**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 3, No. 10, Oktober 2019, hlm. 9823-9831 http://j-ptiik.ub.ac.id

# Pengaruh Serangan *Rushing* Terhadap *Protocol Ad Hoc On Demand Distance Vector* (AODV) pada Jaringan *Mobile Ad Hoc Networks* (MANET)

**Eldyto Puspa Laksana[1], Reza Andria Siregar[2], Achmad Basuki[3]**

Program Studi Teknik Informartika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]eldyto180395@gmail.com, [2]reza.jalin@ub.ac.id, [3]abazh@ub.ac.id

**Abstrak**

*Mobile Ad Hoc Networks* (MANET) adalah salah satu jenis jaringan nirkabel yang ada saat ini, dimana *mobile node*s diasosiasikan dengan tidak terencana atau disebut *ad hoc.* Terdapat berbagai jenis protokol routing pada MANET dan salah satunya adalah *reactive routing.* Salah satu contoh algoritme *reactive routing* adalah Ad hoc On-Demand Distance Vector (AODV). Serangan *rushing* memanfaatkan RREQ pada *route discovery* untuk menjadi *node* penghubung antara *source* dan *destination* paket data pada jaringan. Jumlah *node* yang digunakan 30 *node*, 40 *node*, 50 *node*. Simulasi tersebut dilakukan menggunakan *Network Simulator* (NS-2.35). Serangan *rushing* memberikan dampak pada *routing* protokol AODV dengan menurunkan kinerjanya. Dengan dibuktikan dari nilai *packet delivery ratio, packet loss, throughput,* dan *end to end delay* yang turun kualitasnya. Penurunan paling besar terjadi pada implementasi 4 serangan *rushing* terjadi penurunan kualitas dimana *packet delivary ratio* pada 40 *node* terjadi penurunan sebesar 12,90% , *packet loss* pada 40 *node* terjadi kenaikan sebesar 12,90%, *throughput* pada 40 *node* terjadi penurunan sebesar 18,27 kbps,dan *end to end delay* pada 30 *node* terjadi kenaikan sebesar 4035,3259 ms. Dibandingkan dengan percobaan pada 30 *node* dan 50 *node* terjadinya penurunan kualitas sangat kecil dan cenderung tidak ada penurunan.

**Kata kunci**: *MANET, AODV, Rushing, NS-2.35*

***Abstract***

*Mobile Ad Hoc Networks (MANET) is one type of wireless network that exists today, where mobile nodes are associated with unplanned or called ad hoc. There are various types of routing protocols on MANET and one of them is reactive routing. One example of reactive routing algorithms is Ad hoc On-Demand Distance Vector (AODV). Rush attacks use RREQ on route discovery to become a connecting node between the source and destination data packets on the network. The number of nodes used is 30 nodes, 40 nodes, 50 nodes. The simulation was carried out using Network Simulator (NS-2.35). Rush attacks have an impact on routing the AODV protocol by reducing its performance. It is proven by the value of the packet delivery ratio, packet loss, throughput, and end to end delay, which decreases in quality. The biggest decrease occurred in the implementation of 4 rushing attacks, there was a decrease in quality where packet delivary ratio at 40 nodes decreased by 12.90%, packet loss at 40 nodes increased by 12.90%, throughput at 40 nodes decreased by 18.27 kbps, and end to end delay on 30 nodes increased by 4035.3259 ms. Compared to experiments on 30 nodes and 50 nodes the quality loss is very small and there tends to be no decrease.*

**Keywords** : *MANET, AODV, Rushing, NS-2.35*

## 1. PENDAHULUAN

AODV adalah *distance vector routing protocol* yang termasuk dalam klasifikasi reaktif *routing protocol*, yang hanya me-*request* sebuah rute saat dibutuhkan. Ciri utama dari AODV adalah menjaga *timer-based state* pada setiap *node* sesuai dengan penggunaan tabel *routing*. Tabel r*outing* akan kadaluarsa jika jarang digunakan. AODV memiliki *route discovery* dan *route maintenance*. *Route Discovery* berupa RREQ dan *Route Reply* (RREP). Sedangkan *Route Maintenance* berupa Data, *Route update* dan *Route Error* (RRER) (Sari, Syarif, & Budiardjo, 2010) .

Kelemahan pada MANET adalah keamanannya, hal ini dikarenakan media

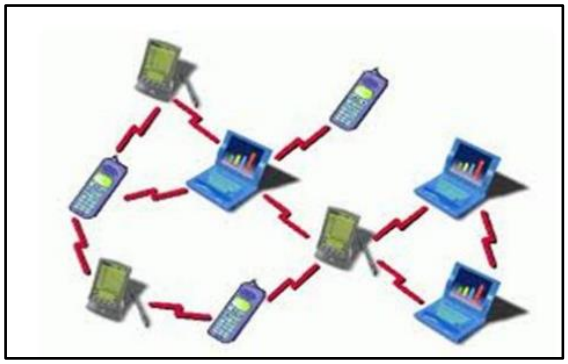
pertukaran data atau informasi pada MANET menggunakan transmisi radio ditambah tidak adanya administrator yang mengawasi perangkat komunikasi yang terhubung, sehingga rentan terjadinya serangan. (Bhattacharyya, 2011).

