ANALISIS OPTIMASI KINERJA PROTOKOL ROUTING AODV DAN AOMDV DENGAN MENGGUNAKAN METODE RFAP UNTUK MENCEGAH RREQ FLOODING ATTACKS PADA JARINGAN MANET

(Analysis of AODV and AOMDV Routing Protocol Performance Optimization Using RFAP for Preventing RREQ Flooding Attacks in MANET)

I Made Windra Yudistiana, Andy Hidayat Jatmika*, Ariyan Zubaidi
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Mataram
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email : windra.yudistiana@gmail.com, [andy, ariyan.zubaidi]@unram.ac.id

Abstract

One sector that greatly influences it is in terms of network security. This is due to the characteristics of the MANET network that are dynamic so that the MANET network is very easily disturbed by irresponsible parties. One of the attacks that can occur in MANET network is Route Request (RREQ) Flooding Attacks. In RREQ flooding attacks in the form of fake nodes that are outside the area of the network and broadcast RREQ to the destination node in the network, so that it meets the bandwidth capacity which results in a decrease in quality in determining the route of sending data or information to the destination node. To prevent the occurrence of RREQ flooding attacks, a prevention method for these attacks is required, namely the RREQ Flooding Attacks Prevention (RFAP). This method works by finding nodes that are likely to be malicious nodes then isolated from the network to be restored to normal nodes. This research will optimize the AODV and AOMDV routing protocols by adding RFAP prevention methods and knowing the performance of the two protocols in terms of throughput, average end-to-end delay and normalized routing load. Based on the results of the simulation, that the application of the method RFAP on AODV routing protocol can produce network quality is better than AOMDV protocol, both in terms of throughput, average end-to-end delay and normalized routing load.

Keywords: *MANET, RREQ, Flooding, RFAP, AODV, AOMDV*

**Penulis korespondensi*

1. PENDAHULUAN

Mobile Ad-Hoc Network (MANET) merupakan sebuah jaringan yang dibentuk secara mendiri kapan saja dan dimana saja, terdiri dari beberapa node saling tersambung yang bisa bergerak ke segala arah dengan bebas. Node-node pada jaringan MANET terdiri dari node sumber sebagai pengirim dan node tujuan sebagai penerima, dan antar node pengirim dan penerima disebut node tengah yang berfungsi sebagai perantara kedua node tersebut. Masing-masing node pada jaringan MANET memiliki level yang sama, artinya semua node berperan sebagai router.

Dalam hal komunikasi antar node, perlu adanya proses routing. Proses ini biasanya dikerjakan oleh suatu protokol routing agar node-node mampu saling berkirim data [1].

Karena prinsip jaringan MANET yang dinamis dan memilki mobilitas node yang tanpa batas, sehingga jaringan MANET sangat rentan terhadap serangan tertentu yang dapat dilakukan dengan cara cara menggangu sumber daya jaringan, proses penentuan rute, proses pengiriman paket data dan sebagainya sehingga secara otomatis akan penurunan kualitas keamanan, kegagalan link dan kendala daya tahan (*lifetime*) rute. Oleh karena itu sektor keamanan jaringan menjadi salah satu hal yang perlu pertimbangan dalam jaringan tersebut.

Salah satu serangan yang dapat terjadi pada jaringan MANET adalah Route Request (RREQ) Flooding Attacks. Menurut [2], serangan RREQ flooding berupa node-node palsu yang berada di luar area jaringan tersebut dan melakukan broadcast RREQ ke node tujuan yang ada di dalam jaringan tersebut, sehingga memenuhi kapasitas bandwidth tersebut yang mengakibatkan penurunan kualitas dalam penentuan rute pengiriman data atau informasi ke node tujuan.

Untuk mencegah dari penuhnya bandwidth serta lalu lintas jaringan akibat dari serangan RREQ flooding, perlu adanya tindakan pencegahan untuk mengurangi dampak dari serangan tersebut. Salah satu cara yang

dilakukan adalah menerapkan metode pencegahan RFAP (RREQ *Flooding Attacks Prevention*). Menurut [3], metode RFAP bekerja dengan cara menemukan node-node yang kemungkinan adalah malicious node kemudian diisolasikan dari jaringan untuk dipulihkan menjadi node normal. Dengan teknik tersebut, metode RFAP dapat mengurangi serangan RREQ flooding, hal ini disebabkan oleh metode tersebut dapat dengan mudah menemukan node penyerang dan melindungi jaringan dari serangan RREQ flooding.

Pada penelitian ini penulis mencoba untuk melakukan optimasi kinerja protokol routing dengan menggunakan metode RFAP. Hasil dari optimasi metode RFAP akan diterapkan pada kerangka protokol routing AODV dan AOMDV dengan harapan hasil penelitian ini dapat meningkatkan kualitas keamanan yang lebih baik pada jaringan MANET akibat serangan RREQ flooding.

2. PENELITIAN TERKAIT

Penelitian terkait optimasi kinerja pada suatu protokol routing pernah dilakukan pada [4]. Penelitian tersebut bertujuan memperbaiki kinerja protokol MEDSR menggunakan metode LET agar dapat menghitung berapa lama suatu link antar node terhubung. Hasil penelitian menunjukkan protokol yang telah dioptimasi tersebut mampu meningkatkan kinerja protocol MEDSR.

Penelitian lain terkait optimasi juga dilakukan oleh [5]. Penelitian tersebut menggunakan algoritma LET untuk memperbaiki protokol DSR standar agar dalam mencari rute terdapat proses penghitungan lamanya suatu link antar node terhubung. Hasil penelitian menunjukkan bahwa metode yang digunakan mampu memperbaiki kinerja protokol DSR di jaringan MANET.

