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

PREVENTION OF SINKHOLE ATTACK ON WIRELESS SENSOR NETWORK TECHNOLOGY USING AODV ROUTING PROTOCOL WITH SHUTDOWN SYSTEM

Trinanda Aditya Arya Wibisono[1], M. Teguh Kurniawan S.T., M.T.[2], Adityas Widjajarto S.T., M.T.[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]rocketr@student.telkomuniveristy.co.id, [2]teguhkurniawan@telkomuniveristy.co.id,
[3]adtwjrt@telkomuniversity.ac.id

Abstrak

Wireless Sensor Network (WSN) merupakan sebuah teknologi jaringan nirkabel yang terdiri dari sejumlah besar *sensor node* berbiaya rendah, berdaya rendah, dan multifungsi. *Sensor node* pada WSN juga memiliki kemampuan routing seperti router. Salah satu protokol *routing* pada WSN adalah Ad hoc On-Demand Distance Vector (AODV). AODV melakukan pencarian jalur *routing* ketika adanya permintaan dari *source node* untuk mengirim pesan ke *destination node*. Dikarenakan *sensor node* yang dipasang di lingkungan dapat diakses secara fisik, maka potensi terjadinya serangan akan meningkat. Serangan *sinkhole* merupakan salah satu ancaman bagi WSN. Serangan *sinkhole* adalah jenis serangan di *network layer* dimana *node* yang dikompromikan mengirimkan informasi *routing* palsu ke tetangganya untuk menarik lalu lintas jaringan ke dirinya sendiri. Untuk mengurangi dampak yang ditimbulkan oleh serangan *sinkhole* tersebut, maka dibutuhkan adanya sebuah mitigasi serangan pada WSN menggunakan protokol routing AODV dengan sistem *shutdown*. Hal ini bertujuan untuk mematikan pengiriman paket antara *source node, sinkhole node* dan *destination node* secara langsung sebelum paket tersebut di proses oleh sistem. Dari hasil pengujian perfomansi jaringan dapat diketahui bahwa serangan *sinkhole* menurunkan performansi jaringan pada *paket delivery ratio* dan *throughput* sedangkan *end to end delay* mengalami kenaikan, dengan penurunan *packet delivery ratio* sebesar 99,8%, penurunan *throughput* 99,8 kbps, lalu *delay* yang mengalami penaikan sebesar 3992 ms. Sedangkan nilai dari *energy consumption* pada sistem *shutdown* stabil. Dengan adanya sistem *shutdown*, serangan *sinkhole* dapat dimitigasi serta tidak menurunkan dan menggangu performansi jaringan pada WSN.

Kata Kunci: ***Wireless sensor network*, serangan *sinkhole*, AODV, sistem *shutdown***

Abstract

Wireless Sensor Network (WSN) is a wireless networking technology that consists of a large number of low-cost, low-power, and multifunctional node sensors. Sensor nodes on WSN also have routing capabilities such as routers. One of the routing protocols on WSN is Ad hoc On-Demand Distance Vector (AODV). AODV performs a routing path search when a request from a source node is sent to the destination node. Because the node sensors installed in the environment are physically accessible, the potential for attack will increase. The sinkhole attack is one of the threats to WSN. A sinkhole attack is a type of attack on a network layer where a compromised node sends false routing information to its neighbor to pull network traffic to itself. To reduce the impact caused by the sinkhole attack, it is necessary to do a mitigation attack on WSN using AODV routing protocol with shutdown system. It aims to turn off packet delivery between the source node, sinkhole node and destination node directly before the packet is processed by the system. From the results of network perfomance testing can be seen that sinkhole attacks reduce network performance in the packet delivery ratio and throughput while the end to end delay increased, with a decrease in packet delivery ratio of 99.8%, decreased throughput 99,8 kbps, then delay increased of 3200 ms. While the value of energy consumption in system shutdown stable. With the system shutdown, sinkhole attacks can be mitigated and not reduce and disrupt network performance on WSN.

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

1. Pendahuluan

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) [1]. IoT sangat menjanjikan untuk mengoptimalkan kehidupan berdasarkan sensor yang cerdas dan peralatan pintar yang bekerjasama melalui jaringan internet [2]. Para ahli telah mengembangkan salah satu *key concept* dalam IoT yaitu jaringan nirkabel (*Wireless*) dengan node *sensor* yang dibuat dalam satu topologi jaringan yang dapat mengintegrasikan suatu sistem secara terpusat dan dapat di *control* serta di *monitoring* dimanapun. *Key concept* tersebut adalah *Wireless Sensor Network*.