Serangan *rushing* memanfaatkan RREQ pada *route discovery* untuk menjadi *node* penghubung antara *source* dan *destination* paket data pada jaringan. Dalam kerjanya, *node* yang menjadi penyerang akan menempatkan dirinya pada jaringan dengan posisi yang paling dekat dengan *node* tujuan. Ketika *source node* mengirimkan RREQ ke jaringan, maka *node* penyerang akan mengirimkan RREQ juga ke *destination node*. *Node* penyerang akan berusaha secepat mungkin untuk mengirimkan RREQ ke *destination node*. Ketika *destination node* menerima RREQ tercepat yang tiba kepadanya, maka *destination node* akan memberi jawaban RREP ke jaringan tanpa memperhatikan asal RREQ yang diterimanya. Dengan demikian, jalur paket data yang akan digunakan oleh jaringan adalah jalur dengan melewati *node* penyerang tersebut. (Seyyedtaj & Jamali, 2014).

## 2. LANDASAN PUSTAKA

### 2.1 *Mobile Ad Hoc Network* (MANET)

*Mobile ad-hoc network* (MANET) adalah sebuah jaringan yang terdiri dari beberapa perangkat bergerak atau yang disebut *node* tanpa memerlukan infrastruktur jaringan yang tetap, sehingga membentuk jaringan yang bersifat sementara (Saputra, 2011). Setiap *node* dapat berfungsi sebagai *host* maupun *routers* sehingga jaringan dapat terbentuk dimana saja dan kapan saja selama dua atau lebih *node* terhubung dan saling berkomunikasi satu sama lain baik secara langsung antara *node* yang saling berhubungan maupun melalui simpul yang terbentuk dari *node* yang saling terhubung sesuai dengan topologinya dikarenakan fleksibilitas dari MANET (Roy, 2011).

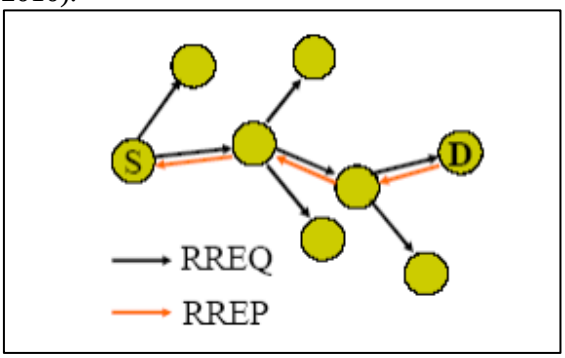


*Gambar 1. Jaringan MANET*

Pada gambar 1 menunjukkan MANET terdiri dari berbagai *mobile platform* yang disederhanakan sebagai *node* yang bergerak secara bebas dan acak.

### 2.2 *Ad Hoc On-Demand Distance Vektor* (AODV)

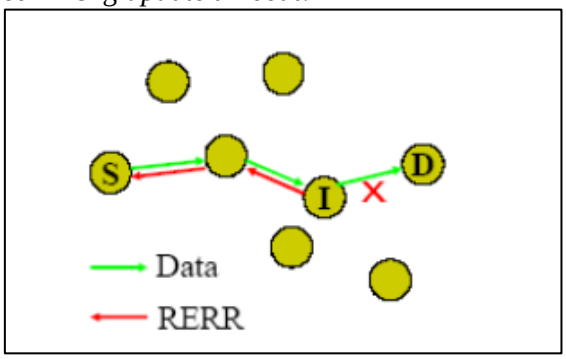
AODV merupakan salah satu protokol *routing reactive* artinya protocol ini akan bekerja ketika ada permintaan untuk mengirimkan data. Pada AODV terdapat tiga pesan utama yang digunakan untuk proses pembentukan jalur dan pemeliharaan jalur yaitu: *route request* (RREQ), *route replay* (RREP), dan *route error* RRER. AODV berjalan secara dinamis, *self-startiing*, dan *routing multihop* (Sari, Syarif, & Budiardjo, 2010).




*Gambar 2. Mekanisme Penemuan Rute*

Penemuan jalur (*Path discovery*) atau *Route discovery* di-inisiasi dengan menyebarkan RREP, seperti terlihat pada gambar 2. Ketika RREP menjelajahi *node*, ia akan secara otomatis men-setup *path*. Jika sebuah *node* menerima RREP, maka *node* tersebut akan mengirimkan RREP lagi ke *node* atau *destination sequence number*. Pada proses ini, *node* pertama kali akan mengecek *destination sequence number*. Pada proses ini, *node* pertama kali akan mengecek *destination sequence number* pada tabel *routing*, apakah

lebih besar dari 1 (satu) pada RREQ, jika benar *node* akan mengirim RREP. Ketika RREP berjalan kembali ke source melalui *path* yang telah di-setup, ia akan men-setup jalur kedepan dan meng-*update timeout*.

