance Analysis of AODV and TORA under DDoS Attack in MANETs", dalam IJSR ISSN (online : 2319-7064), Vol. 3 Issue 10, Okt., 2014

[4]. Dahiya, Brahm Prakash, "Performance Analysis and Evaluation of AODV & AOMDV in MANET", dalam IJAREEIE Vol.3, Issue 1, Jan., 2014

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

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

[7]. Andini. Sarah Setya, Rahardjo. Tegug Budi, dan Nugraha. Eko"IEEE 802.11g" Jurusan Teknik Elektro UGM

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

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

[10]. Sharma. Ritika dan Gupta. Kamlesh, "Comparison based Performance Analysis of UDP/CBR and TCP/FTP Traffic under AODV Routing Protocol in MANET", International Journal of Computer Application, Vol. 56-No.15, 2012

[11]. C.P Agrawal, O.P Vyas, dan M.K Tiwari, "Evaluation of Varrying Mobility Models & Network Loads on DSDV Protocol of MANETs" dalam IJCSEA Vol.1 No.12, 2009.

[12]. Kumar. Ashish, Sharma. Ajay K., dan Singh. Arun, "Comparison and Analysis of Drop Tail and RED Queuing Methodology in PIM-DM Multicasting Network", dalam IJCSIT. Vol. 3 (2), 2012.

[13]. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[14]. S. Lu, L. Li, K.Y. Lam, dan L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," dalam International Conference on Computational Intelligence and Security, 2009.

[15]. Harahap. Evi Hartati, " Analisi Performansi Protokol AODV dan DSR Terhadap Active Attack pada MANET ditinjau dari QOS Jaringan" Makalah Tugas Akhir, dari Telkom University, Bandung, Indonesia, 2011.

[16]. Putri, Rizky A., Jusak, Sukmaji, Anjik, "Analisis Perbandingan Kinerja On-Demand Routing Pada Jaringan Sensor Nirkabel Ad Hoc", Laporan Tugas Akhir Jurusan Sistem Komputer STMIK STIKOM, Surabaya, 2013.