Simulasi Serangan Black Hole Pada Jaringan MANET Menggunakan NS-3

Alfi Syahri Nuzula
Jurusan Teknik Informatika
Fakultas Teknologi Industri, Universitas Islam Indonesia
D.I Yogyakarta, Indonesia
alfisyahrinuzula@gmail.com

Yudi Prayudi
Pusat Studi Forensika Digital Teknik Informatika
Fakultas Teknologi Industri, Universitas Islam Indonesia
D.I Yogyakarta
prayudi@uii.ac.id

***Abstract*— Black hole attack adalah suatu serangan yang terjadi di jaringan Mobile AdHoc Network (MANET), yang akan mengganggu proses pengiriman paket dari node pengirim ke node tujuan. Black hole masuk ke jaringan dan bertindak layaknya node normal lainnya, dan dapat menjadi rute pengiriman paket oleh node pengirim. Namun ketika paket yang dikirimkan sampai ke dirinya, paket tersebut akan dihapus dan tidak akan pernah sampai ke node tujuannya. Penelitian ini akan membahas bagaimana pengaruh black hole terhadap kualitas jaringan yang diserangnya dengan meneliti beberapa parameter Quality of Service (QoS) yaitu throughput, delay dan packet loss. Penelitian dilakukan dengan cara membuat simulasi jaringan menggunakan aplikasi Network Simulator 3 (NS-3). Pengujian dilakukan dengan menggunakan beberapa skenario simulasi, yaitu skenario 4, 20, dan 50 node dengan 1 dan 2 node black hole. Dari hasil analisa beberapa parameter QoS yang telah diujikan, diketahui bahwa black hole mempengaruhi penurunan kualitas jaringan yang diserangnya. Tetapi semakin padat node black hole, pengaruh black hole dapat sedikit berkurang, karena rute pengiriman paket bergantung pada routing table node pengirim, yang mana semakin padat node dalam jaringan, maka semakin banyak pilihan rute yang dapat digunakan node pengirim untuk mengirimkan paketnya.**

Keywords—MANET; AODV; Black Hole attack; Network Simulator 3;

I. PENDAHULUAN

Alasan keamanan saat melakukan proses transmisi data pada jaringan komputer menjadi hal penting yang perlu diperhatikan pada jaringan MANET karena jaringan MANET lebih rentan terhadap serangan. Salah satu contohnya adalah serangan black hole. Black hole adalah serangan pada MANET yang akan mendrop semua paket yang dikirimkan oleh node sender. Node black hole mengadvertise dirinya sebagai node yang memiliki rute tempuh paling pendek untuk menuju node receiver, sehingga node sender akan mengirimkan paketnya melalui node black hole. Ketika paket sampai ke node black hole, paket tersebut tidak di teruskan ke node selanjutnya akan tetapi paket tersebut di drop dan tidak akan sampai ke node receiver. Hal ini akan sangat berbahaya jika paket yang dikirimkan berisi informasi penting atau informasi yang urgent. Untuk itu diperlukan upaya pencegahan agar paket yang kita kirimkan tidak terjebak ke dalam node black hole. Penelitian ini akan membahas bagaimana serangan black hole bekerja pada jaringan MANET dan mensimulasikannya menggunakan Network Simulator 3 (NS-3). Penelitian ini diharapkan agar bisa menjadi upaya antisipasi agar jaringan MANET tidak terkena serangan black hole, sehingga dapat mengurangi kerugian yang akan didapatkan jika terkena serangan black hole.

II. LANDASAN TEORI

A. MANET

Mobile adhoc Network (MANET) adalah jaringan nirkabel yang terdiri dari beberapa node yang bersifat *mobile* sehingga dapat membentuk topologi yang berbeda-beda. Jaringan MANET tidak membutuhkan infrastruktur, tiap-tiap perangkat dapat bertindak seperti *router* yang dalam hal ini akan disebut dengan "node", sehingga jaringan MANET cocok untuk digunakan pada wilayah yang sedang terkena bencana alam, konflik militer dan kondisi darurat lainnya [1]. MANET memiliki beberapa karakteristik seperti berikut ini:

- Multiple Wireless link: Setiap node mampu saling berhubungan dengan node lainnya.
- Limited Resource: Jaringan MANET memiliki daya dan kapasitas memori yang terbatas.
- Dynamic Topology: Tiap-tiap node bersifat mobile, sehingga topologi jaringan yang terbentuk dapat berubah-ubah sesuai dengan jumlah node dan pergerakkannya.
- Low Security: Jaringan MANET menggunakan gelombang radio untuk saling menghubungkan antar node sehingga keamanan dalam jaringan MANET rendah [2].

