JAVA Journal of Electrical and Electronics Engineering
Volume 13, Number 1, April 2015

Pendeteksian Dan Pencegahan Serangan Black Hole & Gray Hole Pada Manet

Istas Pratomo[1], M Hizrian Hizburrahman[2]
Jurusan Teknik Elektro
Institut Teknologi Sepuluh Nopember (ITS)
Surabaya, Indonesia
istaspra@ee.its.ac.id[1], hizrian11@mhs.ee.its.ac.id[2]

***Abstract*—Keamanan proses transmisi data pada jaringan Mobile Ad Hoc (MANET) merupakan hal yang sangat penting , tetapi komunikasi nirkabel, perubahan topologi yang dinamis ,resource terbatas dan tidak adanya pengaturan sccara terpusat membuat MANET rentan terhadap segala macam serangan DoS pada layer network seperti Grayhole dan Blackhole yang dapat mengganggu proses transmisi data dengan membuang paket yang diterima. Paper ini menjelaskan mengenai mekanisme keamanan untuk mendeteksi dan melawan serangan Grayhole dan Blackhole pada salah satu routing protkol yang ada pada MANET yaitu AODV. Metode yang digunakan tidak menggunakan teknik kriptografi yang diterapkan pada paket routing melainkan dengan mendeteksi keberadaan node berbahaya dan menggunakan algoritma yang dapat melawan dan membuang node berbahaya dengan mengisolir node tersebut dari jaringan dimana memanfaatkan paket routing yang tidak hanya membawa informasi mengenai informasi routing tetapi juga membawa informasi mengenai keberadaan node berbahaya yang telah terdeteksi.**

Keywords—Security; Blackhole Attack; Grayhole Attack; AODV; MANET.

I. PENDAHULUAN

Jaringan Mobile Ad Hoc (MANET) merupakan jaringan yang terdiri dari beberapa node yang saling berkoordinasi dan berkomunikasi satu sama lain. Setiap node memiliki keterbatasan jangkauan sehingga digunakan konsep multi – hop forwarding dimana setiap node beroperasi seperti sebuah router yang dapat meneruskan paket node lain pada jaringan. MANET banyak diaplikasikan pada komunikasi militer, peralatan perang otomatis, tim penolong saat bencana , polisi, pemadam kebakaran dan sebagai alat komunikasi saat infrastruktur komunikasi rusak akibat bencana alam. Node – node pada MANET berkomunikasi secara nirkabel dan memilki pergerakan dengan kecepatan tertentu yang menyebabkan topologi jaringan yang selalu berubah. MANET memiliki karakteristik lain seperti keterbatasan bandwidth, kapasitas baterai dan daya komputasi yang rendah.

Meskipun karakteristik – karakteristik yang dimiliki oleh MANET tersebut diperlukan untuk fleksibilitas jaringan , tetapi juga menjadi faktor permasalah pada MANET seperti masalah pengalamatan IP , interferensi radio, protokol routing, keterbatasan daya , perlunya manajemen pergerakan, QoS dan keamanan jaringan. Dimana masalah keamanan pada MANET merupakan hal yang harus diperhatikan karena MANET cukup rentan terhadap berbagai jenis serangan seperti penyadapan , interferensi , peniruan , dan Denial of Service[1]. Dimana satu atau lebih node pada jaringan dapat melakukan serangan tanpa dapat terdeteksi terlebih dahulu. Node penyerang dapat mengirimkan paket routing yang salah, memberikan informasi rute yang salah atau bahkan melakukan flooding ke node lain yang akan meningkatkan trafik jaringan. [11] Dua jenis sernagan DoS pada MANET adalah Grayhole dan Blackhole. Pada serangan Blackhole node penyerang akan membuang semua paket yang diterima, sedangkan grayhole merupakan variasi dari blackhole dimana node akan melakukan serangan dengan membuang paket yang diterima pada selang waktu tertentu dan akan berperilkau normal seperti node lainnya.

Untuk menghadapi masalah keamanan akibat serangan Blackhole dan Grayhole pada protokol routing AODV di MANET, maka dirancang sebuah mekanisme untuk mendeteksi dan menghapus kedua jenis serangan tersebut darijaringan. Mekanisme yang digunakan terdiri dari beberapa prosedur keaman yoaitu Neighborhood Data Collection ; Local Anomaly Detection ; Cooperative Anomaly Detection ; Global Alarm Raiser. Pada mekanisme tersebut terdapat beberapa perubahan pada protokol routing yang digunakan yaitu setiap node menyimpan tabel routing beserta daftar node penyerang. Informasi mengenai node penyerang dikirimkan bersama paket RREP dan RREQ.

