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

WIRELESS SENSOR NETWORK SECURITY SYSTEM USING SIGNATURE BASED INTRUSION DETECTION SYSTEM AND SYSTEM SHUTDOWN FOR MITIGATING BLACKHOLE ATTACK

Ilham Akbar Siswanto[1], M. Teguh Kurniawan [2], Adityas Widjajarto [3]

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

Abstrak

Wireless Sensor Network (WSN) memiliki peran yang cukup besar dalam beberapa bidang seperti penerapan pada area peperangan, penerapan pada rumah pintar, penerapan pada mobil pintar, penelitian tentang lingkungan serta penerapan di bidang kesehatan. Namun WSN memiliki kekurangan dimana tidak adanya sistem keamanan bawaan yang tertanam pada perangkat *sensor* yang tersebar di ruang terbuka. Selain itu *sensor node* juga memiliki keterbatasan daya dan energi, akibatnya WSN sangat rentan terhadap serangan. Salah satu serangan yang dapat mengancam keamanan WSN adalah serangan *blackhole*. Maka dari itu di perlukan sistem untuk menjaga keamanan pada WSN. Dalam penelitian ini membahas cara atau metode untuk mendeteksi dan memitigasi serangan *blackhole*, yaitu dengan menggunakan *signature based Intrusion Detection System* (IDS) dan *system shutdown* pada *sink node*. *System shutdown* yang dibangun pada penelitian ini berhasil diimplementasikan pada WSN. Ketika IDS mendeteksi adanya serangan *blackhole*, *system shutdown* dapat mengamankan data pada *sink node* dengan cara mematikan *sink node* tersebut. Maka dari itu *system shutdown* dapat digunakan sebagai alternatif serta langkah awal dalam mengamankan WSN.

Kata kunci : WSN, *system shutdown*, IDS, *signature approach*, serangan *blackhole*

Abstract

Wireless Sensor Network (WSN) has a significant role in areas such as deployment in warfare areas, smart home deployment, smart car deployment, environmental research and healthcare applications. However, WSN has a deficiency in the absence of an innate security system that is embedded in a sensor device that is spread out in open space. In addition node sensors also have limited power and energy, consequently WSN is very vulnerable to attack. One of the attacks that could threaten the security of the WSN is the blackhole attack. Therefore in need of a system to maintain security on WSN. In this study discuss ways or methods to detect and mitigate blackhole attacks, namely by using the signature based Intrusion Detection System (IDS) and system shutdown on sink nodes. The system shutdown built in this research was successfully implemented on WSN. When IDS detects a blackhole attack, system shutdown can secure data on the sink node by shutting down the node's sink. Therefore the system shutdown can be used as an alternative as well as the initial step in securing WSN.

Keywords: WSN, *system shutdown*, IDS, *signature approach*, *blackhole attack*

1. Pendahuluan

Teknologi wireless memberikan banyak kemudahan dalam bertukar informasi secara nirkabel sehingga penggunaannya merambah ke berbagai bidang. Salah satu penerapan dari teknologi wireless yaitu pada Internet of Things (IoT). Secara umum IoT adalah konsep untuk menghubungkan perangkat-perangkat pintar (*smart object*), sehingga dapat berinteraksi dengan perangkat lain dan lingkungan melalui jaringan internet [1]. Salah satu teknologi yang digunakan pada IoT merupakan pemanfaatan dari *wireless* yaitu *Wireless Sensor Network* (WSN). WSN merupakan sekumpulan sensor otomatis yang tersebar di berbagai tempat, dimana pada setiap titik sensor dilengkapi dengan alat komunikasi *wireless*. Sensor-sensor ini bekerja bersama-sama untuk melakukan pemantauan kondisi lingkungan sekitar seperti suhu, suara, getaran, tekanan, dan lain-lain. Namun WSN memiliki beberapa kekurangan yaitu tidak adanya sistem keamanan bawaan yang tertanam pada node sensor yang tersebar di ruang terbuka. Selain itu node sensor juga memilki keterbatasan memory, energi dan kemampuan komputasi [2].

