EVALUASI KINERJA PROTOKOL AOMDV TERHADAP SERANGAN *RUSHING* DAN *FLOODING* PADA MANET DENGAN MENGGUNAKAN NETWORK SIMULATOR 2 (NS-2)

Muhamad Rifqi Rifquddin[*)], Sukiswo, and Ajub Ajulian Zahra

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

[*)] *Email: mrifqi.rifquddin@gmail.com*

Abstrak

Teknologi MANET berkembang ketika pengguna perangkat bergerak dihadapkan pada suatu keadaan tanpa adanya dukungan infrastruktur jaringan tetap. Teknologi ini memungkinkan komunikasi tanpa adanya infrastruktur yang tetap. Tingginya mobilitas pada jaringan MANET membuatnya sangat rentan terhadap serangan. Serangan pada MANET dapat merusak skema routing yang dibentuk protokol routing. Pada penelitian ini dirancang jaringan MANET dengan menggunakan protokol routing AOMDV. Jaringan disimulasikan menggunakan Network Simulatior 2 v2.35. Jaringan ini diberikan serangan rushing dan flooding. Terdapat 3 skenario yang digunakan dalam penelitian ini, yaitu kondisi jaringan terkena serangan rushing, serangan flooding, dan serangan rushing dan flooding bersamaan. Parameter yang digunakan dalam analisis performansi protokol AOMDV adalah Packet Delivery Ratio (PDR), Throughput, dan Delay. Hasil simulasi menunjukkan penurunan performansi terbesar jaringan dengan protokol AOMDV untuk nilai packet delivery ratio dan throughput terjadi saat terkena serangan rushing dan flooding bersamaan dengan jumlah node flooder sebanyak 10 node. Nilai Packet Delivery Ratio menurun sebesar 17,596%. Nilai throughput mengalami penurunan sebesar 84,23 %. Nilai delay mengalami peningkatan terbesar pada kondisi terkena serangan flooding dengan 10 node flooder. Nilai delay meningkat dari kondisi normal sebesar 59,15 ms menjadi 269,734 ms pada kondisi flooding 10 node flooder.

Kata kunci : MANET, Network Simulator 2, AOMDV, Rushing, Flooding

Abstract

MANET technology develops when the mobile device users are faced situation without support of a fixed network infrastructure. This technology allows communication without a fixed infrastructure. The high mobility in MANET network makes it very vulnerable to attack. Attacks in MANET can destructive routing scheme formed by routing protocols. This study designed a MANET network using a routing protocol AOMDV. Network Simulatior 2 v2.35 is used to simulated this network. In this network is given the rushing and flooding attack. There are three scenarios used in this study, namely network conditions exposed rushing attack, flooding attacks, and the rushing and flooding attack simultaneously. The parameters used in analysis AOMDV protocol is Packet Delivery Ratio (PDR), Throughput, and Delay. Simulation results obtained AOMDV protocol has largest decrease network performance for Packet Delivery Ratio dan throughput value in rushing and flooding attack combination with 10 nodes flooder. Packet Delivery Ratio value is decreased by 17,596 %. Throughput value is decreased by 84,23 %. Delay value has the largest increase in flooding attack condition with 10 nodes flooder. Delay value increases from the normal conditions of 59,15 ms becomes 269,734 ms.

Keywords : MANET, Network Simulator 2, AOMDV, Rushing, Flooding

1. Pendahuluan

Teknologi MANET berkembang ketika pengguna perangkat bergerak dihadapkan pada suatu keadaan tanpa adanya dukungan infrastruktur jaringan yang dapat digunakan. Teknologi ini memungkinkan komunikasi tanpa adanya infrastruktur yang tetap. Teknologi MANET merupakan pengembangan dari teknologi jaringan Ad Hoc (jaringan tanpa kabel tanpa infrastruktur).

Mobile Ad Hoc Network (MANET) adalah jaringan wireless yang terdiri dari mobile- mobile *node* yang tidak

memiliki infrastruktur. Jaringan ini merupakan salah satu mode jaringan *ad hoc* nirkabel dengan pengguna pada jaringan ini bersifat *mobile*. Pada MANET, *node* bebas datang dan meninggalkan jaringan, *node* juga bebas bergerak atau diam pada posisinya. Komunikasi pada MANET dilakukan melalui antar *node* dengan tiap *node* berfungsi sebagai router untuk meneruskan data yang dikirimkan. Untuk berkomunikasi ini dibutuhkan protokol routing yang berfungsi membentuk jalur untuk mengirimkan data dari sumber ke tujuan.

