BAB 4
HASIL DAN PEMBAHASAN

Pada bab ini penulis membahas hasil yang didapatkan dari simulasi jaringan kemudian di jalankan hingga selesai. Hasil yang diamati adalah parameter QoS yang sudah ditentukan yaitu *throughput, delay*, dan *packet delivery ratio*. Pengujian ini bertujuan mengetahui kinerja jaringan VANET setelah terkena serangan *blackhole*. Pada pengujian tersebut penulis menggunakan dua skenario yang akan dijelaskan pada sub bab berikut :

4.1 Skenario 1

4.1.1 *Throughput* perbandingan jumlah *node*

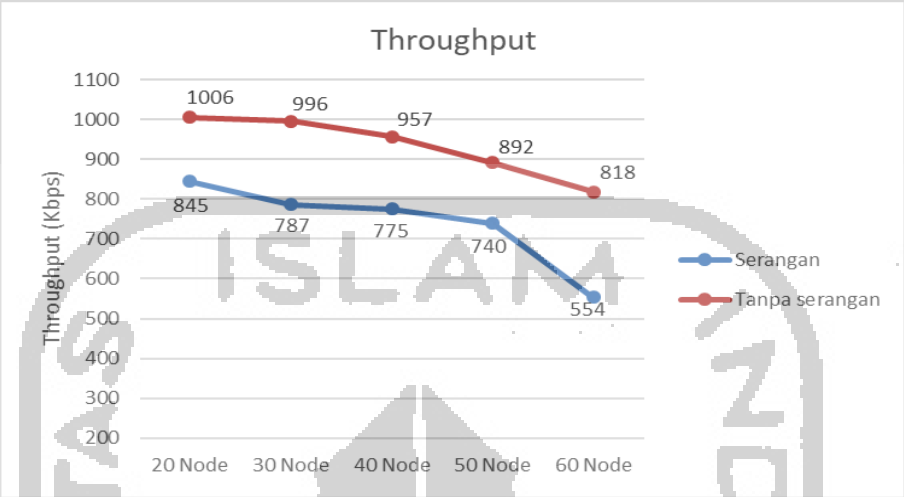
Pada setiap perubahan jumlah *node* saat sebelum dan sesudah terkena serangan nilai *throughput* mengalami penurunan seperti terdapat pada Tabel 4.1 berikut ini :

Tabel 4.1 Rata-rata *throughput*

Jumlah *node*	Sebelum serangan	Sesudah serangan	penurunan *throughput*
20 *node*	1006 Kbps	845 Kbps	161 Kbps
30 *node*	996 Kbps	787 Kbps	209 Kbps
40 *node*	957 Kbps	775 Kbps	182 Kbps
50 *node*	892 Kbps	740 Kbps	152 Kbps
60 *node*	818 Kbps	554 Kbps	264 Kbps

Hasil dari pengamatan *throughput* yang diperoleh *simulator* terlihat pada Gambar 4.1 dengan membandingkan saat sebelum dan sesudah terkena serangan *blackhole* dimana pada setiap *node* menggunakan kecepatan yang konstan yaitu 70km/jam. Pada saat menggunakan 20 *node* normal menghasilkan *throughput* sebesar 1.006 Kbps dan setelah *node* normal diberikan serangan hasil *throughput* menjadi 845 Kbps, kemudian jumlah *node* dirubah menjadi 30 *node* menghasilkan 996 Kbps dan setelah *node* normal diberi serangan hasil *throughput* menjadi 787 Kbps, selanjutnya jumlah *node* menjadi 40 hasil *throughput* yang diperoleh 957 Kbps dan setelah diberikan serangan mengalami penurunan yaitu 775 Kbps, selanjutnya jumlah *node* ditambah menjadi 50 hasil *throughput* yang diperoleh 892 Kbps sedangkan saat terkena serangan menjadi

740 Kbps, kemudian penulis menambah jumlah *node* normal menjadi 60 hasil *throughput* yang diperoleh adalah 818 Kbps dan setelah *node* normal diberi serangan nilai *throughput* menurun menjadi 554 Kbps



