Jurnal Riset Inovasi Bidang Informatika Dan Pendidikan Informatika (KERNEL)
Vol. 2, No. 1, Agustus 2021
ISSN: 774-4345

IMPLEMENTASI METODE IDSAODV UNTUK MENDETEKSI SERANGAN *BLACK HOLE* PADA JARINGAN MANET

Charles Blanov Hasudungan Pakpahan[1)], Siti Agustini[2)]

[1]Jurusan Teknik Informatika, Fakultas Teknik Elektro dan Teknologi Informasi

[2]Jurusan Sistem Komputer, Fakultas Teknik Elektro dan Teknologi Informasi

Institut Teknologi Adhi Tama Surabaya

ABSTRACT

MANET is a group of nodes that form a unit and send packets to other nodes. However, in terms of security, MANET is very vulnerable to various kinds of attacks. A black hole attack is a type of attack on a network that can absorb network traffic and drop it. The way a black hole attack works is to pretend it has fresh enough routes to all destinations requested by all nodes and absorb all network traffic. When the source node broadcasts an RREQ message for the destination node, the black hole node will immediately respond with an RREP message containing the highest sequence number information and this message is considered as if it came from the destination node or from a node that has a fresh enough route to the destination node. IDSAODV is a routing protocol that is used to minimize the effects of black holes. The IDSAODV protocol will check the RREP packet from the black hole node for the minimum path to the destination and the maximum destination sequence number. The IDSAODV protocol will discard the first RREP packet coming from the black hole node and select the second RREP packet coming from the destination node. In this study, a black hole attack trial will be conducted on the MANET environment with a number of nodes as many as 100, 110, 120, 130, 140, and 150 using the AODV and IDSAODV routing protocols. From this experiment, it was found that the highest increase in Packet Delivery Ratio (PDR) was 47.36%, throughput increased by 156.78 Kbps and End-to-End Delay decreased by 27.62 ms.

Article History

Received 2021-07-16
Revised 2021-07-23
Accepted 2021-07-31

Key words

IDSAODV
AODV
Black Hole
MANET

ABSTRAK

MANET adalah sekelompok node yang membentuk kesatuan dan mengirim paket kepada node yang lain. Namun dari segi keamanan, MANET sangat rentan terhadap berbagai macam serangan. Serangan black hole merupakan jenis serangan pada jaringan yang dapat menyerap network traffic dan menjatuhkannya. Cara kerja dari serangan black hole adalah dengan berpura-pura memiliki rute yang cukup fresh ke semua tujuan yang diminta oleh semua node dan menyerap semua network traffic. Saat node sumber melakukan broadcast pesan RREQ untuk node tujuan, node black hole akan segera merespon dengan pesan RREP yang berisi informasi sequence number tertinggi dan pesan ini dianggap seolah-olah datang dari node tujuan atau dari node yang memiliki rute yang cukup fresh ke node tujuan. IDSAODV merupakan suatu routing protokol yang digunakan untuk meminimalisir efek dari black hole. Protokol IDSAODV akan memeriksa paket RREP dari node black hole untuk jalur minimum ke tujuan dan maksimum sequence number tujuan. Protokol IDSAODV akan membuang paket RREP pertama yang datang dari node black hole dan memilih paket RREP kedua yang datang dari node tujuan. Pada penelitian ini akan dilakukan uji coba serangan black hole pada lingkungan MANET dengan jumlah node sebanyak 100, 110, 120, 130, 140, dan 150 dengan menggunakan routing protokol AODV dan IDSAODV. Dari percobaan tersebut didapatkan hasil peningkatan Packet Delivery Ratio (PDR) paling tinggi sebesar 47,36%, peningkatan Throughput sebesar 156,78 Kbps dan penurunan End-to-End Delay sebesar 27,62 ms.