Salah satu serangan yang mengancam keamanan WSN adalah serangan blackhole. Serangan b*lackhole* merupakan salah satu serangan yang terjadi ketika penyerang menangkap dan memprogram ulang satu set *node* dalam jaringan untuk memblokir paket data yang mereka terima tanpa meneruskannya ke stasiun pusat. Akibatnya setiap informasi yang masuk ke wilayah *blackhole* akan terperangkap dan tidak akan sampai ke tujuan [3].

Solusi untuk mengantisipasi terjadinya serangan *blackhole* ini adalah dengan menerapkan *Intrusion Detection System* (IDS) pada WSN menggunakan *signature approach* pada WSN. Sehingga ketika salah satu node menunjukan ciri-ciri dari serangan *blackhole*, maka IDS memberikan peringatan bahwa telah terdeteksi serangan *blackhole*. Namun IDS hanya dapat memberikan peringatan saja, maka dari itu diusulkan sebuah sistem untuk memitigasi serangan *blackhole* ini. Usulan yang diajukan ini adalah menambahkan fitur *system shutdown*. *System shutdown* berfungsi untuk mematikan *sink node* yang merupakan penghubung *node* sensor dan *application layer* diatasnya. Sehingga ketika terjadi serangan *blackhole* pada WSN dan terdeksi oleh IDS menggunakan *signature approach*, *system shutdown* langsung mematikan *sink node* untuk menghindari kesalahan 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*) [4].

2.2 Serangan Blackhole

Serangan *blackhole* merupakan salah satu serangan yang terjadi ketika penyerang menangkap dan memprogram ulang satu set *node* dalam jaringan untuk memblokir atau menyerap paket data yang mereka terima tanpa meneruskannya ke stasiun pusat. Dalam serangan *blackhole*, *node* jahat menyatakan bahwa dirinya memiliki jalur terpendek dan menarik semua lalu lintas data ke arah dirinya sendiri [3].

Mekanisme dalam serangan *blackhole* berawal ketika *node* sumber memulai proses penentuan rute dengan mem-*broadcast* paket *Route Request* (RREQ) ke *node* tetangganya. Seluruh *node* tetangga yang menerima RREQ kemudian meneruskannya ke arah tujuan dengan menambahkan alamat mereka. *Node* jahat mengirimkan paket *Route Reply* (RREP) palsu dengan *squence number* teringgi dan jumlah *hop* paling sedikit sebagai respon terhadap *node* sumber, sehingga ia dapat berpura-pura menjadi *node* tujuan. Apabila *node* sumber menerima lebih dari satu respon, maka ia mulai membandingkan *squence number* RREP yang diterima. Jika kedua RREP memiliki *squence number* yang sama maka yang memiliki jumlah *hop* paling sedikit yang dipilih. Karena RREP dari *node* jahat memiliki *squence number* terbesar, maka *node* sumber mengirimkan semua paket data kepada *node* tersebut. Hal ini mengakibatkan *node* sumber dan *node* tujuan tidak dapat berkomunikasi [5].

2.3 Intrusion Detection System

Intrusion Detection System (IDS) merupakan sebuah sistem yang melakukan pengawasan terhadap lalulintas jaringan dan pengawasan terhadap kegiatan-kegaitan yang mencurigakan didalam sebuah sistem jaringan yang dimonitor dan dilaporkan ke *administrator* atau bagian manajemen jaringan[2]. 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. Pada penelitian ini menggunakan IDS berbasis *signature approach*.

IDS berbasis *signature approach*, juga dikenal sebagai IDS berbasis pola, memiliki aturan yang telah ditetapkan mengenai berbagai serangan keamanan. Apabila perilaku jaringan menunjukkan adanya penyimpangan dari peraturan yang telah ditetapkan, maka tindakan tersebut diklasifikasikan sebagai serangan [9].

2.4 Quality of Service

Quality of Service atau QoS merupakan tolok ukur yang digunakan untuk menghitung kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan *bandwidth*, mengatasi *jitter* dan *delay* [6]. QoS didesain agar performa yang didapatkan sesuai dengan kebutuhan pengguna dalam menjalankan aplikasi pada jaringan [7].

