

Simulasi Integrasi Leach dan Enkripsi untuk Efisiensi Jaringan Sensor Nirkabel

Gede Dimas Putra Pratama^{a1}, I Gede Arta Wibawa^{a2},

^aProgram Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus Udayana, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
¹pratama.2308561007@student.unud.ac.id
²Gede.arta@unud.ac.id

Abstract

The development of Wireless Sensor Network (WSN) has a significant impact on various fields such as smart agriculture, environmental monitoring, and IoT-based security systems. The main drawbacks of WSN are the limited energy, computing capacity, and transmission power of sensor nodes. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol is widely used for energy management by forming clusters and reducing long-distance transmission. However, LEACH does not yet have a built-in security mechanism, making it vulnerable to threats such as eavesdropping and data manipulation. This study proposes the integration of the lightweight encryption algorithm XOR Cipher into the LEACH protocol to improve data security without reducing energy efficiency. Software-based simulations using Python were conducted to compare the performance of standard LEACH and encrypted LEACH. The parameters tested include energy consumption, packet delivery ratio (PDR), delay, and packet loss. The results show that the integration of XOR Cipher adds very little overhead, with slightly increased energy consumption and delay, but the PDR remains above 90%. This proves that XOR Cipher is a lightweight encryption solution that is feasible to be applied to WSN.

Keywords: *Wireless Sensor Network, LEACH, XOR Cipher, Lightweight Encryption, Energy Efficiency*

1. Pendahuluan

Perkembangan teknologi *Wireless Sensor Network* (WSN) telah memberikan dampak signifikan dalam berbagai sektor seperti *smart agriculture*, *monitoring* lingkungan, dan sistem keamanan berbasis *Internet of Things* (IoT). WSN terdiri atas sekumpulan *node sensor* yang tersebar secara acak dan saling berkomunikasi secara nirkabel untuk mengumpulkan, memproses, dan mengirimkan data menuju *base station*. Namun, keterbatasan sumber daya energi, kapasitas komputasi, dan daya transmisi *node sensor* menjadi tantangan utama dalam pengelolaan jaringan ini [3]. Oleh karena itu, dibutuhkan mekanisme manajemen energi yang efisien untuk memperpanjang umur jaringan tanpa mengurangi kualitas layanan.

Salah satu protokol yang banyak digunakan dalam pengelolaan energi WSN adalah *Low-Energy Adaptive Clustering Hierarchy* (LEACH). Protokol ini membentuk *cluster* dan memilih *Cluster Head* (CH) secara periodik berdasarkan probabilitas tertentu, sehingga data dari *node sensor* dikumpulkan terlebih dahulu oleh CH sebelum diteruskan ke *base station*. Mekanisme ini secara signifikan dapat mengurangi konsumsi energi akibat transmisi jarak jauh [3][2]. Meskipun efektif dalam efisiensi energi, LEACH belum memiliki mekanisme keamanan bawaan, sehingga rentan terhadap ancaman seperti penyadapan (*eavesdropping*), modifikasi data, dan serangan *replay* selama proses transmisi data di lingkungan terbuka. Penelitian juga menunjukkan kinerja LEACH jika parameter seperti jumlah *cluster* tidak dioptimalkan [4].

Untuk mengatasi permasalahan tersebut, integrasi algoritma enkripsi data ke dalam WSN menjadi solusi strategis guna meningkatkan keamanan komunikasi data tanpa mengorbankan efisiensi energi secara signifikan [1]. Salah satu pendekatan yang kini berkembang adalah

penerapan algoritma enkripsi ringan (*lightweight encryption*) yang dirancang agar kompatibel dengan perangkat berkinerja rendah seperti *node sensor*. Pada penelitian ini, algoritma XOR *cipher* digunakan sebagai metode enkripsi karena memiliki proses komputasi yang sederhana, ringan, dan cepat, sehingga sesuai diterapkan pada lingkungan WSN yang memiliki keterbatasan sumber daya [5]. Meskipun tergolong algoritma dasar, XOR *cipher* tetap efektif dalam menyamarkan data dan mencegah penyadapan secara langsung pada komunikasi antar *node*. Integrasi metode ini diharapkan mampu menjaga kerahasiaan dan integrasi data sekaligus mempertahankan performa jaringan dari sisi konsumsi energi dan keterlambatan pengiriman data.

