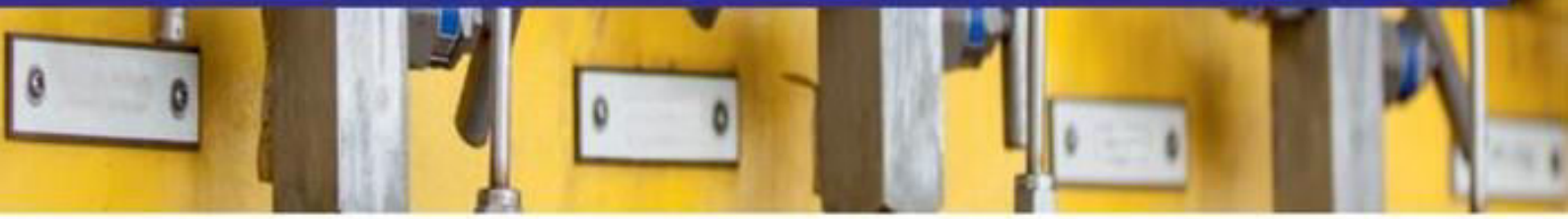
IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 15, Issue 5, May 2026



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 9.867

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

A Distance-Aware and Duty-Cycle-Based Intrusion Detection Framework for Wireless Sensor Networks

Sachin Kumar[1], Sumit Dalal [2], Rohini Sharma[3]

P.G. Student, Department of ECE, Sat Kabir Institute of Technology and Management, Ladrawan, Haryana, India[1]

Assistant Professor, Department of ECE, Sat Kabir Institute of Technology and Management, Ladrawan, Haryana, India[2]

Assistant Professor, Department of CS, GPGCW, Rohtak, Haryana, India[3]

ABSTRACT: Wireless Sensor Networks (WSNs) are widely used in applications such as environmental monitoring, military surveillance, healthcare systems, and smart infrastructure. However, the limited energy resources of sensor nodes and the vulnerability of WSNs to intrusion attacks pose significant challenges for maintaining secure, long-lasting network operation. Traditional intrusion detection approaches often consume excessive energy due to continuous sensing and communication, resulting in reduced network lifetime and degraded coverage. To address these issues, this paper presents a distance-aware, duty-cycle-based intrusion detection framework for wireless sensor networks that improves energy efficiency while maintaining effective intrusion detection. In the proposed framework, sensor nodes are randomly deployed within a sensing field, and intruder movement is simulated dynamically across the network. Intrusion detection is performed using distance-based sensing, in which only nodes within the intruder's sensing range of the intruder actively participate in detection. To further reduce unnecessary energy consumption, a duty-cycling mechanism is incorporated, enabling sensor nodes to alternate between active and sleep states based on network conditions. Additionally, distance-based optimization prioritizes energy use for nodes closer to the intruder while minimizing energy use for distant nodes. Experimental results demonstrate that the proposed framework significantly improves energy efficiency and prolongs network lifetime while maintaining reliable intrusion detection performance and sensing coverage. The integration of duty cycling and distance-aware optimization provides a balanced solution for achieving secure, energy-efficient, and sustainable WSN operation.

KEYWORDS: Intrusion Detection Systems (IDS), WSN, Energy-efficiency, Duty-Cycle

I. INTRODUCTION

A WSN consists of a large number of sensor nodes deployed over a sensing area to monitor physical or environmental conditions and communicate the collected information to a central base station. Due to their distributed nature, low-cost deployment, and wireless communication capability, WSNs offer significant advantages in real-time monitoring applications. However, sensor nodes operate with limited battery energy, processing capability, and communication resources, making energy efficiency one of the most critical design challenges in WSNs. Studies such as Gupta et al. [1] and Gupta and Arora [3] emphasize the importance of optimization techniques for improving network coverage, clustering efficiency, and energy utilization in wireless sensor environments.

In addition to energy constraints, WSNs are highly vulnerable to various security threats because they are often deployed in unattended or hostile environments. Malicious intrusions, unauthorized access, packet manipulation, and routing attacks can severely degrade network performance and reliability. Malik et al. [2] highlighted the growing sophistication of cyberattacks in communication systems, demonstrating the need for robust intrusion detection mechanisms. Traditional security methods are often unsuitable for WSNs due to the computational and communication overhead they introduce. Therefore, lightweight and energy-aware intrusion detection approaches are required to ensure secure and sustainable network operation.

Several intrusion detection techniques have been proposed in the literature, including signature-based, anomaly-based, and hybrid intrusion detection systems. Signature-based methods detect known attacks by comparing network activity with predefined attack patterns [6], while anomaly-based methods identify deviations from normal network behavior

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

[7]. Hybrid intrusion detection approaches combine both techniques to improve detection accuracy and adaptability [8]. Furthermore, machine learning-based intrusion detection methods have shown promising performance in identifying malicious activities efficiently [8], [9]. Despite these advancements, many intrusion detection systems still consume excessive energy due of continuous sensing, monitoring, and communication. To address these challenges, this paper proposes a distance-aware, duty-cycle-based intrusion detection framework for wireless sensor networks that improves energy efficiency while maintaining reliable intrusion detection. The proposed methodology begins with the random deployment of sensor nodes in a predefined sensing field, where each node is initialized with specific energy and sensing parameters. An intruder is then introduced into the network, and its movement is simulated dynamically across the sensing area. At each simulation step, the distance between the intruder and sensor nodes is calculated to determine whether intrusion detection occurs within the sensing range.

The overall process flow of the proposed framework is illustrated in Figure 1. The methodology begins with network initialization, in which sensor nodes are randomly deployed and assigned sensing and energy parameters. An intruder is then introduced into the sensing field, and distance calculations are performed at each simulation step to identify intrusion events within the sensing range of sensor nodes. The framework further incorporates an energy consumption model, along with duty-cycling and distance-based optimization techniques, to reduce unnecessary energy consumption and extend network lifetime. Finally, the system evaluates network performance using metrics such as energy consumption, network lifetime, coverage, and alive node statistics, and then presents the results in a graphical visualization and comparative analysis. The proposed framework incorporates an energy consumption model to estimate the energy usage of sensor nodes during sensing, communication, and idle operation. To reduce unnecessary energy consumption, a duty-cycling mechanism is introduced that alternates nodes between active and sleep states. Only selected nodes remain active for intrusion monitoring, while inactive nodes conserve energy in sleep mode. In addition, a distance-based optimization strategy is employed to adjust energy consumption according to the proximity of sensor nodes to the intruder. Nodes located closer to the intruder participate more actively in detection, whereas distant nodes consume less energy, thereby balancing detection performance and energy efficiency.

