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

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

Tania Almira Pamudji[1], M. Teguh Kurniawan S.T., M.T.[2], Adityas Widjajarto S.T., M.T.[3]

[1]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

[1]almiratania@student.telkomuniversity.ac.id, [2]teguhkurniawan@telkomuniveristy.co.id, [3]adtwjrt@telkomuniversity.ac.id

Abstrak

***Wireless sensor network* (WSN) merupakan sebuah jaringan nirkabel yang terdiri dari sejumlah *sensor node* berukuran kecil untuk memantau kondisi lingkungan tertentu. Setiap *sensor node* akan saling berkomunikasi dan mengirimkan informasi ke *base station*. Seperti halnya *router, sensor node* pada WSN juga memiliki kemampuan *routing*. Protokol *routing* pada WSN salah satunya dalah AODV yang memiliki karakteristik mencari jalur *routing* ketika adanya permintaan dari *souce node* untuk mengirim pesan ke *destination node*. Dikarenakan *sensor node* yang dipasang di lingkungan dapat diakses secara fisik maka meningkatkan potensi terjadinya serangan. Serangan *wormhole* merupakan jenis serangan dimana penyerang memindahkan jalur *routing* pada WSN ke terowongan yang dibuat diantara *source* dan *destination node*. Serangan *wormhole* dapat menjadi pemicu timbulnya serangan lain pada WSN. Berdasarkan kondisi yang rentan terhadap adanya serangan, maka dibutuhkan adanya mitigasi serangan pada *wireless sensor network* menggunakan protokol *routing* AODV dengan sistem *shutdown*. Hal ini bertujuan untuk mematikan *sensor node* yang telah mengalami modifikasi dari penyerang sebelum informasi tersebut diproses oleh sistem dan dikirim ke *user*. Dari hasil pengujian yang dilakukan diketahui bahwa pada penerapan sistem *shutdown* terjadi efisiensi energi yang dikonsumsi dengan tidak adanya penurunan dalam performansi jaringan. Sehingga sistem *shutdown* dapat menjadi salah satu solusi efektif dalam memitigasi serangan *wormhole*.**

Kata kunci: ***Wireless sensor network*, serangan *wormhole*, AODV, *sistem shutdown*.**

Abstract

Wireless sensor network (WSN) is a network that consist of several sensor nodes to monitor certain environmental conditions. Each node sensor will communicate with each other and send information to the base station or sink node. Like addressing in the router, the sensor node on WSN also has routing capabilities. One of routing protocol on WSN is AODV which has access to the routing path when request from the souce node to send the message to the destination node. Because the sensor node can be physically activated, increasing the potential for recovery. The wormhole attack is a type of attack where the attacker connects the route on the WSN to the tunnel created between the source and destination nodes. A wormhole attack can trigger another attack on the WSN. Based on conditions susceptible to existing attacks, it is necessary to mitigate wireless sensor networks using the AODV routing protocol with the shutdown system. The shutdown system will turn off the sensor nodes that have been used from the attacker before the information is processed by the system and sent to the user. From the results of tests known that the implementation of the shutdown system occurs energy efficiency consumed in the absence of a decrease in network performance. So, the shutdown system can be one effective solution in mitigating wormhole attacks.

Keywords: ***Wireless sensor network, wormhole attack*, AODV, *shutdown system*.**

1. Pendahuluan

Kebutuhan akan kemudahan komunikasi data dan suara membuat infrastruktur jaringan mengalami perkembangan dari berbasis kabel menjadi berbasis nirkabel atau yang biasa dikenal dengan *wireless*. Dengan hadirnya jaringan nirkabel, akses jaringan mampu dilakukan dimanapun dan kapanpun menggunakan gelombang radio [1]. Perkembangan jaringan nirkabel sejalan dengan konsep *Internet of Things*, dimana semua perangkat yang mendukung jaringan nirkabel akan dihubungkan dengan *internet* sehingga dapat saling berkomunikasi [2]. Selain itu, perangkat juga ditanamkan sensor yang memungkinkan pengendalian objek secara otomatis melalui *smartphone* atau komputer. Implementasi dari penggunaan sensor dengan biaya ekonomis di seluruh aspek yang mendukung konsep *Internet of Things* memunculkan teknologi baru bernama *wireless sensor network* [3].

Wireless sensor network secara umum dapat digambarkan sebagai jaringan nirkabel yang secara kooperatif digunakan untuk memantau, merasakan, dan mengendalikan kondisi fisik atau lingkungan seperti suhu, suara, getaran, tekanan, gerak atau polutan sehingga memungkinkan adanya interaksi antara orang atau komputer dengan lingkungan sekitar [4]. Seiring berkembangnya teknologi, penerapan *wireless sensor network* saat ini telah mencakup area kesehatan, militer, rumah, transportasi, logistik, dan area komersil lainnya [5]. Contoh penerapannya di kehidupan sehari-hari adalah untuk mendeteksi kebakaran hutan, memantau kelembaban dan suhu di perkebunan, dan mendeteksi penyusup di rumah. Pada penerapannya, *wireless sensor network* terdiri dari beberapa *sensor node* yang diletakkan di tempat yang berbeda untuk memonitor kondisi lingkungan tertentu. *Sensor node* bekerja satu sama lain untuk merasakan beberapa fenomena sesuai indikator yang ditentukan menjadi suatu informasi. Kemudian informasi tersebut dikumpulkan dan diolah untuk mendapatkan hasil yang relevan.

Sensor node yang dipasang di lingkungan dapat diakses secara fisik sehingga meningkatkan potensi terjadinya serangan. Dalam hal ini juga memungkinkan terjadi modifikasi *sensor node* yang mengakibatkan pengiriman informasi tidak sesuai dengan keadaan di lingkungan tersebut. Berbicara mengenai keamanan pada *wireless sensor network*, tidak lepas dari pemahaman mengenai permodelan *layer* di dalam jaringan komputer dan bagaimana mengetahui jenis serangan pada setiap *layer*. Terutama pada *network layer*, hal terpenting yang harus mendapat perhatian lebih adalah protokol *routing*. Protokol *routing* AODV merupakan salah satu protokol *routing single path* yang menerapkan prinsip pemilihan satu jalur terbaik menuju *destination* [6]. Beberapa serangan pada *network layer* diantaranya adalah serangan *blackhole*, serangan *wormhole*, serangan *sybil*, serangan *sinkhole*, dan serangan *hello flood*. Umumnya serangan-serangan tersebut memiliki tujuan tertentu dalam melakukan aksinya. Misalnya pada serangan *wormhole*, di mana serangan ini bertujuan untuk menggandakan paket dan mengubah rute pengiriman paket menuju penyerang dengan membuat sebuah terowongan yang diibaratkan sebagai lubang cacing.