PENDAHULUAN

Mobile Ad Hoc Network (MANET) adalah sekelompok node yang membentuk kesatuan dan mengirim paket kepada node yang lain. MANET adalah sebuah jaringan yang dapat memperluas jangkauan transmisi nirkabel terbatas dengan penerusan paket multi-hop, jadi MANET sangat cocok untuk skenario dimana bantuan infrastruktur tidak dibutuhkan [1]. Namun dari segi keamanan, MANET sangat rentan terhadap berbagai macam serangan mulai dari penyadapan, peniruan, interfensi, dan *Denial of Service* [2]. *Denial of Service* adalah kondisi dimana satu atau

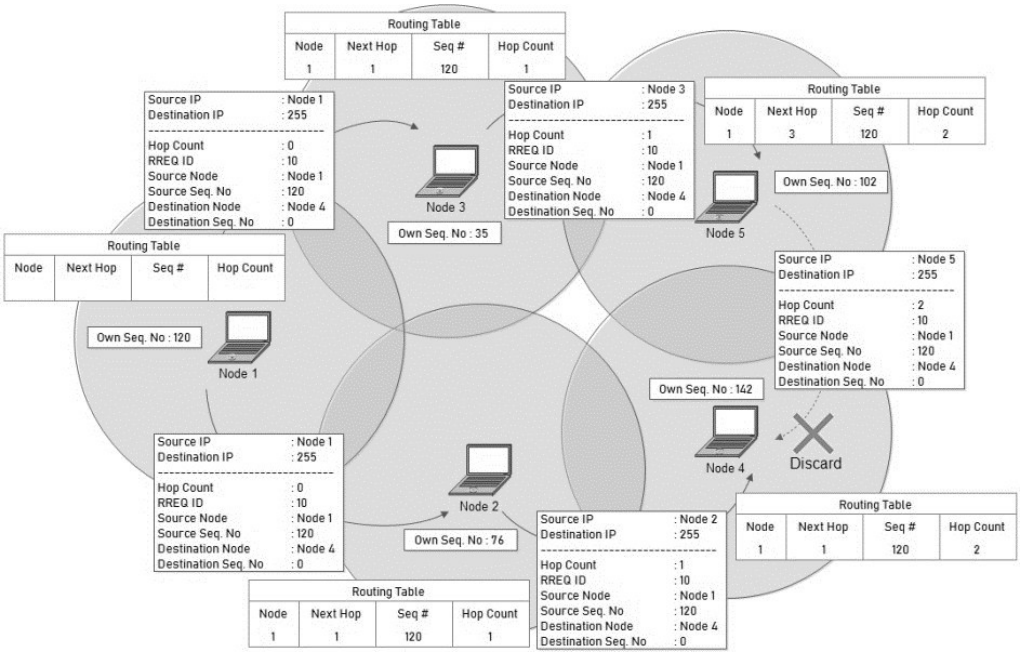
lebih *node* dalam jaringan MANET dapat melakukan serangan tanpa dapat terdeteksi terlebih dahulu. Salah satu jenis dari serangan DoS adalah serangan *black hole,* dimana node akan berpura-pura memiliki *route* yang cukup *fresh* ke semua tujuan yang diminta oleh semua node dan menyerap *network traffic* [3].

Metode IDSAODV merupakan salah satu metode yang datpat digunakan untuk mendeteksi node berbahaya (*black hole*). Pada metode ini, pesan RREP pertama digunakan untuk menginisiasi data transfer tapi jika pesan RREP kedua sampai ke *node* sumber maka akan dialihkan ke *route* yang baru [3]. Pada penelitian kali ini permasalahan yang ingin diselesaikan bagaimana cara mendeteksi serangan DOS pada MANET khususnya serangan *black hole*, metode yang akan digunakan adalah IDSAODV. Pada penelitian ini, akan dilakukan pengujian beberapa skenario dan akan dievaluasi.