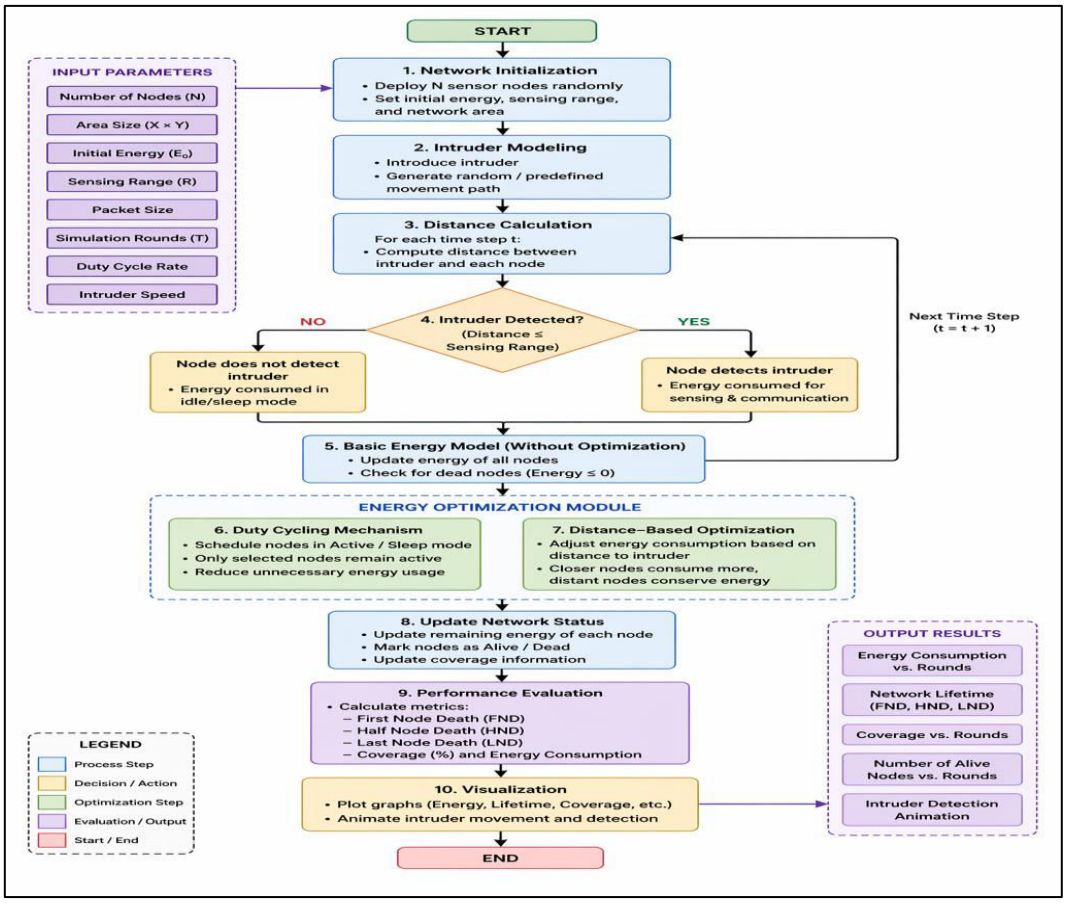


Figure 1: Process Flow of the IDS Framework

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

II. RESEARCH BACKGROUND

Intrusion Detection Systems (IDS) have become an essential component of modern network security due to the rapid growth of cyber threats and unauthorized access attempts in communication systems. Traditional security mechanisms, such as encryption and authentication, are often insufficient to defend against evolving attacks, underscoring the importance of IDS as a secondary layer of protection. Over the years, significant research has been conducted to improve the efficiency, accuracy, and adaptability of intrusion detection techniques through machine learning, anomaly detection, and hardware acceleration**.**

Machine learning has emerged as one of the most promising techniques for intrusion detection because of can automatically learn complex patterns from network traffic and identify malicious activity. Chih-Fong Tsai et al. [10] presented a comprehensive review of machine learning approaches for intrusion detection, highlighting the effectiveness of classification algorithms such as decision trees, neural networks, support vector machines (SVM), and clustering techniques in improving detection performance. Their work demonstrated that intelligent learning-based systems can significantly enhance the capability of IDS to identify both known and unknown attacks compared to traditional rule-based systems. Anomaly-based intrusion detection has also received considerable attention because of its capability to detect previously unseen attacks. Zied Trabelsi and Mahdy [11] proposed an anomaly-detection approach based on associative string processing techniques to efficiently identify abnormal network activity. Unlike signature-based systems, anomaly-based IDS continuously monitors deviations from normal behavior, enabling the detection of zero-day attacks and other sophisticated malicious activities.

To address the increasing computational demands of machine learning-based intrusion detection, researchers have explored hardware acceleration using Field-Programmable Gate Arrays (FPGAs). Michail Papadonikolakis and Bouganis [12] introduced an FPGA-based Support Vector Machine (SVM) classifier capable of achieving faster classification speeds while maintaining high detection accuracy. Similarly, Das et al. [13] proposed an FPGA-based network intrusion detection architecture designed to improve real-time processing efficiency for high-speed networks. Further improvements were introduced by Papadonikolakis and Bouganis [14], who developed a cascade FPGA accelerator for SVM classification, enabling enhanced scalability and performance in intrusion detection applications. Despite the advancements in IDS techniques, intrusion detection systems remain vulnerable to adversarial attacks and evasion strategies. Igino Corona et al. [15] analyzed adversarial attacks against IDS and discussed various open issues and countermeasures associated with secure intrusion detection. Their work emphasized that attackers can manipulate network traffic patterns to bypass machine learning models, thereby reducing detection reliability and highlighting the need for robust and adaptive IDS frameworks.

The evaluation and benchmarking of IDS performance have also played a crucial role in intrusion detection research. Lippmann et al. [16] introduced the DARPA intrusion detection evaluation dataset, which became one of the earliest standardized benchmarks for assessing IDS effectiveness under different attack scenarios. In addition, Kabiri and Ghorbani [17] presented a broad survey of intrusion detection and response systems, discussing the importance of automated response mechanisms in minimizing attack impact and improving network resilience. Although machine learning techniques have shown significant promise, practical deployment challenges still exist. Sommer and Paxson [18] argued that applying machine learning to intrusion detection in real-world environments is difficult due to factors such as dynamic traffic patterns, complex feature selection, false alarms, and evolving attack behaviors. Their work highlighted the importance of developing adaptive and lightweight IDS models capable of balancing detection accuracy with computational efficiency.