Untuk menangani serangan yang terjadi, saat ini telah terdapat beberapa mekanisme deteksi dan penanggulangan misalnya melakukan otentikasi, pengecekan *redudancy, packet leashes* dengan menggunakan info geografi secara temporal, predistribusi kunci, deteksi menggunakan informasi keberadaan tetangga, mengawasi alur multidata, kalkulasi *one hop*, dan sebagainya [7]. Dari masing-masing mekanisme masih memiliki kelemahan seperti protokol *routing* yang digunakan tidak menerapkan desain teknik *single path*, efisiensi energi sangat kecil, adanya *redudancy* data yang dikirimkan, dan tidak adanya pendeteksi jika *sensor node* telah mengalami modifikasi dari penyerang [8].

Berdasarkan kelemahan tersebut, maka diperlukannya sebuah sistem yang dapat memvalidasi informasi dari *sensor node*. Jika terdapat ketidaksesuaian dengan kondisi sebenarnya, maka *sensor node* akan di nonaktifkan dari *base station*. Penelitian ini menggunakan metode *Network Development Life Cycle* yang merupakan suatu metode siklus pengembangan jaringan yang terdiri dari *analysis*, *design*, *simulation prototyping*, *implementation*, *monitoring*, dan *management* [9]

Sehingga judul penelitian ini, yaitu Mitigasi Serangan *Wormhole* pada Teknologi *Wireless Sensor Network* menggunakan *Protokol Routing* AODV dengan Sistem *Shutdown*. Diharapkan penelitian ini dapat menjadi suatu kajian di bidang teknologi jaringan dan menjadi solusi yang tepat dalam kaitannya dengan serangan *wormhole* pada *wireless sensor network*.

2. Tinjauan Pustaka

2.1 *Wireless Network* (Jaringan Nirkabel)

Menurut definisi dari Diane Barrett dan Todd King [10], jaringan nirkabel merupakan teknologi yang memungkinkan adanya komunikasi antara dua komputer menggunakan standar protokol jaringan tanpa menggunakan kabel.

2.2 *Wireless Sensor Network*

Menurut definisi dari Sujoko Sumaryono dan Widyawan [11], *wireless sensor network* adalah

sebuah perangkat elektronik yang menggabungkan teknologi sensor, *mikrokontroller*, memori, sistem operasi, komunikasi radio, dan sumber energi berupa baterai dalam satu *platform* yang terintegrasi. Pada *wireless sensor network*, *sensor node* disebar di sekitar lingkungan yang akan dilakukan *monitoring*. Setiap *sensor node* yang tersebar memiliki kemampuan untuk mendeteksi berbagai parameter fisis. Selanjutnya dilakukan proses transmisi data ke *sink* atau *gateway*. Data yang diterima *sink* atau *gateway* kemudian diberikan ke *smartphone* atau komputer untuk dilihat hasil pembacaannya kapanpun dibutuhkan secara *realtime* [12]. Secara umum *wireless sensor network* terdiri dari beberapa komponen utama yaitu:

1. *Sensor Node*

   Sensor node adalah perangkat yang mendeteksi objek dan mengirimkan data melalui jaringan nirkabel menuju *sink* atau *gateway* [13]. 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* [14].
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* [15].
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*

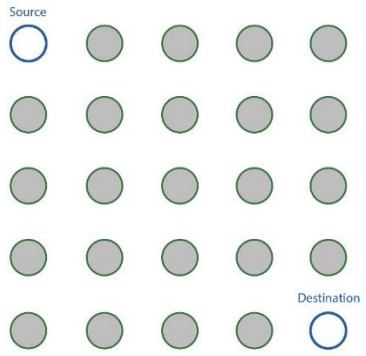
   User dapat mengakses informasi mengenai objek malalui *remote server* secara *real time*. Informasi tersebut diakses melalui koneksi internet atau satelit ke penyimpanan data berbasis *cloud*.

2.3 Persebaran *Node* pada *Wireless Network Network*

Persebaran *node* pada *wireless sensor network* diatur agar dapat melakukan *sensing* secara berkelanjutan dengan memperpanjang masa pakai dan tetap mempertahankan cakupan wilayahnya secara seragam. Persebaran *node* dibagi menjadi dua macam yaitu persebaran *static* dan persebaran acak.

1. Persebaran *Static*

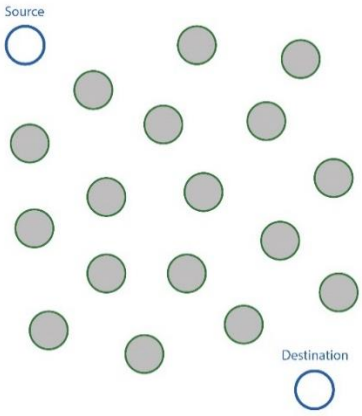
   Persebaran *static* dilakukan dengan memilih lokasi terbaik berdasarkan strategi optimasi dan lokasi *node* tidak akan berpindah. Contoh persebaran *static* pada *wireless sensor network* adalah persebaran *grid*. Area persebaran *grid* berupa persegi dan memiliki jarak yang sama antar *node* [16]. Di dalam persebaran grid, harus terdapat satu *node* yang bertanggung jawab untuk meneruskan informasi *routing* dan pengiriman paket data.



Gambar 1 Persebaran *Grid*

2. Persebaran Acak

   Persebaran acak dilakukan dengan menempatkan *sensor node* secara acak tanpa memperhitungkan jarak antar *sensor node*. Persebaran ini biasanya digunakan pada lingkungan berbahaya dengan *traffic* yang rendah dan pergerakan objek yang rendah, misalnya di kawasan gunung merapi atau tempat yang sering terkena bencana alam [16].



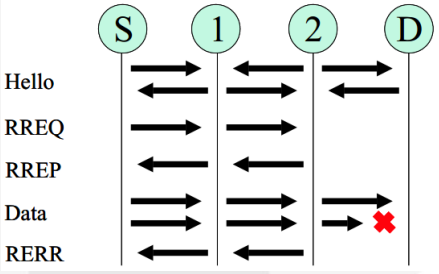
Gambar 2 Persebaran Acak

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* [17].

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 [18].

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 [19]



Gambar 3 Proses Pencarian Rute AODV [19]

2.5 Serangan *Wormhole*

Serangan *wormhole* merupakan jenis serangan pada *wireless sensor network* dimana penyerang mencatat paket pada satu lokasi di jaringan dan memindahkannya dengan membuat terowongan ke lokasi lain [8]. Terowongan ini memberikan ilusi seolah-olah *path* tersebut adalah *path* terpendek menuju *node* tujuan. Tidak seperti jenis serangan lainnya, serangan ini menyesatkan operasi *routing* tanpa sepengetahuan *node* yang sedang berkomunikasi. Karakteristik ini membuat serangan *wormhole* menjadi sangat penting untuk diidentifikasi dan membuat pertahanannya.