Penelitian terkait yang pernah dilakukan oleh [6] melakukan penelitian menggunakan protokol AOMDV, DSDV dan ZRP untuk diukur kinerjanya. Lingkungan simulasi didasarkan pada luas area yang berbeda dan juga jumlah node yang berbeda pula. Parameter kinerja protocol yang diukur meliputi *throughput, end-to-end delay, PDR dan NRL.* Hasil penelitian memperlihatkan bahwa AOMDV memberikan kinerja yang paling baik dilihat dari nilai rata-rata *PDR* dan *throughput.* Sedangkan protokol DSDV memberikan kinerja yang lebih baik dilihat dari NRL dan end-to-end delay.

Penelitian terkait lainnya dilakukan oleh [1] melakukan penelitian menggunakan protocol AODV dan DSR untuk dibandingkan kinerja keduanya dengan lingkungan simulasi yang telah ditentukan. Simulator yang digunakan adalah OPNET Modeler 14.5. Kinerja protocol yang diukur menggunakan parameter uji *jitter*, throughput, *latency* dan *packet loss.* Hasil penelitian menunjukkan bahwa AODV memberikan kinerja yang lebih baik dibanding DSR.

Penelitian yang terkait selanjutnya oleh [7] mengenai pengaruh serangan *flooding* dan *rushing* terhadap kualitas protokol AOMDV dengan menggunakan Network Simulator v.2.35 dengan 3 kondisi simulasi, yaitu dengan serangan *flooding*, serangan *rushing* dan kedua serangan dilakukan bersamaan. Uji kinerja jaringan menggunakan parameter *throughput*, PDR dan *delay*. Berdasarkan hasil simulasi dilakukan bahwa dari segi throughput dan PDR akan menghasilkan *penurunan* yang *paling* tertinggi pada kondisi terkena serangan *flooding* dan rushing serta dari segi delay akan menghasilkan peningkatan yang tertinggi pada *kondisi* terserang oleh serangan *flooding*.

Penelitian yang terkait selanjutnya oleh [3] mengenai tinjauan metode-metode pencegahan dan pendeteksian serangan RREQ *flooding*. Berdasarkan dari peninjauang metode-metode pencegahan RREQ *flooding* bahwa metode RFAP dapat dengan mudah menemukan *node* penyerang dan melindungi jaringan dari serangan RREQ *flooding*. Metode ini dapat memulihkan *node* berbahaya setelah *node* tersebut dikeluarkan serta dimasukkan ke dalam suatu *list-list* pemulihan. dan melindungi jaringan terhadap penyerang. RFAP ini memiliki kemampuan untuk menghentikan dan mengisolasi serangan *flooding* tanpa beban tambahan pada sumber daya jaringan.

Penelitian terkait selanjutnya oleh [8] mengenai penerapan metode RFAP untuk mencegah salah satu serangan, yaitu RREQ *Flooding Attack* (RFA) pada MANET dengan memanfaatkan protokol AODV dan dikondisikan dengan mobilitas *node* yang lebih tinggi. Hasil ini menggambarkan bahwa RFAP memiliki kemampuan untuk memisahkan *node flooder* dari jaringan dengan lebih baik dibandingkan dengan AODV sederhana.

Berdasarkan beberapa penelitian diatas, optimasi pada kerangka protokol routing ternyata dapat meningkatkan kinerja berbagai protokol routing standar pada jaringan MANET. Pada penelitian ini, metode RFAP yang digunakan untuk diterapkan pada kerangka protokol routing AODV dan protokol routing AOMDV dapat meningkatkan kinerja dan mengurangi dampak serangan RREQ *flooding* dari protokol standar yang digunakan.

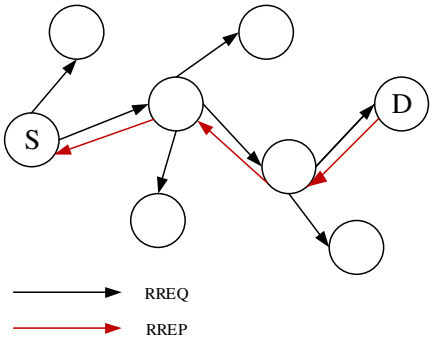
3. DASAR TEORI

Pada bagian ini akan dijelaskan teori yang terkait dengan penelitian ini seperti penjelasan singkat mengenai protokol routing *AODV, AOMDV, RREQ Flooding Attack, dan RREQ Flooding Attack Prevention (RFAP).*

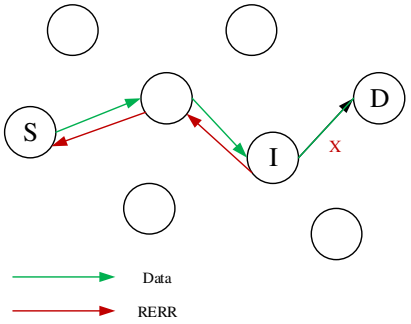
3.1. AODV

Ad Hoc On-Demand Distance Vector atau biasa disingkat AODV termasuk dalam jenis protokol reaktif. Dikatakan reaktif karena rute terbentuk jika ada permintaan dari sebuah node yang akan melakukan pengiriman data ke node tujuan. Rute yang terbentuk akan dicatat di routing table yang dimiliki tiap node. Routing table akan tidak valid jika sudah jarang digunakan. Rute yang ditemukan oleh AODV akan bebas dari yang namanya *routing loop*. AODV memiliki dua mekanisme yaitu *route discovery* dan *route maintenance*. Packet RREQ dan packet RREP akan terbentuk melalui proses *route discovery*, sedangkan packet RERR terbentuk melalui proses *route maintenance* [9]. AODV mempunyai nilai *sequence number* yang digunakan untuk menyediakan informasi *routing* yang terbaru dan untuk menghindari *routing loops* [1].

