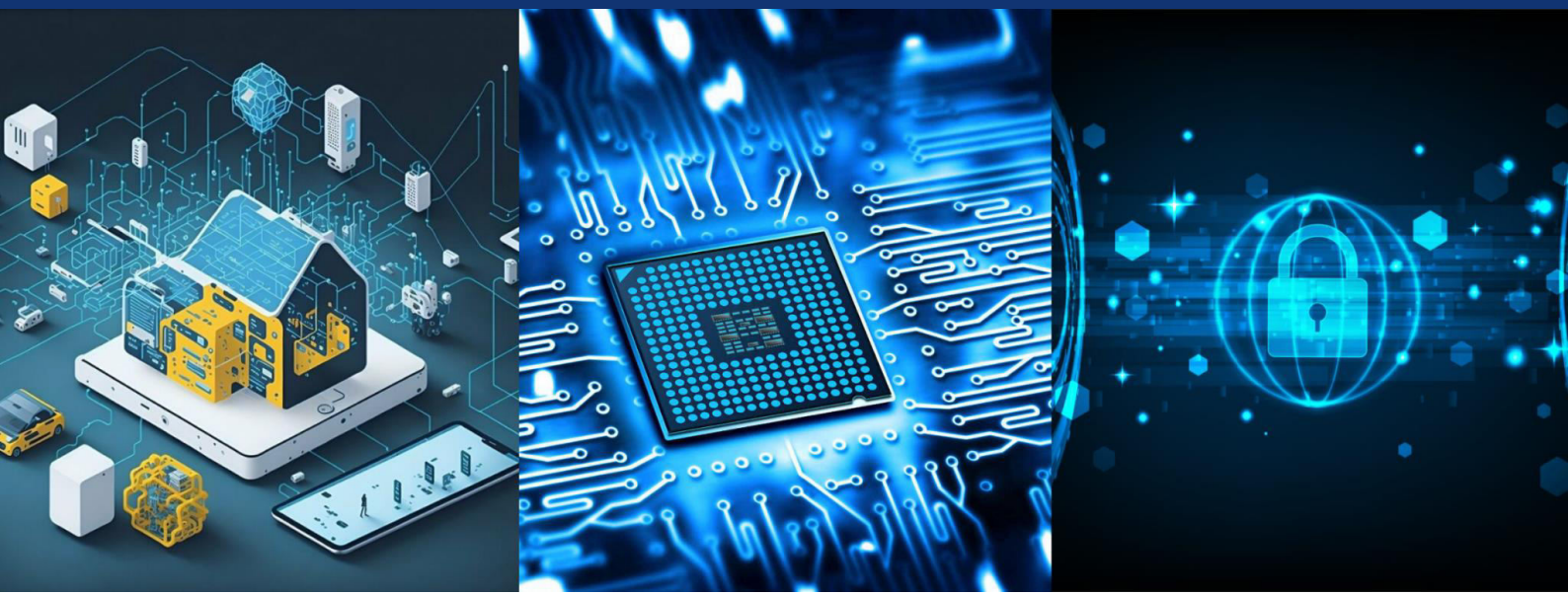
IJIRCCE

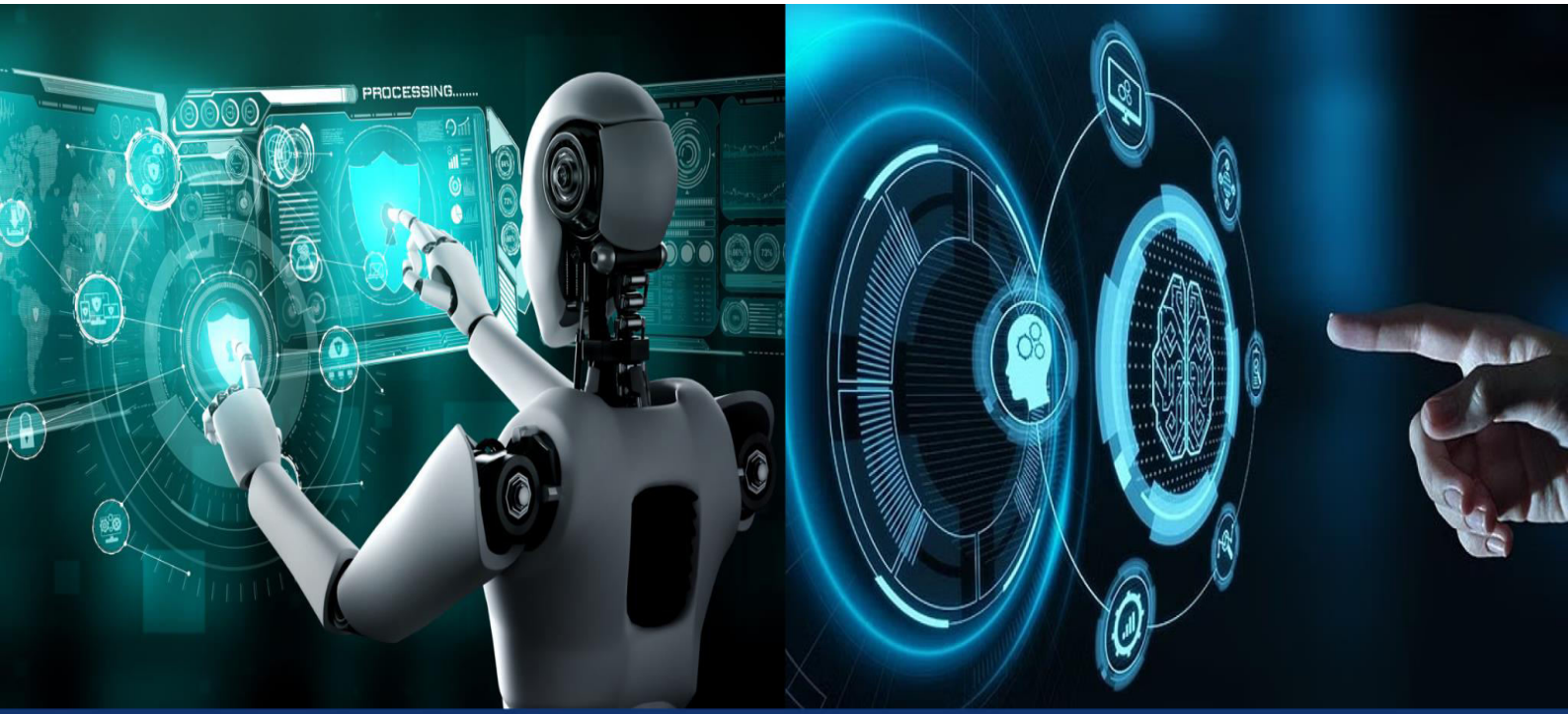
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

An Energy-Efficient Trust-Based Framework for Malicious Node Detection in Wireless Sensor Networks

Chander Shekhar[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 highly vulnerable to malicious node attacks due to their distributed architecture, wireless communication, and limited energy resources. Malicious nodes can disrupt packet transmission, reduce network reliability, and degrade overall communication performance. To address these challenges, this paper presents an energy-efficient trust-based framework for detecting malicious nodes in WSN. The proposed model evaluates sensor node behavior using dynamic trust computation based on packet forwarding behavior, residual energy, and communication reliability. Sensor nodes with trust values below a predefined threshold are identified as malicious and isolated from network communication. Simulation results demonstrate that the proposed trust-aware approach improves network performance and security compared to the non-trust model. Furthermore, the trust-based mechanism maintained better packet delivery performance and reduced the participation of malicious nodes during communication. The results confirm that integrating dynamic trust evaluation with energy-aware communication significantly enhances malicious node detection capability while maintaining efficient resource utilization in WSN environments. The proposed framework provides a reliable and scalable solution for secure wireless sensor network applications, including environmental monitoring, military surveillance, healthcare systems, and IoT-based smart infrastructure.

KEYWORDS: Trust-Based Security, Malicious Node Detection, Trust Management, Intrusion Detection

I. INTRODUCTION

Numerous sensor nodes that work together to sense, process, and transmit data via wireless communication make up a WSN. WSNs are highly susceptible to security risks and malicious node attacks due of their distributed architecture, open wireless medium, and constrained computing and energy resources. Malicious nodes can intentionally drop packets, modify transmitted data, interfere with routing, and degrade the network's overall reliability and performance of the network. As a result, developing safe and effective malicious node detection techniques has emerged as a significant research challenge in wireless sensor networks.

Several researchers have proposed trust-aware security mechanisms to improve malicious node detection in WSNs. Zawaideh and Salamah [1] introduced an efficient, trust-based, weighted scheme for malicious node detection that evaluates node behavior using multiple trust parameters to accurately identify suspicious nodes. Their work demonstrated that weighted trust evaluation can improve secure communication and reduce the impact of compromised nodes in wireless sensor environments. Similarly, Wang et al. [2] proposed a dynamic trust management approach for detecting malicious nodes in wireless weak-link sensor networks. Their model continuously updates trust values based on node behavior and communication reliability, enabling adaptive, real-time detection of malicious activity.