TINJAUAN PUSTAKA

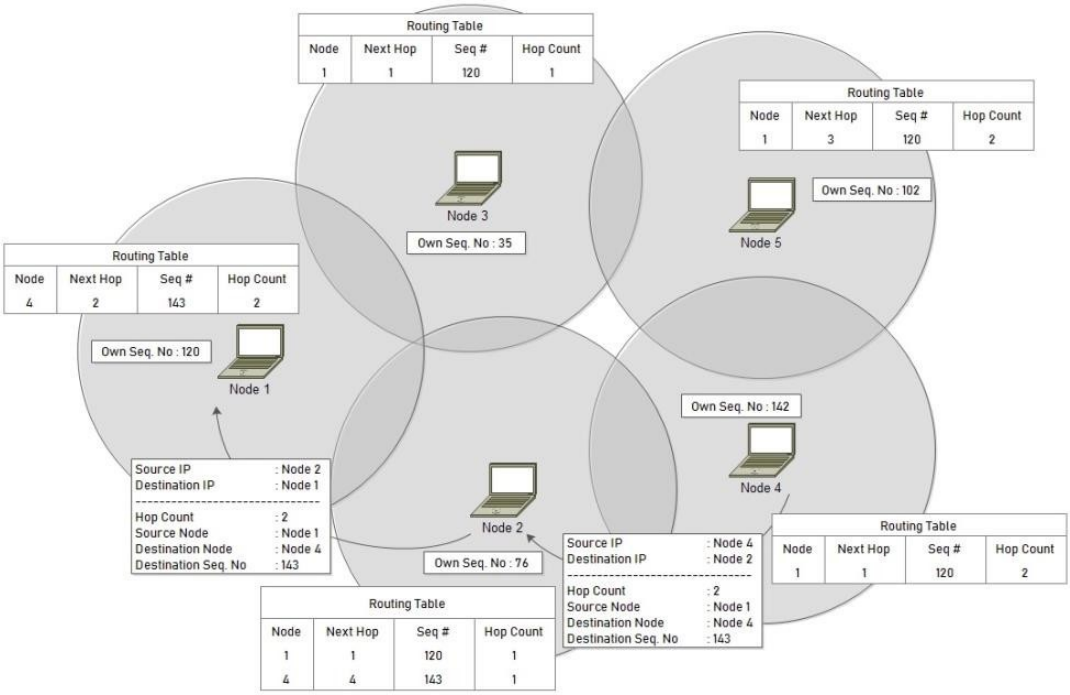
Ad-Hoc On-demand Distance Vector Routing (AODV)

Ad-Hoc On-demand Distance Vector Routing (AODV) adalah jenis routing protokol *on demand* yang digunakan untuk mencari rute antara node sumber dan node tujuan. Routing ini menggunakan pesan seperti *Route Request* (RREQ) dan *Route Reply* (RREP) untuk membangun rute dari node sumber menuju node tujuan [4]. Saat node sumber ingin membuat koneksi dengan node tujuan, node sumber akan melakukan *broadcast* pesan RREQ, seperti yang dapat dilihat pada Gambar 1. Pesan RREQ ini akan disebarkan oleh node sumber, dan akan diterima oleh node tetangga (node perantara) dari node sumber. Node perantara melakukan *broadcast* RREQ ke node tetangganya. Proses ini terus berjalan sampai paket diterima oleh node tujuan atau node perantara yang memiliki *route entry* yang cukup *fresh* untuk node tujuan di dalam tabel *routing*. Cukup *fresh* maksudnya adalah node perantara memiliki rute yang valid ke node tujuan yang *sequence number* tersebut setidaknya sama besar dengan yang terdapat dalam pesan RREQ. Selama paket RREQ melakukan perjalanan melalui jaringan, setiap node perantara meningkatkan *hop count* sebanyak satu. Jika pesan RREQ dengan ID RREQ yang sama diterima, node secara diam-diam membuang RREQ yang baru diterima, mengontrol *ID field* dari pesan RREQ. Ketika node tujuan atau node perantara yang memiliki rute yang cukup *fresh* ke node tujuan menerima pesan RREQ, mereka membuat pesan RREP dan memperbarui tabel routing mereka dengan *hop count* terakumulasi dan *sequence number* dari node tujuan. Setelah itu pesan RREP dikirm ke node sumber [5].