B. AODV

Adhoc On-Demand Distance Vector(AODV) adalah salah satu *routing protocol* yang bersifat reaktif. AODV akan menyimpan *path* dan rute node pada tiap-tiap nodenya. Ketika terdapat node yang ingin mengirim paket namun tidak ada rutenya pada *routing table*, maka node tersebut akan melakukan *route discovery*. Node asal akan melakukan *broadcast* paket *route request* (RREQ) yang berisi alamat node tujuan ke seluruh node yang ada disekitarnya. Selain berisi alamat node tujuan, paket ini juga berisi alamat node asal, nomer urut rute, dan urutan paling akhir nomor node tujuan berada. Ketika node tujuan menerima paket RREQ dari node

asal, node tujuan akan membalasnya dengan mengirimkan paket *route replay* (RREP). Node tujuan mengirimkan paket RREP dengan mengikuti kebalikan dari *path* yang dihasilkan oleh paket RREQ sebelumnya. Setelah node asal menerima paket RREP yang dikirimkan oleh node tujuan, kedua node menambahkan rute di *routing table* dengan RREP ke node tujuannya. Kemudian node asal mengirimkan paket ke node tujuan dengan memilih rute yang melewati node paling sedikit.[3].

C. Black Hole

Black hole adalah suatu node yang menyerang node-node lain dalam suatu jaringan. Node black hole bergerak secara acak dan akan menggangu proses pengiriman paket pada node lainnya. Node black hole bertindak menyerupai node-node normal lainnya, sehingga node lainnya menganggap node black hole aman dan normal. Padahal node ini akan mengganggu proses pengiriman paket yang ada di jaringan tersebut. Ketika node asal mengirimkan RREQ untuk mencari rute ke node tujuan, Node black hole akan mengadvertise bahwa dirinya adalah node yang memiliki jalur tercepat untuk menuju node tujuan, sehingga node asal akan menggunakan jalur yang diberikan oleh node black hole dan mengabaikan masukan rute dari node lainnya. setelah node asal mulai mengirimkan paket melalui node black hole, secara diam-diam node black hole akan menghapus paket yang diterimanya. [4]

D. Parameter Kinerja Jaringan

Suatu jaringan dapat dinilai baik dan buruk kualitasnya dari pengukuran kinerja jaringan atau biasa disebut dengan *Quality of Service* (QoS). QoS dapat didefinisikan sebagai suatu pengukuran tentang seberapa baik kualitas suatu jaringan. Kualitas baik buruknya QoS bergantung pada penilaian dari parameter-parameter berikut ini:

- *Throughput*, adalah ukuran laju data aktual per satuan waktu, atau dapat disebut juga dengan ukuran *bandwidth* yang sebenarnya. Perbedaan dengan *bandwidth* adalah, ukuran *bandwidth* bersifat statis, sedangkan ukuran *throughput* bersifat dinamis bergantung dari trafik yang terjadi [5]. Rumus untuk menghitung *throughput* adalah:

$$Throughput = \frac{\text{Ukuran paket diterima}}{\text{Waktu pengiriman paket}}$$

- *Delay*, adalah waktu tunda suatu paket yang disebabkan proses transmisi dari node asal ke node tujuannya. Dalam suatu jaringan *delay* dapat menjadi acuan penilaian kualitas jaringan. Semakin kecil nilai *delay* yang dihasilkan, maka semakin baik jaringan tersebut [5]. *Delay* dapat dipengaruhi oleh beberapa hal, diantaranya jarak antar node asal ke node tujuan, media transmisi, atau bisa juga karena waktu proses yang lama. Rumus untuk menghitung *delay* adalah:

$$Delay = \text{waktu paket diterima} - \text{waktu paket dikirim}$$

- *Packet Loss*, adalah paket yang hilang selama proses transmisi paket dari node asal ke node tujuan. *Packet loss* dapat terjadi karena beberapa hal diantarnya: antrian yang melebihi kapasitas jaringan, node yang bekerja melebihi kapasitas bufer atau memori node yang terbatas, kontrol jaringan yang mengatur jumlah trafik yang mengalir harus sesuai dengan jumlah besaran *bandwidth*, sehingga jika ada besaran trafik yang melebihi kapasitas bandwidth, maka *policing control* akan membuang kelebihan trafik tersebut dan adanya serangan dalam jaringan [6]. Rumus untuk menghitung *packet loss* adalah:

$$Packet\ Loss = \frac{\text{Paket yang dikirim} - \text{Paket yang diterima}}{\text{Paket yang dikirim}} 100\%$$

