ANALISIS PERFORMANSI PROTOKOL AODV (*AD HOC ON DEMAND DISTANCE VECTOR*) DAN DSR (*DYNAMIC SOURCE ROUTING*) TERHADAP *ACTIVE ATTACK* PADA MANET (*MOBILE AD HOC NETWORK*) DITINJAU DARI QOS (*QUALITY OF SERVICE*) JARINGAN

PERFORMANCE ANALYSIS AODV (AD HOC ON DEMAND DISTANCE VECTOR) AND DSR (DYNAMIC SOURCE ROUTING) PROTOCOL TO ACTIVE ATTACK I MANET (MOBILE AD HOC NETWORK) IN TERM OF NETWORK QOS (QUALITY OF SERVICE)

Evi Hartati Harahap

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom

evi.hartati.26@gmail.com

ABSTRAK

Mobile Ad hoc Network (MANET) merupakan jaringan dengan *node-node* yang berfungsi sebagai *router* dan memiliki infrastruktur jaringan yang tidak tetap. Oleh karena itu, dalam jaringan akan sangat sering terjadi keluar masuk *node-node*. Hal ini tentunya akan sangat rentan terhadap serangan pada jaringan sehingga dibutuhkan suatu protokol yang mampu menjamin pesan dapat dikirimkan dengan aman.

Pada penelitian ini dibandingkan performansi dua protokol routing MANET, yaitu AODV (Ad hoc On Demand Distance Vector) dan DSR (Dynamic Source Routing). Kedua protokol ini diberikan active attack. Active attack yang diberikan adalah *rushing attack*, *sinkhole attack*, *replay attack*, dan *sybil attack*.

Performansi kedua protokol terhadap active attack diuji menggunakan software Network Simuator v2.34 (NS -2.34). Dengan menggunakan mobility pattern random waypoint, jumlah *node* yang digunakan adalah 10, 15, dan 20 dengan kecepatan *node* 15 m/s, 20 m/s, dan 25 m/s. Performansi yang akan diukur adalah jumlah *packet delivery ratio*, rata-rata waktu *delay*, rata-rata *throughput* dan *routing overhead*.

Dari hasil yang diperoleh dapat diketahui bahwa penurunan *packet delivery ratio* terbesar yaitu 16,4242% terjadi pada *sybil attack* menggunakan protokol AODV dengan jumlah *node* 15 dan kecepatan 25 m/s , penurunan *average delay* paling besar terjadi pada *rushing attack* dengan menggunakan AODV pada 20 *node* dan kecepan 15 m/s sebesar 2968,3354 ms, penurunan *throughput* terbesar terjadi pada *sybil attack* pada protokol DSR sebesar 5.4949 Kbps di 15 *node* dengan kecepatan 25 m/s dan penurunan *routing overhead* paling besar terjadi pada *replay attack* dengan protokol AODV sebesar 243.1667% dengan 15 *node* pada kecepatan 20 m/s. Oleh karena itu, penanganan untuk *rushing attack* terbaik menggunakan protocol DSR dengan jumlah *node* 20 dan kecepatan 25 m/s karena penurunan throughput sebesar 0,648% , *sinkhole attack* dapat dihadapi dengan menggunakan protokol DSR dengan 10 *node* dan kecepatan 15 m/s karena dapat mempertahankan *packet delivery ratio*nya, *replay attack* dapat dihadapi dengan menggunakan protokol DSR tanpa ada penurunan *delay* dengan kecepatan 20 m/s pada 20 *node*, dan *sybil attack* dihadapi dengan protokol AODV dengan kecepatan 20 m/s pada 20 *node* dengan tanpa penurunan *routing overhead*.

Kata kunci: MANET, *Rushing*, *Sinkhole*, *Replay*, *Sybil*, AODV, DSR

ABSTRACT

Mobile Ad hoc Network (MANET) is a network with nodes which are used as a router and has dynamic network infrastructure. Hence, nodes move frequently from and to this network. This case is so vulnerable to the attacks so that need a protocol which can make sure the packet can be sent safely.

In this research compared two MANET routing protocol performance, that is AODV (Ad hoc On Demand Distance Vector) and DSR (Dynamic Source Routing). Both of this protocol is given active attack. The active attacks are rushing attack, sinkhole attack, replay attack, and sybil attack.

These two protocol performance to active attack are tested using Network Simulator v2.34 (NS-2.34). By using random waypoint mobility pattern, number of nodes are 10, 15, and 20 nodes with speeds 15 m/s, 20 m/s, and 25 m/s. The performances are measured packet delivery ratio, average delay, average throughput, and routing overhead.

From the result known that the highest decrease packet delivery ratio by 16.4242% in sybil attack AODV protocol 15 nodes and speed 25 m/s , the highest decrease average delay in rushing attack with AODV protocol 20 nodes and speed 15 m/s sebesar 2968.3354 ms, the highest decrease throughput in sybil attack with

DSR protocol 15 nodes and speed 25 m/s by 5.4949 Kbps and the highest decrease routing overhead in replay attack AODV protocol 15 nodes and speed 20 m/s by 243.1667%. Because of that, DSR is the best protocol to face rushing attack with 20 nodes and speed 25 m/s by throughput decrease 0.648%, to face sinkhole attack with DSR protocol in simulation 10 nodes and speed 15 m/s by the stabil packet delivery ratio , to face replay attack with DSR protocol in simulation 20 node and speed 20 m/s without delay decrease, and to face sybil attack with AODV protocol in simulation 20 nodes and speed 20 m/s by without routing overhead decrease.

