JURNAL REKAYASA SISTEM DAN INDUSTRI
e-ISSN: 2579-9142 p-ISSN: 2356-0843
http://jrsi.sie.telkomuniversity.ac.id/index.php/JRSI

Mitigasi Serangan Wormhole pada Teknologi Wireless Sensor Network Menggunakan Protokol Routing Aodv dengan Sistem Shutdown

Mitigation of Wormhole Attack on Wireless Sensor Network Using Aodv Routing Protocol with Shutdown System

Tania Almira Pamudji*, M Teguh Kurrniawan, Adityas Widjajarto

Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

ARTICLE INFO

Article history:
Diterima xx-xx-xx
Diperbaiki xx-xx-xx
Disetujui xx-xx-xx

Kata Kunci:
Wireless sensor network, Serangan *wormhole*, *Protokol routing AODV*, Sistem shutdown

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 adalah *Ad Hoc On-Demand Distance Vector* (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 dengan sistem *shutdown* terjadi efisiensi energi dan performansi dengan penurunan jumlah konsumsi energi secara eksponensial dan tidak adanya penurunan dalam performansi jaringan jika dibandingkan ketika tidak ada serangan dan ada serangan namun tidak mengimplementasikan sistem *shutdown*. Sehingga sistem *shutdown* dapat menjadi salah satu solusi efektif dalam memitigasi serangan *wormhole*.

Keywords:
Wireless sensor network, Wormhole attack, AODV routing protocol, Shutdown system

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 brings energy and performance efficiency by decreasing the amount of exponential energy consumption and there is no decrease in network performance when compared to when there is no attack and there is an attack but does not implement a shutdown system. So, the shutdown system can be one effective solution in mitigating wormhole attacks.

*Penulis korespondensi
Email: almiratania@student.telkomunicersity.ac.id (Pamudji, T.A.), teguhkurniawan@telkomuniversity.ac.id (Kurniawan, M.T.) adtwjrt@telkomuniversity.ac.id (Widjajarto, A.)

doi: https://doi.org/10.25124/jrsi.v5i01.317

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 sistem mendeteksi adanya serangan, maka *attacker node* dan *destination node* akan di nonaktifkan agar tidak terjadi pengiriman informasi yang salah ke *user*. 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. Studi Literatur

2.1 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].

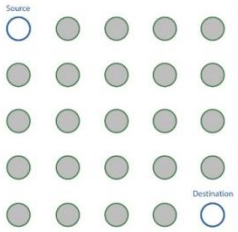
2. *Sink Node* / *Base Station*
   Sink node adalah perangkat yang mengumpulkan informasi dari *sensor node* menuju ke penyimpanan data biasanya dalam bentuk *cloud*. Komponen ini dapat diibaratkan sebagai gerbang keluar masuk *(gateway)* informasi baik dari *sensor node* maupun perangkat lain ke *wireless 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*.

2.2 Klasifikasi Persebaran Node pada Wireless Sensor 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* seperti terlihat pada gambar 1. 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 seperti terlihat pada gambar 2 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].

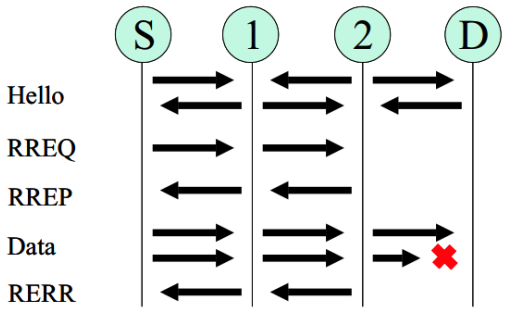
Gambar 2 Persebaran acak

2.3 Protokol Routing pada Wireless Sensor 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].

Seperti terlihat pada gambar 3, 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].

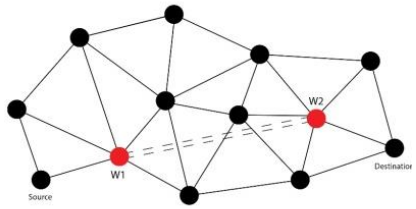
AODV menggunakan *destination sequence number* untuk menjaga informasi mengenai *reverse path* yang mengarah ke *source node*. *Reverse Path* terbentuk saat RREQ menempuh *node* yang dituju, dimana setiap RREQ akan diidentifikasi dari *node* sekitar yang mengirimkan RREQ tadi. Saat *node* yang dituju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

