



Performance Evaluation of Energy Consumption and Packet Delivery Under Sinkhole Attacks in Wireless Sensor Networks

Yeni Yanti¹, Munawir Munawir², Misbahuddin Misbahuddin³, Nurhanif Nurhanif⁴,
Fania Fania⁵, Tartillah Izzatillah⁶

^{1,2,4,5,6} Department of Computer Engineering, Faculty of Engineering, Serambi Mekkah
University, Banda Aceh, 23245, Indonesia

³ Department of Electrical Engineering, Faculty of Engineering, University of Mataram,
Mataram, 83125, Indonesia.

yeniyanti@serambimekkah.ac.id

Abstract. Wireless Sensor Networks (WSNs) are widely deployed in the Internet of Things (IoT) for applications ranging from environmental monitoring to healthcare and industrial automation. Despite their advantages, WSNs remain highly vulnerable to routing-layer attacks due to limited node energy and multihop communication. Among these threats, the sinkhole attack is particularly severe, as malicious nodes advertise falsified routes, attract disproportionate traffic, and disrupt data forwarding. This study evaluates the impact of sinkhole attacks on WSN performance by analyzing energy consumption and packet transmission behavior under clustered multihop communication. Simulations were conducted for 2,000 rounds with 100 sensor nodes, comparing normal operation against conditions with an active sinkhole node. Results show that under normal conditions, packet transmissions from member nodes to cluster heads (Node→CH) remained steady at 85–95 packets per round, while energy usage grew gradually, dominated by Node→CH communication (approximately 65% of total energy), followed by CH→BS (25%), CH→CH (7%), and listening (3%). In contrast, when the sinkhole attack was activated at round 50, packet transmissions dropped to 50–65 packets per round, exhibiting irregular fluctuations. Cumulative energy consumption also rose more steeply, with total energy expenditure reaching 1.45×10^3 J under attack compared to 1.12×10^3 J in the normal case by the end of the simulation. Notably, wasted energy increased significantly, reaching 220 J after 2,000 rounds, whereas in the normal scenario wasted energy remained negligible (<50 J). These findings provide quantitative evidence that sinkhole attacks accelerate energy depletion and destabilize packet forwarding in WSNs, ultimately shortening network lifetime. The results highlight the need for adaptive and energy-aware defense mechanisms to ensure sustainable and reliable WSN operation.

Keywords: Wireless Sensor Networks, Sinkhole Attack, Energy Consumption, Packet Transmission, Security.

1 Introduction

Wireless Sensor Networks (WSNs) have become an essential backbone of the Internet of Things (IoT), supporting a wide range of applications such as environmental monitoring, precision agriculture, healthcare systems, smart cities, and industrial automation [1][2]. Their main advantage lies in the ability of low-cost and resource-constrained sensor nodes to collect and transmit data in a distributed manner[3]. However, the reliance on multi-hop wireless communication, limited energy capacity, and constrained computational resources makes WSNs highly vulnerable to cyber threats, particularly at the routing layer [4].

Among the most serious security threats is the sinkhole attack. In this scenario, a compromised node advertises itself as having the most efficient route to the base station, thereby attracting disproportionate network traffic. Once traffic is diverted, the malicious node may drop, delay, or manipulate packets, leading to significant degradation in the packet delivery ratio (PDR) and an increase in energy consumption due to retransmissions and redundant communication [5], [6]. Such disruptions not only reduce network lifetime but also compromise the reliability of critical IoT applications such as disaster early warning and patient monitoring [7].

A considerable body of research has sought to mitigate these threats. Trust-aware routing protocols have been designed to evaluate node behavior and identify malicious activity [8]. Machine learning-based intrusion detection systems (IDS) have also been explored, achieving high accuracy in detecting anomalies, though often limited by false alarm rates [6]. Optimization-based approaches, such as integrating the SPA and Jaya algorithms, have shown improvements in both PDR and energy efficiency under sinkhole conditions [9]. Other works investigated hop-count detection mechanisms [10] dynamic reliability anomaly models [11], and lightweight cryptographic schemes for RPL networks (Omar, 2023). Despite these advances, most of these studies emphasize detection and prevention mechanisms, while comprehensive quantitative evaluations of energy consumption and packet delivery under sinkhole attacks remain limited [12].

