REPOSITOR, Vol. 2, No. 8, Agustus 2020, Pp. 1133-1142
ISSN : 2714-7975
E-ISSN : 2716-1382

Evaluasi Perbandingan Performa Jaringan Wireless Sensor Network Dalam Serangan Sybil Attack dan Hello Flood Attack

Hawwin Purnama Akbar[*1], Diah Risqiwati[2], Denar Regata Akbi[3]
[1,2,3]Teknik Informatika/Universitas Muhammadiyah Malang
haw2win@gmail.com[*1], risqiwati@umm.ac.id[2], dnarregata@umm.ac.id[3]

Abstrak

Perkembangan ilmu pengetahuan pada bidang teknologi jaringan terjadi sangat cepat karena mengikuti perkembangan kebutuhan manusia. Salah satu teknologi jaringan yang saat ini menarik perhatian masyarakat adalah teknologi Wireless Sensor Network (WSN). WSN adalah jaringan dari kumpulan sensor yang terhubung menggunakan teknologi wireless secara ad-hoc dan setiap sensor node digunakan untuk proses pengumpulan data dan menghubungkan dengan node yang lain melalui jaringan wireless. Karena pada kebanyakan kasus aplikasi WSN digunakan pada lingkungan yang ekstrem dan sensor node harus dapat beroperasi secara otomatis tanpa campur tangan manusia, jaringan ini menjadi rentan akan beberapa ancaman jaringan dan dapat mempengaruhi performa dari jaringannya. Terdapat berbagai macam jenis serangan yang dapat membahayakan jaringan wireless sensor network diantaranya yang paling umum adalah sybil attack dan hello flood attack. Dalam penelitian ini, penulis meneliti performa WSN saat diserang oleh Sybil attack dan hello flood attack dengan cara mengukur throughput, PDR (packet delivery ratio), jitter dan delay dalam jaringan WSN. Penelitian ini juga menganalisa jumlah node yang bervariasi dari 10 node sampai 30 node dengan waktu simulasi dari 10 detik sampai 30 detik lalu dianalisa jaringan ketika jaringan normal dan diserang oleh node penyerang yang bervariasi dari 1 sampai 3 penyerang. Dengan melakukan analisa tersebut, diperoleh data berupa perbandingan dampak serangan dari Sybil attack dan hello flood attack. Dampak dari sybil attack lebih berpengaruh pada parameter throughput dan pdr yang mengalami penurunan nilai hingga 69,9% untuk pdr dan 56,4% untuk throughput. Sedangkan dampak dari hello flood attack lebih berpengaruh pada parameter delay dan jitter yang mengalami kenaikan dari nilai semula 0,05 detik menjadi 0,576 detik untuk delay dan 0,579 detik untuk jitter.

Kata Kunci: *WSN, ad-hoc, Serangan Dalam WSN, Sybil, Hello Flood*

Abstract

The development of science in the field of network technology occurs very quickly because it follows the development of human needs. One of the network technology that is currently attracting public attention is wireless sensor network technology (WSN). WSN is a network of connected sensors using ad-hoc wireless technology and each node sensor are used to process data collection and connect with other nodes over a wireless network. Because in most cases WSN applications are used in extreme environments and node sensors must operate automatically without human intervention, these networks become vulnerable to some network threats and may affect the performance of their networks. There are various types of attacks that can harm wireless sensor network network among the most common is sybil attack and hello flood attack. In this study, authors examined the performance of WSN when attacked by Sybil attack and hello flood attack by measuring throughput, PDR (packet delivery ratio), jitter and delay in WSN network. This study also analyzed the number of nodes that varied from 10 nodes to 30 nodes with simulated time from 10 seconds to 30 seconds and then analyzed the network when the network was normal and attacked by the attacking nodes that varied from 1 to 3 attackers. By doing the analysis, the data can be obtained in the form of comparison of the impact of attacks from Sybil attack and hello flood attack. The impact of the sybil attack is more influential on the parameters of throughput and pdr which has decreased the maximum value up to 69.9% for pdr and 56.4% for throughput. While the impact of hello flood attack is more influential on the delay and jitter parameters that increased from the original value of 0.05 seconds to 0.576 seconds for delay and 0.579 seconds for jitter.