Gambar 1. Penyebaran pesan RREQ pada AODV

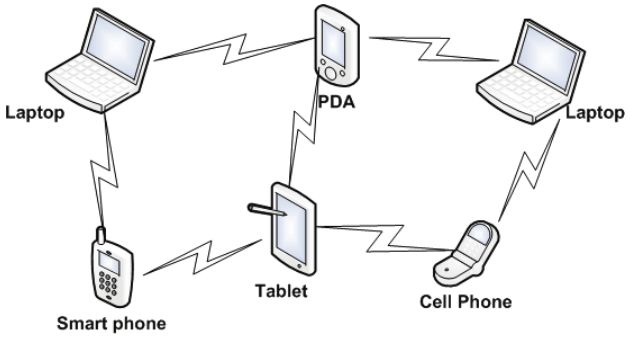
Sementara pesan RREQ dan RREP diteruskan oleh node perantara, node perantara memperbarui tabel routingnya dan menyimpan entri route ini selama 3 detik, yang merupakan nilai konstan *ACTIVE_ROUTE_TIMEOUT* dari protokol AODV. Dengan demikian node mengetahui tetangga mana yang harus dijangkau di 23 tujuan. Dalam terminologi, daftar tetangga untuk tujuan diberi label sebagai "*Precursor List*". Pengiriman RREP dan bagaimana entri route di node perantara diperbarui dapat dilihat pada Gambar 2.



Gambar 2. Pengiriman pesan RREP pada AODV

Mobile Ad-Hoc Network (MANET)

Jaringan MANET adalah kumpulan node nirkabel yang dapat bergerak secara acak di mana saja dan kapan saja tanpa infrastruktur apa pun. Karena jaringan MANET bebas dari infrastruktur tetap, beberapa keuntungan menggunakan jaringan MANET adalah mengurangi biaya dan waktu penerapan [6].



Gambar 3. Jaringan MANET

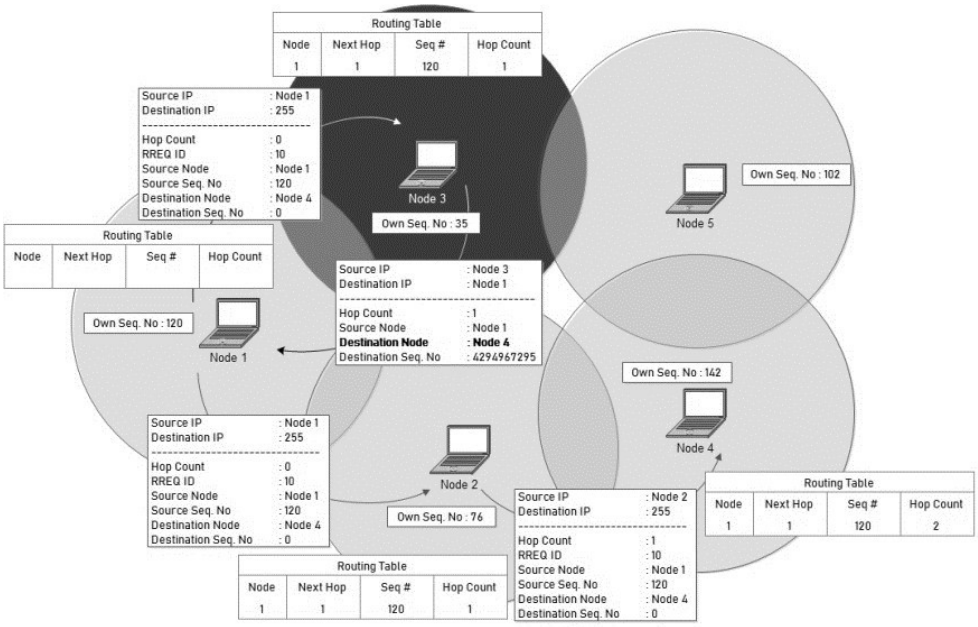
Pada Gambar 3 adalah contoh dari penerapan jaringan MANET yang dibentuk dari kumpulan perangkat *mobile* seperti *smart phone*. Perangkat *mobile* seperti ponsel harus mampu mendeteksi keberadaan perangkat lain disekitarnya dan melakukan pengaturan yang dibutuhkan untuk melakukan komunikasi dan berbagi data. MANET memungkinkan perangkat untuk tetap mempertahankan koneksi ke jaringan serta dapat dengan mudah menambahkan atau menghapus