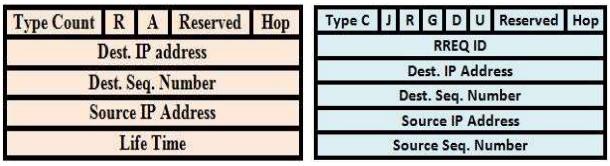
Adapun sistematika penulisan dalam paper ini adalah pada bab 1 dijelaskan pendahuluan dan latar belakang. Bab 2 menjelaskan mengenai dasar teori yang berisi definisi – definisi yang digunakan dalam penelitian ini . Bab 3 menjelaskan mengenai penlitian terkati. Bab 4 akan dijelaskan mengenai mekanisme yang digunakan dalam mengatasi serangan pada jaringan. Bab 5 akan menampilkan hasil simulasi dan analisa performansi dari mekanisme yang digunakan. Bab 6 memberikan kesimpulan dari paper dan saran yang dapat dilakukan pada penilitian selanjutnya.

II. DASAR TEORI

A. Ad Hoc On Demand Distance Vector(AODV)

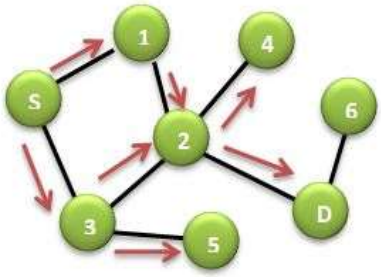
Adhoc On Demand Distance Vector (AODV) adalah protokol reaktif pada MANET yang beroperasi dengan berdasarkan pada permintaan. Rute antar node pada jaringan terbentuk apabila node sumber ingin mengirimkan paket ke node tujuan. Node akan menyimpan tabel routing dengan daftar satu node tujuan dengan satu rute saja [11]. Rute yang tidak

digunakan pada selang waktu tertentu akan dihapus dari tabel. Proses routing pada AODV terbagi menjadi dua, route discovery dengan menggunakan paket Route Request (RREQ) dan route reply (RREP), dan route maintenance dengan paket route error (RERR). Berikut ini adalah format paket RREQ dan RREP



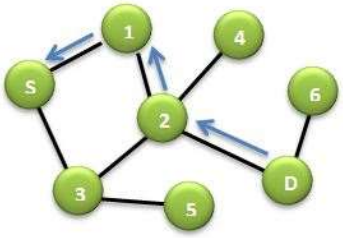
Gambar 1. Format Paket RREQ dan RREP

Proses route discovery terdiri dari dua metode , source routing dan backward learning. Pada source routing, node sumber akan membroadcast paket RREQ ke semua node tetangga dengan alamat node tujuan. Node tetangga tersbut akan kembali membroadcast paket RREQ ke node tetangga yang dimiliki. Setiap node pada jaringan akan mengecek tabel routing untuk mengetahui apakah ia adalah node yang dituju atau memiliki rute untuk mencapi node tujuan. Apabila node tersebut bukan node tujuan, paket RREQ akan diteruskan. Pada saat yang sama dengan broadcast RREQ , jalur balik atau reverse path akan terbentuk.



Gambar 3. Proses Pengiriman Paket RREQ

Node perantara yang memiliki rute ke node tujuan atau node tujuan yang menerima RREQ dapat membalas dengan mengirimkan paket RREP ke node sumber secara unicast dengan menggunakan reverse path yang telah terbentuk atau disebut juga backward learning. Reverse path yang digunakan oleh node tujuan untuk mencapai node sumber yang akan menjadi rute untuk mencapai node tujuan[1].



Gambar 4. Proses Pengiriman Paket RREP

Setelah rute ke node tujuan terbentuk , node sumber bertanggung jawab untuk menjaga rute yang ada. Apabila terjadi kerusakan atau failure , maka paket RERR akan dibroadcast oleh node yang mengalami failure ke semua node pada jaringan hingga mencapi ke node sumber.