Pada Gambar 3 memperlihatkan mekanisme penemuan rute protokol AODV. Garis hitam menunjukkan packet RREQ yang sedang dikirim ke node-node untuk menemukan rute, sedangkan garis merah menunjukkan packet RREP yang dikirim oleh node tujuan sebagai balasan dari packet RREQ. Pada Gambar 3, node S ingin mengirim data ke node D. Karena node S belum memiliki rut eke node D, maka node S akan melakukan broadcast pesan berupa packet RREQ ke node-node tetangganya. Kemudian node tetangga akan meneruskan packet RREQ ke node-node lain yang bertetangga dengannya, begitu seterusnya hingga packet RREQ sampai ke node D. Karena node D merupakan node tujuan, maka node D akan membalas dengan mengirim packet RREP ke node S. Node S akan menerima packet RREP ini dan mengirim data menggunakan rute yang sudah ditemukan. Jika rute mengalami kerusakan, maka node D atau node tengah akan mengirim pesan packet RERR ke node S [9] seperti yang ditunjukkan pada Gambar 4.



Gambar 3. Mekanisme Penemuan Rute AODV



Gambar 4. Mekanisme *Route Error* pada AODV

3.2. AOMDV

Ad Hoc On-Demand Multipath Distance Vector atau biasa disingkat AOMDV merupakan protokol routing bersifat reaktif hasil pengembangan dari protokol routing AODV. Perbedaannya dengan AODV adalah pada jumlah rute yang ditemukan. AODV menemukan satu rute saja, sedangkan AOMDV menemukan lebih dari satu rute. Pengembangan ini memiliki tujuan untuk mengurangi resiko terjadinya kegagalan rute pada jaringan.

Mirip seperti protokol AODV, AOMDV juga memiliki mekanisme route discovery dan route maintenance. Paket yang dikirimkan ketika mencari rute juga sama yaitu paket RREQ dan RREP. Untuk proses route maintenance, AOMDV juga akan mengirim paket RERR seperti halnya AODV [10].

Keuntungan adanya pada satu kali pencarian rute adalah ditemukannya beberapa rute, jika rute utama mengalami kerusakan maka akan digunakan rute lain yang masih ada pada routing table tanpa harus mencari rute lagi dari awal. Pencarian rute dari awal hanya dilakukan ketika semua rute yang ditemukan sudah tidak valid lagi.

3.3 RREQ Flooding Attack

Flooding Attacks adalah jenis serangan aktif dimana penyerang menghabiskan sumber daya jaringan, seperti bandwidth, konsumsi sumber daya node, seperti daya komputasi dan daya baterai atau untuk mengganggu operasi dalam penentuan rute sehingga menyebabkan degradasi yang parah pada kinerja jaringan. Dalam RREQ flooding attacks, teknik penyerangan melalui pembentukan node-node palsu yang tidak terdapat pada suatu jaringan dan melakukan broadcast paket RREQ secara terus menerus sehingga dapat menurunkan kualitas bandwidth jaringan tersebut [2][7].

3.4 RREQ Flooding Attack Prevention (RFAP)

Route Request Flooding Attack Prevention (RFAP) adalah suatu skema untuk mengurangi RREQ flooding attack pada jaringan MANET. Skema ini pertama kali menemukan node flooder, kemudian mengisolasinya dari jaringan, memberikan beberapa tindakan pemulihan dan setelah proses pemulihan selesai akan mempertimbangkan kembali apakah node tersebut merupakan node berbahaya atau tidak. Pada serangan RREQ flooding bekerja dalam dua cara, yaitu dengan cara node menghasilkan beberapa paket-paket RREQ pada void-id dengan nilai TTL maksimum atau flooder menggunakan teknik flooding yang sama tetapi berhenti setelah mengirim beberapa RREQ, kemudian setelah beberapa waktu lagi menghasilkan RREQ palsu yang sama. Dalam hal ini, skema RFAP memiliki kemampuan untuk menghentikan dan mengisolasi kedua jenis serangan tanpa beban tambahan pada sumber daya jaringan. Dikarenakan belum ada skema yang lebih baik secara khusus untuk memerangi serangan RREQ flooding, metode RFAP ini merupakan suatu tambahan yang sangat bagus [3][8].

4. METODE PENELITIAN

Pada bagian ini akan dijelaskan mengenai alir penelitian yang dilakukan, mulai dari studi literature hingga pembuatan laporan akhir.

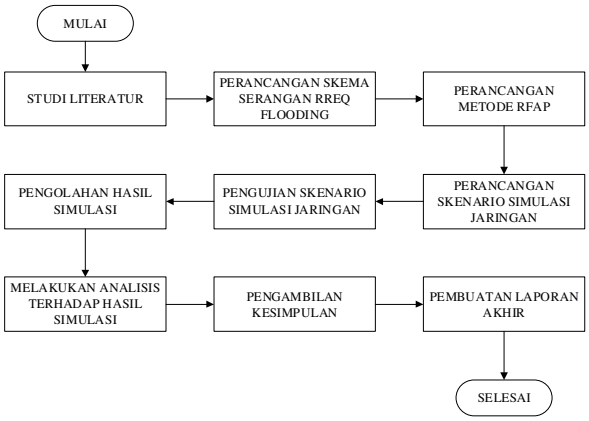
4.1. Lingkungan Simulasi

Dalam penelitian ini akan menggunakan perangkat lunak dan perangkat keras dalam melakukan simulasi jaringan MANET yang terdiri dari Laptop, Sistem Operasi Linux Ubuntu 14.04 LTS, software simulasi jaringan Network Simulator 2.35 dan Microsoft Excel dan Word. Selain itu akan ditentukan parameter lingkungan simulasi yang akan dilakukan seperti pada Tabel I.