2.6 Parameter Uji

Kinerja suatu jaringan komputer dapat diukur dengan parameter *Quality of Service* (QoS) untuk menunjukkan konsistensi dan tingkat keberhasilan pengiriman data. Beberapa parameter yang dapat digunakan untuk mengukur kinerja jaringan komputer antara lain: *throughput*, *end to end delay*, dan *packet delivery ratio* [20]

1. *Throughput*

Throughput adalah jumlah waktu yang diambil oleh paket untuk mencapai tujuan. *Throughput* disebut juga

sebagai *bandwidth* dalam kondisi yang sebenarnya. *Bandwidth* lebih bersifat tetap sementara *throughput* bersifat dinamis tergantung pada trafik yang sedang terjadi. Rumus untuk menghitung *throughput* (1.1) adalah:

$$Throughput = \frac{Jumlah\ data\ dikirim}{waktu\ pengiriman\ data} \text{..... (1.1)}$$

Pada tabel 1 diperlihatkan kategori dari *throughput* menurut TIPHON:

Kategori *Throughput*	Nilai *Throughput (Bps)*	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	< 25	1

Tabel 1 Kategori *Throughput*

2. *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* (1.2) adalah:

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

Pada tabel 2 diperlihatkan kategori dari *end to end delay* menurut TIPHON:

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

Tabel 2 Kategori *Delay*

3. *Packet Delivery Ratio* (PDR)

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 %. Adapun rumus untuk menghitung *packet delivery ratio* (1.3) adalah:

$$PDR = \frac{Paket\ diterima}{Paket\ dikirim} \times 100\% \text{..... (1.3)}$$

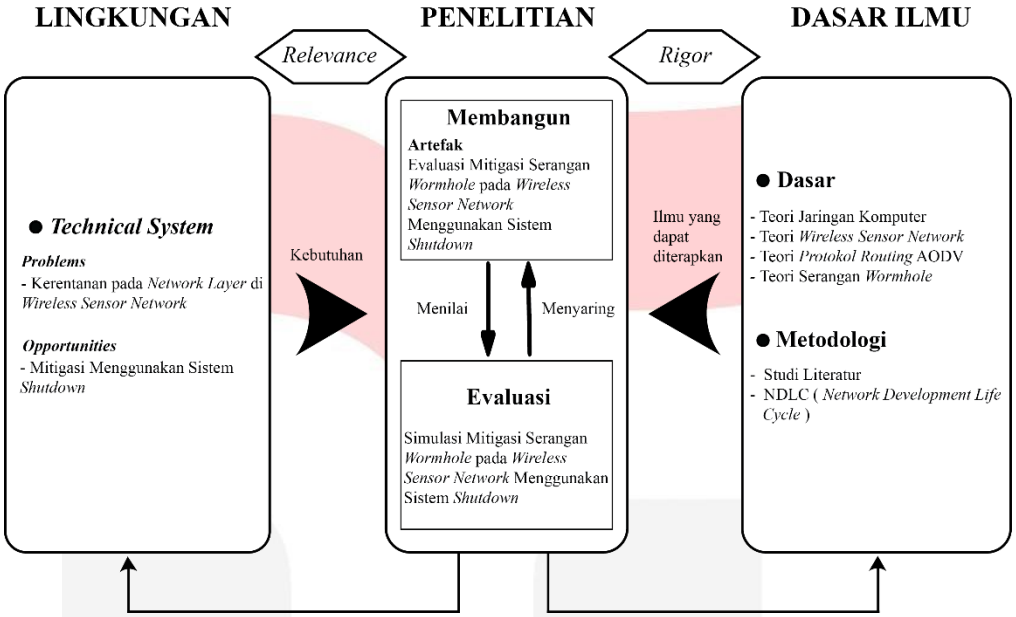
Selain parameter performansi jaringan komputer, parameter yang diuji adalah konsumsi energi. Energi diukur untuk mengetahui seberapa efisien penggunaan daya yang dikonsumsi saat *sensor node* melakukan transmisi paket maupun *receive* paket. Satuan energi adalah Joule. Konsumsi energi dipengaruhi oleh 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*. Adapun rumus untuk menghitung jumlah konsumsi energi (1.4) adalah:

$$Jumlah\ Konsumsi\ Energi = \sum energi\ tiap\ node \text{..... (1.4)}$$

3. Metode Penelitian

3.1 Model Konseptual

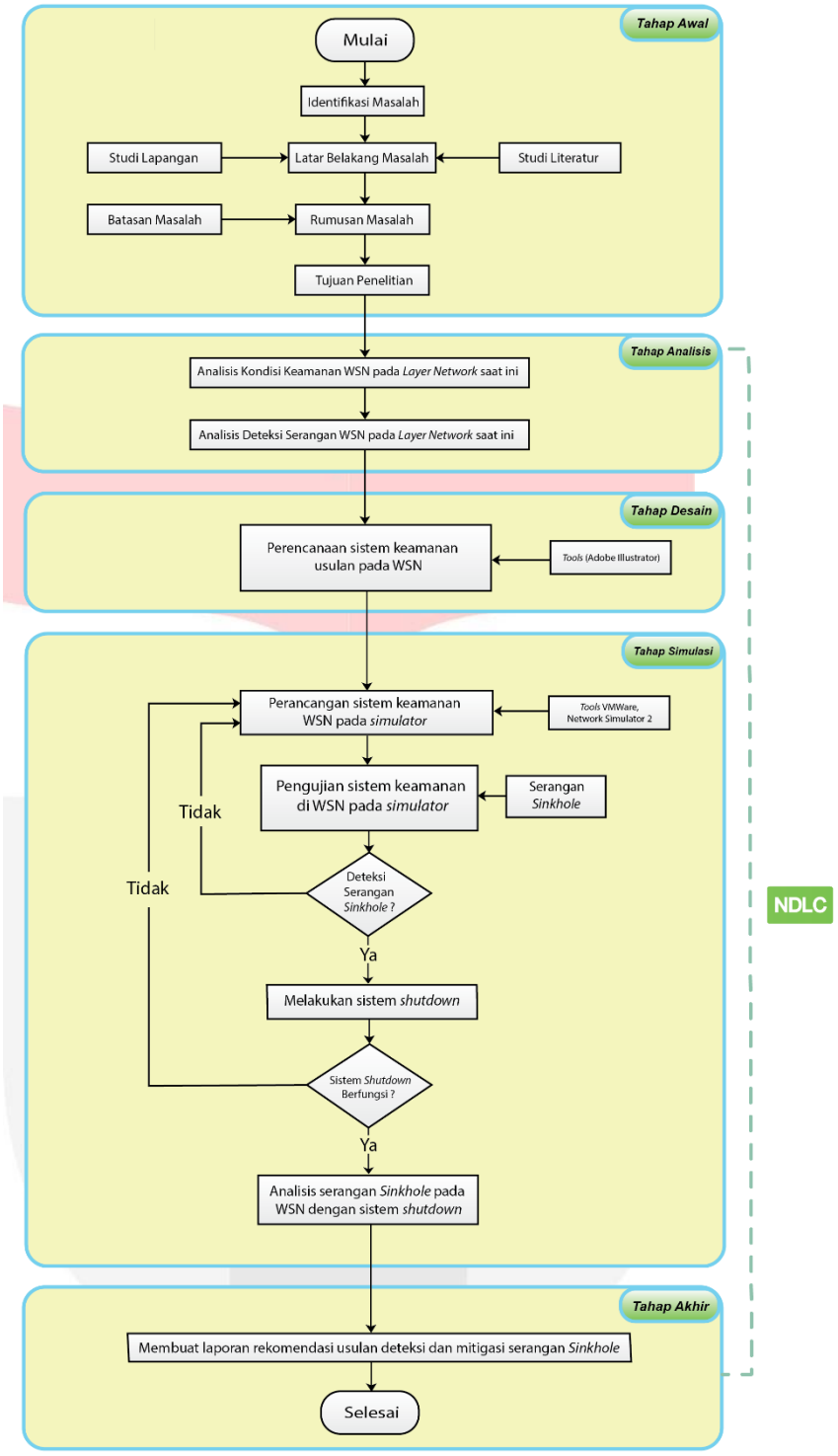
Model konseptual bertujuan untuk mengidentifikasi data dalam proses penelitian sehingga dapat membantu peneliti dalam merumuskan pemecahan masalah yang ada [21]. Model ini juga bertujuan untuk membantu mengidentifikasi faktor-faktor yang relevan, perumusan solusi, dan memberikan penjelasan agar masalah yang ada dapat dipahami dengan mudah. Model konseptual ini menggambarkan kerangka penelitian tugas akhir Deteksi dan Mitigasi Serangan *Sinkhole* pada Teknologi *Wireless Sensor Network* Menggunakan Network Simulator 2 yang bertujuan untuk membuat desain keamanan pada *Wireless Sensor Network* terhadap serangan *Sinkhole* sesuai standar. Gambaran model konseptual penelitian ini terlihat pada Gambar III.1