Tabel 1 Indeks parameter QoS

Nilai	Presentase (%)	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) Delay

Delay adalah waktu tunda paket yang disebabkan oleh proses transmisi dari satu titik asal ke titik tujuan. Waktu tunda mempengaruhi QoS kerena menyebabkan paket lebih lama mencapai tujuan. Waktu tunda yang direkomendasikan oleh TIPHON tidak lebih besar dari 150ms untuk berbagai aplikasi dan dengan memiliki batas 300ms untuk komunikasi suara [7].

$$Rata - rata\ delay = \frac{Total\ waktu}{Total\ paket\ yang\ diterima} \quad (1)$$

Berikut ini rekomendasi waktu delay berdasarkan standar TIPHON dibagi berdasarkan tingkat kenyamanan pengguna.

Tabel 2 Kategorisasi *Delay*

Delay	Kualitas	Index
< 150 ms	Sangat Baik	4
150 s/d 300 ms	Baik	3
300 s/d 450 ms	Sedang	2
> 450ms	Buruk	1

b) Packet Loss

Packet Loss merupakan jumlah paket data yang hilang per detik yang disebabkan oleh faktor-faktor di antaranya: penurunan sinyal media jaringan, paket *corrupt* dan pengiriman data secara bersamaan dengan tujuan yang sama [8].

$$Packet\ Loss = \frac{(Paket\ dikirim - Paket\ diterima)}{Paket\ dikirim} \times 100\% \quad (2)$$

Berikut ini standar TIPHON dalam mengkategorikan *packet loss*.

Tabel 3 Kategorisasi Packet Loss

Kategori	Packet Loss	Index
Sangat Baik	0 %	4
Baik	3 %	3
Sedang	15 %	2
Buruk	25 %	1

c) Throughput

Throughput merupakan *bandwidth* aktual diukur dari kedatangan paket menuju tujuan dengan kecepatan data yang efektif dan diukur dalam satuan bps. *Throughput* menggambarkan jumlah *bit* yang berhasil dikirim pada suatu jaringan [8].

$$Throughput = \frac{Jumlah\ data\ dikirim}{waktu\ pengiriman\ data} \quad (3)$$

Berikut ini standar TIPHON dalam mengkategorikan nilai *throughput*.

Tabel 4 Kategorisasi *Throughput*

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

2.5 Sistem Shutdown

Intrusion Detection System (IDS) berbasis *signature approach* digunakan pada WSN untuk mendeteksi serangan *blackhole*. Langkah selanjutnya yang harus dilakuakan adalah memitigasi serangan pada WSN. Yaitu menggunakan *system shutdown* dengan cara mematikan *sink node* agar tidak mengirimkan informasi

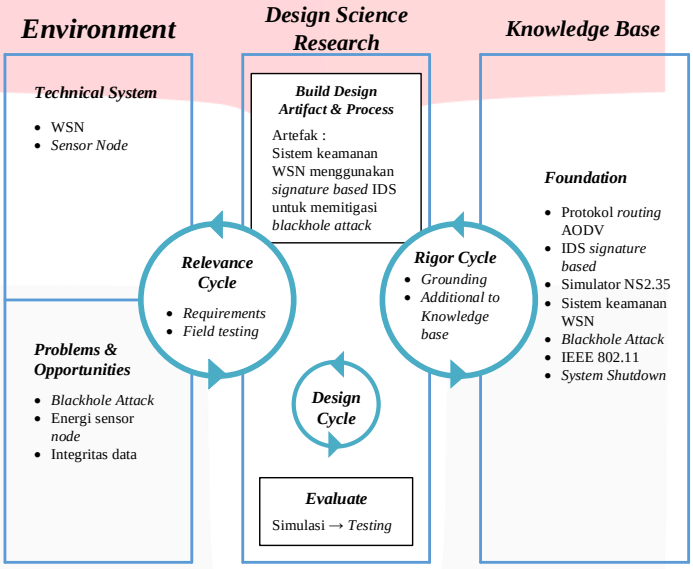
yang salah pada tingkat yang lebih tinggi. *System shutdown* awalnya digunakan untuk mematikan energi *node* pada WSN ketika *node* tidak melakukan aktivitas seperti *transmitting*, *receiving*, dan *idle* [10], namun pada penelitian ini *system shutdown* dimodifikasi sehingga dapat digunakan untuk memitigasi serangan yang terjadi.