TABEL I. PARAMETER LINGKUNGAN SIMULASI JARINGAN

Parameter	Keterangan
Protokol	AODV dan AOMDV
Luas Area Jaringan	500 x 500 m^2
Waktu Simulasi	150 s
Jumlah *Node*	20, 40 dan 60 *node*
Kecepatan *Node*	5 m/s
Jumlah *Node* Penyerang	2, 4, 6, 8 dan 10 *node*
Jumlah *Node* yang Terlibat dalam Transmisi Paket	1 *node* Sumber dan 3 *node* Tujuan
Model Antrian	*Drop tail*
Pergerakan *Node*	*Random Waypoint*
Model Propagasi	*Two Ray Ground*
MAC Layer	IEEE 802.11g
Jenis Antena	*Omni Directional*
Jenis Trafik	*Transmission Control Protocol* (TCP)
Tipe *Transport*	FTP (*File Transfer Protocol*)
Ukuran Paket	100 *Byte*
Jenis Serangan	RREQ *Flooding Attacks*
Jenis Pencegahan	RFAP

4.2 Diagram Alir Penelitian



Gambar 1. Diagram Alir Penelitian

Gambar 1 merupakan gambaran aliran penelitian yang akan dilakukan terkait dengan optimasi metode pencegahan RFAP pada protokol AODV dan AOMDV.

4.2.1. Studi Literatur

Pada bagian ini, peneliti melakukan riset terhadap topik penelitian yang akan dilakukan. Hal ini dilakukan sebagai dasar untuk melakukan penelitian tersebut. Sumber-sumber referensi terkait topik penelitian ini didapatkan melalui beberapa makalah-makalah

penelitian sebelumnya, buku penunjang yang terkait dalam penelitian serta berbagai sumber dari internet.

4.2.2. Perancangan Skema Serangan RREQ Flooding

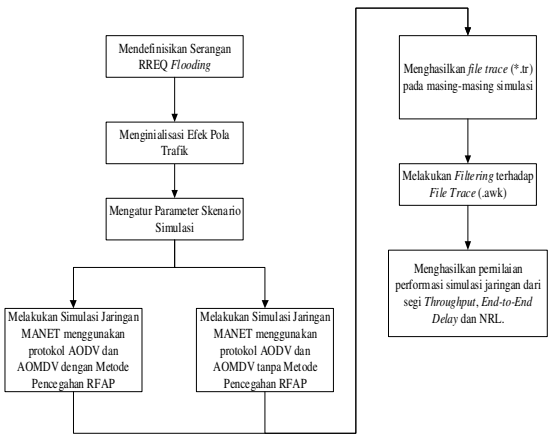
Pada bagian ini, peneliti akan menentukan serangan yang akan diteliti pada simulasi jaringan MANET dengan menggunakan protokol *routing* AODV dan AOMDV. Dalam simulasi ini, peneliti menerapkan serangan *Route Request* (RREQ) *Flooding Attacks*. Dalam hal ini serangan RREQ flooding menerapkan konsep serangan DoS dengan memunculkan *node-node* palsu untuk membanjiri *node* asli dengan *broadcast* RREQ palsu untuk menganggu proses penentuan rute pengiriman data.

4.2.3. Perancangan Metode RFAP

Dalam bagian ini, peneliti melakukan proses perancangan metode untuk melakukan tindakan pencegahan serangan RREQ *flooding*, yaitu RFAP. Dimana skema RFAP ini dilakukan dengan cara menemukan *node* yang terindikasi sebagai *malicious node* dan akan dipulihkan menjadi *node* normal. Dengan melakukan tindakan pencegahan RFAP, dapat mengurangi dampak dari serangan RREQ *flooding*, yaitu berkurangnya tindakan pengiriman RREQ palsu oleh *flooder* melalui proses isolasi dari jaringan dalam kurung waktu tertentu, sehingga mengurangi beban *bandwidth* jaringan yang menyebabkan kualitas pengiriman data akan meningkat.

4.2.4 Perancangan Skenario Simulasi Jaringan

Berikut merupakan diagram alir proses perencanaan skenario simulasi jaringan MANET terkait penelitian dalam mengoptimasikan kualitas keamanan jaringan pada protokol AODV dan AOMDV dengan metode pencegahan RFAP akibat serangan RREQ *flooding* sesuai dengan Gambar 2.



Gambar 2. Diagram Blok Skenario Simulasi.

Dalam simulasi yang dilakukan terdapat beberapa efek pola trafik, yaitu dari segi kapasitas *node* jaringan dan jumlah *node* penyerang (*flooder*). Dimana simulasi akan dilakukan dalam bentuk dua kondisi, yaitu kondisi sebelum penambahan metode pencegahan dan setelah penambahan metode RFAP. Untuk mendapatkan hasil pembandingan kualitas protokol AODV dan AOMDV membutuhkan parameter uji kinerja, yaitu:

a. Throughput

Throughput adalah total paket data aktual atau paket data sebenarnya yang melewati jaringan hingga sampai ke tujuan, penghitungan seperti pada persamaan (1).

$$Throughput = \frac{Jumlah\ paket\ data\ yang\ diterima}{Waktu\ simulasi} \quad (1)$$

b. Average End-to-end Delay

Average End-to-end delay merupakan total waktu yang dibutuhkan paket data dari awal sampai datang di node tujuan, penghitungan seperti pada persamaan (2).

$$Average\ End-to-End\ Delay = \frac{Waktu\ pengiriman}{Jumlah\ paket\ yang\ diterima} \quad (2)$$

c. Normalized Routing Load (NRL)

Normalized Routing Load adalah rasio antara banyaknya paket *routing* yang dikirim dan diteruskan dengan jumlah paket data yang diterima pada jaringan, penghitungan seperti pada persamaan (3).