Gambar 4 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.

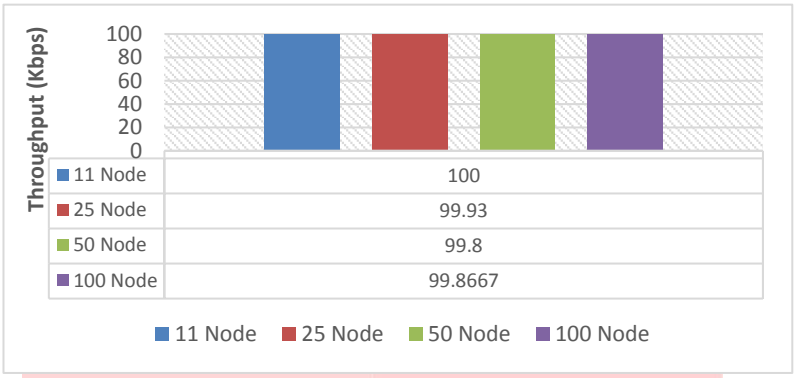


Gambar 5 Sistematika Penelitian

4. Hasil dan Analisis

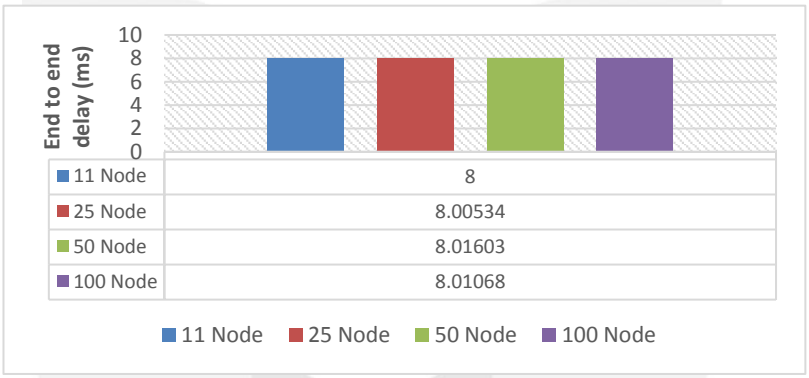
4.1 Pengujian Simulasi Tidak Ada Serangan

Simulasi tidak ada serangan dilakukan pada empat topologi untuk mengukur konsumsi energi dan performansi jaringan seperti *throughput*, *end to end delay*, dan *packet delivery ratio*.



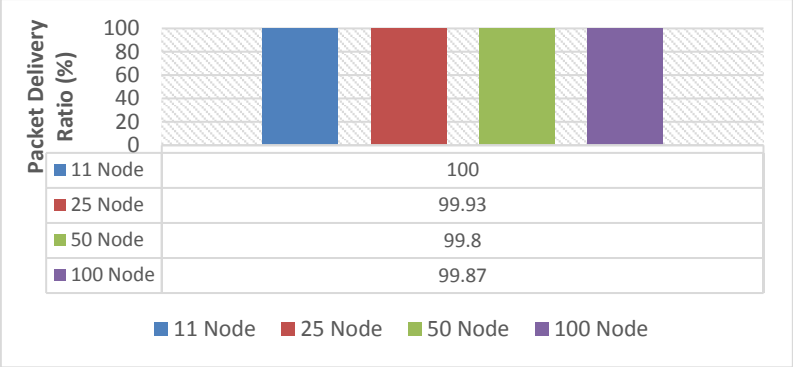
Gambar 6 Grafik nilai *throughput* saat tidak ada serangan

Pada Gambar 6, nilai *throughput* mengalami penurunan di setiap topologi persebaran *node*. Pada topologi 25 *node* nilai *throughput* mengalami penurunan sebesar 0,07 Kbps menjadi 99,83 Kbps. Pada topologi 50 dan 100 *node* mengalami nilai *throughput* juga mengalami penurunan menjadi 99.8 Kbps dan 99.8667 Kbps. Hal ini dikarenakan terdapat banyak *node* yang harus dilewati menuju *destination node*. Semakin banyak *node* yang dilewati semakin berkurang kecepatan paket data. *Data receive* juga berpengaruh terhadap nilai *throughput* karena *transport agent* yang digunakan adalah UDP, sehingga paket data dikirimkan tanpa adanya nomor urut atau pesan *acknowledge* yang memungkinkan adanya paket yang hilang selama pengiriman menuju destinasi.



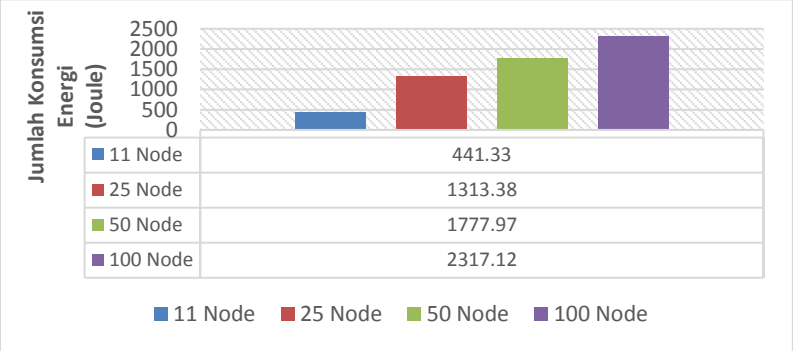
Gambar 7 Grafik nilai *end to end delay* saat tidak ada serangan

