ELKOMIKA | ISSN (p): 2338-8323 | ISSN (e): 2459-9638 | Vol. 6 | No. 2 | Halaman 232 - 243
DOI : http://dx.doi.org/10.26760/elkomika.v6i2.232 Mei 2018

Analisis Kinerja Protokol *Routing* AOMDV pada VANET dengan Serangan *Rushing*

RATNASIH, RISKI MUKTIARTO NUGROHO AJINEGORO, DOAN PERDANA

Universitas Telkom
Email : ratnasih@outlook.com

Received 21 Maret 2018 **|** *Revised* 23 April 2018 **|** *Accepted* 25 Mei 2018

ABSTRAK

Vehicular Ad-hoc Network (VANET) adalah salah satu jaringan mobile Ad Hoc yang memiliki mobilitas tinggi serta topologi yang berubah – ubah secara konstan dalam waktu yang singkat. Sistem broadcast yang diterapkan pada VANET ketika pembentukan arsitektur infrastruktur bisa dijadikan peluang bagi penyerang node untuk melakukan serangan terhadap routing protocol. Rushing Attack adalah sebuah serangan jaringan dimana serangan ini melakukan duplikasi secara cepat dengan transmisi yang lebih tinggi untuk mengacaukan jaringan dan mendapatkan forward akses yang lebih dibandingkan dengan node yang lain. Sasaran utama dari penelitian ini yaitu untuk mengukur dampak dari serangan Rushing pada protocol routing AOMDV (Adhoc on Demand Multipath Distance Vector) menggunakan software NS-2. Nilai QoS yang didapatkan pada hasil penelitian ini tidak maksimal, karena attacker mengirimkan rushed routing packets (RREQ or RREP) yang mempengaruhi routing tabel eksisting dan mengacaukan proses pengiriman paket.

***Kata kunci**: VANET, Rushing Attack, AOMDV, NS-2*

ABSTRACT

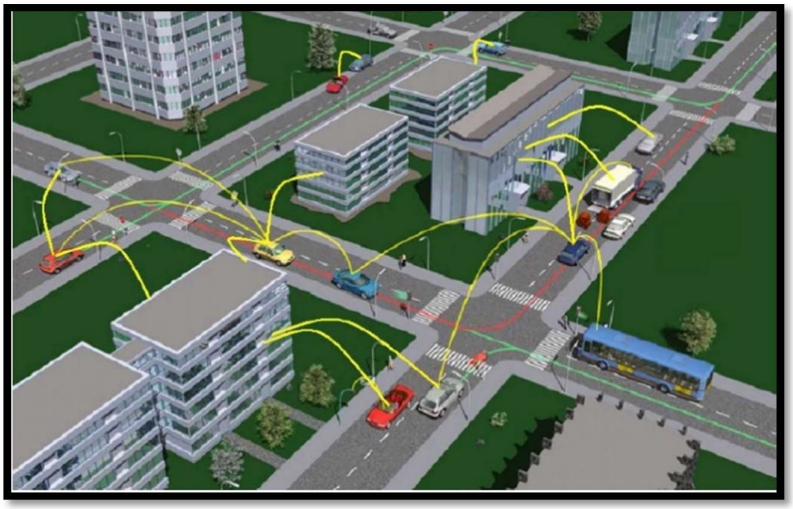
Vehicular Ad-hoc Network (VANET) is kind of an Ad-Hoc mobile network that have high mobility and with changing topology constantly in a short time. The broadcast system that applied to the infrastructure architecture formation when VANET can be used as opportunities for penyerang nodes to perform attacks on the routing protocol. Rushing Attack is an attack on the network that the attacks quickly duplicating with higher transmission to disrupt the network and getting forward more access than the other node. The main target of this project is to measure how big the impact of the rushing attack on AOMDV(Adhoc on Demand Multipath Distance Vector) routing protocol using NS-2 software. On this project did not gets the maximum value for QoS because the attacker sent rushed routing packets (RREQ or RREP) that affect the routing table and disturb the delivery package.

***Keywords**: VANET, Rushing Attack, AOMDV, NS-2*

1. PENDAHULUAN

Teknologi telekomunikasi semakin berkembang dengan cepat untuk meningkatkan mobilitas kerja dan memudahkan kegiatan manusia dalam berbagai aspek. Oleh karena itu dibutuhkan jenis jaringan yang dapat diakses oleh banyak pengguna atau peralatan komunikasi tanpa bergantung pada infrastruktur. VANET adalah salah satu subkelas dari MANET (*Mobile Ad-hoc Network*) yang khusus digunakan sebagai teknologi jaringan *mobile*. VANET merupakan salah satu jaringan yang mempengaruhi *Intelegent Transportation System* untuk meningkatkan keamanan dan kenyamanan pengendara **(Gadkari & Sambre, 2012).**

VANET adalah jenis jaringan ad hoc di mana kendaraan dan pinggir jalan unit adalah communivating node, memberikan satu sama lain dengan informasi, seperti peringatan keamanan dan informasi lalu lintas **(Perdana & Sari, 2015)**. VANET memiliki karakteristik yang sedikit berbeda dari MANET, dengan demikian mobilitas model dalam MANET tidak selalu sesuai ketika digunakan untuk VANET **(Perdana, Munandi, & Manurung, 2017)**. Perbedaan utama antara VANET dengan MANET yaitu VANET adalah jaringan *ad-hoc* yang diimplementasikan pada kendaraan sebagai *node* yang bertindak sebagai *router* yang bergerak dengan mobilitas yang sangat tinggi, sehingga menyebabkan topologi pada VANET berubah ubah dalam jangka waktu yang singkat. VANET memungkinkan komunikasi antar kendaraan saling terhubung dan bertukar informasi satu sama lain melalui *Vehicle to Vehicle* (V2V), dan kendaraan berkomunikasi melewati infrastruktur jaringan melalui *Vehicle to Infrastruktur* (V2I) **(Raw & Das, 2011).**



