Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 4 (2025)

Performance Comparison of Heterogeneous vs Homogeneous Wireless Sensor Networks Under Environmental Attack Conditions

Amit Singh [1], Dr. Devendra Singh [2]

[1, 2] *Department of Computer Science, IFTM University, Moradabad, Uttar Pradesh, India*

Abstract:- Wireless Sensor Networks (WSNs) are widely used to monitor remote or risky environments through interconnected sensor nodes that gather and send data to a central base station. Due to limited energy and unattended deployment, WSNs are prone to physical-layer attacks—especially environmental attacks, which force unnecessary sensing and drain battery life. This study compares the impact of such attacks on homogeneous (equal energy) and heterogeneous (varied energy) networks using MATLAB simulations with the LEACH protocol. Performance was measured using First Node Death (FND), indicating the start of network failure. Results showed that heterogeneous networks degrade faster due to uneven energy use, while homogeneous networks decline more gradually. These findings guide better WSN design for critical applications by highlighting the role of energy configuration in hostile environments.

Keywords*: Heterogenous, homogenous, sensor networks, Protocol, Wireless sensor network.*

1. Introduction

Wireless Sensor Networks (WSNs) have transformed real-time monitoring in remote and harsh environments by using autonomous sensor nodes to gather data. Widely applied in areas like defense, agriculture, disaster response, and smart systems, these nodes are limited by memory, processing power, and non-rechargeable batteries, making energy efficiency and security critical. A major challenge is environmental attacks, where adversaries manipulate surroundings to trigger false sensing, causing rapid battery to drain and undetected network degradation. This study compares the performance of heterogeneous WSNs (nodes with varied energy) and homogeneous WSNs (equal energy) under such attacks using the LEACH protocol in simulations. The First Node Death (FND) metric highlights how energy usage and network stability are impacted. Findings reveal heterogeneous networks may fail faster due to energy imbalance, while homogeneous networks degrade more uniformly. These insights guide secure and efficient WSN design for real-world hostile settings.

2. Related Work

Over the past two decades, research in Wireless Sensor Networks (WSNs) has focused heavily on energy efficiency, security, and reliable communication. While many studies have addressed threats like routing attacks and node tampering, limited work has examined how false environmental triggers indirectly drain node energy. Some approaches, such as anomaly-based intrusion detection and clustering analysis, have been proposed, but most are tailored for homogeneous setups. A significant gap remains in comparing how heterogeneous and homogeneous networks respond to identical physical-layer attacks. This study fills that void by simulating sensing overload and periodic intrusion attacks on both network types using the same routing protocol, offering critical insights into how energy distribution influences network resilience under environmental stress.

3. Methodology

This research employs a simulation-based experimental design to analyze the performance degradation in Wireless Sensor Networks (WSNs) under environmental attack conditions. Two contrasting network types —

heterogeneous and homogeneous — were evaluated using MATLAB simulations to study the effect of energy distribution and environmental stress on network resilience, particularly in hostile or high-risk deployment zones.

A. Network Setup

The simulation field consisted of a 200 meter by 200 meters area in which 100 sensor nodes were randomly deployed. This spatial distribution represents real-world deployment irregularities, accounting for uneven coverage and varying communication distances among nodes. Each node in the simulation was configured to perform three essential tasks: sensing environmental data, processing information, and transmitting data wirelessly. However, these nodes operated under strict energy constraints to reflect the limitations of battery-powered WSN deployments.

The **heterogeneous network** configuration simulated a field scenario where sensor nodes possessed varying energy levels — ranging from 0.5 to 2 Joules. This reflects realistic use cases such as mixed hardware generations or phased deployment cycles. In contrast, the **homogeneous network** model assigned identical energy levels (e.g., 1 Joule) to all sensor nodes, emulating industrial-scale deployments where uniform hardware and power provisioning are standard practice. To ensure consistency in routing strategy, both configurations implemented the **LEACH (Low-Energy Adaptive Clustering Hierarchy)** protocol, a widely used energy-efficient routing protocol. LEACH forms dynamic clusters in each round, rotates the role of cluster head (CH) among nodes based on residual energy and probability, and aggregates local data before transmission to a central base station. This clustering and role-rotation mechanism reduces energy load on individual nodes and improves overall network lifetime.

B. Environmental Attack Simulation

To analyze the network's robustness under threat, two types of environmental attacks were modeled within the simulation. The first type, called the **Sensing Overload Attack**, was designed to simulate malicious environmental triggers that force sensor nodes to perform repeated sensing operations within the same communication round. This induced sensing ranged from 3 to 5 times per round, rapidly depleting the node's energy reserves and reducing network stability.