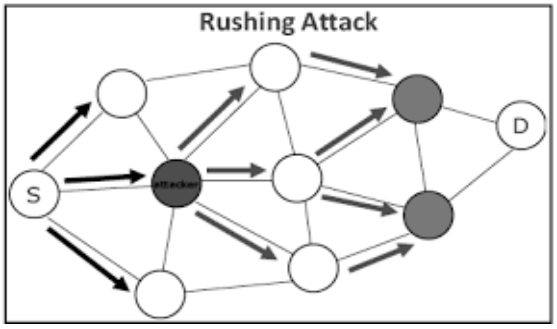



*Gambar 3. Mekanisme Data (Route Update) dan Route Error*

Jika sebuah *link* ke *hop* berikutnya tidak dapat dideteksi dengan metode penemuan rute, maka link tersebut akan diasumsikan putus dan RERR akan disebarkan ke *node* tetangganya seperti terlihat pada gambar 3 Dengan demikian sebuah *node* bisa menghentikan pengiriman data melalui rute ini atau meminta rute baru dengan menyebarkan RREQ kembali

### 2.3 *Rushing*

Serangan *rushing* memanfaatkan RREQ pada *route discovery* untuk menjadi *node* penghubung antara *source* dan *destination* paket data pada jaringan. Dalam kerjanya, *node* yang akan menjadi penyerang akan menempatkan dirinya pada jaringan dengan posisi yang paling dekat dengan *node* tujuan. Ketika *source node* mengirimkan RREQ ke jaringan, maka *node* penyerang akan mengirimkan RREQ juga ke *destination node*. *Node* penyerang akan berusaha secepat mungkin untuk mengirimkan RREQ ke *destination node*. Ketika *destination node* menerima RREQ tercepat yang tiba kepadanya, maka *destination node* akan memberi jawaban RREP ke jaringan tanpa memperhatikan asal RREQ yang diterimanya. Dengan demikian, jalur paket data yang akan digunakan oleh jaringan adalah jalur dengan melewati *node* penyerang tersebut. (Seyyedtaj & Jamali, 2014).




*Gambar 4. Serangan Rushing*

Pada gambar 4 menunjukkan mekanisme serangan *rushing*. *Attacker node* seolah-olah menjadi jalur terpendek sehingga data dikirim melalui *attacker node* dan data tersebut akan di duplikasi oleh *attacker node*.

### 2.4 *Random Way Point*

*Random way point* merupakan model pergerakan secara acak yang digunakan untuk simulasi. Dalam *random way point node* bergerak secara acak dan bebas tanpa adannya batasan dengan arah dan kecepatan yang sudah ditentukan. Untuk membentuk skenario *random way point* digunakan sebuah *tool* yang terdapat pada NS2, *tool* tersebut bernama setdest. Pada *tool* setdest *node* dapat diatur pergerekannnya dan tujuan pergerakannya. Untuk menjalankan setdest, diperlukan perintah sebagai berikut :
"setdest [-v num of version] [-n num of *node*s] [-p pausetime] [-t simtime] [-x max x] [-y max y] > [name file]
Parameter yang digunakan pada perintah untuk menjalankan *tool* setdest dijelaskan pada Tabel 1.

*Tabel 1. Parameter Baris Perintah untuk Menjalankan Setdest*

| No | Parameter | Keterangan |
|---|---|---|
| 1 | -v | Versi yang digunakan |
| 2 | -n | Jumlah *node* |
| 3 | -p | Lama waktu *node* diam ketika tiba di lokasi pergerakan |
| 4 | -M | Kecepatan *node* bergerak |
| 5 | -t | Waktu simulasi |
| 6 | -x | Panjang maksimal area simulasi |
| 7 | -y | Lebar maksimal area simulasi |

## 3. PERANCANGAN SISTEM

Bagian ini mencakup perancangan simulasi, perancangan area simulasi, perancangan letak

posisi *node*, perancangan serangan *rushing*, perancangan pergerakan *node*, dan perancangan parameter pengujian

### 3.1 Perancangan Simulasi

Perancangan simulasi ini akan menjelaskan parameter-parameter yang akan digunakan dalam simulasi serangan. Parameter-parameter ini nantinya digunakan sebagai dasar dalam proses simulasi. Parameter yang berbeda dalam setiap skenario akan menimbulkan perbedaan hasil nantinya. Pada tabel 2 adalah parameter simulasi yang digunakan.

*Tabel 2. Parameter Simulasi*

| Parameter | Nilai |
|---|---|
| Jumlah *Node* | 30, 40, 50 |
| Jumlah *Node Malicious* | 3,4,5 |
| Jenis Protokol | AODV |
| Jenis Serangan | *Rushing* |
| Simulator | *Network Simulator* 2.35 |
| *Chanel Type* | *Wireless Channel* |
| *Mobility Model* | *Random Way Point* |
| Model Propagasi | *Two Ray Ground* |
| *Network Interface* | *WirelessPhy* |
| *Antena Mode* | *OmniAntenna* |
| Ukuran Paket Data | 1024 *bytes* |
| Jenis Trafik | CBR (*Constant Bit Rate*) |
| Luas Area Jaringan | 1000 m x 1000 m |
| Kecepatan *Node* | 10 m/s |
| Waktu Simulasi | 1000 s |

### 3.2 Perancangan Area Simulasi

Perancangan area simulasi bertujuan untuk menentukan area yang digunakan dalam pengujian. Pada penelitian ini menggunakan area simulasi dengan luas 1000x1000m dengan berpatokan pada sumbu kartesius (X, Y). Pada area seluas 1000x1000m ini akan di tempatkan *node* dengan variasi jumlah 30, 40, dan 50. Pada luas 1000x1000m ini juga menjadi batas pergerakan *node* pada simulasi.