B. Keamanan Jaringan

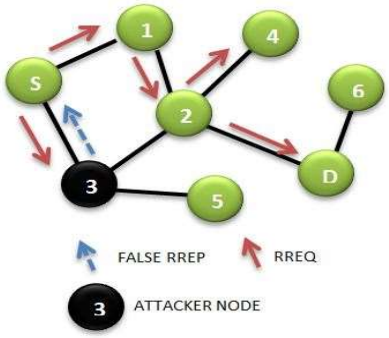
Beberapa mekanisme dapat digunakan untuk memberikan solusi terhadap keamanan jaringan dengan mencegah, mendeteksi atau merespon serangan pada jaringan. Mekanisme yang diberikan harus mengutamakan availability dimana jaringan hanya tersedia untuk user yang terautentikasi ; confidentiality dimana kerahasiaan informasi harus terjaga; integirty dimana proses transmisi harus dilindungi dari segala macam serangan ;authentication dimana jaringan hanya dapat diakses oleh node yang terautentikasi [3]. Beberapa kateogori dari serangan pada jaringan adalah seperti Passive Attack ;Active Attack ;External Attack ;Internal Attack

[12] AODV rentan terhadap serangan dimana penyerang dapat membuang paket, memodifikasi format paket dan meneruskannya, mengirimkan paket palsu setelah mendapat paket routing atau mengirimkan paket palsu tanpa menerima paket routing terlebih dahulu. Node penyerang dapat memalsukan paket RREP dengan cara, Mengatur nilai hop count menjadi 1 ; meningkatkan sequence number tujuan minimal 1 ; mengatur alamat IP sumber menjadi alamat IP yang tidak ada, mengirimkan paket RREP palsu ke node sumber untuk memperoleh rute dari node sumber.

C. Blackhole Attack

Serangan Blackhole dapat dibagi menjadi dua kateogri, serangan berkelompok yang dilakukan oleh lebih dari satu node penyerang yang saling berkerja sama dan serangan sendiri yang hanya dilakukan oleh satu node penyerang [13].

Pada serangan blackhole, node penyerang memperoleh rute yang diinginkan dengan menyatakan pada node sumber bahwa ia memiliki rute terpendek untuk mencapai node tujuan. Setelah menerima paket RREQ, node penyerang langsung mengirimkan paket RREP palsu ke node sumber tanpa melihat informasi mengenai node tujuan. Node penyerang memanipulasi RREP dengan memberikan sequence number dan hop count palsu yang menyatakan node penyerang memiliki rute terpendek dan terbaru.



Gambar 5. Node Penyerang Mengirimkan False RREP

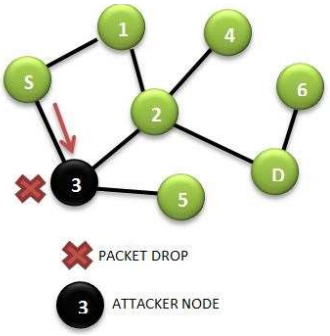
Dengan nilai sequence number node tujuan yang tinggi dan paket RREP yang pertama kali diterima oleh node sumber. Node sumber akan menolak paket RREP yang dikirimkan oleh node lain meskipun memiliki rute yang benar. Sehingga rute antara

node sumber dan node penyerang akan terbentuk dan node sumber mulai mengirimkan paket ke node penyerang. Node penyerang kemudian mulai membuang paket yang diterima [1].

D. Grayhole Attack

Serangan grayhole merupakan variasi dari serangan blackhole dimana node penyerang akan membuang paket yang diterima secara selektif dan dengan pola tertentu. [3] Node penyerang dapat melakukan serangan dengan membuang semua paket UDP dan meneruskan paket TCP atau sebaliknya atau node penyerang dapat membuang semua paket dengan probabilitas tertentu.

Node penyerang juga dapat melakukan serangan dengan membuang semua paket yang datang dan ditujukan untuk node tertentu pada jaringan tetapi akan meneruskan semua paket yang datang dan ditujukan untuk node lainnya. Selain itu node penyerang juga dapat membuang semua paket pada selang waktu tertentu dan akan kembali bertingkah laku seperti node normal. Dengan karakteristik serangan tersebut , node penyerang yang melancarkan serangan grayhole akan sulit untuk terdeteksi.



Gambar 6. Node Penyerang Membuang Paket yang Diterima

III. Penelitian Sebelumnya

Konsep penggunaan nilai batas dilakukan pada protokol DPRAODV [9] dengan menggunakan paket ALARM yang berisi daftar node berbahaya yang akan dikirimkan ke node tetangga untuk menginformasikan bahwa paket RREP dari node berbahaya agar dibuang. Dengan menggunakan protokl ini akan terjadi peningkatan overhead dikarenakan adanya penambahan paket ALARM. Oscar et al [8] juga menggunakan konsep nilai batas untuk menemukan node berbahaya dengan mengamati tingkah laku node. Apabila node berlaku tidak sesuai aturan secara terus menerus hingga melebihi nilai batas maka akan dinyatakan sebagai node berbahaya. Pada metode ini memerlukan waktu untuk memperoleh semua data yang diperlukan untuk mengidentifikasi dan menyatakan sebuah node sebagai node berbahaya. Selain itu node berbahaya tetap dapat membuang paket sebelum dinyatakan sebagai node berbahaya.