Gambar 1. Overview VANET (Raw & Das, 2011)

Pada dasarnya, VANET adalah jaringan *ad-hoc* yang tidak memiliki pengetahuan tentang topologi jaringan yang berada disekitar mereka. Setiap *node* hanya mengirimkan pengumuman kehadirannya dan menyadari keberadaan *node* tetangganya secara otomatis dengan menggunakan *broadcasting packets.* Untuk menemukan *node* tetangga yang terdekat, dibutuhkan protokol *routing*. Selain itu, VANET merupakan jaringan terbuka dan media komunikasi tanpa mekanisme keamanan. Sehingga, ada banyak *node* serangan berbahaya pada VANET. Serangan *rushing* merupakan sebuah serangan jaringan dimana serangan ini melakukan duplikasi secara cepat dengan transmisi yang lebih tinggi untuk mengacaukan jaringan dan mendapatkan *forward* akses yang lebih jika dibandingkan dengan *node* yang lain **(Wafta, 2010).** Maka, perlu dilakukan analisis mengenai dampak

dari serangan berbahaya ini pada *protocol routing* VANET. Analisis ini dilakukan untuk menguji nilai penurunan performansi dari QoS *protocol* AOMDV dengan adanya serangan *rushing* menggunakan skema perubahan jumlah *node* penyerang dan perubahan kecepatan *node* pada VANET.

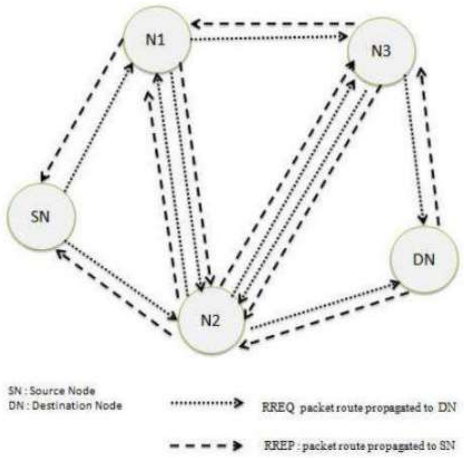
2. METODOLOGI PENELITIAN

2.1. *Routing Protocol* Pada VANET

Protokol merupakan sebuah aturan yang bertugas mengatur setiap *device* untuk saling bertukar informasi melalui sebuah media jaringan, sedangkan *routing* merupakan sebuah proses pemindahan informasi dari pengirim ke penerima melalui sebuah jaringan. Sehingga protokol *routing* sangat dibutuhkan untuk mengirimkan sebuah paket data dari *node* pengirim ke *node* penerima, dengan melewati beberapa *node* penghubung (*intermediate node*), dimana protokol *routing* bertugas untuk mencari rute terbaik dari *link* yang akan dilalui. Pemilihan rute terbaik tersebut dipilih berdasarkan beberapa pertimbangan seperti *bandwith link* dan jaraknya. Selain itu, protokol *routing* juga bertugas untuk mengatur cara komunikasi dua *node* selama pertukaran informasi. Hal ini termasuk prosedur dalam membangun rute, keputusan dalam *forwarding* dan tindakan dalam menjaga rute atau memperbaiki *routing* yang gagal.

Pada umumnya protokol *routing ad-hoc* dikategorikan menjadi tiga bagian, yaitu *flat routing*, *routing* hirarki, dan posisi geografis yang dibantu *routing*. Pada *flat routing* terbagi menjadi dua bagian, yaitu *table driven* atau proaktif *routing* dan *demand routing* atau reaktif *routing*. Reaktif *routing* juga dikenal sebagai *routing* permintaan, karena mereka tidak menjaga informasi *routing* di *node* jaringan ketika tidak ada komunikasi. Jika *node* ingin mengirimkan paket ke *node* lain, maka protokol ini yang akan mencari rute permintaan serta menetapkan komunikasi untuk mengirimkan dan menerima paket-paket. AODV adalah *routing* protokol yang hanya me-*request* sebuah rute saat dibutuhkan **(Prasetia, Perdana, & Negara, 2018)**, begitu pula dengan AOMDV, maka keduanya merupakan salah satu contoh protokol *routing* reaktif.

AOMDV adalah protokol *routing* perkembangan dari protokol AODV. Jumlah rute yang ditemukan setiap kali melakukan pencarian rute adalah perbedaan utama antara AODV dan AOMDV. AOMDV dan AODV menggunakan sebuah sistem *sequence number* untuk memastikan bahwa rute yang dihasilkan adalah *loop-free* serta memiliki informasi *routing* yang paling terbaru. Pada AOMDV dan AODV, terdapat tiga buah pesan utama yang digunakan untuk proses pembentukan jalur *routing* dan pemeliharaan jalur routing yaitu : *route request* (RREQ), *route replay* (RREP) dan *route error* (RERR) **(Awerbuch & Mishra, 2014).** Namun AOMDV pada saat pencarian rute tidak seperti AODV yang hanya memilih satu RREP, tetapi pada AOMDV setiap RREP akan dipertimbangkan oleh *node* asal sehingga beberapa *path* bisa ditemukan dalam satu pencarian rute. Dengan demikian, jika terjadi kegagalan rute pada saat perjalanan maka dapat dialihkan kerute yang lain.