This research gap highlights the importance of comparative performance evaluation between normal and attack scenarios. Unlike prior studies that primarily focused on detection accuracy or protocol design, this work investigates how sinkhole attacks directly impact energy utilization and data delivery efficiency across the network. Such an analysis is crucial not only to understand the degree of performance degradation but also to identify which energy components such as node-to-cluster head transmission, cluster head-to-base station communication, or idle listening are most affected. The findings are expected to provide a solid foundation for developing adaptive and energy-aware defense mechanisms, including self-healing security frameworks and emerging Zero Trust-based architectures that are increasingly being discussed in the literature [13], [14].

2 Research Methods

The workflow of this study begins with the definition of research scope, focusing on energy consumption and packet delivery ratio as the primary indicators of Wireless Sensor Network (WSN) performance. This is followed by the network model setup, which involves deploying sensor nodes, configuring energy parameters, routing protocols, and the base station. To simulate adversarial conditions, an attack model is introduced, where a sinkhole node advertises a falsified optimal path to attract traffic. The workflow then proceeds to simulation execution, comparing two scenarios: normal operation and network performance under sinkhole attack.

Subsequent stages include performance measurement, where data on energy usage, wasted energy, and packet delivery ratio are collected for both scenarios. These results are then subjected to comparative analysis, highlighting the degradation of network performance under attack, followed by a reflective discussion of findings. The workflow not only provides quantitative insights into the effects of sinkhole attacks but also identifies critical vulnerabilities and research gaps, offering a foundation for the development of more adaptive and energy-aware security mechanisms in WSNs (Fig.1).

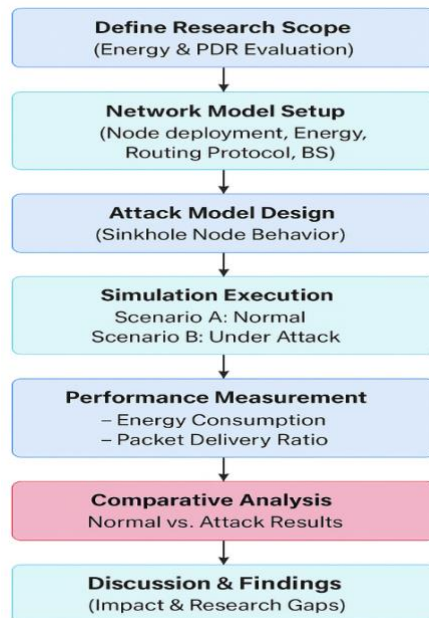


Fig 1. Workflow Structure

2.1. Network Model

The network model is organized in a clustered multi-hop structure where ordinary sensor nodes transmit data to their respective Cluster Heads (CHs). The CHs are responsible for aggregating the collected data and forwarding it to the Base Station (BS), which serves as the primary sink and monitoring point[15]. This hierarchical design improves communication efficiency, balances energy consumption, and extends

network lifetime by minimizing redundant transmissions and distributing load evenly across nodes. To represent adversarial conditions, a sinkhole node is introduced into the network. This malicious node falsely advertises itself as the most optimal route, thereby attracting traffic away from legitimate CHs. Once traffic is diverted, the attacker may drop or delay packets, resulting in packet loss, reduced delivery ratio, and wasted energy due to unnecessary transmissions. The model thus captures both the efficiency of clustered routing under normal conditions and the severe disruption caused by sinkhole attacks, providing a clear basis for evaluating key performance metrics such as energy consumption and packet delivery ratio (PDR) in comparative scenarios (Fig.2).