Keywords: *WSN, ad-hoc, Attacks in WSN, Sybil, Hello Flood*

1. Pendahuluan

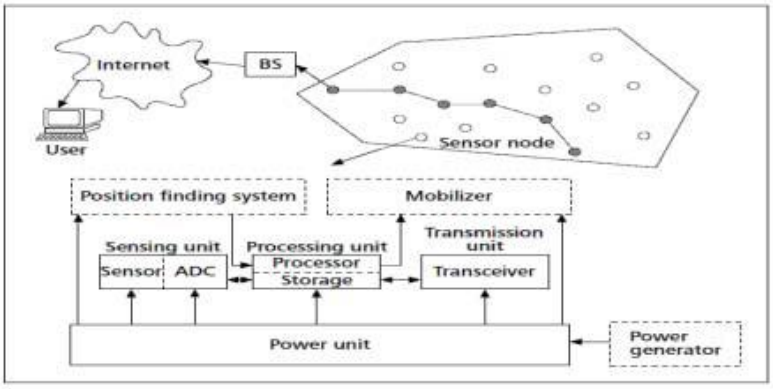
WSN merupakan jaringan dari kumpulan sensor yang terhubung menggunakan teknologi *wireless* secara *ad-hoc* dan setiap sensor *node* digunakan untuk proses pengumpulan data dan menghubungkan dengan *node* yang lain melalui jaringan *wireless*[1]. Banyak aplikasi yang memanfaatkan sistem WSN, misalnya pengumpulan data kondisi suatu lingkungan, pendeteksi bencana alam, monitoring keadaan bangunan, dan lain sebagainya. Karena pada kebanyakan kasus aplikasi WSN digunakan pada lingkungan yang ekstrem dan sensor *node* harus dapat beroperasi secara otomatis tanpa campur tangan manusia, jaringan ini menjadi rentan akan beberapa ancaman jaringan dan dapat mempengaruhi performa dari jaringannya[2]. Terdapat banyak jenis serangan dalam WSN, salah satunya yang paling umum adalah *Sybil Attack.* Dalam serangan ini penyerang menggunakan *node* yang tidak termasuk dalam jaringan atau bisa disebut *malicious node, node* ini menyerang dengan cara mendapat informasi algoritma *routing* dari *node* asli pada jaringan dan menyamar menjadi *node* yang terdapat dalam jaringan[3]. Lalu ada satu lagi jenis serangan yang menyerupai *Sybil attack*, serangan tersebut adalah *Hello Flood Attack.* Dalam serangan ini penyerang menggunakan *malicious node* untuk menyerang dengan cara mengirim *hello request* ke node yang asli dalam jaringan secara terus menerus yang akan menyebabkan gangguan pada sistem keamanan[4]. Kedua jenis serangan ini dapat disimulasikan dengan menggunakan tools atau aplikasi bernama Network Simulator.

Dari penelitian sebelumnya oleh Sher Anusha dengan judul *Simulation of attack in a Wireless* Sensor *Network using NS2* yang meneliti tentang simulasi dari beberapa serangan dalam WSN, dalam penelitian tersebut penulis hanya menggunakan satu parameter pengujian hasil yaitu throughput. Dan hanya menguji untuk satu penyerang dalam setiap skenario. Dari hal itu, penulis mencoba memberi kontribusi dengan menambahkan beberapa parameter penelitian. Dalam penelitian ini, akan diteliti performa WSN saat diserang oleh *Sybil attack* dan *hello flood attack* dengan cara mengukur *throughput*, PDR (*packet delivery ratio*), *jitter* dan *delay* dalam jaringan WSN. Penelitian ini juga menganalisa jumlah *node* dan penyerang dalam jaringan WSN dalam jumlah yang bervariasi dan membandingkan hasil dari masing-masing jumlah *node,* lalu akan di analisa perbandingan dampak yang ditimbulkan pada WSN.

Penelitian ini menggunakan *tools network simulator* (ns-2) simulator untuk menyimulasikan *node* WSN. *Network simulator* merupakan *software* bebasis *open source* yang biasanya digunakan untuk tujuan edukasi dan penelitian. Aplikasi menggunakan dua bahasa yaitu C++ dan OTcl (*Object oriented Tool Command Languange*). Bahasa C++ digunakan untuk mekanisme dalam sistem, dan Otcl untuk tampilan *front-end*. Aplikasi ini mensimulasikan jaringan menggunakan *time-based event*, jadi user dapat menentukan waktu dan kejadian secara *real time*. [5]. Melalui penelitian ini penulis mencoba menganalisa dampak serangan *sybil attack* dan *hello flood attack* dalam jaringan WSN dan membandingkan performa jaringan saat terjadi serangan dan tidak terjadi serangan. Dengan melakukan analisa tersebut, penulis dapat mengetahui karakteristik dari serangan dan performa dari jaringan.

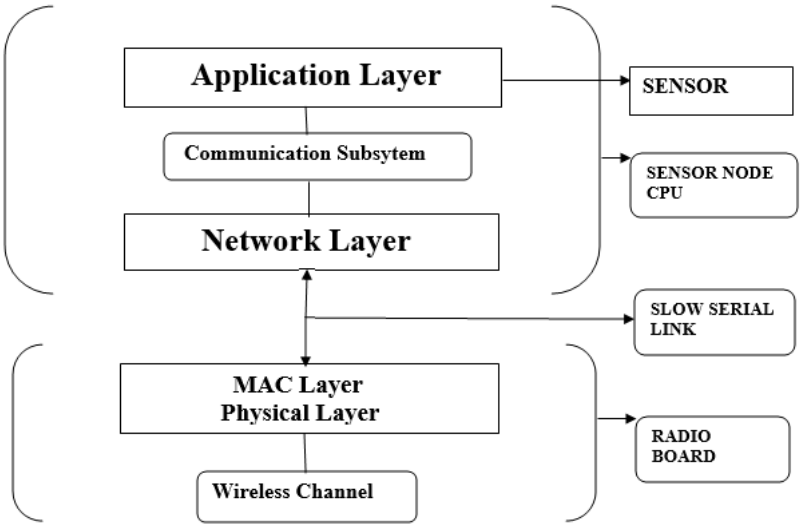
2. Metode Penelitian

WSN mempunyai banyak kegunaan yang diaplikasikan ke berbagai bidang. Tetapi WSN memiliki berbagai kelemahan yang dapat menimbulkan celah untuk serangan. Terdapat berbagai jenis serangan yang dapat mengurangi performa jaringan WSN.