Tingginya mobilitas pada jaringan MANET membuatnya sangat rentan terhadap serangan. Serangan pada MANET dapat menggagalkan dan merusak skema routing yang dibentuk protokol routing. Serangan juga dapat mencuri atau membuang data yang dikirimkan sumber sehingga data tidak sampai ke tujuan. Serangan pada MANET umumnya terjadi pada sistem routing yang telah dibentuk oleh protokol routing.

Dalam tugas akhir ini dianalisis performansi protokol *routing* AOMDV (*Ad hoc On-Demand Multi path Distance Vector*) pada jaringan MANET ketika terkena serangan *Rushing dan Flooding*. Pemilihan Protokol *Routing* AOMDV dikarenakan protokol ini merupakan protokol pengembangan dari AODV dengan perbedaan berbasis *multipath* dan memiliki jalur cadangan saat jalur utama rusak.

Pemilihan jenis serangan *rushing* dan *flooding* memiliki alasan tersendiri. Serangan *rushing* ini membuat paket melalui *node rushing*. Ketika paket melalui jalur *node rushing* maka paket dapat diperlakukan seperti apapun yang diinginkan penyerang. Dalam penelitian ini paket data dibuang untuk menandakan serangan *rushing* bekerja.

Serangan *flooding* merupakan serangan yang memenuhi jaringan dengan RREQ buatan *node flooder* yang tidak berguna dalam jaringan. Serangan ini berbahaya dalam jaringan karena akan membuat paket yang berisi data harus menunggu untuk dilayani jaringan. Serangan *rushing* dan *flooding* yang berbahaya untuk jaringan menarik untuk diteliti.

2 Metode

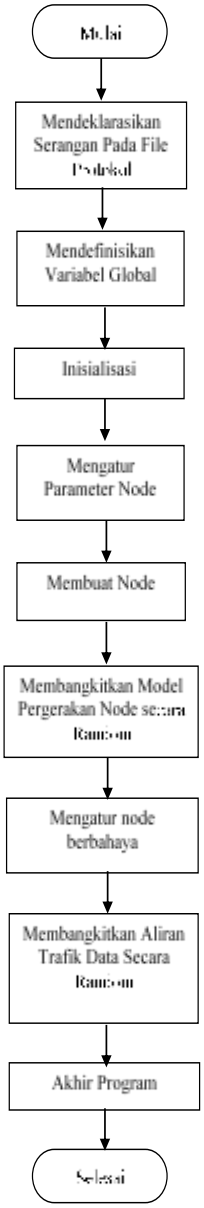
2.1 Simulasi Jaringan MANET

Pembuatan skenario dalam simulasi ini dibagi menjadi beberapa variasi skenario. Skenario pertama yaitu jaringan terkena serangan *Rushing*. Skenario kedua adalah jaringan terkena serangan *Flooding*. Skenario ketiga adalah jaringan terkena serangan *Rushing* dan *Flooding* secara bersamaan. Jumlah *node Flooder* divariasi sebanyak 1, 2, 3, 4, 5, 6, 7, 8, 9, dan 10 *node*, sedangkan Jumlah *node Rushing* dibuat sebanyak 5 *node*. Pola trafik yang dibangkitkan dalam skenario ini adalah TCP.

Pada simulasi ini, *node* tujuan akan meminta paket dengan ukuran yang acak kepada *node* sumber. Selain itu, pada simulasi ini digunakan model pergerakan *node* yang random. Model pergerakan dibangkitkan sebanyak 5 kali dengan persebaran berbeda-beda. Pengambilan data hasil simulasi akan dilakukan sebanyak 5 kali pengulangan sesuai dengan persebaran model pergerakan yang berbeda-beda. Dari masing-masing model akan diambil data hasil simulasi, kemudian dari data-data tersebut akan diambil nilai rata-rata. Nilai rata-rata tersebut yang kemudian akan dianalisis. Dari nilai-nilai tersebut menghasilkan nilai standar deviasi untuk masing-masing skenario.

2.2 Perancangan Sistem

Pada Tugas Akhir ini dibuat suatu jaringan MANET dengan menggunakan Network Simulator 2. Secara keseluruhan, tahapan pembuatan simulasi ditunjukkan pada gambar 1.