Fuzzy logic techniques have also been applied for trust evaluation in WSN security. Ram Prabha and Latha [3] developed a fuzzy trust protocol for malicious node detection that combines fuzzy inference mechanisms with trust management to handle uncertain and dynamic network conditions. Their approach improved malicious node identification accuracy while reducing false detection rates. In addition, Bao et al. [4] proposed a trust-based intrusion

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

detection framework for WSNs that evaluates sensor node interactions and communication behavior to detect intrusions effectively. Their work highlighted the importance of integrating trust computation with intrusion detection for improving network security and reliability. Recent studies have further emphasized the importance of evaluating trust management frameworks in WSNs. Gangwani et al. [5] analyzed various trust management approaches and discussed their effectiveness in improving secure communication, isolating malicious nodes, and enhancing network survivability. Their study indicated that adaptive trust-based mechanisms provide better scalability and security performance in dynamic sensor network environments. Geetha and Chandrasekaran [6] proposed a distributed trust-based secure communication framework that enables cooperative trust evaluation among sensor nodes to ensure secure data transmission and reliable routing. Their framework demonstrated improved resistance against malicious attacks while maintaining communication efficiency.

Apart from security, maintaining sensing coverage and energy efficiency is also critical in WSNs, as sensor nodes operate with limited battery power. Gupta et al. [7] discussed optimization techniques for achieving full coverage in wireless sensor networks while minimizing energy consumption. Their work highlighted that efficient resource management and optimization strategies are essential for extending network lifetime and maintaining reliable network operation. Motivated by these research contributions, this work presents an energy-efficient trust-based framework for malicious node detection in Wireless Sensor Networks. The proposed model integrates dynamic trust evaluation, packet-forwarding analysis, communication reliability assessment, and energy-aware communication to identify malicious nodes and enhance secure routing. The framework also evaluates network performance using metrics such as residual energy, packet delivery ratio, detection accuracy, and network lifetime. The objective of the proposed work is to enhance network security while maintaining efficient resource utilization and reliable communication in WSN environments.

II. RESEARCH BACKGROUND

Due to their applications in environmental sensing, healthcare, military surveillance, industrial automation, and smart city infrastructures, WSNs have emerged as a crucial technology for contemporary communication and monitoring systems. However, because WSNs are wireless and distributed, they are extremely susceptible to a range of security risks, including denial-of-service attacks, packet dropping, malicious node attacks, data injection, and routing manipulation. Communication dependability, network longevity, sensing coverage, and overall system performance are all greatly impacted by these security issues. To strengthen WSNs' resistance to malicious activity, researchers have focused on developing trust-aware, energy-efficient, and secure communication protocols.

Understanding different attack strategies is important for designing secure WSN architectures. Malik et al. [8] discussed various types of attacks in communication systems and highlighted how malicious activities can compromise data integrity, confidentiality, and network reliability. Although their study focused on email system attacks, the concepts of unauthorized access, spoofing, and malicious behavior are also relevant to wireless sensor network security, where compromised nodes may disrupt communication and manipulate transmitted information. Network optimization techniques also play a critical role in improving WSN performance and security. Gupta and Arora [9] proposed an optimization-based approach for balancing coverage and clustering in mobile WSNs. Their work emphasized that efficient clustering and coverage management can improve network connectivity, reduce energy consumption, and maintain reliable communication. Similarly, Pinki et al. [10] reviewed various communication protocols used in WSNs and discussed their impact on routing efficiency, scalability, energy utilization, and network reliability. Their study highlighted the importance of selecting appropriate communication protocols for secure, efficient operation of wireless sensor networks.

Energy conservation remains one of the major challenges in WSNs because sensor nodes are typically powered by limited battery resources. To address this issue, Sharma et al. [11] proposed a sleep-awake and Ant Colony Optimization (ACO)-based resource-saving protocol for WSNs. Their approach reduced unnecessary energy consumption by dynamically controlling node activity and optimizing routing behavior, thereby extending network lifetime and improving energy efficiency. Recently, trust-based security frameworks have gained significant attention for malicious node detection in WSNs. She et al. [12] introduced a blockchain trust model for malicious node detection in wireless sensor networks. Their framework used blockchain technology to maintain secure, tamper-resistant trust information, improving detection reliability and network security against compromised nodes. Zhang et al. [13]

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

proposed a trust-based framework for secure data aggregation in WSNs, integrating trust evaluation into the aggregation process to prevent false data injection and enhance communication integrity.