System shudown diusulkan untuk menonaktifkan *sink node* ketika serangan *blackhole* terdeteksi. Hal ini dilakukan agar tidak terjadi kesalahan dalam pengambilan keputusan pada level yang lebih tinggi. Ketika *sink node* mati maka *administrator* dapat melakukan pemeriksaan *node* manakah yang menyebabkan serangan *blackhole* dan dapat ditangani secepatnya. Dengan demikian diharapkan keamanan pada WSN dapat menjadi lebih baik. *System shutdown* yang ada saat ini hanya digunakan dalam mengefisiensikan energi pada *node* sensor. Sehingga penggunaan fitur *system shutdown* untuk mengamankan WSN merupakan usulan baru dan juga sebagai solusi alternatif dalam mendeteksi dan memitigasi serangan *blackhole*.

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 dengan mengimplementasikan sistem *shutdown* yang diterapkan pada penelitian ini.



Gambar 1 Model Konseptual

4. Perancangan *Hardware* dan *Software*

4.1 Perancangan Sistem

Untuk melakukan pengujian sistem, terlebih dahulu dilakukan identifikasi arsitektur yang terdiri dari spesifikasi *hardware* dan *software* yang digunakan dalam pengujian. Dari spesifikasi software dan hardware pada tabel 5 telah cukup mempuni untuk melakukkan penelitian ini. Selain dapat melakukan pengujian sistem, dengan spesifikasi tersebut juga bisa untuk melakukan pengolahan hasil dari penelitian.

Tabel 5 Spesifikasi *Hardware* dan *Software*

Komponen	Informasi	
Hardware	*Processor*	Intel® Core ™ i3 1.80GHz
	RAM	4 GB
	Hard drive	50 GB
Software	Sistem Operasi	Ubuntu 16.04
	Simulation tool	Ns-*allinone*-2.35
	Analysis tool	Awk, Microsoft Exel
	Editor	Gedit, Microsoft Word 2013, Eclipse Oxygen
	Pemetaan *node*	NSG2.1

4.2 Parameter sistem

4.2.1 Parameter penelitian

Pengujian pada penelitian ini menggunakan beberapa parameter di antaranya :

Tabel 6 Parameter Penelitian

Parameter Penelitian	
Luas area	1000m x 1000m
Jumlah *node*	49
Jarak *node*	100m
Ukuran paket	1000 byte
Protocol transmisi	UDP
Trafik aplikasi	CBR
Waktu simulasi	50 detik
Model propagasi	Two ray ground
Tipe antrian / queue	Drop tail
Model antena	Omni Antenna
Protocol 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
Jenis Serangan	Blackhole

Parameter yang ditampilkan pada tabel 6 ini digunakan sebagai variabel tetap pada pengujian sistem.

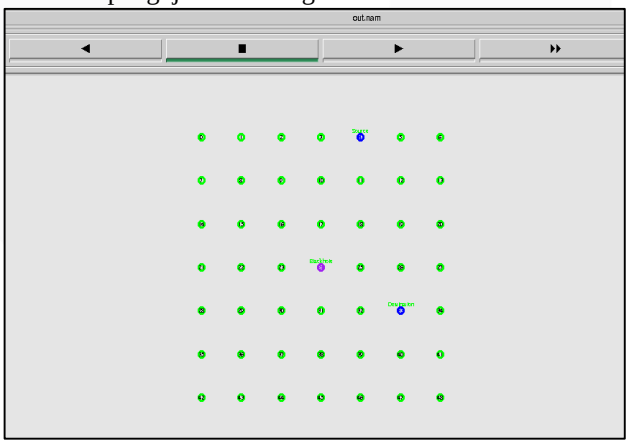
4.2.2 Parameter pengukuran

Terdapat beberapa parameter pengukuran yang digunakan untuk menentukan apakah sistem keamanan yang dirancang memiliki performa yang baik, diantaranya adalah *packet loss*, *delay*, *throughput*, dan energi.