### 3.3 Perancagan Posisi *Node*

Perancangan posisi *node* bertujuan untuk menentukan posisi *node* yang digunakan dalam simulasi. Pada penelitian ini menggunakan beberapa jumlah *node* yang berbeda-beda yaitu 30, 40, dan 50 *node*, dimana *node-node* tersebut menempati posisi yang bersumbu pada sumbu x dan sumbu y.

### 3.4 Perancangan Serangan *Rushing*

Perancagan serangan *rushing* bertujuan untuk menambahakan serangan *rushing* dalam protokol AODV. Pada bagian perancangan serangan dijelaskan tentang skema penyerangan pada protokol *routing* AODV dalam jaringan *Mobile Ad Hoc Network* (MANET) dengan menambahkan beberapa fungsi untuk melakukkan serangan *rushing* pada protokol *routing* AODV. Berikut adalah beberapa fungsi yang ditambahkan untuk membentuk *node malicious* pada file aodv.h, aodv.cc, serta pada file .tcl.

### 3.5 Perancangan Pergerakan *Node*

Pergerakan *node* disusun berdasarkan luas area simulasi yang sudah di rancang. Terdapat 3 variasi jumlah *node* yang akan disimulasikan pada luas area simulasi yaitu 30, 40, dan 50 *node*. Untuk menghasilkan pergerakan *random way point* digunakan *tool* yang bernama setdest. Berikut baris perintah untuk membentuk pergerakan pada *node* 30, 40, dan 50 dengan kecepatan maksimal 10 m/s dan waktu simulasi selama 1000s

### 3.6 Perancangan Parameter Pengujian

Perancangan parameter pengujian dilakukan untuk membantu menganalisis hasil pengujian pada penelitian ini. Berikut parameter pengujian yang ditentukan:

- ***Throughput***

*Throughput* adalah banyaknya *byte* yang diteruma dalam waktu tertentu dengan satuan *byte/second* yang mana merupakan kondisi data *rate* sebenarnya dalam suatu jaringan. Besarnya selang waktu pengukuran dapat mempengaruhi hasil gambaran perilaku jaringan.

$$Throughput = \frac{jumlah\ paket\ yang\ diterima}{total\ waktu\ pengamatan}\ x\ ukuran\ paket$$

- ***End to end delay***

*End to end delay* merupakan waktu yang terjadi pada saat proses pengiriman suatu paket dari titik awal menuju titik tujuan. End to end *delay* merupakan jumlah dari waktu pengiriman, propagasi, proses, dan antrian dari suatu paket pada setiap *node* dalam jaringan.

$$End\ to\ end\ delay = \frac{waktu\ paket\ diterima - waktu\ paket\ dikirimkan}{jumlah\ paket\ yang\ dikirim}$$

- ***Packet loss***

*Packet loss* didefinisikan sebagai kegagalan transmisi paket IP mencapai tujuannya. Kegagalan paket tersebut mencapai tujuan. Hal ini berpengaruh pada retransmisi karena dapat mengurangi efisiensi jaringan secara keseluruhan, walaupun *bandwidth* yang tersedia sudah mencukupi.

$$packet\ loss = \frac{packet\ send - packet\ received}{packet\ send}\ x\ 100\%$$

- ***Packet delivery ratio***

*Packet delivery ratio* (PDR) adalah rasio antara banyaknya paket yang diterima oleh *destination node* dengan banyaknya paket yang dikirimkan oleh *source node*. *Packet delivery ratio* dapat dijadikan sebagai acuan sebagai tingkat keberhasilan sebuah protokol routing dalam pencarian dan pemeliharaan rutenya.

$$PDR = \frac{Pr}{Ps} x100\%$$

## 4 HASIL DAN ANALISIS

### 4.1 Hasil Implementasi Tanpa Serangan *Rushing*

*Tabel 3. Hasil implementasi tanpa serangan rushing*

| Jumlah *Node* | Parameter Ukur | | | |
|---|---|---|---|---|
| | *Packet Delivery Ratio* (%) | *Packet Loss* (%) | *Throughput* (kbps) | *End to End Delay* (ms) |
| 30 *Node* | 99,8346 % | 0,1654 % | 101,86 kbps | 31,9341 ms |
| 40 *Node* | 71,7122 % | 28,2878 % | 101,56 kbps | 19,5681 ms |
| 50 *Node* | 88,751 % | 11,249 % | 92,80 kbps | 356,205 ms |

Pada tabel 3 menunjukkan hasil implementasi tanpa serangan *rushing* dari 30 *node*, 40 *node*, dan 50 *node*.

