SISTEM KEAMANAN *WIRELESS SENSOR NETWORK* MENGGUNAKAN *SIGNATURE BASED INTRUSION DETECTION SYSTEM* DAN SISTEM *SHUTDOWN* UNTUK MEMITIGASI SERANGAN DOS

WIRELESS SENSOR NETWORK SECURITY SYSTEM USING SIGNATURE BASED INTRUSION DETECTION SYSTEM AND SHUTDOWN SYSTEM TO MITIGATE DOS ATTACK

I Made Dwiki Kusuma Pradipta[1], M. Teguh Kurniawan [2], Adityas Widjajarto [3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1] **dwikikusuma@student.telkomuniversity.ac.id**, [2]**teguh.kurniawan@telkomuniversity.ac.id**,
[3]**adtwjrt@telkomuniversity.ac.id**

Abstrak

Wireless Sensor Network (WSN) memiliki peran yang besar di beberapa bidang seperti penerapan pada area peperangan, penerapan pada rumah pintar, penelitian tentang lingkungan serta penerapan di bidang kesehatan. Namun WSN memberikan ancaman dikarenakan tidak adanya sistem keamanan bawaan yang tertanam pada perangkat sensor serta dengan adanya keterbatasan yang dimiliki oleh sensor node. Akibatnya WSN rentan terhadap serangan, salah satunya adalah serangan DoS. Sehingga diperlukan cara mendeteksi dan memitigasi serangan DoS pada WSN. Pada penelitian ini membahas metode deteksi dan mitigasi serangan DoS menggunakan signature based Intrusion Detection System (IDS) dengan mengimplementasikan sistem shutdown pada sink node. Sistem shutdown berhasil diimplementasikan pada jaringan WSN ketika IDS mendeteksi adanya serangan DoS. Sehingga metode sistem shutdown dapat digunakan sebagai langkah awal mitigasi serangan DoS dengan mengamankan data pada sink node.

Kata kunci: WSN, sistem *shutdown*, IDS, serangan DoS

Abstract

Wireless Sensor Network (WSN) has a large role in several areas such as the application of warfare areas, the implementation of smart homes, research on the environment and implementation in the health sector. However, WSN poses a threat due to the absence of an innate security system embedded in the sensor device and with the limitations possessed by the sensor node. As a result, WSN vulnerable to attack, one of them is a DoS attack. So it is necessary how to detect and mitigate DoS attacks on WSN. In this study discuss the method of detection and mitigation of DoS attack using signature based Intrusion Detection System (IDS) by implementing system shutdown on sink node. The shutdown system successfully implement on the WSN network when the IDS detect a DoS attack. So the system shutdown method can be used as a first step to mitigate DoS attacks by securing data on the sink node.

Keywords: WSN, shutdown system, IDS, DoS attack

1. Pendahuluan

Penggunaan teknologi *wireless* sangat memberikan kemudahan dalam bertukar informasi secara nirkabel sehingga implementasinya terus mengalami perkembangan dan salah satu penerapan teknologi *wireless* adalah pada *Internet of Things* (IoT). Secara umum IoT diartikan sebagai sebuah kemampuan untuk menghubungkan objek-objek pintar dan dapat saling berinteraksi dengan objek lain, lingkungan maupun dengan peralatan komputasi cerdas lainnya melalui jaringan internet [1]. Salah satu elemen terpenting dalam pengaplikasian IoT adalah *Wireless Sensor Network* (WSN) [2]. *Sensor node* pada WSN memiliki keterbatasan, seperti pada ruang penyimpanan, kemampuan komputasi, rendahnya ketersediaan sumber daya serta tidak ada sistem keamanan bawaan yang tertanam pada WSN. Berdasarkan keterbatasan tersebut dan karakteristik WSN yang menerapkan sistem komunikasi antar *sensor node* secara *broadcasting*, melakukan pengamanan data pada WSN harus diperhatikan.

Serangan DoS merupakan salah satu serangan yang rentan pada WSN, serangan DoS bertujuan untuk

menghalangi *user* untuk menggunakan sumber daya sebuah jaringan atau sistem dengan cara mengirimkan permintaan palsu secara tidak wajar sehingga dapat menguras penggunaan sumber daya pada jaringan dan meningkatkan konsumsi energi, *delay*, menurunkan *throughput* serta serangan ini termasuk serangan yang cukup sulit dideteksi [3].