III. PENELITIAN TERDAHULU

Beberapa penelitian yang membahas tentang black hole yang digunakan sebagai acuan saat mengerjakan penelitian ini diantaranya adalah penelitian yang dilakukan oleh Istas Pratomo dan M Hizrian Hizburrahman, mereka membahas tentang bagaimana mekanisme keamanan untuk mendeteksi keberadaan serangan black hole dan grey hole di *routing protocol* AODV pada jaringan MANET. dalam penelitian tersebut dijelaskan bagaimana cara menemukan keberadaan node berbahaya dan mengisolir node tersebut dari jaringan dengan cara memanfaatkan informasi yang dibawa oleh paket yang berisi informasi mengenai keberadaan node berbahaya yang telah terdeteksi. Pada penelitian tersebut juga dibahas mengenai pengujian beberapa pengaruh parameter terhadap *Throughput*, pengaruh parameter terhadap *delay* dan pengaruh parameter terhadap daya yang digunakan dengan metode *flow control* yang berbeda-beda. Kesimpulan yang bisa didapatkan dari pengujian diatas adalah untuk pengaruh parameter terhadap *throughput*, semakin besar ukuran jaringan, maka nilai *throughput* akan semakin menurun, hal ini disebabkan karena ukuran paket, ukuran *buffer* dan *packet injection rate* yang tetap apabila ukuran jaringan diperbesar, maka waktu yang diperlukan paket untuk mencapai tujuan akan bertambah sehingga menyebabkan nilai *throughput* menurun. Sedangkan untuk pengaruh parameter terhadap delay, *delay* berbanding lurus dengan ukuran jaringan, nilai delay akan meningkat jika ukuran jaringan ditingkatkan. Untuk dapat menurunkan *delay* maka *paket injection rate*, ukuran paket dan ukuran jaringan harus diperkecil dengan ukuran *buffer* yang diperbesar. Sedangkan untuk pengaruh parameter terhadap daya yang digunkan dapat disimpulkan bahwa peningkatan ukuran jaringan akan membawa dampak meningkatnya penggunaan daya pada jaringan. Maka untuk mengurangi penggunaan daya, ukuran paket, ukuran *buffer*, dan ukuran jaringan juga harus diperkecil [7].

Referensi lainnya yang membahas tentang serangan black hole pada jaringan MANET adalah penelitian yang dilakukan oleh Neelam Janak Kumar Patel dan Dr. Khushboo Tripathi. Jurnal internasional penelitian ini terbit pada mei 2017. Penelitian ini menguji jaringan MANET dengan menggunakan 25 node dengan skenario 0 node black hole, 1 node black hole, 3 node black hole dan 5 node black hole dan menggunakan *routing protocol* AODV. Pembahasan hasil pada penelitian ini juga berdasarkan dari pengukuran nilai *throughput*, *delay* dan *packet loss* yang dihasilkan selama simulasi berlangsung. Dalam hasil analisa penelitian ini dijelaskan bahwa nilai

throughput dan *delay* semakin mengecil seiring dengan bertambahnya jumlah node black hole. Hal ini disebabkan karena semakin bertamah banyak node black hole, maka semakin sedikit atau bahka tidak ada paket yang berjala di jaringan tersebut sehingga tidak ada nilai *throughput* dan *delay* yang tercatat dalam simulasi. Hal ini berbanding terbalik dengan nilai *packet loss* yang dihasilkan, semakin banyak node black hole, maka nilai *packet loss* akan semakin tinggi dibandingkan dengan keadaan jaringan normal [8].

IV. PERANCANGAN SIMULASI

Untuk menjalankan simulasi penelitian ini diperlukan beberapa skenario agar diketahui pengaruh black hole pada jaringan MANET. Pada penelitian ini dibuat 6 skenario simulasi. Skenario pertama mengujikan 4 node dengan 1 node black hole, skenario kedua mengujikan 4 node dengan 2 node black hole, skenario ketiga mengujikan 20 node dengan 1 node black hole, skenario keempat mengujikan 20 node dengan 2 node black hole, skenario kelima mengujikan 50 node dengan 1 node black hole, skenario keenam mengujikan 50 node dengan 2 node black hole. Selain skenario simulasi, juga ditentukan parameter-parameter agar pengujian ditiap skenario simulasi tetap dalam kondisi yang sama. Parameter-parameter yang ditetapkan pada penelitian ini seperti pada tabel berikut.

TABEL I. PARAMETER SIMULASI

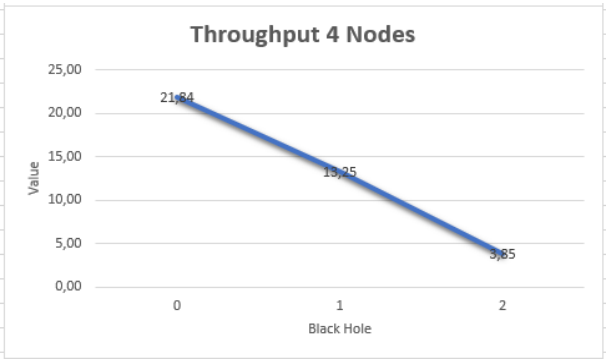
Parameter	Nilai
Routing Protocol	AODV
Tx Power	50
Waktu Simulasi	100 detik
Tipe Pergerakan	Constan position Mobility Model
Tipe Koneksi	UDP
Tipe Wifi Mac	Standart 802.11b
Ukuran Paket	64bytes
Tipe Kanal	Wireless