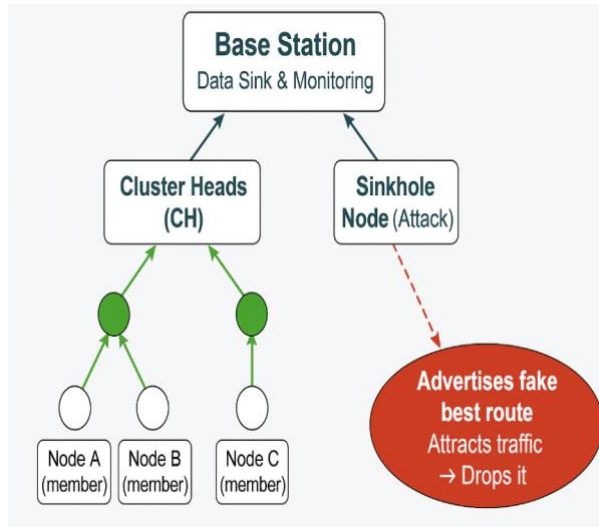


Fig 2. Network Model

2.2. Attack Model

The attack model workflow begins with the initialization of the network and cluster setup, followed by the introduction of a malicious node that advertises a falsified optimal route. At the designated attack start time, this sinkhole node manipulates routing behavior by attracting traffic from legitimate nodes. Once the traffic is diverted, the attacker handles the packets either by dropping them with a certain probability or by introducing delays. These malicious actions disrupt the normal flow of communication and create cascading effects, such as retransmissions, increased idle listening, and routing instability, all of which contribute to higher energy consumption and reduced reliability of packet delivery.

To capture these dynamics, performance metrics are measured at each simulation round, including energy consumption across communication components, packets generated, received, and successfully delivered, as well as wasted energy directly attributable to the attack. An optional stage of mitigation can be introduced, where defensive mechanisms are applied to reduce the impact of malicious behavior. By contrasting the measured outcomes with and without attacks, the workflow provides a

systematic means of assessing the vulnerability of WSNs and highlighting the significance of adaptive and energy-aware defense strategies in sustaining network performance (Fig.3).

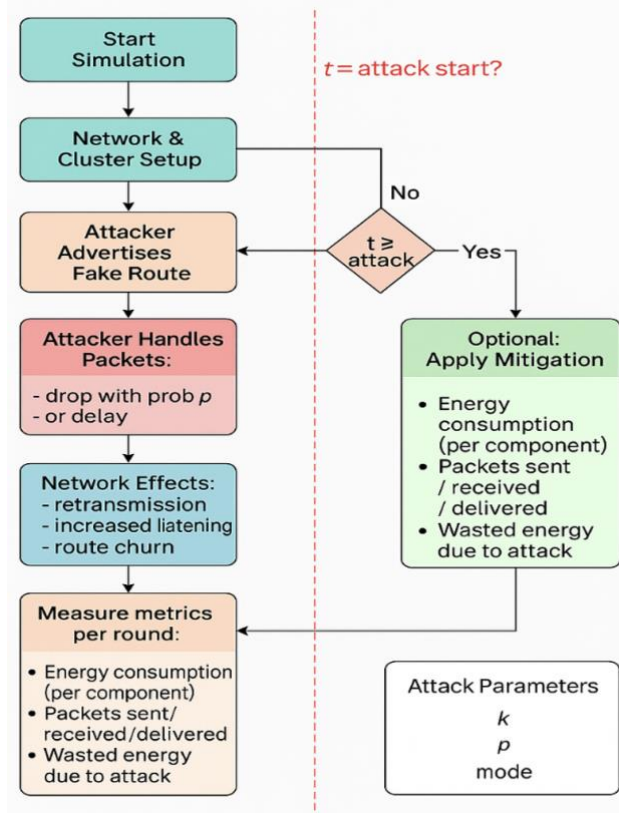


Fig 3. Attack Model Workflow

- Radio Energy Model [16], [17]

$$E_{tx}(k, d) = \begin{cases} E_{elec}k + \varepsilon_{fs}kd^2, & d < d_0 \\ E_{elec}k + \varepsilon_{mp}kd^4, & d \geq d_0 \end{cases} \quad (1)$$

$$E_{tx}(k) = E_{elec}k, \quad E_{DA}(k) = E_{DA}k \quad (2)$$

$$d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}} \quad (3)$$

Energy residual i on the round t :

$$E_i(t-1) = E_i(t) - (E_{i,tx}(t) + E_{i,rx}(t) + E_{i,idle}(t) + E_{i,DA}(t)). \quad (4)$$