Solusi terhadap serangan DoS yang ada saat ini diantaranya dengan menerapkan signature based intrusion detection system (IDS) dalam mendeteksi serangan DoS. Terdapat tiga fase dalam proses pendeteksian serangan yaitu fase information gathering, fase decision making, dan fase attack detection[4]. Selain itu terdapat penelitian yang menerapkan pengecekan batas maksimum dalam melakukan permintaan Route Request (RREQ_RATELIMIT) yang konstan sebesar 10 paket Route Request (RREQ) per detik berdasarkan RFC 3561 [5]. Sehingga apabila terdapat permintaan RREQ yang melampaui RREQ_RATELIMIT maka terindikasi sebagai serangan DoS. Untuk mencegah node memanipulasi nilai RREQ_RATELIMIT menjadi nilai yang sangat tinggi, maka diterapkan batas RREQ yang dapat diterima (RREQ_ACCEPT_LIMIT) sebesar tiga paket RREQ per detik [6]. Ketika permintaan RREQ melebihi nilai RREQ_ACCEPT_LIMIT maka node tetangga (*neighbor node*) akan mencatat permintaan RREQ tersebut sebagai permintaan hitam (RREQ_BLACKLIST_LIMIT). Sehingga permintaan RREQ yang tercatat dalam RREQ_BLACKLIST_LIMIT akan ditolak dalam selang waktu yang telah ditentukan (BLACKLIST_TIMEOUT) [6].

Usulan yang diajukan pada Tugas Akhir ini adalah melakukan mitigasi serangan DoS pada WSN dengan mengadopsi skema penghitungan RREQ_RATELIMIT [6] dan mengimplementasikan signature based IDS serta menambahkan fitur sistem shutdown pada sink node WSN. Sehingga ketika terjadi serangan DoS dengan permintaan RREQ yang melebihi RREQ_RATELIMIT, maka WSN akan melakukan shutdown sink node sehingga mampu mengantisipasi kesalahan dalam pengambilan keputusan pada application layer.

2. Dasar Teori

2.1 Arsitektur WSN

Komponen *sebuah sensor node* umumnya terdiri atas empat subsistem diantaranya memori (*memory*), perangkat komunikasi *(communication device*), kontroler (*controller*), *sensor* / *actuators* dan catu daya (*power supply*) [7]. Tidak adanya sistem keamanan bawaan menjadikan WSN rentan terhadap ancaman keamanan, salah satunya adalah ancaman serangan DoS.

2.2 Serangan DoS

Serangan DoS pada WSN terdiri dari dua macam yaitu *Route Request* (RREQ) dan *Data flooding attack* [8]. Pada penelitian ini membahas tentang serangan terhadap DoS pada RREQ. Serangan DoS pada RREQ dengan cara memilih *node* tertentu pada WSN sebagai *attacker node*. Karena pengiriman RREQ yang banyak akan membanjiri keseluruhan jaringan, sehingga mengakibatkan peningkatan konsumsi energi pada baterai dan *bandwidth* yang memicu serangan DoS sehingga akses ketersediaan jaringan akan terganggu.

2.3 Protokol Routing AODV

Ad Hoc On-Demand Distance Vector (AODV) adalah sebuah protokol *routing* yang bersifat proaktif, protokol ini bersifat *on-demand* yang berarti pembuatan rute pengiriman paket dilakukan ketika adanya permintaan oleh sebuah *node* [9]. AODV terdiri dari dua proses yaitu *Route Discovery* menggunakan *Route Request* (RREQ) dan *Route* Reply (RREP) serta *Route Maintenance* menggunakan *Route Error* (RERR) dan HELLO.