$$\dot{NRL} = \frac{Jumlah\ paket\ routing}{Jumlah\ paket\ yang\ diterima} \quad (3)$$

d. Proses Pengolahan dan Analisis Hasil Simulasi

Pada bagian ini, peneliti mendapatkan hasil dari simulasi jaringan MANET dengan menggunakan NS-2 dimana akan menghasilkan dalam bentuk *file trace* berekstensi *.tr. Kemudian dilakukan pengolahan *file* tersebut dengan cara *filtering* untuk mendapatkan nilai hasil simulasi sesuai dengan parameter uji yang dilakukan melalui pemrograman AWK. Setelah mendapatkan nilai-nilai tersebut dibuat dokumentasi hasil simulasi dalam bentuk grafik dan peneliti melakukan analisa terhadap hasil-hasil dari simulasi tersebut.

e. Pengambilan Kesimpulan

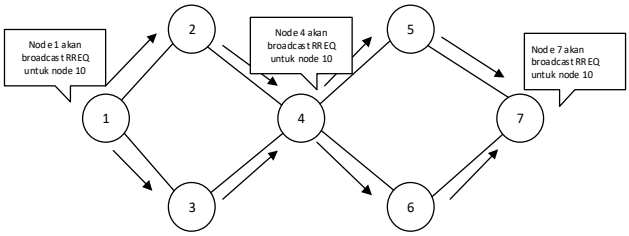
Pada bagian ini, penelitian menentukan kesimpulan dari penelitian yang dilakukan berdasarkan analisa-analisa yang telah dilakukan sebelumnya.

f. Pembuatan Laporan Akhir

Pada bagian ini, peneliti melakukan dokumentasi penelitian secara menyeluruh melalui pembuatan laporan akhir, dimana memiliki tujuan sebagai bahan referensi baru bagi peneliti lain untuk mencoba penelitian lebih lanjut terhadap topik yang diambil.

4.3. Mekanisme RREQ Flooding Attack

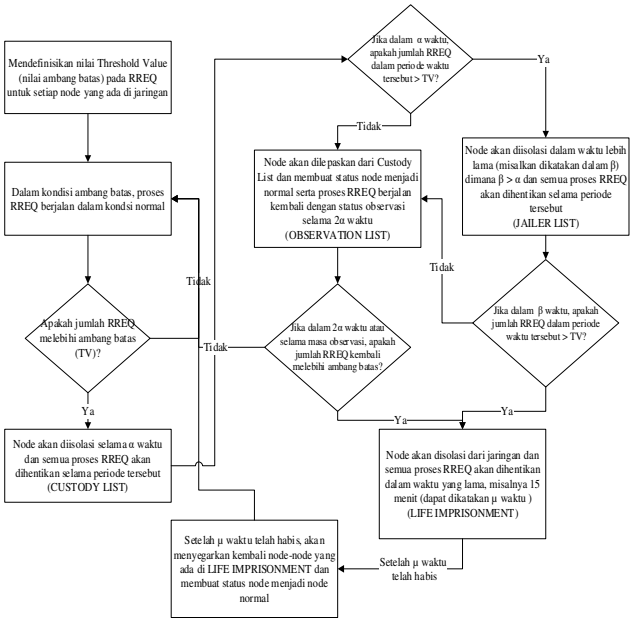
Pada serangan RREQ *flooding*, penyerang melakukan banyak *broadcast* paket RREQ per *interval* waktu dengan menambahkan *node-node* palsu di luar jaringan dan menonaktifkan *limited flooding feature*. Pada protokol *routing on-demand* menggunakan proses pencarian rute untuk mendapatkan rute antara dua *node*. Dalam pencarian rute, *node* sumber melakukan *broadcast* paket RREQ pada jaringan tersebut. Karena prioritas RREQ *control packet* lebih tinggi terhadap paket data maka beban tinggi juga pada paket RREQ dalam melakukan transmisi paket. Oleh karena itulah sebuah *node* jahat (*malicious node*) mengeksploitasi fitur ini pada *on-demand routing* untuk meluncurkan serangan RREQ *flooding* [2][5].



Gambar 6. Mekanisme Serangan RREQ *Flooding*

4.4. Mekanisme Algoritma Metode RFAP

Skema dari RREQ *Flooding Attack Prevention* (RFAP) didasarkan pada skenario di dunia nyata, dimana *node-node* dianggap sebagai manusia. Seorang manusia bila melakukan tindakan kejahatan, maka dia akan dihukum. Sama halnya pada RFAP, ketika *node* melewati nilai ambang batas yang ditentukan maka *node* tersebut akan mendapatkan hukuman.



Gambar 7. Diagram Blok Skema Pencegahan Serangan RREQ *Flooding* dengan Metode RFAP

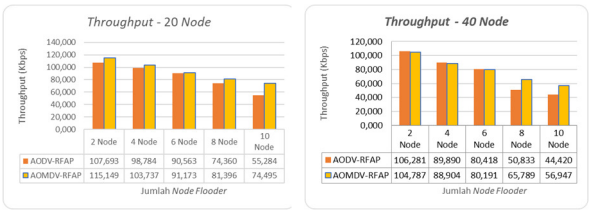
Pada Gambar 7 merupakan alur diagram blok dari metode RFAP, dimana skema RFAP ini menggunakan terminologi yang sangat mirip dengan kehidupan sehari-hari, misalnya jika sebuah *node* tidak mematuhi aturan pada saat pertama kali, maka *node* mendapat hukuman yaitu akan terisolasi dari jaringan untuk beberapa waktu, dalam hal ini dapat ditunjukkan dengan *Custody List*. Selama berada di *Custody List,* jika *node* melakukan pelanggaran kembali maka *node* tersebut akan mendapatkan waktu isolasi yang lebih banyak dan akan dimasukkan ke dalam *Jailer List*. Apabila *node* yang ditahan pada *Custody List* menunjukkan perilaku yang baik, maka *node* akan dilepaskan ke jaringan kembali, akan tetapi masih berada di bawah pengawasan atau diberi kebebasan dengan jaminan. Bila pada masa pengawasan *node* tersebut melewati nilai ambang batas, maka *node* akan diisolasi dengan waktu lebih lama dan dimasukkan ke dalam *Life Imprisonment*. Bila masa *Life Imprisonment* telah habis maka *node* akan dilepaskan menjadi *node* normal dan apabila *node* masih menjalankan masa isolasi pada *Life Imprisonment* sudah bisa berperilaku dengan baik, maka akan dilepaskan ke jaringan dalam status observasi. Skema ini akan me-*refresh* semua *node* setelah masa *Life Imprisonment* berakhir, karena skema ini percaya bahwa jika dalam jaringan MANET apabila sebuah *node* menunjukkan aktivitas jahat maka tidak perlu melakukan hal yang sama setelah waktu tertentu [8].