.

Keywords: MANET, Rushing, Sinkhole, Replay, Sybil, AODV, DSR

1. Pendahuluan

Semakin hari kebutuhan manusia untuk akan komunikasi semakin besar. Saat ini, komunikasi bergerak (*mobile*) menjadi kebutuhan komunikasi yang sudah tidak terpisahkan lagi bagi manusia. Begitu juga halnya dengan kebutuhan komunikasi untuk daerah-daerah yang susah dijangkau oleh infrastruktur tetap.

Untuk itu, kehadiran MANET (*Mobile Ad hoc Network*) menjadi jawaban untuk komunikasi yang belum mempunyai infrastruktur yang tetap. MANET merupakan jaringan yang tidak memiliki infrastruktur yang tetap dan *node-node* yang berada di dalamnya berfungsi sebagi *router* untuk meneruskan informasi yang dikirimkan. Dengan mobilitas *node-node*nya yang tinggi, maka MANET akan sangat rentan untuk disusupi oleh *node-node* jahat.

Dalam melaksanakan tugasnya, MANET dibantu oleh protokol *reactive* dan protokol *proaktive*. Protokol *reactive* dapat membantu MANET untuk mengamankan jaringan dari serangan. Protokol AODV dan DSR akan menghambat *rushing attack*, *sinkhole attack*, *replay attack*, dan *sybil attack*. Serangan-serangan yang diberikan ini akan menurunkan performansi jaringan.

2. Landasan Teori

2.1 *Mobile Adhoc Network* (MANET)

MANET adalah sebuah jaringan yang terdiri dari beberapa *node-node* yang bersifat *mobile*, dimana *node-node mobile* tersebut dapat berkomunikasi dengan tanpa menggunakan jalur komunikasi yang permanen, atau bersifat sementara (*ad hoc*). Berbeda dengan jaringan *wireless* lainnya, MANET tidak memerlukan infrastruktur jaringan dan memiliki topologi yang berubah-ubah setiap saat. Oleh karena itu, MANET memiliki kemampuan untuk mengkonfigurasikan jaringan secara mandiri.

MANET memiliki *node-node* yang bersifat *mobile* yang dapat bergerak ke segala arah untuk melakukan komunikasi. *Node-node* yang ada pada jaringan ini berfungsi juga sebagai *router* yang mampu untuk meneruskan pesan yang akan dikirimkan ke penerima. Setiap *node* pada jaringan MANET harus mampu menentukan rute terbaiknya untuk meneruskan paket informasi dan jika mengalami kegagalan kirim karena ada gangguan rute, maka *node* memperbaiki rute tersebut.

2.1.1. Karakteristik Jaringan *Ad Hoc*

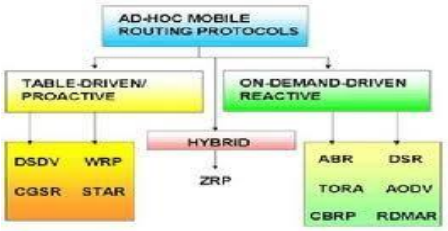
Seperti yang telah diketahui bahwa *node-node* yang ada pada jaringan MANET tidak hanya berperan sebagai *node* pengirim dan penerima saja, tetapi juga berfungsi sebagai *router* yang mampu menentukan rute untuk pengiriman data. Beberapa karakteristik MANET diantaranya :

a. *Multiple wireless link* : setiap *node* memiliki *mobility* yang mampu berhubungan dengan *node* lainnya
b. *Dynamic topology* : karena *node* yang bersifat *mobile*, maka topologi jaringan juga berubah-ubah sesuai dengan keluar masuknya *node* pada jaringan
c. *Limited resource* : jaringan MANET memiliki daya dan kapasitas memori yang terbatas.
d. Keamanan yang terbatas : karena menggunakan gelombang radio untuk mentrasmisikan pesan, keamanan MANET kurang terjamin.

2.1.2. Protokol *Routing* pada MANET

Routing merupakan suatu mekanisme penentuan jalur komunikasi dari *node* pengirim ke *node* penerima. *Routing* bekerja pada layer ketiga OSI (layer Network). Untuk melakukan pengiriman data (informasi) tersebut, maka protokol *routing* akan bertugas untuk menentukan jalur yang akan digunakan untuk mengirimkan data sampai tiba di tempat penerima.

Pada MANET sendiri, terdapat dua jenis protokol *routing*, yaitu protokol proaktif dan protokol reaktif. Protokol proaktif bertugas untuk meng-*udpate* tabel *routing* secara berkala, sedangkan protokol reaktif berfungsi untuk membentuk rute jika suatu *node* meminta untuk dibuatkan rute pengiriman pesan. Berikut beberapa protokol yang ada di MANET :

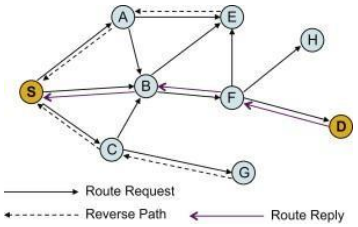


Gambar 2.2 Protokol *routing* pada MANET

2.2. *Ad Hoc On Demand Distance Vector* (AODV)

AODV merupakan protokol *routing* yang bersifat reaktif. Protokol ini bersifat reaktif karena protokol ini mulai bekerja saat ada permintaan dari *source node* untuk mencari tahu jalur-jalur yang akan digunakan untuk mengirimkan pesan ke *node* tujuan. AODV akan berusaha untuk menemukan jalur yang tidak ada *loop* dan menemukan jalur terpendek untuk menuju *node* tujuan.