Gambar 1. Arsitektur dan Komponen WSN [2]

Gambar 1 menjelaskan tentang desain arsitektur dasar dari sistem WSN dan bagaimana semua node terhubung pada jaringan. Dalam satu node terdapat power generator yang berperan sebagai sumber energi ke power unit. Lalu power unit mensuplai sumber energi ke sensing unit, processing unit, dan transmission unit. Setiap sensor node terhubung ke base station untuk berkomunikasi lalu dapat mengirim dan menerima data dari node lain. Masing–masing node juga mempunyai fungsi position finding system untuk menentukan lokasi node dan mobilize untuk pergerakan node [6].



Gambar 2. Arsitektur Layer [2]

Gambar 2 menjelaskan detail dari layer yang berada dalam jaringan sensor network dan proses komunikasi antar node dan perangkat wireless. Sistem WSN terdiri dari apllication Layer network layer, MAC layer, dan physical layer. Sebuah paket yang keluar masuk pada node akan dikirim melalui physical layer sampai ke application layer melalui wireless channel [6].

Dalam penelitian ini penulis mencoba mensimulasikan dua jenis serangan yang umum ditemukan dalam WSN yaitu Sybil attack dan Hello flood attack. Masing–masing dari jenis serangan akan di simulasikan dalam jaringan tersendiri dan dibandingkan dampak dari serangan terhadap sistem WSN. Perbandingan dampak diukur dengan membandingkan QOS saat sistem terkena serangan.

2.1 Perancangan Sistem

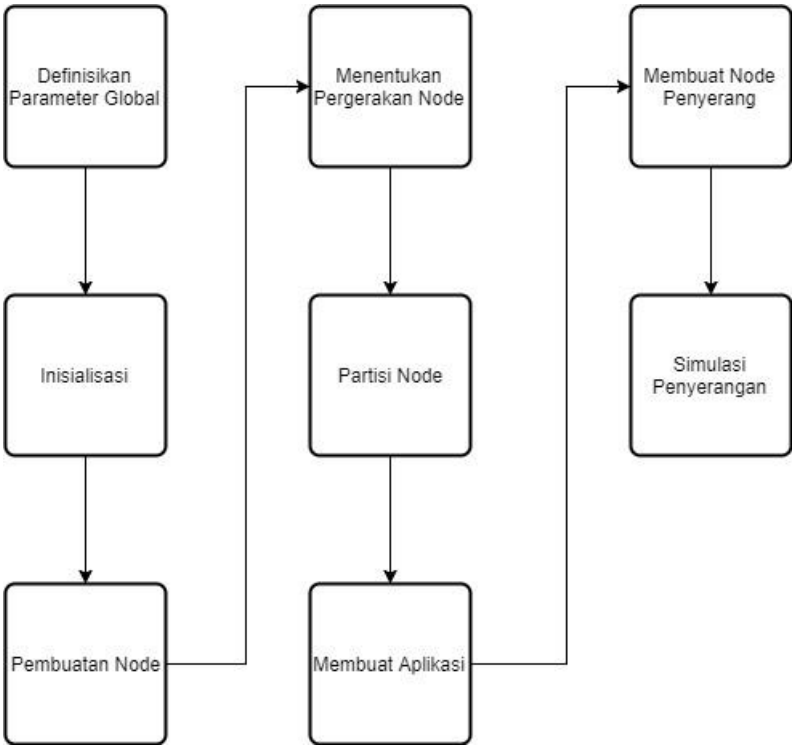
Perancangan simulasi ini akan menggunakan aplikasi *Network Simulator* 2 dengan routing AODV (*Ad-hoc On Demand Vector*) pada jaringan WSN. *Routing* AODV pada jaringan WSN adalah routing jenis *reactive* dimana rute jaringan akan dibuat hanya ketika *node* sumber akan mengirim data ke *node* penerima [7][8]. Pada penelitian ini terdapat parameter-parameter sistem yang dapat mempengaruhi hasil simulasi. Berikut pada Tabel 1 adalah parameter yang didefinisikan untuk simulasi penelitian ini.

Tabel 1. Parameter Perancangan Sistem

Parameter	Nilai
Model Propagasi	Two Ray Ground
Tipe Queue	Droptail/PriQueue
MAC type	802.11
Tipe Routing	AODV
Dimensi topografi	+-2000 x +-1000
Jumlah *node*	10-30
Waktu simulasi	10-30 detik

2.2 Perancangan Diagram Simulasi

Untuk perancangan aplikasi simulasi jaringan ini akan dibagi menjadi beberapa tahapan utama, yaitu mengatur parameter sistem, inisialisasi, pembuatan *node* serta pembuatan koneksi antar *node*, membuat pergerakan *node*, mempartisi *node*, membuat aplikasi, membuat *node* penyerang, simulasi penyerangan, dan akhir simulasi.



