MENGATASI SERANGAN *SYBIL* PADA TEKNOLOGI *WIRELESS SENSOR NETWORK* MENGGUNAKAN PROTOKOL *ROUTING* AODV DENGAN SISTEM *SHUTDOWN*

PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK USING AODV ROUTING PROTOCOL WITH SHUTDOWN SYSTEM

Dicky Naofal Rizaldi[1], M Teguh Kurniawan[2], Adityas Widjajarto3[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]**dickynaofal@student.telkomuniversity.ac.id**, [2]**mtk@telkomuniveristy.ac.id**,
[3]**adtwjrt@telkomuniversity.ac.id**

Abstrak

Wireless Sensor Network (WSN) merupakan sebuah teknologi dengan menggunakan jaringan nirkabel yang terdiri dari beberapa sensor node dengan komponen satu embedded platform yang saling terintegrasi. Pada implementasinya, sensor node diletakkan di lingkungan yang dapat diakses secara real-time, sehingga dapat terjadinya serangan secara langsung. Serangan WSN pada network layer bertujuan untuk mencuri paket atau memodifikasi beberapa informasi routing yang dapat meyebabkan jalur routing terganggu. Berdasarkan kondisi WSN yang rentan terhadap serangan, maka dibutuhkan adanya mitigasi serangan pada WSN dengan sistem shutdown. Hal ini bertujuan untuk mematikan komunikasi secara langsung sebelum informasi tersebut di proses oleh sistem. Penelitian ini dilakukan uji konsumsi energi dan performansi dengan protokol routing AODV yang diberikan serangan sybil dan sistem shutdown menggunakan software NS-2.35. Performansi jaringan yang diukur adalah jumlah packet delivery ratio, throughput, end to end delay. Selain performansi jaringan juga diukur energy consumption. Dari hasil yang diperoleh dapat diketahui bahwa serangan sybil menurunkan performansi jaringan pada packet delivery ratio dan throughput sedangkan performansi jaringan pada delay mengalami kenaikan, dengan penurunan packet delivery ratio yaitu 0.26 %, penurunan throughput 0.26 kbps, lalu delay yang mengalami penaikan sebesar 3000 ms. Hasil tersebut terjadi pada skenario ada serangan dan tanpa mengimplementasikan sistem shutdown menggunakan protokol AODV dengan jumlah node 100. Sedangkan nilai dari konsumsi energi pada sistem shutdown memiliki nilai yang lebih sedikit dibandingkan pada saat tanpa serangan dan ada serangan. Karena energi yang dikonsumsi hanya berasal dari node yang terletak di jalur routing terbaik pada saat melakukan discovery route. Dengan adanya sistem shutdown serangan sybil dapat dihadapi, tetapi penerapan sistem shutdown tidak menurunkan dan menggangu performansi jaringan pada WSN.

Kata Kunci : Wireless sensor network, serangan sybil, AODV, sistem shutdown

Abstract

Wireless Sensor Network (WSN) is a technology using wireless networking that consist of several embedded platform sensor nodes integrated to each other. In the implementation, the sensor nodes are placed in the areas that can be accessed real-time. So that attack may occur directly. WSN attack on network layer is to steal packages or to modify some routing information that can disturb routing lines. Based on WSN vulnerable condition, it needs mitigation attacks on WSN by system shutdown. This is to shutdown communication directly before the information is processed in the system. The research tested the energy consumption and network performance with AODV routing protocol given sybil attack and shutdown system using NS-2.35 software. Network performance measured was the amount of packet delivery ratio, through put, end to end delay. Besides that, energy consumption was also measured. The results showed on that the sybil attack decrease the wireless performance on packet delivery ratio and throughput while wireless performance on delay increase, decrease on Packet Delivery Ratio by 0,26%, decrease on throughput by 0,26 kbps, and increase on delay by 3000 ms. The result showed on scenario of attack occurrence without implementing shutdown system using AODV protocol with node of 100. Energy consumption rate is lower than attack occurrence and nonoccurrence. Because, the energy consumed comes only from the node in the best routing line at discover route. Sybil attacks can be tackle by shutdown system, but the implementation does not decrease on disturb the WSN performance.

Keywords: ***Wireless sensor network, sybil attack, AODV, shutdown system***

1. Pendahuluan

Saat ini kemajuan di dunia teknologi informasi semakin pesat, karena semakin tingginya kebutuhan manusia akan *internet*. Dengan adanya *internet* memungkinkan penggunaan komputer akan mendominasi pekerjaan manusia dan mengalahkan kemampuan komputasi manusia seperti dengan mengontrol peralatan elektronik dari jarak jauh yang disebut dengan *Internet of Things* (IoT). Hal ini terbukti dari penggunaan beberapa teknologi IoT pada pengembangan dan pertumbuhan di berbagai domain aplikasi yang secara garis besar terintegrasi seperti sensor sebagai pembaca data dan *wireless* untuk koneksi *internet.* Teknologi Informasi tersebut adalah *Wireless Sensor Network.* *Wireless Sensor Network* berkomunikasi menggunakan sensor yang ada pada setiap *node*, dimana setiap data akan dikirim/diterima menggunakan *transceiver* dengan protokol IEEE 802.15.4 kepada *device* yang lain. *Wireless Sensor Network* memiliki arsitektur secara terpusat, hirarkis dan terdistribusi [1] yang memungkinkan untuk melakukan pemantauan disetiap aplikasi serta penerimaan data beserta informasinya secara *real-time*, berbasiskan *internet*, *remote* secara maksimal dengan jarak jauh tanpa harus mengakusisi data secara langsung di area sensor. disamping kelebihan dari WSN, WSN memiliki kelemahan yaitu masih sangat rentan terhadap serangan kerena dapat diakses secara fisik sehingga dapat memungkinkan meningkatnya potensi serangan secara langsung atau jarak jauh pada topologi WSN. Serangan pada WSN bertujuan untuk mendapatkan kerahasiaan dan otentikasi, ketersediaan layanan dan integritas data. Penelitian ini berfokus pada serangan yang terjadi di *Network Layer*, dimana *Network Layer* merupakan *layer* ketiga yang berhubungan dengan pengalamatan di dalam jaringan komputer berbasiskan *Internet Protocol* (IP *Address*) serta berperan di dalam proses *Routing* untuk penentuan rute yang harus ditempuh oleh paket data dari komputer pengirim ke komputer tujuan. *Network Layer* sangat rentan terhadap serangan, terutama pada proses *routing* yang memungkinkan jalur *routing* dirubah dan memalsukan informasi *routing* sehingga paket data tidak akan sampai ke tujuan. Salah satu serangan pada *Network Layer* adalah serangan *Sybil*, dimana penyerang akan mencoba memanipulasikan informasi *routing* dan kemudian mengalihkan *traffic* dengan memberikan informasi palsu atau melakukan *dropping* paket sehingga informasi tidak akan sampai ke tujuan.