Gambar 2. Proses Propagasi RREQ dan RREP Pada AOMDV (Dubey, 2014)

Gambar 3 memperlihatkan langkah langkah protokol AOMDV untuk melakukan pencarian rute dan pemeliharaan rute. SN akan membanjiri jaringan dengan paket RREQ ketika ingin melakukan komunikasi dengan *node* tujuan sehingga *node* lain akan mendapatkan beberapa salinan dari RREQ yang sama. Selanjutnya, semua Salinan tersebut diperiksa untuk membuat rute alternatif, namun pemeliharaan rute hanya dibuat menggunakan RREQ yang dapat mempertahankan *loop-freedom* dan *disjointness* mulai dari *node* asal. Ketika *intermediate node* menerima rute pemeliharaan melalui salinan RREQ, *node* ini akan memeriksa apakah ada satu atau lebih *forward paths* ke *node* tujuan yang valid. Jika ada, *node* ini akan membuat paket RREP dan mengirim kembali melalui rute pemeliharaan ke *node* sumber.

Saat *node* tujuan menerima salinan RREQ, *node* tersebut juga membuat rute pemeliharaan dengan cara yang sama dengan yang dilakukan oleh *intermediate node*. Namun, RREP yang dibuat oleh *node* tujuan dibuat dengan aturan yang lebih "longgar". Maksudnya adalah *node* tujuan bisa mengirim RREP melalui rute pemeliharaan yang *loop-free* tanpa harus *disjoint*. Hal ini dilakukan untuk mencegah "*route cutoff*" atau rute yang dihapus karena terjadi *suppressing* atau ketika sebuah *node* harus memilih satu dari dua atau lebih *path*. *Route maintenance* pada AOMDV adalah penambahan sederhana pada AODV. Sama seperti AODV, AOMDV menggunakan paket RERR. Sebuah *node* akan membuat atau meneruskan paket RERR untuk *node* tujuan saat *path* terakhir ke *node* tujuan rusak. AOMDV juga melakukan optimalisasi untuk menyelamatkan paket yang sedang dikomunikasikan melalui *link* yang rusak dengan meneruskan ulang paket tersebut melalui jalur alternatif **(Anisia, Munandi, & Negara, 2016).**

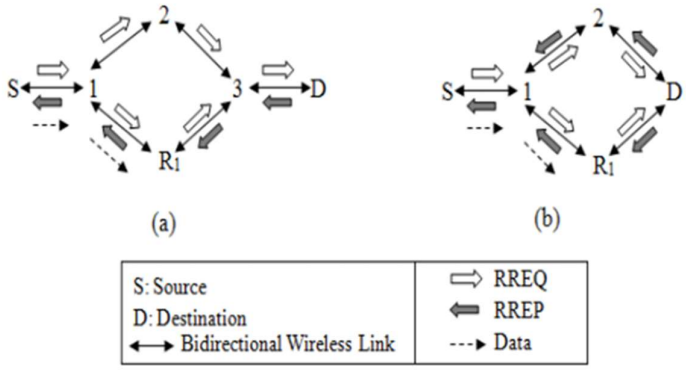
2.2. *Rushing Attack*

Rushing attack adalah serangan *zero delay* dan lebih efektif ketika penyerang dekat dengan *node* sumber atau tujuan. Protokol *routing* berdasarkan permintaan seperti AOMDV lebih rentan terhadap serangan ini, karena setiap kali sumber *node* membanjiri rute permintaan paket dalam jaringan, *node* musuh menerima rute permintaan paket dan mengirim tanpa *hop_count* setiap *update* dan *delay* dalam jaringan. Setiap kali *node* sah menerima paket-paket permintaan *original source*, lalu mereka di *dropped*. Setelah itu ketika *node* sah telah menerima paket dari penyerang dan *treat* saat ini menerima paket seperti paket duplikasi. Dengan demikian, musuh yang disertakan dalam rute akan aktif dan mengganggu fasa penerusan data. *Rushing attack* dapat mengambil tempat di sumber atau di sisi tujuan atau di tengah.

Berikut adalah kondisi *rushing attack* tidak termasuk node aktif :

1. Ketika sumber dan tujuan memiliki komunikasi langsung.
2. Ketika sumber dan tujuan memiliki rute lebih baik daripada *rushing attack*.
3. Ketika *node* penyerang dekat dengan *node* sumber atau tujuan.