Seperti yang telah dijelaskan sebelumnya, AODV akan bekerja ketika ada permintaan dari *source node* untuk menemukan rute menuju *destination node* karena akan ada pengiriman pesan. Untuk menemukan jalur yang terbaik bagi *source node*, maka AODV akan melakukan *Route discovery* dengan menyebarkan *Route Request* (RREQ) ke semua *node* yang bersebelahan dengan *source node*. Bersama dengan pesan RREQ, dikirimkan juga *ID broadcast* dan *sequence number* yang berfungsi untuk menghindari pengiriman pesan yang sama ke suatu *node*. *Node* tetangga tersebut akan mengirimkan RREQ ke *node* tetangganya lagi hingga berakhir di *node* tujuan. Setelah RREQ sampai ke *node* tujuan, maka *node* tujuan akan membalas pesan RREQ dengan *Route Reply* (RREP). Jalur yang akan dipilih tentunya rute dengan jarak terpendek dan cost yang lebih rendah dibandingkan dengan jalur yang lainnya.



Gambar 2.3. Proses *route discovery* pada AODV

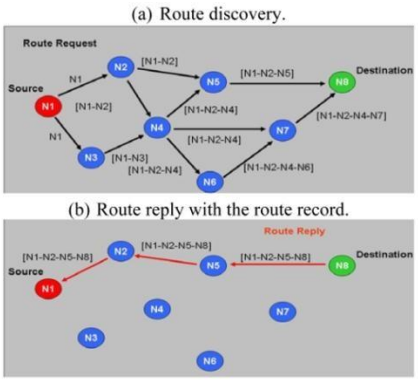
Untuk menghindari terjadinya perubahan topologi jaringan, AODV akan mengirimkan pesan HELLO secara berkala. Jika selama proses pengiriman pesan, terjadi perubahan topologi yang menyebabkan rute menuju *node* tujuan terputus, maka suatu *node* akan mengirimkan *Route Error* (RRER) ke *node* tetangganya hingga ke *source node*. Setiap *node* akan memperoleh pesan RRER dan *source node* akan melakukan *route discovery* lagi untuk menemukan rute menuju *node* tujuan.

2.3. *Dynamic Source Routing* (DSR)

Dynamic Source Routing (DSR) protokol adalah sebuah protokol *routing* reaktif yang bekerja saat ada permintaan dari sourse *node* agar dapat mengirimkan pesan ke *node* tujuan. Dalam melaksanakan tugasnya, DSR dapat menggunakan dua mekanisme yang dapat digunakan untuk memastikan rute tetap terhubung, yaitu *route discovery* dan *route maintenance*.

Berbeda dengan AODV, DSR memiliki *cache memory* yang dapat menyimpan semua informasi *routing* yang ada di dalam jaringan. Hal ini dapat memudahkan DSR untuk proses *recovery* jaringan jika terjadi perubahan topologi secara tiba-tiba. Hal ini efisien dilakukan pada jaringan berkapasitas kecil (jumlah *node* sekitar 2-29 *node*[2])

DSR akan mulai mencari rute dari *source node* ke *node* tujuan dengan *route recovery*. Pada saat *route recovery* ini, DSR akan menyebarkan pesan *Route Request* (RREQ) ke semua *node* tetangga dari *sourcenode*. RREQ yang dikirimkan berisi alamat pengirim dan tujuan pesan. *Node-node* yang menerima RREQ kemudian akan meng-*update* informasi jalur menuju pengirim di dalam *cache* route-nya, menambahkan alamatnya ke dalam paket RREQ, lalu mengirimkannya ke *node* tetangganya, kecuali jika *node* tersebut adalah *node* tujuan atau *node* yang memiliki informasi jalur menuju *node* tujuan di dalam *cache* route-nya[2]. Setelah *node* tujuan menerima RREQ, kemudian *node* tersebut akan mengirimkan pesan *Route Reply* (RREP) menuju *source node*. RREP merupakan pesan yang menandakan bahwa jalur dari *source node* menuju *destination node* telah ditemukan dan berisi informasi rute lengkap ke *node* tujuan.



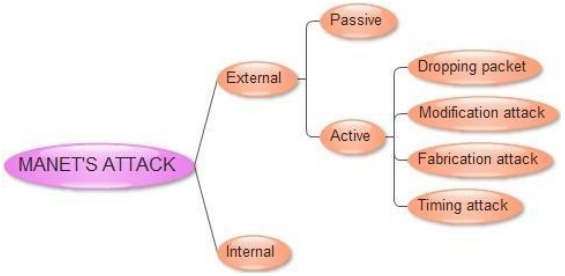
Gambar 2.6 *Route discovery* DSR [4]

Selanjutnya, jika saat pengiriman pesan terjadi perubahan topologi jaringan, maka DSR akan mencari rute lain yang tersedia pada *cache router*/*cache memory*, tanpa harus melakukan *route discovery* lagi. *Cache router* ini berisi semua *routing* yang tersedia pada jaringan. Mekanisme *maintenance* hanya dilakukan jika di dalam jaringan terjadi perubahan topologi pada saat *source node* sedang mengirimkan pesan ke *node* tujuan. Jika hal ini terjadi, maka *node* akan mengirimkan pesan *Route error* (RERR). Untuk mengirimkan pesan, *Source node* akan mencari jalur alternatif dengan menggunakan jalur yang ada pada *cache router*. Oleh karena itu, tabel *routing* yang tersimpan pada *cache router* akan di-*update* secara berkala. Jika keruskakan rute tidak dapat diatasi dengan bantuan *cache* route, maka akan diakukan *route discovery* untuk menemukan jalur terbaru dari *source node* menuju *node* tujuan.