2.4 Wormhole Attack

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 pertahanann



Gambar 4 *Wormhole attack*

2.5 Pencegahan Serangan Wormhole Saat Ini

Protokol untuk mencegah serangan *wormhole* dalam *wireless sensor network* sebenarnya telah banyak ditemukan, akan tetapi setiap protokol masih memiliki masalah efisiensi biaya yang cukup rendah. Protokol berbasis *time synchronization* seperti *temporal packet leash* dan *time of flight* membutuhkan biaya besar dan peralatan yang tidak lazim digunakan untuk mengaplikasikan *time synchronization* ketat di setiap *node*-nya. Sedangkan protokol seperti *geographical packet leashes* dan *echo protocol* membutuhkan biaya besar untuk instalasi peralatan yang dibutuhkan setiap *node*. Protokol APIT mengharuskan *node* memiliki peralatan khusus untuk berada pada posisi tertentu yang terkadang sulit dilakukan di *wireless ad-hoc network*. *Wormhole attack* dengan menggunakan *global positioning system* (GPS) pada *node* dan metode perhitungan *hop* ditemukan kelemahan. Adapun kelemahan tersebut diantaranya pada protokol ini jarak antara *wormhole* dengan *node* terdekat pada sebaran tidak boleh terlalu besar dan peletakkan posisi *node* di dalam jaringan baik *node* GPS maupun *node non*-GPS sangat mempengaruhi kinerja protokol karena akan menyebabkan protokol tidak dapat mendeteksi adanya serangan meskipun protokol tersebut telah mengalami serangan [10].

2.6 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. 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*.

2.6.1 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:

$$\text{PDR} = \frac{Jumlah\ paket\ yang\ diterima}{Jumlah\ paket\ yang\ dikirim} \text{ x } 100\%. \qquad (1)$$

2.6.2 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:

$$End\ to\ end\ delay = \frac{Total\ waktu}{Total\ paket\ yang\ diterima} \qquad (2)$$

2.6.3 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:

$$Throughput = \frac{Jumlah\ data\ dikirim}{Waktu\ pengiriman\ data} \qquad (3)$$

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*.

2.6.4 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.

$$Jumlah\ Konsumsi\ Energi = \sum energi\ tiap\ node \qquad (4)$$

2.7 Parameter Sistem

Simulasi jaringan *wireless sensor network* dilakukan menggunakan simulator *Network Simulator* versi 2.35 (NS-2.35) berdasarkan penelitian sebelumnya. Simulator NS-2.35 merupakan simulator yang dirancang khusus untuk penelitian dalam jaringan komunikasi komputer. Proses simulasi ini menggunakan parameter asumsi berdasarkan penelitian sebelumnya 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 Byte. *Transport agent* yang digunakan adalah UDP (*User Datagram Protocol*) dan *application agent* yang digunakan adalah CBR (*Constant Bit Rate*).

2.8 Perancangan Topologi

Topologi yang digunakan untuk simulasi *wireless sensor network* adalah topologi menggunakan persebaran *grid* dengan jumlah *node* yaitu 11, 25, 50, 100 dan area simulasi seluas 1000 x 1000 m^2. Masing-masing topologi akan diberikan *wormhole attack* dan sistem shutdown sesuai dengan skenario dimana *wormhole node* akan bertindak sebagai *attacker* yang memiliki dua identitas dalam jaringan *wireless sensor network*.

Tabel 1
Parameter Sistem

No	Parameter	Nilai
1	Simulator	NS-2.35
2	Waktu Simulasi	120 detik
3	Jumlah *node*	11, 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 Byte
11	Jenis Serangan	*Wormhole Attack*

Mitigasi serangan *wormhole* pada *wireless sensor network* dengan sistem *shutdown* dibuat menjadi beberapa skenario. Adapun skenario yang dilakukan antara lain:

1. Skenario jaringan tidak ada serangan.
2. Skenario jaringan terserang *wormhole*.
3. Skenario jaringan terserang *wormhole* dan mengimplementasikan sistem *shutdown*.