Wireless Sensor Network (WSN) terdiri dari sejumlah besar simpul sensor berbiaya rendah, berdaya rendah, dan multifungsi yang berkomunikasi jarak pendek melalui jalur nirkabel [3]. WSN menggabungkan jaringan nirkabel, *sensor, microcontroller, memori,* sistem operasi, komunikasi radio dan sumber energi berupa baterai dalam satu *embedded platform* yang saling terintegrasi [4]. WSN berkomunikasi menggunakan sensor yang ada pada setiap node, dimana setiap data akan dikirim/diterima menggunakan *transceiver* kepada device yang lain. Alasan utama *Wireless Sensor Network* sangat dibutuhkan dan penting adalah karena WSN memiliki arsitektur secara terpusat, hirarkis dan terdistribusi [5] yang memungkinkan untuk melakukan pemantauan disetiap aplikasi secara *real-time* dan maksimal dengan jarak jauh tanpa harus mengakusisi data secara langsung di area sensor. *Sensor node* pada WSN juga memiliki kemampuan *routing* seperti *router*. Salah satu protokol *routing* pada WSN adalah Ad hoc On-Demand Distance Vector (AODV). AODV melakukan pencarian jalur *routing* ketika adanya permintaan dari *source node* untuk mengirim pesan ke *destination node.* Tetapi disamping dari kelebihan yang dimiliki oleh WSN, WSN mempunyai beberapa batasan yang memunculkan tantangan dalam penerapannya. Beberapa tantangan dalam WSN antara lain adalah keterbatasan sumber daya (pasokan listrik) pada setiap titik sensor dan faktor keamanan pada media komunikasi yang bersifat *wireless* sehingga sangat rentan kerena dapat diakses secara fisik sehingga potensi serangan secara langsung atau jarak jauh pada topologi WSN meningkat.

Serangan *sinkhole* merupakan salah satu ancaman bagi WSN. Serangan *sinkhole* adalah jenis serangan di *network layer* dimana *node* yang dikompromikan mengirimkan informasi *routing* palsu ke tetangganya untuk menarik lalu lintas jaringan ke dirinya sendiri. Untuk mengurangi dampak yang ditimbulkan oleh serangan *sinkhole,* perlu adanya sebuah mitigasi menggunakan *routing* AODV dengan menggunakan sistem *shutdown* yang akan dianalisis bagaimana konsumsi energi dan perfomansi jaringannya sebelum dan setelah adanya serangan.

2. Tinjauan Pustaka

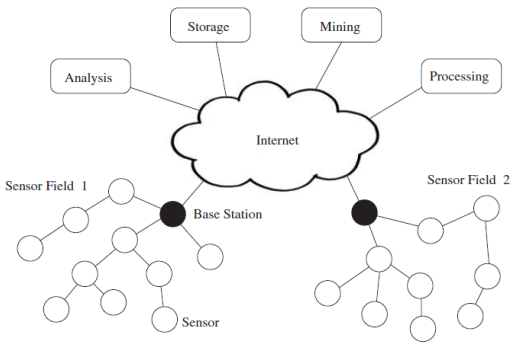
2.1. *Wireless Sensor Network*

Wireless Sensor Network (WSN) terdiri dari sejumlah besar simpul sensor berbiaya rendah, berdaya rendah, dan multifungsi yang berkomunikasi jarak pendek melalui jalur nirkabel [3]. Fokus utama pembuatan jaringan *Wireless Sensor Network* adalah untuk memantau kondisi fisik atau lingkungan, seperti suhu, suara, getaran, tekanan, gerak atau polutan yang menimbulkan adanya komunikasi yang terjadi dalam satu *embedded platform* yang saling terintegrasi dengan manusia [6]. .

Wireless Sensor Network (WSN) pertama kali diimplementasikan oleh militer. 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 mikrosensor [7] Selain di bidang militer, WSN telah berhasil diterapkan dalam berbagai domain aplikasi seperti bidang militer, transportasi, aplikasi kesehatan, pertanian, dan lain-lain.

2.2. Arsitektur *Wireless Sensor Network*

Pada *Wireless Sensor Network*, *sensor node* disebar di sekitar lingkungan yang akan dilakukan *monitoring*. *Sensor node* tersebut memiliki kemampuan untuk merutekan data yang dikumpulkan ke *node* lain yang berdekatan. Data dikirimkan melalui transmisi radio akan diteruskan menuju *Base Station* atau *sink node* yang merupakan penghubung antara *sensor node* dan user. [8]

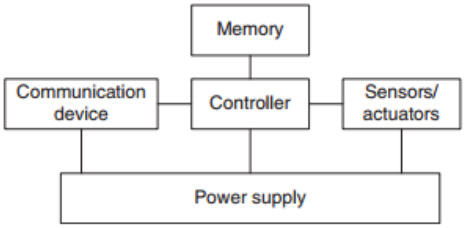


Gambar 1 *Wireless Sensor Network* [9]

Secara umum *wireless sensor network* terdiri dari beberapa komponen utama yaitu:

1. *Sensor Node*

Sensor node adalah bagian utama dalam *Wireless Sensor Network* (WSN) yang dapat digunakan untuk mendeteksi, memproses dan mengirimkan data melalui jaringan nirkabel menuju *sink* atau *gateway* [10] Dalam mengirimkan data, setiap *sensor node* akan mengirimkan secara langsung (*Single-hop*), maupun melewati beberapa *sensor node* (*Multi-hop*) terlebih dahulu untuk menuju *sink* atau *gateway* [11].