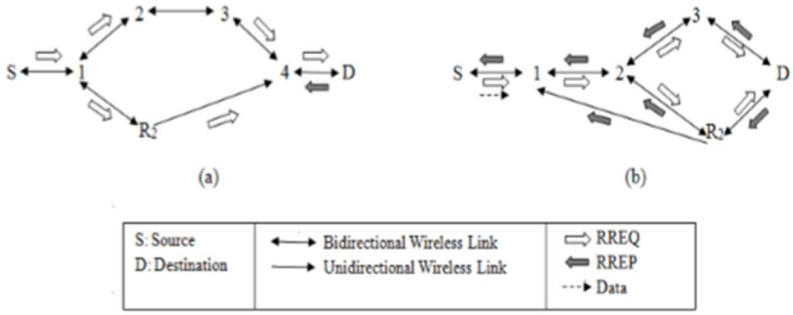
Protokol *routing* AOMDV hanya menganggap penerima pertama paket *routing* sebagai *route discovery*. *Rushing attacker* mengirimkan *rushed routing packets* (RREQ atau RREP) lebih cepat kepada *node* target dibandingkan kepada node pengirim sah lainnya. *Rushing attacker* mengirimkan *routing* paket *rushed* lebih cepat dengan mengabaikan MAC *layer* dan/atau *delay layer routing*, atau dengan menggunakan jangkauan transmisi yang lebih tinggi.



Gambar 3. Rushing Attacker Menolak MAC/Routing Layer Delay (Hazra & Setua, 2012)

Pada Gambar 3 (a), *node* R1 merupakan *rushing attacker* yang mengirimkan *rushed* RREQ lebih cepat ke target *node* 3, dibandingkan dengan *node* 2, dengan mengabaikan *delay*. *Node* 3 membuang RREQ yang terakhir kali diterima dan diteruskan pada *node* 2, dan meneruskan RREQ *rushed* ke destinasi D yang pertama kali diterima R1. Oleh sebab itu, D membalas dengan RREP menuju sumber melalui R1. Hasilnya, sumber akan meneruskan seluruh paket data menuju R1. Pada Gambar 3 (b), *node* R1 merupakan *rushing attacker* yang mengirimkan *rushed* RREP lebih cepat ke target *node* 1, dibandingkan dengan *node* 2, dengan mengabaikan *delay*. Node 1 membuang RREP yang terakhir kali diterima dan diteruskan pada *node* 2, dan meneruskan RREP *rushed* ke destinasi S yang pertama kali diterima R1. Hasilnya, S meneruskan seluruh paket data menuju R1 dan R1 menggunakan data-data tersebut.

Tipe lainnya dari *rushing attacker* adalah mengirimkan *rushed routing packets* menuju node target yang menggunakan jangkauan transmisi yang lebih tinggi. Jangkauan transmisi yang tinggi disini yaitu memiliki minimal *range* dua kali dari *range* normal. Pada Gambar 4 (a), *node* R2 merupakan *rushing attacker* yang mengirimkan *rushed* RREQ kepada target *node* 4 lebih cepat dibandingkan ke *node* 2. *Node* 4 membuang RREP yang sampai ke *node* 2 melalui *node* 3 dan meneruskan *rushed* RREQ ke destinasi D yang pertama kali diterima *node* R2. Oleh sebab itu, D membalas dengan RREP menuju sumber melalui R2. Selama R2 menggunakan jangkauan transmisi yang tinggi, *link wireless* antara *node* 4 dan R2 bukanlah *link bidirectional*. Ketika D meneruskan RREP mencapai *node* 4, maka tidak dapat diteruskan ke R2 karena jangkauan transmisi *node* 4 yang lebih pendek. Hasilnya, *node* S tidak bisa mendapatkan RREP dan tidak ada *route* yang akan disiapkan antara S dan D.



Gambar 4. Rushing Attacker Menggunakan Range Transmisi Tinggi (Hazra & Setua, 2012)

Pada Gambar 4 (b), *node* R2 merupakan *rushing attacker* yang mengirimkan *rushed* RREP menggunakan jangkauan transmisi yang tinggi. R2 mengirimkan *rushed* RREP ke target *node* 1 lebih cepat daripada ke *node* 3. Node 1 membuang RREP yang mencapai *node* 3 melalui *node* 2 yang terakhir diterima dan meneruskan *rushed* RREP ke tujuan S yang pertama kali diterima oleh R2. Oleh sebab itu, S mengirimkan seluruh data ke R2 menuju D. karena R2 menggunakan jangakauan transmisi yang tinggi, *link wireless* antara R2 dan *node* 1 bukanlah *link bidireksional*. Ketika S meneruskan RREP mencapai *node* 1, RREP tersebut tidak dapat diteruskan ke R2 karena jagkauan transmisi *node* 1 yang lebih pendek. Hasilnya, *node* D tidak akan mendapatkan data apapun dari S **(Hazra & Setua, 2012).**

2.3. Skenario Simulasi

Model mobilitas yang akan digunakan adalah *freeway based on map*. Skenario simulasi yang digunakan adalah jaringan VANET dengan protokol *routing* AOMDV, dengan skenario sebagai berikut:

1. Perbedaan jumlah *node* dengan *range* 15, 20, 25, 30, 35, dan 40 *node* dengan *node malicious* sebanyak 3 buah *node*.
2. Perbedaan jumlah *node malicious* dengan *range* 1, 2, 3, 4, 5 dan 6 *node* dengan menggunakan jumlah *node* yang konstan sebanyak 30 buah *node*.
3. Perbedaan kecepatan mobilitas *node* dengan kecepatan 70 km/jam, 80 km/jam, 90 km/jam, 100 km/jam, 110 km/jam, dan 120 km/jam, dengan *node malicious* sebanyak 3 *node* dan jumlah total *node* sebanyak 30 *node* yang konstan.
4. Perbedaan jumlah *node malicious* sebanyak 1, 2, 3, 4, 5, dan 6 *node* dengan kecepatan yang tetap yaitu 90 km/jam.