.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

III. PROPOSED METHODOLOGY

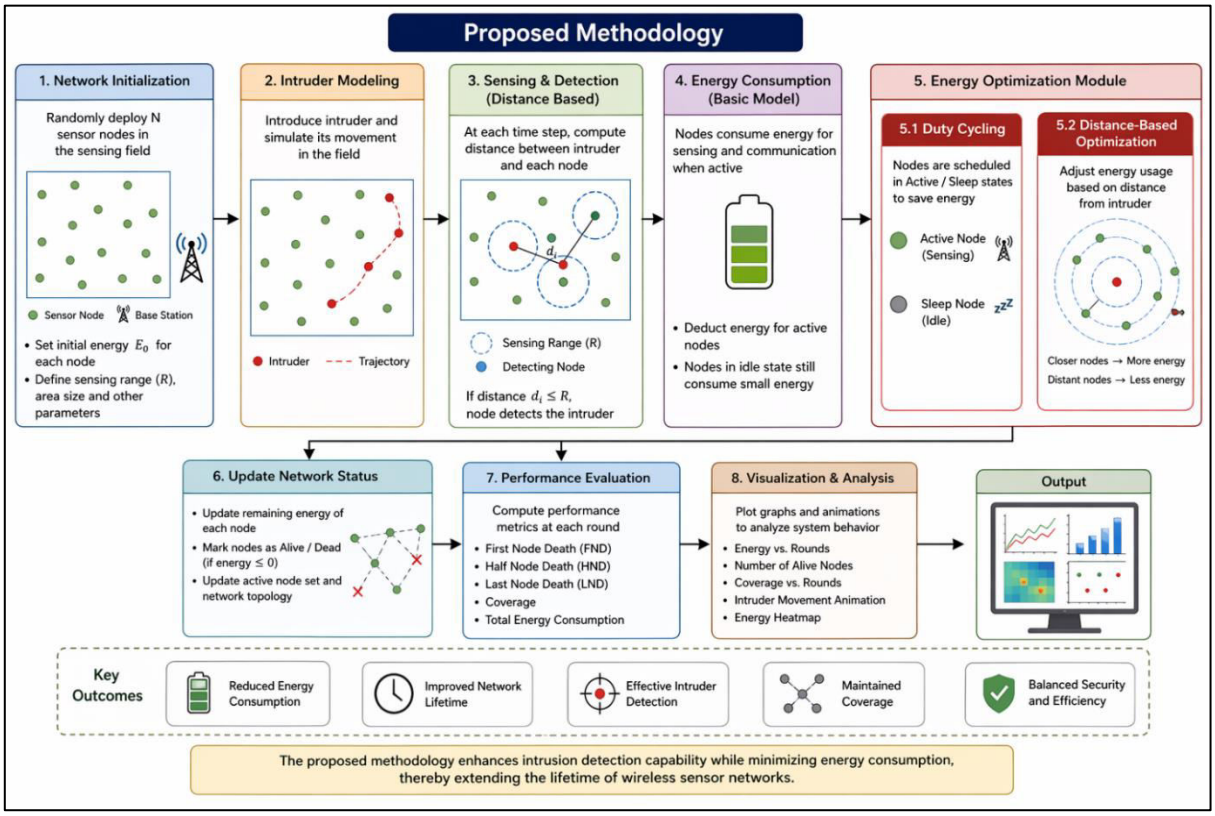


Figure 2: Outline of Methodology

Step 1: Network Initialization

In the network initialization phase, N sensor nodes are randomly deployed in a two-dimensional sensing area of size X×YX \times YX×Y. Each sensor node is assigned an initial energy E_0 and a sensing radius Rs. The position of the i^{th} sensor node is mathematically represented as:

$$S_i = (x_i, y_i), i = 1,2,3, \dots \dots \dots N \qquad (1)$$

where x_i and y_i denote the coordinates of the sensor node in the sensing field. The sensing coverage area of each sensor node is calculated using:

$$A_s = \pi R_S^2 \qquad (2)$$

This stage establishes the sensing environment and network topology required for intrusion monitoring and network operation.

Step 2: Intruder Modeling

In the proposed framework, an intruder is introduced into the sensing field to simulate unauthorized movement within the WSN. The intruder moves dynamically across the network area, enabling the intrusion detection system to evaluate sensing, tracking, and energy-optimization performance under realistic conditions. The position of the intruder at simulation time t is mathematically represented as:

$$I(t) = (x_1(t), y_1(t)) \qquad (3)$$

where $x_1(t)$ and $y_1(t)$ denote the x-coordinate and y-coordinate of the intruder at time t, respectively.

The movement of the intruder is continuously updated using its velocity v and direction θ. The position update equations are given by:

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

$$x_1(t+1) = x_1 + v\cos\theta \qquad (4)$$

$$y_1(t+1) = y_1 + v\sin\theta \qquad (5)$$

where: v represents the speed of the intruder, θ denotes the movement angle or direction, x1, y1 represent the updated coordinates of the intruder at the next simulation step.

The total displacement of the intruder between two consecutive time intervals can be calculated as:

$$D = \sqrt{(x1(t+1) - x1(t))^2 + (y1(t+1) - y1(t))^2} \qquad (6)$$

Step 3: Identification of Intruder Using Distance Measurement

At each simulation round, the proposed framework calculates the Euclidean distance between the intruder and each sensor node to determine whether an intrusion occurs within a node's sensing region of a node. Let the position of the i^{th} sensor node be represented as:

$S_i = (x_i, y_i)$, and the position of the intruder at time t is represented using Equation 3. An intrusion is detected when the calculated distance satisfies the sensing condition:

$$d_i \leq R_s \qquad (7)$$

where Rs represents the sensing radius of the sensor node. If this condition is satisfied, the intruder lies within the sensing coverage area of the node, and the corresponding sensor node becomes an active detection node. The detection status of the i^{th} node can therefore be mathematically represented as:

$$D_i = \begin{cases} 1, d_i \leq R_s \\ 0, \ d_i > R_s \end{cases} \qquad (8)$$

where:

Di =1 indicates successful intrusion detection, and Di =0 indicates no intrusion detection. The total number of active detecting nodes at a given simulation round is calculated as:

$$N_{detect} = \sum_{i=1}^{N} D_i \qquad (9)$$

where N is the total number of deployed sensor nodes. This distance-based intrusion identification mechanism ensures that only nearby nodes actively participate in sensing and communication, thereby reducing unnecessary energy consumption and improving network efficiency.