Gambar 2 Komponen *Sensor Node* [12]

Sensor node terdiri dari 5 komponen utama [12] yaitu:

a. Kontroler atau *Processor*

Kontroler berfungsi untuk melakukan perhitungan aritmatika dan logika yang berkaitan dengan proses data. Komponen ini sering disebut sebagai otak dari *sensor node*, karena dapat mengirim paket, menerima paket, mengatur mode *sleep*, dan sebagainya. Karena *sensor node* berukuran kecil, kontroler yang digunakan pada umumnya berukuran mikro [9].

b. Memori

Memori digunakan untuk menyimpan kode program dan data. Saat ini keberadaan memori bersifat opsional karena media penyimpanan juga dapat dilakukan oleh mikrokontroler.

c. Sensor atau aktuator

Sensor berfungsi untuk mendeteksi keadaan pada objek sesuai dengan *parameter* yang ditentukan (suhu, suara, getaran, kelembaban, dan lain-lain).

d. Perangkat komunikasi

Untuk mengkomunikasikan *sensor node* ke jaringan diperlukan perangkat komunikasi untuk mengirim dan menerima informasi melalui jaringan nirkabel.

e. *Power supply*

Power supply berfungsi sebagai pusat daya untuk *sensor node*. Saat ini *power supply* tidak hanya berupa baterai namun juga panel surya sehingga memungkinkan adanya pengisian kembali daya dengan tenaga matahari.

2. *Sink Node / Base Station*

Sink node adalah perangkat yang mengumpulkan informasi dari *sensor node* menuju ke penyimpanan data biasanya dalam bentuk *cloud*. Komponen ini dapat diibaratkan sebagai gerbang keluar masuk *(gateway)* informasi baik dari *sensor node* maupun perangkat lain ke *wireless sensor network* [13].

3. *Internet*

Internet digunakan sebagai media menuju penyimpanan data berbasis *cloud*. Karena setiap data dari *sink node* dikirimkan ke penyimpanan data berbasis *cloud* yang akan diakses oleh *user* melalui komputer.

4. *User*

User dapat mengakses informasi mengenai objek malalui *remote server* secara *real time*. Informasi tersebut diakses melalui koneksi internet atau satelit ke penyimpanan data berbasis *cloud*.

2.3 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* [8].

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*

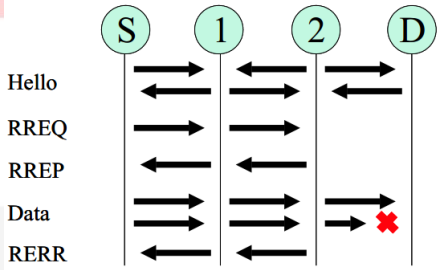
Menempatkan *sensor node* secara *random* dilakukan oleh persebaran *random* tanpa memperhitungkan jarak antar *sensor node*. Persebaran *random* biasanya digunakan pada lingkungan yang berbahaya dengan *traffic* yang rendah, misalnya di kawasan pegunungan atau tempat yang sering terkena bencana alam.

2.4 Protokol Routing pada Ad-Hoc on Demand Distance Vector (AODV) Wireless Network Network

AODV adalah protokol *routing* reaktif yang didesain untuk *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. *Node* pada AODV akan menyimpan tabel *routing* hanya satu *node* tujuan untuk satu rute. Pada *routing* AODV, jika rute tidak digunakan pada waktu yang sudah ditentukan maka rute akan dihapus dari tabel *routing* [14].

AODV memiliki *route discovery* dan *route maintenance*. *Route discovery* berupa *route request* (RREQ) dan *route reply* (RREP). Saat *node* sumber melakukan permintaan rute, ia akan melakukan broadcast RREQ ke seluruh jaringan yang terhubung dengannya. Sedangkan *route maintenance* berupa data dan *Route Error* (RRER)**.** RREQ berjalan dari satu *node* ke *node* yang lain, secara otomatis membentuk jalur untuk kembali dari semua *node* yang di lalui ke sumber *node* yang meminta RREQ [15].

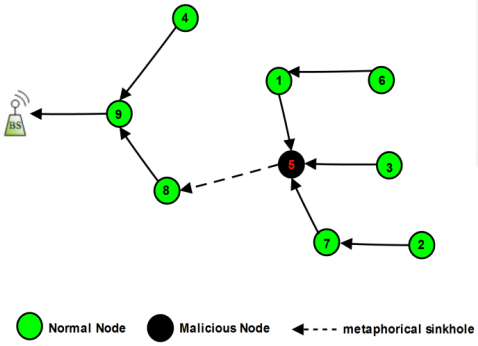
AODV menggunakan *destination sequence number* untuk menjaga informasi mengenai *reverse path* yang mengarah ke *source node*. *Reverse Path* terbentuk saat RREQ menempuh *node* yang dituju, dimana setiap RREQ akan diidentifikasi dari *node* sekitar yang mengirimkan RREQ tadi. Saat *node* yang dituju 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 [16]



Gambar 3 Proses Pencarian Rute AODV [16]

2.5 *Sinkhole Attack*

Serangan *sinkhole* merupakan ancaman utama bagi jaringan sensor nirkabel. Serangan *sinkhole* adalah jenis serangan lapisan jaringan dimana node yang dikompromikan mengirimkan informasi *routing* palsu ke tetangganya untuk menarik lalu lintas jaringan ke dirinya sendiri. Karena sifat jaringan ad-hoc dan banyak sekali pola komunikasi jaringan sensor nirkabel, banyak node mengirim data ke satu *base station*. Berdasarkan arus komunikasi di WSN, Sinkhole tidak perlu menargetkan semua node dalam jaringan namun cukup dengan *node* yang dekat dengan *base station* [17].