2.4. Serangan pada MANET

Salah satu karakteristik MANET adalah keamanan yang terbatas. Serangan-serangan yang diberikan terhadap MANET bertujuan untuk mengetahui informasi yang dikirimkan antar *node* dengan cara menyusup diantara *node-node* yang ada pada jaringan ataupun dengan cara membanjiri jaringan dengan *node-node* yang jahat.

Pada dasarnya serangan pada MANET dapat dibagi ke dalam dua kategori, yaitu *Passive attack* dan *Active attack*. *Passive attack* biasanya tidak menyerang sistem secara langsung, melainkan hanya memonitoring pengiriman data pada jaringannya untuk mengetahui informasi yang dikirimkan, kemudian „mencuri" informasi yang diinginkan. *Active attack* akan menyerang jaringan secara langsung sehingga perubahan yang terjadi pada paket data akan terlihat. Cara yang biasa digunakan pada *active attack* adalah dengan *dropping paket*, *modification*, *fabrication*, dan *timing attack*. Perubahan pada jaringan akan lebih mudah teramati dengan *active attack*. Berikut kasifikasi serangan pada MANET :



Gambar 2.7 Klasifikasi jenis serangan pada MANET

Kemudian klasifikasi serangan di atas dapat dikelompokkan lagi berdasarka OSI layer. Tabel di bawah ini mengklasifikasikan serangan pada MANET berdasarkan OSI layer.

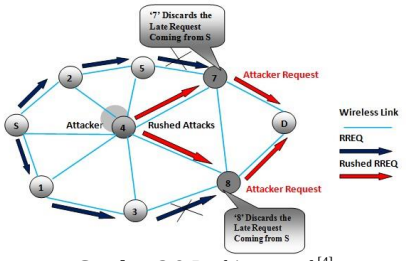
Tabel 2.1 Tabel klasifikasi serangan MANET berdasarkan layer

No	Layer	Types of *Attacks*
1	*Application*	*Malicious code*, *Data corruption*, *Viruses and worms*
2	*Transport*	*Session hijcking attack*, SYN *Flooding attack*
3	*Network*	*Blackhole*, *Wormhole*, *Sinkhole*, *Link spoofing*, *Rushing attack*, *Replay attack*, *Link withholding*, Resource consumption attack, *Sybil attack*, *Byzantine attack*, *Flooding attack*

4	*Data Link*	*Selfish misbehaviour, Malicious behaviour, Traffic analysis*
5	*Physical*	*Eavesdropping, Jamming, active interference*

2.4.1. Rushing Attack

Rushing attack merupakan bagian dari *timing attack*. Serangan ini akan mengganggu proses yang ada pada *route discovery*. *Node* yang diinisialisasi sebagai penyerang akan berada memanfaatkan RREQ pada proses *route discovery* untuk melancarkan aksinya.

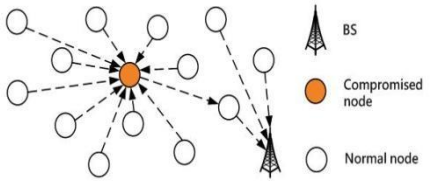


Gambar 2.8 *Rushing attack*[4]

Seperti yang terlihat pada gambar di atas, *rushing attack* 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. Akhirnya, *node* penyerang akan dengan mudahnya mengetahui informasi yang ada pada data yang dikirimkan dan *dropping* data yang diinginkan.

2.4.2. *Sinkhole Attack*

Sinkhole attack merupakan salah satu *active attack* yang berada pada layer network. Serangan *sinkhole* ini akan memberikan informasi *routing* yang salah pada *node-node* yang ada pada jaringan, sehingga informasi yang dikirimkan dapat diketahui oleh penyerang.



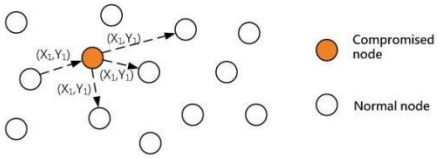
Gambar 2.9 Serangan *sinkhole*[4]

Cara kerja serangan ini biasanya menggunakan kelemahan protokol yang digunakan pada jaringan. Serangan pada AODV akan dilakukan dengan memaksimalkan *sequence number* atau meminimalkan jumlah *hop* pada jaringan AODV. Sedangkan untuk DSR, serangan ini akan memanfaatkan pesan RREQ yang berisi alamat pengirim atau tujuan dengan memasukkan *node sinkhole* sebagai *hop* tujuan.

Node yang akan digunakan untuk menjebak akan diletakkan di dalam jaringan diantara *node* lainnya. Peletakan *node sinkhole* ini akan sangat menentukan. *Node* tersebut dibuat dengan penawaran bandwidth yang paling hemat dan *cost* yang paling murah. Dengan begitu, maka pemilihan jalur pada kedua protokol dapat melibatkan *node* tersebut.