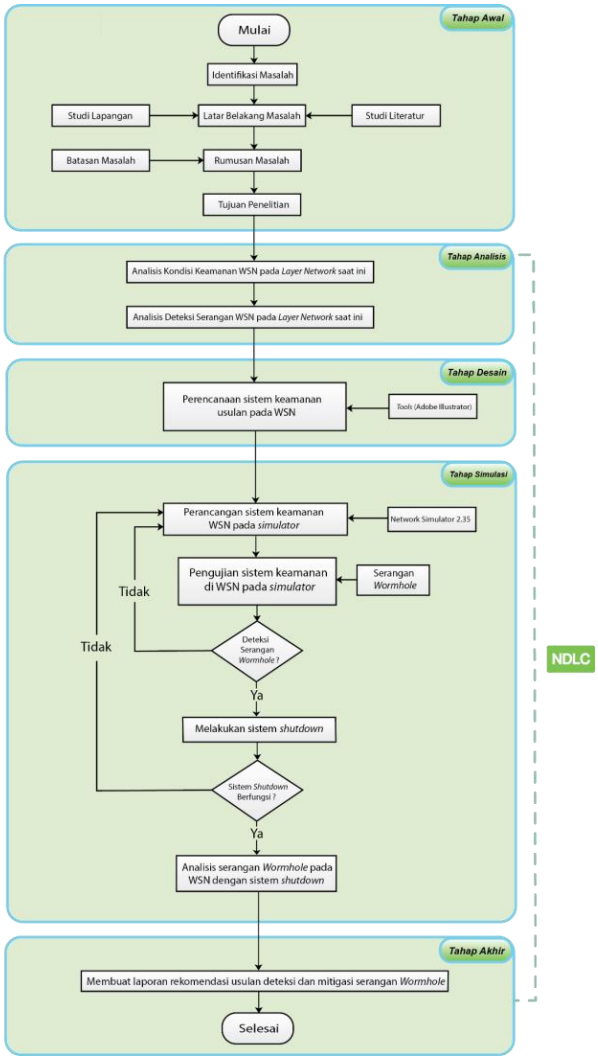
Parameter yang diukur pada simulasi adalah energi dan performansi jaringan seperti *throughput*, *end to end delay*, dan *packet delivery ratio*. Suatu jaringan dikatakan memiliki performansi yang sangat baik jika nilai *throughput* 100%, nilai *end to end delay* <150 ms, dan nilai *packet delivery ratio* 100%. 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 sistem melakkan *revoke* antara *security key* dengan *key* yang didapatkan pada saat melakukan *route discovery*. Jika *security key* tidak sama dengan *key* yang didapatkan saat melakukan *route discovery* AODV maka simulasi terindikasi adanya serangan dan saat itu juga sistem *shutdown* aktif mematikan *attacker node* dan *destination node*.

3. Metode Penelitian

Metode yang digunakan pada penelitian ini dijelaskan menggunakan 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. Sehingga peneliti dapat menjelaskan tentang model konseptual pada penelitian tugas akhir ini yang bertujuan untuk membuat racangan usulan deteksi dan mitigasi pada keamanan *wireless sensor network* terhadap serangan *wormhole*.

Permasalahan dan peluang yang ada pada penelitian ini berada pada bagian lingkungan, yaitu pada *technical system*. Berdasarkan hasil analisis didapatkan sebuah kesimpulan bahwa, permasalahan pada *technical system* adalah adanya kerentanan di *network layer* pada *wireless sensor network*. Dari permasalahan tersebut, didapatkan peluang untuk mengurangi kerentanan pada *network layer* yaitu dengan melakukan mitigasi serangan *wormhole* menggunakan sistem *shutdown*. Dengan masalah dan peluang yang ada pada bagian penelitian dihasilkan sebuah artefak berupa evaluasi mitigasi serangan *wormhole* pada *wireless sensor network* menggunakan sistem *shutdown*.

Untuk menghasilkan evaluasi mitigasi serangan *wormhole* pada *wireless sensor network* menggunakan sistem *shutdown*, maka diperlukan dasar ilmu dan metode yang dapat membantu untuk membuat evaluasi. Adapun dasar ilmu yang digunakan antara lain teori jaringan komputer, teori *wireless sensor network*, teori protokol *routing* AODV, dan teori serangan *wormhole*. Sedangkan metode yang digunakan yaitu studi literatur dan metodologi *Network Development Life Cycle* (NDLC). Evaluasi yang dihasilkan berupa simulasi mitigasi serangan *wormhole* pada *wireless sensor network* menggunakan sistem *shutdown*. Adapun tahapan yang dilakukan dalam penelitian ini diantaranya adalah tahap awal (tahap identifikasi), tahap analisis, tahap desain, dan tahap simulasi seperti terlihat pada Gambar 5.