Gambar 4 Ilustrasi serangan *sinkhole* [18]

Serangan *sinkhole* dilakukan dengan membuat *node* yang dikompromikan terlihat lebih menarik bagi semua *node* tetangga yang memiliki jalur perutean yang efektif menuju tempat tujuan dengan tingkat energi yang tinggi. Misalnya node itu mungkin adalah sebuah laptop dengan energi tinggi dan berkinerja tinggi. Pertama, *node* dikompromi mengiklankan bahwa ia memiliki koneksi *single hop* berkualitas tinggi dengan *base station* ke *node* tetangganya. Setelah itu semua *node* mengalihkan semua lalu lintas mereka untuk melewati simpul penyusup ke *base station*. Dengan demikian *sinkhole* attack diluncurkan.

Serangan *sinkhole* sulit dideteksi karena informasi *routing* yang diberikan oleh masing-masing *node* sulit untuk diverifikasi. Setelah penyerang melakukan serangan *sinkhole*, dia dapat melakukan serangan jenis apa pun di WSN karena seluruh lalu lintas mengalir melalui *node sinkhole* sehingga dia dapat mengumpulkan semua data melalui node tersebut dan menyalahgunakan data yang dikumpulkan. Dia bahkan bias memasukkan semua paket atau beberapa paket serangan seperti *selective forwarding*, serangan *wormhole, flood attack*, serangan *sybil*, serangan *black hole*.

2.6 Parameter Uji

Pengujian perfomansi atau kinerja suatu layanan jaringan komputer dapat diukur dengan parameter Quality of Service (QoS) untuk menunjukkan konsistensi, tingkat keberhasilan pengiriman data, dan lain-lain. Ada beberapa contoh parameter yang dapat digunakan untuk mengukur kualitas kinerja suatu jaringan computer, antara lain: throughput, end to end delay, dan packet delivery ratio **[19]**.

1. *Packet Delivery Ratio*
   Packet Delivery Ratio adalah rasio antara banyaknya paket yang diterima oleh *destination* dengan banyaknya paket yang dikirim oleh *source*. PDR yang sangat bagus memiliki nilai 100 %.
   $$PDR = \frac{Paket\ diterima}{Paket\ dikirim} \times 100\% \text{ …….. (1.1)}$$

2. *Throughput*
   Throughput adalah jumlah waktu yang diambil oleh paket untuk mencapai tujuan. *Throughput* disebut juga sebagai *bandwidth* dalam kondisi yang sebenarnya*andwidth* lebih bersifat tetap sementara *throughput* bersifat dinamis tergantung pada trafik yang sedang terjadi. *Throughput* mempunyai satuan Bps (*Bit per second*). Rumus untuk menghitung *throughput* adalah:
   $$Throughput = \frac{Jumlah\ data\ dikirim}{waktu\ pengiriman\ data} \text{ …….. (1.2)}$$

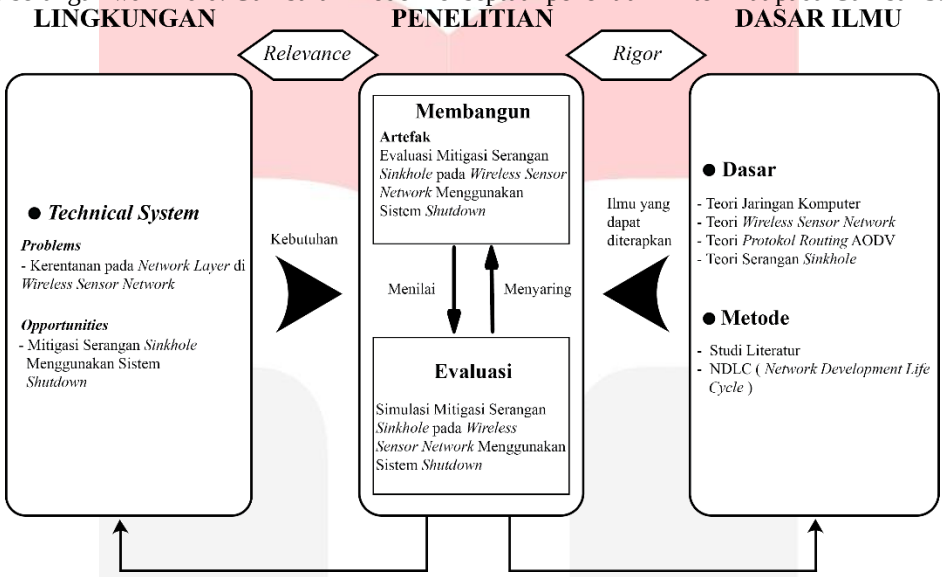
3. *End to End Delay*
   End to end delay adalah waktu rata-rata yang ditempuh paket data untuk mencapai *destination* termasuk *delay* yang disebabkan oleh antrian dalam transmisi paket data dan proses penemuan rute. Hanya paket data yang berhasil dikirim ke *destination* yang dihitung. *End to end delay* mempunyai satuan ms (*milisecond*). Adapun rumus untuk menghitung *end to end delay* adalah:
   $$End\ to\ end\ delay = \frac{Total\ waktu}{Total\ paket\ yang\ diterima} \text{ …….. (1.3)}$$