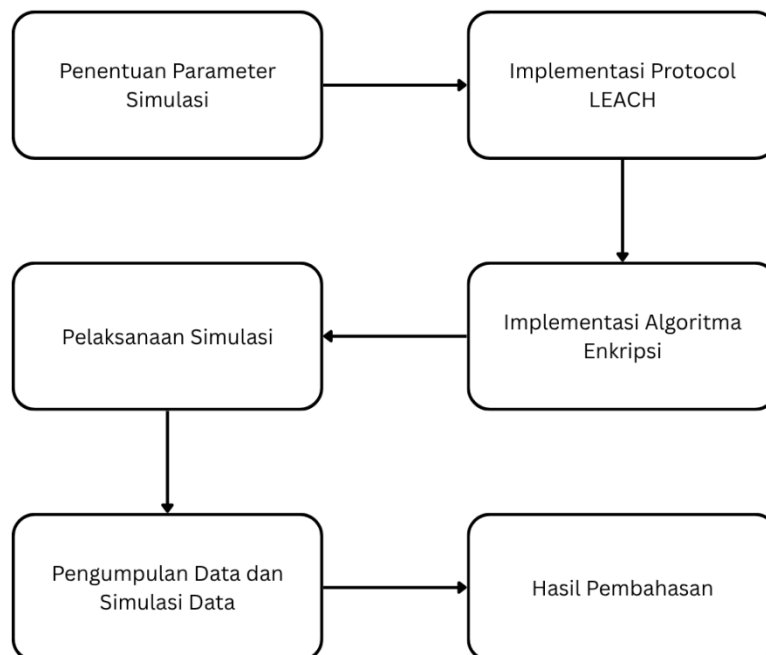
Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan simulasi integrasi protokol *LEACH* dengan enkripsi data ringan dalam jaringan sensor nirkabel berbasis *software-only*. Penelitian ini akan menganalisis dampaknya terhadap parameter performa utama seperti *energy consumption*, *packet delivery ratio* (PDR), *delay*, dan *packet loss*. Hasil simulasi diharapkan dapat memberikan gambaran tentang efektivitas integrasi protokol *LEACH* dan enkripsi data ringan dalam meningkatkan efisiensi serta keamanan komunikasi data pada jaringan sensor nirkabel.

2. Metode Penelitian

2.1 Desain Penelitian

Penelitian ini merupakan studi eksperimental berbasis simulasi *software* yang bertujuan untuk menganalisis performa jaringan sensor nirkabel menggunakan protokol *LEACH*, baik dalam kondisi standar maupun setelah integrasi dengan algoritma enkripsi ringan menggunakan XOR. Pengujian dilakukan melalui simulasi *software-only* tanpa perangkat keras fisik, dengan membandingkan tiga skenario :

- a. *Direct Routing*
- b. *LEACH* tanpa enkripsi
- c. *LEACH* dengan dengan enkripsi ringan berbasis XOR



Gambar 1. Alur Simulasi Protokol *LEACH*

2.2 Alat dan Bahan

Simulasi dalam penelitian ini dilakukan menggunakan bahasa pemrograman *Python* versi 3.12.7 karena versi ini memiliki fleksibilitas tinggi dalam pengolahan data serta dukungan berbagai *library* yang dapat digunakan untuk simulasi jaringan. *Library NetworkX* versi 3.5 digunakan karena memiliki performa yang baik dan kemudahan dalam penggunaannya, serta fitur visualisasi *graf* dan pengelolaan topologi jaringan yang lebih stabil dibandingkan versi sebelumnya. Kelebihan inilah yang menjadikan *NetworkX* versi ini sesuai untuk kebutuhan simulasi WSN yang memerlukan visualisasi cepat, *layout* konsisten, dan analisis *graf* yang kompleks. *Library* ini nantinya digunakan untuk membentuk topologi jaringan sensor serta mengatur proses pembentukan *cluster* dan pemilihan *Cluster Head* (CH) dalam protokol *LEACH*. Kemudian untuk visualisasi hasil simulasi, digunakan *library Matplotlib* versi 3.10.3 yang memiliki performa *rendering* grafik yang baik, visualisasi yang lebih canggih, dan dukungan antarmuka yang lebih ramah. *Library* ini digunakan untuk memvisualisasikan hasil simulasi dalam bentuk grafik, seperti grafik konsumsi energi, *Packet Delivery Ratio* (PDR), dan *delay*.