Gambar 3. Diagram Skenario Simulasi Jaringan

Pada Gambar 3 dijelaskan alur dari simulasi jaringan WSN yang akan dilakukan dalam penelitian ini. Langkah pertama telah dijelaskan dalam Tabel 1 di atas tentang parameter global dari simulasi yang digunakan. Selanjutnya langkah inisialisasi yang membahas persiapan dan penetapan variabel umum yang akan digunakan. Lalu dilakukan pembuatan *node* dan menentukan pergerakan *node* yang ada dalam jaringan. Setelah itu melakukan partisi *node* untuk menandai *node* tertentu yang akan digunakan. Pembuatan aplikasi yang digunakan dalam simulator untuk mengindikasi jaringan transimisi pada jaringan. Selanjutnya menetapkan *node* penyerang yang akan melakukan serangan. Lalu langkah terakhir yaitu melakukan simulasi penyerangan dan mengambil hasil pengujian dari serangan yang dilakukan.

2.3 Rancangan Pengujian

Pengujian dilakukan dengan merekam hasil dari simulasi berupa data berisi jumlah paket yang terkirim, waktu pengirman data, dan ukuran data yang diterima yang akan diproses dengan menghitung menggunakan rumus parameter QoS yang telah ditentukan. Dari hasil QoS akan dianalisa dampak serangan dan dibandingkan antara kedua serangan yang disimulasikan. Hasil dari data yang diuji dapat digambarkan melalui bentuk grafik. Berikut adalah rumus perhitungan parameter QoS yang digunakan.

Throughput adalah laju data aktual per satuan waktu. *Throughput* dapat dikatakan sebagai *bandwith* dalam kondisi yang sebenarnya [9]. *Throughput* diukur dalam satuan bit per detik(bps atau *bit per second*). Semakin besar nilai *throughput* maka semakin cepat laju pengiriman data, seperti pada Persamaan 1.

$$throughput = \frac{ukuran\ data\ yang\ diterima(bit)}{waktu\ pengiriman\ data\ (s)}\ [9] \quad (1)$$

Packet Delivery Ratio (PDR) pada Persamaan 2 adalah rasio antara banyaknya paket yang diterima oleh tujuan dibanding dengan banyaknya paket yang dikirim oleh sumber. PDR diukur dalam satuan persen (%). Semakin besar nilai PDR maka semakin baik pengiriman data [9].

$$PDR = \frac{paket\ yang\ diterima}{paket\ yang\ dikirim} \times 100\% \text{ [9]} \quad (2)$$

Delay pada Persamaan 3 adalah waktu tunda atau jeda waktu antara pengiriman data dari satu pengirim ke penerima. Nilai *delay* diperoleh dengan selisih antara waktu data diterima dan waktu data dikirim yang dipresentasikan dengan satuan *milisecond* (ms). Semakin kecil delay maka semakin baik pengiriman data [9].

$$delay = waktu\ data\ diterima - waktu\ data\ dikirim \text{ [9]} \quad (3)$$

Jitter adalah variasi *delay* antar paket yang diakibatkan oleh panjangnya *queue* dalam suatu pengolahan data dan padatnya trafik pengiriman data pada jaringan. Semakin besar nilai *jitter* pada jaringan maka semakin besar peluang terjadingan tumbukan antar paket data sehingga menyebabkan turunnya kualitas QOS data [9]. Seperti ditunjukkan pada Persamaan 4.

$$Jitter = \frac{total\ variasi\ delay(ms)}{total\ paket\ yang\ diterima-1} \text{ [9]}$$
$$total\ variasi\ delay(ms) = (delay2 - delay1) + (delay3 - delay2) + \cdots + (delay\ n - delay\ (n-1)) \quad (4)$$

Untuk menghitung persentase kenaikan dan penurunan data digunakan rumus kenaikan dan pernurunan seperti pada Persamaan 5 dan Persamaan 6.

$$kenaikan = \frac{data\ setelah\ naik - data\ semula}{data\ semula} \times 100\% \text{ [10]} \quad (5)$$

$$penurunan = \frac{data\ semula - data\ setelah\ turun}{data\ semula} \times 100\% \text{ [10]} \quad (6)$$

2.4 Skenario Pengujian

Dalam penelitian ini akan dilakukan skenario pengujian berupa perbedaan waktu, pergerakan node, dan jumlah node. Untuk setiap skenario akan dilakukan pengujian dari dua serangan yang akan diteliti. Dalam setiap serangan terdapat 3 penyerang yang akan dianalisa. Lalu terdapat skenario dimana terdapat gabungan dari 1 penyerang dari sybil attack dan 1 penyerang dari hello flood attack. Semua hasil akan di catat dalam bentuk tabel dan digambarkan dalam bentuk graph.