2.4.3. *Replay Attack*

Serangan ini memanfaatkan karakteristik MANET yang ber-*mobility* tinggi. Karena setiap *node* yang ada pada MANET dapat masuk dan pergi dari jaringan setiap saat, sehingga tidak menutup kemungkinan *node-node* yang bergabung di dalam jaringan tersebut adalah *node* yang memiliki niat jahat terhadap jaringan. Oleh sebab itu, hal ini dimanfaatkan *replay attack* untuk mengganggu kerja jaringan.



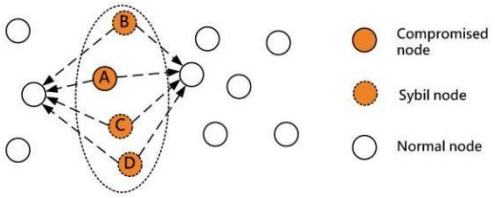
Gambar 2.10 Gambar *replay attack*[4]

Dalam melancarkan aksinya, *node replay attack* yang berada di dalam jaringan akan merekam data valid yang diterimanya. Kemudian *node* tersebut akan mengirimkan kembali data valid yag telah tertangkap sebelumnya ke *node-node* lain di dalam jaringan. *Node-node* yang menerima kiriman paket

data tersebut akan meng-*update table routing*-nya dengan paket data yang sudah "basi". Tujuannya adalah untuk menyebabkan traffik jaringan yang padat dan gangguan operasi MANET.

2.4.4. *Sybil Attack*

Serangan ini merupakan serangan ke sekelompok *node*. *Node* yang akan menyerang memiliki beberapa identitas yang dapat digunakan untuk mengelabui *node-node* lain. identitas-identitas tersebut diperoleh dengan cara diciptakan sendiri atau mengambil identitas *node* lain yang ada pada jaringan.



Gambar 2.11 *Sybil attack*

Dengan identitas-identitas yang dimilikinya, *sybil attack* dapat menggunakan beberapa *node* untuk melakukan serangan. *Node-node sybil* ini akan mengetahui informasi yang dikirimkan. Ketika paket data tersebut akan diteruskan ke *node* penerima, maka *sybil node* akan mengubah atau *dropping* paket data yang diterimanya.

3. Pemodelan dan Perancangan Sistem

3.1. Asumsi Sistem

Skenario dibangun menjadi dua skenario untuk membandingkan hasil performansi jaringan, dengan tanpa serangan dan dengan serangan. Adapun kondisi lingkungan yang diciptakan adalah :

No	Parameter	Nilai
1	Simulator	NS-2.34
2	Waktu simulasi	100 detik
3	Jumah node	10, 15, dan 20
4	Routing protocol	AODV and DSR
5	Traffik model	CBR
6	Area simulasi	500 x 500 meter
7	Kecepatan node	15, 20 dan 25 m/s
8	Model pergerakan	*Random Waypoint*
9	Background traffic	Tidak ada
10	Ukuran paket	512 bit
11	Jenis serangan	*Rushing*, *Sinkhole*, *Replay*, dan *Sybil*

3.2. Perancangan Topologi

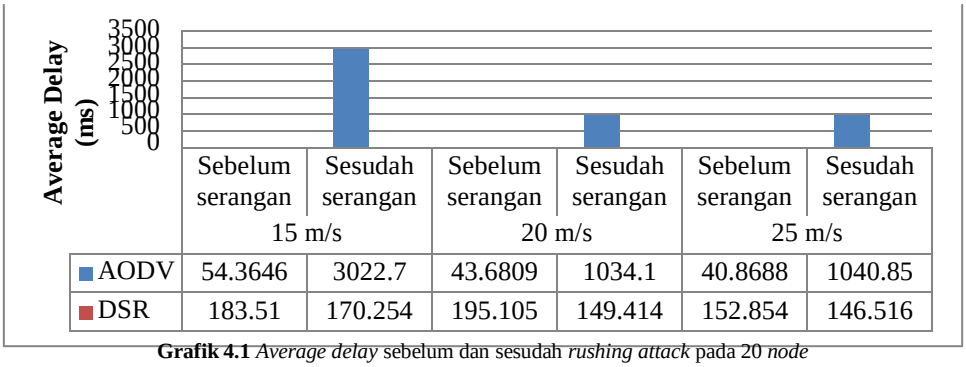
Topologi yang digunakan dibagi menjadi tiga, yaitu topologi 10 *node*, 15 *node*, dan 20 *node*. Masing-masing *node* disimulasikan dengan kecepatan 15, 20, dan 25 m/s. Tiap-tiap topologi diberi serangan *rushing*, *sinkhole*, *replay*, dan *sybil* serta dijalankan dengan protokol AODV dan DSR. Penyerang berasal dari *node* yang berada di dalam jaringan. *Node* penyerang ditentukan sesuai topologi jaringan karena posisi *node* penyernag akan menentukan keberhasilan serangan pada jaringan.

4. Implementasi dan Analisa Hasil Sistem

Simulasi dilakukan pada protocol AODV dan DSR dengan menghitung *packet delivery ratio*, *average delay*, *average throughput*, dan *routing over head*.