Proses enkripsi data dilakukan menggunakan algoritma XOR *Cipher* yang disimulasikan pada *layer* aplikasi. Algoritma ini dipilih karena sifatnya yang ringan, cepat dan sederhana, sehingga sesuai diterapkan untuk lingkungan WSN yang memiliki keterbatasan energi dan kapasitas komputasi. Dan seluruh simulasi dijalankan dalam *software Visual Studio Code* versi 1.101.2 sebagai *Integrated Development Environment* (IDE), karena kemudahan integrasi dengan *Python* dan antarmuka pengguna yang ringan serta fleksibel untuk pengembangan program simulasi jaringan.

Tabel 1. Spesifikasi Alat Simulasi

No	Alat/Perangkat Lunak	Keterangan
1	<i>Python</i> 3.12.7	Bahasa pemrograman utama simulasi.
2	<i>NetworkX</i> 3.5	Pembentukan dan manipulasi topologi jaringan.
3	<i>Matplotlib</i> 3.10.3	Visualisasi grafik hasil simulasi.
4	<i>Visual Studio Code</i>	<i>Software</i> untuk melakukan simulasi.
5	XOR <i>Cipher</i>	Simulasi enkripsi ringan pada layer aplikasi.

2.3 Prosedur Simulasi

Tahapan simulasi dilakukan melalui beberapa langkah berikut:

- a. Penentuan Parameter Simulasi
Menentukan parameter-parameter awal simulasi, seperti jumlah *node*, ukuran area jaringan, energi awal *node*, jumlah *cluster*, dan jumlah ronde simulasi. Nilai parameter disesuaikan dengan acuan literatur.
- b. Implementasi Protokol *LEACH*
Implementasi dilakukan menggunakan protokol *LEACH* yang menjalankan proses pembentukan *cluster*, pemilihan *Cluster Head* (CH) secara probabilistik, dan pengiriman data dari *node* ke CH lalu ke *sink*.
- c. Integrasi Algoritma Enkripsi
Pada skenario kedua, algoritma XOR *Cipher* disisipkan di sisi pengiriman. Data dienkripsi sebelum dikirim dari *node* ke CH dan dari CH ke *sink*. Enkripsi bersifat ringan dan menambah sedikit konsumsi energi dan *delay*.
- d. Pelaksanaan Simulasi
Simulasi dijalankan pada ketiga skenario:

- *Direct Routing*
- Tanpa enkripsi
- Dengan enkripsi data

Simulasi dilakukan sebanyak 100 ronde untuk masing-masing skenario.

e. Pengumpulan dan Analisis Data
Parameter yang diukur meliputi :

- *Energy Consumption*: Energi total yang tersisa pada setiap *node* per *round*.
- *Packet Delivery Ratio* (PDR): rasio paket yang diterima di sink terhadap paket yang dikirim.
- *Delay*: waktu rata-rata pengiriman paket dari *node* ke *sink*.
- *Packet Loss*: jumlah paket yang hilang selama transmisi.

2.4 Variable Penelitian

Variable bebas:

- Integrasi enkripsi ringan (XOR) pada protokol *LEACH* (ya/tidak)

Variable terikat:

- *Energy Consumption*
- *Packet Delivery Ratio* (PDR)
- *Delay*
- *Packet Loss*

2.5 Indikator Keberhasilan

Keberhasilan simulasi diukur dari:

- Sistem dengan enkripsi tetap menjaga efisiensi secara kompetitif.
- Nilai PDR di atas 90% dalam skenario terenkripsi.
- Kenaikan *delay* tetap dalam batas wajar (≤ 10 ms per *packet*).
- Konsumsi energi pada skenario terenkripsi tidak jauh lebih boros dari skenario tanpa enkripsi.