3. Hasil dan Pembahasan

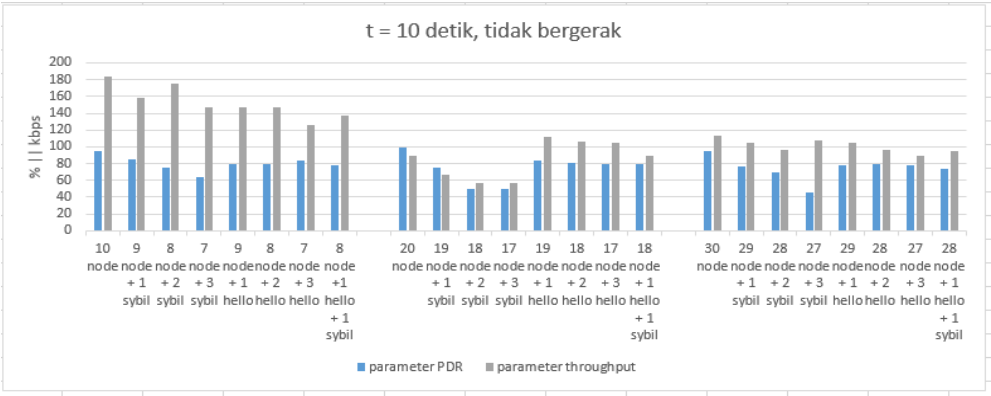
Setelah melakukan semua skenario simulasi akan didapatkan data berupa rekaman lalu lintas jaringan yang dapat di analisa dengan parameter QOS. Analisa hasil pengujian dilakukan untuk mengukur perbedaan dampak dari serangan *sybil attack* dan *hello flood attack.* Skenario yang akan diuji adalah jumlah node yang bervariasi dari 10 node, 20 node, dan 30 node. Lalu panjang waktu simulasi yaitu 10 detik, 20 detik, dan 30 detik. Terdapat pula skenario saat node diam dan node bergerak secara *random.*

3.1 Pengujian node saat tidak bergerak

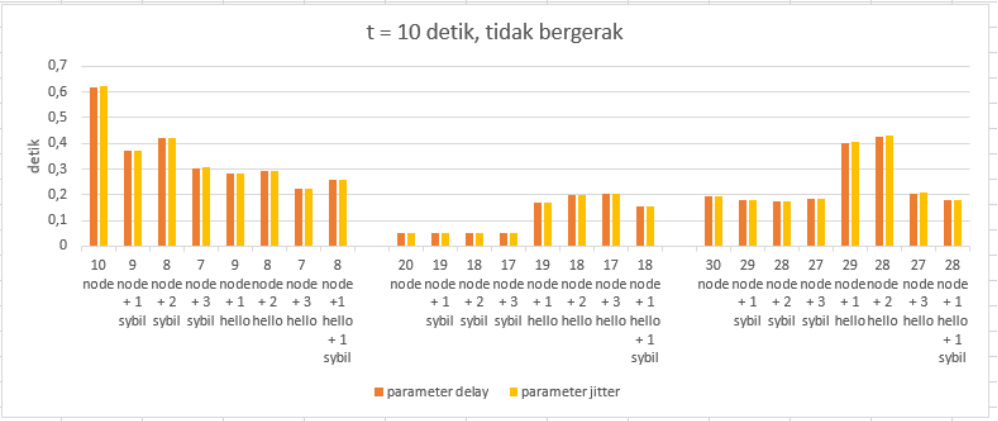
Dalam pengujian ini node dalam jaringan tidak melakukan pergerakan sehingga hasil pengujian akan berubah secara signifikan terhadap jumlah dan jenis serangan yang dipakai. Hal ini dikarenakan penempatan node penyerang harus berada diantara transmisi node sumber dan tujuan. Berikut adalah hasil pengujian QOS saat node tidak bergerak.

3.1.1 Node tidak bergerak dengan waktu = 10 detik

Dalam pengujian ini waktu ditetapkan adalah 10 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.