Gambar 4.1 *Throughput* jumlah *node*

Dari hasil perbandingan sebelum dan sesudah terkena serangan *blackhole* maka dapat di simpulkan bahwa nilai *throughput* seiring perubahan jumlah *node* saat sebelum terkena serangan *blackhole* nilai *throughput* menurun, hal tersebut disebabkan banyaknya *node* yang berada pada lingkungan tersebut membuat *traffic* jaringan semakin sibuk sehingga proses pengiriman dan penerimaan paket kurang ditangani dengan baik. *Throughput* yang dihasilkan setelah terkena serangan *blackhole* semakin menurun, hal tersebut dikarenakan *node blackhole* menjatuhkan setiap ada paket yang melewatinya, jatuhnya paket terjadi dimana peningkatan jumlah *node* mengakibatkan kemacetan jaringan sehingga banyak paket yang dijatuhkan karena tabrakan data pada jaringan.

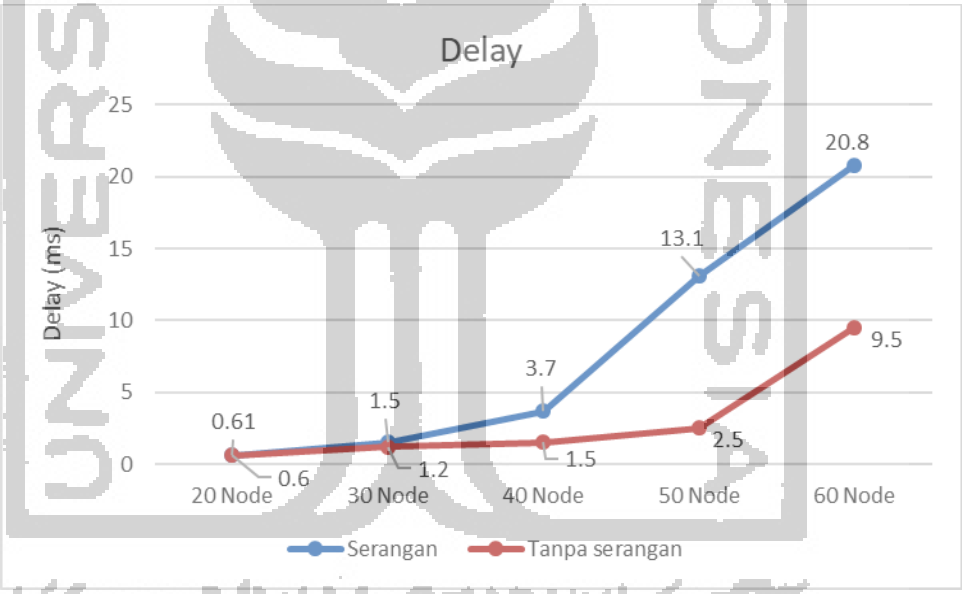
4.1.2 *Delay* perubahan jumlah *node*

Hasil dari pengamatan *delay* yang didapatkan dari *simulator* yang terlihat pada Tabel 4.2. Pada saat kondisi normal menggunakan 20 *node* menghasilkan 0,6 ms, namun saat terkena serangan *blackhole, delay* meningkat menjadi 0,61 ms. Kemudian penambahan jumlah *node* menjadi 30 menghasilkan 1,2 ms setelah terkena serangan *blackhole, delay* meningkat menjadi 1,5 ms. Selanjutnya penulis menambah jumlah *node* menjadi 40 menghasilkan *delay* sebesar 1,5 ms dan setelah diberi *node blackhole delay* menjadi 3,7 ms. Pada saat penulis menambah jumlah *node* menjadi 50 menghasilkan nilai *delay* sebesar 2,5 ms dan setelah diberi *node blackhole, delay* menjadi 13,1 ms. Kemudian untuk melihat apakah nilai *delay* bertambah maka penulis menambahkan 60 *node* yang menghasilkan 9,5 ms dan setelah diberi *node blackhole, delay*

menjadi 20,8 ms dimana mengalami peningkatan *delay* sebesar 11,3 ms. Pada setiap perubahan jumlah *node* saat sebelum dan sesudah terkena serangan, nilai *delay* mengalami peningkatan seperti terdapat pada Tabel 4.2 berikut ini :