3. Hasil dan Diskusi

Dibagian ini menyajikan hasil dari simulasi dan implementasi dari protokol *LEACH* yang tidak terintegrasi dengan algoritma enkripsi XOR dan yang sudah terintegrasi dengan algoritma enkripsi XOR pada *Wireless Sensor Network* (WSN). Simulasi dilakukan berdasarkan parameter yang telah ditentukan pada **Tabel 2**. Parameter Simulasi, seperti jumlah *node*, ukuran area, energi awal *node*, jumlah ronde, serta metode *routing* dan algoritma enkripsi yang digunakan. Evaluasi kinerja dilakukan dengan membandingkan tiga skenario yaitu *Direct Routing*, *LEACH* tanpa enkripsi, dan *LEACH + XOR*. Parameter performa utama yang diukur meliputi total konsumsi energi per ronde, *Packet Delivery Ratio* (PDR), dan rata-rata *delay*. Hasil pengujian disajikan dalam bentuk tabel dan grafik, diikuti dengan analisis terhadap perbedaan performa antar metode serta dampak integrasi enkripsi XOR terhadap efisiensi dan kualitas komunikasi data dalam jaringan.

Tabel 2. Parameter Simulasi

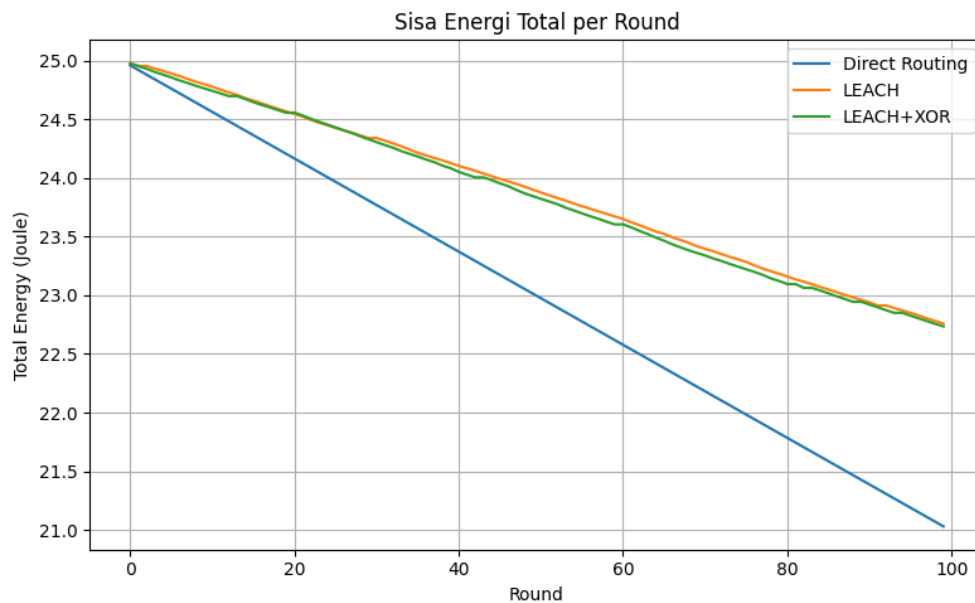
Parameter	Nilai
Jumlah <i>node sensor</i>	50

Parameter	Nilai
Area	100 x 100 m
Energi awal <i>node</i>	0.5 Joule
Protokol <i>routing</i>	LEACH
Algoritma enkripsi	XOR Cipher
Jumlah <i>round</i>	100

3.1 Sisa Energi Total per Round

Tabel 3. Total Energy per Round

Metode	Energy Awal (J)	Energy Akhir (J)	Penurunan (%)	Analisis
Direct Routing	25	21.1	15.6%	Konsumsi energi paling boros karena setiap <i>node</i> mengirim langsung ke <i>sink</i> .
LEACH	25	22.8	8.8%	Lebih efisien karena adanya pengelompokan dan peran <i>Cluster Head</i> (CH).
LEACH + XOR	25	22.75	9.0%	Penambahan enkripsi XOR menambah konsumsi energi sedikit (0.2%).