Adapun beberapa parameter yang digunakan dalam skenario simulasi pada penelitian ini adalah sebagai berikut:

Tabel 1. Parameter Simulasi

Parameter	Nilai
Jumlah *Node*	15, 20, 25, 30, 35, 40 Node
Node Malicious	1, 2, 3, 4, 5, 6 Node
Kecepatan	70, 80, 90, 100, 110, 120 km/jam
Routing Protocol	AOMDV
Mac Type	IEEE 802.11p
Attack	Rushing attack
Waktu Simulasi	350 detik

2.4. Parameter Uji Perfomansi

Parameter uji performansi merupakan salah satu usaha untuk mengetahui kinerja jaringan oleh performansi *routing protocol*. Parameter uji performansi identik dengan *Quality of Service* (QoS). Dalam penelitian ini, digunakan parameter QoS, yaitu:

1. *Packet Delay Ratio* (PDR)
   Packet Delay Ratio merupakan hasil perbandingan antara jumlah paket data yang berhasil dikirim ke *node* tujuan dengan jumlah paket data yang dikirim dari *node* sumber. Semakin tinggi nilai PDR, maka performansi protokol lebih baik. Rumus perhitungan PDR yaitu:

$$Packet\ Delay\ Ratio = (\sum \mathrm{Pr})/(\sum Ps)x100\% \quad (1)$$

   Dimana Pr adalah paket yang diterima, dan Ps adalah paket yang dikirim.

2. Rata-rata *End-to-End-Delay*
   Rata-rata *End-to-End-Delay* (EED) sebuah jumlah waktu total yang dibutuhkan oleh paket data yang dikirim dari ujung sumber ke tujuan akhir. Untuk parameter ini, semakin kecil waktu yang digunakan, maka semakin baik performansinya [16]. Rumus perhitungan rata-rata EED yaitu:

$$EED = \sum(waktu\ terima - waktu\ kirim) \quad (2)$$

3. *Throughput*
   Throughput merupakan jumlah bit yang berhasil diterima dalam selang waktu tertentu. Semakin tinggi nilai *throughput,* maka performansi protokolnya semakin baik juga. Rumus perhitungan *throughput* yaitu:

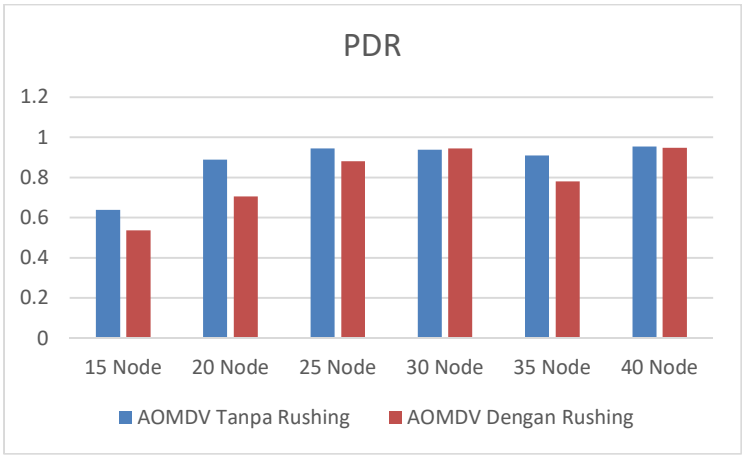
$$Throughput = \frac{Jumlah\ data\ yang\ diterima}{Waktu\ pengiriman\ data} \quad (3)$$