Tabel 4.2 Rata-rata *delay*

Jumlah *node*	**Sebelum serangan**	**Sesudah serangan**	**peningkatan *delay***
20 *node*	0,6 ms	0,61 ms	0,01 ms
30 *node*	1,2 ms	1,5 ms	0,3 ms
40 *node*	1,5 ms	3,7 ms	2,2 ms
50 *node*	2,5 ms	13,1 ms	10,6 ms
60 *node*	9,5 ms	20,8 ms	11,3 ms



Gambar 4.2 *Delay* jumlah *node*

Dari hasil perbandingan penambahan jumlah *node* saat sebelum terkena serangan *blackhole*, *delay* meningkat karena padatnya jumlah *node* sehingga pengiriman data secara terus menerus mengakitbatkan data bertumpuk membuat *node* bingung untuk menerima informasi. Setelah terkena serangan *delay* semakin besar dikarenakan *routing* AODV membutuhkan waktu yang lama dalam proses pencarian jalur, dimana AODV mengacu kepada karakteristik *routing* reaktif yang tidak selalu memperbaharui tabel *routing* secara berkala. ketika salah satu *node* yang menggunakan *routing protocol* AODV maka *node* tersebut akan menanggapi seluruh RREQ yang

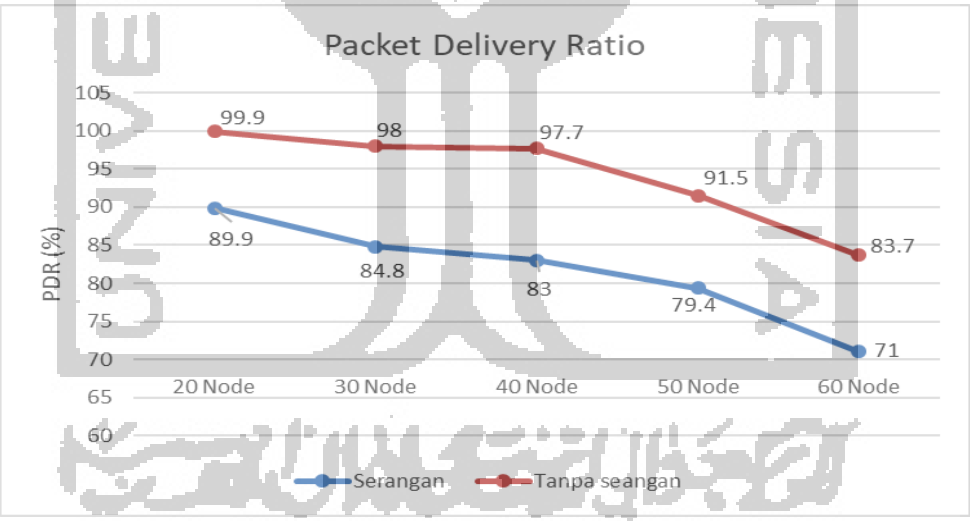
diterima, sehingga mengakibatkan kemacetan pada proses pencarian rute [20]. Selain itu *delay* meningkat disebabkan karena kecepatan data yang tinggi sedangkan mobiltas rendah.

4.1.3 PDR perubahan jumlah *node*

Pada setiap perubahan jumlah *node* saat sebelum dan sesudah terkena serangan, nilai *packet delivery ratio* mengalami penurunan seperti terdapat pada Tabel 4.3 berikut ini :

Tabel 4.3 Rata-rata *PDR*

Jumlah *node*	Sebelum serangan	Sesudah serangan	penurunan PDR
20 *node*	99,9 %	89,9 %	10 %
30 *node*	98 %	84,8 %	13,2 %
40 *node*	97,7 %	83 %	14,7 %
50 *node*	91,5 %	79,4 %	12,1 %
60 *node*	83,7 %	71 %	12,7 %