Ketika sebuah *node* hendak mengirimkan paket menuju *node* tujuan dan rute menuju *node* tujuan belum terbentuk, maka *node* sumber mengirimkan RREQ kepada *node* tetangganya (*neighbor node*). Apabila *neighbor node* tidak memiliki alamat yang diminta maka *neighbor node* akan membuat *reverse path* untuk *node* sumber dan mengirimkan ulang RREQ tersebut dengan memperbaharui *sequence number* hingga mencapai *node* tujuan. Bila RREQ telah sampai pada *node* tujuan maka *node* tujuan akan memberikan pesan balasan dengan mengirimkan RREP menuju *node* sumber, dan terbentuklah rute pengiriman paket. Sehingga tabel *routing* terbentuk dan apabila ditemukan rute yang lebih pendek dengan *sequence number* tertinggi maka secara otomatis tabel *routing* akan diperbaharui [9].

2.4 Intrusion Detection System

Intrusion Detection System (IDS) merupakan sebuah sistem yang melakukan pengawasan terhadap lalulintas jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan di dalam sebuah sistem jaringan yang dimonitor dan dilaporkan ke *administrator* atau bagian manajemen jaringan[10]. Keterbatasan yang dimiliki WSN membuat IDS sangat mungkin untuk diterapkan karena tidak memerlukan

komputasi yang kompleks untuk mendeteksi dan mengidentifikasi adanya serangan pada sebuah jaringan

2.5 Quality of Service

Quality of Service atau QoS merupakan terminologi yang digunakan untuk mendefinisikan kemampuan suatu jaringan untuk menyediakan tingkat jaminan layanan yang harus dipenuhi untuk memberikan layanan yang lebih baik. QoS didesain agar performa yang didapatkan sesuai dengan kebutuhan pengguna dalam menjalankan aplikasi pada jaringan. Terdapat tiga variabel yang diukur pada penelitian ini untuk menghitung QoS pada WSN, yaitu:

1. *Delay*
2. *Packet Loss*
3. *Throughput*

2.6 Sistem Shutdown

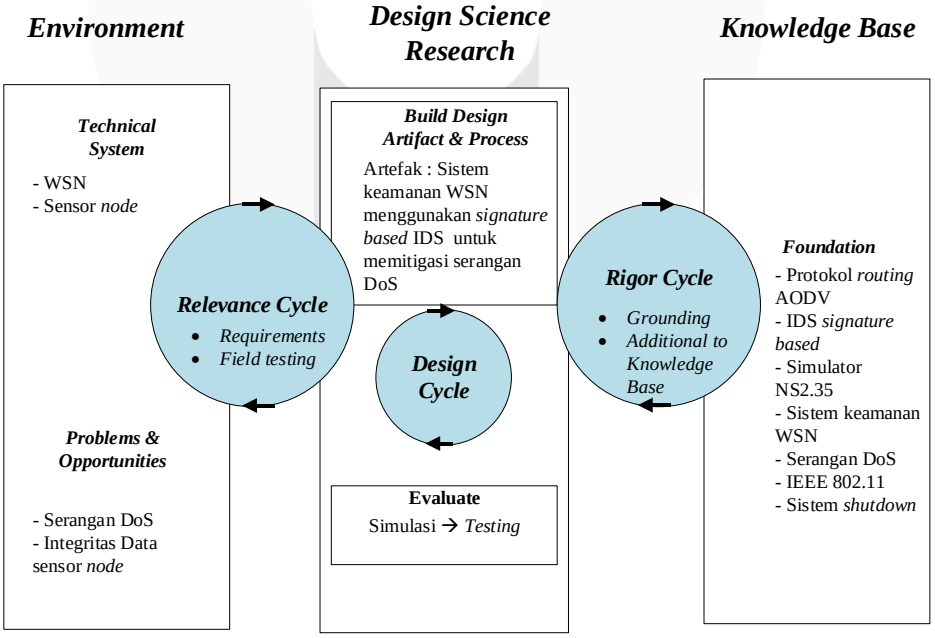
Pada jaringan WSN *sensor node* diletakkan tersebar pada suatu wilayah yang telah ditentukan. Setiap *sensor* mengirimkan data sekitarnya kemudian dikirimkan ke *sink node*. Sebuah *node* yang melakukan serangan DoS akan melakukan pemintaan rute *routing* palsu secara terus-menerus sehingga membanjiri WSN dan *node* yang berada di sekitar penyerang akan mengalami peningkatan konsumsi energi yang signifikan. *Node* yang seharusnya dapat bekerja lebih lama akan kehilangan lebih banyak energi dari pada semestinya. Selain energi, jumlah paket yang hilang lebih banyak karena *node* yang seharusnya dapat meneruskan paket tidak dapat melakukan tugasnya karena kehabisan energi. Data akan kehilangan integritas dan dapat menyebabkan kesalahan pengambilan keputusan di sisi *application layer*. Adanya sistem *shutdown* dapat menonaktifkan *node* sehingga dapat melindungi integritas data pada WSN.