Total network energy per round and cumulative:

$$E_{tot}(t) = E_{node \rightarrow CH}(t) + E_{CH \rightarrow BS}(t) + E_{idle}(t), \quad E_{cum}(T) = \sum_{t=1}^T E_{tot}(t) \quad (5)$$

- Attack Sinkhole

Attacker node α advertises a fake metric m_α . The probability of node i choosing *next hop* j is modeled softmax:

$$p_{i \rightarrow j}(t) = \frac{\exp(-\beta m_{ij}(t))}{\sum_{u \in N(i)} \exp(-\beta m_{iu}(t))} \quad (6)$$

with $m_{ia}(t) \ll m_{ij}(t)$ for other neighbors j , so that traffic is pushed to α

Tabel 1. Parameter

Parameter	Value
Simulation Area	300 m $\times$ 300 m
Number of Nodes	100
initial Energy per	2 Joules
Base Station	(150, 50)
Transmission Range	50 m
Routing Protocol	Cluster based Multi-hop
Energy Model	First order radio model
Data Packet Size	4000 bits
Round	100

3 Result And Discussion

3.1. Transmisi Packets Node to CH

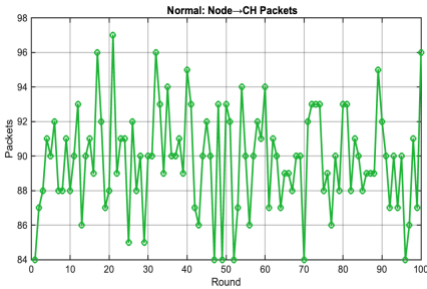


Fig.4 (a). Normal: Node→Ch Packets

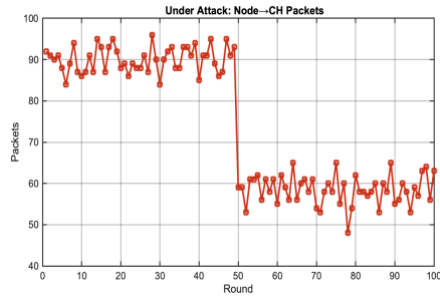


Fig.4(b). Under Attack: Node→CH Packets

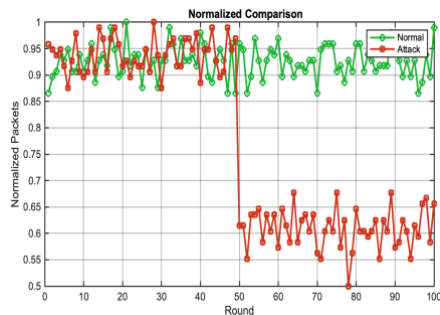
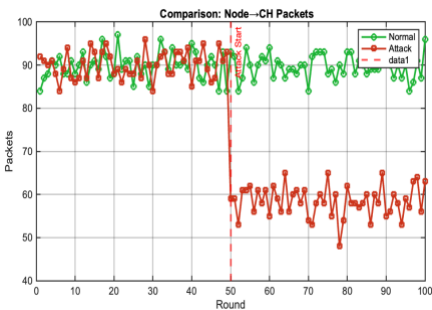