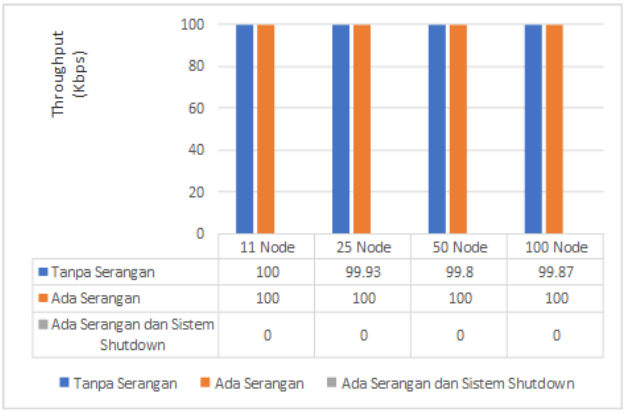


Gambar 5 Tahapan yang dilakukan pada penelitian

Hasil Pengujian Dan Analisis

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.

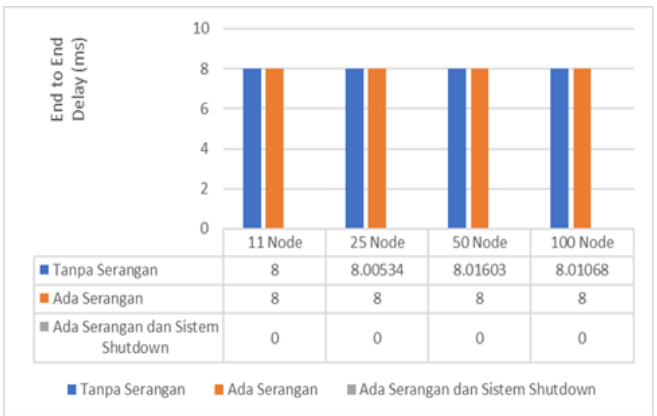


Gambar 6 Perbandingan nilai *throughput* seluruh skenario

Hasil pengukuran *throughput* dari seluruh skenario dapat dilihat pada Gambar 6, di mana nilai tertinggi *throughput* adalah sebesar 100 Kbps pada topologi 11 *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.

Dari ketiga skenario dapat diambil kesimpulan bahwa ketika tidak ada serangan, nilai *throughput* dipengaruhi oleh banyaknya *node* dan jalur *routing*. Dengan adanya serangan *wormhole*, nilai *throughput* menjadi stabil karena motivasi serangan *wormhole* adalah merubah jalur *routing* menjadi lebih pendek dan hanya melakukan *eavesdropping*, tidak merusak atau men-*drop* paket yang dikirim ke *destination node*.

Ketika sistem *shutdown* diimplementasikan, nilai *throughput* tidak dapat diukur karena sistem *shutdown* mendeteksi terjadinya serangan *wormhole* pada saat *route discovery* oleh protokol *routing* AODV. Sistem *shutdown* membuat paket tidak terkirim dengan mematikan komunikasi dari sumber ke destinasi sehingga *attacker node* tidak melakukan *eavesdropping* pada paket yang dikirimkan.

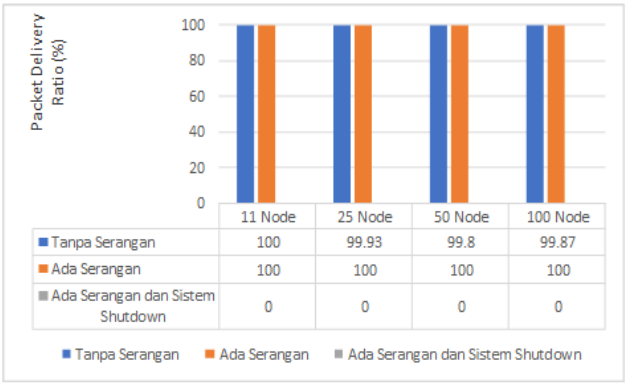


Gambar 7 Perbandingan nilai *end to end delay* seluruh skenario

Hasil pengukuran *end to end delay* dari seluruh skenario dapat dilihat pada Gambar 7, di mana nilai tertinggi *end to end delay* adalah sebesar 8,01603 ms pada skenario tidak ada serangan dan 8 ms 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.

Dari ketiga skenario dapat diambil kesimpulan bahwa ketika tidak ada serangan, nilai *end to end delay* dipengaruhi oleh jalur *routing* dan banyaknya *node*. Dengan adanya serangan *wormhole*, nilai *end to end delay* menjadi stabil karena motivasi serangan *wormhole* adalah melakukan *eavesdropping* dan merubah jalur *routing* menjadi lebih pendek.