Dalam memberikan aspek keamanan pada WSN, adapun tujuan keamanan pada *Wireless Sensor Network* yaitu *Confidentiality, Integrity, Availability,* dan *Authentication,* tanpa adanya salah satu aspek keamanan tersebut, maka *wireless sensor network* yang digunakan dapat dikategorikan rentan terhadap serangan *sybil*. Oleh karena itu, dalam penelitian ini penulis melakukan mitigasi serangan *sybil* pada *wireless sensor network* menggunakan *routing* AODV dengan sistem *shutdown*. Kemudian akan dilakukan analisis terhadap konsumsi energi dan performansi jaringan sebelum dan sesudah diberikan serangan dan sistem *shutdown*.

2. Tinjauan Pustaka

2.1 *Wireless Sensor Network*

Wireless Sensor Network (WSN) merupakan sebuah perangkat elektronik yang menggabungkan jaringan nirkabel, *sensor, microcontroller, memory,* sistem operasi, komunikasi radio dan sumber energi berupa baterai dalam satu *embedded platform* yang saling terintegrasi. [2] [3] [4]

Pengaplikasian mengenai Wireless Sensor Network (WSN) pertama kali di implementasikan pada aplikasi militer. Pada waktu itu, aplikasi jaringan sensor di bidang militer mencakup sistem pengawasan di laut berskala besar untuk mendeteksi kapal selam yang digunakan secara acak untuk pengawasan di medan perang dengan menggunakan *microsensor* [5]. Saat ini WSN telah mendapatkan popularitas yang cukup besar karena fleksibilitasnya di berbagai domain aplikasi sehingga WSN dapat berpotensi mengubah hidup manusia dengan memecahkan masalah dalam bidang apapun. WSN telah berhasil diterapkan dalam berbagai domain aplikasi seperti bidang militer, transportasi, aplikasi kesehatan, pertanian, dan lain-lain [6]**.**

2.2. Arsitektur *Wirelesss Sensor Network*

Pada arsitektur WSN, *sink* dapat berkomunikasi dengan *task manager* atau *end user* melalui *internet* atau satelit atau jenis jaringan nirkabel (seperti WiFi, sistem seluler dan WiMAX).

Secara umum terdapat beberapa komponen utama pada *wireless sensor network*, yaitu:

1. *Sensor node*
   Sensor node merupakan elemen utama yang ada dalam teknologi *Wireless Sensor Netowrk* (WSN) yang dapat merasakan, memproses dan berkomunikasi dalam mengeksekusi protocol komunikasi dan algoritma pemrosesan data melalui jaringan nirkabel yang menuju *gateway* dan *sink*.
2. *Sink Node*
   Sink node merupakan perangkat yang digunakan untuk mengumpulkan data atau informasi dari *sensor node* menuju ke *storage*. Selain itu *sink node* juga sebagai *gateway* informasi dari *sensor node*
3. *Internet*
   Internet dapat digunakan sebagai media penyimpanan berbasis *cloud*. Karena sebagian besar data dari *sink node* akan dikirimkan ke dalam pentimpanan data berbasis *cloud* dan akan diakses oleh *user* menggunakan komputer.

4. *User*
   User pada *wireless sensor network* dapat mengakses informasi *sensor node* melalui *remote server* secara *real time* dan dapat diakses menggunakan koneksi internet atau satelit.

2.2.1 Klasifikasi Persebaran Node pada Wireless Sensor Network

Persebaran *node* pada jaringan *wireless sensor network* diatur agar dapat melakukan proses *sensing* secara berkelanjutan dengan tujuan memperpanjang masa penggunaan. Pada persebaran *node* dilaukan pengaturan untuk mengurangi nilai redudansi, memperoleh konektivitas, dan mengurangi biaya pemeliharaan pada jaringan wsn. Pada WSN persebaran *node* dibagi menjadi dua, yaitu persebaran *static* dan persebaran *random* [7].

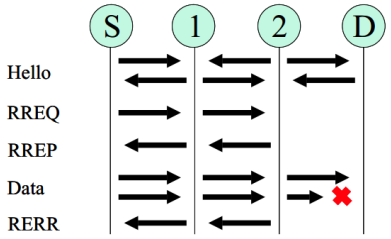
1. Persebaran *static*
   Memilih lokasi terbaik dilakukan persebaran *static* berdasarkan strategi optimasi dan lokasi *node* yang tetap tidak berpindah-pindah. Salah satu penerapan persebaran *static* pada *wireless sensor network* adalah persebaran *grid*, dimana area pada persebaran ini membentuk persegi dan memiliki jarak yang sama antar *node* satu dengan *node* yang lainnya.
2. Persebaran *random*
   Menempatkan *sensor node* secara *random* dilakukan oleh persebaran *random* tanpa memperhitungkan jarak antar *sensor node*. Persebaran *random* biasanya digunakan pada lingkungan yang berbahaya dengan *traffic* yang rendah, misalnya di kawasan pegunungan atau tempat yang sering terkena bencana alam.