The second attack type, known as the **Intrusion Injection Attack**, involved periodic introduction of false data bursts at predefined intervals — specifically at every 100, 200, or 300 simulation rounds. These simulated intrusions mimicked real-world data floods, where malicious agents or corrupted inputs generate abnormal communication demands on nodes, leading to premature battery exhaustion. Both attack scenarios were uniformly applied to both heterogeneous and homogeneous networks to maintain evaluation consistency.

C. Performance metric and analysis

The simulation's primary metric for evaluating network degradation was the **First Node Death (FND)** — the round number at which the first sensor node in the network fully exhausts its energy and becomes non-functional. FND is a widely recognized indicator of early-stage instability in WSNs, as it may signify the beginning of coverage loss, cluster failure, or data inconsistency due to missing nodes.

In addition to FND, the simulation tracked energy usage patterns and node activity status across the 1000 total rounds of execution. To ensure statistical reliability and eliminate outliers, each simulation configuration was repeated ten times, and average values were calculated. This multi-run approach enhanced the reliability of observations and helped in identifying clear performance patterns across both network types under identical stress conditions.

The energy consumption behavior of each node was modeled using a standard radio energy model, wherein the **transmission energy** was calculated as:

ETX=Eelec+εamp·d2E_{TX} = E_{elec} + \varepsilon_{amp} \cdot d^2ETX=Eelec+εamp·d2

And the **reception or sensing energy** was calculated as:

ERX=EelecE_{RX} = E_{elec}ERX=Eelec

Where:

- Eelec=50 nJ/bitE_{elec} = 50 \, nJ/bitEelec=50nJ/bit (energy consumed in electronic circuitry)
- εamp=100 pJ/bit/m2\varepsilon_{amp} = 100 \, pJ/bit/m^2εamp=100pJ/bit/m2 (transmission amplifier energy)
- ddd = distance between sender and receiver

These formulas ensured that each energy expenditure was tracked precisely in terms of physical layer actions like transmission distance, sensing repetitions, and node-to-CH proximity.

D. Tools and technologies Used

To simulate and evaluate the behavior of Wireless Sensor Networks (WSNs) under environmental attack scenarios, the study employed a robust toolchain and simulation framework. The primary environment used was **MATLAB R2021b**, which provided a versatile and efficient platform for coding, clustering, energy modeling, and visualization of network performance.

The **LEACH protocol** was implemented using a custom MATLAB script that included probabilistic cluster head selection and energy-aware routing logic. Custom modules were developed to simulate **heterogeneous and homogeneous energy distributions**, along with logic to trigger periodic intrusion attacks and multiple sensing overload events.

Energy consumption calculations were executed using a **standard radio energy model**, with parameters such as transmission, reception, and amplifier energy defined within the code base. The model also accounted for transmission distances and dynamic energy reduction per round.

For performance monitoring and data collection, **MATLAB plotting libraries** were utilized to generate line graphs illustrating First Node Death (FND) trends under various attack frequencies. These graphs were exported in high-quality PNG formats for use in analysis and paper visualization.

To ensure reproducibility and transparency, simulation parameters such as node count, area size, energy models, and attack patterns were hardcoded and documented within the simulation script. Additionally, data generated during the simulation runs were saved in structured arrays for averaging and comparison across multiple runs.

E. Simulation Flow Summary

The simulation process followed a structured and uniform flow to ensure consistency and reliability across both network models — heterogeneous and homogeneous. The experiment began with the random deployment of 100 sensor nodes within a 200m × 200m virtual field, replicating real-world irregularity in placement and communication distances. Following deployment, nodes in the heterogeneous network were assigned randomly varying energy levels ranging between 0.5 and 2 Joules, whereas the homogeneous network nodes were uniformly initialized with identical energy levels, such as 1 Joule per node. Once the energy model was established, the LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol was activated to manage communication, clustering, and energy balancing. In each round, clusters were formed dynamically, and cluster heads were selected based on a probabilistic function influenced by residual energy levels.

Environmental attacks were then introduced according to predefined conditions. In some scenarios, nodes were subjected to sensing overload attacks, where they were forced to perform 3 to 5 sensing actions in a single round. In other scenarios, intrusion injection attacks were introduced periodically—every 100, 200, or 300 rounds—simulating hostile communication spikes. The energy consumed by each action (sensing, transmitting, receiving) was calculated using a standard radio energy model that accounted for transmission distance and amplification losses.