Gambar 4. 3 *packet delivery ratio* jumlah *node*

Hasil pengamatan *packet delivery ratio* yang didapatkan dari *simulator* terlihat pada Gambar 4.3. Pada kondisi normal dengan menggunakan 20 *node* nilai PDR 99,9% dengan diberi *node* serangan nilai PDR menjadi 89,9%. Percobaan kedua menggunakan 30 *node* menghasilkan PDR 98% dan saat diberi *node* serangan nilai PDR menjadi 84,8%. Percobaan ketiga menggunakan 40 *node* dimana menghasilkan nilai PDR 97,7% kemudian diberikan *node* serangan nilai PDR menjadi 83%. Kemudian penulis menambah jumlah *node* menjadi 50 menghasilkan nilai PDR 91,5% dengan diberikan *node* serangan nilai PDR menjadi 79,4%. Selanjutnya penulis

menambahkan kembali jumlah *node* menjadi 60 dimana nilai PDR 83,7% lalu diberikan *node* serangan menjadi 71% dimana penambahan jumlah *node* mengakibatkan penurunan nilai PDR sebesar 12,7%.

Dari hasil perbandingan sebelum dan sesudah terkena serangan *blackhole* dapat disimpulkan bahwa dengan penambahan jumlah *node* saat kondisi normal PDR mengalami penurunan, hal tersebut dipengaruhi oleh nilai *throughput* apabila *throughput* menurun maka PDR juga menurun. Dimana *throughput* adalah kecepatan transfer data dalam proses pengiriman paket apabila kecepatan tersebut melambat maka jumlah paket yang dikirim dan diterima juga semakin sedikit yang diperoleh. Setelah terkena serangan *blackhole* nilai PDR semakin menurun, hal ini disebabkan padatnya pengguna jaringan yang menimbulkan perebutan paket sehingga data yang dikirim dan diterima mengalami kemacetan.

4.2 Skenario 2

4.2.1 *Throughput* perubahan kecepatan

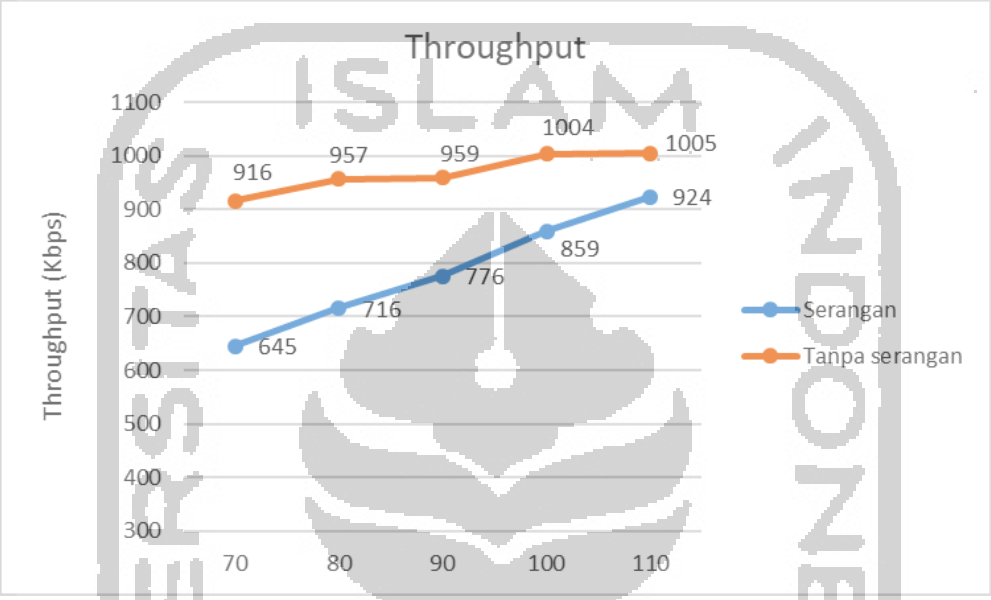
Setiap perubahan kecepatan *node* saat sebelum dan sesudah terkena serangan, nilai *throughput* mengalami penurunan seperti terdapat pada Tabel 4.4 berikut ini :