2.2.2 Protokol Routing pada Wireless Sensor Network

Protokol *routing* pada *wireless sensor network* memiliki peran sangat penting yang digunakan untuk menentukan rute pengiriman data dari *sensor node* sumber ke *node* tujuan. AODV adalah protokol *routing* reaktif yang dapat didesain untuk *Wireless Sensor Network* (WSN) dan *Mobile Ad-Hoc Networks* (MANET). AODV dikembangkan oleh C.E. Perkins, E.M. Belding-Royer dan S. Das pada RFC 3561. Protokol *routing* AODV melakukan *routing* berdasarkan permintaan (*on-demand*) artinya rute dari *node* satu ke *node* lain akan dibuat jika *node* sumber menginginkan adanya pengiriman paket ke *node* tujuan yang dipilih. Pada AODV *node* akan menyimpan tabel *routing* hanya untuk satu rute. Jika jalur *routing* tidak digunakan pada waktu yang sudah ditentukan maka jalur *routing* akan dihapus dari tabel *routing* [8].

AODV memiliki dua fase, yaitu *route discovery* dan *route maintenance*. *Route discovery* terdapat proses *route request* (RREQ) dan *route reply* (RREP). Saat *node* sumber melakukan *route request*, *node* asal melakukan *broadcast* permintaan rute RREQ ke seluruh jaringan yang terhubung dengannya dimana disertakan nomor *sequence* tujuan. Ketika *node* tujuan menerima paket RREQ, *node* tersebut mulai memeriksa nomor *sequence* tujuan yang sampai ketika paket tiba dan memastikan bahwa nomor *sequence* sama dengan RREQ. [9].

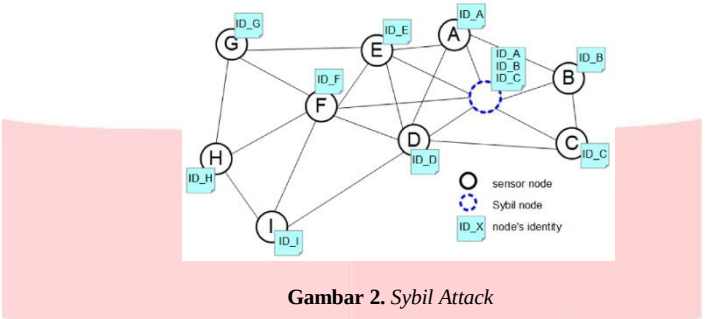
Protokol *routing* AODV menggunakan *destination sequence number* untuk menjaga informasi mengenai *reverse path* yang mengarah ke *source node*. *Reverse path* berfungsi agar *destination node* dapat mencapai *source node* yang nantinya akan dijadikan rute untuk pengiriman paket data. *Reverse Path* terbentuk saat RREQ menempuh *node* yang dituju, dimana setiap RREQ akan diidentifikasi dari *node* sekitar yang mengirimkan RREQ tadi. Selanjutnya jika rute sudah terbentuk, maka yang akan bertanggungjawab untuk menjaga rutenya adalah *source node*. Saat *node* yang dituju mempunyai informasi rute menuju *node* tujuan menerima paket RREQ, maka nilai *destination sequence number* yang ada pada RREQ akan dibandingkan. Apabila nilai *sequence number* pada RREQ lebih besar dari nilai yang ada pada *node* yang menerima, maka paket RREQ akan diteruskan lagi ke *node* sekitarnya [10]. Sebaliknya apabila nilai *destination sequence number* pada *node* penerima sama atau lebih besar dengan nilai di RREQ maka paket RREP akan dikirimkan oleh *node* tersebut kembali ke *source node* dengan memakai *reverse path* yang telah dibuat sebelumnya. Apabila terdapat kerusakan, maka *route maintenance* yang akan bekerja dengan cara mengirimkan paket *route error* (RERR) ke *node* yang mengalami kerusakan ke semua *node* yang ada pada jaringan sampai ke sumbernya lag [8].



Gambar 1. Proses Pencarian Rute AODV

2. 3 *Sybil Attack*

Serangan *Sybil* merupakan jenis serangan aktif yang terjadi di *Network Layer*, di mana *node* jahat dapat mengakusisi beberapa identitas asli dengan identitas palsu di jaringan *Wireless Sensor Network* yang dapat menyebabkan redudansi pada jaringan [11]. Serangan *Sybil* juga dapat disebut jenis serangan spoofing dimana *attacker* meniru suatu sistem pada jaringan Dengan diambilnya identitas tersebut, *node sybil* dapat bertindak seakan-akan merupakan bagian dari dalam jaringan tersebut dan mendapatkan perbuatan yang sama seperti node yang memiliki identitas yang dicurinya. Serangan *Sybil* bertujuan untuk mendapatkan beberapa informasi pada *node* dan merusak jalur *routing*. Secara khusus, jaringan pada *Wireless Sensor Network* lebih rentan terhadap serangan *Sybil* karena implementasi jaringan WSN pada area atau lingkungan yang terbuka sehingga dapat memungkinkan terjadi serangan *Sybil*



Gambar 2. *Sybil Attack*

2.5 Parameter Uji

Performansi suatu jaringan dapat diukur dengan menggunakan parameter *Quality of Service* (QoS) untuk mengetahui tingkat keberhasilan pengiriman data, menampilkan konsistensi, dan lain-lain [12]. Penelitian seluruh skenario pengujiuan sistem menggunakan beberapa parameter yang digunakan untuk mengukur performansi jaringan antara lain *packet delivery ratio*, *end to end delay*, dan *throughput*.

1. *Packet Delivery Ratio*
   Pengujian menggunakan parameter ini dilakukan untuk mengetahui berapa jumlah rasio antara banyaknya paket yang diterima oleh *node destination*. Perhitungan parameter *packet delivery ratio* adalah :

$$\text{PDR} = \frac{Jumlah\ paket\ yang\ diterima}{Jumlah\ paket\ yang\ dikirim} \text{ x } 100\% \text{..... (1.1)}$$

2. *End to end delay*
   Rata-rata waktu *delay* merupakan waktu yang dibutuhkan dalam jaringan untuk dapat menyampaikan informasi dari *source node* sampai ke *node* tujuan. Satuan pada *end to end delay* adalah ms (*milisecond*) Adapun rumus pada *end to end delay* adalah :

$$End\ to\ end\ delay = \frac{Total\ waktu}{Total\ paket\ yang\ diterima} \text{..... (1.2)}$$