4.1. *Rushing Attack*

Rushing attack dilakukan dengan memanfaatkan proses *route discovery*. Pada saat RREQ dikirimkan, *node* penyerang yang menerimanya, akan mem*forward* RREQ yang diterimanya ke *node* tetangganya dengan mengabaikan *delay* pada mekanisme *routing*. Dengan begitu, *destination node* akan membalas RREP pada RREQ yang pertama kali tiba padanya. Akhirnya, node penyerang turut serta dalam rute pengiriman paket data. Ketika paket data sudah diterima, pada AODV *node* penyerang, maka *node* penyerang akan men*delay* paket yang ditermanya dan pada DSR paket data yang diterima di*drop*. Tentunya ini akan meningkatkan *average delay* jaringan. Berikut hasil simulasi :



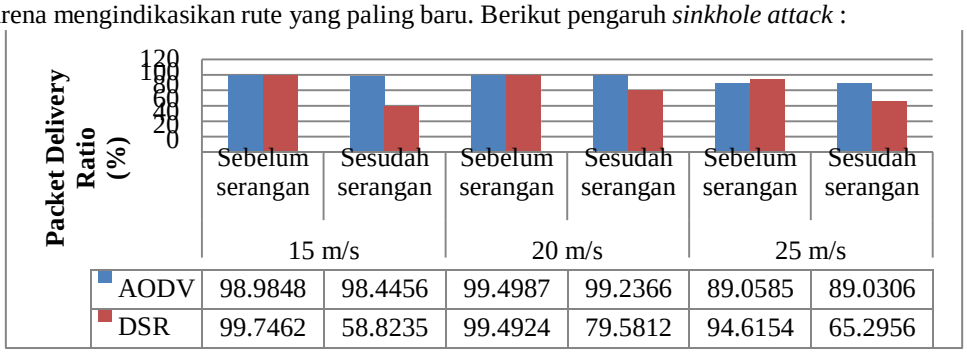
	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan
	15 m/s		20 m/s		25 m/s	
AODV	54.3646	3022.7	43.6809	1034.1	40.8688	1040.85
DSR	183.51	170.254	195.105	149.414	152.854	146.516

Grafik 4.1 *Average delay* sebelum dan sesudah *rushing attack* pada 20 *node*

Dari hasil diatas, dapat dilihat bahwa *rushing attack* menyebabkan delay yang sangat besar di dalam jaringan. Untuk *packet delivery ratio*, DSR memiliki ketahanan yang lebih besar dibandingkan dengan AODV. Hal ini sangat memungkinkan karena DSR memiliki *route cache* yang dapat membantunya dalam *route maintenance*. Akibatnya, *throughput* jaringan DSR lebih handal dibandingkan dengan AODV. sedangkan pada *routing overhead*, AODV lebih baik dibandingkan dengan DSR.

4.2. *Sinkhole Attack*

Saat proses *route discovery* sedang berlangsung dan *node* penyerang mendapatkan RREQ, maka RREQ yang diterima diubah dengan memaksimalkan *sequence number*nya sehingga bisa dipilih oleh *destination node* karena mengindikasikan rute yang paling baru. Berikut pengaruh *sinkhole attack* :



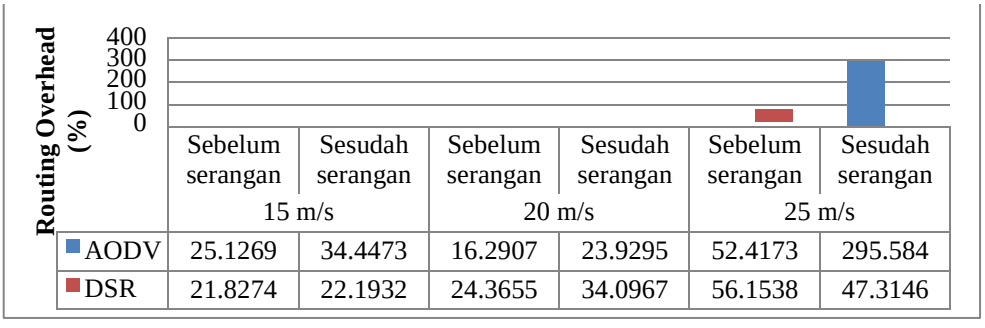
	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan
	15 m/s		20 m/s		25 m/s	
AODV	98.9848	98.4456	99.4987	99.2366	89.0585	89.0306
DSR	99.7462	58.8235	99.4924	79.5812	94.6154	65.2956

Grafik 4.2 *Packet delivery ratio* sebelum dan sesudah *sinkhole attack* pada 15 *node*

Dari hasil diatas terlihat penurunan *packet delivery ratio* pada DSR lebih besar dibandingkan dengan AODV. Ini dikarenakan DSR memilih *node* penyerang sebagai bagian dari rute pegiriman paket data disebakan mekanisme DSR yang me*reply* semua RREQ yang sampai padanya, termasuk RREQ *node* penyerang. Sedangkan pada AODV hanya akan *reply* RREQ yang tiba lebih dulu sehingga kemungkinan *node* penyerang lebih sedikit. *Packet delivery ratio* DSR turun diiringi dengan *throughput* yang menurun dan *routing overhead* yang meningkat. *Routing overhead* meningkat karena jumlah *packet routing* yang meningkat akibat kegiatan DSR yang berusaha menyelamatkan paket data yang terkena serangan. Akibat lainnya, *delay* yang lebih singkat karena paket data yang tak tersampaikan.

