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

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

Afrizal Hamzah[1], M. Teguh Kurniawan [2], Adityas Widjajarto [3]

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

Abstrak

Wireless Sensor Network (WSN) biasanya diterapkan pada pemantauan lingkungan, pemantauan jembatan, pemantauan aktivitas gunung api, komponen pendukung *smart city*, atau juga bisa pada pemantauan dan kontrol aktivitas di bidang pertanian. Pada WSN terkadang sulit untuk mengimplementasikan keamanan, karena dalam WSN tidak ada sistem keamanan bawaan dikarenakan tingkat pemrosesan dan sumber daya yang terbatas. Salah satu serangan yang ada pada teknologi WSN adalah *Hello Flood Attack. Hello Flood Attack* ini membanjiri *node-node* tetangga dengan *hello packet*, sehingga energi yang dimiliki *node* tetangganya berkurang hingga habis. Pada penelitian ini membahas metode untuk mendeteksi dan mitigasi menggunakan *signature based* IDS dan implementasi *system shutdown* pada *sink node*. IDS adalah mekanisme untuk mendeteksi aktivitas mencurigakan atau serangan pada jaringan. IDS bersifat pasif dan hanya bisa mendeteksi aktivitas mencurigakan, tidak bisa melakukan tindak pencegahan dan membunyikan *alarm*. Pada saat serangan *hello flood* terjadi, IDS akan mendeteksi serangan dan *system shutdown* akan diimplementasikan pada *sink node*

Kata kunci : WSN, *system shutdown*, IDS, serangan *Hello Flood*

Abstract

Wireless Sensor Network (WSN) is usually applied to environmental monitoring, monitoring bridges, monitoring volcanic activity, supporting components of smart city, or also for monitoring and control of agricultural activities. WSN are difficult to implement security, because in WSN there is no default security system due to limited processing and resource levels. One of the attacks on WSN technology is Hello Flood Attack. This Hello Flood Attack floods neighboring nodes with hello packet, so the energy of its neighboring nodes is reduced to exhaustion. In this study discusses methods for detecting and mitigating using signature based IDS and system shutdown implementation on sink nodes. IDS is a mechanism to detect suspicious activity or attacks on the network. IDS is passive and can only detect suspicious activity, can not take precautions and sound an alarm. At the time of the hello flood attack occurs, IDS will detect the attack and system shutdown will be implemented on the sink node

Keywords: WSN, *shutdown system*, IDS, *Hello Flood attack*

1. Pendahuluan

Teknologi yang berkembang saat ini tentu akan sangat mempermudah manusia dalam melakukan berbagai aktivitas sehari-hari, diantaranya mengakses data ataupun informasi. Dengan memanfaatkan perkembangan jaringan internet pada saat ini, pengguna dapat mengakses informasi dengan cepat, mudah, serta akurat. Cara memperoleh data atau informasi tersebut adalah dengan mengakses internet. Saat ini ada beberapa macam tipe koneksi ke internet, salah satunya adalah koneksi tanpa menggunakan kabel (wireless).

Dengan teknologi yang canggih pada saat ini, internet sudah menjadi bagian dari hidup manusia. Salah satu pemanfaatan kecanggihan internet saat ini adalah munculnya konsep Internet of Things (IoT). IoT ini adalah konsep tentang menghubungkan perangkat agar terintegrasi satu sama lain. Salah satu penerapan teknologi wireless dan sekaligus menerapkan tentang Internet of Things adalah teknologi jaringan sensor nirkabel atau WSN (Wireless Sensor Network)[1].