### 4.2 Hasil Implementasi Serangan *Rushing*

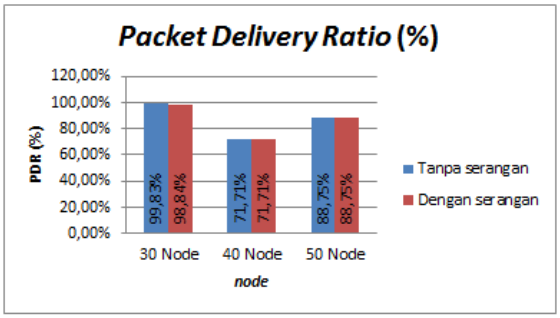
Berikut adalah hasil implementasi serangan *rushing* dengan keadaan diam dan bergerak dengan jumlah *node* 30, 40, dan 50 *node* dengan parameter ukur *packet delivery ratio, packet loss, throughput, dan end to end delay*.

- **Hasil Implementasi Serangan *Rushing* dengan 3 Serangan**

*Tabel 4. Hasil implementasi 3 serangan*

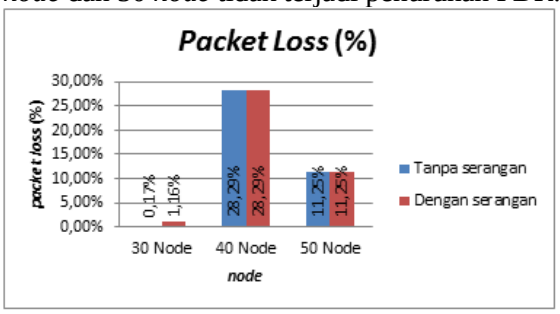
| Jumlah *Node* | Parameter Ukur | | | |
|---|---|---|---|---|
| | *Packet Delivery Ratio* (%) | *Packet Loss* (%) | *Throughput* (kbps) | *End to End Delay* (ms) |
| 30 *Node* | 98,842 % | 1,15798 % | 100,85 kbps | 790,375 ms |
| 40 *Node* | 71,7122 % | 28,2878 % | 101,56 kbps | 52,1334 ms |
| 50 *Node* | 88,751 % | 11,249 % | 92,80 kbps | 377,791 ms |

Table 4 menunjukkan hasil implementasi 3 serangan *rushing* dari 30 *node*, 40 *node*, dan 50 *node*.



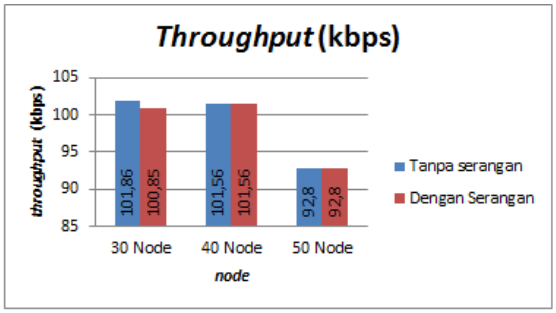

*Gambar 5. Grafik packet delivery ratio dari 3 node serangan rushing*

Pada gambar 5 menunjukkan hasil *packet delivery ratio* (PDR) dari hasil implementasi serangan *rushing* dengan jumlah 3 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *packet delivery ratio* (PDR) dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 0,99 %, 40 *node* dan 50 *node* tidak terjadi penurunan PDR.



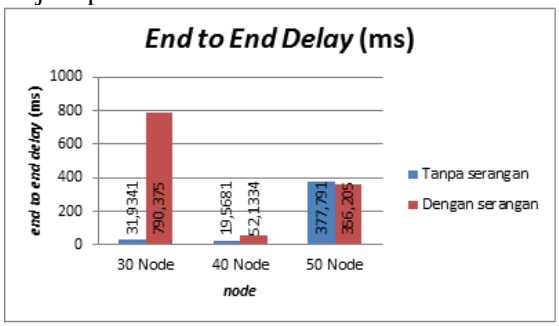

*Gambar 6. Grafik packet loss dari 3 node serangan rushing*

Pada gambar 6 menunjukkan hasil *packet loss* dari hasil implementasi serangan *rushing* dengan jumlah 3 *node*. Dapat dilihat dari grafik terdapat penaikan nilai *packet loss* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi kenaikan sebanyak 0,99 %, 40 *node* dan 50 *node* tidak terjadi kenaikan.




*Gambar 7. Grafik throughput dari 3 node serangan rushing*

Pada gambar 7 menunjukkan hasil *throughput* dari hasil implementasi serangan *rushing* dengan jumlah 3 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *throughput* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 1,01 kbps, 40 *node* dan 50 *node* tidak terjadi penurunan.




*Gambar 7. Grafik end to end delay dari 3 node serangan rushing*

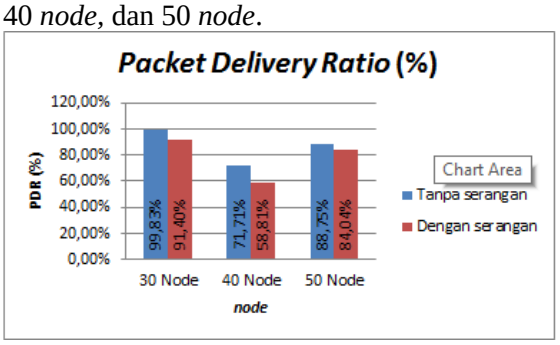
Pada gambar 7 menunjukkan hasil *end to end delay* dari hasil implementasi serangan *rushing* dengan jumlah 3 *node*. Dapat dilihat dari grafik terdapat kenaikan nilai *end to end delay* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi kenaikan sebanyak 758,4409 ms, 40 *node* terjadi kenurunan sebanyak 32,5653 ms, dan 50 *node* terjadi penurunan sebanyak 21,586 ms. Penaikan nilai *end to end delay* pada implementasi 3 serangan *rushing* paling besar terdapat pada 30 *node* dengan penaikan sebanyak 758,4409 ms.