Gambar 1. Diagram alir simulasi

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

Tabel 1. Parameter simulasi

Parameter	Nilai
MAC Type	IEEE 802.11g
Jenis Antena	Omni Directional
Model Propagasi	Two Ray Ground
Tipe Protokol Routing	AOMDV
Disiplin antrian	Droptail
Jumlah node	50
Dimensi topografi	850x850 m^2
Durasi simulasi	200 detik
Model Pergerakan *node*	*Random Waypoint*
Jenis trafik	TCP
Jenis serangan	*Rushing* dan *Flooding*

2.3 Metode Pengambilan Data

Data hasil simulasi tersedia dalam bentuk *trace file. Trace file* berisi semua kejadian yang terjadi pada saat simulasi berjalan. Dari *trace file* dapat diambil data yang diinginkan. Data dapat diambil dengan menggunakan *file awk.* Data kemudian diolah untuk mendapatkan nilai parameter performansi jaringan.

Penilaian performansi jaringan terdiri dari beberapa parameter yaitu : [25]

1. *Packet Delivery Ratio (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.

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

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

2. *Throughput*

   Throughput adalah laju rata-rata dari paket data perdetik yang berhasil diterima melalui kanal komunikasi.

$$\text{Throughput} = \sum_{i=T_t}^{i=T_{t+1}} P_i \qquad ; 0 \le t \le T \qquad (2)$$

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

3. Waktu Tunda

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

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

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

ITU-T G.114 merekomendasikan waktu tunda tidak lebih besar dari 150 ms untuk berbagai aplikasi, dengan batas 400 ms yang masih dapat diterima untuk komunikasi suara. [26] Nilai delay dapat divalidasi dengan menggunakan *teorema little* yang ditunjukkan pada persamaan 4. Validasi dapat dilakukan dengan

membandingkan nilai jumlah paket rata-rata dalam sistem dengan jumlah paket rata-rata saat simulasi dilakukan.

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

Keterangan :
N = Jumlah paket rata- rata dalam sistem (paket)
λ = laju kedatangan (paket/detik)
T = waktu rata-rata dalam sistem (detik)

3. Hasil dan Analisis

3.1 Statistik Simulasi

3.1.1 Kondisi Normal

Kondisi jaringan normal merupakan kondisi saat jaringan dengan protokol AOMDV tidak mengalami serangan. Kondisi ini menjadi acuan untuk mengevaluasi kinerja AOMDV saat terkena serangan. Pada kondisi normal ini didapatkan statistik keadaan jaringan saat simulasi dijalankan. Statistik ini ditunjukkan pada tabel 2

.

Tabel 2. Statistik simulasi pada kondisi normal

Skenario	Paket data kirim (pkt)	Paket Hello kirim (pkt)	Paket data terima (pkt)	Paket Hello terima (pkt)	Paket yang hilang (pkt)
I	3812	11640	3740	152522	72
II	3840	11972	3779	154017	61
III	3811	12659	3780	148109	31
IV	3897	12333	3794	137533	103
V	3950	14977	3824	142013	126
Rata-rata	**3862**	**12717**	**3784**	**146839**	**78**

Tabel 2 berisi data yang nantinya akan berubah jika terkena serangan. Data ini merupakan data permintaan dari penerima dengan semua data dapat terkirim dalam waktu simulasi yang ditetapkan.

3.1.2 Kondisi *Rushing*

Statistik kejadian yang ada pada saat protokol AOMDV terserang *rushing* ditunjukkan pada tabel 3.

Tabel 3. Statistik simulasi pada kondisi *rushing*

Skenario	Paket Data kirim (pkt)	Paket Hello kirim (pkt)	Paket Data terima (pkt)	Paket Hello terima (pkt)	Total paket hilang (pkt)	Paket hilang karena *rushing* (pkt)
I	3090	11655	3003	158188	87	57
II	3858	12521	3717	157674	141	92
III	2696	11976	2625	155563	71	56
IV	2576	13293	2469	151407	107	87
V	3052	13938	2936	147399	116	65
Rata-rata	**3055**	**12677**	**2950**	**154047**	**105**	**72**

Serangan *rushing* membuat jumlah paket yang dikirim dan diterima lebih sedikit dibandingkan dengan kondisi normal. Pada tabel 3 terlihat rata-rata paket data yang diterima menurun sebesar 22,04%. Kondisi paket dikirim lebih sedikit terjadi karena *node rushing* terus menerus membuang paket yang dikirimkan ketika melewatinya. Serangan *rushing* membuat pengiriman paket menjadi gagal. Ketika paket yang dikirim terus menerus dibuang maka jumlah paket yang diterima tidak akan sesuai dengan permintaan paket yang dikirimkan. Hal ini menyebabkan data tidak dapat diterima oleh penerima.