V. HASIL DAN PEMBAHASAN

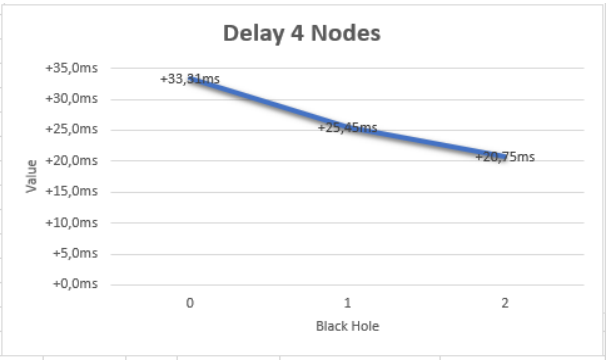
Hasil dari beberapa skenario simulasi diatas akan dianalisa 3 parameter QoS, dengan membagi skenario menjadi 3 kelompok, yaitu kelompok skenario 4 node, kelompok skenario 20 node dan kelompok skenario 50 node. Dalam pembahasan juga akan dibadingkan skenario jaringan yang terserang black hole dengan jaringan normal yang tidak terdapat node black hole. Hal ini dilakukan agar diketahui bagaimana kualitas jaringan berdasarkan paramenter QoS sebelum jaringan terserang serangan black hole dan bagaimana kualitas jaringan sesudah terserang black hole.

A. Skenario 4 Node, Dengan 1 dan 2 Node Black Hole

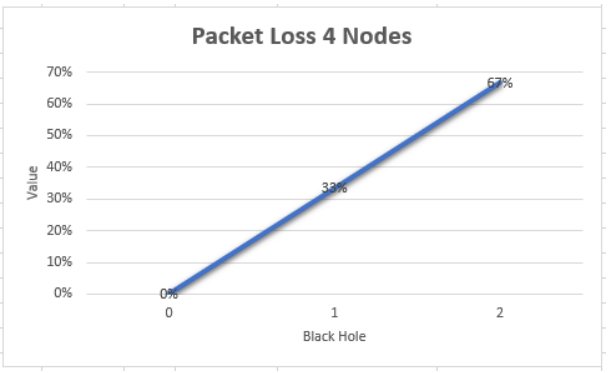
Hasil perhitungan rata-rata *throughput*, *delay* dan *packet loss* pada skenario 4 node dengan 1 dan 2 node black hole dapat dilihat pada gambar 1-3 berikut ini.



Gambar 1. Grafik *throughput* skenario 4 node



Gambar 2. Grafik *delay* skenario 4 node



Gambar 3. Grafik *packet loss* skenario 4 node

Dari grafik pada gambar 1, dapat dilihat nilai rata-rata *throughput*, semakin bertambahnya node black hole, maka nilai *throughput* semakin turun. Rata-rata penurunan *throughput* pada skenario 4 node ini sebesar 12,98 Kbps. Hal ini disebabkan karena node black hole yang menghapus paket data yang dikirimkan dari node asal sehingga semakin sedikit paket data yang bertransmisi dalam jaringan. Nilai yang dihasilkan simulasi juga dapat dipengaruhi karena letak black hole yang berada dekat dengan node sumber, sehingga banyak paket data yang terperangkap ke node black hole.

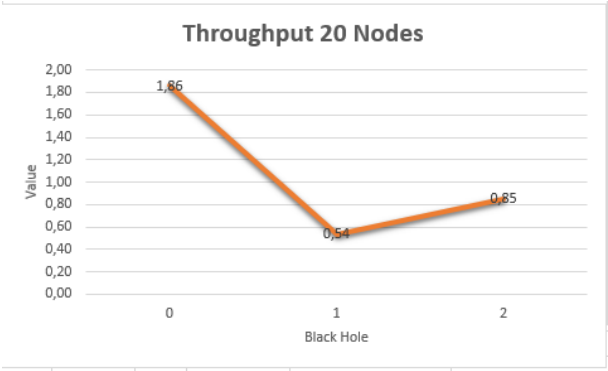
Dari grafik pada gambar 2, dapat dilihat bahwa *delay* yang terjadi semakin menurun dengan semakin banyaknya node black hole yang ada dalam jaringan. Rata-rata penurunan *delay* sebesar +26,5ms. Hal ini terjadi karena pada skenario ini, semakin banyak node black hole maka semakin besar kemungkinan paket yang hilang karena terperangkap node

black hole, sehingga tidak ada paket yang bertransmisi dalam jaringan, membuat tidak ada nilai *delay* yang dihitung dan membuat nilai *delay* semakin menurun.