- **Hasil Implementasi Serangan *Rushing* dengan 4 Serangan**

*Tabel 5. Hasil implementasi 4 serangan*

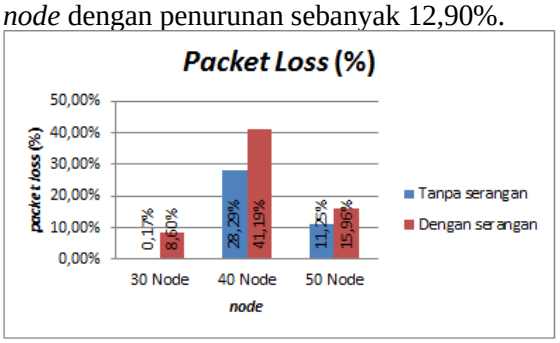
| Jumlah *Node* | Parameter Ukur | | | |
|---|---|---|---|---|
| | *Packet Delivery Ratio* (%) | *Packet Loss* (%) | *Throughput* (kbps) | *End to End Delay* (ms) |
| 30 *Node* | 91,3978 % | 8,6021 5 % | 93,25 kbps | 4067,26 ms |
| 40 *Node* | 58,8089 % | 41,1911 % | 83,29 kbps | 256,856 ms |
| 50 *Node* | 84,0364 % | 15,9636 % | 81,59 kbps | 1265,02 ms |

Pada tabel 5 menunjukkan hasil implementasi 4 serangan *rushing* dari 30 *node*, 40 *node*, dan 50 *node*.




*Gambar 8. Grafik packet delivery ratio dari 4 node serangan rushing*

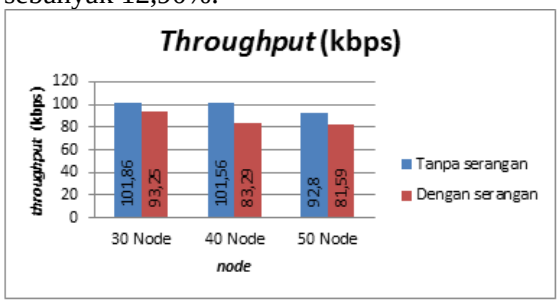
Pada gambar 8 menunjukkan hasil *packet delivery ratio* (PDR) dari hasil implementasi serangan *rushing* dengan jumlah 4 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *packet delivery ratio* (PDR) dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 8,44%, 40 *node* terjadi penurunan sebanyak 12,90%, dan 50 *node* terjadi penurunan sebanyak 4,71%. Penurunan nilai PDR pada implementasi 4 serangan *rushing* paling besar terdapat pada 40 *node* dengan penurunan sebanyak 12,90%.




*Gambar 9. Grafik packet loss dari 4 node serangan rushing*

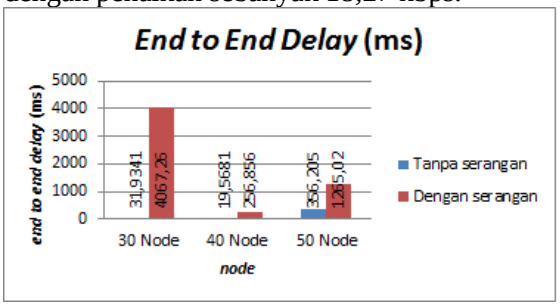
Pada gambar 9 menunjukkan hasil *packet loss* dari hasil implementasi serangan *rushing* dengan jumlah 4 *node*. Dapat dilihat dari grafik terdapat kenaikan nilai *packet loss* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penaikan sebanyak 8,44%, 40 *node* terjadi penaikan sebanyak 12,90%, dan 50 *node* terjadi penaikan sebanyak 4,71%. Penaikan nilai *packet loss* pada implementasi 4 serangan *rushing* paling

besar terdapat pada 40 *node* dengan penaikan sebanyak 12,90%.




*Gambar 10. Grafik throughput dari 4 node serangan rushing*

Pada gambar 10 menunjukkan hasil *throughput* dari hasil implementasi serangan *rushing* dengan jumlah 4 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *throughput* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 8,61 kbps, 40 *node* terjadi penurunan sebanyak 18,27 kbps, dan 50 *node* terjadi penurunan sebanyak 11,21 kbps. penurunan nilai *throughput* pada implementasi 4 serangan *rushing* paling besar terdapat pada 40 *node* dengan penaikan sebanyak 18,27 kbps.