3.1.3 Kondisi *Flooding*

Statistik kejadian yang ada pada saat protokol AOMDV terserang flooding ditunjukkan pada tabel 4

Tabel 4. Statistik simulasi kondisi *flooding*

Jumlah Node Flooder (node)	Paket data kirim (pkt)	Paket Hello kirim (pkt)	Paket data terima (pkt)	Paket Hello terima (pkt)	Total paket hilang (pkt)
1	3401	133744	3259	1123098	142
2	3003	205414	2856	1594848	147
3	2346	276703	2204	2059943	142
4	2032	323274	1905	2287252	127
5	1968	357933	1856	2409073	112
6	1380	404072	1272	2600668	108
7	1359	429107	1233	2639117	126
8	1101	459369	983	2704380	118
9	1017	476507	902	2719194	115
10	886	494656	769	2742613	117

Pada kondisi saat terkena serangan *flooding*, jumlah paket data yang dikirimkan menurun dibanding kondisi normal. Jumlah paket data yang dikirimkan saat terkena serangan *flooding* 10 *node flooder* menurun menjadi 886 paket dibandingkan kondisi normal 3862 paket. Penurunan pengiriman paket ini terjadi akibat kondisi jaringan yang dipenuhi oleh RREQ buatan *node flooder*. Paket RREQ yang dikirimkan pada jumlah *node flooder* sebanyak 10 *node* meningkat menjadi sebesar 494656 paket, dibandingkan dengan kondisi normal sebesar 12717 paket. Padatnya jaringan membuat trafik TCP tidak bisa mengirimkan paket kedalam jaringan. Kondisi ini menyebabkan pengirim tidak bisa mengirimkan data dengan jumlah yang diminta penerima. Penurunan pengiriman paket data menyebabkan penerimaan paket data menjadi lebih sedikit. Paket data yang diterima pada kondisi *node flooder* sebanyak 10 *node* menurun menjadi 769 paket, dibandingkan dengan kondisi normal sebanyak 3784 paket.

3.1.4 Kondisi *Rushing* dan *Flooding*

Statistik kejadian yang ada pada saat protokol AOMDV terserang *rushing* dan *flooding* ditunjukkan pada tabel 5.

Tabel 5. Statistik simulasi kondisi *rushing* dan *flooding*

Node Flood (node)	Paket data kirim (pkt)	Paket Hello kirim (pkt)	Paket data terima (pkt)	Paket Hello yang terima (pkt)	Total paket hilang (pkt)	Paket hilang akibat *rushing* (pkt)
1	2709	144827	2610	1321213	99	50
2	2280	223591	2164	1872080	116	50
3	2123	288495	2008	2237742	115	48
4	1797	334330	1692	2438290	105	31
5	1646	367061	1529	2544299	117	30
6	1551	397649	1441	2612082	110	26
7	1222	428704	1106	2698305	116	20
8	1099	456001	971	2731907	128	26
9	926	473245	814	2761678	112	12
10	678	493851	565	2795991	113	9

Pada kondisi saat protokol AOMDV terkena serangan *rushing* dan *flooding* bersamaan, jumlah paket data yang dikirimkan menurun dibanding kondisi normal. Paket data yang dikirimkan pada variasi jumlah *node flooder* sebanyak 10 *node* menurun sebesar 3184 paket. Penurunan jumlah paket data yang dikirimkan menyebabkan penurunan penerimaan data. Paket data yang diterima saat kondisi *node flooder* 10 *node* sebanyak 565 paket. Jumlah tersebut menurun dibandingkan kondisi normal sebesar 3784 paket. Penurunan penerimaan paket data ini membuat penerima tidak menerima paket sesuai permintaan. Penurunan penerimaan paket data diakibatkan serangan *rushing* yang membuang paket data dan serangan *flooding* yang memenuhi jaringan dengan RREQ sehingga paket tidak dapat dibangkitkan untuk dikirim.

Serangan *rushing* dan *flooding* telah membuat jumlah paket data yang dikirimkan semakin menurun sehingga membuat penerimaan paket data semakin menurun. Kondisi ini menunjukkan serangan *rushing* dan *flooding* secara bersamaan berbahaya jika ditinjau dari sisi penerimaan paket data.

3.2 Analisis *Packet Delivery Ratio*

Pada simulasi didapatkan nilai *packet delivery ratio* untuk masing-masing skenario. Nilai *packet delivery ratio* ditunjukkan pada tabel 6.