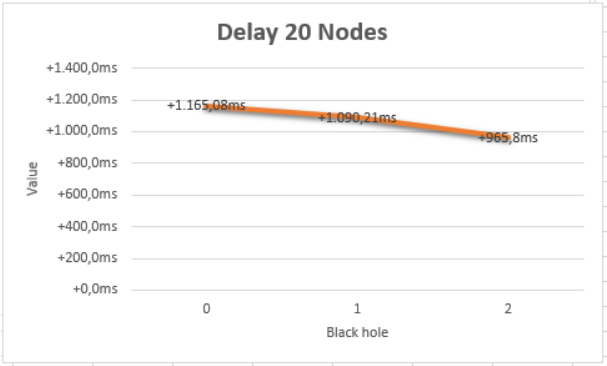
Dari grafik pada gambar 3, persentase terjadinya *packet loss* dalam jaringan skenario 4 node semakin meningkat, berbanding lurus dengan peningkatan jumlah node black hole dalam jaringan.

B. Skenario 20 Node, dengan 1 dan 2 Black Hole

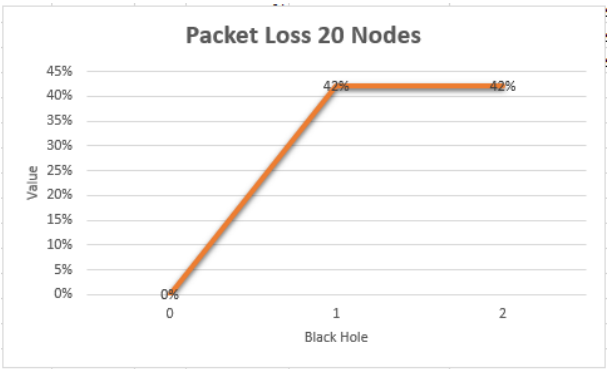
Hasil perhitungan rata-rata throughput, *delay* dan *packet loss* pada skenario 20 node dengan 1 dan 2 node black hole dapat dilihat pada gambar 4-6 berikut ini.



Gambar 4. Grafik *throughput* skenario 20 node



Gambar 5. Grafik *delay* skenario 20 node



Gambar 6. Grafik *packet loss* skenario 20 node

Dari grafik pada gambar 4 dapat dilihat nilai rata-rata *throughput* turun dan naik. Pada skenario ke 3 yang mana terdapat 1 node black hole dan 20 node, nilai *throughput* mengalami penurunan dibandingkan jaringan yang tidak terdapat node black holenya. Tetapi terjadi peningkatan nilai *throughput* pada skenario 2 node black hole, hal ini dapat terjadi karena beberapa faktor, salah satunya pada simulasi skenario 3 letak node black hole yang mempengaruhi *routing table* yang membuat node sumber mengirimkan paket melewati node black hole sebelum sampai ke node tujuan. Sehingga banyak paket yang terperangkap ke node black hole, terutama pada node-node tujuan yang dekat dengan node sumber yang memiliki nilai *throughput* lebih besar daripada node yang letaknya jauh dari node sumber, sehingga sedikit yang bertransmisi pada jaringan tersebut dan membuat rata-rata *throughput* pada skenario ke 3 menjadi rendah.

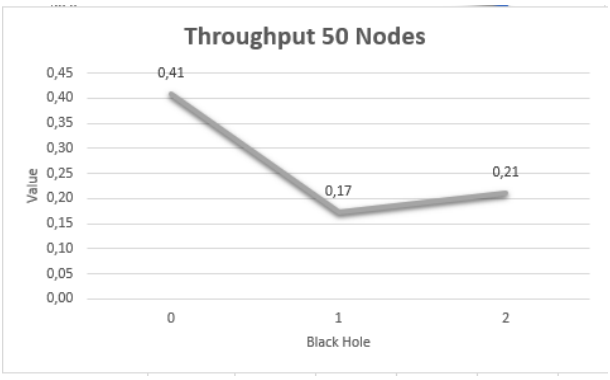
Dibandingkan dengan skenario yang ke 4, walaupun memiliki node black hole yang lebih banyak dari skenario ke 3, tetapi letak node black hole membuat paket yang hilang terjadi pada node-node yang letaknya jauh dari node sumber yang nilai throughputnya tidak besar, sehingga membuat rata-rata nilai *throughput* pada skenario 4 lebih tinggi jika dibandingkan dengan rata-rata *throughput* skenario ke 3. Rata-rata perubahan nilai *throughput* pada skenario 4 node ini sebesar 1,08 Kbps