Step 4: Energy Consumption Model

In the proposed intrusion detection framework, sensor nodes consume energy during sensing, data transmission, data reception, and idle operation. Since wireless sensor nodes operate with limited battery resources, efficient energy management is essential to extend network lifetime and maintain sensing coverage. The residual energy of the i^{th} sensor node at simulation time t+1 is updated based on the total energy consumed during network operations. The energy update equation is expressed as:

$$E_i\ (t+1) = E_i(t) - E_{sense} - E_{tx} - E_{rx} \qquad (10)$$

Where, $E_i(t)$ represents the residual energy of the node at time t, E_{sense} denotes sensing energy consumption, E_{tx} represents transmission energy, and E_{rx} corresponds to reception energy. The transmission energy required to send a packet over a distance d is calculated using:

$$E_{tx} = k(E_{elec} + \in_{amp}\ d^n) \qquad (11)$$

where k is the packet size in bits, Eelec is the electronic circuitry energy, ϵamp represents amplifier energy, and n is the path loss exponent. Similarly, the energy required for receiving data packets is given by:

$$E_{rx} = kE_{elec} \qquad (12)$$

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

Sensor nodes operating in idle or sleep mode consume significantly lower energy, represented as:

$$E_i(t+1) = E_i(t) - E_{idle} \qquad (13)$$

A sensor node is considered dead when its remaining energy reaches zero or becomes negative.

Step 5: Duty Cycle Mechanism

To reduce unnecessary energy consumption and extend the operational lifetime of the WSN, the proposed framework employs a duty-cycle mechanism in which sensor nodes alternate between active and sleep states. In traditional WSN operation, all sensor nodes remain continuously active for sensing and communication, resulting in rapid battery depletion. The duty-cycling approach minimizes this problem by allowing only a subset of nodes to remain active for intrusion monitoring, while the rest remain in low-power sleep mode. This strategy significantly reduces idle listening, redundant sensing, and unnecessary communication overhead. The duty cycle ratio of a sensor node is mathematically defined as:

$$DC = \frac{T_{active}}{T_{active} + T_{sleep}} \qquad (14)$$

where: DC represents the duty cycle ratio, Tactive denotes the active duration of the node, Tsleep denotes the sleep duration of the node. During the active state, sensor nodes perform sensing, intrusion detection, data transmission, and reception tasks, consuming higher energy. In sleep mode, nodes consume only minimal idle energy. The overall energy consumption of a node under duty cycling is calculated as:

$$E_{DC} = DC\ X\ E_{active} + (1 - DC)\ XE_{sleep} \qquad (15)$$

Equation 15 indicates that the total energy consumption depends on the proportion of time the node remains active versus asleep. By reducing the active duration of nodes that are not directly involved in intrusion detection, the duty-cycling mechanism conserves significant energy and extends network lifetime.

Step 6: Distance-Based Optimization

The proposed framework incorporates a distance-based optimization mechanism to improve energy efficiency during intrusion detection in the Wireless Sensor Network (WSN). Instead of allowing all sensor nodes to participate equally in sensing and communication, the framework prioritizes nodes based on their proximity to the intruder. Sensor nodes closer to the intruder become more actively involved in detection and communication, whereas nodes farther away reduce their operational activity and conserve energy. This selective participation minimizes unnecessary energy consumption and helps extend overall network lifetime. Based on this distance, an optimization weight is assigned to each sensor node. Nodes located closer to the intruder have higher optimization weights, while distant nodes receive lower weights. Consequently, nearby nodes are given higher priority for sensing and communication.

Step 7: Update Network Status and Performance Evaluation Metrics

After each simulation round, the proposed framework updates the overall status of the wireless sensor network based on each sensor node's remaining energy and operational condition of each sensor node. During intrusion detection and communication processes, sensor nodes continuously consume energy for sensing, transmitting, and receiving data. As the simulation progresses, some nodes gradually lose their energy and may eventually stop functioning. Therefore, monitoring the status of each node is essential for evaluating network performance and lifetime. In this stage, the framework checks the residual energy of every sensor node to determine whether the node remains alive or becomes dead. Nodes with sufficient remaining energy continue participating in sensing, communication, and intrusion detection activities, whereas nodes with depleted energy are marked as inactive and removed from further network operations. The network topology and sensing coverage are also dynamically updated based on the availability of active nodes. The update process further tracks important network conditions, including the total number of alive nodes, dead nodes, remaining network energy, and sensing coverage, after every simulation round. These updated parameters help analyze how efficiently the proposed duty cycling and distance-based optimization mechanisms conserve energy over time. Additionally, network lifetime metrics, such as First Node Death (FND), Half Node Death (HND), and Last Node Death (LND), are continuously monitored to assess the survivability and sustainability of the wireless sensor network. This stage ensures that the framework maintains accurate network information throughout the simulation and supports effective performance evaluation of the proposed intrusion detection system.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

IV. SIMULATIONS AND OUTPUTS

Table 1: Parameters and their values

Parameter	Description	Value
Number of Nodes (N)	Total sensor nodes in the network	200
Simulation Area	Size of sensing field	100 × 100 units
Simulation Time (Steps)	Total number of iterations	1000
Initial Energy (E_0)	Starting energy of each node	1 Joule (normalized)
Sensing Range (R)	Maximum detection distance	15 units
Node Deployment	Distribution of nodes	Random
Intruder Movement	Path followed by an intruder	Sinusoidal + linear (dynamic)
Basic Energy Consumption	Energy used per detection (basic model)	0.015
Optimized Energy Consumption	Energy used per detection (optimized model)	0.01 + distance factor
Duty Cycle Threshold	Probability of node being active	0.9 (rand > 0.1)