Gambar 2. Grafik Sisa Energi Total per Round

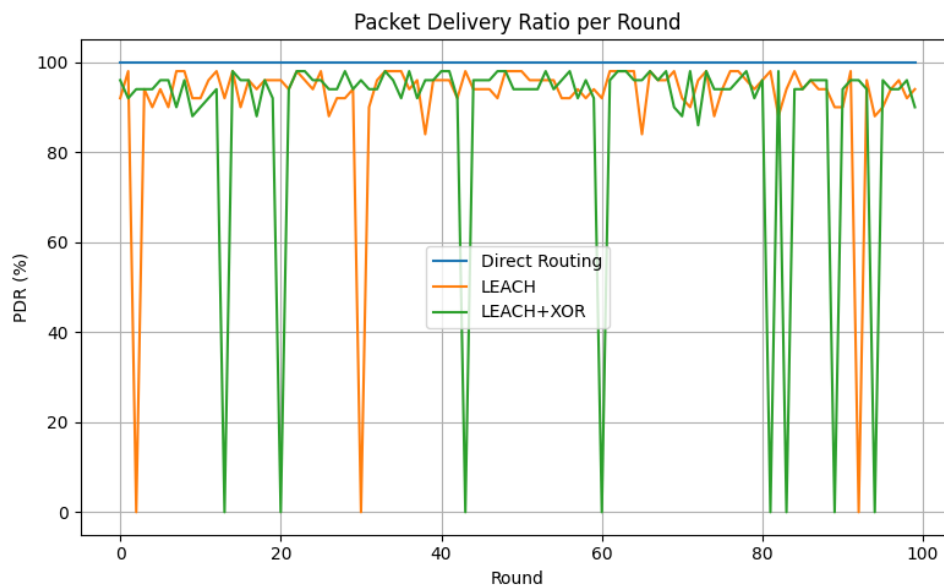
Hasil simulasi pada **Tabel 3** menunjukkan bahwa metode *Direct Routing* memiliki konsumsi energi paling tinggi dibandingkan dengan metode lainnya. Hal ini disebabkan karena pada *Direct Routing*, seluruh *node sensor* mengirimkan data langsung ke *sink* tanpa melalui proses *clustering* atau pengumpulan data oleh CH. Jarak pengiriman yang relatif jauh dari setiap *node* ke *sink* menyebabkan energi cepat habis. Sebaliknya, metode *LEACH* mampu menekan konsumsi energi dengan signifikan. Hal ini didukung oleh mekanisme *clustering*, dimana data dari *node* dikirim terlebih dahulu ke CH yang berperan sebagai perantara sebelum diteruskan ke *sink* mekanisme ini efektif mengurangi transmisi jarak jauh yang boros energi. Pada metode *LEACH*

+ XOR, konsumsi energi sedikit meningkat sebesar 0.2% dibandingkan *LEACH* tanpa enkripsi. Hal ini terjadi akibat penambahan proses enkripsi XOR pada tiap data yang dikirim. Meski demikian, peningkatan tersebut masih tergolong sangat kecil dan berada di batas toleransi sistem WSN yang mengutamakan efisiensi energi. Berdasarkan hasil tersebut *LEACH* terbukti jauh lebih efisien dibandingkan metode *direct* karena mekanisme pengumpulan data oleh *Cluster Head* (CH) mengurangi transmisi jarak jauh yang boros energi. Enkripsi XOR menambah sedikit beban namun masih dalam batas efisiensi yang dapat diterima untuk WSN.

3.2 Packet Delivery Ratio per Round

Tabel 4. Packet Delivery Ratio per Round

Metode	Rata-rata PDR	Fluktuasi	Analisis
<i>Direct Routing</i>	100	Stabil	Sangat stabil karena tidak adanya <i>overhead</i> atau beban protokol tambahan.
<i>LEACH</i>	93 - 98	Ada <i>spike</i> ke 0%	Umumnya stabil, tetapi terdapat beberapa ronde gagal.
<i>LEACH + XOR</i>	90 - 96	Ada <i>spike</i> ke 0%	Enkripsi menambah kompleksitas komunikasi beberapa paket gagal diproses.