Dari grafik pada gambar 5, dapat dilihat bahwa rata-rata *delay* yang dihasilkan pada skenario 3 dan 4 semakin menurun. Karena semakin banyak node black hole, semakin banyak paket yang terperangkap dan tidak sampai ke tujuan, sehingga sedikit terjadi proses transmisi paket dalam jaringan yang mengakibatkan tidak ada *delay* yang terjadi pada simulasi jaringan di skenario 3 dan 4. Rata-rata penurunan *delay* yang terjadi pada skenario 3 dan 4 ini adalah +1.073,7ms

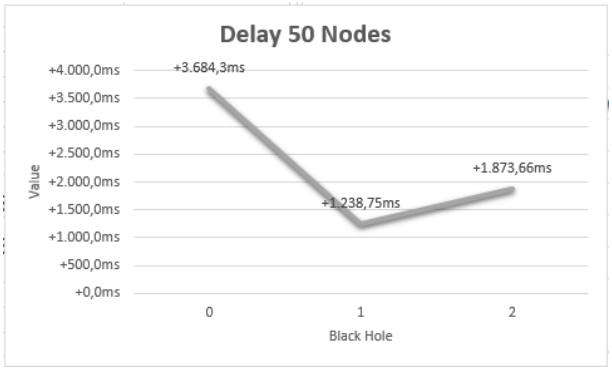
Dari grafik pada gambar 6 menunjukkan bahwa *packet loss* pada simulasi skenario 3 dan 4 sama-sama menunjukkan angka 42%. Tetapi jika dilihat dari tabel hasil simulasi skenario 3 dan 4 yang penulis lampirkan, paket yang hilang atau tidak sampai ke node tujuan, berbeda antara skenario 3 dengan skenario 4.

C. Skenario 50 Node, dengan 1 dan 2 Black Hole

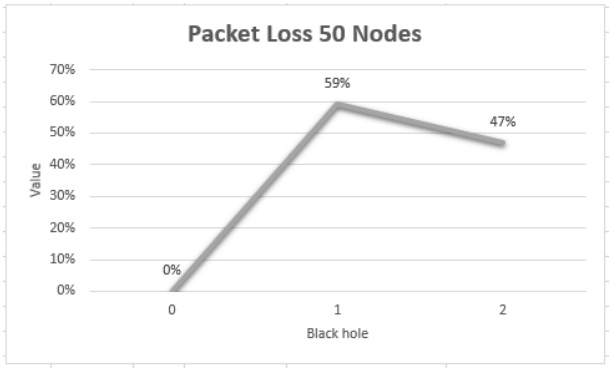
Hasil perhitungan rata-rata *throughput, delay* dan *packet loss* pada skenario 50 node dengan 1 dan 2 node black hole dapat dilihat pada gambar 7-9 berikut ini.



Gambar 7. Grafik *throughput* skenario 50 node



Gambar 8. Grafik *delay* skenario 50 node



Gambar 9. Grafik *packet loss* skenario 50 node

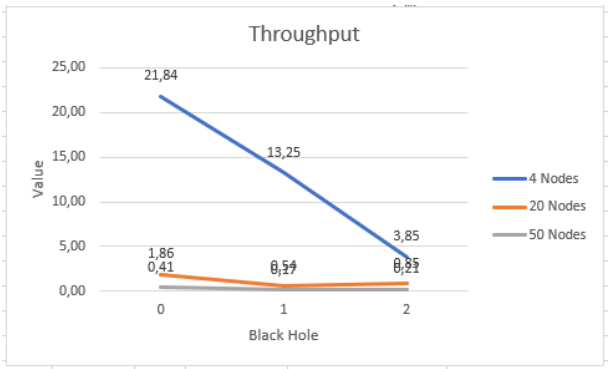
Dari grafik pada gambar 7 dapat dilihat nilai rata-rata *throughput* turun dan naik sama seperti dengan skenario 3 dan 4. Pada skenario ke 5 yang mana terdapat 1 node black hole dan 50 node, nilai *throughput* lebih rendah dibandingkan dengan nilai *throughput* jaringan keadaan normal dan *throughput* skenario 6. Jika dilihat dari tabel hasil simulasi skenario 5 dan 6 yang dilampirkan, node black hole pada skenario 5 lebih banyak menghapus paket data yang ada di jaringan, dibandingkan dengan skenario 6, sehingga rata-rata *throughput* yang dihasilkan lebih rendah daripada rata-rata *throughput* dari skenario 6. Rata-rata perubahan nilai *throughput* pada skenario 5 dan 6 node ini sebesar 0,26 Kbps