WSN adalah teknologi yang terdiri dari perangkat kecil dengan daya rendah yang mengintegrasikan kemampuan algoritma, sensor dan komunikasi yang terbatas. Seperti contohnya smartphone, lampu, mesin cuci bahkan mobil sekalipun. Bahkan IoT juga diterapkan pada komponen mesin seperti pesawat terbang, robot militer dan lain-lain [1]. Pada WSN sulit untuk mengimplementasikan pertahanan, dikarenakan tingkat pemrosesan dan sumber daya yang terbatas. Oleh karena itu WSN rentan terhadap serangan. Serangan pada WSN dapat dibagi menjadi dua, yaitu serangan aktif dan serangan pasif. Serangan aktif adalah serangan yang dapat menyebabkan gangguan fungsi normal jaringan, dengan menghapus atau modifikasi informasi, contoh dari serangan aktif adalah jamming, impersonating, modifikasi, dan denial of service (DoS) [2]. Sedangkan serangan pasif adalah serangan dengan mendapatkan data tanpa mengganggu aktifitas pertukaran data yang ada pada jaringan tersebut, contoh dari serangan pasif adalah eavesdropping, traffic analysis, dan traffic monitoring [2]. Protokol routing yang digunakan untuk WSN sangat sederhana dan sangat rentan terhadap serangan [3]. Sebagian besar serangan routing adalah hello flood attack, sybil attack, wormhole attack, blackhole attack dan selective forwarding attack [3]. Beberapa serangan memanipulasi data pengguna secara langsung dan beberapa serangan mempengaruhi protokol routing [3].

Salah satu serangan yang menyerang pada network layer adalah hello flood attack. Hello Flood Attack membanjiri node-node tetangga dengan hello messages, sehingga energi yang dimiliki node tetangganya berkurang hingga habis. Node tersebut menyebarkan hello messages yang digunakan untuk meyakinkan bahwa node tersebut adalah tetangganya [4].

Improvement yang dilakukan pada laporan ini adalah membuat fitur shutdown system. Dengan menggunakan IDS dengan signature approach, hello flood attack yang menyerang WSN kemudian terdeteksi oleh IDS dengan menggunakan signature approach kemudian secara otomatis sistem WSN melakukan shutdown

2. Dasar Teori

2.1 Arsitektur WSN

Komponen *sebuah* sensor *node* dikelompokkan atas empat bagian, yaitu memori (*memory*), perangkat komunikasi *(communication device*), kontroler (*controller*), *sensor* / *actuators* dan catu daya (*power supply*) [5].

2.2 Serangan Hello Flood

Serangan Hello Flood atau *Hello Flood Attack* merupakan salah satu serangan yang mungkin terjadi dalam penggunaan teknologi WSN. *Hello Flood attack* adalah serangan yang terjadi pada *layer network*. ketika penyerang menambahkan *node* atau memprogram ulang *node* yang telah ada, penyerang membuat *node* tersebut menyebarkan *hello messages* terus menerus dan meyakinkan *node* tetangga bahwa *node* tersebut adalah anggota dalam satu jaringan. Beberapa protokol mengharuskan *node* untuk mengirim *hello messages* untuk menunjukan bahwa *node* tersebut adalah anggota satu jaringan. Jika *node* yang lain menerima *hello messages* tersebut, maka *node* yang lain berasumsi bahwa node tersebut adalah tetangga mereka. Tapi terkadang asumsi ini salah, karena penyerang dapat dengan mudah mengirimkan hello messages dengan kekuatan yang cukup meyakinkan bahwa node penyerang adalah tetangganya. Tapi kekuatan pengiriman data yang dimiliki node yang berada di jaringan tersebut lebih sedikit daripada yang dimiliki node penyerang, sehingga paket-paket yang dikirim menjadi hilang, dan serangan itu menyebabkan WSN tersebut mengalami kebingungan [6].

2.3 Intrusion Detection System

Intrusion Detection System (IDS) adalah mekanisme untuk mendeteksi aktivitas mencurigakan atau serangan pada jaringan. IDS bersifat pasif dan hanya bisa mendeteksi aktivitas mencurigakan, tidak bisa melakukan pencegahan dan hanya membunyikan alarm. Saat serangan terjadi, sudah menjadi tugas administrator untuk melakukan pencegahan pada serangan tersebut. Pada WSN ada tiga kategori IDS, yaitu signature approach, anomaly approach dan hybrid approach [7].

2.5 Quality of Service

Quality of Service adalah suatu pengukuran tentang beberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan [8]. Terdapat tiga variable yang diukur untuk menghitung QoS pada WSN, yaitu :

Tabel 1 Indeks parameter QoS

Nilai	Persentase (%)	Indeks
3,8 – 4	95 – 100	Sangat memuaskan
3 – 3,9	75 – 94,75	Memuaskan
2 – 2,99	50 – 74,75	Kurang memuaskan
1 – 1,99	25 – 49,75	Buruk

a) Troughput

Throughput merupakan jumlah total kedatangan paket yang sukses diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut [9].