Tabel 6. Nilai *Packet Delivery Ratio*

Skenario	Jumlah Node Flooder (node)	PDR Rata-Rata (%)	Deviasi
Normal	-	97,976	0,924
Rushing	-	96,590	0,654
Flooding	1	95,790	1,152
	2	95,024	1,628
	3	93,876	1,027
	4	93,560	1,559
	5	94,152	1,754
	6	91,340	3,975
	7	89,520	5,515
	8	87,420	6,505
	9	85,628	8,509
	10	82,858	11,048
Rushing dan Flooding	1	96,228	1.062
	2	94,862	1,590
	3	94,564	0,715
	4	93,990	1,468
	5	92,592	3,033
	6	91,838	4,437
	7	88,570	6,413
	8	86,066	6,711
	9	85,466	8,111
	10	80,38	10,242

Serangan *rushing* dan *flooding* bersamaan memberikan efek yang paling besar untuk nilai PDR pada jaringan dengan protokol AOMDV ini. Efek yang paling besar ini terjadi pada saat jumlah *node flooder* sebanyak 10 *node.* Nilai PDR yang didapatkan sebesar 80,38 %. Nilai ini turun 17,596 % dibandingkan dengan keadaan normal yaitu 97,976 %.

Kondisi serangan *flooding* dan *rushing* bersamaan dapat lebih menurunkan nilai PDR. Kedua serangan bekerja dengan cara kerjanya masing-masing. Serangan *flooding* terus menerus mengirimkan paket RREQ. *Node flooder* membuat jaringan semakin padat sehingga menimbulkan kemacetan dalam jaringan. Kondisi ini membuat TCP tidak mengizinkan pengirim untuk mengirimkan paket sampai kondisi jaringan kosong. Selain itu paket yang sudah berada dalam jaringan akan dibuang oleh *node* yang dilewatinya karena penuhnya antrian.

Serangan *rushing* bekerja membuang paket informasi yang melewatinya. Ketika paket dibuang maka *ack* tidak akan diterima oleh pengirim sehingga pengirim belum bisa mengirimkan paket lainnya. Pengirim akan mengirimkan paket lagi ketika waktu *timeout* berakhir. Kombinasi serangan *flooding* dan *rushing* mengakibatkan jaringan sangat padat dan paket informasi dibuang. Kondisi ini menyebabkan PDR semakin menurun.
AOMDV memiliki karakteristik mengirimkan *hello* paket kepada *node* tetangga sehingga memastikan bahwa jalur untuk mengirimkan paket tersedia. Namun, walaupun jalur tersedia tetapi tidak menjamin paket akan terkirim karena adanya *node* penyerang.

3.3 Analisis *Throughput*

Pada simulasi didapatkan nilai *throughput* untuk skenario yang ada. Nilai *throughput* ditunjukkan pada tabel 7.

Tabel 7. Nilai *throughput*

Skenario	Jumlah Node Flooder (node)	Throughput Rata-Rata (Kbps)	Deviasi
Normal	-	203	25,572
Rushing	-	136	20,840
	1	141	15,677
	2	122	12,789
	3	94	10,827
	4	85	14,164
	5	81	15,985
Flooding	6	58	23,191
	7	54	19,106
	8	43	19,464
	9	42	19,911
	10	36	20,275
	1	118	20,203
	2	101	16,103
	3	94	15,333
	4	77	15,466
Rushing dan	5	70	10,643
Flooding	6	62	25,333
	7	50	20,545
	8	42	21,667
	9	33	15,634
	10	32	21,155

Serangan *flooding* dan *rushing* aktif bersamaan memberikan efek yang paling besar untuk nilai *throughput* pada jaringan dengan protokol AOMDV ini. Serangan *rushing* dan *flooding* pada variasi jumlah *node flooder* sebanyak 10 *node* menurunkan nilai *throughput* sebesar 84,23 %. Penurunan nilai *throughput* terjadi akibat menurunnya jumlah paket yang diterima dalam jaringan. Ketika jumlah paket yang diterima menurun, dengan waktu pengamatan yang sama maka nilai *throughput* akan menjadi lebih kecil.

Penurunan nilai *throughput* terjadi akibat node *rushing* membuang paket informasi yang melewatinya. *Node rushing* membuat jalur pengiriman paket saat pencarian jalur melewatinya. Ketika paket informasi melewatinya, maka *node rushing* akan membuang paket informasi tersebut. *Node rushing* akan terus menerus membuang paket informasi yang melewatinya. Pengirim akan menunggu waktu timeout berakhir untuk melakukan pengiriman ulang paket yang sama. Ketika batas pengiriman ulang paket terlampaui maka paket informasi akan dibuang. Kondisi tersebut mengakibatkan paket data yang diterima penerima menurun sehingga menyebabkan nilai *throughput* menurun.

