Karapan Network
Journal

Vol.02, No.01, January 2026
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Analisis Kerentanan Serangan Sinkhole Pada Wireless Sensor Network Dan Strategi Mitigasinya

Ach. Ramadani[1)*], Alvin hidayat putra [2)]

[1) 2)]*Universitas Madura, Pamekasan, Indonesia*

[1)]ach.ramadani77@gmail.com, [2)]alvinhidayatullab@gmail.com

Abstrak

Wireless Sensor Network (WSN) banyak digunakan dalam berbagai aplikasi kritis seperti pemantauan lingkungan, sistem kesehatan, dan industri karena kemampuannya dalam mengumpulkan serta mengirimkan data secara efisien. Namun, keterbatasan sumber daya dan sifat komunikasi nirkabel menjadikan WSN rentan terhadap berbagai serangan keamanan, salah satunya adalah serangan sinkhole. Serangan ini memungkinkan node berbahaya menarik lalu lintas data dari node lain dengan memanipulasi informasi routing, sehingga menyebabkan penurunan kinerja jaringan dan kehilangan data. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan WSN terhadap serangan sinkhole serta mengevaluasi efektivitas strategi mitigasi yang diterapkan. Analisis dilakukan dengan membandingkan kinerja jaringan pada tiga kondisi, yaitu kondisi normal, kondisi jaringan yang mengalami serangan sinkhole, dan kondisi setelah penerapan mekanisme mitigasi. Parameter kinerja yang digunakan meliputi Packet Delivery Ratio (PDR), End-to-End Delay, konsumsi energi, dan stabilitas rute. Hasil pengujian menunjukkan bahwa serangan sinkhole menyebabkan penurunan signifikan pada PDR, peningkatan delay pengiriman data, serta ketidakseimbangan konsumsi energi antar node. Setelah strategi mitigasi diterapkan, kinerja jaringan mengalami perbaikan yang signifikan dan mendekati kondisi normal. Hal ini menunjukkan bahwa mekanisme mitigasi yang diusulkan mampu meningkatkan keamanan dan keandalan Wireless Sensor Network terhadap serangan sinkhole.

***Kata Kunci*:** Wireless Sensor Network, Sinkhole Attack, Keamanan Jaringan, Routing, Mitigasi Serangan.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Perkembangan teknologi jaringan nirkabel dalam dua dekade terakhir telah mendorong lahirnya berbagai sistem cerdas yang mampu bekerja secara mandiri dan terdistribusi[1]. Salah satu teknologi yang memiliki peran penting dalam mendukung sistem tersebut adalah Wireless Sensor Network (WSN)[2]. WSN merupakan kumpulan node sensor berukuran kecil yang memiliki kemampuan untuk melakukan penginderaan, pemrosesan data, dan komunikasi secara nirkabel.[3] Jaringan ini banyak diterapkan pada berbagai bidang strategis, seperti pemantauan lingkungan, pertanian cerdas, sistem kesehatan, militer, hingga smart city[4]. Karakteristik WSN yang fleksibel, hemat biaya, dan mampu menjangkau area luas menjadikannya solusi yang sangat menarik dalam pengumpulan data secara real-time . Namun demikian, di balik keunggulan tersebut, WSN juga memiliki keterbatasan yang signifikan, terutama dari sisi sumber daya[5]. Node sensor umumnya memiliki kapasitas energi, daya komputasi, memori, dan bandwidth yang sangat terbatas[6]. Keterbatasan ini menyebabkan penerapan mekanisme keamanan konvensional yang umum digunakan pada jaringan komputer tradisional menjadi tidak selalu efektif atau bahkan tidak memungkinkan untuk diterapkan secara langsung[7]. Akibatnya, WSN menjadi target yang rentan terhadap berbagai jenis serangan keamanan, baik pada lapisan fisik, data link, jaringan, transport, maupun aplikasi[8].

Salah satu serangan yang dianggap sangat berbahaya pada WSN adalah serangan sinkhole[9]. Serangan ini termasuk dalam kategori serangan pada lapisan jaringan (network layer) yang bertujuan untuk memanipulasi proses routing data[10]. Dalam serangan sinkhole, node berbahaya (malicious node) berusaha menarik lalu lintas data dari node-node lain dengan mengiklankan jalur palsu yang tampak lebih optimal, misalnya dengan mengklaim memiliki jarak terpendek ke base station, latensi paling rendah, atau kualitas jalur terbaik. Ketika node lain mempercayai informasi tersebut, sebagian besar data jaringan akan diarahkan melalui node berbahaya tersebut. Dalam serangan sinkhole, node berbahaya (malicious node) berusaha menarik lalu lintas data dari node-node lain dengan mengiklankan jalur palsu yang tampak lebih optimal, misalnya dengan mengklaim memiliki jarak terpendek ke base station, latensi paling rendah, atau kualitas jalur terbaik. Ketika node lain mempercayai informasi tersebut, sebagian

* Ach. Ramadani

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.X.X.pp-pp

besar data jaringan akan diarahkan melalui node berbahaya tersebut[11]. Dampak dari serangan sinkhole sangat serius terhadap kinerja dan keandalan WSN. Node penyerang dapat melakukan berbagai tindakan merugikan, seperti menjatuhkan paket data (packet dropping), memodifikasi isi data, melakukan analisis lalu lintas untuk memperoleh informasi sensitif, atau menjadi pintu masuk bagi serangan lanjutan seperti selective forwarding, wormhole, dan Denial of Service (DoS)[12]. Dalam konteks aplikasi kritis, seperti pemantauan bencana alam atau sistem militer, keberhasilan serangan sinkhole dapat menyebabkan kegagalan sistem secara keseluruhan dan menimbulkan risiko yang besar[13].