perangkat pada jaringan. Karena node pada MANET yang pergerakannya dinamis membuat topologi jaringan pada MANET dapat berubah dengan cepat dan tidak terduga dari waktu ke waktu. Jaringan MANET memiliki sifat desentralisasi, yang berarti organisasi jaringan dan pengiriman pesan harus dijalankan oleh node itu sendiri [7]. Karakteristik dan kompleksitas MANET [8] diantaranya adalah :

1. Jaringan topologi dinamis
2. Menggunakan *multi-hop routing*
3. Energi dan *bandwidth* yang terbatas
4. Keterbatasan keamanan
5. Melakukan pembangunan serta pengaturan jaringan secara mandiri.

Serangan Black Hole

Di dalam serangan *black hole* pada jaringan MANET, protokol routing digunakan menyatakan dirinya ke node perantara lainnya sebagai node yang memiliki rute terpendek ke node tujuan [9]. Setelah menerima pesan RREQ dari node, node *black hole* dapat memalsukan pesan RREP seolah-olah memiliki rute yang cukup fresh ke node tujuan. Untuk menekan pesan RREP lain yang asli yang mungkin diterima oleh node sumber dari node lain, penyerang dapat memalsukan pesan RREP palsu dengan meningkatkan sequence number tujuan [10].



Gambar 4. Ilustrasi serangan Black Hole

Pada Gambar 4, diasumsikan node 3 adalah node berbahaya. Saat node 1 menyebarkan pesan RREQ untuk node 4, node 3 segera merespon ke node 1 dengan pesan RREP yang memuat nilai *sequence number* tertinggi dari node 4, seolah-olah berasal dari node 4. Node 1 mengasumsikan bahwa Node 4 berada di belakang Node 3 dengan 1 hop dan membuang paket RREP yang baru diterima berasal dari Node 2. Setelah itu Node 1 mulai mengirimkan paket datanya ke node 3 dan percaya bahwa paket-paket ini akan mencapai Node 4 tetapi Node 3 akan menjatuhkan semua paket data.

IDSAODV

IDSAODV merupakan suatu routing protokol yang digunakan untuk meminimalisir efek dari black hole dan untuk meningkatkan *Packet Delivery Ratio* (PDR) [3]. Karena node *black hole* mengirim sebuah pesan RREP tanpa memeriksa tabel, kemungkinan besar pesan RREP yang

datang pertama kali berasal dari node black hole. IDSAODV akan melakukan pengecekan paket RREP dari node black hole untuk jalur minimum menuju node tujuan dan maksimum *sequence number* tujuan. Protokol IDSAODV akan membuang paket RREP pertama yang datang dari node black hole dan memilih paket RREP kedua yang datang dari node tujuan. Protokol IDSAODV akan memilih jalur lain yang menuju node tujuan, selain jalur yang mengarah ke node black hole.

METODE

Pada perancangan routing protokol IDSAODV ini, akan diimplementasikan dengan cara yang hampir sama seperti saat membuat serangan *black hole*, yaitu dengan mengcloning routing AODV dan diganti namanya menjadi IDSAODV beserta file-file yang ada didalamnya seperti aodv.cc dan aodv.h.