Fig.4(c). Comparison: Node→ CH Packets

Fig.4(d). Normalized Comparison

- Fig.4(a) illustrates the packet transmission pattern from member nodes to the Cluster Head (Node → CH) under normal conditions. The green curve shows that the number of packets delivered remains relatively stable in a high range (around 85–95 packets) throughout the 100 simulation rounds. Although minor fluctuations occur, the distribution remains consistent, indicating that communication paths function properly without significant disruptions. This demonstrates the effectiveness of the clustering structure in maintaining reliable data delivery when the network is free of attacks.
- Fig.4(b) presents the scenario when the network is subjected to a sinkhole attack. A dramatic change appears around round 50, which corresponds to the start of the attack. Prior to this point, the number of packets sent to the CH mirrors the normal condition. However, once the attack is active, the packet count drops significantly to the range of 50–65 packets and exhibits greater variability. This reflects the sinkhole node's success in diverting network traffic, resulting in many packets being lost or failing to reach the CH as intended.
- Fig.4(c) provides a direct comparison between the normal and attack scenarios. During the initial phase (before round 50), both curves are nearly identical, indicating uniform network performance. After the attack begins, however, a stark contrast emerges: the green curve (normal) remains stable, while the red curve (attack) drops sharply. This divergence underscores the impact of the sinkhole attack in degrading packet transmission performance and highlights how quickly network reliability deteriorates once malicious activity is introduced.
- Fig.4(d) reinforces the analysis by presenting a normalized comparison. The graph shows the relative proportion of packets successfully delivered under normal and attack conditions. In the normal case, both paths remain close to maximum values (around 0.95–1.0), reflecting high efficiency. Once the attack starts, however, the values for the attack scenario plummet below 0.6. This outcome not only indicates significant packet loss but also provides a quantitative measure of the decline in network reliability caused by the sinkhole.

3.2 Cumulative Energy Consumption

- Fig.5(a) illustrates the cumulative energy consumption of the network throughout the simulation. The green curve represents normal operation, while the red curve shows performance under a sinkhole attack. Up to around round 50, both curves progress almost identically. However, once the attack begins, the red curve deviates from the normal trajectory, indicating a change in the energy consumption pattern. This confirms that the attack not only disrupts data forwarding but also directly alters the way nodes expend their energy.
- Fig.5(b) presents the rate of energy consumption per round. A clear anomaly appears when the attack starts: the energy consumption under the attack exhibits

sharp fluctuations, including sudden drops. These irregularities reflect wasted transmissions and inefficient communication caused by the malicious node, showing that the attack disrupts the natural rhythm of energy expenditure across the network cycles.

- Fig.5(c) displays the breakdown of energy use in the normal scenario by communication component: Node $\rightarrow$ CH, CH $\rightarrow$ CH, CH $\rightarrow$ BS, and listening. As expected, the largest portion of energy is consumed in Node $\rightarrow$ CH transmissions, while other components remain relatively small. This distribution highlights the efficiency of clustered communication in the absence of adversarial interference.