4. *Energy Consumption*
   Energi diukur untuk mengetahui seberapa efisien penggunaan daya yang dikonsumsi saat sensor node melakukan transmisi paket maupun receive paket. Satuan energi adalah Joule. Konsumsi energi dipengaruhi oleh 3 parameter yaitu initial energy, transmit power, dan receive power. Semakin banyak paket yang dikirim, maka transmit power akan semakin besar, begitu juga dengan paket yang diterima akan mempengaruhi receive power. Selain itu nilai throughput juga menentukan besarnya energy consumption.
   $$\boldsymbol{Jumlah\ Konsumsi\ Energi} = \sum \boldsymbol{energi\ tiap\ node} \text{ …….. (1.4)}$$

3. Metode Penelitian

3.1 Model Konseptual

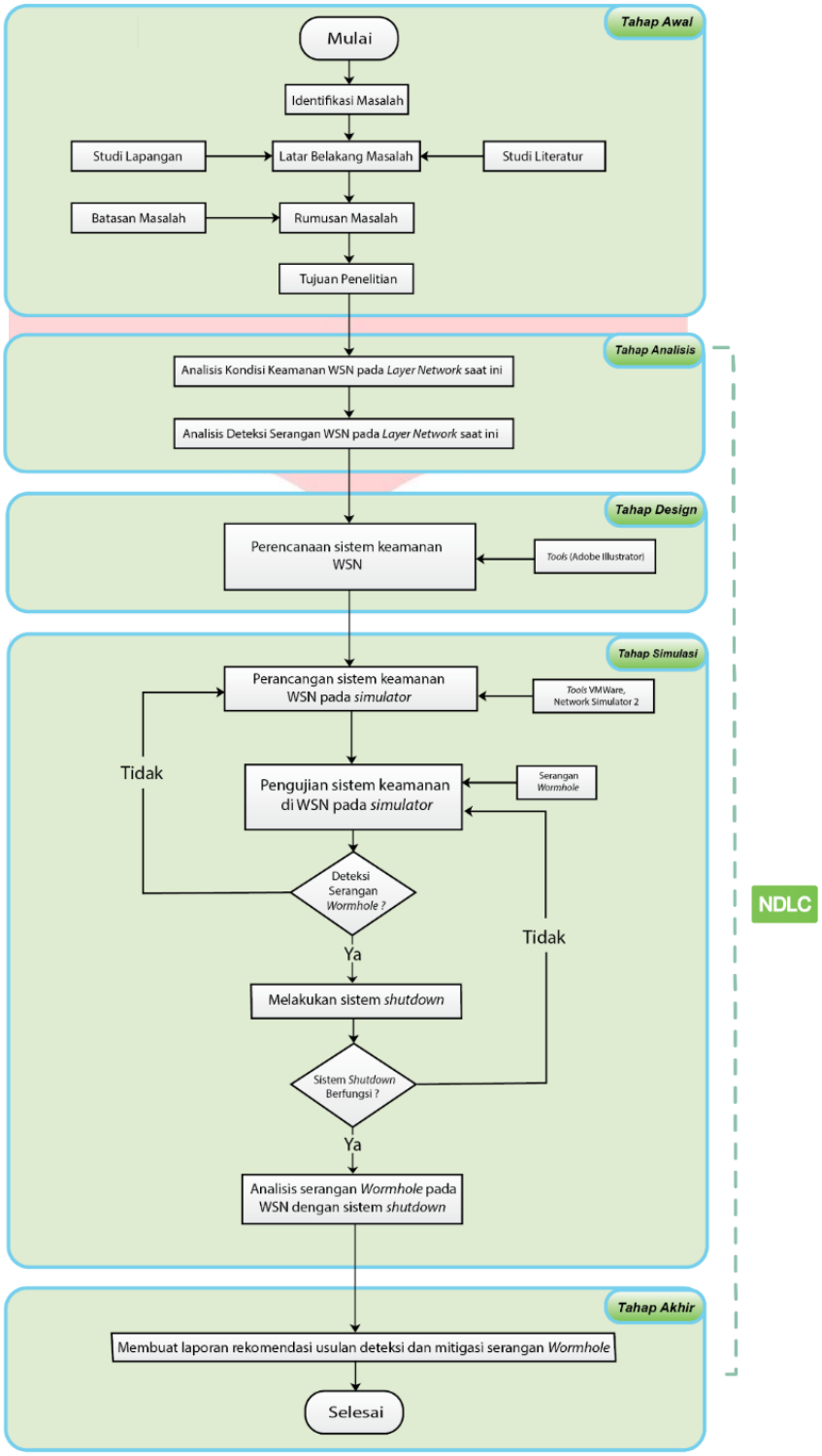
Model konseptual bertujuan untuk mengidentifikasi data dalam proses penelitian sehingga dapat membantu peneliti dalam merumuskan pemecahan masalah yang ada [20]. Model ini juga bertujuan untuk membantu mengidentifikasi faktor-faktor yang relevan, perumusan solusi, dan memberikan penjelasan agar masalah yang ada dapat dipahami dengan mudah. Model konseptual ini menggambarkan kerangka penelitian tugas akhir yang bertujuan untuk membuat rancangan usulan deteksi dan mitigasi pada keamanan *wireless sensor network* terhadap serangan *wormhole*. Gambaran model konseptual penelitian ini terlihat pada Gambar 3.