Gambar 4. Grafik Percobaan 10 detik pdr dan Throughput

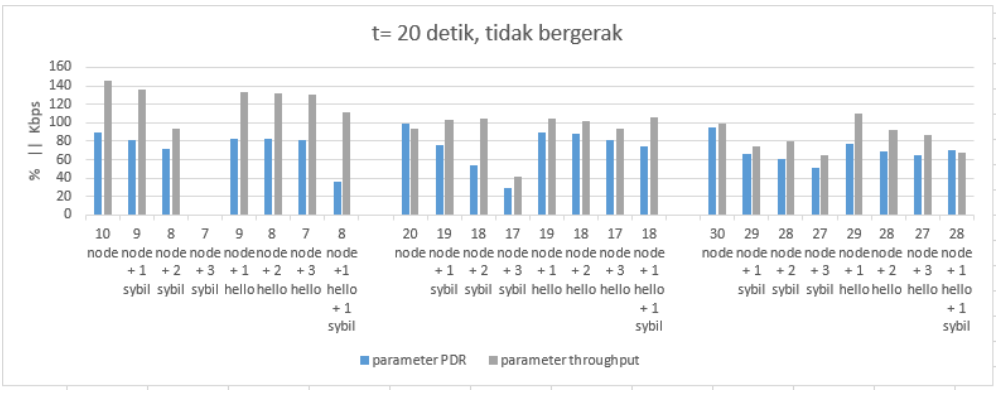


Gambar 5. Grafik Percobaan 10 detik Delay dan Jitter

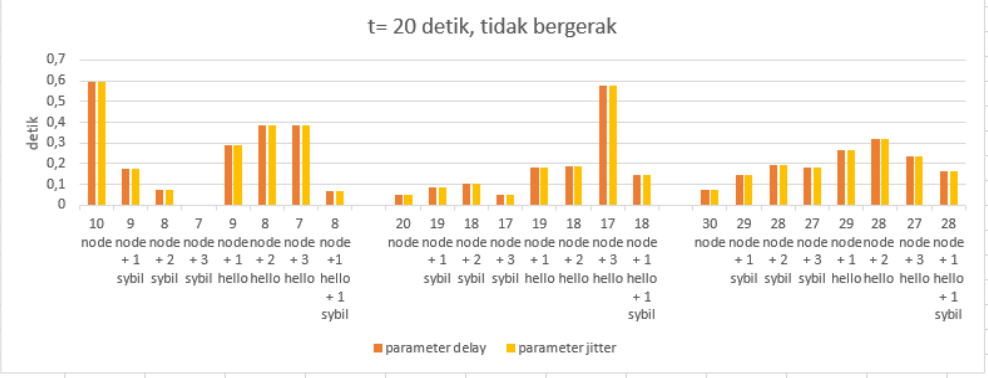
Dari hasil pengujian Gambar 4 dan Gambar 5 diatas dapat dilihat hasil parameter QoS pdr dan throughput yang turun secara signifikan saat terjadi serangan sybil attack. Sedangkan untuk serangan hello flood terjadi perubahan untuk setiap jumlah serangan tetapi tidak signifikan. Untuk parameter delay dan jitter akan bertambah nilainya jika terjadi lalu lintas yang padat dalam jaringan, jadi jika terjadi serangan yang menyebabkan lalu lintas berkurang, maka nilai delay dan jitter akan berkurang juga.

3.1.2 Node tidak bergerak dengan waktu = 20 detik

Gambar 6 dan Gambar 7 berikut adalah hasil dari pengujian dalam waktu 20 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.



Gambar 6. Grafik Percobaan 20 detik pdr dan Throughput

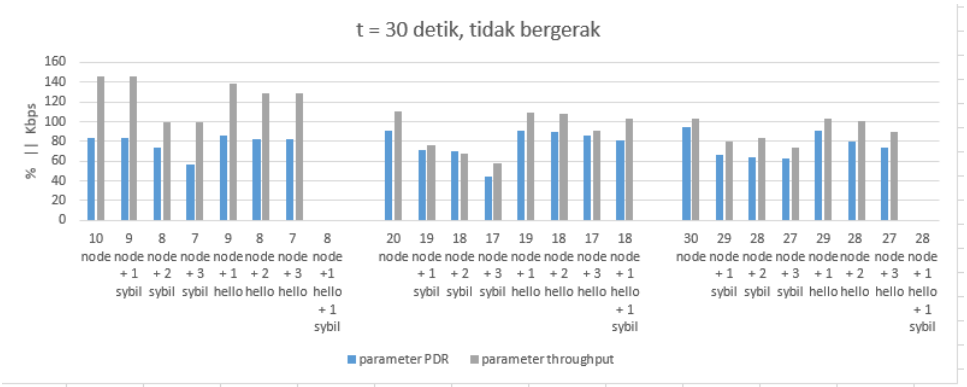


Gambar 7. Grafik Percobaan 20 detik Delay dan Jitter

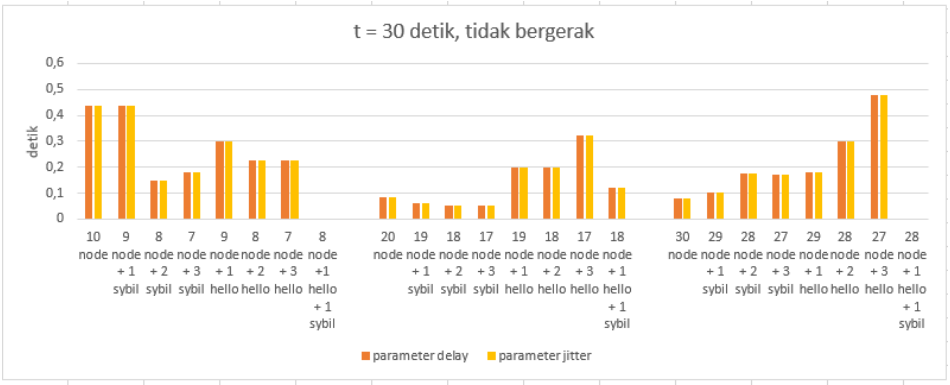
Dari hasil pengujian diatas dapat dilihat hasil parameter QoS saat tidak terjadi serangan lebih kecil dari skenario saat waktu = 10 detik. Parameter QoS saat terkena serangan juga mengalami penurunan sejumlah banyaknya jumlah serangan. Dalam percobaan 10 node dengan 3 serangan sybil tidak menghasilkan hasil karena simulasi mengalami error packet remove. Hal ini disebabkan kebanyakan paket yang dikirim tidak terkirim ke tujuan.

3.1.3 Node tidak bergerak dengan waktu = 30 detik

Gambar 8 dan Gambar 9 berikut adalah hasil dari pengujian dalam waktu 30 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.