Pada Tabel II.3 diperlihatkan kategori dari *end to end delay* menurut standar TIPHON:

Kategori *Delay*	Nilai *Delay* (ms)	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 – 300 ms	3
Sedang	300 – 450 ms	2
Buruk	> 450 ms	1

Tabel 1 Kategori Delay

3. *Throughput*
   Throughput adalah jumlah waktu yang diambil oleh paket untuk mencapai tujuan. *Throughput* dapat juga disebut dengan *bandwidth* dalam kondisi yang sebenarnya. *Throughput* mempunyai satuan Bps (*Bit per second*). Rumus untuk menghitung nilai *throughput* adalah:

$$Throughput = \frac{Jumlah\ data\ dikirim}{Waktu\ pengiriman\ data} \text{..... (1.3)}$$

Selain parameter yang digunakan untuk mengukur performansi jaringan, penelitian ini mengukur *energy consumption* untuk mengukur konsumsi energi pada saat sebelum atau sesudah diberikan serangan dan sistem *shutdown*.

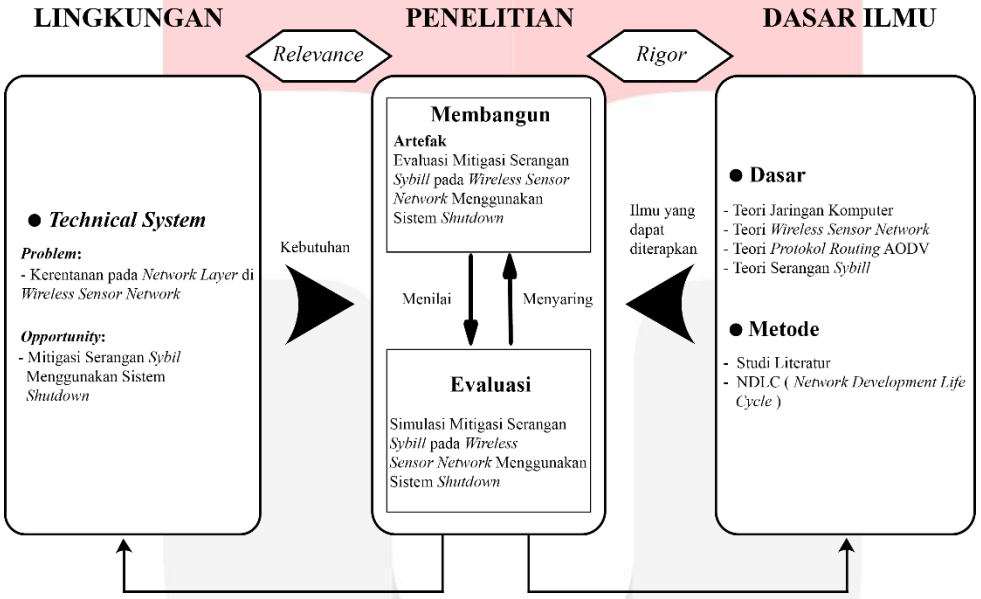
1. *Energy Consumption*
   Pengujian pada parameter ini bertujuan untuk mendapatkan nilai total konsumsi energi yang dibutuhkan untuk mengirim dan menerima paket dari *node* sumber ke *node* tujuan. Parameter ini memiliki satuan joule dalam mengukur. Jika jumlah konsumsi energi pada *node* semakin kecil, maka *node* yang digunakan akan semakin baik.

$$Jumlah\ Konsumsi\ Energi = \sum energi\ tiap\ node \quad \ldots\ldots\ldots(1.4)$$

3. Pengujian dan Analisis Sistem

3.1 Model Konseptual

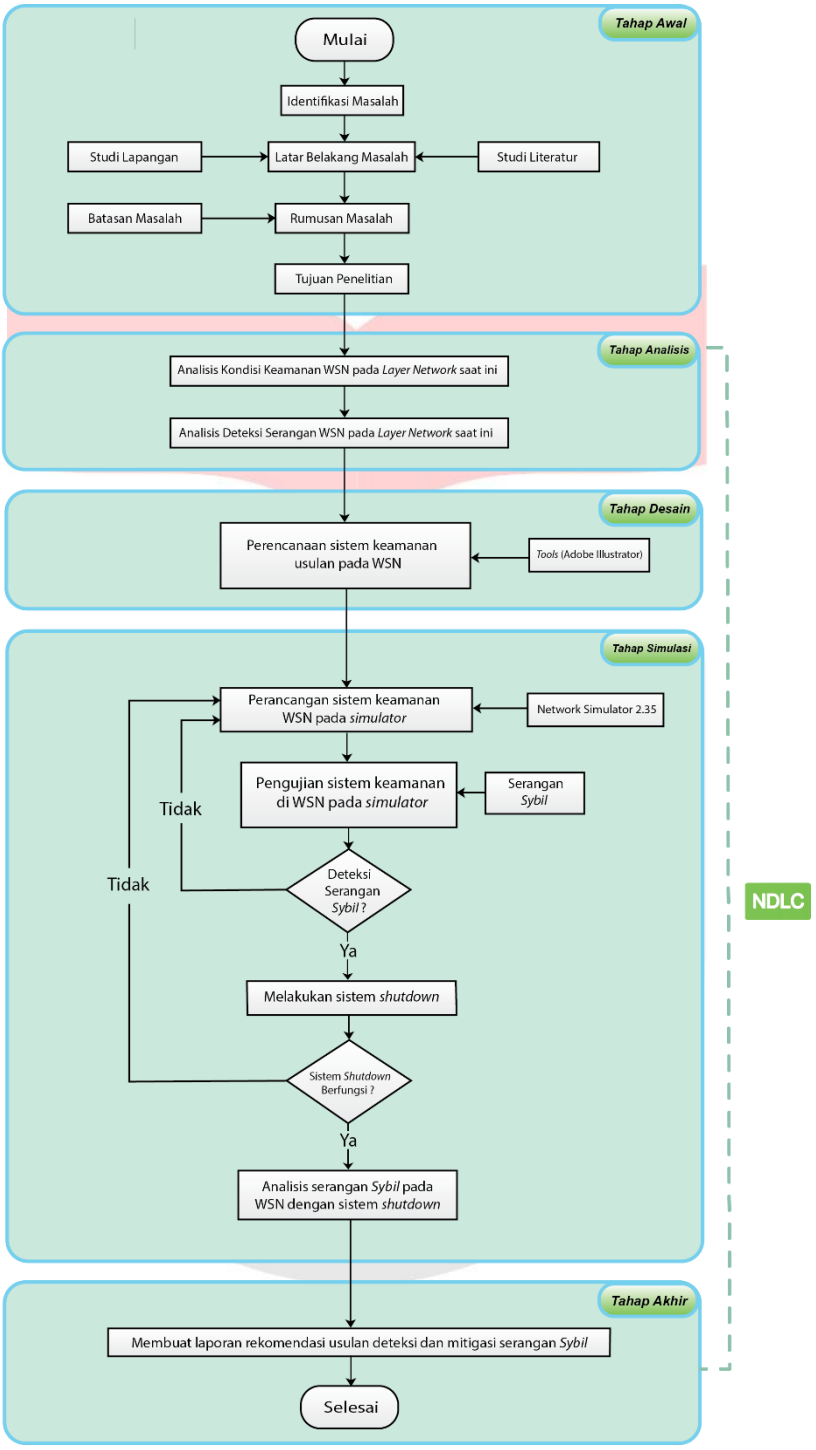
Model konseptual merupakan sebuah kerangka abstraksi dalam proses pemecahan model menjadi spesifik dalam melakukan penelitian dari kondisi sesungguhnya. Model konseptual bertujuan untuk membantu peneliti dalam mengidentifikasi data dalam suatu proses penelitian sehingga dapat merumuskan pemecahan masalah yang ada [13]. Selain membantu dalam merumuskan pemecahan masalah, model konseptual juga bertujuan untuk memberikan gambaran dalam mengidentifikasi faktor-faktor yang relevan, sehingga memberikan penjelasan dan solusi agar masalah yang ada dapat dipahami dengan mudah. Gambaran model konseptual penelitian ini terlihat pada Gambar 3.