4.3. *Replay Attack*

Saat *node* penyerang menerima RREQ yang dikirimkan *source node*, maka *node* penyernag menunda pengiriman RREQ yang diterimanya beberapa saat, lalu menyebarkan RREQ "basi" tersebut ke tetangga sekitarnya. Akibatnya, *node-node* tetangganya akan meng*update routing table* mereka dengan RREQ "basi" tersebut. *Replay attack* bertujuan untuk meningkat *routing overhead* jaringan dan memberikan informasi *routing* yang salah. Berikut peformansi jaringan akibat *reply attack* :



	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan	Sebelum serangan	Sesudah serangan
	15 m/s		20 m/s		25 m/s	
AODV	25.1269	34.4473	16.2907	23.9295	52.4173	295.584
DSR	21.8274	22.1932	24.3655	34.0967	56.1538	47.3146

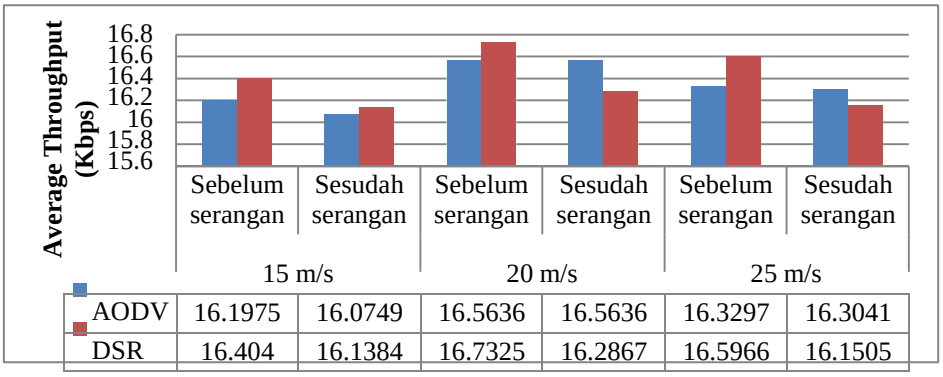
Grafik 4.3 *Routing overhead* sebelum dan sesudah *replay attack* pada 15 *node*

Dari grafik diatas terlihat peningkatan *routing overhead* akibat *replay attack*. *Routing overhead* pada AODV meningkat lebih tajam dibanding DSR. *Replay attack* bekerja optimal ketika jumlah *node* semakin banyak dan kecepatan *node* meningkat. Dengan kondisi tersebut maka *node* penyerang akan dengan mudah menyebarkan *routing packet* "basi"nya. Semakin tiggi kecepatn *node* di dalam jaringan, maka *link failure* akan semakin banyak dan meminta AODV untuk melakukan *route discovery* lebih sering. Akibatnya *packet routing* meningkat di jaringan. Sedangkan pada DSR, *route discovery* dapat diminimalisir selama *cache memory* pada setiap *node* mampu meng*cover* kebutuhan rute akibat *link failure*.

Peningkatan *routing overhead* ini diiringi dengan meningkatnya *packet delivery ratio* dan *throughput* jaringan. Ini menunjukkan usaha protokol untuk menjaga performance jaringannya walaupun harus melakukan proses *route discovery* lebih sering.

4.4. *Sybil Attack*

Sybil attack merupakan serangan yang berusaha untuk mengelabui *node-node* pada jaringan. Untuk melancarkan aksinya, *Sybil attack* mengambil identitas node yang ada pada jaringan. Dengan identitas tersebut, maka *node* penyerang dapat bertindak seolah-olah merupakan bagian dari jaringan tersebut dan berusaha untuk mendapatkan perlakuan yang sama seperti *node* yang memiliki identitas yang dicurinya.



AODV	16.1975	16.0749	16.5636	16.5636	16.3297	16.3041
DSR	16.404	16.1384	16.7325	16.2867	16.5966	16.1505

Grafik 4.4 *Average throughput* sebelum dan sesudah *sybil attack* pada 20 *node*

Dari hasil ini dapat disimpulkan bahwa protokol DSR mengalami penurunan average throughput akibat sybil attack lebih besar dibandingkan dengan yang dialami AODV. Hal ini disebabkan oleh jumlah paket data yang mampu dikirmkan DSR jauh lebih sedikit dibandingkan sebelum adanya sybil attack. Penurunan throughput ini diiringi dengan penigkatan routing overhead pada DSR. Artinya, DSR berusaha ntuk mengirimkan paket datanya tiba di pengirima secara kesuluruhan.

Selain itu, semakin banyak jumlah node di dalam jaringan maka akan semakin menurunkan performansi DSR untuk menghandle node-nodenya. Keadaan semakin sulit dnegan kecepatan node yang tinggi. semakin tinggi kecepatan node, maka semakin sering terjadi link failure dan cache memory node juga akan sulit untuk menstabilkan routing tabelnya. Akibatnya, DSR harus melakukan route discovery ulang untuk mengirimkan paket datanya.