Meskipun berbagai penelitian terkait keamanan WSN telah dilakukan, serangan sinkhole masih menjadi tantangan yang kompleks dan relevan hingga saat ini[14]. Hal ini disebabkan oleh sifat serangan yang sulit dideteksi, karena node penyerang sering kali berperilaku seolah-olah sebagai node normal dan mengikuti protokol routing yang berlaku, namun dengan informasi yang dimanipulasi[15]. Selain itu, beragamnya protokol routing WSN, seperti LEACH, PEGASIS, dan Directed Diffusion, menyebabkan mekanisme mitigasi yang efektif pada satu protokol belum tentu optimal pada protokol lainnya[16]. Berbagai strategi mitigasi serangan sinkhole telah diusulkan dalam literatur, mulai dari pendekatan berbasis kriptografi, sistem deteksi intrusi (Intrusion Detection System), mekanisme trust dan reputasi, hingga teknik berbasis pembelajaran mesin. Setiap pendekatan memiliki kelebihan dan keterbatasan masing-masing[17]. Pendekatan kriptografi, misalnya, mampu meningkatkan keamanan data, namun sering kali membutuhkan konsumsi energi dan komputasi yang tinggi[18]. Sementara itu, metode berbasis deteksi anomali dan kepercayaan dapat lebih ringan dari sisi sumber daya, tetapi berpotensi menghasilkan false positive yang memengaruhi kinerja jaringan[19].Sementara itu, metode berbasis deteksi anomali dan kepercayaan dapat lebih ringan dari sisi sumber daya, tetapi berpotensi menghasilkan false positive yang memengaruhi kinerja jaringan[20].

Oleh karena itu, diperlukan suatu analisis yang komprehensif mengenai karakteristik serangan sinkhole pada WSN, termasuk pola serangan, dampaknya terhadap performa jaringan, serta efektivitas berbagai strategi mitigasi yang telah dikembangkan[21]. Analisis semacam ini penting tidak hanya untuk memahami kelemahan sistem yang ada, tetapi juga sebagai dasar dalam merancang mekanisme keamanan WSN yang lebih adaptif, efisien, dan sesuai dengan keterbatasan sumber daya[22].Oleh karena itu, diperlukan suatu analisis yang komprehensif mengenai karakteristik serangan sinkhole pada WSN, termasuk pola serangan, dampaknya terhadap performa jaringan, serta efektivitas berbagai strategi mitigasi yang telah dikembangkan. Analisis semacam ini penting tidak hanya untuk memahami kelemahan sistem yang ada, tetapi juga sebagai dasar dalam merancang mekanisme keamanan WSN yang lebih adaptif, efisien, dan sesuai dengan keterbatasan sumber daya[23]. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis kerentanan serangan sinkhole pada Wireless Sensor Network serta mengkaji berbagai strategi mitigasi yang telah diusulkan dalam penelitian-penelitian sebelumnya[24]. Fokus analisis diarahkan pada mekanisme kerja serangan sinkhole, dampaknya terhadap kinerja jaringan, serta perbandingan kelebihan dan kekurangan metode mitigasi yang ada. Diharapkan hasil penelitian ini dapat memberikan kontribusi ilmiah dalam pengembangan sistem keamanan WSN yang lebih andal, sekaligus menjadi referensi bagi peneliti dan praktisi dalam merancang jaringan sensor nirkabel yang aman dan berkelanjutan[25].

II. TINJAUAN PUSTAKA

Wireless Sensor Network (WSN) merupakan jaringan yang terdiri dari sejumlah besar node sensor yang saling berkomunikasi secara nirkabel untuk mengumpulkan dan mengirimkan data ke base station atau sink node[26]. Setiap node sensor umumnya memiliki komponen utama berupa unit penginderaan, unit pemrosesan, unit komunikasi, dan sumber energi yang terbatas. Keterbatasan sumber daya ini menjadi karakteristik utama WSN sekaligus faktor yang memengaruhi desain arsitektur jaringan, protokol komunikasi, serta mekanisme keamanan yang diterapkan[27]. Dalam WSN, proses pengiriman data sangat bergantung pada protokol routing yang efisien dan adaptif terhadap kondisi jaringan. Protokol routing pada WSN dirancang untuk meminimalkan konsumsi energi, memperpanjang umur jaringan, serta menjaga keandalan pengiriman data[28]. Namun, fokus utama pada efisiensi energi sering kali menyebabkan aspek keamanan menjadi kurang optimal[29]. Kondisi ini membuka peluang bagi berbagai serangan pada lapisan jaringan, salah satunya adalah serangan sinkhole.

Serangan sinkhole merupakan bentuk serangan aktif di mana node berbahaya berusaha menarik lalu lintas data dari node-node di sekitarnya dengan memalsukan informasi routing[30]. Node penyerang biasanya mengiklankan jalur terbaik menuju base station dengan parameter yang tampak sangat meyakinkan, seperti jarak hop yang lebih pendek atau kualitas sinyal yang lebih baik. Akibatnya, node lain akan memilih rute melalui node tersebut tanpa menyadari bahwa informasi yang diberikan tidak valid[31]. Setelah berhasil menguasai aliran data, penyerang memiliki kendali penuh terhadap paket-paket yang melewatinya[32]. Kerentanan WSN terhadap serangan sinkhole dipengaruhi oleh beberapa faktor, antara lain sifat jaringan yang bersifat self-organizing, penggunaan komunikasi broadcast, serta minimnya mekanisme autentikasi yang kuat pada protokol routing. Selain itu, node sensor yang ditempatkan di

lingkungan terbuka dan tidak terkontrol meningkatkan risiko kompromi fisik terhadap node[33]. Node yang berhasil dikuasai secara fisik dapat dengan mudah dimodifikasi untuk bertindak sebagai node penyerang dalam jaringan[34].

Dampak serangan sinkhole terhadap kinerja WSN sangat signifikan. Serangan ini dapat menyebabkan penurunan tingkat pengiriman paket (packet delivery ratio), peningkatan latensi komunikasi, serta pemborosan energi akibat pengiriman ulang paket yang gagal[35]. Dalam skenario tertentu, serangan sinkhole juga dapat menyebabkan terjadinya kegagalan jaringan secara menyeluruh, terutama apabila node penyerang berada pada posisi strategis di dekat base station[36]. Kondisi ini menjadikan sinkhole sebagai salah satu ancaman paling serius dalam konteks keamanan WSN[37]. Berbagai pendekatan mitigasi serangan sinkhole telah dikembangkan untuk meningkatkan ketahanan WSN[38]. Pendekatan berbasis kriptografi bertujuan untuk menjamin keaslian dan integritas informasi routing melalui mekanisme enkripsi dan autentikasi[39]. Meskipun efektif dalam mencegah manipulasi data, pendekatan ini sering kali membutuhkan sumber daya komputasi dan energi yang besar, sehingga kurang sesuai untuk node sensor dengan keterbatasan daya[40].