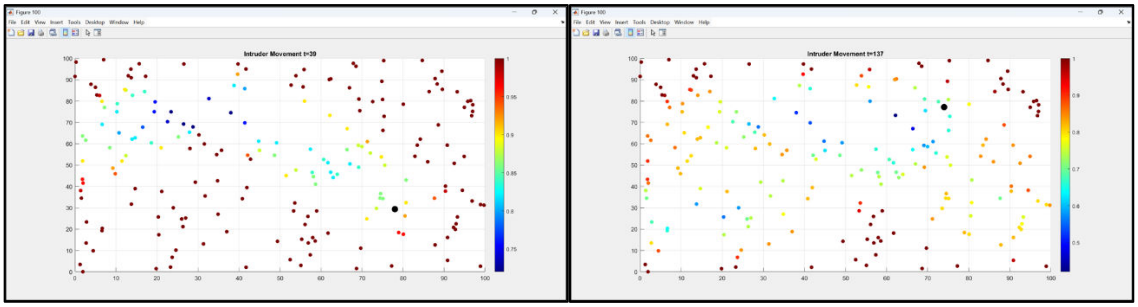


Figure 3(a): Intruder Movement at t=39 3 (b): Intruder Movement at t=137

The figure 3(a) & 3(b) shows a snapshot of the wireless sensor network at time steps t = 39 & t = 137, depicting the interaction between the sensor nodes and the moving intruder. The colored dots in the plot represent the deployed sensor nodes distributed across the sensing field (100 × 100 area). Each node is assigned a color based on its energy level, as indicated by the color bar on the right side. Nodes shown in red/orange have higher remaining energy, while nodes in blue/green have lower energy levels, indicating they have consumed more energy during the detection process. The black circular marker in the figure represents the intruder's current position at that specific time step. As the intruder moves through the network, nearby sensor nodes become active and participate in detection, thereby increasing their energy consumption. It can be observed that nodes closer to the intruder tend to have lower energy (cool colors) because they are actively sensing and communicating, while nodes farther away retain higher energy (warm colors) because they remain inactive or in sleep mode. This behavior reflects the effectiveness of the proposed distance-based energy-optimization and duty-cycling mechanism.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

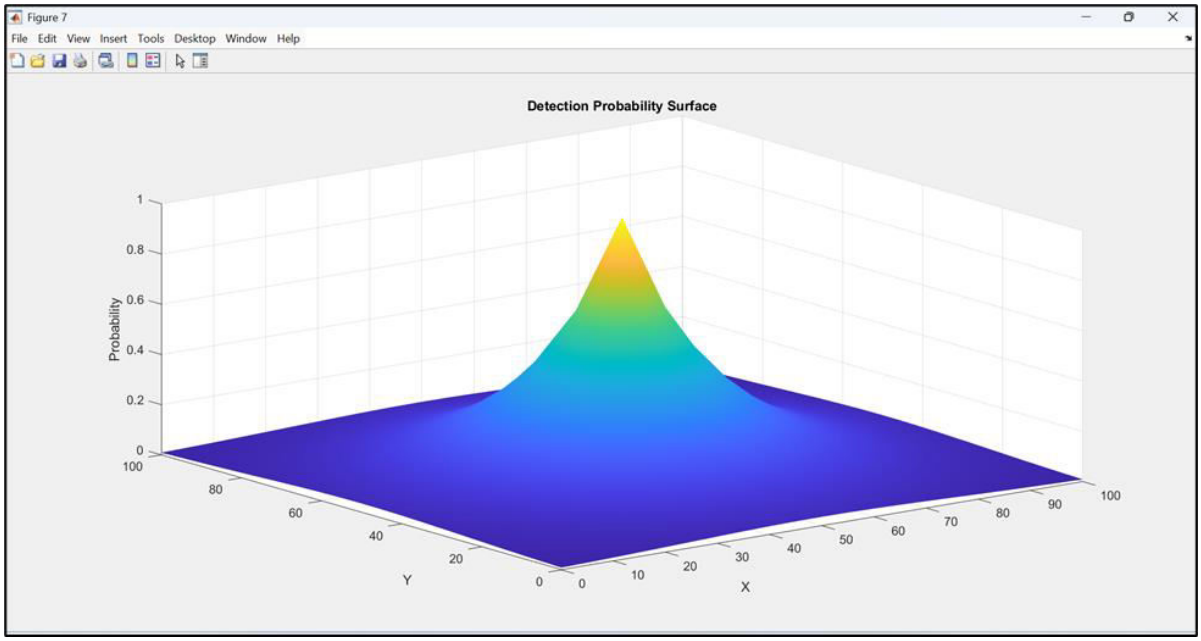


Figure 4: Detection Probability Surface

Figure 4 shows the Detection Probability Surface of the proposed intrusion detection framework in the wireless sensor network. The X and Y axes represent the sensing field coordinates, while the Z-axis represents the probability of intrusion detection. The detection probability is highest near the center region, where sensor coverage is strongest, and gradually decreases toward the outer regions as the distance from active sensing nodes increases. This demonstrates that the proposed distance-based detection mechanism provides more reliable intrusion detection in areas with stronger sensor participation while efficiently optimizing network energy usage.

Figure 5 presents the Energy Level Comparison between the network operating with optimization and without optimization over simulation time. The red curve represents the network without optimization, while the blue curve represents the proposed optimized framework using duty cycling and distance-based optimization. It can be observed that the energy of the non-optimized network decreases rapidly due to continuous sensing and communication by all sensor nodes. In contrast, the optimized model preserves higher average energy throughout the simulation by reducing unnecessary node activity and efficiently managing energy consumption. This demonstrates that the proposed optimization techniques significantly improve energy efficiency and help extend the overall lifetime of the wireless sensor network.

Figure 6 illustrates the Network Lifetime Comparison between the optimized and non-optimized wireless sensor network models. The X-axis represents simulation time, while the Y-axis shows the number of alive sensor nodes remaining in the network. The red curve shows the network without optimization, where sensor nodes die rapidly due to higher energy consumption from continuous sensing and communication. In contrast, the blue curve represents the proposed optimized framework, where duty cycling and distance-based optimization significantly slow node energy depletion, allowing more nodes to remain alive for longer. This result demonstrates that the proposed optimization techniques effectively improve network lifetime and enhance the sustainability of the wireless sensor network.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