Berdasarkan Gambar 7, nilai *end to end delay* mengalami kenaikan pada setiap topologi persebaran *node*. Pada topologi 25 *node* nilai *end to end delay* mengalami kenaikan sebesar 0.00534 ms dibandingkan topologi 11 *node*. Sedangkan pada *node* 50 dan 100 nilai *end to end delay* mengalami kenaikan menjadi 8.01603 ms dan 8.01068. Nilai *end to end delay* bernilai kecil dikarenakan tidak adanya hambatan dalam proses pengiriman paket antara *source node* dengan *destination node*. Selain itu variasi jumlah *node* juga berdampak pada waktu yang dibutuhkan dalam pengiriman paket data walaupun tidak jauh berbeda. Semakin banyak jumlah *hop* yang dilalui maka semakin besar juga *delay* yang terjadi. Mengacu pada standar TIPHON tentang waktu *end to end delay*, nilai setiap topologi baik topologi 11 *node*, 25 *node*, 50 *node*, maupun 100 *node* termasuk kategori sangat bagus karena nilai *end to end delay* yang dihasilkan kurang dari 150 ms serta kualitas pengiriman dan penerimaan data yang baik.



Gambar 8 Grafik nilai *packet delivery ratio* saat tidak ada serangan

Seperti pada Gambar 8, nilai *packet delivery ratio* mengalami penurunan yang tidak jauh berbeda. Pada topologi 11 *node*, nilai *packet delivery ratio* mencapai nilai 100%. Hal ini menunjukkan bahwa jumlah paket data yang dikirimkan oleh *source node* sama dengan yang diterima pada *destination node*. Pada topologi 25 *node* terjadi penurunan nilai *packet delivery ratio* sebesar 0,07%. Sedangkan pada topologi 50 *node* terjadi penurunan sebesar 0,2% dan pada *node* 100 terjadi penurunan sebesar 0,13%. Penurunan nilai *packet delivery ratio* dipengaruhi oleh banyaknya *node* dan jalur *routing* AODV yang dilewati. Semakin banyak *node* maka semakin banyak *hop* yang harus dilewati untuk sampai ke destinasi. Sehingga jumlah paket data yang dikirim dan diterima menjadi semakin kecil walaupun tidak jauh berbeda.

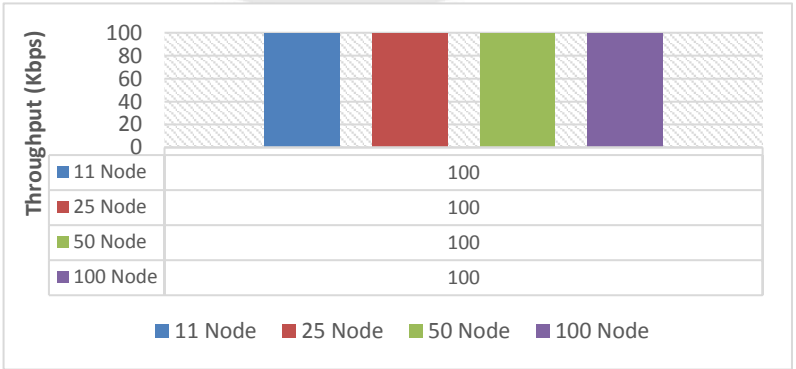


Gambar 9 Grafik jumlah energi saat tidak ada serangan

Gambar 9 menunjukkan grafik jumlah energi saat melakukan simulasi tanpa ada serangan. Perubahan nilai energi cenderung meningkat dari topologi 11 *node* hanya 441,33 Joule, topologi 25 *node* sebesar 1313,38 Joule, topologi 50 *node* sebesar 1777,97 Joule, dan topologi 100 *node* sebesar 2317,12 Joule. Hal ini berarti variasi jumlah *node* berpengaruh signifikan terhadap nilai energi yang digunakan. Semakin banyak *node* maka semakin banyak juga *node* yang harus dilewati untuk sampai ke *destination*. Jika *node* yang dilewati oleh suatu simulasi banyak maka jumlah energi yang digunakan tiap *node* juga akan semakin besar.

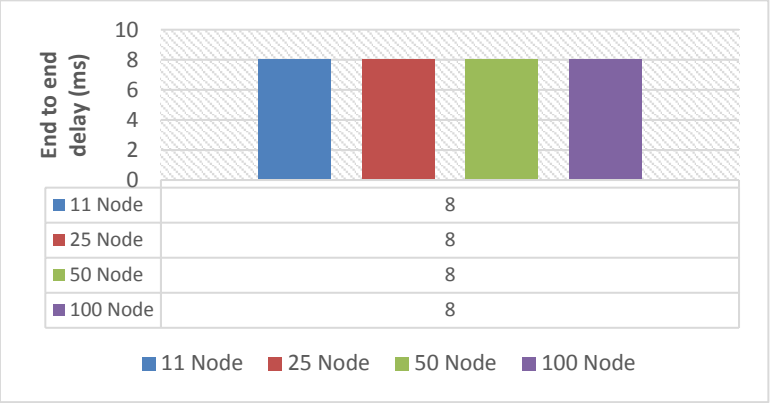
4.2 Pengujian Simulasi dengan Serangan

Simulasi dengan serangan dilakukan pada empat topologi untuk menghitung pengaruh adanya serangan terhadap energi dan performansi jaringan.



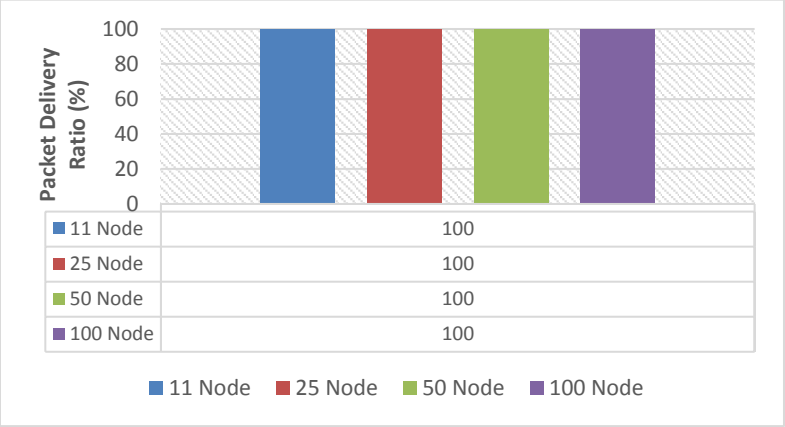
Gambar 10 Grafik nilai *throughput* saat ada serangan

Pada Gambar 10, terlihat bahwa nilai *throughput* saat ada serangan tidak mengalami perubahan baik di *node* 11, 25, 50, dan 100. Hal ini membuktikan bahwa banyaknya jumlah *node* tidak mempengaruhi nilai *throughput* meskipun terdapat *serangan wormhole.* Serangan *wormhole* mempengaruhi nilai *throughput* dikarenakan motivasi serangan *wormhole* adalah melakukan *eavesdropping* pada paket yang dikirimkan menuju *destination node*. Serangan *wormhole* juga melakukan perubahan jalur *routing* yang memperpendek jalur pengiriman sehingga nilai *throughput* tidak mengalami penurunan. Karena jalur yang ditempuh oleh *node* lebih pendek, maka keberhasilan paket data sampai ke tujuan lebih besar. Hal ini yang membuat nilai *throughput* pada setiap *node* tidak mengalami perubahan.