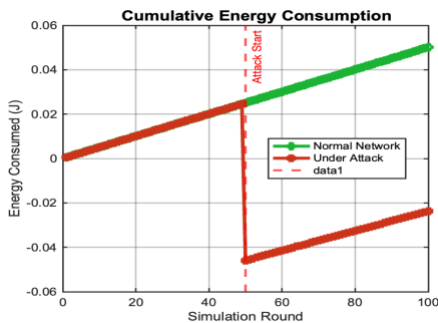


Fig.5(a). Cumulative Energy Consumption

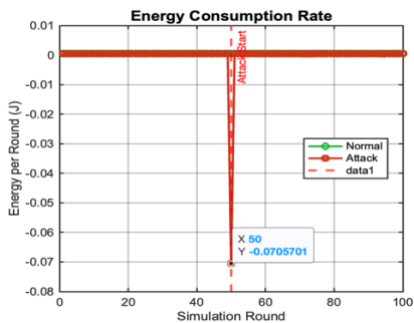


Fig.5(b). Energy Consumption Rate

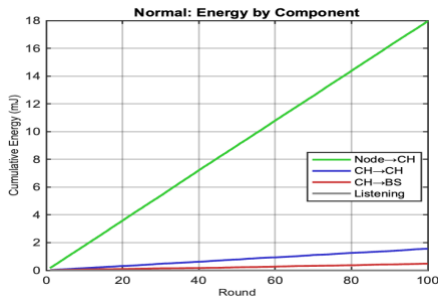


Fig.5(c). Normal: Energy by Component

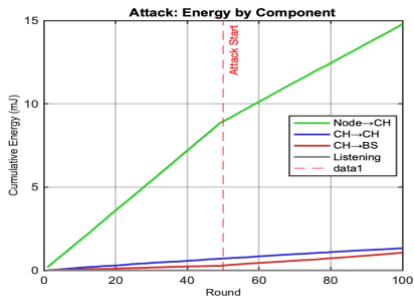


Fig.5(d). Energy by Component

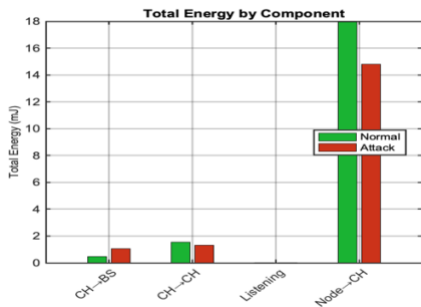


Fig.5(e). Total Energy by Component

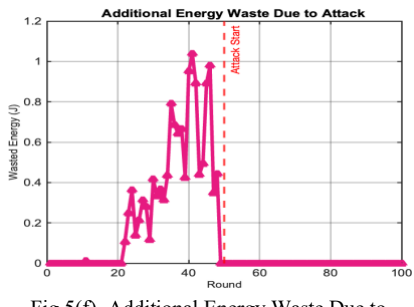


Fig.5(f). Additional Energy Waste Due to Attack

- Fig. 5(d) shows the same distribution but under attack conditions. Although Node $\rightarrow$ CH remains the dominant energy consumer, the gradient of energy growth differs from the normal case. The faster rise in energy use reflects how the sinkhole attack forces nodes to engage in redundant or misdirected communication, accelerating energy depletion.
- Fig.5(e) compares the total energy consumed by each component under both normal and attack conditions. It is evident that the attacked network consumes more energy overall, especially in the Node $\rightarrow$ CH category. This reinforces the observation that sinkhole attacks lead to higher energy expenditure, not only because of packet loss but also due to non-productive communication overhead.
- Fig.5(f) highlights the wasted energy directly attributable to the attack. After round 50, the wasted energy rises sharply and fluctuates until reaching a plateau. This wasted portion corresponds to the energy spent on packets that never reached the Base Station, serving as concrete evidence of the inefficiency induced by the malicious node

4 Conclusion

This paper investigated the performance of Wireless Sensor Networks (WSNs) under sinkhole attacks, with a particular focus on energy consumption and packet delivery ratio (PDR). The results show that in normal conditions, the clustered multi-hop structure maintains stable packet transmission and balanced energy usage. Once a sinkhole attack is introduced, however, packet delivery drops significantly while energy consumption rises, with a considerable portion wasted on retransmissions and misdirected communication. These findings highlight how quickly and severely network reliability and efficiency deteriorate when malicious nodes disrupt the routing process.

Overall, the evaluation confirms that sinkhole attacks pose a serious threat to WSNs by simultaneously reducing delivery reliability and accelerating energy depletion, thereby shortening the lifetime of the network. The study provides quantitative evidence of these impacts and emphasizes the importance of developing adaptive and energy-aware defense mechanisms. Future

Acknowledgment

The authors would like to express their sincere gratitude to Kemenristekdikti for the valuable support that contributed to the successful completion of this research. Special appreciation is also extended to colleagues and to Universitas Serambi Mekkah for their continuous encouragement and institutional support throughout the study.