Node flooder memenuhi jaringan dengan RREQ yang dibuatnya sehingga menyebabkan jaringan semakin padat. Ketika jaringan padat maka TCP akan menahan pengirim untuk mengirimkan paket informasi. *Node flooder* yang terus menerus memenuhi jaringan dengan RREQnya membuat paket informasi yang dibangkitkan pengirim menjadi lebih sedikit dibandingkan permintaan dari penerima. Kondisi ini menyebabkan paket yang diterima menjadi lebih sedikit dibandingkan permintaan penerima.

3.4 Analisis *Delay*

Pada simulasi didapatkan nilai *delay* untuk masing-masing skenario. Nilai delay dianalisis dan dibandingkan perubahannya dengan kondisi normal. Nilai *delay* ditunjukkan pada tabel 8.

Tabel 8. Nilai *Delay*

Skenario	Node Flood (node)	Delay Total (ms)	Deviasi	*Trace File* Rata-Rata Paket Dalam Sistem (paket)	Perhitungan Rata-rata Paket dalam Sistem (paket)
Normal	-	59.150	11,022	16	16
Rushing	-	46.369	10,443	10	10
	1	90,592	18,856	77	77
	2	109,481	15,377	129	129
	3	129.911	35,678	194	194
	4	141,065	28,890	242	242
Flooding	5	145.800	36,959	274	274
	6	204.154	79,614	425	425
	7	210.347	52,750	464	464
	8	213.039	105,113	496	496
	9	259,308	172,913	631	631
	10	269,734	221,193	681	681
	1	61,191	12,629	52	52
	2	67,434	11,286	82	82
	3	96.093	36,243	147	147
	4	111,404	45,841	193	193
Rushing	5	123.503	46,874	235	235
dan	6	147.863	84,547	304	304
Flooding	7	205.984	146,452	457	457
	8	158.337	68,601	365	365
	9	229,065	154,215	552	552
	10	263,229	160,499	660	660

Kondisi saat serangan *flooding* aktif memberikan efek yang paling besar untuk nilai *delay* pada jaringan dengan protokol AOMDV. Serangan ini memberikan efek yang paling besar ini pada jenis trafik dengan jumlah *node flooder* sebanyak 10 *node.* Nilai *delay* yang didapatkan sebesar 269,734 ms. Nilai ini meningkat dibandingkan dengan keadaan normal yaitu 59,15 ms.

Kondisi peningkatan delay ini terjadi akibat menumpuknya RREQ tidak berguna yang dihasilkan *node flooder.* RREQ ini memenuhi antrian sehingga pelayanan terhadap paket informasi menjadi tertunda. Semakin banyak *node flooder,* maka semakin penuh jaringan sehingga pelayanan paket informasi semakin terganggu.
Akumulasi serangan *flooding* dan *rushing* yang terjadi terlihat tidak lebih meningkatkan nilai *delay* jaringan dibandingkan dengan serangan *flooding*. Hal ini terjadi akibat perbedaan karakteristik serangan *rushing* dan *flooding.* Serangan *rushing* yang membuang paket

informasi yang dikirimkan justru membuat jaringan lebih kosong karena pengirim menunggu waktu *timeout*. Kondisi ini membuat *node flooder* membutuhkan waktu yang lebih lama untuk memenuhi jaringan dengan RREQnya. Selain itu, jaringan yang lebih kosong akibat menunggu waktu *timeout* juga menyebabkan paket yang lain dapat lebih cepat dilayani.

AOMDV memiliki jalur cadangan ketika jalur utama rusak. Pembentukan jalur pengiriman juga lebih cepat karena RREQ ganda yang diterima *node* yang sama tidak langsung dibuang. Hal ini meminimalkan nilai *delay* yang terjadi. Selain itu protokol AOMDV tidak mengupdate *routing table* kecuali waktu *time out* telah habis ataupun jalur cadangan telah habis. Hal ini membuat paket dapat terus dikirimkan tanpa menunggu pencarian rute baru.
Pada tabel 9, nilai *delay* proses menggambarkan nilai *delay* antrian karena pada NS2 tidak diketahui nilai *delay* layanan. Nilai *delay* total sangat dipengaruhi oleh nilai *delay* antrian seperti ditunjukkan pada tabel 9. Nilai delay antrian dominan karena paket harus mengantri terlebih dahulu dalam jaringan sebelum ditransmisikan. Antrian paket pada kondisi serangan *flooding* terjadi akibat penumpukan paket RREQ yang dihasilkan *node flooder*. Kinerja protokol AOMDV saat terkena serangan *flooding* dan gabungan serangan *rushing* dan *flooding* memiliki nilai *delay* dibawah standar ITU T ketika variasi jumlah *node flooder* 10 *node*.