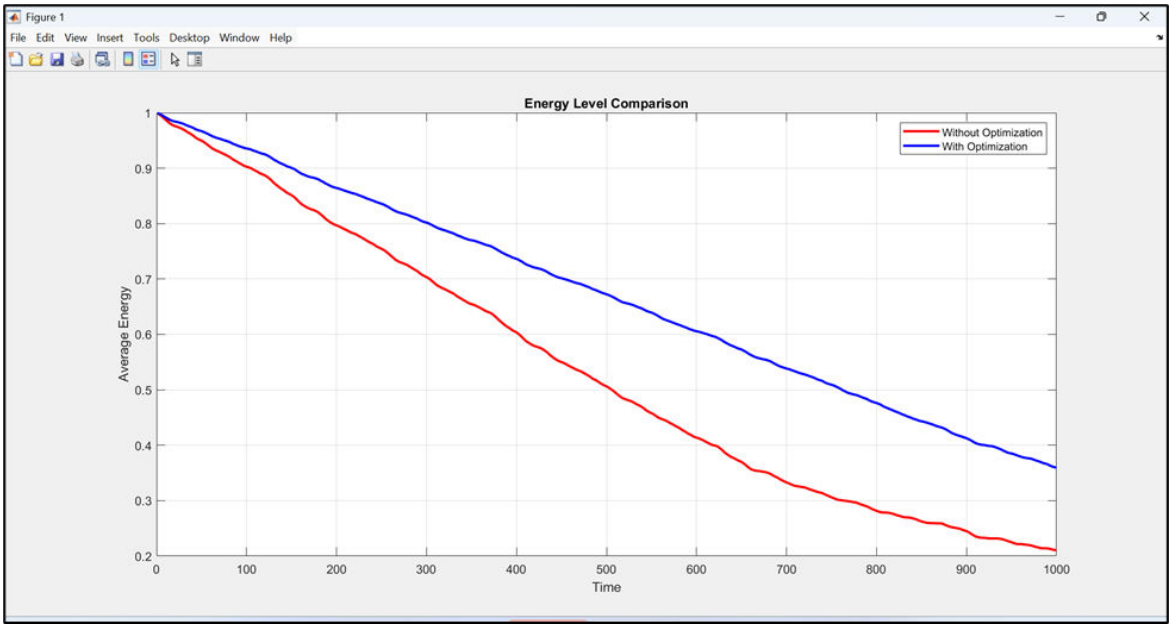


Figure 5: Comparison of Energy Levels

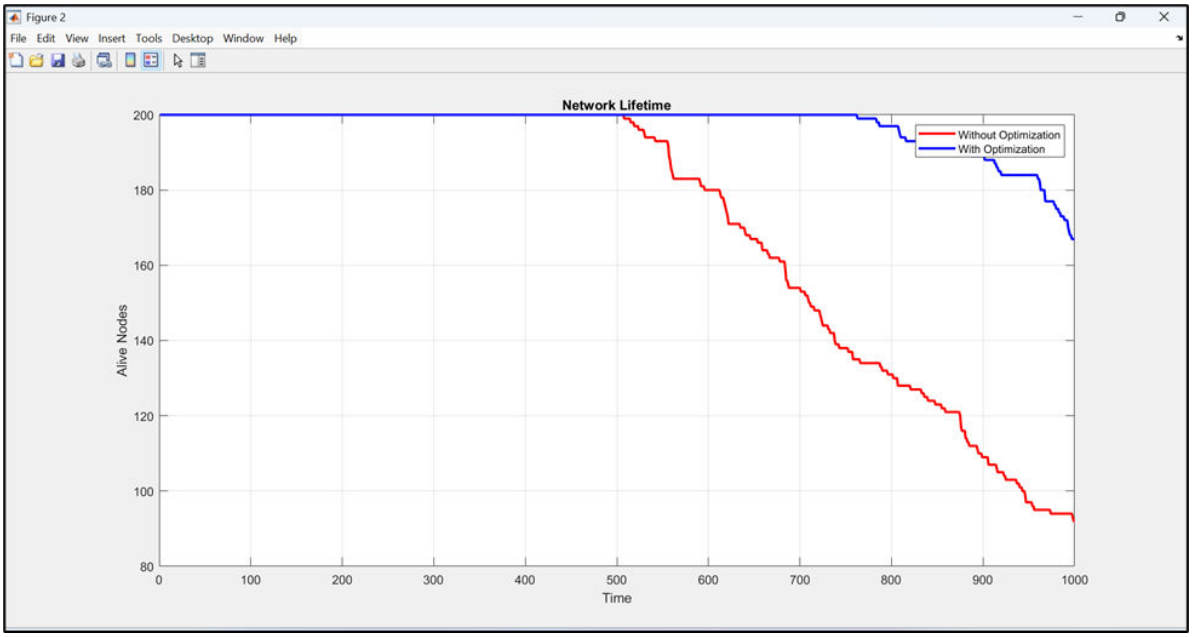


Figure 6: Network Lifetime

Figure 7 presents the Coverage Comparison between the optimized and non-optimized wireless sensor network models over simulation time. The X-axis represents time, while the Y-axis indicates the network coverage achieved during intrusion monitoring. The red curve corresponds to the network without optimization, where coverage gradually decreases and becomes unstable as sensor nodes lose energy and die more rapidly. In contrast, the blue curve represents the proposed optimized framework, which maintains higher, more consistent coverage throughout the simulation through the implementation of duty cycling and distance-based optimization. By conserving node energy and reducing unnecessary sensing activity, the optimized model extends active sensor participation, thereby improving sensing coverage and overall network reliability.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