Tabel 2 Kategorisasi *Troughput*

Kategori	*Throughput*	indeks
Sangat Baik	100%	4
Baik	75%	3
Sedang	50%	2
Buruk	<25%	1

b) *Delay*

Delay merupakan keterlambatan yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama [9].

Tabel 3 Kategorisasi *Delay*

Delay	Kualitas	Indeks
0 – 150 ms	Sangat Baik	4
150 – 300 ms	Baik	3
300 – 450 ms	Sedang	2
>450 ms	Buruk	1

c) *Packet Loss*

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukan jumlah jumlah total paket yang hilang. Salah satu penyebab *packet loss* adalah antrian yang melebihi kapasitas buffer pada setiap node [9].

Tabel 4 Kategorisasi *Packet Loss*

KATEGORI	*Packet Loss*	Indeks
Sangat Baik	0	4
Baik	3 %	3
Sedang	15 %	2
Buruk	25 %	1

2.6 Sistem *Shutdown*

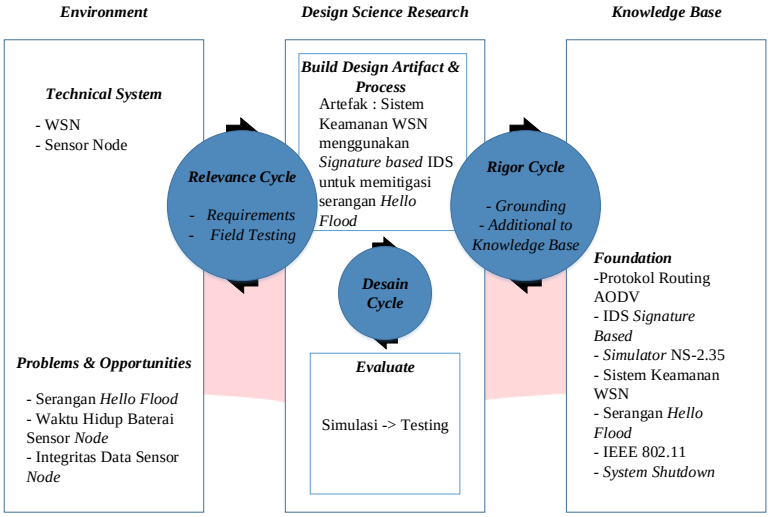
Sistem *Shutdown* adalah salah satu cara untuk memitigasi dari serangan yang terjadi pada WSN. Untuk mendeteksi serangan *hello flood* pada WSN, digunakan *signature based Intrusion Detection System* (IDS). Setiap WSN ingin mengirimkan data, *source node* melakukan *request* kepada *sink node* agar jalur yang dilalui adalah jalur yang terpendek, lalu *sink node* melakukan *reply request* dari *source node* dan menunjukkan jalur terpendek yang dapat dilalui. Pada saat terdapat *node hello flood* membanjiri jaringan WSN dengan mengirimkan *hello message* secara terus-menerus, maka data yang telah mempunyai jalur menuju *sink node* terputus. Hal itu menyebabkan paket yang telah dikirim dari *source node* menuju *sink node* tidak sampai karena *node hello flood* terlalu cepat mengirimkan *hello messages* yang menyebabkan jaringan WSN mengalami kebingungan dan data tidak sampai ke sink node. Karena *source node* melakukan *request* terus menerus, kemudian *node* kehabisan energi.

Sistem *shutdown* ditambahkan untuk mematikan *sink node* pada saat serangan *hello flood* terdeteksi. Setelah data yang dikirimkan dari *source node* sampai ke *sink node*, kemudian *administrator* melakukan pemeriksaan data. Mitigasi ini dilakukan agar tidak terjadi kesalahan pengambilan keputusan oleh *administrator*. Pada saat *system shutdown* diimplementasikan, ketika *sink node* mati, *administrator* akan melakukan *maintenance* untuk memeriksa *node* yang terkena serangan *hello flood*.