Pendekatan lain yang banyak digunakan adalah mekanisme berbasis trust dan reputasi. Dalam metode ini, setiap node akan mengevaluasi perilaku node lain berdasarkan pola komunikasi dan tingkat keandalan pengiriman data. Node yang menunjukkan perilaku mencurigakan akan diberi nilai kepercayaan rendah dan dihindari dalam proses routing[41]. Pendekatan ini relatif ringan dari sisi sumber daya, namun sangat bergantung pada akurasi model penilaian kepercayaan dan rentan terhadap kesalahan deteksi[42]. Selain itu, sistem deteksi intrusi pada WSN juga dikembangkan untuk mengidentifikasi aktivitas abnormal yang mengindikasikan adanya serangan sinkhole[43]. Sistem ini umumnya bekerja dengan memantau pola lalu lintas jaringan, perubahan rute yang tidak wajar, atau anomali dalam parameter jaringan. Tantangan utama dalam pendekatan ini adalah menjaga keseimbangan antara tingkat deteksi yang tinggi dan konsumsi sumber daya yang rendah[44]. Pendekatan berbasis pembelajaran mesin mulai banyak diadopsi untuk meningkatkan akurasi deteksi serangan sinkhole. Teknik ini memungkinkan sistem untuk mengenali pola serangan yang kompleks dan adaptif terhadap perubahan lingkungan jaringan[45]. Namun, penerapan pembelajaran mesin pada WSN masih menghadapi kendala berupa kebutuhan data pelatihan, kompleksitas komputasi, serta keterbatasan implementasi pada node sensor[46].

Berdasarkan kajian pustaka tersebut, dapat disimpulkan bahwa belum terdapat satu pendekatan mitigasi yang sepenuhnya mampu mengatasi serangan sinkhole secara optimal[47]. Setiap metode memiliki kelebihan dan keterbatasan masing-masing, sehingga diperlukan analisis yang lebih mendalam untuk menentukan strategi mitigasi yang sesuai dengan karakteristik dan kebutuhan aplikasi WSN[48].

III. METODE

A. Metode Penelitian

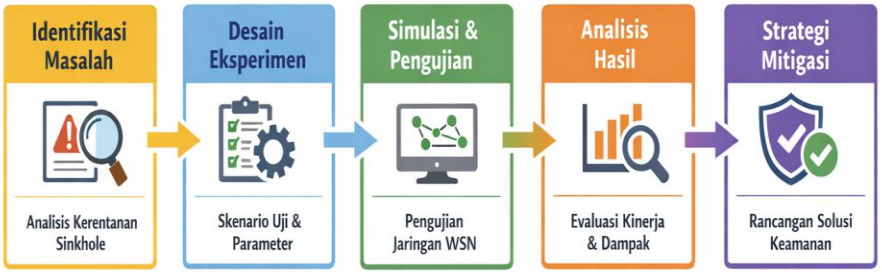
Penelitian ini menggunakan pendekatan analitis dan eksperimental untuk mengkaji kerentanan serangan sinkhole pada Wireless Sensor Network (WSN) serta mengevaluasi efektivitas strategi mitigasinya. Metode penelitian dirancang secara sistematis agar mampu memberikan gambaran menyeluruh mengenai mekanisme serangan, dampak terhadap kinerja jaringan, dan kemampuan sistem mitigasi dalam menekan pengaruh serangan tersebut.

B. Desain Penelitian

Desain penelitian diawali dengan pemodelan arsitektur WSN yang merepresentasikan kondisi jaringan sensor pada umumnya, yaitu terdiri dari sejumlah node sensor, satu base station, serta protokol routing yang digunakan untuk pengiriman data. Pada tahap ini ditentukan skenario jaringan normal dan skenario jaringan yang mengalami serangan sinkhole. Setiap skenario diuji dengan parameter yang sama agar hasil analisis dapat dibandingkan secara objektif.

C. Arsitektur Sistem

Arsitektur sistem WSN yang digunakan dalam penelitian ini menggambarkan hubungan komunikasi antara node sensor dan base station. Beberapa node sensor berperan sebagai node normal, sementara satu atau lebih node dikonfigurasi sebagai node berbahaya yang menjalankan serangan sinkhole[49].



Gambar 1. Alur Umum Penelitian Kerentanan Sibkhole Pada WSN

Pada kondisi normal, setiap node sensor akan mengirimkan data secara multi-hop menuju *base station* melalui jalur terbaik berdasarkan protokol routing. Namun pada skenario serangan, node sinkhole mengiklankan rute palsu sehingga sebagian besar lalu lintas data dialihkan melalui node tersebut.

D. Skenario Serangan Sinkhole

Skenario serangan dirancang dengan memodifikasi perilaku node penyerang agar mengirimkan informasi routing yang tidak sesuai dengan kondisi sebenarnya. Node sinkhole mengklaim memiliki jalur paling optimal menuju base station, sehingga node lain mempercayai dan memilih rute tersebut. Serangan ini dilakukan secara aktif selama simulasi berlangsung untuk mengamati perubahan pola lalu lintas jaringan dan degradasi kinerja WSN.

E. Strategi Mitigasi

Strategi mitigasi yang dianalisis dalam penelitian ini mencakup mekanisme deteksi dan pencegahan berbasis pemantauan perilaku routing. Node sensor melakukan evaluasi terhadap konsistensi informasi rute dan pola pengiriman data. Apabila terdeteksi anomali yang signifikan, node yang dicurigai akan diisolasi dan tidak lagi dilibatkan dalam proses routing.

F. Parameter dan Metode Evaluasi

Evaluasi kinerja jaringan dilakukan dengan membandingkan beberapa parameter utama pada kondisi normal, kondisi terserang sinkhole, dan kondisi setelah mitigasi diterapkan. Parameter yang dianalisis meliputi rasio pengiriman paket, latensi end-to-end, konsumsi energi, dan stabilitas rute.