3. HASIL DAN PEMBAHASAN

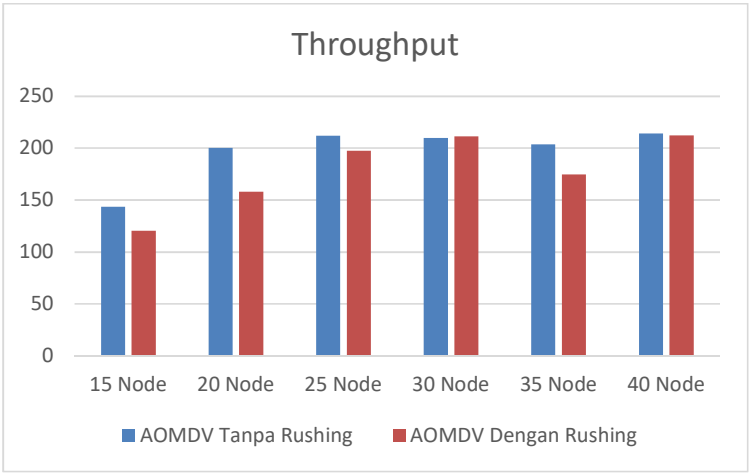
3.1. Analisa Hasil Simulasi

3.1.1. Hasil Simulasi Menggunakan Perubahan Jumlah *Node*

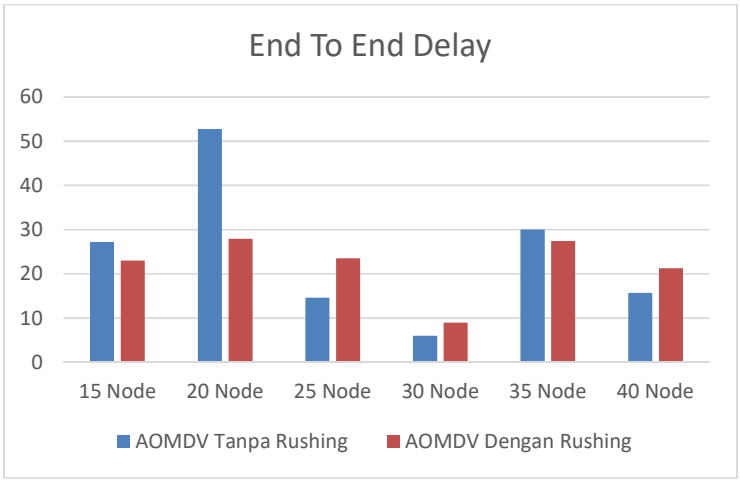
Berikut ini adalah hasil pengukuran menggunakan *routing protocol* AOMDV dengan perubahan jumlah *node* dari 15, 20, 25, 30, 35, dan 40 *node*. Lalu 3 *node* penyerang dengan membandingkan hasil pengukuran VANET dengan serangan *rushing* dan VANET tanpa serangan *rushing.* Gambar 5 memperlihatkan bahwa grafik AOMDV terhadap serangan *rushing* memiliki nilai PDR yang kurang baik dibandingkan dengan nilai PDR tanpa adanya serangan *rushing*. Nilai PDR naik secara perlahan mulai dari jumlah *node* 15 buah sampai jumlah *node* sebanyak 30 buah, lalu mengalami penurunan pada *node* 35 yang selanjutnya mengalami kenaikan pada *node* 40.



Gambar 5. Hasil PDR dengan Perubahan Jumlah *Node*



Gambar 6. Hasil *Throughput* dengan Perubahan Jumlah *Node*

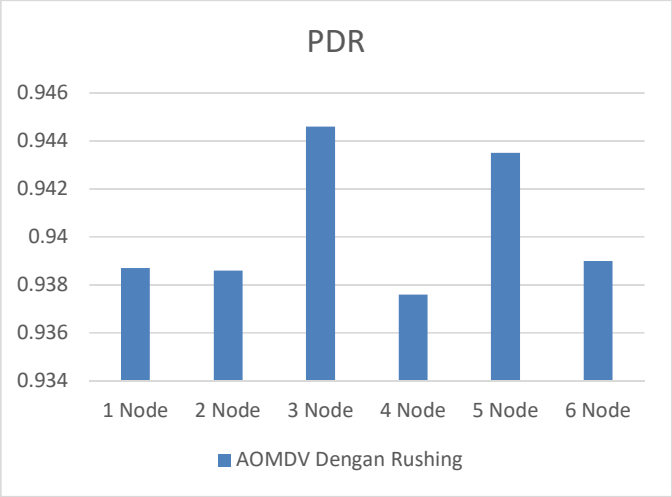


Gambar 7. Hasil *End-to-End-Delay* dengan Perubahan Jumlah *Node*

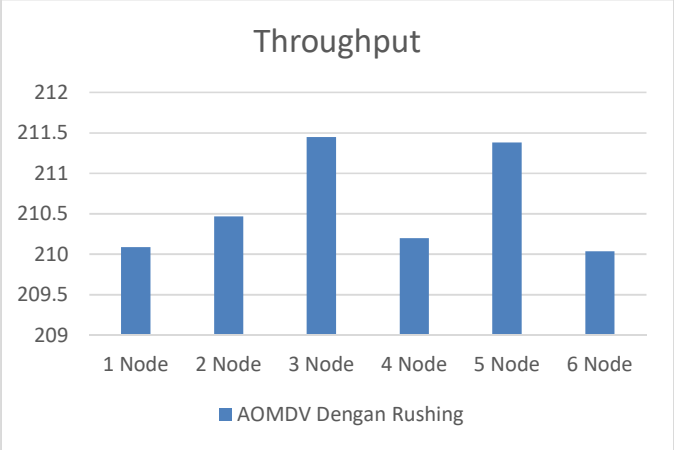
Gambar 6 menunjukan bahwa grafik AOMDV terhadap serangan *rushing* memiliki nilai *througput* yang kurang baik dibandingkan dengan nilai *throughput* tanpa adanya serangan *rushing*. Nilai *throughput* naik pada jumlah *node* 25 buah dan mengalami penurunan secara perlahan pada *node* 30 dan 35 yang selanjutnya mengalami kenaikan pada *node* 40. Gambar 7 memperlihatkan bahwa grafik AOMDV terhadap serangan *rushing* memiliki nilai *End-to-End-Delay* yang fluktuatif serta memiliki nilai yang lebih besar daripada nilai *End-to-End-Delay* tanpa adanya serangan *rushing*.