| DOI:10.15662/IJAREEIE.2026.1505008 |

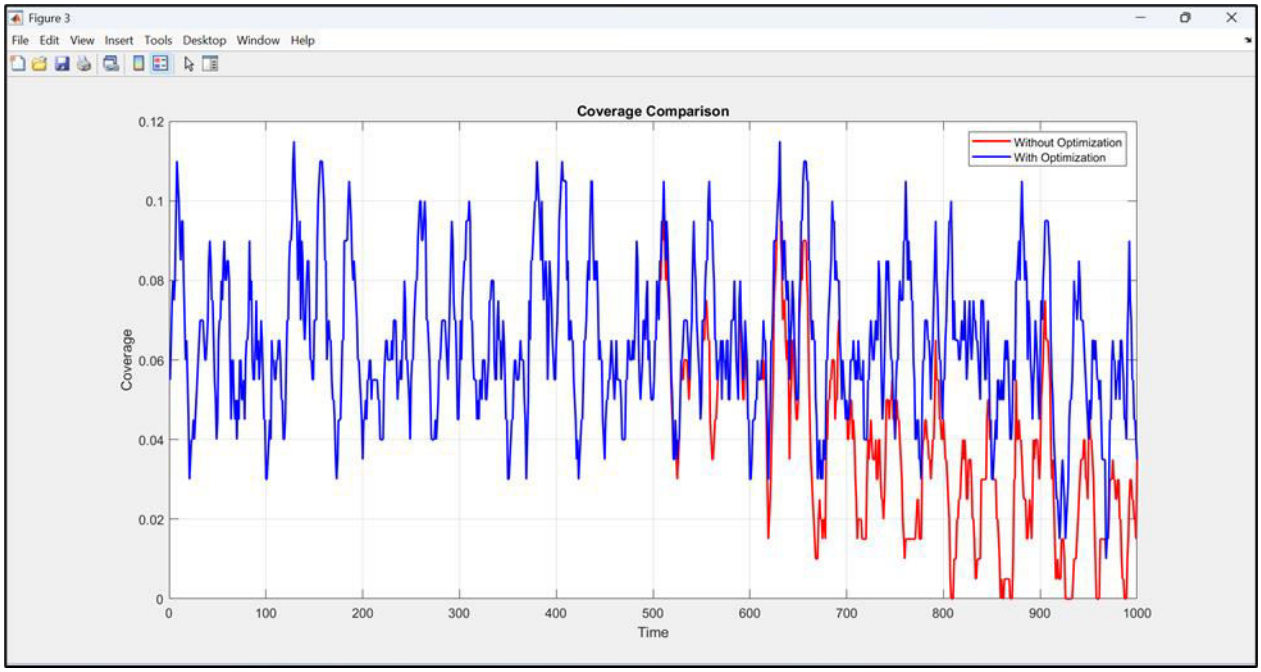


Figure 7: Coverage Comparison

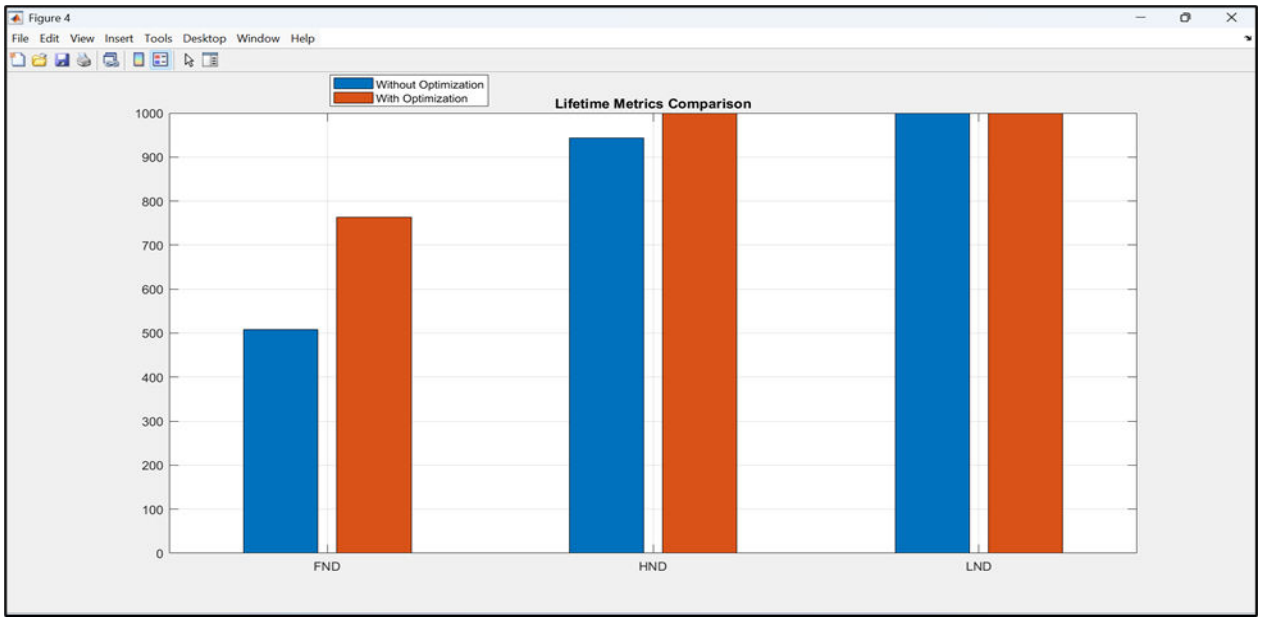


Figure 8: Lifetimes Metrics (FND, HND, and LND) Comparison

Figure 8 shows the Lifetime Metrics Comparison between the optimized and non-optimized wireless sensor network models using three important network lifetime parameters: First Node Death (FND), Half Node Death (HND), and Last Node Death (LND). The bars indicate that the proposed optimized framework achieves significantly better network lifetime performance compared to the non-optimized model. In the optimized approach, the first sensor node dies much later, demonstrating improved energy conservation during early network operation. Similarly, the Half Node Death point is delayed, indicating that a larger number of sensor nodes remain operational for a longer period. The Last Node Death metric also reaches the maximum simulation duration, showing that the optimized framework successfully prolongs the overall network lifetime. These improvements are achieved through the implementation of duty cycling and distance-based optimization, which reduce unnecessary energy consumption and balance node activity efficiently across the network

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 9.867 | A Monthly Peer Reviewed & Refereed Journal |