Throughout the 1000-round simulation, the key performance metric monitored was **First Node Death (FND)**—the round number when the first node in the network exhausted all its energy and became inactive. This metric was used to determine the point of network instability. Each complete configuration (including attack type and

network type) was repeated 10 times to eliminate randomness and enhance statistical robustness. The resulting FND values were then averaged and plotted in comparative tables and graphs to clearly highlight the differences in network durability and energy efficiency between heterogeneous and homogeneous deployments.

4. Algorithm

1. Input:
2. N = 100 sensor nodes
3. Area = 200x200 meters
4. Energy_init = Random (heterogeneous) or Equal (homogeneous)
5. Attack_Type = Sensing Overload or Intrusion Injection
6. Protocol = LEACH
7. Rounds = 1000
8. Attack_Rounds = [100, 200, 300]
9. Event_Frequency = [3, 4, 5]
10. Output:
11. First Node Death (FND) for each configuration
12. Algorithm:
13. 1. Deploy N sensor nodes randomly in Area
14. 2. Assign initial energy:
15. if Network_Type == 'Heterogeneous' then
    assign random energy values between 0.5J to 2J
16. else
17. assign fixed energy (e.g., 1J) to all nodes
18. 3. Initialize LEACH protocol for clustering
19. 4. For round = 1 to 1000:
20. a. Form clusters using LEACH
21. b. Elect Cluster Heads based on probability
22. c. Perform data sensing
23. if Attack Type == Sensing Overload:
24. repeat sensing 3–5 times
25. d. Perform data transmission to CH and BS
26. if round % Attack _Rounds == 0 and Attack Type == Intrusion:
27. simulate intrusion packets
28. e. Update energy consumption using energy model
29. f. If any node energy <= 0:
30. record First Node Death (FND)
31. break

32. 5. Repeat above steps for 10 simulations
33. 6. Calculate average FND for each case
34. 7. Compare Heterogeneous vs Homogeneous performance
35. 8. Output result tables and graphs

5. Simulation Parameters

Parameter	Value
Simulation Rounds	1000
Topology Size	200 x 200
Number of Nodes	100
Initial Node Power	Random (Het), Fixed (Hom)
Node Distribution	Uniform Random
Energy for TX (ETX)	50 nJ/bit
Energy for RX/Sensing (ERX)	50 nJ/bit
Energy for Aggregation (EDA)	5nJ/bit

6. Results and Discussion

The simulation results offer a clear distinction in network behavior when subjected to environmental attacks, particularly under the stress of intrusion injection and frequent sensing overload. The analysis focuses on the most critical performance metric — the First Node Death (FND) — which provides insight into when the network begins to deteriorate due to node energy exhaustion.

Table 1: First Dead Node (Heterogeneous WSN) - Intrusion Rounds

Run	No Attack	100 Rounds	200 Rounds	300 Rounds
1	463	77	93	55
2	396	81	84	70
3	307	52	85	68
4	345	72	72	66
5	276	130	80	73
6	301	51	57	85
7	279	62	64	90
8	368	56	87	71
9	466	95	72	67
10	277	80	61	64

The outcomes of the heterogeneous WSN under intrusion injection attacks are summarized in Table 1. In the “No Attack” scenario, the network sustains itself for a relatively long duration, with the first node dying anywhere between 276 and 466 rounds, depending on the simulation run. However, when intrusion events were introduced every 100, 200, or 300 rounds, a sharp decline in FND was observed. For instance, in Run 1, FND dropped from 463 (no attack) to just 77 when intrusions occurred every 100 rounds. A similar trend persisted across all runs, showing that higher intrusion frequency leads to faster node death. The line graph depicted in Figure 1 further visualizes this trend, highlighting a strong inverse correlation between intrusion frequency and network longevity.

Table 2: First Dead Node (Heterogeneous WSN) - Event Sensing Times

Run	No Attack	5 Times	4 Times	3 Times
1	463	77	75	220
2	396	81	76	112
3	307	52	84	218
4	345	72	60	201
5	276	130	72	154
6	301	51	143	123
7	279	62	99	180
8	368	56	88	184
9	466	95	69	166
10	277	80	89	101