5. HASIL DAN PEMBAHASAN

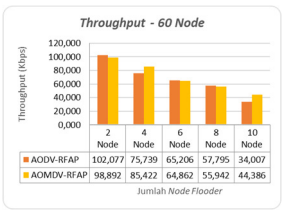
Pada bagian ini akan dijelaskan mengenani analisis yang dilakukan terhadap hasil ujicoba penelitian yang dilakukan seperti analisis throughput, end-to-end delay, dan normalized routing load.

5.1. Analisis Throughput

Throughput dipengaruhi oleh beberapa faktor, seperti lamanya suatu *link* bertahan untuk pengiriman paket data serta proses menemukan rute. Pada situasi ini serangan RREQ *flooding* telah mengganggu kualitas throughput karena adanya serangan tersebut membuat kondisi trafik jaringan akan padat. *Node* penyerang yang terus menerus menyerang trafik jaringan dengan paket RREQ palsunya mengakibatkan paket data yang dibangkitkan oleh node pengirim akan lebih sedikit dengan pemintaan dari penerima dalam hal ini adalah node tujuan, sehingga paket yang diterima akan semakin sedikit. Akan tetapi bila diterapkan metode RFAP pada kedua protokol tersebut menunjukkan kualitas *throughput* meningkat dan lebih baik dari sebelum menggunakannya, karena metode tersebut melakukan tindakan isolasi terhadap *node* yang melakukan serangan *flooder* sehingga trafik jaringan akan kembali normal.



(a) (b)



(c)

Gambar 8. Grafik Kualitas *Throughput* terhadap Penambahan Jumlah *Node Flooder* setelah Penerapan Metode RFAP dengan jumlah *node* terlibat sebanyak (a) 20 *node*, (b) 40 *node* dan (c) 60 *node*

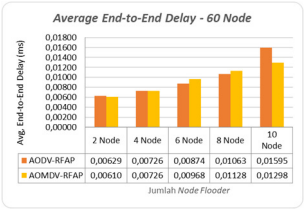
Berdasarkan grafik *throughput* di pada Gambar 8, menunjukkan bahwa kondisi jumlah *node* awal sebanyak 20 *node*, AOMDV memiliki kualitas lebih baik daripada protokol AODV diseluruh kondisi jumlah *flooder* dengan masing-masing selisih kualitas sebanyak 7,456, 4,953, 0,611, 7,036 dan 19,211 Kbps dari AODV. Kemudian pada kondisi jumlah *node* awal sebanyak 40 *node,* protokol AODV lebih baik pada 3 dari 5 kondisi jumlah *node flooder*, yaitu 2, 4 dan 6 *node* dengan masing-masing selisih kualitas sebanyak 1,494, 0,987 dan 0,227 Kbps. Sedangkan pada kondisi jumlah *node* awal sebanyak 60 *node*, AODV memiliki kualitas lebih baik pada 3 dari 5 kondisi jumlah *node flooder*, yaitu 2, 6 dan 8 *node* dengan masing-masing selisih kualitas sebanyak 3,185, 0,344 dan 1,853 Kbps.

Hasil penelitian setelah menerapkan metode RFAP pada protokol AODV dan AOMDV, memperlihatkan bahwa protokol AODV menghasilkan *throughput* yang lebih baik dibanding dengan AOMDV dalam kondisi jumlah *node* awal sebanyak 40 dan 60 *node*. Sedangkan AOMDV hanya memiliki kualitas lebih baik dengan AODV pada kondisi jumlah node awal sebanyak 20 *node*.

5.2. Analisis Average End-to-End Delay

Delay terjadi akibat dari *routing protocol* ketika mencari rute. Sebelum mengirim pesan, *node* sumber terlebih dahulu harus melakukan pengecekan rute yang diminta apakah ada dalam table routingnya. Hal lain yang menyebabkan delay adalah pengiriman paket dari satu *node* ke *node* lainnya karena membutuhkan waktu untuk menganalisis paket tersebut untuk dibawakan kemana serta kemana harus dibawakan paket tersebut. Dengan adanya serangan dari RREQ *flooding* akan menggangu proses pengiriman paket data, gangguan terjadi akibat adanya RREQ yang tidak dibutuhkan. Paket RREQ tersebut secara otomatis memenuhi *buffer* sehingga pengiriman paket data menjadi tertunda. Apabila terdapat banyak *node flooder*, maka jaringan semakin penuh sehingga pengiriman paket akan makin terganggu. Namun dengan adanya penerapan metode RFAP, dapat mengurangi waktu delay dari setiap paket karena berkurangnya jumlah paket RREQ yang tidak berguna karena *node flooder* telah diisolasi dari jaringan.