Tabel 4.4 Rata-rata *throughput*

Kecepatan *node*	Sebelum serangan	Sesudah serangan	Penurunan *throughput*
70 km/h	916 Kbps	645 Kbps	271 Kbps
80 km/h	957 Kbps	716 Kbps	241 Kbps
90 km/h	959 Kbps	776 Kbps	183 Kbps
100 km/h	1004 Kbps	859 Kbps	145 Kbps
110 km/h	1005 Kbps	924 Kbps	81 Kbps

Pada penelitian *throughput* menggunakan *simulator* dapat dilihat pada Gambar 4.4 dengan membandingkan saat sebelum dan sesudah terkena serangan *blackhole* dimana pada setiap perubahan kecepatan mengunakan *node* yang konstan yaitu 40 *node*. Percobaan pertama penulis menggunakan kecepatan 70 km/jam dengan kondisi normal menghasilkan *throughput* 916 Kbps kemudian diberikan *node* serangan nilai *throughput* menjadi 645 Kbps. Percobaan kedua merubah kecepatan yaitu 80 km/jam dengan kondisi normal menghasilkan 957 Kbps saat diberi *node*

serangan *throughput* menjadi 716 Kbps. Percobaan ketiga merubah kecepatan *node* yaitu 90 km/jam dengan kondisi normal menghasilkan *throughput* 959 Kbps kemudian diberi *node* serangan *throughput* menjadi 776 Kbps. Kemudian penulis merubah kecepatan *node* menjadi 100 km/jam dengan kondisi normal menghasilkan 1.004 Kbps dengan diberikan node serangan *throughput* menjadi 859 Kbps. Kemudian penulis merubah kecepatan *node* menjadi 110 km/jam dimana menghasilkan 1.005 Kbps kemudian diberi *node* serangan nilai *throughput* menjadi 924 Kbps.



Gambar 4. 4 Gambar 4.5 *Throughput* perubahan kecepatan *node*

Dari hasil perbandingan kecepatan *node* pada saat sebelum terkena serangan dapat disimpulkan bahwa nilai *throughput* sebelum terkena serangan *blackhole*, *throughput* mengalami peningkatan untuk setiap perubahan kecepatan, disebabkan dengan meningkatkan kecepatan maka kemungkinan *node* satu dengan *node* lain akan sering berpapasan dalam satu zona sehingga proses pengiriman paket lebih cepat [21]. Pada saat sesudah terkena serangan nilai *throughput* menurun karena dengan meningkatkan kecepatan mengakibatkan semakin cepat paket yang melewati *blackhole* maka semakin banyak paket rute yang dijatuhkan sehingga proses *transfer* data dari *node* ke *node* lainnya terganggu.

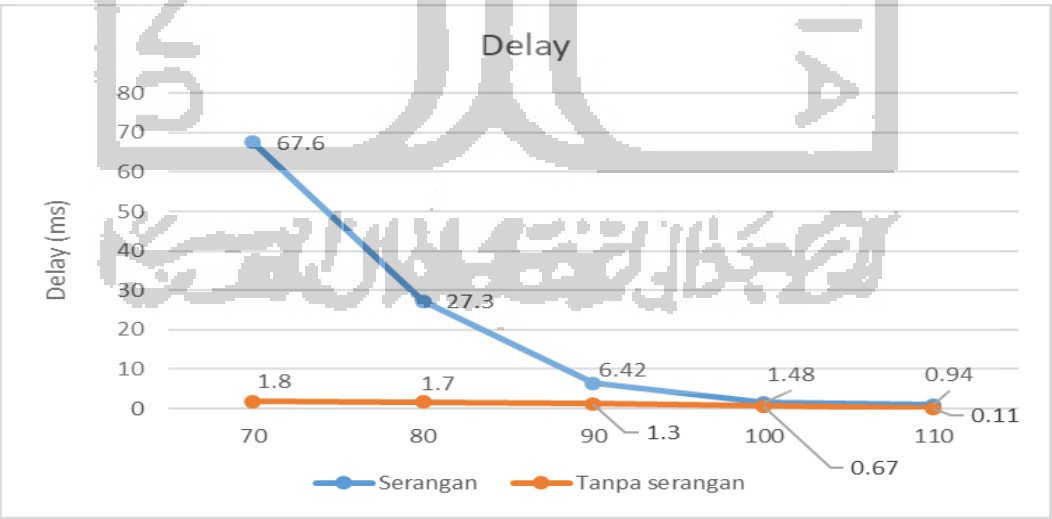
4.2.2 *Delay* perubahan kecepatan

Pada perubahan kecepatan *node* setelah terkena serangan nilai *delay* mengalami peningkatan seperti terdapat pada Tabel 4.5 berikut ini :