Karena node *black hole* mengirim pesan RREP tanpa memeriksa tabel, kemungkinan besar pesan RREP pertama berasal dari node *black hole*. Protokol IDSAODV akan memeriksa paket RREP dari node *black hole* untuk jalur minimum ke tujuan dan maksimum *sequence number* tujuan. Protokol IDSAODV akan membuang paket RREP pertama yang datang dari node *black hole* dan memilih paket RREP kedua yang datang dari node tujuan. Protokol IDSAODV akan memilih jalur lain yang menuju node tujuan, selain jalur yang mengarah ke node *black hole*.

Untuk mengimplementasi routing protokol IDSAODV akan dilakukan modifikasi pada fungsi penerimaan pesan RREP (recvReply) dan membuat mekanisme *caching* RREP untuk memeriksa pesan RREP dari node *black hole* seperti pada Gambar 5 dan Gambar 6.

```
void
idsAODV::rrep_insert(nsaddr_t id) {
	idsBroadcastRREP *r = new idsBroadcastRREP(id);

	assert(r);
	r->expire = CURRENT_TIME + BCAST_ID_SAVE;
	r->count ++;
	LIST_INSERT_HEAD(&rrephead, r, link);
}
idsBroadcastRREP *
idsAODV::rrep_lookup(nsaddr_t id) {
	idsBroadcastRREP *r = rrephead.lh_first;
	for( ; r; r = r->link.le_next) {
		if (r->dst == id)
			return r;
	}
	return NULL;
}
void
idsAODV::rrep_remove(nsaddr_t id) {
	idsBroadcastRREP *r = rrephead.lh_first;

	for( ; r; r = r->link.le_next) {
		if (r->dst == id)
			LIST_REMOVE(r,link);
		delete r;
		break;
	}
}
void
idsAODV::rrep_purge() {
	idsBroadcastRREP *r = rrephead.lh_first;
	idsBroadcastRREP *rn;
	double now = CURRENT_TIME;

	for(; r; r = rn) {
		rn = r->link.le_next;
		if(r->expire <= now) {
			LIST_REMOVE(r,link);
			delete r;
		}
	}
}
```

Gambar 5. Mekanisme caching RREP pada IDSAODV

```
void
idsAODV::recvReply(Packet *p) {
idsBroadcastRREP *r = rrep_lookup(rp->rp_dst);

if (ih->daddr() == index) {
        if (r == NULL) {
             count = 0;
             rrep_insert(rp->rp_dst);
      } else {
             r->count++;
             count = r->count;
      }
}

          UPDATE ROUTE TABLE

      } else {
           Forward(p);
      }
}
```

Gambar 6. Fungsi "recvReply" pada IDSAODV

HASIL DAN PEMBAHASAN

Packet Delivery Ratio (PDR)

Rasio paket data yang dibawa sampai ke tujuan yang dibuat menggunakan sumber *Constant Bitrate* (CBR). Packet Delivery Ratio (PDR) menunjukkan cara protokol melakukan pengiriman dengan sukses dari pengirim ke penerima. Nilai yang lebih tinggi meningkatkan hasil. Packet Delivery Ratio (PDR) didapatkan dari hasil perhitungan seperti pada contoh persamaan 1.

$$\text{PDR} = \frac{\sum \textit{paket yang diterima}}{\sum \textit{paket yang terkirim}} \times 100\% \quad (1)$$

Berikut ini adalah hasil kenaikan PDR yang terjadi pada percobaan serangan black hole pada routing protokol IDSAODV:

Tabel 1. Perubahan PDR 1 Black Hole

No.	Jumlah Node	Kenaikan PDR
1	100	20.03%
2	110	47.36%
3	120	12.81%
4	130	25.99%
5	140	9.05%
6	150	19.74%