Multiple-level trust management approaches have also been explored to improve the accuracy of trust evaluation. Zhang et al. [14] developed a multi-level trust management framework that considers various trust parameters, such as communication behavior, node reliability, and interaction history, to identify malicious nodes more effectively. Their work demonstrated that combining multiple trust metrics can significantly improve intrusion detection performance and reduce false-positive rates. More recently, adaptive trust systems have been proposed for dynamic and real-time malicious node detection. Saidi [15] introduced an adaptive trust system for misbehavior detection in WSNs, in which trust values are continuously updated based on node behavior and network conditions. The study showed that adaptive trust mechanisms can effectively detect malicious activities while maintaining network scalability, reliability, and communication efficiency.

Overall, previous studies demonstrate that trust management, blockchain security, energy-efficient routing, optimization techniques, and adaptive detection mechanisms play an important role in improving secure communication and detecting malicious nodes in Wireless Sensor Networks. However, challenges such as balancing security with energy efficiency, reducing computational overhead, maintaining sensing coverage, and improving real-time malicious node detection still remain open research issues. These challenges motivate the development of intelligent, trust-aware, and energy-efficient frameworks for secure WSN communication and malicious node detection.

III. PROPOSED METHODOLOGY

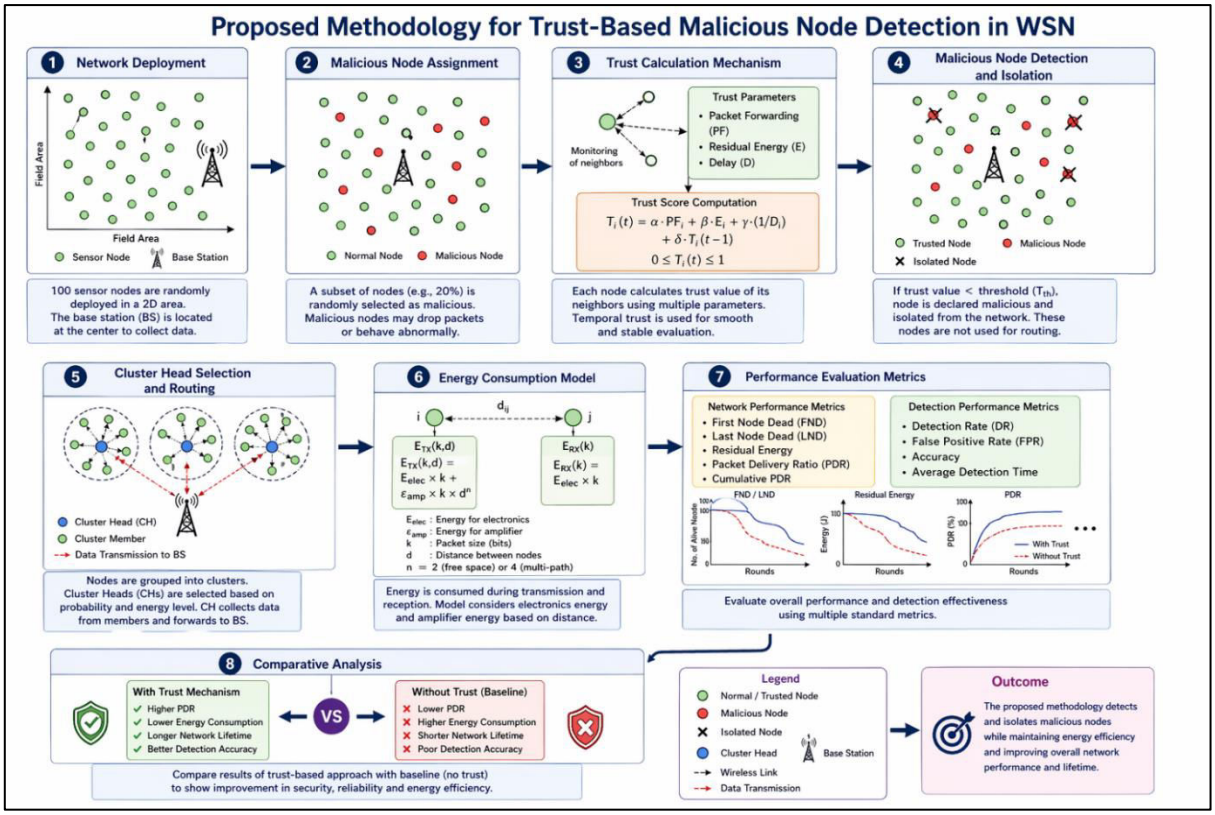


Figure 1: Outline of Proposed Methodology

Step 1: Network Deployment: In the first stage of the proposed methodology, a WSN is deployed randomly within a predefined two-dimensional sensing area. A fixed number of sensor nodes are distributed across the network field to monitor communication activities and environmental conditions. Each node is initialized with equal energy and is capable of sensing, transmitting, and receiving data packets. A base station or sink node is positioned at a specific