Sistem *shutdown* awalnya digunakan untuk mematikan energi *node* pada WSN ketika *node* tidak melakukan aktivitas seperti *transmitting*, *receiving*, dan *idle* [11]. Pada penelitian ini sistem *shutdown* dimodifikasi dan diimplementasikan pada *sink node*. Sehingga apabila serangan DoS terdeteksi maka mitigasi yang dilakukan adalah melakukan sistem *shutdown* pada *sink node.* Sistem shutdown pada *sink* node dilakukan untuk mencegah data-data yang diterima tidak utuh dan dapat mencegah kesalahan dalam pengambilan keputusan di sisi *application layer*.

3. Metodologi Penelitian

3.1 Model Konseptual

Model konseptual merupakan sebuah kerangka kerja yang memberikan gambaran hubungan antara faktor-faktor secara logis yang saling berkaitan. Pada Gambar 1 Model Konseptual dalam perancangan sistem keamanan WSN menggunakan *signature based* dengan mengimplementasikan sistem *shutdown* yang diterapkan pada penelitian ini.



Gambar 1 Model Konseptual

4. Perancangan *software* dan *hardware*

4.1 Perancangan sistem

Dalam melakukan perancangan sistem keamanan WSN menggunakan *signature based* IDS untuk memitigasi serangan DoS dilakukan identifikasi komponen *hardware* dan *software* pendukung yang digunakan dalam melakukan simulasi.

Tabel 1 Spesifikasi *Hardware* dan *Software*

	Komponen	Informasi
Hardware	Prosesor	5th *Generation* Intel® Core™ i5-4210U *processor* (3M *Cache*, up to 2.7 GHz)
	Memori RAM	8 GB
	Kapasitas	500 GB
Software	Sistem Operasi	Xubuntu 16.04 64bit (*one boot*)
	Framework	NS2.35
	Pengolah tampilan *framework*	Nam 1.15
	Pengolah grafik	*Google Spreadsheet , Excel*
	Pengolah topologi	NSG2.1

Dengan mengacu Tabel 1 dalam melakukan perancangan simulasi keamanan WSN tidak ditemukan kendala sehingga spesifikasi pada Tabel 1 dapat dijadikan acuan penelitian dalam mengembangkan rancangan sistem keamanan WSN dengan menggunakan aplikasi NS2.35.

4.2 Parameter sistem

4.2.1 Parameter penelitian

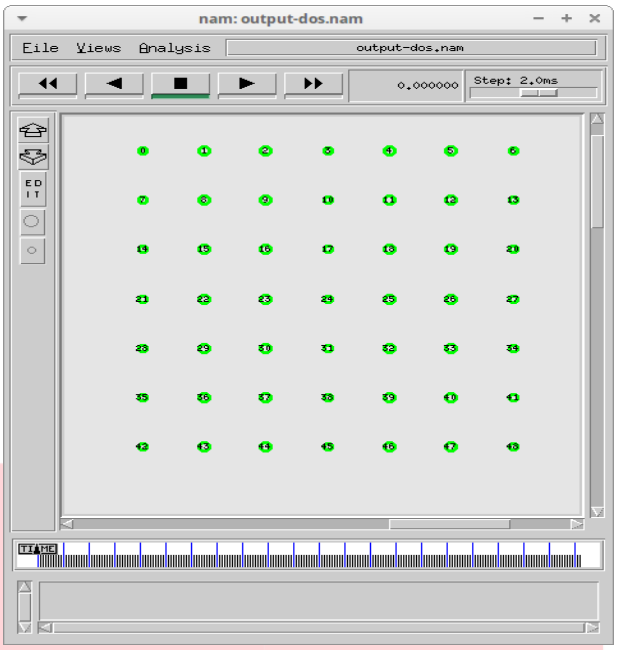
Percobaan pada penelitian ini menggunakan parameter penelitian dan parameter serangan yang terdapat pada Tabel 2.