|| Volume 15, Issue 5, May 2026 ||

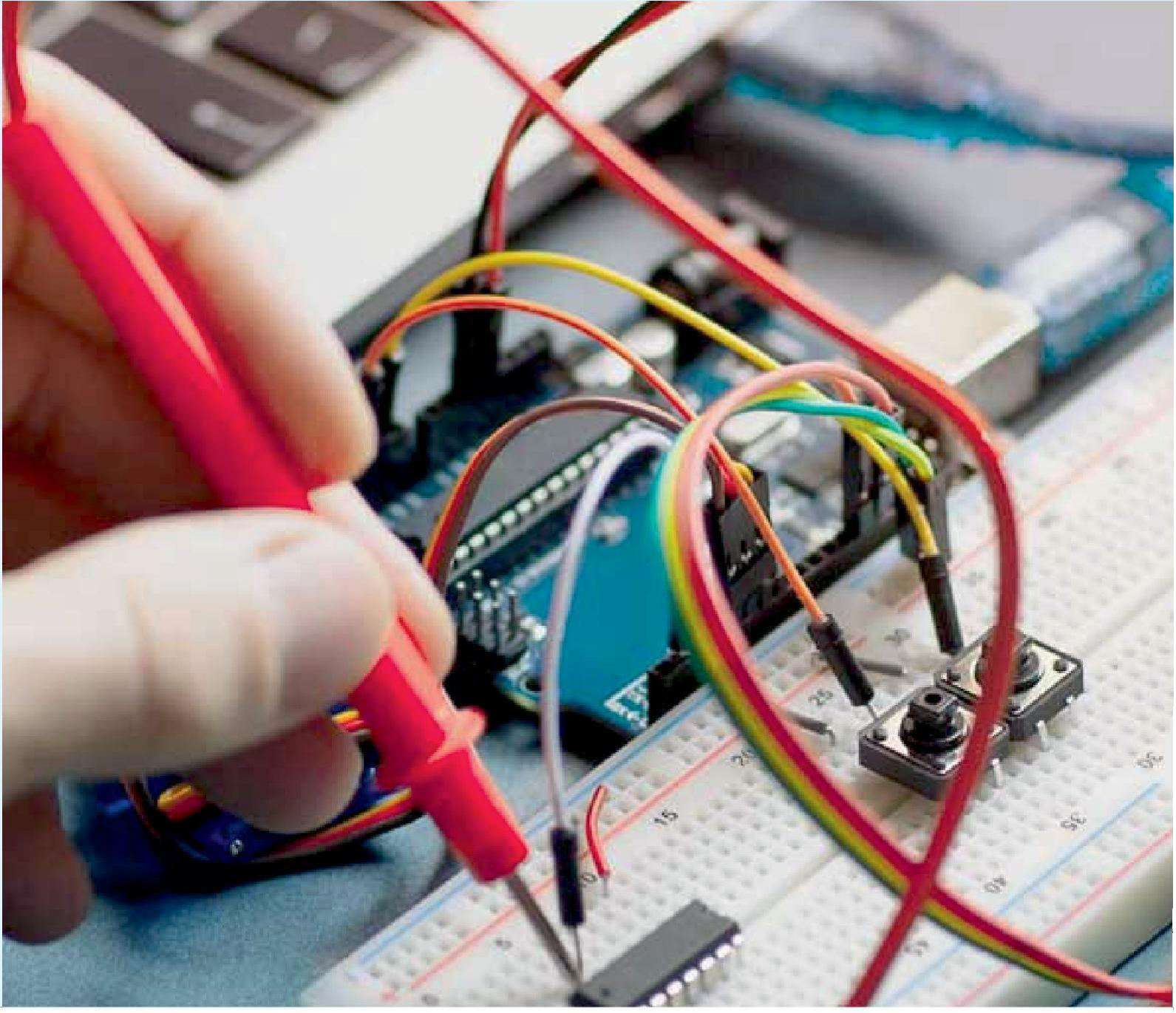
| DOI:10.15662/IJAREEIE.2026.1505008 |

V. CONCLUSION

This paper presented a distance-aware and duty-cycle-based intrusion detection framework for wireless sensor networks (WSNs) aimed at improving energy efficiency while maintaining reliable intrusion detection performance. The proposed methodology incorporated random sensor node deployment, dynamic intruder movement simulation, distance-based intrusion detection, energy consumption modeling, duty cycling, and distance-based optimization techniques to reduce unnecessary energy usage in the network. By allowing only nearby sensor nodes to actively participate in intrusion detection while scheduling distant or inactive nodes into sleep mode, the framework effectively minimized redundant sensing and communication overhead. The proposed system was implemented and evaluated through MATLAB simulation using multiple performance metrics, including average energy consumption, network lifetime, sensing coverage, alive node statistics, and detection probability. Simulation results demonstrated that the optimized framework significantly outperformed the non-optimized model in terms of energy conservation and network sustainability. The energy level comparison showed slower energy depletion in the optimized network, while lifetime analysis confirmed delayed node deaths and prolonged network operation. Similarly, the coverage comparison indicated that the proposed optimization techniques maintained more stable sensing coverage throughout the simulation period.

REFERENCES

[1] Gupta, S., Arora, M., Sharma, R. (2025). Achieving full coverage in wireless sensor networks through optimization techniques, *Journal of Engineering, Mechanics and Modern Architecture*, 4(6), pp. 47-54.
[2] Malik, S., Arora, M., Sharma, R. (2025). Comprehensive Guide to Different Types of Attacks on Email Systems, *Information Horizons: AMERICAN Journal of LibraryAnd Information Science Innovation,* 2(6).
[3] Gupta, S. and Arora, M., 2025. Balancing Coverage and Clustering in Mobile WSNs: An Optimization-Based Approach. *International Journal of Computer Technology and Electronics Communication*, *8*(1), pp.10062-10068.
[4] Pinki, Dalal, S., Sharma, R., Sumiran, Communication Protocols for Wireless Sensor Networks (WSNs): A Comprehensive Review, *International Journal of Research Publication and Reviews*, 5(4), pp. 3929-3933.
[5] R. S., Gopal Sharma, Sumit Dalal, "Sleep-Awake and ACO based Resource Saving Protocol for WSN," Int. J. Innov. Res. Comput. Commun. Eng., vol. 11, no. 6, pp. 8456–8462, 2023.
[6] S. Kim and J.-Y. Lee, "A system architecture for high-speed deep packet inspection in signature-based network intrusion prevention," J. Syst. Archit., vol. 53, no. 5–6, pp. 310–320, 2007.
[7] Z. Trabelsi and R. Mahdy, "An anomaly intrusion detection system employing associative string processor," in Proc. Int. Conf. Netw., 2010, pp. 220–225.
[8] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid intrusion detection with weighted signature generation over anomalous internet episodes," IEEE Trans. Dependable Secure Comput., vol. 4, no. 1, pp. 41–55, Jan.-Mar. 2007.
[9] L. Khan, M. Awad, and B. Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering," Int. J. Very Large Data Bases, vol. 16, no. 4, pp. 507–521, 2007.
[10] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," Expert Syst. Appl., vol. 36, no. 10, pp. 11994–12000, 2009.
[11] Z. Trabelsi and R. Mahdy, "An anomaly intrusion detection system employing associative string processor," in Proc. Int. Conf. Netw., 2010, pp. 220–225.
[12] M. Papadonikolakis and C. Bouganis, "A novel FPGA-based SVM classifier," in Proc. Field-Programmable Technol., 2010, pp. 283–286.
[13] A. Das, D. Nguyen, J. Zambreno, G. Memik, and A. Choudhary, "An FPGA-based network intrusion detection architecture," IEEE Trans. Inform. Forensics Security, vol. 3, no. 1, pp. 118–132, Mar. 2008.
[14] M. Papadonikolakis and C.-S. Bouganis, "Novel cascade FPGA accelerator for support vector machines classification," IEEE Trans. Neural Netw. Learn. Syst., vol. 23, no. 7, pp. 1040–1052, Jul. 2012.
[15] I. Corona, G. Giacinto, and F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues," Inf. Sci., vol. 239, pp. 201–225 Aug. 2013.
[16] R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cunningham, and M. A. Zissman, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," in Proc. DARPA Inform. Survivability Conf. Expo., 2000, pp. 12–26.
[17] P. Kabiri and A. A. Ghorbani, "Research on intrusion detection and response: A survey," Int. J. Netw. Security, vol. 1, no. 2, pp. 84–102, 2005.
[18] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security Privacy, 2010, pp. 305–316.



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details