Gambar 3 Model Konseptual Penelitian

3.2 Sistematika Penelitian

Sistematika penelitian merupakan penjabaran secara deskriptif tentang hal-hal yang dilakukan selama penelitian berlangsung. Tahapan yang dilakukan adalah tahap yang terdapat pada metode NDLC (*Network Development Life Cycle*), diantaranya: tahap awal, tahap analisis, tahap desain, dan tahap simulasi. Sistematika ilustrasi framework penelitian untuk pengembangan sistem dijelaskan pada Gambar 4.



Gambar 4 Sistematika Penelitian

4. Perancangan Sistem

4.1 Parameter Sistem

Simulasi jaringan *wireless sensor network* dilakukan menggunakan simulator *Network Simulator* versi 2.35. Daerah *sensor node* yang tersebar seluas 1000 x 1000 m^2 dengan topologi *grid*. Protokol *routing* yang digunakan adalah AODV (*Ad-hoc On-Demand Distance Vektor*) dengan waktu simulasi selama 120 detik dan *packet size* yang dikirim sebesar 1000 Bytes. *Transport agent* yang digunakan adalah UDP (*User Datagram Protocol*) dan *application agent* yang digunakan adalah CBR (*Constant Bit Rate*).

No	Parameter	Nilai
1	Simulator	NS-2.35
2	Waktu Simulasi	120 detik
3	Jumlah *node*	10, 25, 50, dan 100
4	*Routing protocol*	AODV
5	*Application Agent*	CBR
6	*Transport Agent*	UDP
7	Area Simulasi	1000 x 1000
8	Topologi	Grid
9	*Packet Size*	1000 Bytes
11	Jenis Serangan	*Sybi Attack*

Tabel 2. Parameter penelitian yang digunakan

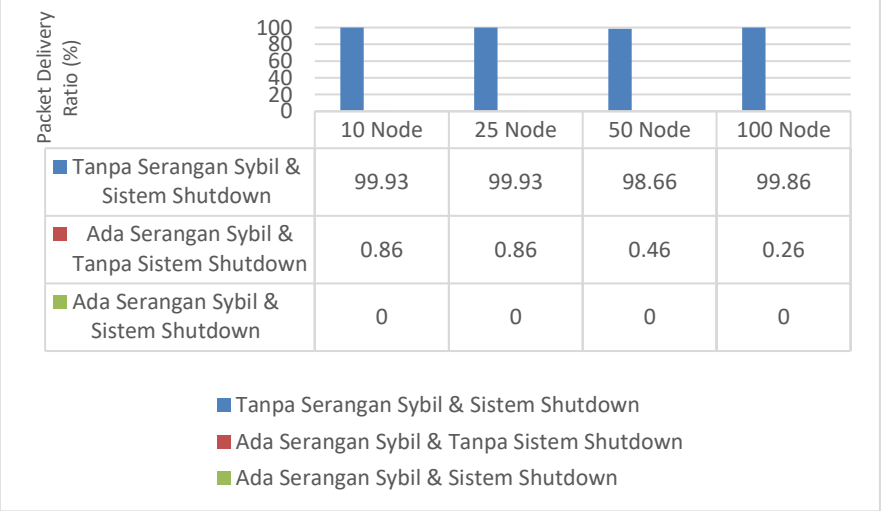
4.2 Perancangan Topologi

Topologi yang digunakan untuk simulasi *wireless sensor network* adalah topologi menggunakan persebaran *grid* dengan jumlah *node* yaitu 10, 25, 50, 100 dan area simulasi seluas 1000 x 1000 m^2. Masing-masing topologi akan diberikan *sybil attack* dan sistem shutdown sesuai dengan skenario dimana *sybil node* akan bertindak sebagai *attacker* yang memiliki dua identitas dalam jaringan *wireless sensor network*.