Gambar 5 Model Konseptual Penelitian

3.2 Sistematika Penelitian

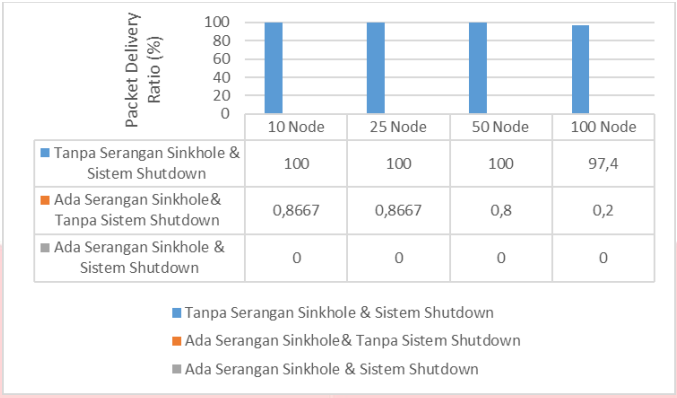
Sistematika penelitian merupakan penjabaran secara deskriptif tentang hal-hal yang akan dilakukan selama penelitian berlangsung. Tahapan yang dilakukan adalah tahap yang terdapat pada metode NDLC (*Network Development Life Cycle*), diantaranya: tahap awal (tahap identifikasi), tahap analisis, tahap desain, dan tahap simulasi.



Gambar 6 Sistematika Penelitian

4. Pengujian dan Analisis Sistem

4.1 *Packet Delivery Ratio*



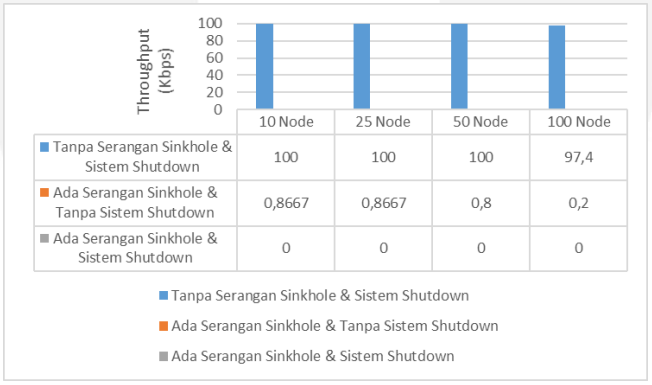
Grafik 4.1 *Packet Delivery Ratio* dengan hasil pada setiap skenario

Pada Grafik V.4.1 simulasi skenario tanpa serangan *sinkhole* memiliki nilai *packet delivery ratio* tertinggi dengan nilai keberhasilan pengiriman paket ke *destination node* sebesar 100%, selanjutnya *packet delivery ratio* pada skenario ada serangan *sinkhole* memiliki nilai tertinggi sebesar 0.8667%. Sedangkan nilai terendah untuk *packet delivery ratio* terjadi pada skenario ada serangan *sinkhole* dan sistem *shutdown* dengan nilai *packet delivery ratio* sebesar 0%.

Dari ketiga skenario dapat diambil kesimpulan bahwa ketika tidak ada serangan, nilai *packet delivery ratio* dipengaruhi oleh banyaknya *node* dan jalur *routing* AODV. Dengan adanya serangan *sinkhole*, nilai *packet delivery ratio* mengalami penurunan yang jauh berbeda karena motivasi serangan sinkhole untuk merusak paket ketika pengiriman paket berhasil dilakukan. Sehingga tidak semua paket yang dikirimkan sampai ke *destination node.*

Ketika mengimplementasikan sistem *shutdown* , nilai *packet delivery ratio* tidak dapat diukur karena sistem *shutdown* mendeteksi serangan *sinkhole* pada saat AODV melakukan *route discovery*. Sistem *shutdown* membuat paket tidak terkirim dengan mematikan komunikasi dari sumber ke destinasi sehingga *sinkhole node* tidak melakukan perusakan paket pada paket yang dikirimkan.

4.2 *Throughput*



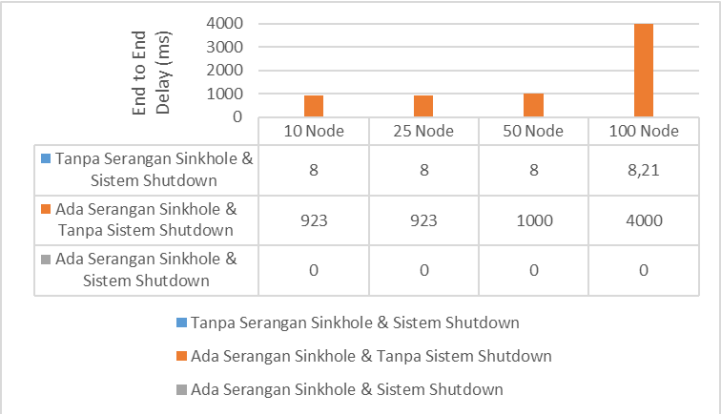
Grafik 4.2 *Throughput* dengan hasil pada setiap skenario