Tabel 2 Parameter Node WSN pada NS2.35

Kategori	Keterangan
Luas area	800m x 800m
Jumlah *node*	49
Jarak *node*	100 m
Ukuran paket	512 bytes
Protokol transmisi	UDP
Trafik aplikasi	CBR
***Bandwidth* CBR**	0.1Mb
Waktu simulasi	50 detik
Model propagasi	Two ray ground
Tipe antrean/*queue*	Drop Tail
Model antena	*Omni Directional Antenna*
Protokol *routing*	AODV
Energi awal	3.4 J
Tx power	0.33 J
Rx power	0.1 J
Idle power	0.05 J
Sleep power	0.03 J

4.3 Perancangan topologi

Pada penelitian ini menggunakan topologi *Grid* [12]. Topologi *Grid* terdiri dari 49 *node* yang disebar membentuk persegi 7x7 dengan luas area 800 m x 800 m seperti yang terlihat pada Gambar 2. Topologi *Grid* dipilih karena mampu memberikan performa yang baik dan dapat memperpanjang waktu hidup (*lifetime*) WSN [12].



Gambar 2 Topologi WSN pada Simulator NS2.35

4.4 Skenario pengujian

4.4.1 Skenario I: Kondisi WSN tanpa adanya serangan DoS

Pada skenario I disimulasikan kondisi WSN ketika dalam kondisi normal tidak ada serangan DoS dan tidak ada implementasi sistem *shutdown.*

4.4.2 Skenario II: Kondisi WSN dengan serangan DoS dan implementasi IDS

Pada skenario II disimulasikan kondisi WSN ketika adanya serangan DoS. Serangan DoS dimulai pada detik ke sepuluh ketika simulasi berlangsung.

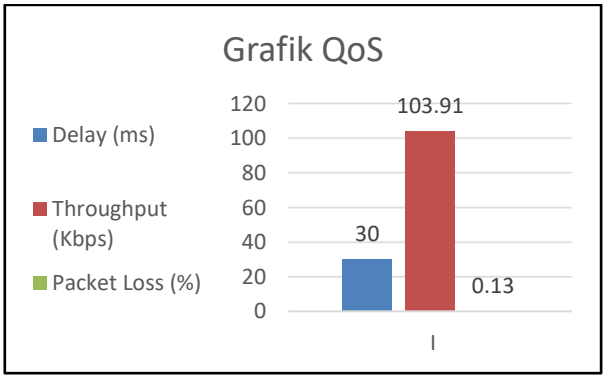
4.4.3 Skenario III: Kondisi WSN dengan serangan DoS dan implementasi IDS serta *shutdown Sink node*

Pada skenario III disimulasikan kondisi WSN ketika adanya serangan DoS dan mengimplementasikan *signature based* IDS ketika serangan DoS terdeteksi serta menerapkan sistem *shutdown* pada *sink node.*

5. Pengujian dan Analisis Sistem

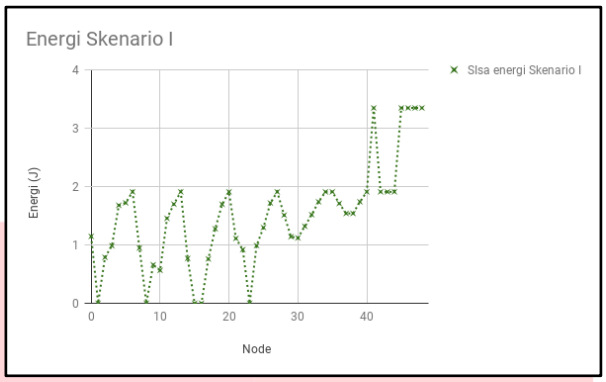
5.1 Skenario I: Kondisi WSN tanpa adanya serangan DoS

Hasil simulasi Skenario I dapat dilihat pada Gambar 3, hasil yang diperoleh diantaranya adalah nilai *delay* sebesar 30 ms menunjukkan kualitas *delay* pada jaringan yang sangat baik, nilai *throughput* sebesar 103.91 kbps menunjukkan kualitas *throughput* pada jaringan yang sangat baik, nilai *packet loss* sebesar 0.13% menunjukkan kualitas *packet loss* pada jaringan yang sangat baik. Kesimpulan yang diperoleh dari Skenario I tersebut adalah jaringan WSN memiliki performa yang sangat baik dilihat dari *delay*, *throughput* serta *packet loss* yang dimiliki.