4.3 Perancangan topologi

Topologi yang digunakan dalam pengujian ini adalah topologi grid yang digunakan untuk mempermudah dalam melihat rute pengiriman paket. Terdapat 49 node yang tersebar pada daerah seluas 1000 meter x 1000 meter dimana node 33 berperan sebagai sink node. Dalam penempatan node diperhatikan kemampuan jangkauan setiap node agar penggunaan routing AODV dapat berjalan.

Topologi yang digunakan dalam pengujian ini sebagai berikut :



Gambar 2 Topologi pengujian

4.4 Skenario pengujian

4.4.1 Skenario I

Pada skenario I ini menjalankan WSN tanpa serangan dan tanpa menggunakan IDS serta sistem usulan yaitu system shutdown. Hal ini dilakukan untuk melihat wsn dalam kondisi normal.

4.4.2 Skenario II

Pada skenario II ini menjalankan WSN dengan adanya serangan blackhole yang telah ditanamkan sejak awal pengujian berjalan, namun tanpa menggunakan IDS dan system shutdown. Hal ini dilakukan untuk melihat pengaruh yang dihasilkan oleh serangan yang ada.

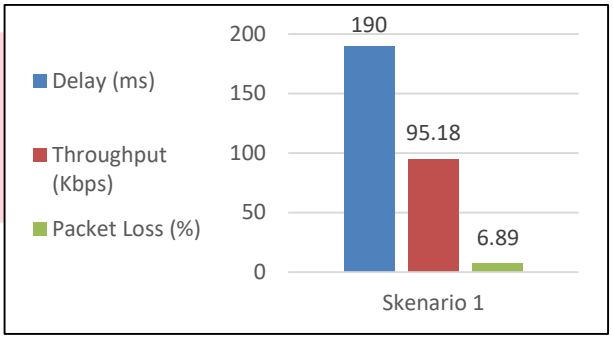
4.4.3 Skenario III: Kondisi WSN dengan serangan DoS/IDS dan shutdown sink node

Pada skenario III ini menjalankan WSN dengan mengimplementasikan IDS, system shutdown dan serangan blackhole. Hal ini dilakukan untuk melihat bagaimana kinerja dari sistem usulan dalam memitigasi serangan blackhole.

5. Pengujian dan Analisis Sistem

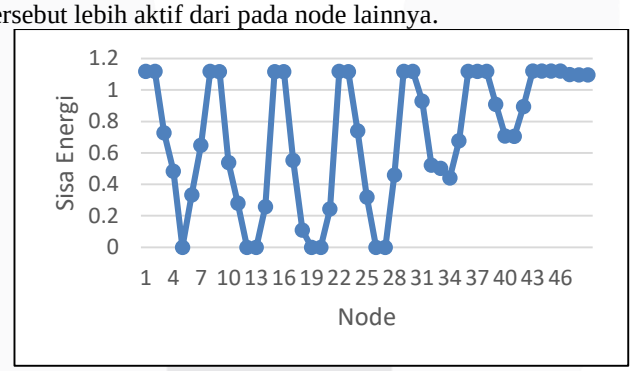
5.1 Skenario I

Hasil dari pengujian menggunakan skenario I ditunjukan oleh gambar 3, hasil yang diperoleh adalah *delay* sebesar 0.19 s atau 190 ms, *throughput* sebesar 95.18 kbps dan *packet loss* sebesar 6.89%. . Nilai delay dari skenario ini terbilang cukup besar menurut standar TIPHON dimana delay yang baik adalah nilainya dibawah 150 ms, sehingga nilai delay dari skenario ini masuk dalam kategori sedang. Menurut standar TIPHON nilai throughput dari skenario ini masuk dalam kategori sangat baik karena memiliki nilai diatas 75%. Nilai packet loss yang didapat masuk dalam kategori baik menurut standar TIPHON karena memiliki nilai dibawah 15%.