Ketika sistem *shutdown* diimplementasikan, perfomansi jaringan tidak dapat diukur karena sistem *shutdown* mendeteksi terjadinya serangan *wormhole* pada saat protokol *routing* AODV melakukan *route discovery*. Sistem *shutdown* membuat paket tidak terkirim dengan mematikan komunikasi dari sumber ke destinasi sehingga *attacker node* tidak melakukan *eavesdropping* pada paket yang dikirimkan.



Gambar 8 Perbandingan nilai *packet delivery ratio* seluruh skenario

Gambar 8 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.

Ketika sistem *shutdown* diimplementasikan, nilai PDR tidak dapat diukur karena sistem *shutdown* mendeteksi terjadinya serangan *wormhole* pada saat terjadinya

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* dapat 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. Sistem *shutdown* yang diterapkan mematikan *sensor node* yang telah mengalami modifikasi dari penyerang sebelum informasi tersebut diproses oleh sistem dan dikirim ke *user*.
3. Penerapan sistem *shutdown* tidak mempengaruhi performansi jaringan komputer baik dari segi *throughput, end to end delay*, dan *packet delivery ratio* dibuktikan dengan hasil yaitu sebesar 0. Hal ini disebabkan karena sistem *shutdown* aktif menghentikan seluruh komunikasi antara *attacker node* dan *destination node* yang menyebabkan paket tidak sampai ke tujuan dan tidak dapat mengukur performansi jaringan.
4. Nilai dari konsumsi energi pada sistem *shutdown wireless sensor network* menurun eksponensial 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 *route discovery*.

Referensi

[1] D. Georgoulas and K. Blow, "Wireless Sensor Network Management and Functionality: An Overview", Wireless Sensor Network, vol. 01, no. 04, pp. 257-267, 2009.

[2] Cisco, "What Is a Wireless Network? - Wi-Fi Network", 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/wireless-network.html. [Accessed: 21- Jun- 2019].

[3] H. N. Saha, A. Mandal and A. Sinha, "Recent trends in the Internet of Things," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, pp. 1-4, 2017.

[4] J. A. Manrique, J. S. Rueda-Rueda and J. M. T. Portocarrero, "Contrasting Internet of Things and Wireless Sensor Network from a Conceptual Overview," 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, pp. 252-257, 2016.

[5] M. Matin dan M. N. Islam, "Overview of Wireless Sensor Network," 2012.

[6] P. Maidamwar, "A Survey on Security Issues to Detect Wormhole Attack in Wireless Sensor Network", International Journal on AdHoc Networking Systems, vol. 2, no. 4, pp. 37-50, 2012.

[7] P. R. Satav and P. M. Jawandhiya, "Review on single-path multi-path routing protocol in manet: A study," 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, pp. 1-7, 2016.

[8] J. Sen, "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security, pp. 59-82, 2009.

[9] S. Gowrishankar, B. Gangaraju, M. D. H, S.K Sarkar "Issues in Wireless Sensor Networks," Proceeding of the World Congress on Engineering, 2008.

[10] T. Wirahman. Cryptography and Security Schemes for Wireless Sensor Network. Pusat Penelitian Informatika, Lembaga Ilmu Pengetahuan Indonesia 2012.

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

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

[13] A. Suhada, "Sistem Keamanan Gedung Berbasis Wireless Sensor Network dengan Modul NRF24," e-Proceeding of Engineering. Vol. 3 No.2. 2016.

[14] F. D. Nugraheni, I. D. Irawati, Y.S Hariyani "Implementasi Wireless Sensor Network untuk Aplikasi Lampu dan Kipas," e-Proceeding of Engineering. Vol 2 No 3. 2016.

[15] A. A. Laksono, B. Rahmat, J. Holomoan "Rancangan Bangun Prototipe Pemantauan Posisi Kereta Berbasis Wireless Sensor Network," Vol 3. No 3. 2016.

[16] M. B. Aufar, R. Munadi, T Adiprabowo"Analisis Simulasi Routing Protokol Hierarkial Leach dan Pegasis pada Wireless Sensor Network," Vol 4. No 1. 2017.

[17] D. Sharma, S. Verma dan K. Sharma, "Network Topologies in Wireless Sensor Networks: A Review," Vol 4. No. 3. 2013.

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

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

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

[21] S. A. Sasongko, Sukiswo Dan A. A. Zahra, "Analisis Performansi Dan Simulasi Protokol Zrp (Zone Routing Protocol) Pada Manet (Mobile Ad Hoc Network) Dengan Menggunakan Ns-2," 2012.

[22] R. Wulandari, "Analisis Qos (Quality Of Service) Pada Jaringan Internet," Jurnal Teknik Informatika dan Sistem Informasi Vol 2. No 2. 2016.