5. Pengujian dan Analisis Sistem

Pada penelitian ini, *sybil attack* mengambil identitas pada salah satu *node* yang berada pada jaringan yang merupakan bagian dari rute pengiriman informasi, sehingga *sybil node* dapat mengubah paket yang diterimanya. Pada protokol *routing* AODV *sybil attack* secara langsung mengambil alih jalur pengiriman paket data melakukan pencruian data atau *drop packe*, sehingga paket data tersebut tidak sampai ke *node* tujuan. Berikut ini adalah hasil pengujian dari ketiga skenario yang menghasilkan *output* dari parameter *energy consumption* dan performansi jaringan seperti *packet delivery ratio, throughput,* dan *end to end delay*.

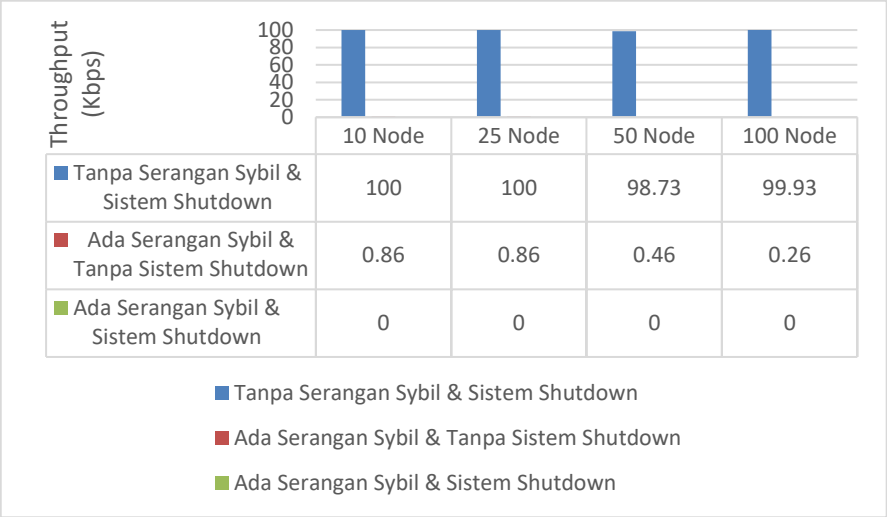
5.1 *Packet Delivery Ratio*



Grafik 1 *Packet Delivery Ratio* dengan hasil pada setiap skenario

Pada Grafik 1 *packet delivery ratio* yang memiliki nilai rata-rata tertinggi terjadi pada simulasi skenario tanpa serangan *sybil* dan sistem *shutdown* dengan nilai keberhasilan pengiriman paket ke *node* tujuan sebesar 99%, selanjutnya *packet delivery ratio* pada skenario ada serangan *sybil* tanpa mengimplementasikan sistem shutdown memiliki nilai tertinggi sebesar 0.86%. Sedangkan nilai terendah untuk pengukuran *packet delivery ratio* terjadi pada skenario ada serangan *sybil* dan sistem *shutdown* dengan nilai *packet delivery ratio* sebesar 0%. Dari ketiga skenario dapat diambil kesimpulan bahwa rendahnya nilai *packet delivery ratio* disebabkan oleh adanya serangan *sybil* yang merusak jalur *routing*, kemudian sistem *shutdown* yang mematikan komunikasi dan jalur *routing* pada *node* tujuan di jaringan WSN ketika mendeteksi adanya serangan *sybil* sehingga paket tidak terkirim ke *node* tujuan dan semakin banyak jumlah *node* yang dapat berpengaruh pada rendahnya nilai *packet delivery ratio*.

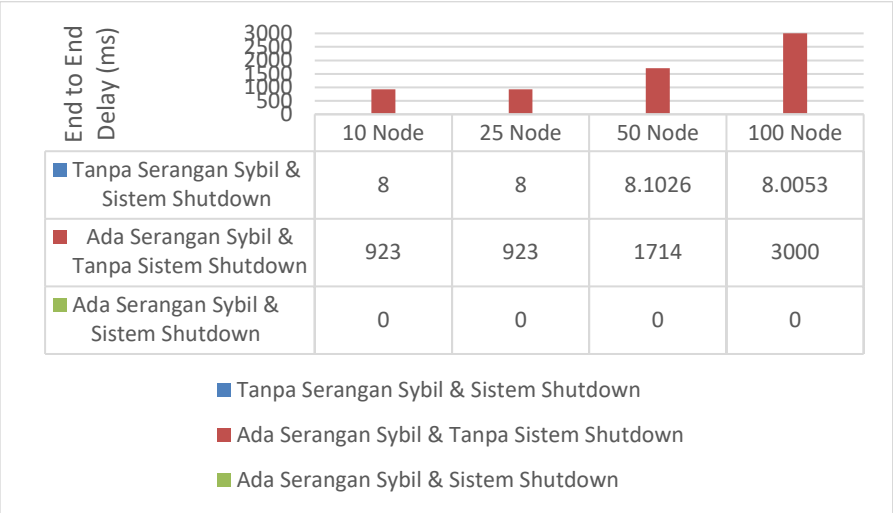
5.2 *Throughput*



Grafik 2 *Throughput* dengan hasil pada setiap skenario

Hasil pengukuran *throughput* dari seluruh skenario dapat dilihat pada Grafik 2, dimana nilai tertinggi *throughput* dari keseluruhan skenario terdapat pada skenario tanpa serangan dan sistem *shutdown* yaitu sebesar 100 kbps pada jumlah *node* 10 dan 25. Pada skenario ada serangan dan tanpa mengimplementasikan sistem *shutdown* mengalami penurunan nilai *throughput* yang sangat signifikan dibandingkan dengan skenario tanpa serangan dengan nilai *throughput* tertinggi sebesar 0.86 kbps yang terdapat pada jumlah *node* 10 dan 25 dan nilai terendah di skenario tersebut terdapat pada jumlah *node* 100 yaitu 0.26 kbps. Sedangkan nilai *throughput* terendah dari semua skenario terdapat pada skenario ada serangan dan sistem *shutdown* dengan nilai yang konsisten pada setiap jumlah *node* dengan nilai *throughput* dengan nilai sebesar 0. Hal ini dapat disebabkan dari keseluruhan skenario yang dapat berpengaruh pada nilai *throughput* yaitu adanya serangan *sybil* yang membuat nilai *throughput* pada skenario adanya serangan *sybil* tanpa mengimplementasikan sistem *shutdown* mengalami penurunan yang sangat signifikan. Kemudian pengaruh rendahnya nilai *throughput* karena adanya sistem *shutdown* yang diimplementasikan pada skenario ada serangan dan sistem *shutdown*, dimana ketika sistem *shutdown* mendeteksi terjadinya serangan *sybil*, sistem *shutdown* akan mematikan komunikasi dari *node* sumber ke *node* tujuan yang membuat paket tidak akan terkirim dan *sybil node* tidak dapat mencuri paket yang akan dikirimkan. Sistem *shutdown* tersebut yang menyebabkan tidak dapat mengukur jumlah total paket yang datang pada *node* tujuan dengan kecepatan (*rate*) pengiriman data efektif, tetapi sistem tersebut dapat mencegah dari serangan *sybil* yang ingin mencuri paket.