Gambar 3 Grafik QoS pada Skenario I

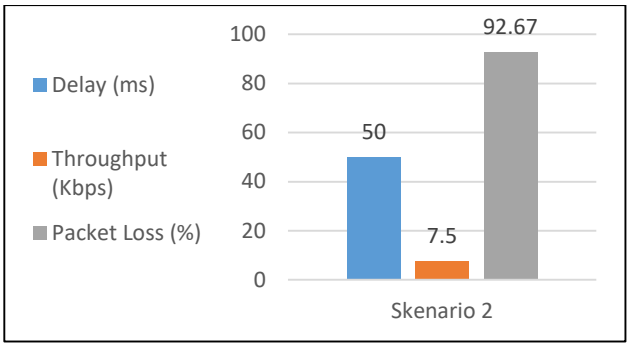
Pada gambar 4 menunjukan sisa energy dari setiap node setelah dilakukan pengujian skenario I. dapat dilihat sisa energi dari setiap node pada skenario ini cukup bervariasi dan terdapat 7 buah node yang kehabisan energi. Node yang kehabisan energi ini merupakan node yang menjadi jalur pengiriman paket, sehingga node-node tersebut lebih aktif dari pada node lainnya.



Gambar 4 Grafik Sisa Energi pada Skenario I

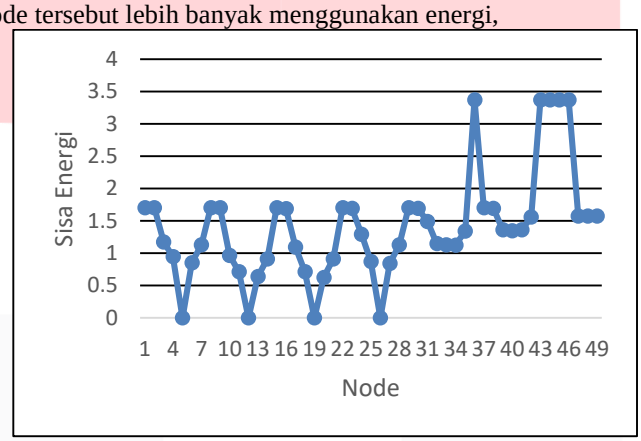
5.2 Skenario II

Dari pengujian skenario II yang dilakukan menunjukan hasil pengukuran seperti pada gambar 5. Delay yang dihasilkan dari skenario ini sebesar 0.05 s atau 50 ms. Dari hasil yang didapat nilai delay pada skenario ini masuk dalam kategori sangat baik menurut standar TIPHON karena nilainya lebih kecil dari 150 ms. Nilai *throughput* yang dihasilkan dari skenario ini sebesar 7.5 kbps . Menurut standar TIPHON nilai tersebut masuk dalam kategori buruk karena nilainya dibawah 25%. Nilai packet loss yang dihasilkan dari skenario ini sebesar 92.67%. banyaknya paket yang hilang atau tidak sampai ke tujuan ini terjadi karena node blackhole yang menarik atau menyerap semua paket yang ada. Hanya beberapa paket saja yang berhasil terkirim yaitu ketika node blackhole kehabisan energinya. Menurut standar TIPHON nilai packet loss pada skenario ini masuk dalam kategori buruk karena nilainya diatas 25%.