Hasil pengukuran *throughput* dari seluruh skenario dapat dilihat pada Grafik V.4.2, dimana nilai tertinggi *throughput* dari keseluruhan skenario terdapat pada skenario tanpa serangan dan sistem *shutdown* yaitu sebesar 100 kbps pada jumlah *node* 10,25, dan 50. Pada skenario ada serangan dan tanpa mengimplementasikan sistem *shutdown* mengalami penurunan nilai *throughput* yang sangat signifikan dibandingkan dengan skenario tanpa serangan dan sistem *shutdown* dengan nilai *throughput* tertinggi sebesar 0.86 kbps yang terdapat pada jumlah *node* 10 dan 25. 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.

Dari ketiga skenario dapat diambil kesimpulan bahwa ketika tidak ada serangan, nilai *throughput* dipengaruhi oleh banyaknya *node* dan rute jalur pengiriman paket. Dengan adanya serangan *sinkhole*, nilai *throughput* menjadi jauh lebih kecil karena serangan *sinkhole* membuat banyak paket tidak berhasil terkirim ke *destination node*.

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 *sinkhole* pada saat *route discovery* oleh AODV, sistem *shutdown* membuat paket tidak terkirim dengan mematikan komunikasi dari *source node* ke *destination node* sehingga *sinkhole node* tidak dapat memanipulasi jalur *routing* dan merusak paket yang akan dikirimkan.

4.3 *End to End Delay*



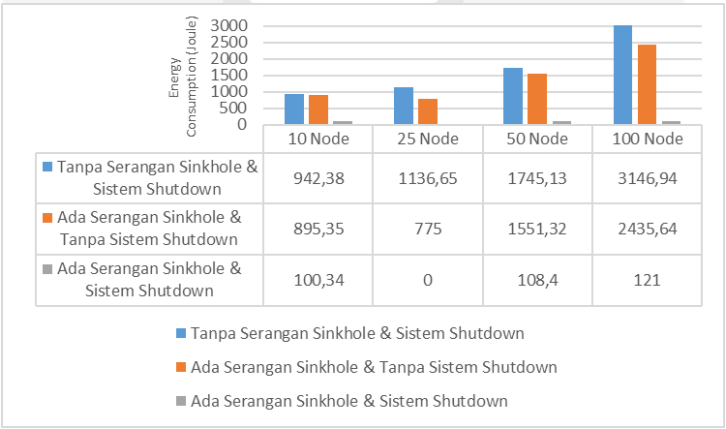
Grafik 4.3 *End to End Delay* dengan hasil pada setiap skenario

Pada Grafik V.4.3 terlihat nilai hasil pengukuran *end to end delay* pada semua skenario untuk mengetahui waktu yang dibutuhkan paket data dalam menempuh jarak dari *source node ke destination node*. *End to end delay* dengan nilai *delay* terbesar dari semua skenario terdapat pada skenario ada serangan *sinkhole* dan tanpa sistem *shutdown* dengan nilai *end to end delay* tertinggi sebesar 4000 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 8,21 ms dengan jumlah *node* sebanyak 100 *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 jumlah *node* yang banyak, adanya serangan *sinkhole* yang dapat membuat waktu delay semakin besar dengan mengambil alih jalur *routing* dan menarik paket ke *sinkhole node* sehingga paket tidak terkirim ke *destination node*.

Sedangkan nilai *end to end delay* yang kecil dapat dipengaruhi karena adanya sistem *shutdown* yang mendeteksi serangan *sinkhole*. Seperti yang sudah dijelaskan sebelumnya, sistem *shutdown* menghentikan komunikasi sebelum mengirimkan paket data yang menjadikan waktu *end to end delay* menjadi 0, karena *sinkhole attack* yang terdeteksi pada saat *node* sumber belum mengirimkan paket ke *destination node*. Semakin tinggi nilai *end to end delay*, maka semakin buruk waktu yang dibutuhkan pengiriman data dari *source node* ke *destination node*, dengan diterapkannya sistem *shutdown* dapat meminimalisir waktu *end to end* delay ketika terjadi serangan *sinkhole*.

4.4 *Energy Consumption*



Grafik 4.4 *Energy Consumption* dengan hasil pada setiap skenario

Energy consumption pada Grafik V.4.4 yang memiliki nilai pengukuran total konsumsi energi yang paling besar terdapat pada skenario tanpa serangan *sinkhole* dan sistem *shutdown* dengan nilai total konsumsi energi sebesar 3146,94 Joule dari jumlah 100 *node*. Setelah diberikan serangan pada skenario ada serangan dan tanpa sistem *shutdown* beberapa jumlah *node* mengalami penurunan yang tidak terlalu berbedas, hanya pada jumlah *node* 50 yang mengalami kenaikan jumlah total energi.