Tabel 2. Perubahan PDR 2 Black Hole

No.	Jumlah Node	Kenaikan PDR
1	100	13.50%
2	110	12.62%
3	120	18.49%
4	130	12.13%
5	140	22.19%
6	150	38.38%

Tabel 3. Perubahan PDR 3 Black Hole

No.	Jumlah Node	Kenaikan PDR
1	100	12.43%
2	110	37.79%
3	120	19.27%
4	130	12.70%
5	140	32.33%
6	150	32.45%

Sehingga dengan menggunakan metode routing protokol IDSAODV didapatkan hasil kenaikan PDR dengan kenaikan paling rendah adalah 9.05% dan kenaikan paling tinggi adalah 47.36% dengan skenario jumlah *black hole* 1, 2, 3 dan jumlah node 100, 110, 120, 130, 140 dan 150.

Throughput

Jumlah paket yang melewati *channel* dalam satuan waktu tertentu. Metrik kinerja ini menunjukkan jumlah total paket yang telah dibawa secara efektif dari sumber ke tujuan, dan dapat ditingkatkan kecepatannya. Throughput didapatkan dari hasil perhitungan seperti pada contoh persamaan 2.

$$\text{Throughput} = \frac{\sum ukuran\ paket\ data\ yang\ diterima}{waktu\ simulasi} \quad (2)$$

Berikut ini adalah hasil kenaikan Throughput yang terjadi pada percobaan serangan black hole pada routing protokol IDSAODV:

Tabel 4. Perubahan Throughput 1 Black Hole

No.	Jumlah Node	Kenaikan Throughput
1	100	50.75 Kbps
2	110	104.65 Kbps
3	120	67.27 Kbps
4	130	-37.4 Kbps
5	140	-5.16 Kbps
6	150	24.84 Kbps

Tabel 5. Perubahan Throughput 2 Black Hole

No.	Jumlah Node	Kenaikan Throughput
1	100	10.89 Kbps
2	110	156.78 Kbps
3	120	94.53 Kbps
4	130	17.89 Kbps
5	140	50.27 Kbps
6	150	-3.09 Kbps

Tabel 6. Perubahan Throughput 3 Black Hole

No.	Jumlah Node	Kenaikan Throughput
1	100	-125.35 Kbps
2	110	18.29 Kbps
3	120	84.67 Kbps
4	130	25.47 Kbps
5	140	145.02 Kbps
6	150	45.99 Kbps

Sehingga dengan menggunakan metode routing protokol IDSAODV didapatkan hasil kenaikan Throughput dengan kenaikan paling rendah adalah -125.35 Kbps dan kenaikan paling tinggi adalah

156.78 Kbps dengan skenario jumlah *black hole* 1, 2, 3 dan jumlah node 100, 110, 120, 130, 140 dan 150.

End-to-End Delay

Metrik kinerja ini digunakan untuk menghitung selisih waktu pengiriman tiap paket data sampai paket data tersebut berhasil diterima dan dirata-rata terhadap waktu pengamatan. End-to-End Delay didapatkan dari hasil perhitungan seperti pada contoh persamaan 3.

$$\text{End-to-End Delay} = \sum(waktu\ terima - waktu\ kirim) \quad (3)$$

Berikut ini adalah hasil penurunan End-to-End Delay yang terjadi pada percobaan serangan black hole pada routing protokol IDSAODV:

Tabel 7. Perubahan End-to-End Delay 1 Black Hole

No.	Jumlah Node	Penurunan End-to-End Delay
1	100	-0.31 ms
2	110	0.64 ms
3	120	2.33 ms
4	130	6.89 ms
5	140	-0.93 ms
6	150	21.22 ms

Tabel 8. Perubahan End-to-End Delay 2 Black Hole

No.	Jumlah Node	Penurunan End-to-End Delay
1	100	12.55 ms
2	110	0.85 ms
3	120	13.65 ms
4	130	27.62 ms
5	140	14.08 ms
6	150	18.8 ms