Tabel 4.5 Rata-rata *delay*

Kecepatan *node*	Sebelum serangan	Sesudah serangan	Peningkatan *delay*
70 km/h	1,8 ms	67,6 ms	65,8 ms
80 km/h	1,7 ms	27,3 ms	25,6 ms
90 km/h	1,3 ms	6,42 ms	5,12 ms
100 km/h	0,67 ms	1,48 ms	0,81 ms
110 km/h	0,11 ms	0,94 ms	0,83 ms

Pada penelitian d*elay* menggunakan *simulator* terlihat pada Gambar 4.5 melakukan perbandingan saat sebelum dan setelah terkena serangan dimana pada setiap perubahan kecepatan menggunakan *node* yang konstan yaitu 40. Pada percobaan pertama menggunakan kecepatan 70 km/jam dimana pada kondisi normal *delay* yang diperoleh yaitu 1,8 ms dengan adanya *node blackhole delay* menjadi 67,6 ms. Percobaan kedua penulis merubah kecepatan *node* menjadi 80 km/jam pada kondisi normal *delay* yang didapatkan 1,7 ms kemudian saat diberi *node blackhole delay* menjadi 27,3 ms. Percobaan ketiga dengan kecepatan 90 km/jam pada kondisi normal *delay* 1,3 ms dan saat diberi *node blackhole delay* menjadi 6,42 ms. Pada kecepatan 100 dan 110 km/jam *delay* mengalami penurunan pada kondisi normal dan kondisi terkena serangan *blackhole* sebesar 0,83%.



Gambar 4.6 *Delay* perubahan kecepatan *node*

Hasil yang diperoleh dari simulasi dapat disimpulkan bahwa saat sebelum terkena serangan *blackhole* Seiring perubahan kecepatan nilai *delay* megalami penurunan, hal ini terjadi karena dengan meningkatkan kecepatan kendaraan kemungkinan *node* satu dengan *node* lain akan sering

berpapasan dalam satu zona sehingga proses pengiriman data sampai ke tujuan menjadi lebih cepat, dan *delay* menjadi lebih kecil [10]. Ketika terkena serangan nilai *delay* lebih besar dari kondisi normal hal ini terjadi akibat *blackhole* melakukan pembuangan data sehingga paket tidak sampai kepada *node* tujuan sepenuhnya, karena hal tersebut membuat routing AODV akan terus berulang memastikan jalur tersedia dan meminta *node* sumber mengirim paket hingga sampai ke tujuan.