Tabel 9. Nilai masing-masing delay

Skenario	Node Flood (node)	Delay Transmisi (ms)	Delay Propagasi (ms)	Delay Proses (ms)
Normal	-	8	0,001	51,148
Rushing	-	8	0,001	38,367
	1	8	0,001	82.591
	2	8	0,001	101,480
	3	8	0,001	121,909
	4	8	0,001	133,063
Flooding	5	8	0,001	137,798
	6	8	0,001	196,152
	7	8	0,001	202,345
	8	8	0,001	205,037
	9	8	0,001	251,307
	10	8	0,001	261,733
	1	8	0,001	53,190
	2	8	0,001	59.433
	3	8	0,001	88,091
	4	8	0,001	103,402
Rushing dan	5	8	0,001	115,501
Flooding	6	8	0,001	139,861
	7	8	0,001	197,982
	8	8	0,001	150,335
	9	8	0,001	221,064
	10	8	0,001	255,228

Nilai *delay* dapat divalidasi menggunakan teorema little pada persamaan 4. Persamaan 4 digunakan untuk menghitung jumlah rata-rata total paket yang berada dalam sistem pada waktu pengamatan. Nilai tersebut kemudian akan dibandingkan dengan nilai yang ada pada *trace file*. Waktu pengamatan yang dimaksud adalah nilai *delay* rata-rata pengiriman paket. Contoh perhitungan menggunakan persamaan 4 dengan data pada kondisi *rushing* dan *flooding* variasi 8 *node flooder*, sebagai berikut

$$N = \lambda T$$

$$N = (1/0.000434356) \text{ x } 0.158337 = 365 \text{ paket}$$

Jumlah paket rata-rata dalam waktu pengamatan pada *trace file* adalah 365 paket. Nilai paket dalam jaringan untuk kondisi lain dapat dilihat pada tabel 8.

Nilai rata-rata paket dalam sistem yang didapatkan saat perhitungan bernilai sama dengan jumlah rata-rata paket dalam sistem yang didapatkan dari *trace file*. Hal ini membuktikan bahwa hasil simulasi yang dilakukan telah sesuai dengan teorema little.

4. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini adalah serangan *Rushing* dan *flooding* menurunkan performasi jaringan dengan indikator jumlah paket data yang diterima lebih sedikit dibandingkan dengan permintaan. Saat serangan *rushing*, nilai penerimaan paket sebesar 2950 paket, sementara saat serangan *flooding* nilai penerimaan paket terendah sebesar 769 paket. Saat serangan *rushing* dan *flooding* bersamaan, nilai penerimaan paket sebesar 565 paket dibandingkan permintaan sebesar 3784 paket. Penurunan performansi terbesar jaringan dengan protokol AOMDV untuk nilai *packet delivery ratio* dan *throughput* terjadi saat terkena serangan *rushing* dan *flooding* bersamaan dengan jumlah *node flooder* sebanyak 10 *node*. Nilai *Packet Delivery Ratio* menurun sebesar 17,596 %. Nilai *throughput* menurun sebesar 84,23 %. Sementara nilai delay meningkat dari kondisi normal sebesar 59,15 ms menjadi 269,734 ms pada kondisi serangan *flooding* 10 *node flooder*. Untuk penelitian selanjutnya dapat menggunakan protokol dan jenis serangan lain. Selain itu untuk mendapatkan nilai *throughput* yang lebih besar dapat digunakan sistem modulasi dan standar WiFi yang lebih tinggi dataratenya.

Referensi

[1] E. H. Harahap, "Analisis Performansi Protokol AODV (Ad Hoc On Demand Distance Vector) dan DSR (Dynamic Source Routing) Terhadap Active Attack Pada MANET (Mobile Ad Hoc Network) Ditinjau dari Qos (Quality Of Service)," *Tugas Akhir Telkom Univ.*, vol. 34, 2014.

[2] K. M. Verma, "Performance of AODV under Flooding Attack," vol. 4, no. 8, pp. 1000–1003, 2014.

[3] P. Bansal and A. K. Gupta, "Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol," *Int. J. Innov. Eng. Technol.*, vol. 3, no. 4, pp. 90–99, 2014.