Dari grafik pada gambar 8 dapat dilihat bahwa rata-rata *delay* yang dihasilkan pada skenario 5 dan 6 menunjukkan grafik yang menurun menjadi +1.238,75ms, tetapi pada skenario 6 *delay* kembali naik menjadi +1.873,66ms. Jika dilihat di tabel hasil simulasi, black hole pada skenario 5 lebih banyak menghapus paket yang bertransmisi dalam jaringan, terutama paket-paket yang mempunyai tujuan di node-node yang jauh dari node sumber yang pada keadaan normal menghasilkan nilai *delay* yang tinggi, sehingga menghasilkan rata-rata *delay* yang rendah. Sedangkan pada skenario 6, walaupun memiliki node black hole yang lebih banyak dari skenario 5, tetapi paket yang hilang dalam jaringan saat bertransmisi lebih sedikit daripada skenario 5, sehingga membuat rata-rata *delay* yang dihasilkan lebih tinggi daripada skenario 5. Rata-rata perubahan *delay* yang terjadi pada skenario 50 node ini adalah +2.265,57ms.

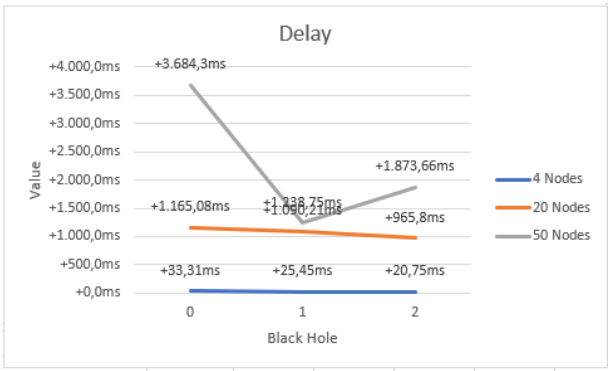
Dari grafik pada gambar 9 menunjukkan bahwa *packet loss* pada simulasi skenario 5, *packet loss* mencapai 59% tetapi pada skenario 6 *packet loss* lebih rendah yaitu 47%. jika dilihat di tabel hasil simulasi yang dilampirkan, paket yang hilang di skenario 5, lebih banyak berada pada node yang jauh dari node sumber.

D. Analisa Hasil Seluruh Skenario

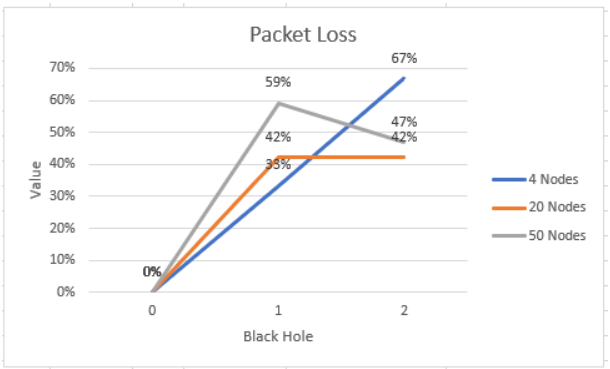
Setelah semua analisa masing -masing skenario dilakukan, maka lakukan analisa seluruh skenario secara bersamaan agar diketahui pengaruh black hole terhadap kualitas jaringan dan kepadatan node dalam jaringan. Hasil dari analisa tersebut dapat dilihat Digambar 10-12 berikut ini.



Gambar 10. Grafik *throughput* seluruh skenario



Gambar 11. Grafik *delay* seluruh skenario



Gambar 12. Grafik *packet loss* seluruh skenario

Dari grafik pada gambar 10 dapat dilihat Banyaknya jumlah node dalam jaringan mempengaruhi besaran *throughput* dalam jaringan tersebut. Semakin padat jumlah node dalam jarinngan, maka semakin kecil *throughput* yang dihasilkan. Untuk pengaruhnya dengan node black hole, dari grafik dapat

dilihat semakin banyak node black hole dalam jaringan tidak selalu akan menurunkan *throughput* seketika, seperti pada skenario simulasi 20 node dan skenario simulasi 50 node. Black hole mempengaruhi *throughput* tergantung dari *routing table* pada node sumber untuk menuju node tujuan dan letak black hole itu sendiri. Jika letak black hole berada dekat dengan node sumber, maka kemungkinan black hole untuk menghapus paket yang dikirimkan node sumber menjadi lebih besar dan membuat rata-rata *throughput* menjadi lebih kecil karena tidak ada nilai *throughput* yang dihitung pada paket yang hilang.

Dari grafik pada gambar 11 di atas dapat disimpulkan *delay* berkebalikan dengan *throughput.* Dalam keadaan normal, semakin banyak node dalam jaringan, maka akan menghasilkan nilai *delay* yang tinggi. Karena sifat dari *routing protocol* AODV yang akan mengirimkan RREQ terlebih dahulu untuk mencari rute ke node tujuan sebelum mengirimkan paket. Untuk pengaruhnya dengan node black hole, hal ini juga bergantung dari letak black holenya, jika letak black hole mampu mempengaruhi *routing table* node sumber untuk mengirimkan banyak paket melalui dirinya, maka nilai *delay* akan semakin rendah dari keadaan normal karena nilai *delay* pada paket yang hilang tidak dapat dihitung.