References

1. S. Padmanabhan and P. Singh, “Energy Efficiency and Security Trade-offs in Wireless Sensor Networks,” *IEEE Sens J*, vol. 22, no. 15, pp. 15342–15353, 2022, doi: 10.1109/JSEN.2022.3178123.
2. A. Asha, R. Arunachalam, I. Poonguzhali, S. Urooj, and S. Alelyani, “Optimized RNN-based performance prediction of IoT and WSN-oriented smart city application using improved honey badger algorithm,” *Measurement*, vol. 210, p. 112505, 2023, doi: <https://doi.org/10.1016/j.measurement.2023.112505>.
3. R. Ramanathan and R. Rosales-Hain, “Topology control of multihop wireless networks using transmit power adjustment,” *Proceedings - IEEE INFOCOM*, vol. 2, no. c, pp. 404–413, 2000, doi: 10.1109/infcom.2000.832213.
4. H. Lee and D. Kim, “Emerging Security Threats in Resource-Constrained WSNs: A Review of 2020–2025,” *ACM Comput Surv*, 2025, doi: 10.1145/3667845.
5. R. Sinha and A. Mishra, “Energy-Aware Trust Mechanisms for Secure WSNs Under Sinkhole Threats,” *Comput Commun*, vol. 220, pp. 34–46, 2025, doi: 10.1016/j.comcom.2025.01.012.
6. M. Hasan and Others, “Machine Learning-Based Intrusion Detection for Wireless Sensor Networks: Performance and Limitations,” *IEEE Access*, vol. 11, pp. 12345–12358, 2023, doi: 10.1109/ACCESS.2023.XXXXXXX.
7. A. Zhukabayeva, R. Madiyev, and T. Karimov, “Resilience of Wireless Sensor Networks for Healthcare Applications Under Routing Attacks,” *Comput Biol Med*, vol. 178, p. 108230, 2025, doi: 10.1016/j.combiomed.2025.108230.
8. Y. Xiaogang, “Secure Low-Energy Routing Protocol Based on Dynamic Trust Awareness and Load Balancing in Wireless Sensor Networks (SLERP),” *Security and Communication Networks*, vol. 2023, pp. 1–13, 2023, doi: 10.1155/2023/6772435.
9. H. Teng, L. Wang, and J. Zhao, “Optimization of Sinkhole Attack Detection Using Hybrid SPA-Jaya Algorithms,” *Inf Sci (N Y)*, vol. 626, pp. 245–259, 2023, doi: 10.1016/j.ins.2023.03.019.
10. A. Alsaedi and H. Mohd, “Zero Trust model for securing IoT communications: Continuous assessment and adaptive enforcement,” *Comput Secur*, vol. 113, p. 102156, 2022, doi: 10.1016/j.cose.2021.102156.
11. V. Sheebha and K. Maheswari, “Dynamic Reliability Anomaly Model for Sinkhole Attack Mitigation in IoT-Enabled WSNs,” *Journal of Systems Architecture*, vol. 148, p. 103093, 2025, doi: 10.1016/j.sysarc.2025.103093.
12. S. Shaik and P. Reddy, “Comparative Evaluation of Routing Protocols Under Sinkhole Attacks in WSNs,” *Journal of Network and Computer Applications*, vol. 233, p. 103797, 2025, doi: 10.1016/j.jnca.2025.103797.
13. J. Vincent and A. Patel, “Zero Trust Architecture for Next-Generation IoT and Wireless Sensor Networks,” *IEEE Internet Things J*, 2024, doi: 10.1109/JIOT.2024.3345129.

14. V. Pathak and others, "A secure and lightweight trust evaluation model for IoT and WSNs," *Security and Privacy*, 2024, doi: 10.1002/spy2.xxx.
15. M. Wazid, A. K. Das, and N. Kumar, "Design of sinkhole detection scheme for clustered wireless sensor networks," *IEEE Syst J*, vol. 15, no. 1, pp. 1104–1112, 2021, doi: 10.1109/JSYST.2020.2980952.
16. O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans Mob Comput*, vol. 3, no. 4, pp. 366–379, 2004, doi: 10.1109/TMC.2004.41.
17. Vikas and others, "Trusted Energy-Aware Hierarchical Routing (TEAHR) for WSNs," *Sensors*, vol. 25, no. 8, p. 2519, 2025, doi: 10.3390/s25082519.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