Tabel 9. Perubahan End-to-End Delay 3 Black Hole

No.	Jumlah Node	Penurunan End-to-End Delay
1	100	-0.74 ms
2	110	17.42 ms
3	120	2.73 ms
4	130	17.37 ms
5	140	26.89 ms
6	150	4.38 ms

Sehingga dengan menggunakan metode routing protokol IDSAODV didapatkan hasil penurunan End-to-End Delay dengan penurunan paling rendah adalah -0.93 ms dan penurunan paling tinggi adalah 27.62 ms dengan skenario jumlah *black hole* 1, 2, 3 dan jumlah node 100, 110, 120, 130, 140 dan 150.

KESIMPULAN

Kesimpulan yang dapat diambil dari hasi pengujian dan analisis pada penelitian ini adalah sebagai berikut :

1. Dari hasil uji coba dapat disimpulkan bahwa setelah adanya metode routing IDSAODV, nilai PDR dapat meningkat saat adanya serangan *black hole* dibandingkan

dengan saat menggunakan routing AODV dengan kenaikan nilai PDR sebesar 47.36% (diambil dari nilai tertinggi).

2. Untuk nilai Throughput dan End-to-End Delay dari hasil uji coba setelah adanya metode routing IDSAODV, nilainya tidak semua mengalami kenaikan. Untuk nilai throughput mengalami kenaikan sebesar 156.78 Kbps (diambil dari nilai tertinggi). Sedangkan untuk nilai End-to-End Delay mengalami penurunan sebesar 27.62 ms (diambil dari nilai tertinggi).

DAFTAR PUSTAKA

[1] A. Dorri and S. R. Kamel, "Security Challenges in Mobile Ad Hoc Networks: A Survey," *Int. J. Comput. Sci. Eng. Surv.*, vol. 6, no. 1, pp. 15–29, 2015, doi: 10.5121/ijcses.2015.6102.

[2] J. Sen, M. Girish Chandra, S. G. Harihara, H. Reddy, and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile ad hoc networks," *2007 6th Int. Conf. Information, Commun. Signal Process. ICICS*, pp. 0–4, 2007, doi: 10.1109/ICICS.2007.4449664.

[3] S. Dokurer, Y. M. Erten, and C. E. Acar, "Performance analysis of ad-hoc networks under black hole attacks," *Conf. Proc. - IEEE SOUTHEASTCON*, pp. 148–153, 2007, doi: 10.1109/SECON.2007.342872.

[4] C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," 1999.

[5] C. E. Perkins, S. R. Das, and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," pp. 167–169, 2003.

[6] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," *J. Commun. Netw.*, vol. 3, no. 3, pp. 60–66, 2004.

[7] P. Rohal, R. Dahiya, and P. Dahiya, "Study and Analysis of Throughput, Delay and Packet Delivery Ratio in Manet Based DSR Routing Protocols," *Int. J. Adv. Res. Eng. Technol.*, vol. 1, no. 2, 2013.

[8] S. S. Suradkar and A. R. Surve, "A Protocol for Reducing Routing Overhead in Mobile Ad Hoc Networks," *Int. J. Comput. Sci. Eng. Technol.*, vol. 5, no. 02, pp. 115–117, 2014.

[9] S. Dixit, K. K. Joshi, and N. Joshi, "A Review: Black Hole and Gray Hole Attack in MANET," *Int. J. Futur. Gener. Commun. Netw.*, vol. 8, no. 4, pp. 287–294, 2015, doi: 10.14257/ijfgcn.2015.8.4.28.

[10] Usha and Bose, "Comparing the impact of black hole and gray hole attacks in mobile adhoc networks," *J. Comput. Sci.*, vol. 8, no. 11, pp. 1788–1802, 2012, doi: 10.3844/jcssp.2012.1788.1802.