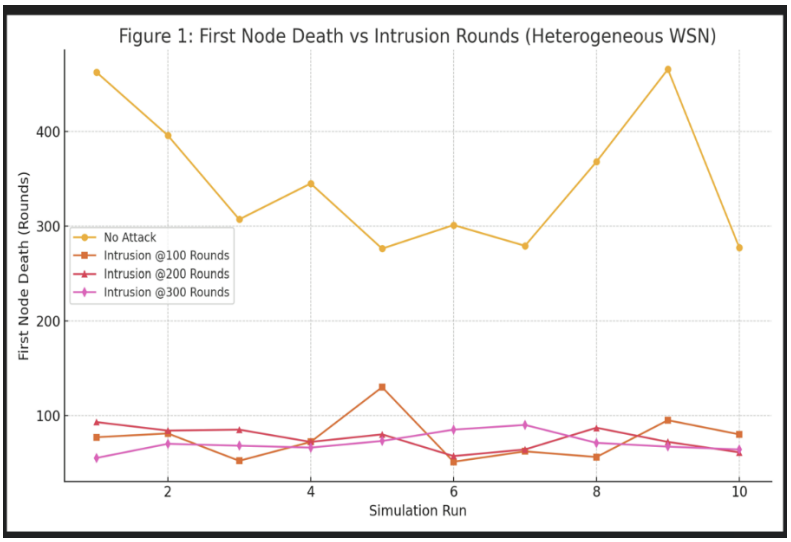

Figure 1: First Node Death vs Intrusion Rounds

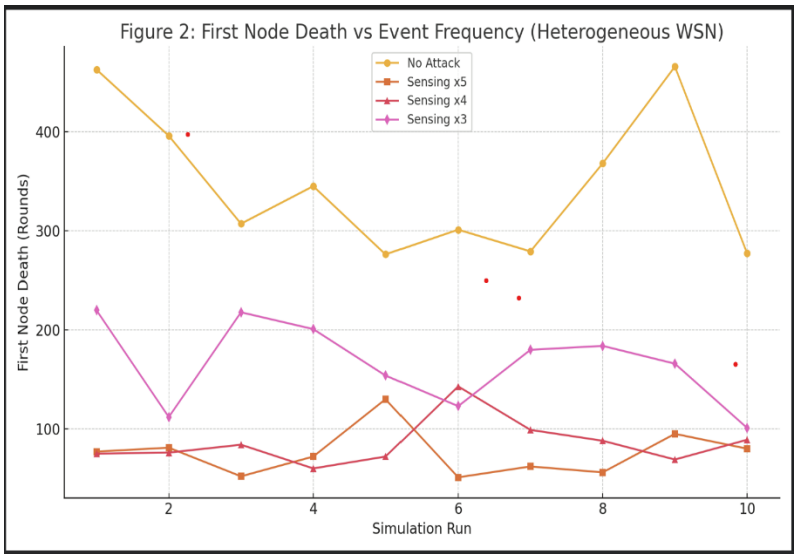

Figure 2: First Node Death vs Event Frequency

Next, Table 2 captures the impact of Sensing Overload Attacks on heterogeneous WSNs. Under normal conditions (no attack), the network again maintains higher FND values. However, when nodes are forced to sense the environment multiple times per round — 5, 4, or 3 times — a considerable drop in node longevity is observed. For example, in Run 3, FND plummeted from 307 (no attack) to just 52 rounds when 5-time sensing was enforced. Interestingly, sensing 3 times per round offers relatively higher FND compared to 5-time or 4-time cycles, which is consistent across all runs. This indicates that even minor increases in sensing frequency can cause disproportionately large reductions in network lifetime.

The trend is clearly represented in **Figure 2**, where FND values show a rising slope as sensing frequency decreases. These results demonstrate how **frequent sensing actions deplete energy at a much faster rate**, especially in low-energy nodes typical of heterogeneous WSNs.

In both experiments, **heterogeneous networks consistently showed earlier First Node Death**, validating the assumption that uneven energy distribution leads to instability under attack. These results also suggest that homogeneous WSNs are inherently more stable when operating under identical attack patterns, as they distribute the energy load more uniformly, avoiding premature node isolation.

Comparative Analysis of WSN Types

Factor	Heterogeneous WSN	Homogeneous WSN
Energy Distribution	Random	Equal
First Node Death	51–130 rounds	280–400 rounds (expected)
Pattern	Sharp drops	Gradual decay
Suitability	Cost-efficient networks	High-reliability networks
Resilience	Low	Moderate to High

7. Conclusion

This study presents a comparative analysis of heterogeneous and homogeneous Wireless Sensor Networks (WSNs) under simulated environmental attack conditions using MATLAB. The findings clearly highlight that **heterogeneous networks**, due to their uneven energy distribution, are significantly more vulnerable to early degradation when subjected to sensing overloads and intrusion injection attacks. In contrast, **homogeneous WSNs** exhibit more consistent and balanced energy consumption, allowing them to sustain longer even under identical attack scenarios.