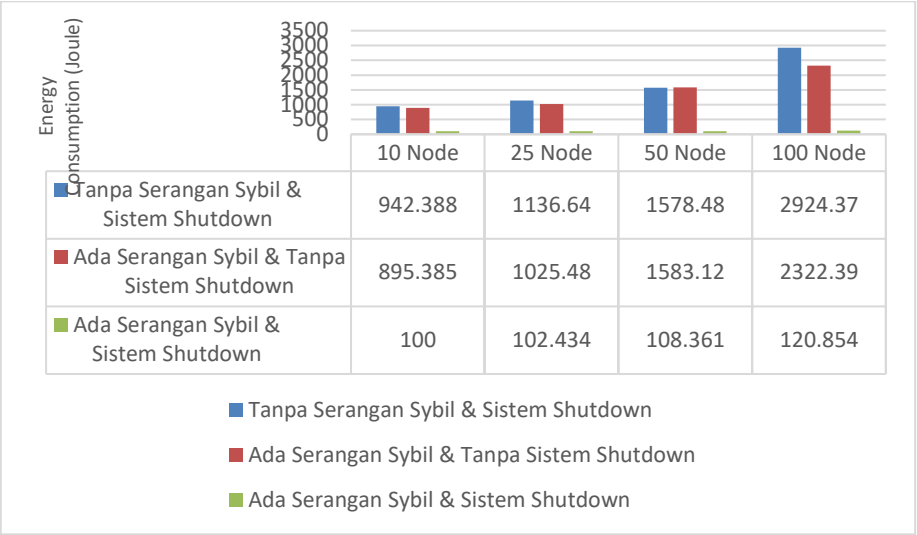
5.3 *End to end delay*



Grafik 3 *Throughput* dengan hasil pada setiap skenario

Pada Grafik 3 diperlihatkan nilai hasil pengukuran *end to end delay* pada semua skenario untuk mengetahui waktu yang dibutuhkan paket data dalam menempuh jarak dari *node* sumber ke *node* tujuan. *End to end delay* dengan nilai *delay* terbesar dari semua skenario terdapat pada skenario ada serangan *sybil* dan tanpa sistem *shutdown* dengan nilai *end to end delay* tertinggi sebesar 3000 ms dengan jumlah *node* sebanyak 100 *node*. Kemudian skenario dengan jumlah end to end delay dengan skenario tanpa serangan dan sistem shutdown memiliki nilai *end to end delay* tertinggi sebesar 8.1026 ms dengan jumlah node sebanyak 50 node. Sedangkan skenario dengan nilai *end to end delay* terendah dari semua skenario terdapat pada skenario ada serangan dan sistem *shutdown* sebesar 0 ms. Nilai *end to end delay* yang besar dari semua skenario dapat dipengaruhi oleh jarak node yang sangat jauh, jumlah *node* yang banyak, adanya serangan *sybil* yang dapat membuat waktu *delay* semakin besar dengan mengambil alih jalur *routing* dan mengalihkan semua paket ke *sybil node* sehingga paket tidak terkirim ke *node* tujuan. Sedangkan nilai *end to end* yang kecil dapat dipengaruhi karena adanya sistem *shutdown* ketika terdeteksi serangan *sybil* dengan menghentikan aksi dari serangan *sybil* dalam mencuri paket. Sistem *shutdown* menghentikan komunikasi sebelum mengirimkan paket data yang menjadikan waktu *end to end delay* menjadi 0, karena *sybil attack* yang terdeteksi pada saat proses *route discovery* ketika *node* sumber belum mengirimkan paket ke *node* tujuan. Semakin tinggi nilai *end to end delay*, maka semakin buruk waktu yang dibutuhkan pengiriman data dari *node* sumber ke *node* tujuan, dengan diterapkannya sistem *shutdown* dapat meminimalisir waktu *end to end delay* ketika terjadi serangan *sybil*. Hasil dari semua skenario dapat disimpulkan bahwa nilai *end-to-end delay* pada skenario tanpa serangan *sybil* termasuk kedalam kategori bagus yang menghasilkan nilai kurang dari 150 ms menurut standar TIPHON, sedangkan nilai *end to end delay* dengan skenario ada serangan *sybil* ternasuk kedalam kategori buruk karena menghasilkan nilai *end to end delay* lebih dari 450 ms menurut standar TIPHON.

5.4 *Energy Consumption*



	10 Node	25 Node	50 Node	100 Node
Tanpa Serangan Sybil & Sistem Shutdown	942.388	1136.64	1578.48	2924.37
Ada Serangan Sybil & Tanpa Sistem Shutdown	895.385	1025.48	1583.12	2322.39
Ada Serangan Sybil & Sistem Shutdown	100	102.434	108.361	120.854