Parameter Evaluasi Kinerja WSN

Parameter	Deskripsi
Packet Delivery Ratio (PDR)	Persentase paket data yang berhasil diterima oleh tujuan dibandingkan dengan yang dikirimkan.
End-to-End Delay	Waktu rata-rata yang dibutuhkan untuk pengiriman paket data dari sumber ke tujuan.
Konsumsi Energi	Jumlah energi yang digunakan oleh node selama proses pengiriman data.
Stabilitas Rute	Tingkat perubahan rute dan ketidakstabilan jalur akibat serangan.

Gambar 2. Parameter Evaluasi Kinerja WSN

Hasil pengukuran parameter tersebut dianalisis secara komparatif untuk menilai tingkat kerusakan jaringan akibat serangan sinkhole serta sejauh mana strategi mitigasi mampu memperbaiki kinerja jaringan.

G. Tahapan Penelitian

Secara umum, tahapan penelitian meliputi pemodelan jaringan WSN, implementasi skenario serangan sinkhole, penerapan strategi mitigasi, serta analisis hasil pengujian. Setiap tahap dilakukan secara berurutan untuk memastikan validitas dan keterulangan hasil penelitian. Melalui metode penelitian ini, diharapkan diperoleh pemahaman yang komprehensif mengenai karakteristik serangan sinkhole serta efektivitas strategi mitigasi yang dapat diterapkan pada Wireless Sensor Network dengan keterbatasan sumber daya yang ada. Pendekatan ini dipilih karena relatif ringan dari sisi komputasi dan sesuai dengan keterbatasan sumber daya WSN. Selain itu, metode ini memungkinkan adaptasi terhadap perubahan topologi jaringan tanpa memerlukan overhead komunikasi yang besar[50].

IV. HASIL

Bagian ini menyajikan hasil analisis kinerja Wireless Sensor Network (WSN) pada tiga kondisi utama, yaitu kondisi jaringan normal, kondisi jaringan yang mengalami serangan sinkhole, dan kondisi jaringan setelah diterapkan strategi mitigasi. Evaluasi dilakukan berdasarkan parameter kinerja yang telah ditetapkan, meliputi Packet Delivery Ratio, End-to-End Delay, konsumsi energi, dan stabilitas rute. Hasil pengujian digunakan untuk menggambarkan dampak serangan sinkhole terhadap performa jaringan serta efektivitas mekanisme mitigasi yang diterapkan. Pada kondisi jaringan normal, WSN menunjukkan performa yang stabil dan optimal. Nilai Packet Delivery Ratio berada pada tingkat tinggi, yang menandakan bahwa sebagian besar paket data yang dikirim oleh node sensor berhasil diterima oleh base station. Jalur routing terbentuk secara efisien dengan perubahan rute yang minimal, sehingga komunikasi data berlangsung secara konsisten. Selain itu, End-to-End Delay relatif rendah karena pemilihan rute didasarkan pada jalur yang paling optimal sesuai dengan protokol routing yang digunakan. Konsumsi energi pada kondisi ini juga cenderung merata di antara node sensor, yang menunjukkan distribusi beban komunikasi yang seimbang.

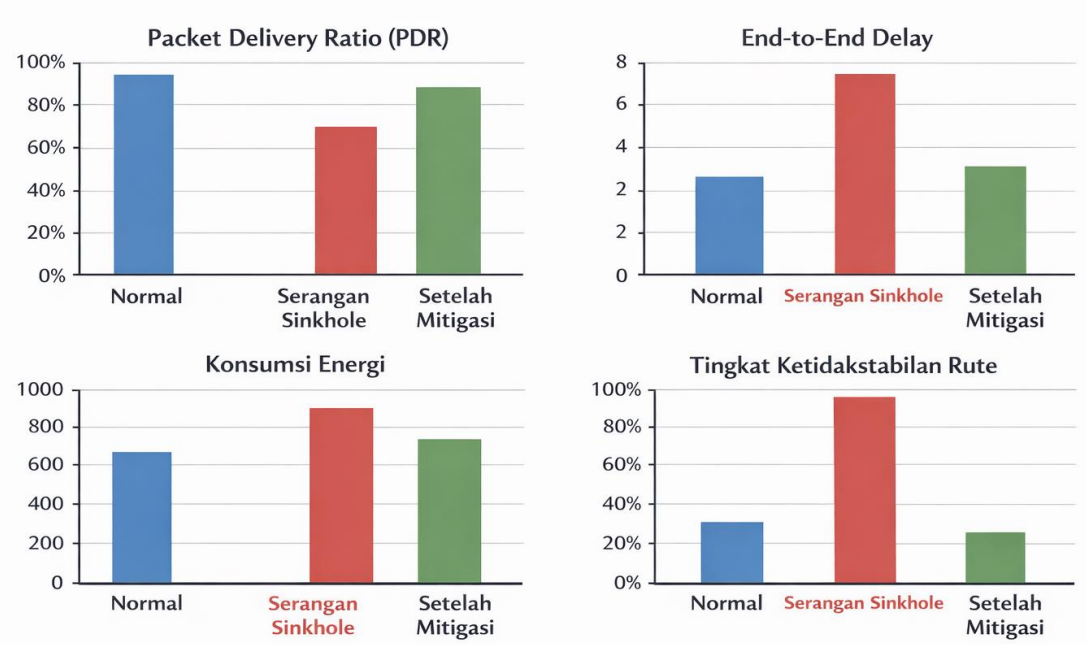
Ketika serangan sinkhole mulai diterapkan, terjadi perubahan yang signifikan pada kinerja jaringan. Node penyerang berhasil menarik sebagian besar lalu lintas data dengan mengiklankan jalur routing palsu yang tampak lebih baik dibandingkan jalur sebenarnya. Akibatnya, Packet Delivery Ratio mengalami penurunan yang cukup tajam. Sebagian paket data tidak berhasil mencapai base station karena dijatuhkan atau dimanipulasi oleh node sinkhole. Kondisi ini menunjukkan bahwa serangan sinkhole secara langsung memengaruhi keandalan pengiriman data dalam WSN. Selain penurunan rasio pengiriman paket, End-to-End Delay juga mengalami peningkatan pada saat jaringan berada dalam kondisi terserang. Paket data membutuhkan waktu yang lebih lama untuk sampai ke base station karena terjadinya penumpukan lalu lintas pada node sinkhole serta kemungkinan terjadinya pengiriman ulang paket. Peningkatan latensi ini berdampak negatif pada aplikasi WSN yang bersifat real-time dan membutuhkan respons cepat.