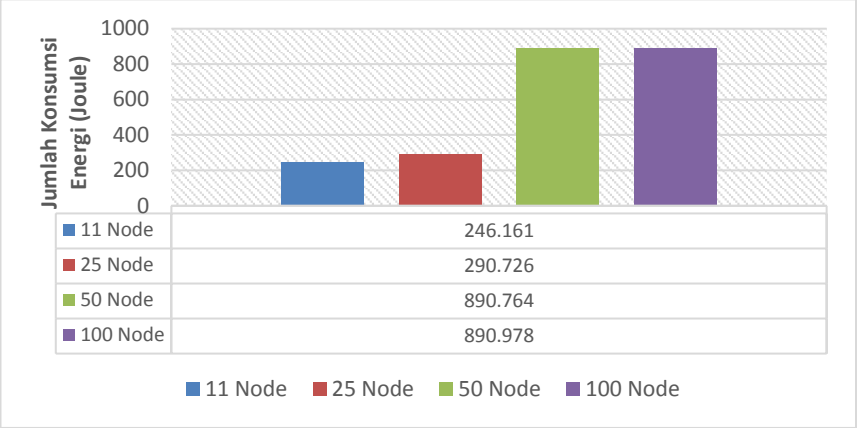
Gambar 11 Grafik nilai *end to end delay* saat ada serangan

Seperti pada Gambar 11 terlihat bahwa nilai *end to end delay* saat ada serangan tidak mengalami perubahan baik di *node* 11, 25, 50, dan 100. Hal ini membuktikan bahwa jumlah *node* tidak mempengaruhi nilai *end to end delay* meskipun terdapat *serangan wormhole.* Serangan *wormhole* membuat nilai *end to end delay* stabil karena jalur yang ditempuh oleh data lebih pendek, maka data lebih cepat sampai ke tujuan. Mengacu pada standar TIPHON tentang waktu *end to end delay*, nilai setiap topologi baik topologi 11 *node*, 25 *node*, 50 *node*, dan 100 *node* termasuk kategori sangat bagus karena nilai *end to end delay* yang dihasilkan kurang dari 150 ms meskipun ada serangan *wormhole*.



Gambar 12 Grafik nilai *packet delivery ratio* saat ada serangan

Gambar 12 menunjukkan grafik tingkat keberhasilan pengiriman paket data sampai ke *destination node* pada topologi 11, 25, 50, dan 100 *node* sebesar 100%. Hal ini membuktikan bahwa jumlah *node* tidak mempengaruhi nilai *packet delivery ratio* meskipun terdapat *serangan wormhole.* Serangan *wormhole* membuat nilai *packet delivery ratio* stabil karena motivasi serangan *wormhole* hanya melakukan *eavesdropping*, tidak merusak atau men-*drop* paket yang dikirim ke destinasi. Selain itu jalur yang ditempuh oleh *node* lebih pendek, maka persentase keberhasilan pengiriman data lebih besar.



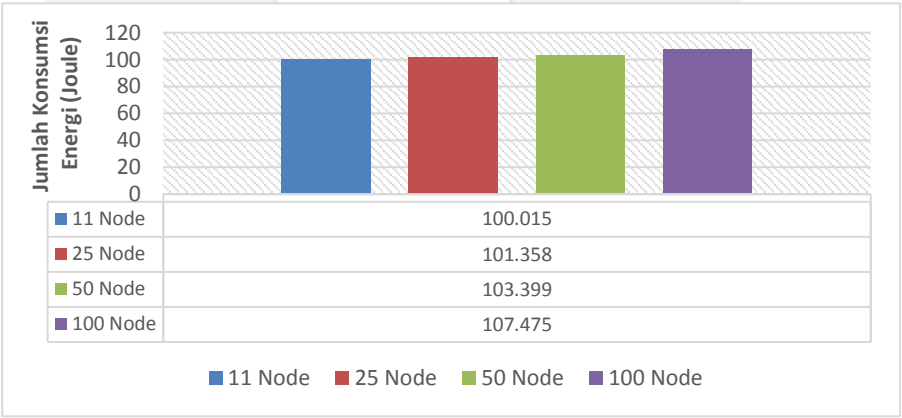
Gambar 13 Grafik jumlah energi saat ada serangan

Berdasarkan Gambar 13 jumlah energi yang digunakan oleh *node* ketika ada serangan mengalami peningkatan. Misalnya pada topologi persebaran 11 *node* yang di dalamnya terdapat 3 *attacker node*, energi yang dihasilkan adalah sebesar 264.161 Joule. Sedangkan pada topologi persebaran 50 *node* di mana terdapat 2 *attacker node* diantara 50 *node* tersebut, energi yang dihasilkan adalah sebesar 890,764 Joule. Hal ini menunjukkan bahwa adanya serangan dan variasi jumlah *node* mempengaruhi jumlah energi yang dikonsumsi. Semakin banyak jumlah *sensor node* dan *attacker node*, semakin besar jumlah energi yang dikonsumsi oleh *node*.

4.3 Pengujian Simulasi dengan Serangan dan Mengimplementasikan Sistem *Shutdown*

Simulasi dengan serangan dan mengimplementasikan sistem *shutdown* dilakukan untuk mengetahui keefektifan dari sistem *shutdown* dalam memitigasi serangan yang diukur dengan perubahan energi dan performansi jaringan. Sistem *shutdown* menggunakan *revocation* untuk mendeteksi adanya serangan *wormhole*, dimana setiap *node* diberikan *security key* sebagai identitas. Ketika WSN melakukan validasi *security key* ke semua *node* sebelum paket dikirimkan dan terdapat salah satu *node* yang tidak cocok dengan *security key* yang telah didaftarkan, maka *node* tersebut merupakan *attacker node*.

Ketika sistem mendeteksi adanya *attacker node* pada simulasi maka sistem *shutdown* akan menghentikan seluruh komunikasi pada *attacker node* dan *destination node* agar tidak ada pengiriman paket data yang salah ke *user*. Hal tersebut terjadi karena serangan dimulai pada detik ke 0 sesuai dengan mulainya *routing* AODV dalam melakukan *route discovery*, maka di saat itu juga sistem *shutdown* aktif sehingga nilai *throughput*, *end to end delay*, dan *packet delivery ratio* adalah 0.