Protokol Secure AODV [4] digunakan untuk mengurangi dampat dari serangan blackhole dengan memanfaatkan feedback dari node tetangga sebelum meneruskan paket data ke node lain. Keputusan diambil berdasarkan jumlah paket RREQ dan RREP yang berhasil diteruskan oleh suatu node sehingga dapat diketahui apakah node tersebut node berbahaya atau node biasa. Dengan menggunakan metode ini akan memerlukan waktu yang lebih lama.

Piyush et.al [7] memberikan solusi dimana node sumber dan tujuan melakukan pemeriksaan secara end – to – end untuk menentukan apakah paket data telah diterima oleh node tujuan atau belum. Apabila proses pengecekan gagal dilakukan maka akan dilakukan proses pengecekan terhadap node berbahaya. Solusi yang ditawarkan hanya dapat beroperasi dengan asumsi bahwa setiap node pada jaringan memiliki tingkat kepercayaan satu sama lain sebagai node normal dibandingkan menganggap sebagai node penyerang. Selain itu apabila jumlah node penyerang lebih banyak dari yang diperkirakan maka solusi yang diterima menjadi rentan terhadap serangna.

Deng et.al [10] menawarkan mekanisme untuk mendeteksi adanya node berbahaya. Saat node sumber menerima paket RREP, akan dilakukan verifikasi pada node – node perantara pada rute yang menuju node tujuan apakah node yang mengirimkan paket RREP tersebut memang memiliki rute untuk mencapai node tujuan dan node node perantara lainnya. Apabila tidak maka node tersebut akan dinyatakan sebagai node berbahaya. Dengan menggunakan algoritma ini serangan blackhole dapat terdeteksi apabila hanya dilakukan oleh satu node penyerang. Apabila serangan dilakukan oleh lebih dari satu node penyerang maka akan rentan terhadap serangan. Selain itu juga terjadi delay end – to – end akibat proses verifikasi yang dilakukan oleh node sumber.

IV. Mekanisme Untuk Mendeteksi Serangan Grayhole & Black Hole

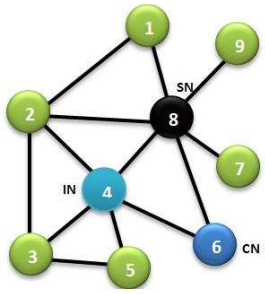
Jaringan MANET yang digunakan terdiri dari node dengan jenis sama yang dapat bergerak dengan bebas atau diam pada lokasi tertentu pada selang waktu tertentu. Setiap node dapat bergabung dan meninggalkan jaringan dan mengalami masalah setiap saat. Node – node pada jaringan melakukan komunikasi secara peer – to – peer secara nirkabel dengan multi-hop dan keterbatasan bandwidth. Setiap node memiliki Nonzero ID dimana semua link pada jaringan merupakan bi-directional. Pada jaringan memungkinkan terdapat lebih dari satu node penyerang yang akan melakukan serangan grayhole dan blackhole.

Mekanisme pendeteksian yang ditawarkan terdiri dari pendeteksian secara lokal maupun global dan pemberitahuan jaringan mengenai keberadaan node penyerang yang telah terdeteksi. Dengan demikian node penyerang dapat diisolasi dan tidak diperbolehkan untuk menggunakan sumber daya jaringan. Mekanisme pendeteksian terdiri dari empat proses yang berkerja secara berurutan yaitu : 1) Pengumpulan Data Node Tetangga ; 2) Pendeteksian Lokal; 3) Pendeteksian Global ; 4) Peringatan Global

A. Pengumpulan Data Node Tetangga

Pada proses pengumpulan node tetangga, node yang ada pada jaringan dimana disebut sebagai Initiator Node (IN) akan mengumpulkan informasi routing yang dilakukan oleh setiap node tetangga. Informasi yang telah diperoleh akan disimpan dalam sebuah tabel informasi routing yang terdiri dari iima kolom yaitu NodeID, DARI, KE, RTS/CTS, CHECKBIT. Kolom NodeID menunjukkan node tetangga. Pada kolom DARI

diberi tanda '1' apabila telah meneruskan paket yang datang dari node tersebut. Sedangkan pada kolom KE diberi tanda '1' apabila telah meneruskan paket yang ditujukan ke node tersebut. RTS/CTS (Request to Send/Clear to Send) merupakan ratio antara jumlah request yang diterima oleh sebuah node dan jumlah paket yang ditransmisikan oleh node tersebut. Kolom Checkbit akan dberi tanda '1' apabila paket ProbeCheck telah diterima oleh Initiator Node dari node tetangga tertentu.