Gambar 3.Grafik Hasil Wsn

Dari sisi konsumsi energi, hasil pengujian menunjukkan adanya ketidakseimbangan penggunaan energi antar node. Node yang berada di sekitar node sinkhole mengalami konsumsi energi yang lebih tinggi akibat meningkatnya aktivitas komunikasi. Sementara itu, node sinkhole sendiri cenderung mengalami konsumsi energi yang tidak wajar, yang dapat dijadikan indikasi awal adanya aktivitas mencurigakan dalam jaringan. Ketidakseimbangan ini berpotensi mempercepat kegagalan node tertentu dan mengurangi umur jaringan secara keseluruhan. Setelah strategi mitigasi diterapkan, kinerja WSN menunjukkan perbaikan yang signifikan dibandingkan kondisi terserang. Mekanisme deteksi berbasis pemantauan perilaku routing mampu mengidentifikasi node yang menunjukkan anomali dalam penyampaian informasi rute. Node yang terdeteksi mencurigakan kemudian diisolasi dari proses routing, sehingga lalu lintas data tidak lagi terpusat pada node sinkhole. Hal ini berdampak langsung pada peningkatan Packet Delivery Ratio, yang mendekati nilai pada kondisi jaringan normal.

Penerapan mitigasi juga berhasil menurunkan nilai End-to-End Delay. Jalur routing kembali terbentuk secara lebih seimbang, sehingga waktu tempuh paket data menjadi lebih stabil. Meskipun demikian, pada beberapa skenario masih ditemukan sedikit peningkatan latensi dibandingkan kondisi normal, yang disebabkan oleh proses evaluasi dan penyesuaian rute selama tahap mitigasi berlangsung. Dari aspek konsumsi energi, strategi mitigasi mampu mendistribusikan kembali beban komunikasi secara lebih merata antar node. Konsumsi energi ekstrem pada node tertentu dapat ditekan, sehingga umur jaringan menjadi lebih panjang. Stabilitas rute juga mengalami peningkatan,

ditandai dengan berkurangnya perubahan jalur routing yang tidak perlu selama simulasi. Secara keseluruhan, hasil penelitian menunjukkan bahwa serangan sinkhole memberikan dampak yang signifikan terhadap kinerja Wireless Sensor Network, terutama pada keandalan pengiriman data, latensi komunikasi, dan efisiensi energi. Namun, penerapan strategi mitigasi yang tepat terbukti mampu mengurangi dampak tersebut dan meningkatkan kembali performa jaringan. Hasil ini menegaskan pentingnya integrasi mekanisme keamanan yang ringan dan adaptif dalam perancangan WSN untuk menghadapi ancaman serangan sinkhole.



Gambar 4. Grafik Evaluasi Kinerja WSN

V. PEMBAHASAN

Hasil penelitian menunjukkan bahwa serangan sinkhole memberikan dampak yang signifikan terhadap kinerja Wireless Sensor Network, terutama pada aspek keandalan pengiriman data, latensi komunikasi, serta efisiensi penggunaan energi. Pada kondisi jaringan normal, protokol routing mampu membangun jalur komunikasi yang relatif stabil dan efisien. Namun, ketika node sinkhole mulai beroperasi dengan mengiklankan informasi rute palsu, mekanisme routing menjadi rentan terhadap manipulasi, sehingga lalu lintas data terpusat pada node penyerang. Kondisi ini mengakibatkan penurunan Packet Delivery Ratio secara drastis, yang mengindikasikan berkurangnya kemampuan jaringan dalam mengirimkan data sensor secara andal ke base station. Peningkatan End-to-End Delay pada saat serangan sinkhole juga menjadi temuan penting dalam penelitian ini. Penumpukan paket data pada node sinkhole serta proses pengiriman ulang paket menyebabkan latensi komunikasi menjadi lebih tinggi. Hal ini sangat berpengaruh terhadap aplikasi WSN yang membutuhkan respon waktu nyata, seperti pemantauan lingkungan dan sistem peringatan dini. Selain itu, peningkatan latensi juga mencerminkan ketidakefisienan jalur routing yang terbentuk akibat manipulasi informasi rute oleh node penyerang.

Dari sisi konsumsi energi, serangan sinkhole menyebabkan terjadinya ketidakseimbangan distribusi energi antar node. Node yang berada di sekitar jalur sinkhole mengalami peningkatan aktivitas komunikasi yang berlebihan, sehingga energi yang dikonsumsi menjadi lebih tinggi dibandingkan node lainnya. Ketidakseimbangan ini berpotensi mempercepat kegagalan node tertentu dan memperpendek umur jaringan secara keseluruhan. Temuan ini menegaskan bahwa serangan sinkhole tidak hanya berdampak pada aspek keamanan data, tetapi juga pada keberlanjutan operasional jaringan. Penerapan strategi mitigasi yang diusulkan dalam penelitian ini terbukti mampu mengurangi dampak serangan sinkhole secara signifikan. Mekanisme deteksi berbasis pemantauan perilaku routing memungkinkan sistem mengidentifikasi node yang menunjukkan pola komunikasi tidak normal. Isolasi node mencurigakan dari proses routing membantu mendistribusikan kembali lalu lintas data secara lebih merata. Dampaknya terlihat pada peningkatan Packet Delivery Ratio, penurunan End-to-End Delay, serta perbaikan distribusi

konsumsi energi. Meskipun masih terdapat sedikit overhead akibat proses deteksi dan evaluasi rute, overhead tersebut relatif kecil dibandingkan peningkatan kinerja dan keamanan jaringan yang diperoleh.