3. Metodologi Penelitian

3.1 Model Konseptual

Model konseptual adalah menjelaskan tentang bagaimana sistem keamanan WSN pada saat ini. Sistem WSN pada saat ini masih jarang digunakan dan memiliki resource yang terbatas. Dengan menggunakan standar IEEE 802.11, penelitian ini mengusulkan Shutdown System untuk keamanan WSN apabila ada serangan yang terjadi



.

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 *hello flood* dilakukan identifikasi komponen *hardware* dan *software* pendukung yang digunakan dalam melakukan simulasi.

Tabel 5 Spesifikasi hardware dan software

Komponen	Informasi	
Hardware	*Processor*	Intel Core i3
	RAM	8 Gigabyte
	Hard Drive	50 Gigabyte
	Resolusi	1366x768
Software	*Simulation tools*	NS-allinone-2.35
	Analysis tools	Awk
	Editor	Gedit
	Pemetaan node	NSG

4.2 Parameter sistem

4.2.1 Parameter penelitian

Percobaan pada penelitian ini menggunakan parameter penelitian dan parameter serangan yang terdapat pada Tabel 6 dan Tabel 7.

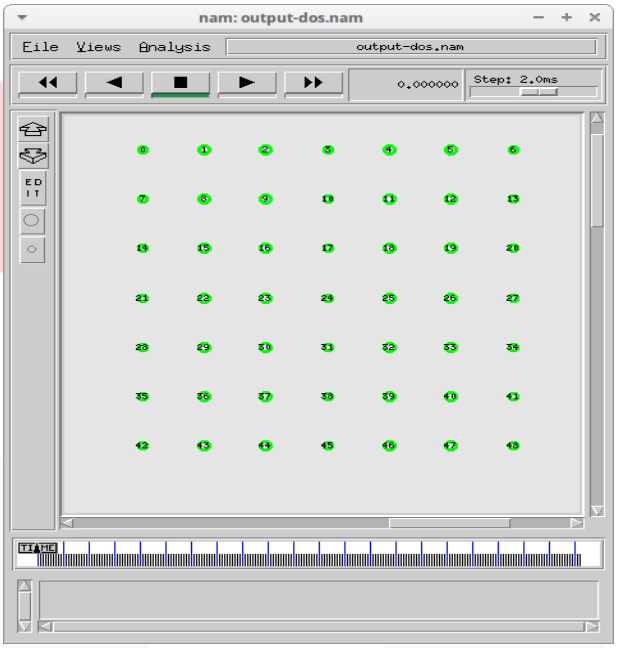
Tabel 1 Parameter penelitian

Luas Area	**:**	**1600 x 1600**
Jumlah *Node*	:	49
Jarak *Node*	:	100 m
Ukuran Paket	:	1000
Protokol Transmisi	:	UDP
Trafik Aplikasi	:	CBR
Waktu Simulasi	:	25 s
Model Propagansi	:	Two Ray Ground

Tipe Antrian/*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 topologi WSN terdiri dari 49 *node* yang disebar membentuk persegi 7x7 dengan luas area 1600mx1600m



Gambar 2 Topologi WSN pada simulator NS2.35

4.4 Skenario pengujian

4.4.1 Skenario I: Kondisi WSN normal tanpa serangan.

Pada skenario I ini disimulasikan teknologi WSN ketika keadaan normal atau tanpa serangan. Pada skenario I ini juga tidak dilakukan mitigasi menggunakan system shutdown. Hal ini dilakukan untuk mengukur bagaimana kondisi lalu lintas data dan konsumsi energi pada kondisi normal.

4.4.2 Skenario II: Kondisi WSN dengan serangan Hello Flood dan IDS

Pada skenario II disimulasikan teknologi WSN ketika terdapat serangan dan bagaimana IDS mendeteksi serangan yang terjadi pada salah satu node yang terdapat pada satu jaringan tersebut. Pada skenario II ini belum dilakukan implementasi system shutdown. Pada topologi yang telah dirancang sebelumnya, diantara 49 node yang tersebar ada 1 node yang dirancang sebagai node penyerang.