(a) (b)



(c)

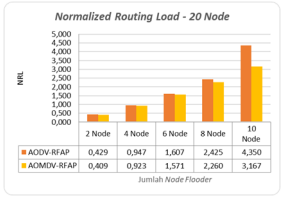
Gambar 9. Grafik Kualitas *Average End-to-End Delay* terhadap Penambahan Jumlah *Node Flooder* setelah Penerapan Metode RFAP dengan jumlah *node* terlibat sebanyak (a) 20 *node*, (b) 40 *node* dan (c) 60 *node*

Berdasarkan grafik *average end-to-end delay* pada Gambar 9, menunjukkan bahwa kondisi jumlah *node* awal sebanyak 20 *node*, AODV memiliki kualitas lebih baik daripada protokol AOMDV pada 4 dari 5 kondisi jumlah node *flooder*, yaitu 2, 4, 6 dan 8 *node* dengan masing-masing selisih kualitas sebanyak 0,00011, 0,00009, 0,00049 dan 0,00088 ms. Kemudian pada kondisi jumlah *node* awal sebanyak 40 *node,* protokol AODV lebih baik pada 4 dari 5 kondisi jumlah *node flooder*, yaitu 4, 6, 8 dan 10 *node* dengan masing-masing selisih kualitas sebanyak 0,00061, 0,00098, 0,00105 dan 0,00069 ms. Sedangkan pada kondisi jumlah *node* awal sebanyak 60 *node*, AODV memiliki kualitas lebih baik pada 3 dari 5 kondisi jumlah *node flooder*, yaitu 4, 6 dan 8 *node* dengan masing-masing selisih kualitas sebanyak 0,000004, 0,00095 dan 0,00065 ms.

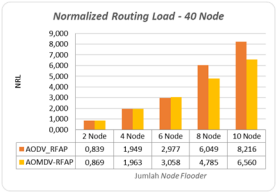
Berdasarkan dari pembandingan kualitas jaringan MANET setelah menerapkan metode RFAP pada protokol AODV dan AOMDV, menujukkan bahwa protokol AODV menghasilkan nilai *average end-to-end delay* yang lebih baik dibanding dengan AOMDV dalam kondisi jumlah *node* awal sebanyak 20 node hingga 60 *node*.

5.3. Analisis Normalized Routing Load

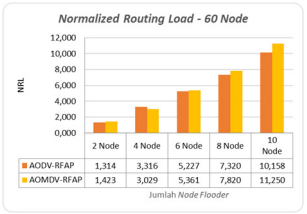
Dengan adanya serangan RREQ *flooding* akan menimbulkan nilai NRL meningkat dikarenakan lalu lintas jaringan yang semakin padat yang disebabkan oleh paket RREQ yang tidak berguna oleh *node flooder* menyebabkan proses menemukan rute semakin sulit sehingga membuat paket *routing* yang dikirim tiap protokol semakin besar ukuran paketnya. Namun dengan adanya metode RFAP pada setiap protokol dapat menurunkan nilai NRL dikarenakan lalu lintas jaringan akan berkurang akibat *node flooder* diisolasi dari jaringan sehingga proses pencarian rute lebih mudah.



(a)



(b)



(c)

Gambar 12. Grafik Kualitas NRL terhadap Penambahan Jumlah *Node Flooder* setelah Penerapan Metode RFAP dengan jumlah *node* terlibat sebanyak (a) 20 *node*, (b) 40 *node* dan (c) 60 *node*

Berdasarkan grafik NRL pada Gambar 12, menunjukkan bahwa pada kondisi jumlah *node* awal sebanyak 20 *node*, AOMDV memiliki kualitas lebih baik daripada protokol AODV di seluruh kondisi jumlah node *flooder* masing-masing selisih kualitas sebanyak 0,020, 0,025, 0,036, 0,165 dan 1,183. Kemudian pada kondisi jumlah *node* awal sebanyak 40 *node,* protokol AODV lebih baik pada 3 dari 5 kondisi jumlah *node flooder*, yaitu 2, 4 dan 6 *node* masing-masing selisih kualitas sebanyak 0,030, 0,014 dan 0,080. Sedangkan pada kondisi jumlah *node* awal sebanyak 60 *node*, AODV memiliki kualitas lebih baik pada 4 dari 5 kondisi jumlah *node flooder*, yaitu 2, 6, 8 dan 10 *node* masing-masing selisih kualitas sebanyak 0,109, 0,133, 0,500 dan 1,092.

Berdasarkan dari pembandingan kualitas jaringan MANET setelah menerapkan metode RFAP pada protokol AODV dan AOMDV, bahwa protokol AODV memiliki kualitas NRL yang lebih baik dengan AOMDV dalam kondisi jumlah *node* awal sebanyak 20 hingga 60 *node*.

6. KESIMPULAN DAN SARAN

6.1. Kesimpulan

Berdasarkan hasil uji coba dan analisis penelitian yang dilakukan terhadap metode yang diusulkan maka dapat ditarik kesimpulan sebagai berikut :