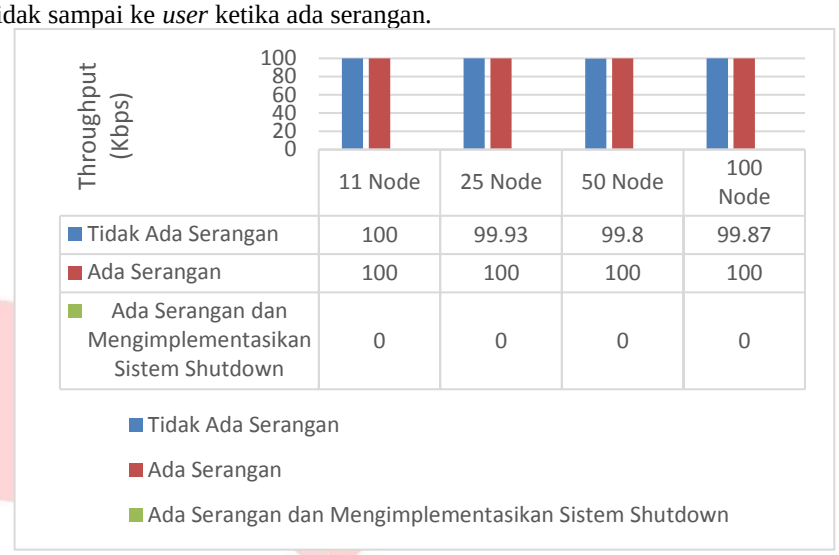


Gambar 14 Grafik jumlah energi saat ada serangan dan sistem *shutdown*

Jika nilai performansi jaringan seperti *throughput*, *end to end delay*, dan *packet delivery ratio* pada simulai saat ada serangan dan sistem *shutdown* adalah 0, berbeda dengan jumlah energi yang digunakan. Jumlah energi yang digunakan pada skenario ini mengalami peningkatan. Hal ini menunjukkan bahwa banyaknya *sensor node*, *attacker node*, dan adanya sistem *shutdown* meningkatkan jumlah energi yang dikonsumsi oleh *node*.

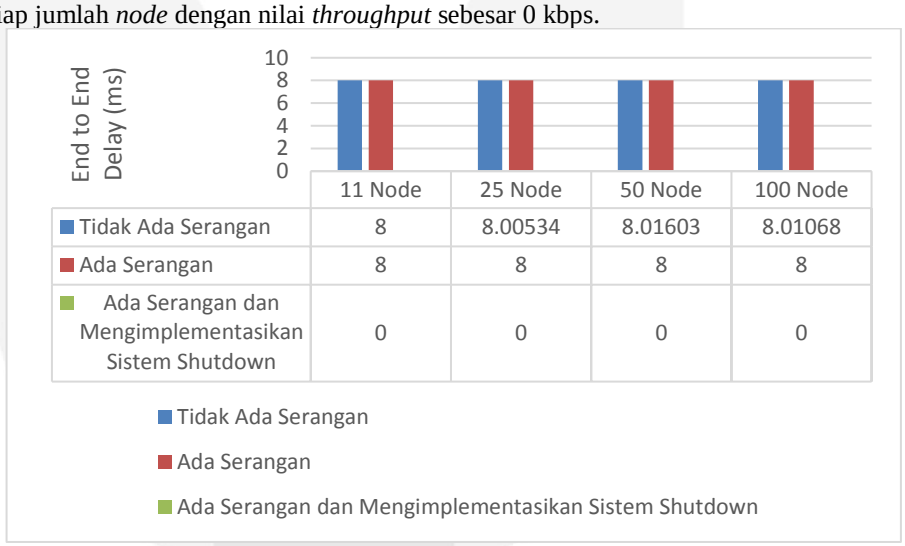
4.4 Analisis Sistem Secara Keseluruhan

Secara keseluruhan adanya serangan *wormhole* dan sistem *shutdown* tidak mempengaruhi nilai performansi jaringan pada *wireless sensor network* namun hanya berpengaruh pada jumlah energi yang digunakan. Adanya sistem *shutdown* terbukti menjadi sarana efektif untuk menghentikan komunikasi agar pengiriman paket tidak sampai ke *user* ketika ada serangan.



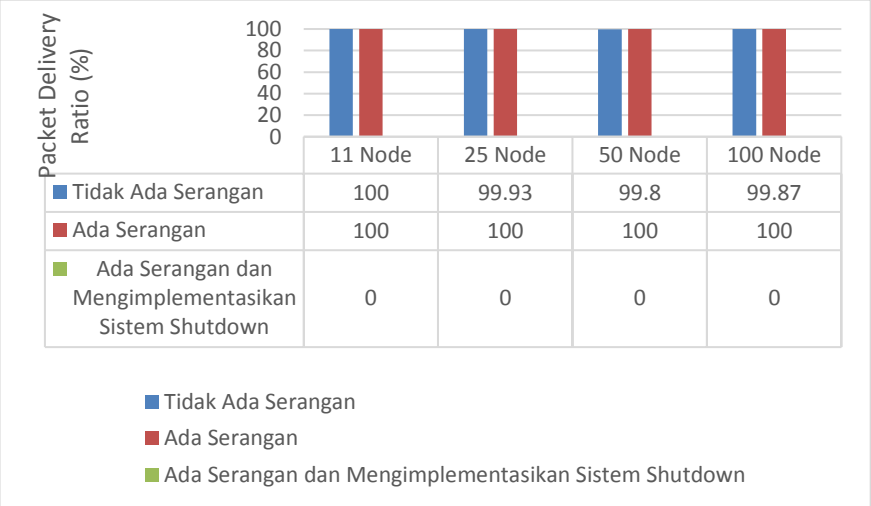
Gambar 15 Perbandingan Nilai Throughput Seluruh Skenario

Hasil pengukuran *throughput* dari seluruh skenario dapat dilihat pada Gambar 15, di mana nilai tertinggi *throughput* adalah sebesar 100 Kbps pada topologi 10 *node* di skenario tidak ada serangan dan pada seluruh topologi persebaran *node* di skenario ada serangan. Sedangkan nilai *throughput* terendah dari semua skenario terdapat pada skenario ada serangan dan mengimplementasikan sistem *shutdown* dengan nilai yang konsisten pada setiap jumlah *node* dengan nilai *throughput* sebesar 0 kbps.



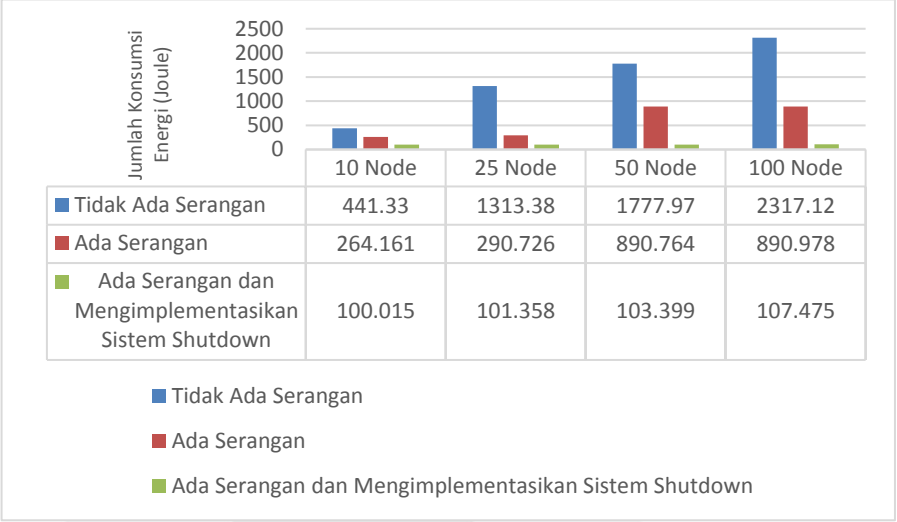
Gambar 16 Perbandingan Nilai End to End Delay Seluruh Skenario