Dari grafik pada gambar 12 di atas dapat dilihat bahwa banyaknya jumlah node black hole tidak berbanding lurus dengan persentase *packet loss* dalam jaringan. Persentase *packet loss* akan semakin besar bergantung dari topologi jaringan dan *routing table* dari node sumber itu sendiri. Walaupun node black hole lebih banyak, kalau *routing table* node sumber tidak melewatkan paketnya melalui node black hole untuk sampai ke node tujuan, maka tidak ada *packet loss* yang tercatat. Dan semakin padat node dalam jaringan, maka semakin banyak pilihan rute bagi node sumber untuk mengirimkan paketnya menuju node tujuan.

VI. KESIMPULAN

Berdasarkan hasil uji coba menggunakan beberapa parameter QoS, menunjukan bahwa black hole dapat menurunkan kualitas jaringan. Penurunan kualitas jaringan terhadap black hole bergantung pada topologi jaringan yang sedang terbentuk dan letak black hole itu sendiri. Semakin banyak node black hole tidak menjamin akan semakin banyak paket data yang hilang, karena proses pengiriman paket bergantung rute yang ada di *routing table* pada node sumber. Semakin padat node dalam jaringan, mampu mengurangi dampak black hole, karena node sumber akan mempunyai banyak pilihan rute pada *routing table* yang dapat digunakan untuk mengirimkan paketnya agar sampai ke node tujuan.

REFERENSI

[1] D. Irawan, "Simulasi Model Jaringan Mobile Ad-Hoc (Manet) Dengan Ns-3," *Badan Pengkaj. dan Penerapan Teknol. Jakarta. J. Konf. Nas. Sist. dan Inform. 2011; Bali, Novemb. 12, 2011.*, pp. 335–339, 2011.

[2] M. Chitkara and M. W. Ahmad, "Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols," *Int. J. Comput. Sci. Mob. Comput.*, vol. 32, no. 2, pp. 432–437, 2014.

[3] A. nur Pratama, M. H. Azaim, and V. Fauzi, "Routing Protocol (AODV, DSR, DSDV)," *17 Febuari 2015*, 2015. [Online]. Available: http://menulicious.student.telkomuniversity.ac.id/routing-protocol-aodv-dsr-dsdv/. [Accessed: 19-Nov-2017].

[4] S. Adiwicaksono, "Deteksi Malicious Node pada Zone Routing Protocol di Jaringan Mobile Adhoc Network," Doctoral dissertation, Institut Teknologi Sepuluh Nopember, 2017.

[5] N. Jiatmiko, and Y. Prayudi, "Simulasi Jaringan MANET Dengan NS3 Untuk Membandingkan Performa Routing Protokol AODV dan DSDV," *Seminar Nasional Teknologi Informasi Komunikasi dan Industri*, no. 7, p. 104, 2015.

[6] Y. Ekaputra, "Pemanfaatan Teknologi Mobile Ad-Hoc Network (Manet) Dan Simulasinya Menggunakan Network Simulator 3 (NS-3)," Doctoral dissertation, UII, 2016.

[7] I. Pratomo, and M. H. Hizburrahman, "Pendeteksian Dan Pencegahan Serangan Black Hole & Grey Hole Pada Manet," *JAVA Journal of Electrical and Electronics Engineering*, vol. 13, no. 4, pp. 47–53, 2015.

[8] N. J. K. Patel, and K. Tripathi, "Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 5, no. 5, pp. 194–205, 2017.

[9] A. Ali Pangera, *Menjadi Administrator Jaringan Nirkabel*. Yogyakarta: ANDI, 2008.

[10] A. Khozaimi, "Catatan khozaimi: MANET : Karakteristik," 2013. [Online]. Available: http://khozaimi.blogspot.co.id/2013/05/manet-karakteristik.html. [Accessed: 22-Aug-2017].

[11] A. Sanjaya, "Pengertian Wireless Jenis Teknologi Nirkabel (WPAN, WWAN, WLAN) MANET, WMN dan Ad Hoc dan Infrastruktur," 2015. [Online]. Available: http://www.landasanteori.com/2015/10/pengertian-wireless-jenis-teknologi.html. [Accessed: 20-Nov-2017].

[12] Nusanet, "Standar Protokol Jaringan Wireless IEEE 802.11," *6 Mei 2016*, 2016. [Online]. Available: https://www.nusa.net.id/blog/article/standar-protokol-jaringan-wireless-ieee-802-11/. [Accessed: 19-Nov-2017].