3.1.2. Hasil Simulasi Menggunakan Perubahan Jumlah *Node* Penyerang

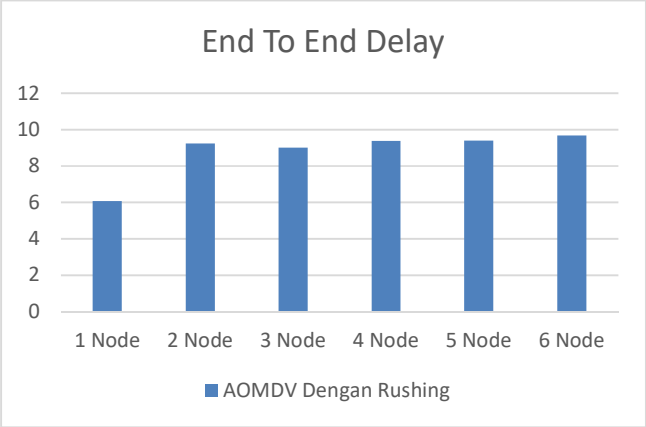
Berikut ini adalah hasil pengukuran menggunakan protokol *routing* AOMDV dengan perubahan jumlah *node malicious* sebanyak 1, 2, 3, 4, 5 dan 6 *node* dengan jumlah *node* sebanyak 30 buah *node*. Terlihat pada Gambar 8 bahwa grafik AOMDV dengan skema *rushing attack* terhadap perubahan jumlah *node malicious* memiliki nilai PDR yang fluktuatif. Pada jumlah 3 *node* penyerang, nilai PDR naik dari 0.9386 menuju 0.9446 lalu turun kembali pada jumlah *node* 4.



Gambar 8. Hasil PDR dengan Perubahan Jumlah Penyerang



Gambar 9. Hasil *Throughput* dengan Perubahan Jumlah Penyerang

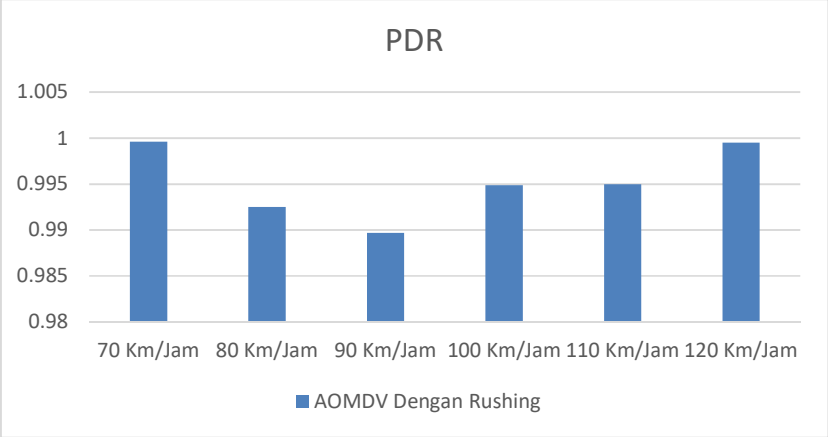


Gambar 10. Hasil *End-to-End-Delay* dengan Perubahan Jumlah *Penyerang*

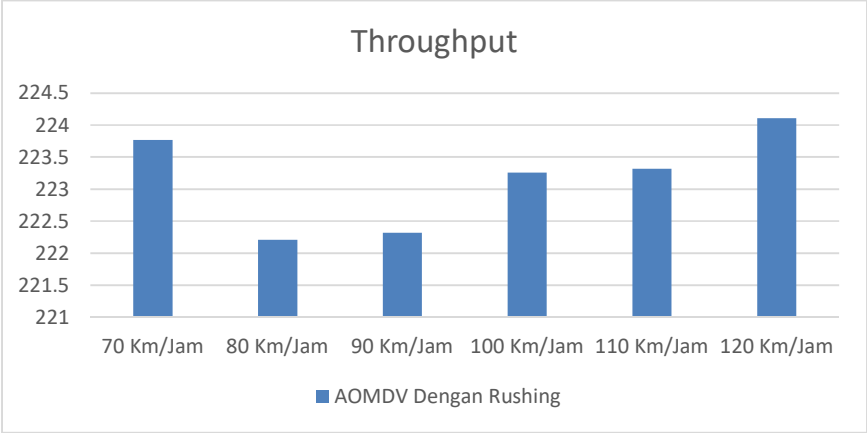
Gambar 9 memperlihatkan bahwa grafik AOMDV dengan skema serangan *rushing* terhadap perubahan jumlah *node* penyerang memiliki nilai *throughput* yang fluktuatif. Pada jumlah 3 *node* penyerang, nilai *throughput* naik dari 210,47 kbps menuju 211,45 kbps, lalu mengalami fluktuatif bergantian mulai dari *node* 2 sampai *node* 6. Terlihat pada Gambar 10 bahwa grafik AOMDV dengan skema serangan *rushing* terhadap perubahan jumlah *node* memiliki nilai *End-to-End-Delay* yang fluktuatif pada *node* 1 sampai dengan *node* 3, kemudian mengalami kenaikan perlahan dimulai dari *node* 4 sampai *node* 6 dengan rata – rata 9 ms.