Grafik 4.4 *Throughput* dengan hasil pada setiap skenario

Energy consumption pada Grafik 4 yang memiliki nilai pengukuran total konsumsi energi yang paling besar terdapat pada skenario tanpa serangan *sybil* dan sistem *shutdown* dengan nilai total konsumsi energi sebesar 2924.37 Joule dari jumlah 100 *node*. Setelah diberikan serangan pada skenario ada serangan dan tanpa sistem *shutdown* beberapa jumlah *node* mengalami penurunan yang tidak begitu signifikan, hanya pada jumlah *node* 50 yang mengalami kenaikan jumlah total energi. Kemudian pada skenario ada serangan dan sistem *shutdown* setelah diberikan sistem *shutdown* energi mengalami penurunan dari skenario sebelumnya, tetapi pada jumlah *node* di skenario tersebut tidak begitu signifikan dalam perubahan nilai nya. Hal ini dapat disebabkan dari semakin banyak jumlah *node* pada jaringan, maka semakin banyak total penggunaan energi yang dikonsumsi, adanya serangan *sybil* yang berpengaruh pada total penggunaan energi karena paket yang dikirimkan ke *node* tujuan diambil alih jalur *routing* oleh serangan *sybil*. Skenario dengan adanya serangan dan sistem *shutdown* mendapatkan nilai pengukuran total energi *consumption* yang paling rendah daripada skenario sebelumnya yaitu dengan nilai tertinggi pada skenario tersebut sebesar 120.854. Total konsumsi energi yang rendah dapat disebabkan oleh, adanya serangan *sybil* yang mempengaruhi konsumsi energi pada setiap *node* di jaringan, dan adanya sistem *shutdown* yang membuat energi pada *node* tujuan menjadi 0

6. Kesimpulan dan Saran

6.1 Kesimpulan

Dari hasil penelitian mitigasi serangan *sybil* menggunakan protokol *routing* AODV dengan system *shutdown* dapat disimpulkan:

1. Simulasi serangan *sybil* pada jaringan *wireless sensor network* dibuat dengan memodifikasi *script* tcl dan AODV file khususnya pada AODV.cc dan AODV.h. Modifikasi dilakukan agar *node* pada saat simulasi mempunyai dua identitas dimana identitas tersebut menjadi serangan *sybil* yang dapat mancuri paket pada jalur *routing* AODV sehingga paket data yang dikirimkan akan dicuri oleh serangan *sybil* yang membuat paket data tidak sampai ke tujuan.
2. Sistem *shutdown* bekerja ketika sistem mendeteksi adanya serangan *sybil* pada saat simulasi dijalankan maka sistem shutdown akan menghentikan seluruh komunikasi pada *sybil node* dan *destination node* sehingga tidak ada pengiriman paket data. Serangan *sybil* dideteksi dengan cara melakukan *revocation* antara *estimated key* dengan *key* yang didapatkan pada saat melakukan *discovery route*. Jika *estimated key* sama dengan *key* yang didapatkan saat melakukan *discover route* AODV maka saat sebelum mengirimkan paket data pada simulasi terindikasi adanya serangan dan saat itu juga sistem shutdown aktif mematikan *sybil node* dan *destination node*.
3. Penerapan sistem *shutdown* tidak menurunkan dan menggangu performansi jaringan pada WSN baik dari segi *throughput, end to end delay*, dan *packet delivery ratio.* Dengan adanya sistem *shutdown* pada saat terdeteksi serangan nilai *throughput*, *end to end delay*, dan *packet delivery ratio* mendapatkan nilai yang sama yaitu 0, Hal ini disebabkan karena setelah sistem *shutdown* aktif seluruh komunikasi dihentikan yang menyebabkan paket tidak sampai ke tujuan dan tidak dapat mengukur performansi jaringan.
4. Nilai dari konsumsi energi pada sistem *shutdown* memiliki nilai yang lebih sedikit dibandingkan pada saat tanpa serangan dan ada serangan. Karena energi yang dikonsumsi hanya berasal dari *node* yang terletak di jalur *routing* terbaik pada saat melakukan *discovery route.* Dilihat dari hasil konsumsi energi bahwa danya sistem shutdown terbukti menjadi sarana efektif untuk menghentikan komunikasi agar pengiriman paket tidak sampai ke tujuan dan tidak dapat dicuri ketika terjadi suatu serangan.

6.2 Saran

Untuk penelitian selanjutnya, disarankan beberapa hal :

1. Serangan dilakukan dengan skala *node* lebih dari 100 dan waktu simulasi lebih dari 120 detik.
2. Parameter performansi jaringan yang diukur tidak hanya terbatas pada *packet delivery ratio, throughput*, dan *end to end delay* seperti *response time.*
3. Melakaukan *prototyping* dari sistem *shutdown.*
4. *Wireless sensor network* yang diusulkan diintegrasikan dengan aplikasi *internet of things.*

7. Daftar Puataka

[1] K. Georgoulas, "Wireless Sensor Network Management and Funcionality: An Overview," pp. 1-11, 2009.

[2] Waltenegus dan Christian, Fundamentals of Wireless Sensor Networks: Theory and Practice, John Wiley & Sons, 2010.

[3] S. Sumaryono dan Widyawan, "Pengembangan Wireless Sensor Network untuk Aplikasi Home Controlling," *Jurnal Ilmu Pengetahuan dan Teknologi Tepat Guna,* pp. 1-10, 2012.

[4] M. Matin dan M. M. Islam, "Overview of Wireless Sensor Network," pp. 1-22, 2012.

[5] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler dan K. Pister, "System Architecture Directions fot Networked Sensors," 2000.

[6] I. F. Akyildiz, *A Survey on Sensor Networks,* p. 13, 2002.

[7] D. Sharma, S. Verma dan K. Sharma, "Network Topologies in Wireless Sensor Networks: A Review," 2013.

[8] A. Sanjaya, "Analisis Kualitas Video Streaming Dengan Protokol Routing OLSR Dan AODV Pada Mobile Adhoc Network," 2015.

[9] H. Hartadi, "Analisis Perbandingan Kinerja Routing Protokol AODV dan DSR terhadap Serangan Black Hole Pada Jaringan Manet," 2018.

[10] I. D. Chakeres dan E. M. Belding-Royer, "AODV Routing Protocol Implementation Design," 2003.

[11] R. Lakhanpal dan S. Sharma, "Detection & Prevention of Sybil Attack in Ad hoc Network using Hybrid MAP & MAC Technique," *IEEE,* 2016.

[12] R. Wulandari, "ANALISIS QoS (QUALITY OF SERVICE) PADA JARINGAN INTERNET," 2016.

[13] Hevner, Ram, March dan &. Park, "Design Science in Information System Research," 2004.