Berdasarkan hasil pembahasan, dapat dirangkum beberapa poin utama sebagai berikut:

1. Serangan sinkhole terbukti secara signifikan menurunkan kinerja WSN, terutama pada keandalan pengiriman data, latensi komunikasi, dan efisiensi energi.
2. Parameter Packet Delivery Ratio, End-to-End Delay, dan konsumsi energi efektif digunakan sebagai indikator untuk mendeteksi dan menganalisis dampak serangan sinkhole.
3. Strategi mitigasi yang diterapkan mampu meningkatkan kembali kinerja jaringan dan menjaga stabilitas routing, sehingga layak dipertimbangkan sebagai solusi keamanan pada lingkungan WSN yang rentan terhadap serangan sinkhole.

VI. KESIMPULAN

Penelitian ini membahas analisis kerentanan serangan sinkhole pada Wireless Sensor Network serta mengevaluasi efektivitas strategi mitigasi yang diterapkan. Hasil penelitian menunjukkan bahwa serangan sinkhole memiliki dampak yang signifikan terhadap kinerja jaringan, khususnya pada aspek Packet Delivery Ratio, End-to-End Delay, konsumsi energi, dan stabilitas rute. Pada kondisi terserang, jaringan mengalami penurunan keandalan pengiriman data, peningkatan latensi komunikasi, serta ketidakseimbangan distribusi energi antar node, yang berpotensi mempercepat penurunan umur jaringan. Penerapan strategi mitigasi berbasis pemantauan perilaku routing terbukti mampu mengurangi dampak negatif serangan sinkhole. Mekanisme ini memungkinkan identifikasi dan isolasi node yang berperilaku mencurigakan, sehingga lalu lintas data dapat dialihkan kembali ke jalur yang lebih aman dan efisien. Hasil evaluasi menunjukkan adanya peningkatan Packet Delivery Ratio, penurunan End-to-End Delay, serta perbaikan distribusi konsumsi energi setelah mitigasi diterapkan. Selain itu, stabilitas rute jaringan juga mengalami peningkatan, yang mencerminkan kemampuan sistem dalam menjaga konsistensi jalur komunikasi.

Secara keseluruhan, penelitian ini menegaskan pentingnya integrasi mekanisme keamanan yang ringan dan adaptif dalam perancangan Wireless Sensor Network. Strategi mitigasi yang diusulkan dapat dijadikan dasar pengembangan sistem keamanan WSN yang lebih andal untuk menghadapi ancaman serangan sinkhole di berbagai skenario aplikasi.

Kontribusi Penulis: Ach. Ramadani: Konseptualisasi, Metodologi, Penulisan-Draf Awal, Penulisan-Tinjauan & Penyuntingan, Supervisi. Ach. Ramadani merancang konsep dan metodologi penelitian, memimpin proses penulisan, serta melakukan penyuntingan dan validasi akhir naskah. **Moh. Alvin hidayat putra:** Perangkat Lunak, Investigasi, Kurasi Data, Penulisan-Draf Awal. Moh. Alvin Hidayat putra bertanggung jawab pada pengembangan perangkat lunak analisis berbasis *IndoBERT* dan *RoBERTa IndoSent*, pengumpulan data ulasan dari Instagram, serta penyusunan draf awal hasil penelitian.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.
Ketersediaan Data: -
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.
Penulis Pertama: https: -
Penulis Kedua: https: -
Penulis Ketiga: -

REFERENSI

[1] F. Prasetyo, E. Putra, F. Muslim, N. Hasanah, R. Paradina, and R. Alim, “Jurnal Sistim Informasi dan Teknologi Analisis Komparasi Protokol Websocket dan MQTT Dalam Proses Push Notification,” vol. 5, pp. 63–72, 2024, doi: 10.60083/jsisfotek.v5i4.325.

[2] F. P. E. Putra, D. T. Agustina, T. S. K. Khotimah, and T. Ramadhanty, “Analisis Kinerja Jaringan 5G dalam Meningkatkan Konektivi-tas Internet of Things (IoT),” 2025, *researchgate.net*. doi: 10.55606/jitek.v5i1.5836.

[3] F. P. E. Putra, D. E. Arissandi, A. Rofiqi, and M. F. Hidayat, “Pemanfaatan Mikrotik Dalam Manajemen Bandwidth Pada Jaringan Sekolah,” 2025, *researchgate.net*. doi: 10.31294/evolusi.v7i2.5843.

[4] B. Minh Nguyen *et al.*, “Dholes Hunting-A Multi-Local Search Algorithm Using Gradient Approximation

and Its Application for Blockchain Consensus Problem," *IEEE Access*, vol. 12, pp. 93333–93349, 2024, doi: 10.1109/ACCESS.2024.3419172.

[5] F. P. E. Putra, M. A. Mahmud, and I. S. Maqom, "Pengembangan Sistem Pemantauan Lingkungan Berbasis Internet of Things (IoT) di Kampus," 2023, *researchgate.net*. doi: 10.47709/digitech.v3i2.3457.

[6] H. Lanya, M. Zayyadi, D. R. Anjarani, F. P. E. Putra, and ..., "PEMBERDAYAAN SEKOLAH INKLUSI MELALUI E-MODUL BERJENJANG SEBAGAI PENGEMBANGAN KOMPETENSI GURU DALAM PEMENUHAN …." doi: 10.37303/peduli.v8i2.681.

[7] A. K. V. K. Vamsi Krishna Reddy and K. V. L. Komanapalli, "Investigation of a Multi-Strategy Ensemble Social Group Optimization Algorithm for the Optimization of Energy Management in Electric Vehicles," *IEEE Access*, vol. 10, pp. 12084–12124, 2022, doi: 10.1109/ACCESS.2022.3144065.

[8] F. P. E. Putra, U. Ubaidi, M. A. Huda, and ..., "Computer network management optimization through big data analysis using time series analysis method," *Brill. Res. …*, 2024, doi: 10.47709/brilliance.v4i1.4373.

[9] M. S. Ali, M. S. Islam, M. Asif, W. U. Khan, F. Lin, and O. Waqar, "On Efficient DCT Type-I Based Low Complexity Channel Estimation for Uplink NB-IoT Systems," *IEEE Access*, vol. 9, pp. 129756–129770, 2021, doi: 10.1109/ACCESS.2021.3112279.