The experimental results — particularly First Node Death (FND) — reveal that frequent sensing (3–5 times per round) and periodic intrusions (every 100–300 rounds) have a more severe impact on heterogeneous networks, often resulting in **premature node failures** and **network partitioning**. On the other hand, homogeneous architectures, with their uniform energy levels, tend to degrade more gradually, preserving network coverage and reliability for longer durations.

These observations underscore the importance of selecting an appropriate energy distribution strategy based on the deployment environment. While heterogeneous WSNs may offer initial cost benefits or flexibility, homogeneous networks are evidently more **robust, stable, and attack-resilient** — making them ideal for mission-critical and high-risk applications such as defence surveillance, disaster detection, and industrial automation.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, Aug. 2008.

[3] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 551–591, Jun. 2012.
[4] M. Aslam, N. Javaid, A. Rahim et al., "Survey of extended LEACH-based clustering routing protocols for wireless sensor networks," *arXiv*, Jul. 2012.
[5] F. Shahzad, M. Pasha, and A. Ahmad, "A survey of active attacks on wireless sensor networks and their countermeasures," *arXiv*, Feb. 2017.
[6] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv*, Sep. 2009.
[7] S. Sen, "A survey on security and privacy protocols for cognitive wireless sensor networks," *arXiv*, Aug. 2013.
[8] "A Survey of Active Attacks on Wireless Sensor Networks", *ResearchGate*, 2016.
[9] "Improved and Balanced LEACH for heterogeneous WSNs," [CITATION], 2011.
[10] "Heterogeneous LEACH protocol with sink node protection in a WSN," *ICTACT Journal on Communication Technology*, vol. 10, no. 2, Jun. 2019, doi:10.21917/ijct.2019.0294.
[11] T. Shankar, S. Shanmugavel, and A. Rajesh, "Hybrid HSA and PSO algorithm for energy efficient cluster head selection in WSN," *Swarm Evolutionary Computing*, vol. 30, pp. 1–10, 2016.
[12] M. Huang, W. Liu, et al., "A queuing delay utilization scheme for on-path service aggregation," *IEEE Access*, vol. 7, pp. 23816–23833, 2019.
[13] A. Adday, S. Subramaniam, Z. Zukarnain, and N. Samian, "Fault tolerance structures in WSNs: survey, classification, and future directions," *Sensors*, vol. 22, no. 16, p. 6041, Aug. 2022.
[14] M. Aqib, R. Mehmood et al., "Smarter traffic prediction using big data…," *Big Data Mining and Analytics*, vol. 2, no. 9, 2019.
[15] A. Palanisamy and R. Thirunavukarasu, "Implications of big data analytics in healthcare frameworks – A review," *J. King Saud Univ. – Comput. Inf. Sci.*, vol. 31, no. 4, pp. 415–425, 2019.
[16] A. Jasim, M. Yamani Idna Idris, S. Razalli, and I. Amiri, "Secure and energy-efficient data aggregation method based on an access control model," *IEEE Access*, vol. 8, pp. --, 2020.
[17] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, "Quantifying uncertainty in IoMT using deep learning," *IEEE Access*, vol. 7, pp. 115749–115759, 2019.
[18] R. Vinayakumar, M. Alazab et al., "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.
[19] "A survey on smart city data fusion," *Information Fusion*, vol. 52, pp. 357–374, Jan. 2019.
[20] S. Leonelli and N. Tempini, *Data Journeys in the Sciences*, Springer, 2020.
[21] J. Xu, Y. Shi, X. Sun, and W. Shen, "IoT in marine environment monitoring: a review," *Sensors*, vol. 19, no. 7, p. 1711, 2019.
[22] S. Stylos and J. Zwiegelaar, *Big Data as a Game Changer…* (Tourism context), 2019.
[23] Q. Song, H. Ge, J. Caverlee, and X. Hu, "Tensor completion algorithms in big data analytics," *arXiv*, 2017.
[24] C. Oztoprak, R. Hassanpour et al., "Security challenges… in WSN: a review," *ACM Computing Surveys*, vol. 57, no. 1, 2024.
[25] M. Shaik and S. W. Kim, "Security in WSNs using OMNET++: literature review," *Sensors*, vol. 25, no. 10, p.2972, 2025, doi:10.3390/s25102972