Gambar 3 Grafik QoS Skenario I

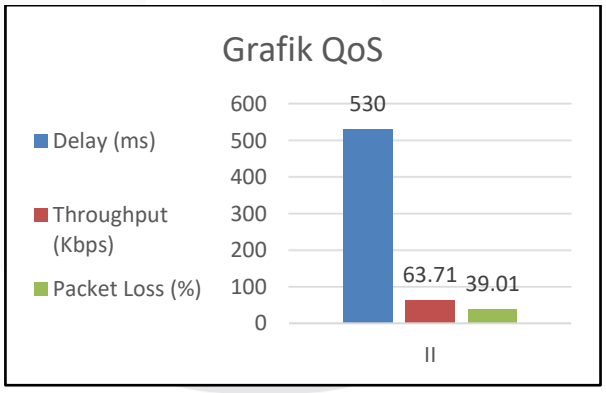
Gambar 4 menunjukkan sisa energi tiap *node* pada Skenario I dengan tanpa adanya serangan DoS. Terdapat lima *node* yang tidak memiliki sisa energi hingga waktu simulasi berakhir, yaitu *node* 1, *node* 8, *node* 15, *node* 16, dan *node* 23. Apabila dilihat pada simulasi Skenario I, *node* tersebut menunjukkan rute paket dari sumber ke tujuan, sehingga *node* yang memiliki konsumsi energi tertinggi adalah *node* 1, *node* 8, *node* 15, *node* 16, dan *node* 23 yang merupakan *node* yang berada pada jalur *routing* WSN.



Gambar 4 Grafik Energi pada Skenario I

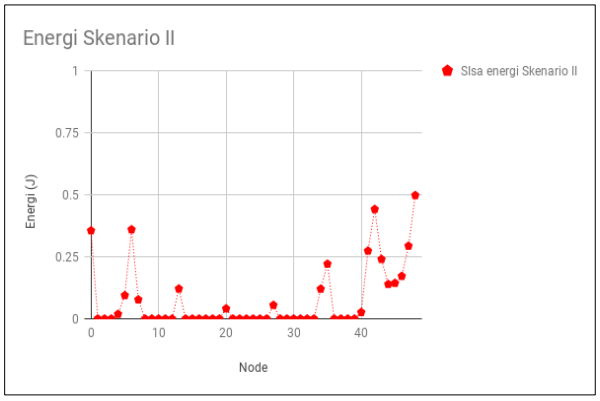
5.2 Skenario II: Kondisi WSN dengan serangan DoS dan implementasi IDS

Hasil simulasi Skenario II dapat dilihat pada Gambar 5, , hasil yang diperoleh diantaranya adalah nilai *delay* sebesar 530 ms menunjukkan kualitas *delay* pada jaringan yang buruk, nilai *throughput* sebesar 63.71 kbps menunjukkan kualitas *throughput* pada jaringan tergolong baik, nilai *packet loss* sebesar 39.01% menunjukkan kualitas *packet loss* pada jaringan buruk. Nilai *delay* yang besar diperoleh dari adanya permintaan RREQ yang dilakukan terus menerus dengan interval 0.09 detik yang dilakukan oleh *attacker node* pada WSN yang mengakibatkan paket RREQ membanjiri jaringan. Banyaknya RREQ paket yang membanjiri jaringan, menyebabkan waktu tunggu paket dari *sensor node* asal ke *sensor node* tujuan menjadi lebih lama dan memiliki nilai *delay* yang tinggi. Selain itu *sensor node* tidak dapat menampung seluruh paket sehingga menyebabkan banyak paket yang hilang selama pengiriman dari *sensor node* asal ke *sensor node* tujuan yang menyebabkan nilai *packet loss* sebesar 39.01 %.