[10] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *... Educ. ...*, 2023, doi: 10.51211/itbi.v8i1.2441.

[11] F. Prasetyo, E. Putra, F. Iqbal, and N. Muhammad, "Twitter sentiment analysis about economic recession in indonesia," vol. 7, no. 1, pp. 1–7, 2023, doi: 10.31763/businta.v7i1.592.

[12] J. Wu, Y. Sun, J. Qian, Y. Cui, Q. Wang, and L. Zhuo, "Distributed Resilient Clustering Algorithm for Virtual Power Plants Under Cyber Attacks," *IEEE Access*, vol. 13, pp. 38714–38725, 2025, doi: 10.1109/ACCESS.2025.3546103.

[13] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and ..., "Analisis kecepatan dan kinerja jaringan 5G (generasi ke 5) pada wilayah perkotaan," *... J. Informatics*, 2023, doi: 10.51211/itbi.v8i1.2439.

[14] D. S. Kumar and R. Thenmozhi, "AI-Driven TrafNet-DCMCRP for Congestion-Aware Routing and Traffic Management in VANETs," *Int. J. Intell. Eng. Syst.*, vol. 18, no. 5, pp. 239–251, 2025, doi: 10.22266/ijies2025.0630.18.

[15] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, and ..., "Tinjauan performa RouterOS Mikrotik dalam jaringan internet: Analisis kinerja dan kelayakan," *Digit. …*, 2023, doi: 10.47709/digitech.v3i2.3446.

[16] S. Khera, N. Turk, and N. Kaur, "HC-WSN: a Hibernated Clustering based framework for improving energy efficiency of wireless sensor networks," *Multimed. Tools Appl.*, vol. 82, no. 3, pp. 3879–3894, 2023, doi: 10.1007/s11042-022-13446-2.

[17] R. Roy and S. K. Dwivedy, "Nonlinear dynamics of magnetically coupled double beam based piezoelectric energy harvester under galloping excitation," *Sensors Actuators A Phys.*, vol. 371, 2024, doi: 10.1016/j.sna.2024.115288.

[18] I. Jo, B. Kim, H. Won, S. Kim, K. Choi, and D. Choi, "Evaluation of MWCNT/PU sponge-based triboelectric nanogenerator for harvesting mechanical energy," *Funct. Compos. Struct.*, vol. 7, no. 3, 2025, doi: 10.1088/2631-6331/adf60b.

[19] Y. Zi, C. Zhou, J. Chen, Z. Han, Y. Huang, and X. Wu, "Hyperspectral Methane Plume Segmentation Through Foundation Computer Vision Models," *IEEE Access*, vol. 13, pp. 143031–143041, 2025, doi: 10.1109/ACCESS.2025.3597991.

[20] M. G. Busto, M. J. José Prieto, J. A. Martín-Ramos, J. A. Martínez Esteban, and A. M. Pernía, "Current Source Strategy for Energy Injection from a CapMix Cell," *Electron.*, vol. 13, no. 1, 2024, doi: 10.3390/electronics13010042.

[21] G. Savithri and N. R. Sai, "A Reliable Hybrid Framework for Anomaly Detection in Secure and Robust Wireless Sensor Networks," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 4, pp. 25789–25797, 2025, doi: 10.48084/etasr.11494.

[22] M. Soleymani, I. Santamaría, and P. J. Schreier, "Distributed Algorithms for Spectral and Energy-Efficiency Maximization of K-User Interference Channels," *IEEE Access*, vol. 9, pp. 96948–96963, 2021, doi: 10.1109/ACCESS.2021.3094976.

[23] S. Oak, D. Lee, G. Sim, S. Kim, and G. Park, "Real-Time Personalized Car-Following Control With Online Parameter Adaptation for Intelligent Regenerative Braking Systems," *IEEE Access*, vol. 13, pp. 168055–168066, 2025, doi: 10.1109/ACCESS.2025.3611825.

[24] M. Zheng, Y. Zhao, and W. Liang, "CHR: A Novel Channel-Hopping-Based Retransmission Scheme in WIA-FA Networks," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 7107–7115, 2024, doi: 10.1109/JIOT.2023.3314438.

[25] D. Lee, S. Lee, S. Oh, and D. Park, "Energy-Efficient FPGA Accelerator with Fidelity-Controllable Sliding-Region Signal Processing Unit for Abnormal ECG Diagnosis on IoT Edge Devices," *IEEE Access*, vol. 9, pp. 122789–122800, 2021, doi: 10.1109/ACCESS.2021.3109875.

[26] L. Chen, L. Sun, and C. Zhong, "Interpretability-Oriented Adjustment of K-Means: A Multiple-Objective Particle Swarm Optimization Framework," *IEEE Access*, vol. 13, pp. 68084–68096, 2025, doi: 10.1109/ACCESS.2025.3558716.

[27] H. Alsmadi, E. Saleh, M. Alsmadi, and S. Ikki, "Hardware Impairments Effects on Over the Air System Assisted by Unmanned Aerial Vehicle," *IEEE Commun. Lett.*, vol. 28, no. 7, pp. 1609–1613, 2024, doi: 10.1109/LCOMM.2024.3395439.

[28] D. Pandey and V. Kushwaha, "An Exploratory Study of Optimization Techniques for Congestion Control in Wireless Sensor Networks," *Ad-Hoc Sens. Wirel. Networks*, vol. 58, no. 1–2, pp. 79–125, 2024, doi: 10.32908/ahswn.v58.10241.

[29] L. Zhu, "Research on Multi-Objective Coordinated Planning of Distribution Networks Based on Improved Generative Adversarial Networks," *IEEE Access*, vol. 13, pp. 134129–134142, 2025, doi: 10.1109/ACCESS.2025.3592675.

[30] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, "Unweighted Voting Method to Detect Sinkhole Attack in RPL-Based Internet of Things Networks," *Comput. Mater. Contin.*, vol. 77, no. 1, pp. 491–515, 2023, doi: 10.32604/cmc.2023.041108.