Gambar 8. Grafik Percobaan 30 detik pdr dan Throughput



Gambar 9. Grafik Percobaan 30 detik Delay dan Jitter

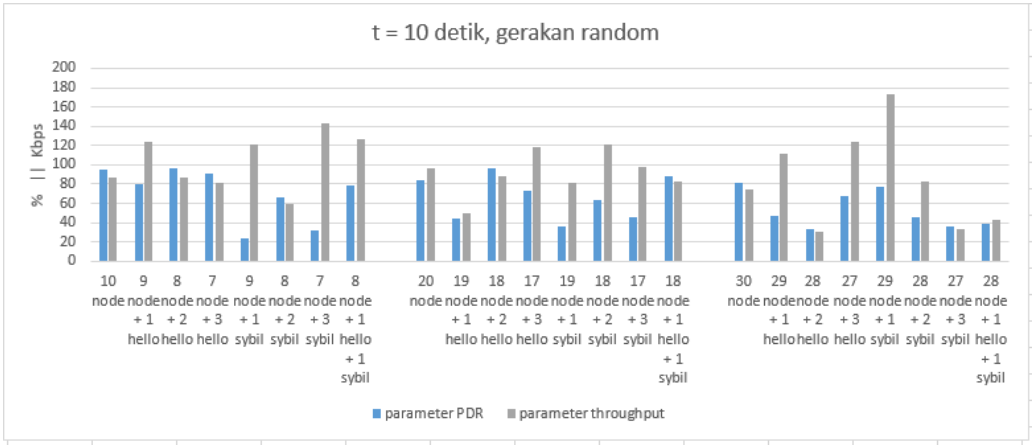
Dari hasil pengujian dalam waktu 30 detik, parameter QoS saat tidak terjadi serangan juga semakin menurun. Error packet remove juga terjadi pada percobaan 1 sybil + 1 hello dalam jaringan 10 node dan 30 node.

3.2 Pengujian saat node bergerak

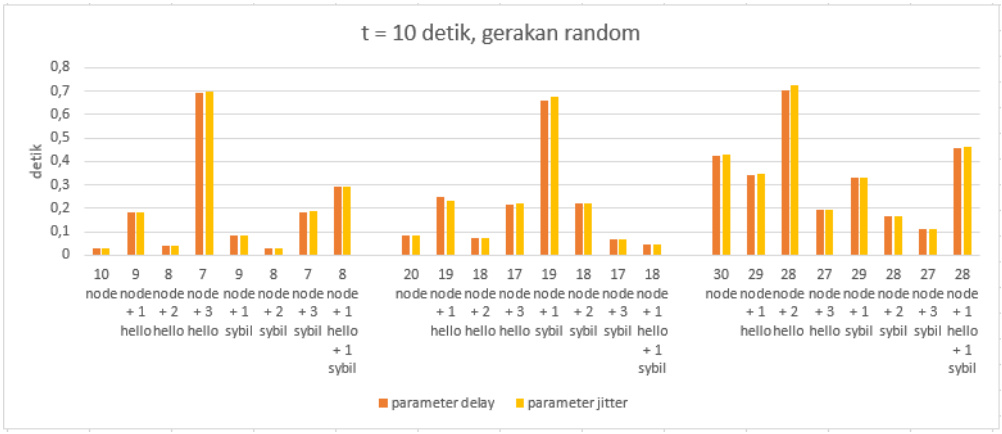
Pengujian ini dilakukan untuk mengetahui dampak saat node bergerak secara random dalam ruang lingkup topografi yang telah ditetapkan. Waktu saat node bergerak juga secara acak. Berikut adalah hasil pengujian saat node bergerak.

3.2.1 Node bergerak secara random dengan waktu = 10 detik

Gambar 10 dan Gambar 11 berikut adalah hasil dari pengujian dalam waktu 10 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.



Gambar 10. Grafik Percobaan 10 detik pdr dan Throughput

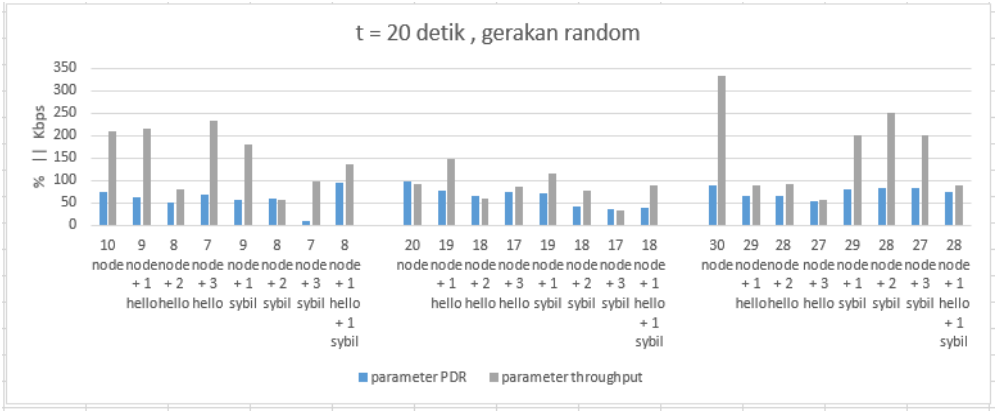


Gambar 11. Grafik Percobaan 10 detik Delay dan Jitter

Dari hasil pengujian node bergerak dalam waktu 10 detik dapat dilihat nilai parameter QoS yang tidak signifikan. Hal ini dikarenakan node dalam jaringan bergerak secara random ke berbagai arah sehingga node sumber dapat kehilangan tujuan pengiriman jika node yang dituju tidak terjangkau oleh node lain. Sama halnya dengan node penyerang yang tidak dapat aktif jika bergerak ke arah yang tidak terjangkau oleh node lain.