Gambar 5 Grafik QoS pada Skenario II

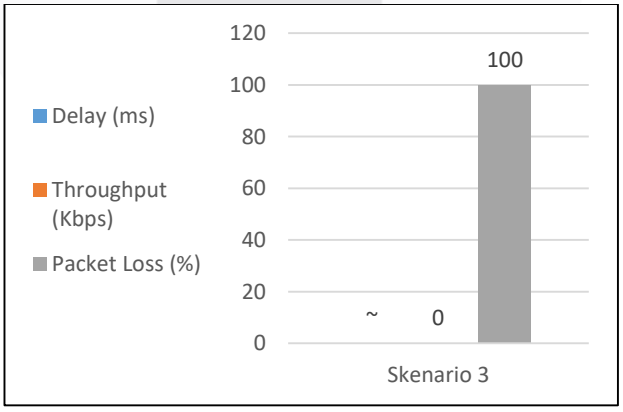
Pada gambar 6 menunjukan grafik sisa energi pada setiap node untuk pengujian menggunakan skenario II dengan satuan joule (J). Dari grafik dapat dilihat bahwa sisa energi pada skenario ini cukup bervariasi karena perbedaan keaktifan node itu sendiri. Terdapat 4 buah node yang kehabisan energi yang merupakan jalur pengiriman paket yang digunakan pada skenario ini yaitu jalur menuju node blackhole. Karena node blackhole menyerap atau menarik semua paket yang ada, node-node yang berada di sekitar node blackhole dan node sumber yang menjadi lebih aktif. Akibatnya node-node tersebut lebih banyak menggunakan energi,



Gambar 6 Grafik Sisa Energi pada Skenario II

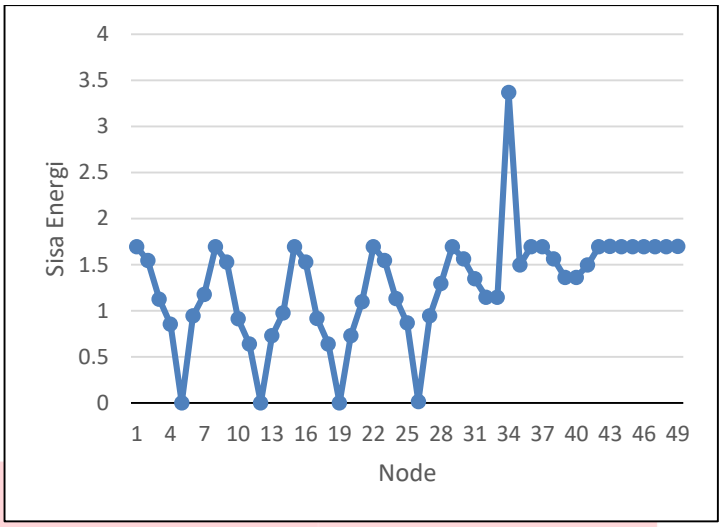
5.3 Skenario III

Dari pengujian skenario III menunjukan hasil seperti pada gambar 7. Pada skenario ini tidak ada paket yang sampai pada node tujuan. Hal ini terjadi karena node blackhole menyerap semua paket yang ada. Ketika node blackhole kehabisan energi, paket tidak dapat terkirim ke node tujuan karena node tersebut telah dimatikan oleh system shutdown yang telah diimplementasikan untuk mengamankan data dan mencegah kesalahan dalam pengambilan keputusan pada application layer. Akibatnya delay yang dihasilkan menjadi tidak terdefinisi, throughput yang dihasilkan sebesar 0 kbps dan packet loss yang dihasilkan sebesar 100%.



Gambar 7 Grafik QoS pada Skenario III

Pada gambar V.3.3 menunjukan grafik sisa energi dari setiap node untuk pengujian menggunakan skenario III dengan satuan joule (J). Dari grafik dapat dilihat sisa energi pada skenario ini sedikit berbeda, karena pada node 33 yang merupakan sink node sekaligus node tujuan sisa energi yang dimiliki masih banyak. Hal ini terjadi karena pada skenario ini system shutdown telah diimplementasikan dan ketika IDS mendeteksi adanya serangan sink node dimatikan. Namun node lain masih berkerja sesuai dengan kondisi yang ada. Yaitu node blackhole yang menyerap atau menarik paket yang ada sehingga node yang letaknya disekitar node blackhole menjadi lebih aktif.



Gambar 8 Grafik Sisa Energi pada Skenario III

5.4 Analisis Hasil Pengujian

Dari pengujian yang telah dilakukan, parameter pengujian dapat dikelompokan berdasarkan standar dari TIPHON menjadi sangat baik, baik, sedang dan buruk. Berikut ini pengelompokan parameter uji dari setiap skenario pengujian :

Tabel 7 Pengelompokan Parameter Uji dari Skenario I

Skenario I	Sangat Baik	Baik	Sedang	Buruk	Node Mati	Indeks
Delay		v				3
Throughput	v					4
Packet Loss		v				3
Indeks QoS						3,33
Energi		v			7	-

Pada tabel 7 menunjukan hasil indeks QoS sebesar 3.33 yang berarti QoS dari skenario I masuk dalam kategori memuaskan.