Gambar 7. Jaringan yang Digunakan

Dengan menggunakan topologi jaringan seperti gambar 7 dengan node 4 sebagai IN , maka Tabel Informasi Routing node 4 sebagai berikut

Tabel 1. Tabel Informasi Routing

NodeID	DARI	KE	RTS/CTS	CHECKBIT
2	0	1	2	1
3	0	0	5	0
5	1	0	6	1
6	1	1	4	0
8	0	0	10	1

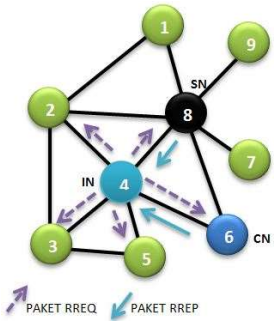
Setelah IN membuat tabel informasi routing, IN akan menganalisa untuk mencari node tetangga yang belum melakukan komunikasi dengan nya pada selang waktu tertentu. IN akan mencari node tetangga yang memiliki nilai '0' pada kolom DARI dan KE dan dengan nilai RTS/CTS tinggi. Setelah IN menentukan node yang diduga sebagai node penyerang atau Suspected Node (SN) , IN akan menjalankan proses berikutnya yaitu Pendeteksian Lokal.

B. Pendeteksian Lokal

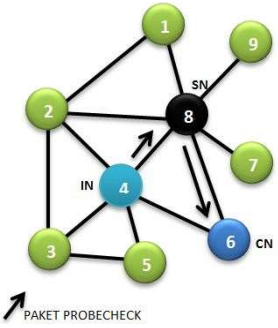
Pada pendeteksian lokal, IN akan memilih Cooperative Node (CN) dari node tetangga dengan mengacu pada Tabel Informasi Routing. IN akan memilih node yang memiliki nilai '1' pada kolom DARI dan KE untuk menjadi CN.

Setelah menentukan CN, IN akan membroadcast paket RREQ ke node tetangga yang berjarak 1 hop untuk meminta rute menuju CN. IN akan menerima paket RREP dari node tetangga dan juga dari Suspected Node (SN) yang diduga akan melakukan serangan.

IN akan mengirimkan paket ProbeCheck ke CN melalui SN dengan nilai Time to Live (TTL) tertentu setelah menerima paket RREP dari SN. Setelah nilai TTL paket tersebut habis , IN akan menanyakan kepada CN apakah CN telah menerima paket ProbeCheck atau belum. Apabila CN telah menerima paket ProbeCheck, In akan memberi nilai '1' pada kolom CheckBit untuk node CN pada Tabel Informasi Routing yang berarti SN tidak terbukti sebagai node penyerang pada waktu tersebut. Sedangkan apabila CN tidak menerima paket ProbeCheck, IN akan meningkatkan kecurigaan pada SN dan menjalankan proses berikutnya yaitu Pendeteksian Global.



Gambar 8. Permintaan rute menuju CN oleh IN



Gambar 9. Pengiriman Paket ProbeCheck

C. Pendeteksian Global

Proses Pendeteksian Global dilakukan dengan tujuan meningkatkan reliabilitas dari proses pendeteksian lokal dengan mengurangi probabilitas adanya kesalahan dalam deteksi karena faktor link failure.

Pada proses ini, IN akan mengirimkan paket CooperativeDetectionRequest (CDREQ) ke semua node tetangga SN. Node tetangga SN akan mengirimkan paket RREQ ke SN setelah menerima paket CDREQ untuk meminta rute menuju IN.

Node tetangga dari SN akan mengirimkan paket FurtherProbe (FRPROBE) ke IN melalui rute yang telah diberikan oleh Sn pada paket RREP sebagai balasan dari paket RREQ. Selain mengirimkan paket FRPORBE, node tetangga juga mengirimkan paket NOTIF ke IN yang berarti bahwa paket FRPORBE telah dikirimkan ke IN. Pengiriman paket NOTIF menggunakan rute yang tidak melalui SN.

Setelah menerima paket FRPROBE dan NOTIF, IN akan membuat tabel ProbeCheck yang berisi NodeID dan ProbeStatus. Dimana nodeID menunjukkan node mana yang mengirimkan paket NOTIF dan ProbeStatus bernilai '1' apabila node IN telah menerima paket FRPROBE dari node tersebut.