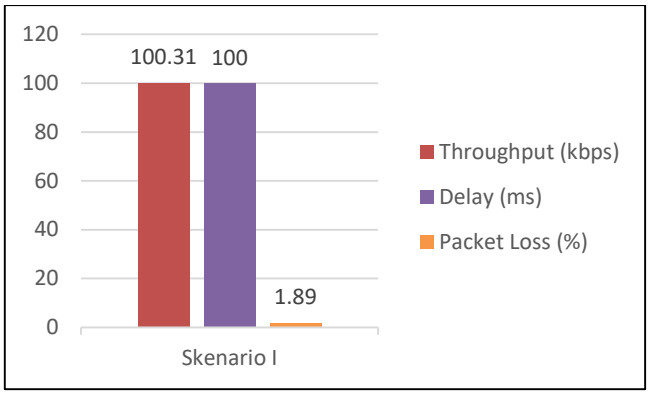
4.4.3 Skenario III: Kondisi WSN dengan serangan Hello Flood, IDS dan shutdown sink node

Pada skenario III mengimplementasikan *signature based* IDS yang diberikan mitigasi berupa sistem *shutdown* pada *sink node.*

5. Pengujian dan Analisis Sistem

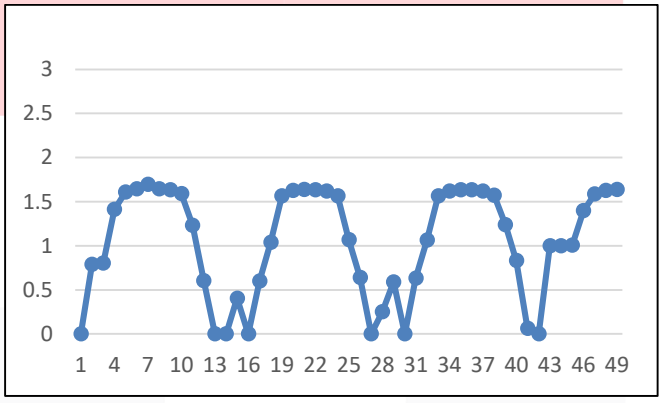
5.1 Skenario I: Kondisi WSN tanpa adanya serangan Hello Flood

Hasil simulasi skenario I dapat dilihat pada Gambar 3, hasil yang diperoleh diantaranya adalah nilai *throughput* sebesar 100.31kbps menunjukkan kualitas jaringan yang sangat baik, nilai *delay* sebesar 100 menunjukkan kualitas jaringan yang sangat baik, nilai *packet loss* sebesar 1.89% menunjukkan kualitas jaringan yang sangat baik menurut TIPHON. Kesimpulan yang diperoleh dari skenario I tersebut adalah jaringan WSN memiliki performa yang sangat baik dilihat dari *throughput*, *delay* dan *packet loss*.



Gambar 3 Grafik QoS Skenario I

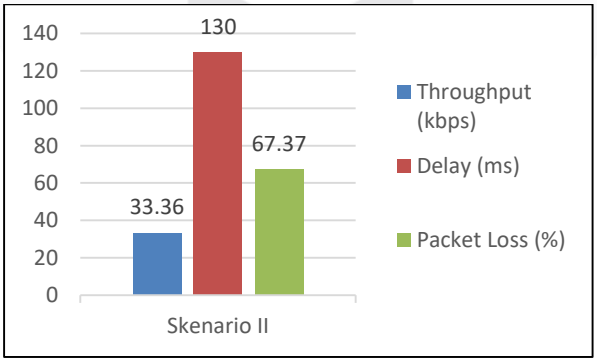
Gambar 4 menunjukkan sisa energi tiap *node* pada skenario I dengan tanpa adanya seranga. Terdapat tujuh *node* yang tidak memiliki sisa energi, yaitu *node* 1, *node* 8, *node* 15, *node* 16, dan *node* 23.