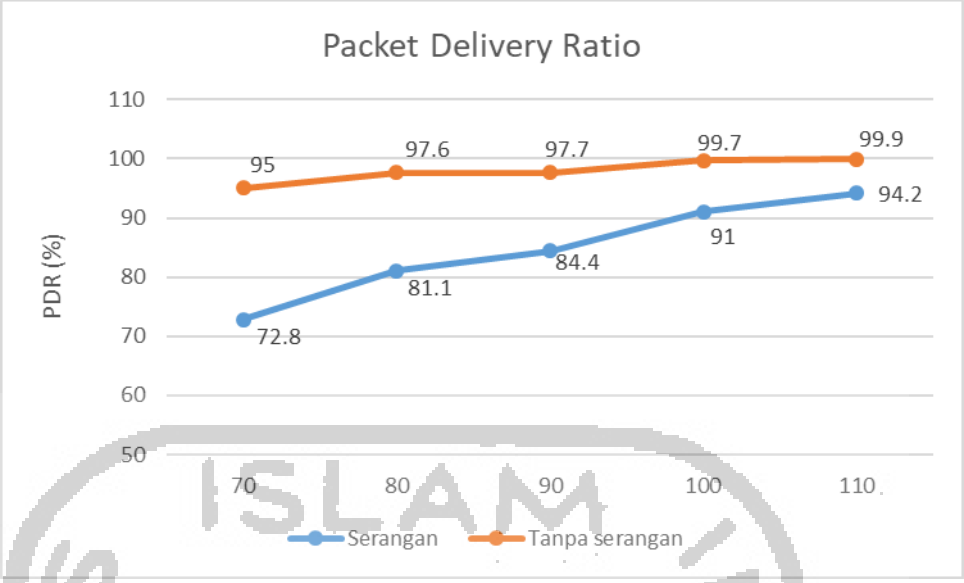
4.2.3 PDR perubahan kecepatan

Pada setiap perubahan kecepatan *node* nilai *packet delivery ratio* mengalami penurunan seperti terdapat pada Tabel 4.6 berikut ini :

Tabel 4.6 Rata-rata *PDR*

Kecepatan *node*	**Sebelum serangan**	**Sesudah serangan**	**penurunan PDR**
70 km/h	95 %	72,8 %	22,2 %
80 km/h	97,6 %	81,1 %	16,5 %
90 km/h	97,7 %	84,4 %	22,2 %
100 km/h	99,7 %	91 %	22,2 %
110 km/h	99,9 %	94,2 %	22,2 %

Pada penelitian *packet delivery ratio* menggunakan *simulator* terlihat pada Gambar 4.6 melakukan perbandingkan sebelum dan sesudah terkena serangan *blackhole* dimana menggunakan jumlah *node* yang konstan yaitu 40 *node*. Pada percobaan pertama penulis menggunakan kecepatan awal yaitu 70 km/jam dengan kondisi normal menghasilkan nilai PDR 95% kemudian diberi *node blackhole* nilai PDR menjadi 72,8%. Percobaan kedua menggunakan kecepatan 80 km/jam dalam kondisi normal nilai PDR diperoleh 97,6% dan saat diberi *node blackhole* nilai PDR menjadi 81,1%. Percobaan ketiga penulis merubah kecepatan *node* menjadi 90 km/jam pada kondisi normal nilai PDR yang diproleh 97,7% dengan diberikan *node blackhole* PDR menghasilkan 84,4%. kemudian pada percobaan perubahan kecepatan 100 dan 110 km/jam pada kondisi normal menghasilkan 99,7% dan 99,9% dan setelah diberikan *node blackhole* nilai PDR mengalami penurunan menjadi 91% dan 94,2%.



Gambar 4.7 *Packet delivery ratio* perubahan kecepatan *node*

Dari hasil simulasi perubahan kecepatan dapat disimpulkan bahwa kondisi saat sebelum terkena serangan *blackhole* nilai PDR mengalami peningkatan, hal ini dipengaruhi oleh nilai *throughput* dimana *throughput* meningkat maka nilai PDR juga meningkat dimana *throughput* adalah kecepatan *transfer* data dalam proses pengiriman paket apabila kecepatan tersebut semakin besar maka jumlah paket yang dikirim dan diterima juga semakin besar. Dimana AODV memiliki karakteristik mengirimkan hello paket ke *node* tetangga memastikan bahwa jalur tersedia apabila paket tidak terkirim maka AODV meminta *node* sumber untuk mengirim ulang hingga sampai ke *node* tujuan. Setelah terkena serangan nilai PDR menurun disebabkan *blackhole* menjatuhkan setiap paket yang melewatinya, pemutusan tautan antar *node* komunikasi lebih cepat dan sering terjadi sehingga paket belum mengirimkan data tetapi tautan telah terputus sebelumnya.

Penelitian ini diperoleh selisih pada kondisi sebelum dan sesudah terkena serangan dengan dua skenario menambah jumlah *node* dan variasi kecepatan. Hasil tersebut guna mempermudah penelitian selanjutnya untuk menambah data dan informasi yang ingin mengembangkan dampak serangan *blackhole* pada sistem jaringan VANET, seperti mitigasi serangan *blackhole.* Penggunaan dua skenario tersebut untuk mengetahui berapa jumlah *node* yang dapat meminimalisir serangan *blackhole* dan berapa kecepatan *node* yang digunakan untuk mencegah serangan *blackhole*.