Setiap node akan mengirimkan tiga buah paket FRPROBE dengan interval yang sempit. Hal ini dilakukan untuk

mengurangi probabilitas paket FRPROBE tidak sampai ke IN karena faktor collision , buffer overflow atau link failure lainnya.

Apabila IN tidak menerima ketiga paket FRPROBE, maka SN dinyatakan sebagai node penyerang pada rentang waktu tersebut dan SN akan diisolasi dari jaringan melalui proses berikutnya yaitu Peringatan Global.

D. Peringatan Global

Proses Peringatan Global digunakan untuk memberikan peringatan secara menyeluruh pada jaringan mengenai keberadaan node penyerang yang telah terdeteksi.

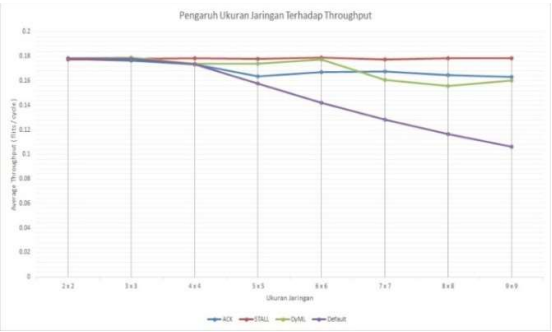
Setelah node penyerang terdeteksi, node pada jaringan akan mengirimkan paket GLOBALARM yang diberi sign berupa private key ke semua node tetangga. Setelah semua k nodes pada jaringan memberia sign berupa private key masing masing pada paekt GLOBALARM, node penyerang akan diisolasi dari jaringan.

NodeID dari node penyerang akan masuk pada list AttackerList yang berisi node – node penyerang yang telah terdeteksi. List tersebut akan diperbaharui secara periodik apabila terdapat perubahan. Dimana proses propagasi dari AttackerList dapat dilakukan melalui dua cara , yang pertama dengan membroadcast ke semua node dengan menumpang pada paket RREQ dan RREP. Kedua setiap node hanya menyimpan AttackerList sebagian , yang hanya berisi node – node tetangga 1 hop nya saja dan hanya diperbaharui apabila terjadi perubahan pada node tetangga.

V. HASIL DAN ANALISA

A. Pengaruh Parameter Desain Terhadap Throughput

Parameter desain yang akan diuji pengaruhnya terhadap *throughput* adalah ukuran jaringan, packet injection rate, ukuran paket , ukuran *buffer*. Dengan parameter desain yang berubah – ubah nilainya , dilakukan perbandingan untuk metode *flow control* berbeda – beda yang digunakan.



Gambar 10. Grafik Pengaruh Ukuran Jaringan Terhadap *Throughput*

Tabel 2. Tabel ProbeCheck

NodeID	ProbeStatus
2	1
3	1
5	1
6	0

Bahwa dengan memperbesar ukuran jaringan yaitu dari 2 x 2 hingga 8 x 8 menyebabkan perubahan pada nilai *throughput*.

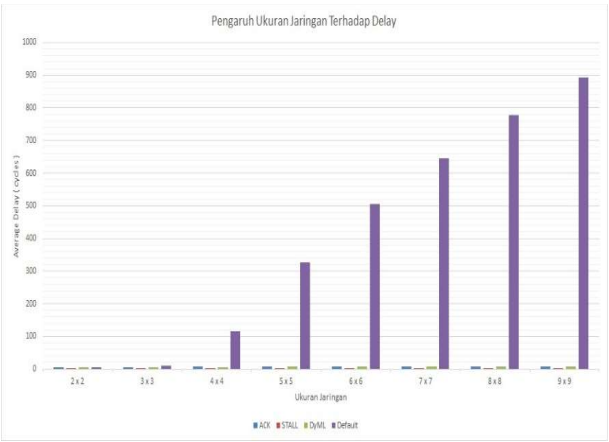
Untuk jaringan dengan *flow control* default, semakin besar ukuran jaringan menyebabkan *throughput* menurun, perubahan *throughput* mulai menurun secara signifikan saat ukuran jaringan adalah 5 x 5 dengan nilai *throughput* saat itu adalah sebesar 0.15779 flits/cycle dan *throughput* menurun sebesar 0.0187 flits / cycle dengan laju penurunan hingga ukuran jaringan 8 x 8 adalah sebesar 0.013387 flits / cycle / ukuran jaringan. Hal tersebut dikarenakan *throughput* dihitung dalam satuan flits/cycle, dengan ukuran paket, ukuran *buffer* dan packet injection rate yang tetap apabila ukuran jaringan diperbesar maka waktu yang diperlukan oleh sebuah flit untuk mencapai tujuan akan bertambah sehingga menyebabkan *throughput* menurun. Selain itu metode pengiriman yang hanya mengizinkan mengirimkan 1 flit sebelum menerima ack menjadi salah satu faktor yang menurunkan *throughput* apabila ukuran jaringan diperbesar.