*Gambar 11. Grafik end to end delay dari 4 node serangan rushing*

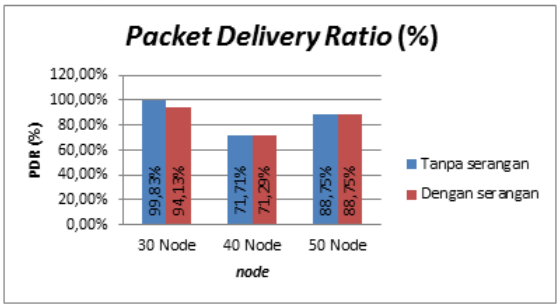
Pada gambar 11 menunjukkan hasil *end to end delay* dari hasil implementasi serangan *rushing* dengan jumlah 4 *node*. Dapat dilihat dari grafik terdapat kenaikan nilai *end to end delay* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi kenaikan sebanyak 4035,3259 ms, 40 *node* terjadi kenaikan sebanyak 237,2879 ms, dan 50 *node* terjadi kenaikan sebanyak 908,815 ms. Penaikan nilai *end to end delay* pada implementasi 4 serangan *rushing* paling besar terdapat pada 30 *node* dengan penaikan sebanyak 4035,3259 ms.

- **Hasil Implementasi Serangan *Rushing* dengan 5 Serangan**

*Tabel 6. Hasil implementasi 5 serangan*

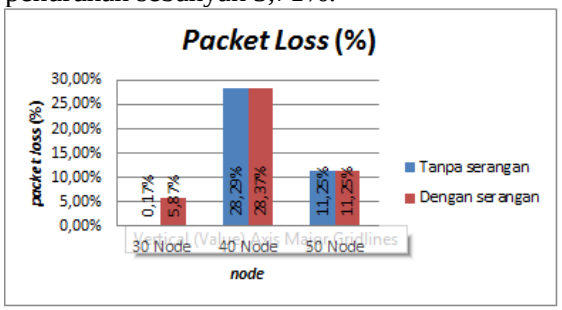
| Jumlah *Node* | Parameter Ukur | | | |
|---|---|---|---|---|
| | *Packet Delivery Ratio* (%) | *Packet Loss* (%) | *Throughput* (kbps) | *End to End Delay* (ms) |
| 30 *Node* | 94,1274 % | 5,87262 % | 96,04 kbps | 772,44 ms |
| 40 *Node* | 71,294 % | 28,3706 % | 101,44 kbps | 18,2695 ms |
| 50 *Node* | 88,751 % | 11,249 % | 90,53 kbps | 1337,27 ms |

Pada tabel 6 menunjukkan hasil implementasi 4 serangan *rushing* dari 30 *node*, 40 *node*, dan 50 *node*.




*Gambar 12. Grafik packet delivery ratio dari 5 node serangan rushing*

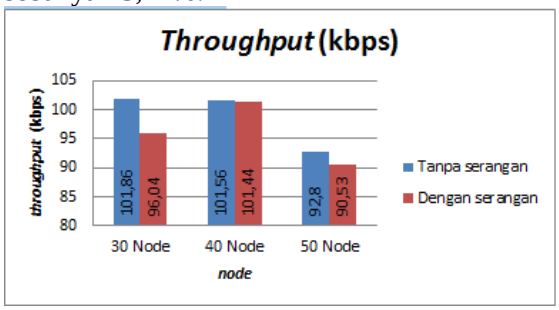
Pada gambar 12 menunjukkan hasil *packet delivery ratio* (PDR) dari hasil implementasi serangan *rushing* dengan jumlah 5 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *packet delivery ratio* (PDR) dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 5,71%, 40 *node* terjadi penurunan sebanyak 0,42%, dan 50 *node* tidak terjadi penurunan. Penurunan nilai PDR pada implementasi 5 serangan *rushing* paling besar terdapat pada 30 *node* dengan penurunan sebanyak 5,71%.




*Gambar 13. Grafik packet loss dari 5 node serangan rushing*

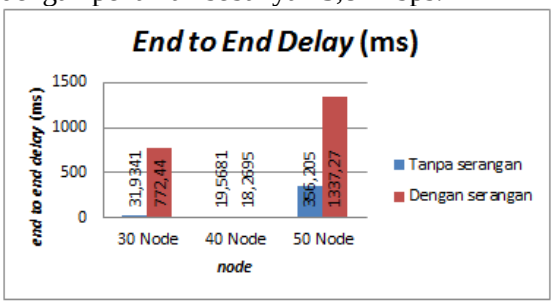
Pada gambar 13 menunjukkan hasil *packet loss* dari hasil implementasi serangan *rushing* dengan jumlah 5 *node*. Dapat dilihat dari grafik terdapat kenaikan nilai *packet loss*

dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi kenaikan sebanyak 5,71%, 40 *node* terjadi kenaikan sebanyak 0,42%, dan 50 *node* tidak terjadi kenaikan. Kenaikan nilai *packet loss* pada implementasi 5 serangan *rushing* paling besar terdapat pada 30 *node* dengan penaikan sebanyak 5,71%.