3.2.2 Node bergerak secara random dengan waktu = 20 detik

Berikut adalah hasil dari pengujian dalam waktu 20 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.



Gambar 12. Grafik Percobaan 20 detik Throughput dan Jitter

Gambar 13. Grafik Percobaan 20 detik Delay dan Jitter

Hasil pengujian Gambar 12 dan Gambar 13, node bergerak dalam waktu 20 detik juga menghasilkan nilai parameter QoS yang tidak signifikan.

3.2.3 Node bergerak secara random dengan waktu = 30 detik

Gamabr 14 dan Gambar 15 berikut adalah hasil dari pengujian dalam waktu 20 detik. Terdapat hasil pengujian saat tidak terjadi serangan, terjadi serangan sybil, terjadi serangan hello flood, dan campuran serangan dari sybil dan hello flood.

Gambar 14. Grafik Percobaan 30 Detik Throughput dan pdr

Gambar 15. Grafik Percobaan 30 Detik Delay dan Jitter

Hasil pengujian node bergerak dalam waktu 30 detik juga menghasilkan nilai parameter QoS yang tidak signifikan.

4. Kesimpulan

Dari hasil implementasi dan pengujian yang telah dilakukan, diperoleh data berupa perbandingan dampak serangan dari Sybil attack dan hello flood attack. Dampak dari sybil attack lebih berpengaruh pada parameter throughput dan pdr berupa nilai minimal 29,6% untuk pdr dan 41kbps untuk throughput mengalamai penurunan sebesar 69,9% dari nilai no. Sedangkan dampak dari hello flood attack lebih berpengaruh pada parameter delay dan jitter berupa nilai maksimal 0,576 detik untuk delay dan 0,579 detik untuk jitter. Dalam skenario node yang tidak bergerak menghasilkan dampak yang signifikan dibandingkan dengan skenario node yang bergerak secara acak. Hal ini dikarenakan node dapat kehilangan tujuan pengiriman jika bergerak ke lokasi yang tidak terjangkau node lain. Untuk kedepannya dapat di teliti mekanisme untuk memastikan pengiriman data yang aman dan menghindari serangan dalam WSN. Parameter yang menentukan performa jaringan dapat di hitung dari simulasi yang telah dilakukan. Terdapat banyak serangan yang dapat menyerang sistem WSN, tetapi sistem keamanan dalam WSN masih dinilai kurang.

Referensi

[1] I. P. A. Eka Pratama and S. Suakanto, “Wireless Sensor Network,” p. 603, 2015.
[2] A. Sher, “Simulation of Attacks in a Wireless Sensor Network using NS2,” pp. 1–44, 2015.
[3] J. Newsome, E. Shi, D. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” *Proc. third Int. Symp. Inf. Process. Sens. networks IPSN04*, pp. 259–268, 2004.
[4] V. P. Singh, S. Jain, and J. Singhai, “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks,” *Int. J. Comput. Sci.*, vol. 7, no. 3, pp. 23–27, 2010.
[5] M. H. Rehmani, S. Doria, and M. R. Senouci, “A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2),” *Network*, vol. 50, 2010.
[6] C. Sciences, C. Christi, A. Sher, C. Members, and C. Chairperson, “Simulation of Attacks in a Wireless Sensor Network using NS2,” 2015.
[7] J. Satiti, I. D. Irawati, L. V. Yovita, F. T. Elektro, and U. Telkom, “Analisis Perbandingan Performansi Protokol Routing Aodv Dan Dsdv Pada Wireless Sensor Network Comparative Analysis of Aodv and Dsdv Routing Protocols Performance on Wireless Sensor Network,” vol. 2, no. 2, pp. 1–6, 2015.
[8] P. Samundiswary and P. Dananjayan, “Performance Analysis of Trust Based AODV for Wireless Sensor Networks,” *Int. J. Comput. Appl.*, vol. 4, no. 12, pp. 6–13, 2010.
[9] V. Mehta and N. Gupta, “Performance Analysis of QoS Parameters for Wimax Networks,” *Int. J. Eng. Innov. Technol.*, vol. 1, no. 5, pp. 105–110, 2012.
[10] A. F. N. Huda, A. Makhsun, and A. A. R, “Kontribusi Penjualan Koran Dan Pendapatan Iklan terhadap Pendapatan Usaha Periode 2015 dan 2016 pada PT LMG Contribution of Newspaper ’ s Sales and Advertising Revenue to Operating Revenue Period 2015 and 2016 at PT LMG,” pp. 1–7, 2016.