B. Pengaruh Parameter Desain Terhadap Delay

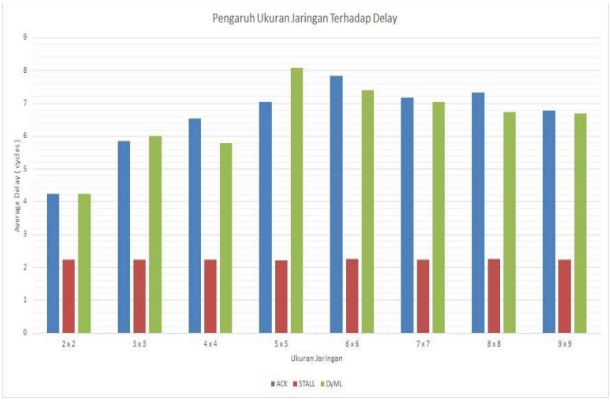
Salah satu parameter performansi jaringan yang diamati adalah *delay* dimana dihitung dalam satuan cycles. *Delay* berkaitan dengan beberapa parameter desain , dimana dilakukan pengujian dengan menggunakan 3 metode *flow control* untuk didapat pengaruhnya terhadap perubahan *delay*. Diharapkan suatu jaringan memiliki *delay* yang rendah.

Gambar 10 dan Gambar 11 menunjukkan hasil pengaruh ukuran jaringan yang berubah – ubah terhadap *delay* yang terjadi pada jaringan

Bahwa pengaruh ukuran jaringan terhadap *delay* dan dilakukan perbandingan terhadap tiga metode *flow control* dimana diperoleh hasil yang berbeda – beda untuk masing – masing *flow control* yang digunakan. *Delay* berbanding lurus dengan ukuran jaringan pada jaringan yang menggunakan *flow control* default. Sedangkan jaringan yang menggunakan *flow control* Stall, perubahan ukuran jaringan tidak memberikan pengaruh yang signifikan. Sedangkan *flow control* Ack dan DyML mengalami peningkatan *delay* hingga ukuran jaringan sebesar 5 x 5 dan kemudian *delay* menurun apabila ukuran jaringan ditingkatkan.



Gambar 11. Grafik Pengaruh Ukuran Jaringan Terhadap *Delay*



Gambar 12. Trafik Pengaruh Ukuran Jaringan Terhadap *Delay*

Untuk jaringan yang menggunakan *flow control* default, kenaikan *delay* yang terjadi adalah sebesar 126.79 cycles dengan *delay* yang terjadi pada ukuran jaringan 9 x 9 adalah sebesar 893.02 cycles. Saat ukuran jaringan berukuran 5 x 5 terjadi kenaikan *delay* yang terbesar yaitu sebesar 210.44 cycles.

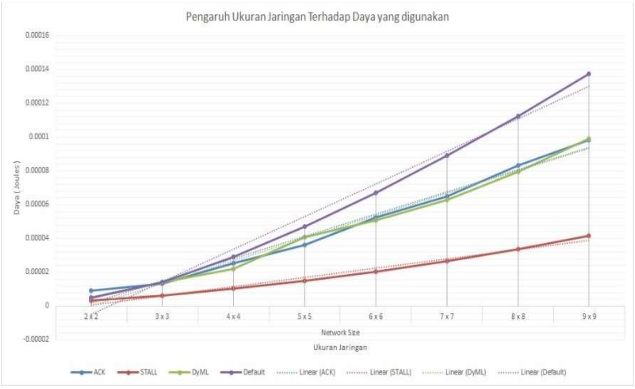
Untuk *flow control* Stall , dengan meningkatnya ukuran dari jaringan , cenderung tidak memberikan dampak yang signifikan terhadap *delay* pada jaringan. *Delay* rata – rata yang terjadi adalah sebesar 2.239 cycles dengan *delay* yang terjadi saat ukuran jaringan 9 x 9 adalah sebesar 2.243 cycles

Sedangkan untuk flow control DyML dan Ack memiliki karakteristik yang hampir sama , dimana terjadi peningkatan delay seiring dengan peningkatan ukuran jaringan dan pada ukuran jaringan tertentu dicapai delay maksimum sebelum delay yang terjadi pada jaringan menurun seiring dengan peningkatan dari ukuran jaringan.