Gambar 4 Grafik energi pada skenario I

5.2 Skenario II: Kondisi WSN dengan serangan Hello Flood dan IDS

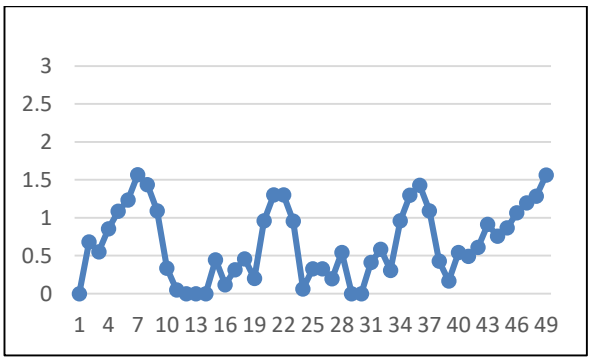
Pada skenario II, throughput dari skenario II yang telah diuji., throughput yang didapatkan pada hasil Skenario II sebesar 33.36 kbps. Nilai throughput yang diperoleh pada skenario II ini menurut standar TIPHON termasuk dalam kategori sedang. Delay yang dihasilkan 130 ms menunjukan bahwa kualitas delay pada saat serangan terjadi masih dalam kategori sangat baik. Packet loss yang dihasilkan 130 ms menunjukan bahwa kualitas delay pada saat serangan terjadi masih dalam kategori sangat baik.



Gambar 5 Grafik QoS Skenario II

grafik energi dari skenario II yang telah diuji. Pada skenario II, terdapat 6 node yang kehabisan energi, yaitu node 0, node 11, node 12, node 13, node 28 dan node 29. Node 0, node 11, node 12, node 13 tersebut kehabisan energi karena serangan hello flood membanjiri WSN dengan hello messages, sehingga paket

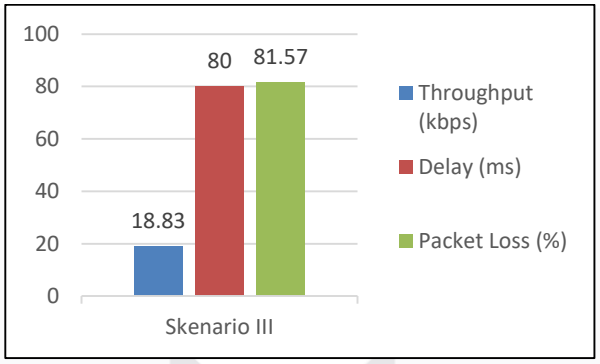
yang melewati jalur yang sudah tersedia tidak dapat lewat.



Gambar 6 Grafik energi pada skenario II

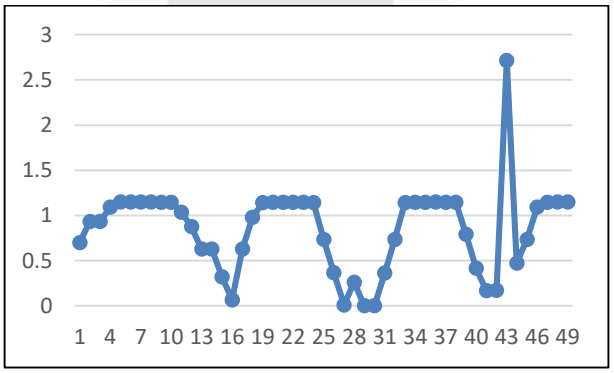
5.3 Skenario III: Kondisi WSN dengan serangan Hello Flood dan IDS dan shutdown sink node

Pada gambar 7, grafik throughput, delay, dan packet loss dari skenario III yang telah diuji. Nilai throughput yang didapatkan pada hasil skenario III ini sebesar 18.83 kbps. Nilai throughput yang diperoleh pada skenario III menurut standar TIPHON termasuk dalam kategori buruk. Nilai delay pada skenario III sebesar 80ms, hal ini terjadi karena pada saat IDS mendeteksi adanya serangan, system shutdown bekerja mematikan sink node, sehingga paket yang sampai ke sink node hanya paket yang dikirim sebelum system shutdown mematikan sink node, delay pada skenario III menurut TIPHON termasuk pada kategori sangat baik. Packet loss yang dihasilkan pada skenario III adalah 81.57%. Nilai packet loss meningkat dibandingkan dengan skenario sebelumnya, yaitu sebesar 67.37%. Peningkatan ini terjadi karena setelah setelah IDS mendeteksi adanya serangan, kemudian system shutdown bekerja, sehingga tidak ada paket yang terkirim ke sink node, yang menyebabkan packet loss lebih besar