Gambar 3. Grafik Packet Delivery Ratio per Round

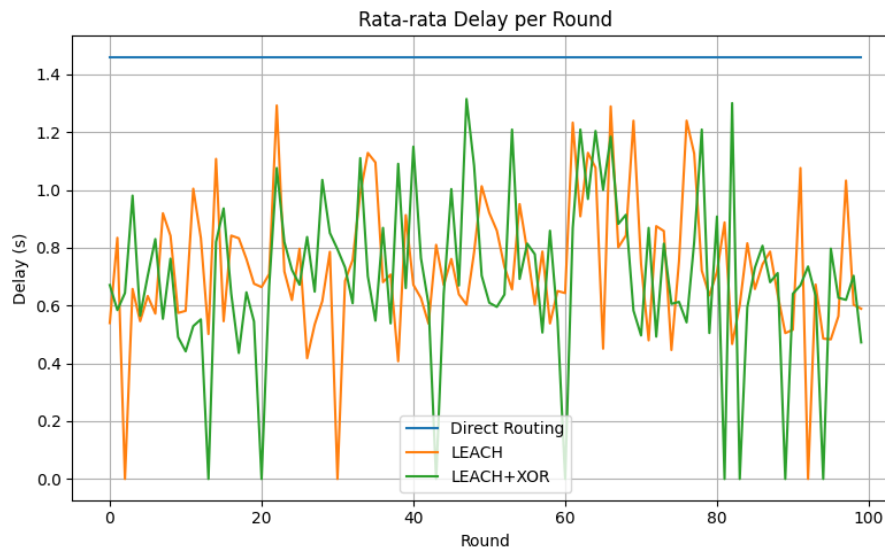
Dari **Tabel 4**, terlihat bahwa *Direct Routing* memiliki nilai PDR sempurna sebesar 100% tanpa fluktuasi. Hal ini dikarenakan tidak adanya proses *clustering* ataupun enkripsi yang menambah kompleksitas pengiriman data. Namun, keunggulan ini diperoleh dengan konsekuensi konsumsi energi yang jauh lebih besar. Pada metode *LEACH*, PDR berada di kisaran 93%-98%. Fluktuasi nilai PDR disebabkan oleh beberapa faktor seperti CH yang tidak terbentuk optimal atau *node* yang kehabisan energi. Selain itu, proses pengelompokan data terkadang menghadapi kondisi jaringan yang tidak stabil saat simulasi berlangsung. Metode *LEACH + XOR* mengalami PDR sedikit lebih rendah di kisaran 90%-96%. Hal ini terjadi akibat penambahan proses enkripsi XOR yang menambah sedikit waktu pemrosesan, sehingga peluang paket tidak sampai dalam waktu yang ditentukan meningkat. Meski demikian, nilai PDR masih berada diatas ambang batas keberhasilan 90%, yang menunjukkan bahwa metode ini tetap layak diterapkan. Jadi kondisi terbaik secara performa murni tanpa enkripsi ada pada *LEACH*. Namun, jika mempertimbangkan

aspek keamanannya dalam jaringan WSN, maka *LEACH + XOR* merupakan kondisi yang cukup baik karena nilai PDRnya yang masih berada diatas ambang keberhasilan 90%.

3.3 Rata-rata Delay per Round

Tabel 5. Rata-rata Delay per Round

Metode	Rata-rata Delay	Fluktuasi	Analisis
<i>Direct Routing</i>	1.45	Stabil	Delay konstan dan tinggi karena transmisi langsung jarak jauh.
<i>LEACH</i>	0.65 - 0.85	Tinggi	Delay relatif rendah, namun fluktuatif tergantung jarak node ke CH.
<i>LEACH + XOR</i>	0.60 - 0.90	Tinggi	XOR menambah sedikit delay, namun tetap lebih rendah dibanding <i>direct</i> .