Tabel 8 Pengelompokan Parameter Uji dari Skenario II

Skenario II	Sangat Baik	Baik	Sedang	Buruk	Node Mati	Indeks
Delay	v					4
Throughput				v		1
Packet Loss				v		1
Indeks QoS						2
Energi	v				4	-

Pada tabel 8 menunjukan hasil indeks QoS sebesar 2 yang berarti QoS dari skenario II masuk dalam kategori kurang memuaskan.

Tabel 9 Pengelompokan Parameter Uji dari Skenario III

Skenario III	Sangat Baik	Baik	Sedang	Buruk	Node Mati	Indeks
Delay				v		1
Throughput				v		1
Packet Loss				v		1
Indeks QoS						1
Energi	v				4	-

Pada tabel 9 menunjukan hasil indeks QoS sebesar 1 yang berarti QoS dari skenario III masuk dalam kategori buruk.

6. Kesimpulan

1. Dalam pengujian pengamanan *Wireless Sensor Network* ini, *Intrusion Detection System signature approach* dapat mendeteksi serangan *blackhole* dengan baik serta memberikan *alert*. Namun IDS hanya mendeteksi dan memberikan peringatan tanpa melakukan tindakan pengamanan.
2. Kinerja WSN setelah mengimplementasikan IDS *based on signature approach* dan *system shutdown* pada skenario I menunjukan performa yang memuaskan dengan indeks QoS sebesar 3,33. Pada

skenario II menunjukan performa yang kurang memuaskan dengan indeks QoS sebesar 2. Pada skenario III menunjukan performa yang buruk dengan indeks QoS sebesar 1, namun berhasil mengamankan data pada *sink node.*

3. Penerapan IDS dan *system shutdown* pada WSN dapat dilakukan dengan melakukan *shutdown* pada *sink node* ketika terjadi serangan. *System shutdown* dapat mengamankan *sink node* yang merupakan penghubung sensor dengan admin sebagai pengambil keputusan. Tetapi *system shutdown* tidak berpengaruh banyak kepada serangannya. Namun *system shutdown* dapat menjadi alternatif pertolongan pertama yang dapat dilakukan dalam mengamankan WSN.

UCAPAN TERIMAKASIH

Daftar Pustaka:

[1] Meutia, E. D. (2015). Internet of Things – Keamanan dan Privasi. Seminar Nasional Dan Expo Teknik Elektro 2015, 85–89.

[2] Ioannou, C., Vassilioi, & Sergiou, C. (2017). An Intrusion Detection System for Wireless Sensor Network. IEEE, 5.

[3] Rathiga, & Sathappan. (2016). Hybrid Detection of Black hole and Gray hole attacks in MANET.

[4] Dinata, Y. M. (2015). Rancangan Bangun Wireless Remote Sensing Sistem untuk Memantau Temperatur dengan Menggunakan Protokol ZigBee.

[5] Ghugar, U., & Pradhan, J. (2017). A Study on Black Hole Attack in Wireless Sensor Networks.

[6] Jonathan, P. (2011). Network Traffic Management, Quality of Services (QoS), Congestion Control dan Frame Relay.

[7] Darmawan, Alif, & Basuki. (2013). Analisis Qos (Quality of Service) Pada Jaringan Internet.

[8] Farizi, M. (2014). Analisis Perbandingan Kinerja Codec H.264 Dan Codec Dirac Untuk Kompresi Live Streaming Pada Perangkat Nsn Flexi Packet Radio(Aplikasi Pada Laboratorium Sistem Komunikasi Radio FT-USU).

[9] Alrajeh, N. A., Khan, & Shams, B. (2013). Intrusion Detection System in Wireless Sensor Network: A Review.

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