1. Metode pencegahan RFAP dapat diterapkan pada jaringan MANET, terutama pada protokol AODV dan AOMDV. Dimana dalam implementasi metode RFAP tersebut dilakukan dengan cara menentukan nilai ambang dari paket RREQ yang diterima oleh node. Apabila dikondisikan melebihi ambang batas, maka metode RFAP akan menjalankan fungsi isolasi jaringan kepada *node-node* yang kemungkinan *sebagai flooder.* Dalam waktu isolasi tertentu, akan membuang paket yang dikirim oleh *flooder.*
2. Secara keseluruhan simulasi yang dilakukan, menunjukkan bahwa protokol routing AODV menerapkan metode RFAP lebih baik daripada penerapan metode RFAP pada protokol AOMDV, baik dari segi throughput, average end-to-end delay dan NRL.
3. Dari segi kualitas throughput, menunjukkan bahwa kondisi jumlah node awal sebanyak 20 node, AOMDV memiliki kualitas lebih baik daripada protokol AODV diseluruh kondisi jumlah flooder dengan masing-masing selisih kualitas sebanyak 7,456, 4,953, 0,611, 7,036 dan 19,211 Kbps dari AODV. Kemudian pada kondisi jumlah node awal sebanyak 40 node, protokol AODV lebih baik pada 3 dari 5 kondisi jumlah node flooder, yaitu 2, 4 dan 6 node dengan masing-masing selisih kualitas sebanyak 1,494, 0,987 dan 0,227 Kbps. Sedangkan pada kondisi jumlah node awal sebanyak 60 node, AODV memiliki kualitas lebih baik pada 3 dari 5 kondisi jumlah node flooder, yaitu 2, 6 dan 8 node dengan masing-masing selisih kualitas sebanyak 3,185, 0,344 dan 1,853 Kbps.
4. Dari segi kualitas average end-to-end delay, menunjukkan bahwa kondisi jumlah node awal sebanyak 20 node, AODV memiliki kualitas lebih baik daripada protokol AOMDV pada 4 dari 5 kondisi jumlah node flooder, yaitu 2, 4, 6 dan 8 node dengan masing-masing selisih kualitas sebanyak 0,00011, 0,00009, 0,00049 dan 0,00088 ms. Kemudian pada kondisi jumlah node awal sebanyak 40 node, protokol AODV lebih baik pada 4 dari 5 kondisi jumlah node flooder, yaitu 4, 6, 8 dan 10 node dengan masing-masing selisih kualitas sebanyak 0,00061, 0,00098, 0,00105 dan 0,00069 ms. Sedangkan pada kondisi jumlah node awal sebanyak 60 node, AODV memiliki kualitas lebih baik pada 3 dari 5 kondisi jumlah node flooder, yaitu 4, 6 dan 8 node dengan masing-masing selisih kualitas sebanyak 0,000004, 0,00095 dan 0,00065 ms.
5. Dari segi kualitas normalized routing load, menunjukkan bahwa pada kondisi jumlah node awal sebanyak 20 node, AOMDV memiliki kualitas lebih baik daripada protokol AODV di seluruh kondisi jumlah node flooder masing-masing selisih kualitas sebanyak 0,020, 0,025, 0,036, 0,165 dan 1,183. Kemudian pada kondisi jumlah node awal sebanyak 40 node, protokol AODV lebih baik pada 3 dari 5 kondisi jumlah node flooder, yaitu 2, 4 dan 6 node masing-masing selisih kualitas sebanyak 0,030, 0,014 dan 0,080. Sedangkan pada kondisi jumlah node awal sebanyak 60 node, AODV memiliki kualitas lebih baik pada 4 dari 5 kondisi jumlah node flooder, yaitu 2, 6, 8 dan 10 node masing-masing selisih kualitas sebanyak 0,109, 0,133, 0,500 dan 1,092.

6.2. Saran

Dari hasil penelitian yang telah dilakukan terhadap metode pencegahan serangan RREQ *flooding*, bahwa metode RFAP mampu mengurangi dampak dari serangan RREQ *flooding* dengan baik. Diharapkan pada penelitian selanjutnya dapat mencoba metode pencegahan RFAP pada protokol *routing* lainnya, kemudian dalam penentuan parameter efek pola trafik dan parameter uji perlu ditambahkan untuk memaksimalkan hasil yang didapatkan.

DAFTAR PUSTAKA

[1] Anggraini, Nugroho, and Cahyadi, "Analisis Perbandingan Performasi Protokol Routing AODV Dan DSR Pada Mobile Ad-Hoc Network (MANET)," *Tek. Telekomounikasi, Sekol. Tinggi Teknol. Telemat. Telkom*, 2017.

[2] Nalayini, Katiravan, and Prasad, "Flooding Attacks on MANET – A Survey," *Natl. Conf. Inf. Commun. Eng.*, 2017.

[3] S. Bhalodiya and K. Vaghela, "Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET," *Int. J. Sci. Res.*, vol. 4, no. 1, pp. 2013–2016, 2015.

[4] A. H. Jatmika, S. Djanali, and M. Husni, "Optimasi Routing Pada Jaringan MANET Menggunakan MEDSR dan LET," *Semin. Nas. Manaj. Teknol. XIII. Progr. Stud. MMT-ITS*, 2011.

[5] A. H. Jatmika, "Perbaikan Unjuk Kerja Protokol Routing Dsr Pada Mobile Adhoc Network (Manet) Menggunakan Let," *Dielektrika*, vol. 2, no. 2, pp. 173–179, 2015.

[6] Fatkhurrozi, E. R. Widasari, and A. Bhawiyuga, "Analisis Perbandingan Kinerja Protokol AOMDV , DSDV , Dan ZRP Sebagai Protokol Routing Pada Mobile Ad-Hoc Network (MANET)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 10, pp. 3671–3680, 2018.

[7] Rifquddin, Sukiswo, and Zahra, "Evaluasi Kinerja Protokol AOMDV Terhadap Serangan Rushing Dan Flooding Pada MANET Dengan Menggunakan Network Simulator 2," *Jur. Tek. Elektro – Univ. Diponegoro Semarang*, 2015.

[8] K. Laeeq, "RFAP, a preventive measure against route request flooding attack in MANETS," *2012 15th Int. Multitopic Conf. INMIC 2012*, pp. 480–487, 2012.

[9] R. F. Sari, A. Syarif, and B. Budiardjo, "Analisis Kinerja Protokol Routing Ad Hoc on-Demand Distance Vector (Aodv) Pada Jaringan Ad Hoc Hybrid: Perbandingan Hasil Simulasi Dengan Ns-2 Dan Implementasi Pada Testbed Dengan Pda," *MAKARA Technol. Ser.*, vol. 12, no. 1, 2012.

[10] R. Anisia, R. Munadi, and R. M. Negara, "Analisis Performansi Routing Protocol OLSR Dan AOMDV Pada Vehicular Ad Hoc Network (VANET)," *J. Nas. Tek. Elektro*, vol. 5, no. 1, p. 87, 2018.