Gambar 4. Grafik Rata-rata Delay per Round

Delay pada metode *Direct Routing* konsisten tinggi karena setiap *node* mengirimkan data langsung ke *sink*. Jarak pengiriman yang jauh menyebabkan waktu propagasi lebih lama. Metode *LEACH* berhasil menekan nilai *delay* berkat mekanisme *clustering*. Data dikirim ke CH terdekat sebelum diteruskan ke *sink*, sehingga mengurangi jarak pengiriman dan waktu propagasi. Nilai *delay* sedikit fluktuatif tergantung jarak antar *node* dan CH serta posisi CH ke *sink*. *LEACH + XOR* menunjukkan *delay* sedikit lebih besar dibanding *LEACH* tanpa enkripsi, akibat tambahan waktu komputasi saat proses enkripsi XOR. Meski demikian, *delay* masih jauh lebih rendah dibanding *Direct Routing*. Nilai *delay* ini tetap dalam batas wajar dan tidak mengganggu kinerja sistem. Sehingga jika dibandingkan dari ketiga kondisi tersebut, metode yang paling optimal adalah *LEACH + XOR*. Meskipun terdapat sedikit peningkatan *delay*, nilainya tetap dalam rentang toleransi yang tidak mengganggu kinerja jaringan. Selain itu metode ini memiliki keunggulan tambahan berupa keamanan data yang lebih baik selama proses transmisi, tanpa memberikan dampak signifikan terhadap efisiensi energi dan kualitas layanan jaringan WSN.

4. Kesimpulan

Penelitian ini telah berhasil mensimulasikan integrasi protokol *LEACH* dengan algoritma enkripsi ringan XOR dalam jaringan sensor nirkabel (WSN) berbasis simulasi perangkat lunak. Hasil

simulasi menunjukkan bahwa penambahan proses enkripsi XOR tidak memberikan dampak signifikan terhadap efisiensi energi jaringan. Konsumsi energi pada skenario terenkripsi hanya meningkat sekitar 0.2% dibandingkan skenario *LEACH* tanpa enkripsi, yang menunjukkan bahwa algoritma XOR cukup ringan dan efisien untuk diterapkan pada perangkat sensor dengan keterbatasan energi. Selain itu, nilai rata-rata *Packet Delivery Ratio* (PDR) pada skenario dengan enkripsi tetap berada di atas 90%, meskipun terdapat beberapa fluktuasi dan *spike* kegagalan pengiriman. *Delay* rata-rata juga tetap dalam batas wajar, dibawah ambang maksimum 10 milidetik per paket, yang menunjukkan bahwa enkripsi tidak secara signifikan memperlambat proses komunikasi. Secara keseluruhan, integrasi algoritma XOR mampu meningkatkan aspek keamanan komunikasi data pada jaringan WSN tanpa mengorbankan performa pada jaringan. Oleh karena itu pendekatan ini dinilai layak untuk diimplementasikan, khususnya pada sistem WSN yang membutuhkan perlindungan data dengan tetap menjaga efisiensi energi dan keterlambatan pengirim. Untuk pengembangan lebih lanjut, disarankan agar penelitian ini diperluas dengan menggunakan algoritma enkripsi yang lebih kompleks, serta dilakukan pengujian pada lingkungan nyata menggunakan perangkat keras untuk mendapatkan hasil yang lebih komprehensif dan aplikatif.

Daftar Pustaka

- [1] N. Puspitasari, A. Kusyanti, dan F. A. Bakhtiar, "Implementasi Algoritme Acorn untuk Pengamanan Data pada WSN," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 1, pp. 82-89, 2020.
- [2] N. S. Harianja, I. Santoso, dan T. Prakoso, "Optimasi Energi pada Jaringan Sensor Nirkabel Menggunakan Algoritme LEACH," *Transient: J. Ilm. Tek. Elektro*, vol. 11, no. 1, pp. 9-16, 2022.
- [3] R. N. Aimah, P. H. Trisnawan, dan R. A. Siregar, "Studi Pengaruh Jumlah Cluster pada Wireless Sensor Network (WSN) menggunakan Protokol LEACH," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 10, pp. 5043-5049, 2022.
- [4] W. Berlianto, A. S. Budi, dan M. H. H. Ichsan, "Implementasi Protokol LEACH pada Wireless Sensor Network berbasis nRF24L01," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 10, pp. 4680-4688, 2021.
- [5] Y. A. Pratama, A. S. Budi, dan A. Kusyanti, "Implementasi Algoritma Enkripsi Snow-V pada WSN," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 10, pp. 4689-4697, 2021.