[4] G. S. Chandel and R. Chowksi, "Study of Rushing Attack in MANET," *Int. J. Comput. Appl.*, vol. 79, no. October, pp. 43–45, 2013.

[5] V. B. Kute and M. U. Kharat, "Analysis of Quality of Service for the AOMDV Routing Protocol," *ETASR - Eng. Technol. Appl. Sci. Res.*, vol. 3, pp. 359–362, 2013.

[6] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovi, *Mobile Ad Hoc Networking*, vol. 10. 2004.

[7] D. Harinath, "OSI Reference Model – A Seven Layered Architecture of OSI Model," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 3, no. 8, pp. 338–346, 2013.

[8] F. Domingo and C. Hernandez Benet, "Study of TCP Available Bandwidth Using NS2 and Its Forecasting Based on Genetic Algorithm," Karlstads Universitet, 2014.

[9] Circuit Design.inc, "Propagation loss in free space / over flat terrain." [Online]. Available: http://www.cdt21.com/parts/guide_image/guide_g307e.gif

[10] A. Goldsmith, *Wireless Communications*. 2005.

[11] P. Ghosekar, G. Katkar, and D. P. Ghorpade, "Mobile Ad Hoc Networking: Imperatives and Challenges," *IJCA Spec. Issue "Mobile Ad-Hoc Networks,"* 2010.

[12] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," *Comput. Syst.*, vol. 54, pp. 1–12, 1999.

[13] S. A. Sasongko and A. A. Zahra, "Analisis Performansi Dan Simulasi Protokol ZRP (Zone Routing Protocol) Pada MANET (Mobile AdHoc Network) Dengan Menggunakan NS-2," *Tugas Akhir Univ. Diponegoro*, 2010.

[14] K. Higgins, R. Egan, S. Hurley, and M. Lemur, "Ad Hoc Networks." [Online]. Available: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/.

[15] M. K. Marina and S. R. Das, "Ad Hoc on-demand Multipath Distance Vector Routing," *Wirel. Commun. Mob. Comput.*, vol. 6, no. 7, pp. 969–988, 2006.

[16] W. Elmannai, A. Razaque, and K. Elleithy, "TCP-UB: A New Congestion Aware Transmission Control Protocol Variant," *Int. J. Comput. Networks Commun.*, vol. 4, no. 4, pp. 129–141, 2012.

[17] C. P. Agrawal, O. P. Vyas, and M. K. Tiwari, "Evaluation of Varrying Mobility Models & Network Loads on DSDV Protocol of MANETs," vol. 1, no. 2, pp. 40–46, 2009.

[18] A. Kumar, A. K. Sharma, and A. Singh, "Comparison and Analysis of Drop Tail and RED Queuing Methodology in PIM-DM Multicasting Network," vol. 3, no. 2, pp. 3816–3820, 2012.

[19] Gagandeep, Aashima, and P. Kumar, "Analysis of different security attacks in MANETs on protocol stack a-review," *Int. J. Eng. Adv. Technol.*, vol. 1, no. 5, pp. 269–275, 2012.

[20] V. Palanisamy and P. Annadurai, "Impact of Rushing attack on Multicast in Mobile Ad Hoc Network," *Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 1, pp. 184–189, 2009.

[21] M. Chhabra, B. Gupta, and A. Almomani, "A Novel Solution to Handle DDOS Attack in MANET," *J. Inf. Secur.*, vol. 4, no. 3, pp. 165–179, 2013.

[22] E. Bayu Wirawan, Andi dan Indarto, *Mudah Membangun Simulasi dengan Network Simulator-2 (NS- 2)*. Yogyakarta: ANDI, 2004.

[23] T. Issariyakul and E. Hossain, "Introduction to Network Simulator NS2," *Network*, vol. 2, pp. 1–16, 2009.

[24] G. K. Permatasari, and I. Santoso, "Analisis Kinerja TCP Westwood Untuk Pencegahan Kongesti Pada Jaringan LTE Dengan Menggunakan Network Simulator 2.33 (NS2.33)," 2014.

[25] C. H. Manurung and Sukiswo, "Perbandingan Tipe MAC pada Jaringan VSAT Mesh dengan NS-2," Diponegoro University, 2011.

[26] ITU, "G.114 (05/2003)," *Networks*, 2003.

[27] J. Monfort, "Basic Requirements to Quality of Service (IP centric)," ITU-T SG 12, France Telecom, Geneva, May 2003

[28] Cisco, "Cisco Aironet 1130AG Series IEEE 802 . 11A / B / G Access Point," 2009 [Online]. Tersedia : http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/product_data_sheet0900aecd801b9058.html