Hasil pengukuran *end to end delay* dari seluruh skenario dapat dilihat pada Gambar 16, di mana nilai tertinggi *end to end delay* adalah sebesar 8,01603 ms pada skenario tidak ada serangan dan 8ms di semua *node* pada skenario ada serangan. Sedangkan nilai *end to end delay* terendah dari semua skenario terdapat pada skenario ada serangan dan mengimplementasikan sistem *shutdown* dengan nilai yang konsisten pada setiap jumlah *node* dengan nilai *end to end delay* sebesar 0 ms.



Gambar 17 Perbandingan Nilai PDR Seluruh Skenario

Gambar 17 berisi hasil pengukuran PDR dari seluruh skenario, di mana nilai tertinggi PDR adalah sebesar 100%. Sedangkan nilai PDR terendah dari seluruh skenario terdapat pada skenario ada serangan dan mengimplementasikan sistem *shutdown* dengan nilai yang konsisten pada setiap jumlah *node* dengan nilai PDR sebesar 0%. Dari ketiga skenario dapat diambil kesimpulan bahwa ketika tidak ada serangan, nilai PDR dipengaruhi oleh banyaknya *node* dan jalur *routing* AODV. Dengan adanya serangan *wormhole*, nilai PDR menjadi stabil karena motivasi serangan *wormhole* adalah merubah jalur *routing* menjadi lebih pendek dan melakukan *eavesdropping*, tidak merusak atau men-*drop* paket yang dikirim ke destinasi.



Gambar 18 Perbandingan Jumlah Energi Seluruh Skenario

Jumlah konsumsi energi pada Gambar 18 yang memiliki nilai paling besar terdapat pada skenario tidak ada serangan dengan nilai total konsumsi energi sebesar 2317,12 Joule pada topologi 100 *node.* Pada skenario ada serangan, seluruh topologi persebaran *node* mengalami peningkatan konsumsi energi. Perubahan jumlah konsumsi energi yang tidak jauh berbeda terjadi pada saat mengimplementasikan sistem *shutdown*.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian Mitigasi Serangan *Wormhole* Pada Teknologi *Wireless Sensor Network* Menggunakan Protokol *Routing* AODV Dengan Sistem *Shutdown*, dapat disimpulkan bahwa:

1. Simulasi serangan *wormhole* dilakukan dengan menggunakan NS-2.35 pada sistem operasi Ubuntu 16.04. Serangan dibuat dengan cara memodifikasi *script* tcl dan MAC *layer* pada NS-2.35. Modifikasi dilakukan agar terbentuk *tunnel* antara *attacker node* sehingga paket data yang dikirimkan tidak melewati jalur *routing* yang seharusnya.
2. Cara kerja sistem *shutdown* adalah ketika sistem mendeteksi adanya serangan *wormhole* pada simulasi, maka sistem *shutdown* akan menghentikan seluruh komunikasi pada *attacker node* dan *destination node* sehingga tidak ada pengiriman paket data yang salah ke *user*. Serangan *wormhole* dideteksi dengan cara melakukan *revoke* antara *estimated key* dengan *key* yang didapatkan pada saat melakukan *route discover*. Jika *estimated key* sama dengan *key* yang didapatkan saat melakukan *discover route* AODV maka simulasi terindikasi adanya serangan dan saat itu juga sistem *shutdown* aktif mematikan *attacker node* dan *destination node*.
3. Penerapan sistem *shutdown* tidak menurunkan performansi jaringan komputer baik dari segi *throughput, end to end delay*, dan *packet delivery ratio*. Performasi tidak mengalami penurunan karena baik ada maupun tidak ada serangan *shutdown* nilai dari *throughput, end to end delay*, dan *packet delivery ratio* tetap sama dan tidak mengalami perubahan.
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 *node* yang terletak di jalur *routing* terbaik pada saat melakukan *discover route*.

5.2 Saran

Adapun saran yang dapat diberikan untuk penelitian selanjutnya adalah:

1. Serangan dilakukan dengan jumlah node lebih dari 100 node dan waktu yang lebih lama yaitu lebih dari 120 detik.
2. Parameter performansi jaringan yang diukur lebih bervariasi misalnya mengukur *response time*.

6. Daftar Pustaka

[1] CISCO, "What Is a Wireless Network?: The Basics," 26 September 2017. [Online]. Available: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/wireless-network.html.

[2] P. H. N. Saha, A. Mandal and A. Sinha, "Recent Trends in the Internet of Things," 2017.

[3] J. A. Manrique, J. S. Rueda-Rueda and J. M. Portocarrero, "Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview," 2016.

[4] M. Matin and M. Islam, "Overview of Wireless Sensor Network," 2012.

[5] P. Maidamwarr and N. Chavhan, "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network," 2012.

[6] P. R. Satav and D. P. M. Jawandhiya, "Review on Single-Path Multi-Path Routing Protocol in Manet: A Study," 2016.

[7] J. Sen, "A Survey on Wireless Sensor Network Security," 2009.

[8] G. S, T. Bassavaraju, M. D.H and S. K. Sarkar, "Issues in Wireless Sensor Networks," 2008.

[9] J. E. Goldman and P. T. Rawles, Applied Data Communications, A business-Oriented Approach, 2001.

[10] D. Barrett and T. King, Computer Networking Illuminated, Sudbury: Jones and Bartlett Publisher, 2005.

[11] S. Sumaryono and Widyawan, "Pengembangan Wireless Sensor Network untuk Aplikasi Home Controlling," 2012.

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

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

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

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

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

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

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

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

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

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

[22] T. I. Assosiation, Telecommunication Industry Assosiation, TIA-942 Standard, 2012.

[23] Y. Sidharta and D. Widjaja, "Perbandingan Unjuk Kerja Protokol Routing Ad Hoc On-Demand Distance Vector (AODV) dan Dynamic Source Routing (DSR) pada Jaringan Manet," 2013.

[24] B. Nugrooho, N. A. Setiawan and S. Fauziati, "Analisis Kinerja Protokol Reaktif pada Jaringan Manet dalam Simulasi Jaringan Menggunakan Network Simulator dan Tracegraph," 2013.

[25] S. A. Sasongko, Sukiswo and A. A. Zahra, "ANALISIS PERFORMANSI DAN SIMULASI PROTOKOL ZRP (ZONE ROUTING PROTOCOL) PADA MANET (MOBILE AD HOC NETWORK) DENGAN MENGGUNAKAN NS-2," 2012.

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