3.1.3. Hasil Simulasi Menggunakan Perubahan Kecepatan *Node*

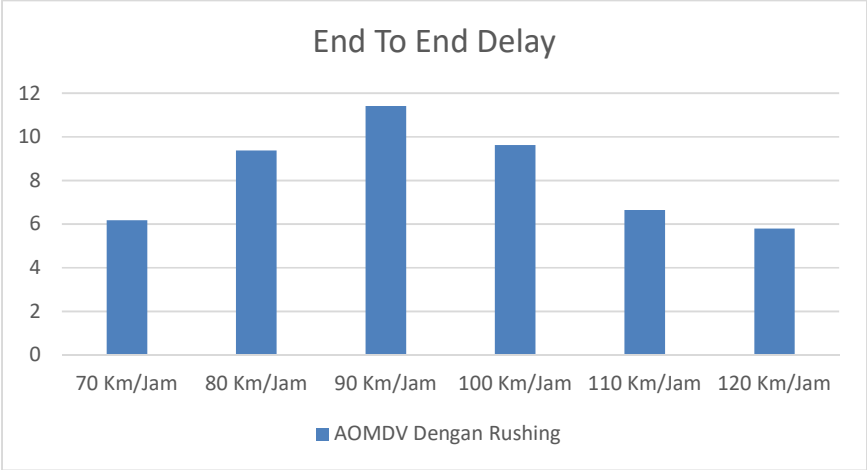
Berikut ini adalah hasil pengukuran menggunakan protokol *routing* AOMDV dengan perubahan kecepatan *node* dengan variasi kecepatan 70 km/jam, 80 km/jam, 90 km/jam, 100 km/jam, 110 km/jam, dan 120 km/jam. Skenario tersebut dilengkapi dengan total jumlah *node* sebanyak 30 *node* yang berisikan 3 *node malicious.* Gambar 11 menunjukan nilai PDR yang fluktuatif. Pada saat 70 km/jam, nilai PDR semakin menurun, namun naik secara perlahan kembali ketika 100 km/jam sampai 120 km/jam.



Gambar 11. Hasil PDR dengan Perubahan Kecepatan *Node*



Gambar 12. Hasil *Throughput* dengan Perubahan Kecepatan *Node*



Gambar 13. Hasil *End-To-End-Delay* dengan Perubahan Kecepatan *Node*

Gambar 12 menunjukkan hasil dari throughput bergerak secara fluktuatif. Nilai *throughput* tertinggi ada pada saat kecepatan 120 km/jam dan nilai terendah ada pada saat 80 km/jam. Gambar 13 menunjukkan hasil dari *End-to-End Delay* yang bergerak secara fluktuatif. Nilai terendah berada pada saat kecepatan 70 km/jam dan paling tinggi ada di kecepatan 90 km/jam.

4. KESIMPULAN

Penelitian mengenai kinerja jaringan VANET dengan skema serangan *rushing attack* ini menghasilkan kesimpulan sebagai berikut:

1. Pada kondisi tanpa adanya serangan *rushing*, performansi QOS AOMDV dengan skenario perubahan jumlah *node* memiliki nilai performansi yang baik dikarenakan ketika proses pengiriman data tidak mengalami gangguan.
2. Pada kondisi dengan adanya serangan *rushing*, performansi QOS AOMDV pada skenario perubahan *node* memilki nilai yang kurang baik dibandingkan dengan tanpa adanya serangan. Hal ini dikarenakan adanya gangguan yang disebabkan oleh *node* penyerang yang menganggu proses *routing*. Dengan begitu, didapatkan nilai rata-

rata *throughput* sebesar 204.5 kbps, lalu nilai PDR sebesar 0.944 %, serta nilai *end-to-end delay* sebesar 42.37 ms.

3. Pada kondisi dengan adanya serangan *rushing*, performansi QOS AOMDV pada skenario perubahan jumlah *node* penyerang memiliki nilai yang fluktuatif, dimana nilai performansi QOS berada pada titik terendah ketika kondisi jaringan memiliki 3 node penyerang. Hal ini dipengaruhi oleh banyak faktor seperti posisi, mobilitas dan *traffic* yang ada pada jaringan tersebut.
4. Pada kondisi dengan perubahan kecepatan, performansi QOS AOMV memiliki nilai yang fluktuatif. Hal ini terjadi karena faktor jumlah *node malicious*, mobilitas, serta *traffic* yang ada pada jaringan AOMDV tersebut.n

DAFTAR RUJUKAN

Gadkari, M. Y., & Sambre, N. B. (2012). VANET : Routing Protocols, Security Issues and Simulation Tools. *IOSR Journal of Computer Engineering* (IOSRJCE), 28-38.

Perdana , D., & Sari, R. F. (2015). Performance Evaluation of Corrupted Signal Caused by Random Way Point and Gauss Markov Mobility Model on IEEE 1609.4 Standards. *IEEE*.

Perdana, D., Munandi, R., & Manurung, R. C. (2017). Performance Evaluation of Gauss-Markov Mobility Model in Hybrid LTE-VANET Networks. *TELKOMNIKA*, 606-621.

Raw, R. S., & Das, S. (2011). Performance Comaparison of Posistion-based Routing Protocols in Vehicle-to-Vehicle (V2V) Communication. *International Journal of Engineering Science and Technology* (IJEST).

Wafta, M. (2010). Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. Hershey: Information Science Reference.

Prasetia, D. R., Perdana, D., & Negara, M. R. (2018). Analisis Kinerja GPSR dan AODV pada VANET dengan Skema Pengimbangan Beban Trafik. *Jurnal ELKOMIKA*.

Awerbuch, B., & Mishra, A. (2014). Ad Hoc On Demand Distance Vector (AODV) Routing Protocol. Departement of Computer Science.

Dubey, S. (2014). Implementation of AOMDV, OLSR & ZRP Protocol for Analysis of Performance Matrices in VANET Scenario. *IJESRT*, 3.

Anisia, R., Munandi, R., & Negara, R. M. (2016). Simulasi Dan Analisis Performansi Protokol Routing OLSR DAN AOMDV Pada Jaringan Vehicular Ad-Hoc Network (VANET). *Jurnal Nasional Teknik Elektro*, 5.

Hazra, S., & Setua, S. K. (2012). Rushing Attack Defending Context Aware Trusted AODV in Ad-Hoc Network. *International Journal of Security, Privacy and Trust Management* (IJSPTM).