[31] H. Tang, P. Wang, D. Li, Y. Zhang, and X. Chen, "An Adaptive Virtual Tunnel Routing Protocol With Eliminating Boundary Effects for Flying Ad-Hoc Networks," *IEEE Internet Things J.*, vol. 12, no. 16, pp. 34068–34085, 2025, doi: 10.1109/JIOT.2025.3577510.

[32] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, "Attack Detection for Medical Cyber-Physical Systems-A Systematic Literature Review," *IEEE Access*, vol. 11, pp. 41796–41815, 2023, doi: 10.1109/ACCESS.2023.3270225.

[33] M. Kinnas, J. Violos, N. I. Karapiperis, and I. Kompatsiaris, "Selecting Images With Entropy for Frugal Knowledge Distillation," *IEEE Access*, vol. 13, pp. 28189–28203, 2025, doi: 10.1109/ACCESS.2025.3540384.

[34] T. Wang, J. Geng, J. Wang, and X. Yan, "Video Refereeing Model of Soccer Match Based on Fuzzy Clustering and Cuckoo Optimization Algorithm," *IEEE Access*, vol. 12, pp. 82536–82548, 2024, doi: 10.1109/ACCESS.2024.3401705.

[35] F. Tosoni, P. Bille, V. Brunacci, A. d. De Angelis, P. Ferragina, and G. Manzini, "Toward Greener Matrix Operations by Lossless Compressed Formats," *IEEE Access*, vol. 13, pp. 56756–56779, 2025, doi: 10.1109/ACCESS.2025.3555119.

[36] L. Prashad, H. C. Mohanta, and A. J. A. Abdullah Al-Gburi, "Dual Band Rectenna for Electromagnetic Energy Harvesting at 2.4 GHz and 5 GHz Frequencies," *Prog. Electromagn. Res. B*, vol. 108, pp. 75–88, 2024, doi: 10.2528/PIERB24072102.

[37] D. Lin, Z. Chen, X. Liu, L. Kong, and Y. L. Guan, "ESWCM: A Novel Energy-sustainable Approach for SWIPT-enabled WSN with Constrained MEAP Configurations," *IEEE Trans. Mob. Comput.*, vol. 23, no. 9, pp. 9012–9028, 2024, doi: 10.1109/TMC.2024.3357771.

[38] M. Niranjan, S. Gupta, and B. Singh, "Sensor node localization with improved hop-size using PSODESA optimization," *Wirel. Networks*, vol. 29, no. 4, pp. 1911–1934, 2023, doi: 10.1007/s11276-023-03242-7.

[39] G. Zhao, K. Lin, and T. Hao, "A feasibility study of LoRaWAN-based wireless underground sensor networks for underground monitoring," *Comput. Networks*, vol. 232, 2023, doi: 10.1016/j.comnet.2023.109851.

[40] O. K. Om Kumar, S. Gajendran, and S. Marappan, "Enhancing Intrusion Detection Through Federated Learning With Enhanced Ghost_BiNet and Homomorphic Encryption," *IEEE Access*, vol. 12, pp. 24879–24893, 2024, doi: 10.1109/ACCESS.2024.3362347.

[41] H. K. Khalid Alkahtani, H. Mahgoub, F. A. Alotaibi, K. M. Othman, R. Allafi, and A. S. Salama, "Design of Hybrid Snake Optimizer Based Route Selection Approach for Unmanned Aerial Vehicles Communication," *IEEE Access*, vol. 12, pp. 54426–54434, 2024, doi: 10.1109/ACCESS.2024.3383031.

[42] H. Guo *et al.*, "Assessment of energy harvesting and signal transmission in traffic markings with embedded piezoelectric film transducers," *J. Intell. Mater. Syst. Struct.*, vol. 36, no. 7, pp. 443–454, 2025, doi: 10.1177/1045389X251326335.

[43] M. H. Hashemi, U. Kiliç, and S. Dikmen, "Applications of Novel Heuristic Algorithms in Design Optimization of Energy-Efficient Distribution Transformer," *IEEE Access*, vol. 11, pp. 15968–15980, 2023, doi: 10.1109/ACCESS.2023.3245327.

[44] R. Wielgat *et al.*, "A Concept of Smart Agro-Photovoltaic Tunnels," *IEEE Access*, vol. 12, pp. 40765–40794,

2024, doi: 10.1109/ACCESS.2024.3376411.

[45] A. Ometov, K. Zeman, P. Masek, L. Balazevic, and M. Komarov, "A Comprehensive and Reproducible Comparison of Cryptographic Primitives Execution on Android Devices," *IEEE Access*, vol. 9, pp. 54625–54638, 2021, doi: 10.1109/ACCESS.2021.3069627.

[46] J. B. Barreiro, S. Z. Fernández, and V. D. Diaz-Casas, "Internet of Things in Energy-Sensitive Processes: Application in a Refrigerated Warehouse," *IEEE Access*, vol. 12, pp. 76257–76276, 2024, doi: 10.1109/ACCESS.2024.3406992.

[47] C. Ma *et al.*, "Banana Individual Segmentation and Phenotypic Parameter Measurements Using Deep Learning and Terrestrial LiDAR," *IEEE Access*, vol. 12, pp. 50310–50320, 2024, doi: 10.1109/ACCESS.2024.3385280.

[48] Y. Gao, H. Zhu, X. Li, and M. J. V Amuri, "Trust-Based Distributed H∞ Diffusion Filtering for Target Tracking under Cyber Attacks," *IEEE Access*, vol. 11, pp. 119388–119395, 2023, doi: 10.1109/ACCESS.2023.3326874.

[49] R. Santos, D. Castanheira, A. Silva, and A. Gameiro, "Pipelined Multi-User IR-HARQ Scheme for Improved Latency Performance in URLLC," *IEEE Access*, vol. 12, pp. 33473–33485, 2024, doi: 10.1109/ACCESS.2024.3371994.

[50] S. Baek, G.-H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian, and J.-P. Hong, "A Reconfigurable SRAM Based CMOS PUF with Challenge to Response Pairs," *IEEE Access*, vol. 9, pp. 79947–79960, 2021, doi: 10.1109/ACCESS.2021.3084621.