Gambar 5 Grafik QoS Skenario II

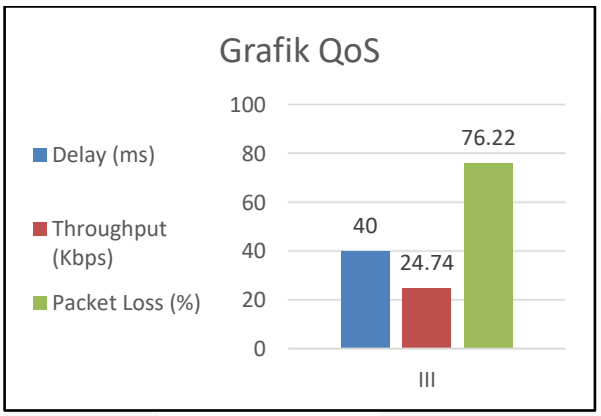
Gambar 6 menunjukkan sisa energi tiap *node* pada Skenario II dengan adanya serangan DoS, terdapat banyak *node* yang kehilangan banyak energi hingga waktu simulasi berakhir, hanya beberapa *node* yang memiliki sisa energi diantaranya adalah *node* 0, *node* 6, *node* 41, *node* 42, *node* 47, dan *node* 48 yang memiliki sisa energi diantara 0.25 Joule dan 0.5 Joule. *Node-node* di sekitar *attacker node* mengalami peningkatan konsumsi energi karena harus mencari rute yang diminta oleh *attacker node* dan melakukan broadcast RREQ ke seluruh *node* tetangganya secara terus menerus dengan interval 0.09 detik menyebabkan energi yang digunakan menjadi lebih besar, sehingga menyebabkan banyak *node* kehabisan energi.



Gambar 6 Grafik Energi pada Skenario II

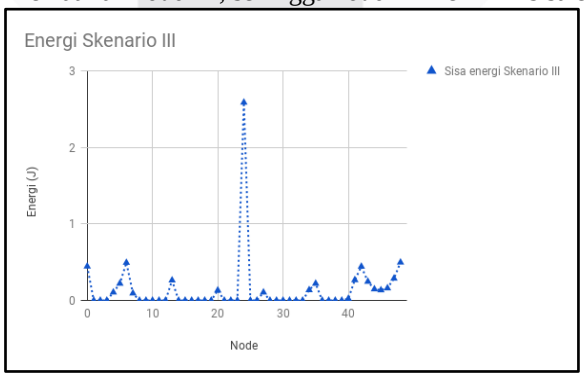
5.3 Skenario III: Kondisi WSN dengan serangan DoS dan implementasi IDS serta *shutdown sink node*

Hasil simulasi skenario III dapat dilihat pada Gambar 7, hasil yang diperoleh diantaranya adalah nilai *delay* sebesar 40 ms menunjukkan kualitas *delay* pada jaringan yang sangat baik, nilai *throughput* sebesar 24.74 kbps menunjukkan kualitas *throughput* pada jaringan yang buruk, nilai *packet loss* sebesar 76.22% menunjukkan kualitas *packet loss* pada jaringan yang buruk. Nilai *packet loss* yang besar terjadi karena ketika serangan DoS terdeteksi oleh IDS maka *sink node* menjalankan sistem *shutdown* sehingga energi pada *sink node* akan bernilai nol dan tidak dapat menerima dan mengirimkan data dari WSN ke *node* penerima di *application layer*.



Gambar 7 Grafik QoS Skenario III

Gambar 8 menunjukkan sisa energi tiap *node* pada Skenario III dengan adanya serangan DoS dan sistem *shutdown* pada *sink node*. Sebagian besar *node* tidak memiliki sisa energi. Energi *node* rata-rata dibawah 1 Joule dan hanya node 24 yang berperan sebagai *sink node* memiliki sisa energi diantara 2 Joule dan 3 Joule. Energi *node* 24 hanya mengalami sedikit pengurangan karena apabila serangan DoS terdeteksi maka sistem *shutdown* akan mematikan *node* 24, sehingga *node* 24 memiliki sisa energi yang cukup besar.