*Gambar 14. Grafik throughput dari 5 node serangan rushing*

Pada gambar 14 menunjukkan hasil *throughput* dari hasil implementasi serangan *rushing* dengan jumlah 5 *node*. Dapat dilihat dari grafik terdapat penurunan nilai *throughput* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi penurunan sebanyak 5,82 kbps, 40 *node* terjadi penurunan sebanyak 0,12 kbps, dan 50 *node* terjadi penurunan sebanyak 2,27 kbps. penurunan nilai *throughput* pada implementasi 5 serangan *rushing* paling besar terdapat pada 30 *node* dengan penaikan sebanyak 5,82 kbps.




*Gambar 15. Grafik end to end delay dari 5node serangan rushing*

Pada gambar 15 menunjukkan hasil *end to end delay* dari hasil implementasi serangan *rushing* dengan jumlah 5 *node*. Dapat dilihat dari grafik terdapat kenaikan nilai *end to end delay* dibandingkan dengan implementasi tanpa serangan. Pada 30 *node* terjadi kenaikan sebanyak 740,5059 ms, 40 *node* terjadi penurunan sebanyak 1,2986 ms, dan 50 *node* terjadi kenaikan sebanyak 981,065 ms. Kenaikan nilai *end to end delay* pada implementasi 5 serangan *rushing* paling besar terdapat pada 50 *node* dengan penaikan sebanyak 981,065 ms.

## 6 ANALSIS

Berdasarkan dari implementasi yang dilakukan didapatkan simpulan bahwa serangan *rushing* memepengaruhi kinerja dari *routing* protokol AODV dengan mengubah jalur yang seharusnya dilalui. Serangan *rushing* berdampak pada ketiga jumlah *node* yang diujikan 30 *node*, 40 *node*, dan 50 *node* dengan adanya penurunan kualitas dengan ditunjukkan nilai pada *packet delivery ratio* yang turun, *packet loss* yang naik, *throughput* yang turun, dan *end to end delay* yang naik dibandingkan dengan implementasi tanpa serangan *rushing*. Penurunan paling besar terjadi pada implementasi 4 serangan *rushing* terjadi penurunan kualitas dimana *packet delivary ratio* pada 40 *node* terjadi penurunan sebesar 12,90% , *packet loss* pada 40 *node* terjadi kenaikan sebesar 12,90%, *throughput* pada 40 *node* terjadi penurunan sebesar 18,27 kbps,dan *end to end delay* pada 30 *node* terjadi kenaikan sebesar 4035,3259 ms. Dibandingkan dengan percobaan pada 30 *node* dan 50 *node* terjadinya penurunan kualitas sangat kecil dan cenderung tidak ada penurunan.

Berdasarkan hal tersebut serangan *rushing* secara keseluruhan memberikan dampak yang lebih pada jumlah node yang sedikit, namun serangan *rushing* sangat dipengaruhi oleh posisi *node* serangan, pergerakan *node* serangan, pergerakan *node sender* dan *receiver*, dan pergerakan *node sekitarnya*.

## 7 KESIMPULAN

1. Serangan *rushing* memepengaruhi kinerja dari *routing* protokol AODV dengan mengubah jalur yang seharusnya dilalui.
2. Serangan *rushing* memberikan dampak pada *routing* protokol AODV dengan menurunkan kinerjanya. Dengan dibuktikan dari nilai *packet delivery ratio, packet loss, throughput*, dan *end to end delay* yang turun kualitasnya. Penurunan paling besar terjadi pada implementasi 4 serangan *rushing* terjadi penurunan kualitas dimana *packet delivary ratio* pada 40 *node* terjadi penurunan sebesar 12,90% , *packet loss* pada 40 *node* terjadi kenaikan sebesar 12,90%, *throughput* pada 40 *node* terjadi

penurunan sebesar 18,27 kbps,dan *end to end delay* pada 30 *node* terjadi kenaikan sebesar 4035,3259 ms. Dibandingkan dengan percobaan pada 30 *node* dan 50 *node* terjadinya penurunan kualitas sangat kecil dan cenderung tidak ada penurunan. Berdasarkan hal tersebut serangan *rushing* secara keseluruhan memberikan dampak yang lebih pada jumlah node yang sedikit, namun serangan *rushing* sangat dipengaruhi oleh posisi *node* serangan, pergerakan *node* serangan, pergerakan *node sender* dan *receiver*, dan pergerakan *node sekitarnya*.

## 8 DAFTAR PUSTAKA

Bhattacharyya, A., Banerjee, A., & Bose, D. (2011). Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques. Rasearch Gate.

Pratomo, I., & Hizburrahman, M. H. (2015). Pendeteksian Dan Pencegahan Serangan Black Hole & Gray Hole Pada Manet. JAVA Journal of Electricl and Electronics Engineering.

Sari, R. F., Syarif, A., & Budiardjo, B. (2010). 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 of Technology Series, 12(1). doi:10.7454/mst.v12i1.517

Seyyedtaj, M., & Jamali, M. A. (2014). Different Types of Attacks and Detection Techniques in Mobile Ad Hoc Network. International Journal of Computer Applications Technology and Research, 3(9), 541-546. doi:10.7753/ijcatr0309.1002

Thilagarasi, R., & Geetha, D. (2015). Review On Rushing Attack And Its Prevention Techniques In MANET. Retrieved August 20, 2018.