C. *Pengaruh Parameter Desain Terhadap Daya yang Digunakan*

Dalam suatu jaringan terdapat banyak komponen dan faktor yang dapat mempengaruhi penggunaan daya seperti algoritma routing, fungsi selection yang digunakan serta kondisi router.

Sehingga dengan meningkatkan ukuran jaringan akan berdampak pada meingkatnya pula penggunaan daya pada jaringan baik yang menerapkan *flow control* default maupun yang menerapkan metode *flow control* lainnya.



Gambar 13.Grafik Pengaruh Ukuran Jaringan Terhadap Daya

VI. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini setelah dilakukan pengukuran dan analisis data dari hasil ketiga metode flow control yang diperoleh adalah:

1. Flow Control Stall / Go , Ack / Nack dan DyML memberikan pengaruh pada jaringan yang mengalami saturasi
2. Dengan kombinasi parameter desain Packet Injection Rate dan ukuran buffer, flow control Stall / Go , Ack / Nack dan DyML tidak menimbulkan saturasi hingga packet injection rate yang digunakan sebesar 0.3
3. Dengan kombinasi parameter desain Ukuran Paket dan Packet Injection Rate, flow control Stall / Go , Ack / Nack dan DyML tidak menimbulkan saturasi hingga ukuran paket yang digunakan sebesar 20 – 22 flit.
4. Dengan kombinasi parameter desain Ukuran Paket dan Packet Injection Rate flow control Ack/Nack dan DyML mencamai throughput terbesar saat ukuran paket 8 – 10 flit
5. Untuk dapat meningkatkan throughput , maka Packet Injection Rate, Ukuran Paket , Ukuran Buffer dan Ukuran Jaringan harus diperbesar,
6. Untuk dapat menurunkan delay , maka Packet Injection Rate, Ukuran Paket dan Ukuran Jaringan harus diperkecil dengan Ukuran Buffer yang diperbesar
7. Untuk dapat mengurangi penggunaan daya, maka Packet Injection Rate, Ukuran Paket, Ukuran Buffer dan Ukuran Jaringan harus diperkecil

DAFTAR PUSTAKA

[1] Chancal Lohi, S. K. Sharma "A Survey of Mitigation Techniques to Black Hole Attack and gray Hole Attack in MANET" IJCTA, Volume 5, pp 560 – 567

[2] M. Medadian, K. Fardad, A. Mebabdi "Proposing a Methode to Remove Gray Hole Attack in AODV Protocol in MANET" IJESIT, Volume 2, Issue 6, 2013

[3] V. Shanmuganathan, T. Anand, "A Survey on Gray Hole Attack in MANET"IRACST, Volume 2, No 8, 2012

[4] K.S. Sujatha et, al. "Design of Genetic Algorithm Based IDS for MANET" ICRTIT 2012, IEEE, pp 28-33

[5] Rajes Yerneni and A.K. Sarje "Secure AODV Protocol to Mitigate Black Hole Attack in Mobile Ad Hoc Networks" ICCCNT 2012, IEEE, pp 248-252

[6] Maha Abdelhaq et, al "A Local Intrusion Detection Routing Security Over MANET Network" 2011 International Conference on Electrical Engineering and Informatics, 2011, IEEE

[7] Piyush Agrawal, R. K. Ghosh and Sajal K Das " Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2nd International Conference on Ubiquitous Information Management and Communication , 2008, pp 310-314

[8] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Paviou "Detectoin and Accusation of Packet Forwarding Misbehaviour in Mobile Ad- Hoc Networks", Journal of Internet Engineering , Vol2, no1, June 2008, pp 181-192

[9] Payat N Raj and Prahsant B. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET" International Journal of Computer Science Issues , Vol 2, Issue 3, 2010, pp. 54-59

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, " Routing Security in Wireless Ad-Hoc Network", IEEE Communicatoins Magazine, Issue 40, 2002, pp 70-75.

[11] G. Usha and S. Bose "Comparing The Impact of Blackhole and Grayhole Attacks in Mobile Ad Hoc Networks", Journal of Computer Science 2012, Volume 8, Issue 11 , pp. 1788 – 1802

[12] G. Usha and S. Bose, "Impact of Gray Hole Attack on Ad Hoc Networks "

[13] Mehdi Medadian, Khossro Fardad, Ahmad Mebadi, "Proposing a Method to Remove Gray Hole Attack in AODV Protocol in MANET", IJESIT, Volume 2, Issue 6 November 2013