Gambar 8 Grafik energi pada skenario III

6. Kesimpulan

Simulasi WSN dengan mengimplementasikan *signature based* IDS untuk mendeteksi serangan DoS diterapkan pada Skenario II dan Skenario III. Performa IDS pada Skenario II dan Skenario III berjalan dengan sangat baik karena mampu mendeteksi serangan DoS ketika sebuah permintaan RREQ melebihi ketentuan yang telah ditentukan. IDS tidak memberikan pengaruh terhadap serangan DoS, karena IDS hanya berperan untuk memberitahukan peringatan telah terjadi serangan DoS.

Serangan DoS memberikan pengaruh performa pada layanan WSN. Skenario I menunjukkan WSN dalam keadaan normal tanpa serangan dengan menghasilkan performa sangat memuaskan, Skenario II menunjukkan WSN dalam keadaan adanya serangan DoS dan menghasilkan performa buruk, Skenario III menunjukkan WSN dalam keadaan adanya serangan DoS dan terdapat implementasi sistem *shutdown* pada IDS. Skenario III mampu menunjukkan performa yang lebih baik dibandingkan dengan Skenario II.

Penerapan sistem *shutdown* pada *signature based* IDS dapat direalisasikan dengan mematikan energi pada *sink node* ketika IDS mendeteksi adanya serangan DoS, sehingga dapat mencegah data yang diterima tidak utuh. Sistem *shutdown* dapat dijadikan sebagai langkah awal untuk melakukan mitigasi ketika terjadi serangan DoS pada WSN. Ketika serangan DoS terdeteksi oleh IDS, IDS akan membangkitkan sistem *shutdown* pada *sink node* yang mengakibatkan *sink node* tidak dapat menerima paket dari manapun.

Daftar Pustaka:

[1] E. D. Meutia, “Internet of Things – Keamanan dan Privasi,” *Semin. Nas. dan Expo Tek. Elektro 2015*, pp. 85–89, 2015.

[2] Ferrovial *et al.*, “How will city infrastructure and sensors be made smart?,” *White Pap.*, vol. 6, no. 11, p. 113, 2007.

[3] K. Kaushal and V. Sahni, “Early Detection of DDoS Attack in WSN,” *Int. J. Comput. Appl.*, vol. 134, no. 13, pp. 14–18, 2016.

[4] N. M. Saravana Kumar, S. Deepa, C. N. Marimuthu, T. Eswari, and S. Lavanya, “Signature Based Vulnerability Detection Over Wireless Sensor Network for Reliable Data Transmission,” *Wirel. Pers. Commun.*, vol. 87, no. 2, pp. 431–442, 2015.

[5] E. B.-R. C. Perkins, “Ad hoc On-Demand Distance Vector (AODV) Routing,” *RFC 3561*, 2003.

[6] A. Jain and P. P. Dhasal, “Prevention of DOS-attack for AODV Routing Protocol in,” vol. 1, no. 4, pp. 1–4, 2015.

[7] I. M. E, B. Sugiarto, and I. Sakti, “Rancang Bangun Sistem Monitoring Kualitas Udara Menggunakan Teknologi Wireless Sensor Network (WSN),” vol. III, no. 1, pp. 90–96, 2009.

[8] R. Choubey, S. Sahu, R. S. Dubey, and S. Dubey, “Flooding Attack Prevention Algorithm in AODV Protocol for Mobile Ad-hoc Network,” vol. 1, no. 6, pp. 191–195, 2011.

[9] X. Wu and B. Bhargava, “AO2P : A d Hoc O n-Demand P osition-Based P rivate Routing Protocol,” vol. 4, no. 4, pp. 335–348, 2005.

[10] M. E. Aminanto and G. N. L, “MENANGANI SERANGAN INTRUSI MENGGUNAKAN IDS DAN IPS,” *STEI.ITB.AC.ID*, 2013. [Online]. Available: https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/.

[11] H. Hasnorhafiza, “Performance Evaluation of Random Node Shutdown Technique in Wireless Sensor Network for Improving Energy Efficiency,” pp. 16–20, 2012.

[12] Y. Chen and C. Kuo, “Study of Grid-based Routing in Wireless Sensor Networks,” *4th IEEE Int. Conf. Mob. Wirel. Commun. Netw.*, 2002.