Dari ketiga skenario tersebut, dapat diambil kesimpulan bahwa nilai jumlah konsumsi energi dipengaruhi oleh banyaknya *node*, adanya serangan *sinkhole* dan sistem *shutdown*. Pada saat tidak ada serangan, jumlah konsumsi energi lebih banyak. Dengan adanya serangan *sinkhole*, jumlah konsumsi energi mengalami penurunan dikarenakan oleh *sinkhole node* yang mengambil alih jalur lalu lintas pengiriman data, sehingga *node* lainnya tidak bekerja dengan maksimal. Ketika diimplementasikan sistem *shutdown*, jumlah komsumsi energi kecil karena *node* hanya menggunakan energi untuk melakukan *route discovery*.

5. Kesimpulan dan Saran

5.2 Kesimpulan

Pada penelitian ini dapat ditarik kesimpulan, sebagai berikut:

1. Simulasi serangan *sinkhole* dilakukan dengan menggunakan NS-2.35 pada sistem operasi Ubuntu 16.04. Serangan dibuat dengan cara memodifikasi *script* tcl dan MAC *layer* khususnya pada *file* aodv.cc dan aodv.h. Modifikasi dilakukan agar terbentuk *attacker node* atau *sinkhole node* untuk mencemari *node*.
2. Cara kerja sistem *shutdown* adalah ketika sistem mendeteksi adanya serangan *sinkhole* pada simulasi maka sistem *shutdown* akan menghentikan seluruh komunikasi pada *sinkhole node* dan *destination node* sehingga tidak ada pengiriman paket yang salah ke *user*. Serangan *sinkhole* dideteksi dengan cara melakukan *revoke* antara *estimated key* dengan *key* yang didapatkan pada saat melakukan *discovery route.* Jika *estimated key* sama dengan *key* yang didapatkan saat melakukan *discovery route* AODV maka simulasi terindikasi adanya serangan dan saat itu juga sistem *shutdown* aktif mematikan *sinkhole node* dan *destination node*.
3. Penerapan sistem *shutdown* membuat performansi jaringan komputer baik dari segi *throughput*, end to end delay, dan *packet delivery ratio* tidak bias diukur. Karena dengan menerapkan system *shutdown*, komunikasi jaringan terputus sehingga tidak ada aktifitas pengiriman dan penerimaan paket.
4. Nilai dari konsumsi energi pada sistem *shutdown wireless sensor network* lebih sedikit dibandingkan pada saat tanpa serangan dan ada serangan. Karena energi yang dikonsumsi hanya berasal dari *discover route* AODV.

5.3 Saran

Adapun saran yang dapat diberikan untuk penelitian selanjutnya adalah:

1. Serangan dilakukan dengan jumlah *node* yang lebih besar dari 100 node dan waktu yang lebih lama dari 120 detik.
2. Parameter performansi jaringan yang diukur tidak hanya terbatas pada *throughtput, end to end delay*, dan *packet delivery ratio*, seperti *Respond Time*.

6. Daftar Pustaka

[1] A. Junaidi, "Internet of Things, Sejarah, Teknologi dan Penerapannya : Review," *Jurnal Ilmiah Teknologi Informasi Terapan,* pp. 1-5, 2015.

[2] H. Tschofenig, S. L. Keoh dan S. S. Kumar , "Securing the Internet of Things: A Standardization Perspective," *IEEE Internet of Things Journal,* pp. 265-275, 2014.

[3] A. Liu, M. Kim, L. B. Oliveira dan H. Tan, "Wireless Sensor Network Security," *International Journal of Distributed Sensor Networks,* 2013.

[4] W. Sujoko Sumaryono, "Pengembangan Wireless Sensor Network untuk Aplikasi Home Controlling," *Jurnal Ilmu Pengetahuan dan Teknologi Tepat Guna,* pp. 1-10, November 2012.

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

[6] M. I. M. A Matin, "Overview of Wireless Sensor Network, " pp. 1-22, 2012.

[7] K. S. J. Pister, "Military applications of sensor networks," *of Institute for Defense Analyses, Defense Science Study Group,* p. 3531, 2000.

[8] Sugiarto dan Sakti, "Rancang Bangun Sistem Monitoring Kualitas Udara Menggunakan Teknologi Wireless Sensor Networ (WSN)," *INKOM,* pp. 90-96, 2009.

[9] A. Suhada, "Sistem Keamanan Gedung Berbasis Wireless Sensor Network dengan Modul NRF24," 2016.

[10] F. D. Nugraheni, "Implementasi Wireless Sensor Network untuk Aplikasi Lampu dan Kipas," 2016.

[11] A. A. Laksono, "Rancangan Bangun Prototipe Pemantauan Posisi Kereta Berbasis Wireless Sensor Network," 2016.

[12] H. Karl dan A. Willig, Protocols and Architectures for Wireless Sensor Networks, Chichester: John Wiley & Sons Ltd, 2005.

[13] M. B. Aufar, "Analisis Simulasi Routing Protokol Hierarkial Leach dan Pegasis pada Wireless Sensor Network," 2017.

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

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

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

[17] Keerthana, "Detecting Sinkhole Attack in Wireless Sensor Network using Enchaned Particle Swarm Optimization Technique," *International Journal of Security and Its Applications,* pp. 41-54', 2016.

[18] A. Dahane, A. Loukil dan B. Nasr-eddine, "Safety of Mobile Wireless Sensor Networks Based on Clustering Algorithm," *International Journal of Wireless Networks and Broadband Technologies,* pp. 73-102, 2016.

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

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