Gambar 7 Grafik QoS pada Skenario III

Pada skenario III, terdapat 2 node yang benar-benar kehabisan energi, yaitu node 28 dan node 29. Hal ini terjadi karena node tersebut terus menerus mengirimkan hello messages, sehingga node 28 dan node 29 kehabisan energi. Pada skenario III ini WSN terdapat serangan dan IDS mendeteksi serangan tersebut. Pada skenario III system shutdown sudah dijalankan.



Gambar 8 Grafik energi pada skenario III

6. Kesimpulan

Setelah melakukan beberapa pengujian dan penelitian, dapat ditarik beberapa kesimpulan, yaitu :

1. Serangan *hello flood* mempengaruhi performa pada WSN. Pada skenario I saat WSN dalam keadaan normal tanpa serangan, IDS, dan *system shutdown* menghasilkan performa yang sangat memuaskan. Pada skenario II saat WSN dalam keadaan terkena serangan *hello flood* menghasilkan performa kurang memuaskan. Pada skenario III WSN dalam keadaan terkena serangan, kemudian IDS mendeteksi adanya serangan tersebut, dan *system shutdown* memitigasi serangan tersebut dengan cara mematikan *sink node*. Pada skenario III menunjukan performa yang buruk, tetapi dengan adanya *system shutdown* ini, WSN masih dapat diamankan dan data yang terkirim ke *sink node* tidak menyebabkan kesalahan pengambilan keputusan.
2. Pengamanan WSN dengan menggunakan IDS *Signature Based Approach* dapat diimplementasikan dengan baik ketika mendeteksi serangan *Hello Flood*. IDS *Signature Based Approach* hanya dapat memberikan *alert*, tetapi dengan adanya mitigasi dengan menggunakan *system shutdown*, maka serangan *hello flood* dapat di deteksi.
3. Pada serangan *hello flood, node hello flood* menyerang *node* lain sehingga energi yang dimiliki *node* di sekitar *node hello flood* berkurang dan lama kelamaan habis. Hal ini bisa diantisipasi dengan menggunakan IDS pada WSN untuk mendeteksi adanya serangan yang dilakukan oleh *node hello flood*. Jika hanya mendeteksi tanpa adanya mitigasi, tidak ada tindakan dari jaringan untuk mengamankan *sink node*. Oleh karena itu ditambahkan *system shutdown* pada pengujian ini agar WSN tidak hanya mendeteksi serangan menggunakan IDS, tetapi juga melakukan mitigasi menggunakan *system shutdown*. Meskipun indeks QoS menghasilkan indeks yang buruk, tetapi mitigasi menggunakan *system shutdown* berhasil.

Daftar Pustaka:

[1] I. Abdullah, M. Muntasir Rahman, and M. Chandra Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 3, pp. 50–56, 2015.

[2] T. Lupu and V. Parvan, "Main Types of Attacks in Wireless Sensor Networks," *WSEAS Int. Conf. Proceedings. Recent Adv. Comput. Eng.*, pp. 180–185, 2009.

[3] P. A. S. Ervices, M. Cesana, and P. Milano, "P Erformance E Valuation of Umts," vol. 17, no. 1, pp. 38–56, 2003.

[4] A. Dubey, D. Meena, and S. Gaur, "A Survey in Hello Flood Attack in Wireless Sensor Networks," vol. 3, no. 1, pp. 1882–1888, 2014.

[5] 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.

[6] V. PalSingh, A. S. Anand Ukey, and S. Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks," *Int. J. Comput. Appl.*, vol. 62, no. 15, pp. 1–6, 2013.

[7] N. Alrajeh, S. Khan, and B. Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," *... J. Distrib. Sens. Networks*, vol. 2013, 2013.

[8] S. S. D. O. J. Costa, "QoS (Quality of Service)," *Quality*, no. 08650101, pp. 29–55, 2006.

[9] Jonathan, P. A. (2011). Network Traffic Management, Quality of Services (QoS), Congestion Control dan Frame Relay, 12–24