5. Penutup

5.1. Kesimpulan

1. *Active attack* menurunkan performansi jaringan dengan penurunan *packet delivery ratio* terbesar yaitu 16,4242% terjadi pada *sybil attack* menggunakan protokol AODV dengan jumlah *node* 15 dan kecepatan 25 m/s , penurunan *average delay* paling besar terjadi pada *rushing attack* dengan menggunakan AODV pada 20 *node* dan kecepan 15 m/s sebesar 2968,3354 ms, penurunan *throughput* terbesar terjadi pada *sybil attack* pada protokol DSR sebesar 5.4949 Kbps di 20 *node* dengan kecepatan 20 m/s dan penurunan *routing overhead* paling besar terjadi pada *replay attack* dengan protokol AODV sebesar 243.1667% dengan 15 *node* pada kecepatan 25 m/s.
2. Karena adanya penurunan performansi akibat *active attack*, maka penanganan untuk *rushing attack* terbaik menggunakan protocol DSR dengan jumlah *node* 20 dan kecepatan 25 m/s karena penurunan throughput sebesar 0,648% , *sinkhole attack* dapat dihadapi dengan menggunakan protokol DSR dengan 10 *node* dan kecepatan 15 m/s karena dapat mempertahankan *packet delivery ratio*nya, *replay attack* dapat dihadapi dengan menggunakan protokol DSR tanpa ada penurunan *delay* dengan kecepatan 20 m/s pada 20 *node*, dan *sybil attack* dihadapi dengan protokol AODV dengan kecepatan 20 m/s pada 20 *node* dengan tanpa penurunan *routing overhead*.

5.2. Saran

1. Serangan dilakukan dengan skala *node* yang lebih besar
2. Pengiriman paket data dengan *transport agent* TCP dan *background traffic*
3. Adanya variasi paket data yang dikirimkan

DAFTAR PUSTAKA

[1] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Detection of Sinkhole Attack inWirelessSensor Networks", Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia

[2] Alfarizi, Faizal. 2011. Analisis Pengaruh Mobilitas *Node* Terhadap Performansi Jaringan Manet Menggunakan *Routing Protocol* OLSR Dan DSDV. Bandung : IT Telkom.

[3] Arif, Faizal. 2011. Analisis Performansi Protokol *Routing* DSDV, AODV, dan DSR pada MANET terhadap Model Pergerakan Manhattan Grid. Bandung : IT Telkom.

[4] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security *Attack*s in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology Vol 1, 5 June 2012

[5] Gajendra Singh Chandel, Rajul Chowksi, "Study of Rushing Attack in MANET" International Journal of Computer Application, Vol 79, No. 10, October 2013

[6] Gandhewar, Nisarg., Sheikh, Rahila. 2012. Performance Valuation of AODV Under Sinkhole Attack In MANET Using NS2. Jerman: Lambert Academic Publishing

[7] Ganesh Reddy, www.wirelessnetworksecurity11.blogspot.com/rushing-attack.html diakses pada tanggal 3 Januari 2014

[8] Immanuel John Raja Jebadurai, Elijah Blessing Rajsingh, "A Survey on Sinkhole Attack Detection Methods in Mobile Ad-hoc Network", 3rd International Conference on Mechine Learning and Computing, Vol. 4, 2011

[9] Jane Zhen, Sampalli Srinivas, "Preventing Replay Attacks for Secure Routing in Ad Hoc Networks", pp. 140-150, Springer-Verlag Berlin Heideberg 2003

[10] Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj, "Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET", International Journal of Engineering Research and Application, Vol 3, Issue 2, March-April 2013

[11] Mr. Hepi kumar, R. Khirasariya, "Simulation Study of Jellyfish Attack in MANET (Mobile Ad hoc Network) Usind AODV Routing Protocol" Journal of Information, Knowledge and Research in Computer Engineering, Vol 02, Issue 02, October 2013

[12] Ms. Sonal R. Jathe, Prof.D.M. Dakhane, "Detection of Sinkhole Attack against DSR Protocol MANET", Iternational Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 4, April 2012

[13] Pratama, Fajar Wahyu. 2011. Analisis dan Implementasi Algoritma Modifikasi *Ad-hoc On Demand Distance Vector* (AODV) untuk Mengatasi *Blackhole Attack* dan *Wormhole Attack* pada *Mobile Ad-hoc Network* (MANET). Bandung : IT Telkom.

[14] Priyanka Goyal, Vinti Parmar, Rahul Rishi, " MANET : Vulnerabilities, Challenges, *Attack*s, Applicatio" International Journal of Computational Engineering & Management, Vol 11, January 2011

[15] Satyam Shrivastava, "Rushing Attack and Its Prevention Technique", International Journal of Application or Innovation in Engineering & Management, Vol 2, April 2013

[16] Shaohe Lv, Xiaodong Wang, Xin Zhao, Xingming Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Network", International Conference on Computational Intelligence and Security", IEEE 2008

[17] Sinaga, Handico Christian. 2011. Analisis Perbandingan Performansi *Reactive Routing* protokol AODV dan DSR pada Jaringan *Ad hoc*. Bandung : IT Telkom

[18] Sohail Abbas, Madjid Merabti, David Liewellyn-Jones, Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE System Journal, Vol 7, No 2, June 2013

[19] S Sharmila, G Umamaeshwari, "Energy and Hop based Detection of Sybil attack for Mobile Wireless Sensor Networks", International Journal of Emerging Technology and Advanced Engineering, Vol 4, Issue 4, February 2014

[20] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" In Proceedings of the ACM Workshop on Wireless Security (WiSe), San Diego, California, USA, September 19,2003,pp. 30-40

[21] Zolidah Kasiran, Juliza Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", IEEE 2014