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

location to collect network information and coordinate communication. This deployment stage establishes the network topology, communication environment, and sensing coverage required for malicious node detection and secure data transmission. Each sensor node is assigned an initial energy value E_0 and is capable of sensing, transmitting, and receiving data packets. The position of the ith sensor node is represented as:$S_i = (xi_i, y_i)$.

Step 2: Malicious Node Assignment: After network deployment, a subset of sensor nodes is randomly selected and designated as malicious nodes. These nodes exhibit abnormal behavior, dropping packets, modifying transmitted data, delaying communication, or disrupting routing operations. The malicious node assignment stage is essential for simulating realistic attack scenarios within the WSN environment. By introducing malicious behavior into the network, the proposed framework can evaluate the effectiveness of the trust mechanism in identifying compromised nodes and maintaining secure communication. Let the total number of deployed sensor nodes be N, and let the ratio of malicious nodes be α. The total number of malicious nodes is calculated as: $N_m = \alpha\ X\ N$. A node is classified as malicious when its communication behavior deviates significantly from normal network behavior. The malicious behavior condition can be expressed as:

$$Node_i = \begin{cases} Normal, PF_i \geq \beta \\ Malicious, PF_i < \beta \end{cases} \quad (1)$$

Where PFi is the packet forwarding behaviour. For normal nodes PF is approximately equal to 1. However, malicious nodes intentionally reduce forwarding performance.

Step 3: Trust Calculation Mechanism: In this stage, each sensor node calculates trust values for its neighbors based on multiple trust evaluation parameters, such as packet-forwarding behavior, residual energy, communication reliability, and transmission delay. Nodes that consistently cooperate and forward packets correctly receive higher trust values, whereas suspicious nodes receive lower trust scores. The trust calculation mechanism continuously updates trust information over time to reflect real-time node behavior. This dynamic trust evaluation enables the framework to distinguish between trusted and malicious nodes efficiently while adapting to changing network conditions. Nodes that consistently cooperate and forward packets correctly receive higher trust values, whereas nodes showing abnormal or suspicious activities receive lower trust scores.

Step 4: Malicious Node Detection and Isolation: The calculated trust values are compared with a predefined trust threshold to identify malicious nodes within the network. Sensor nodes with trust values below the threshold are classified as malicious or compromised. Once detected, these nodes are isolated from communication and routing operations to prevent them from participating in data transmission. The isolation process reduces the impact of malicious activities such as packet dropping, false data injection, and routing disruption. This stage significantly improves network security, communication reliability, and resistance to intrusions**.**

Step 5: Cluster Head Selection and Routing: To improve communication efficiency and reduce energy consumption, the sensor nodes are grouped into clusters. A Cluster Head (CH) is selected within each cluster based on factors such as residual energy, trust value, and communication capability. The cluster head collects data from cluster members, performs aggregation if required, and forwards the information to the base station. Trust-aware routing ensures that data transmission paths avoid malicious nodes and utilize secure communication links. This clustering approach reduces communication overhead and improves network scalability.

Step 6: Multi-Hop Routing: In large-scale WSN environments, direct communication between cluster heads and the base station may consume excessive energy due to long transmission distances. Therefore, the proposed framework uses multi-hop routing, in which data packets are forwarded through intermediate trusted nodes before reaching the sink node. Multi-hop communication reduces energy consumption in transmission and improves routing efficiency. Trust-aware multi-hop routing further ensures that only reliable and secure nodes participate in packet forwarding, thereby minimizing the chances of malicious interference during communication.

Step 7: Energy Consumption Model: The energy consumption model evaluates the energy used by sensor nodes during sensing, transmission, reception, routing, and trust computation. Sensor nodes consume more energy during active communication and less during idle operation. The proposed framework monitors residual node energy continuously to analyze energy depletion and network lifetime. Energy-efficient communication and trust-aware routing help minimize unnecessary energy consumption and prolong the operational lifetime of the wireless sensor network.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

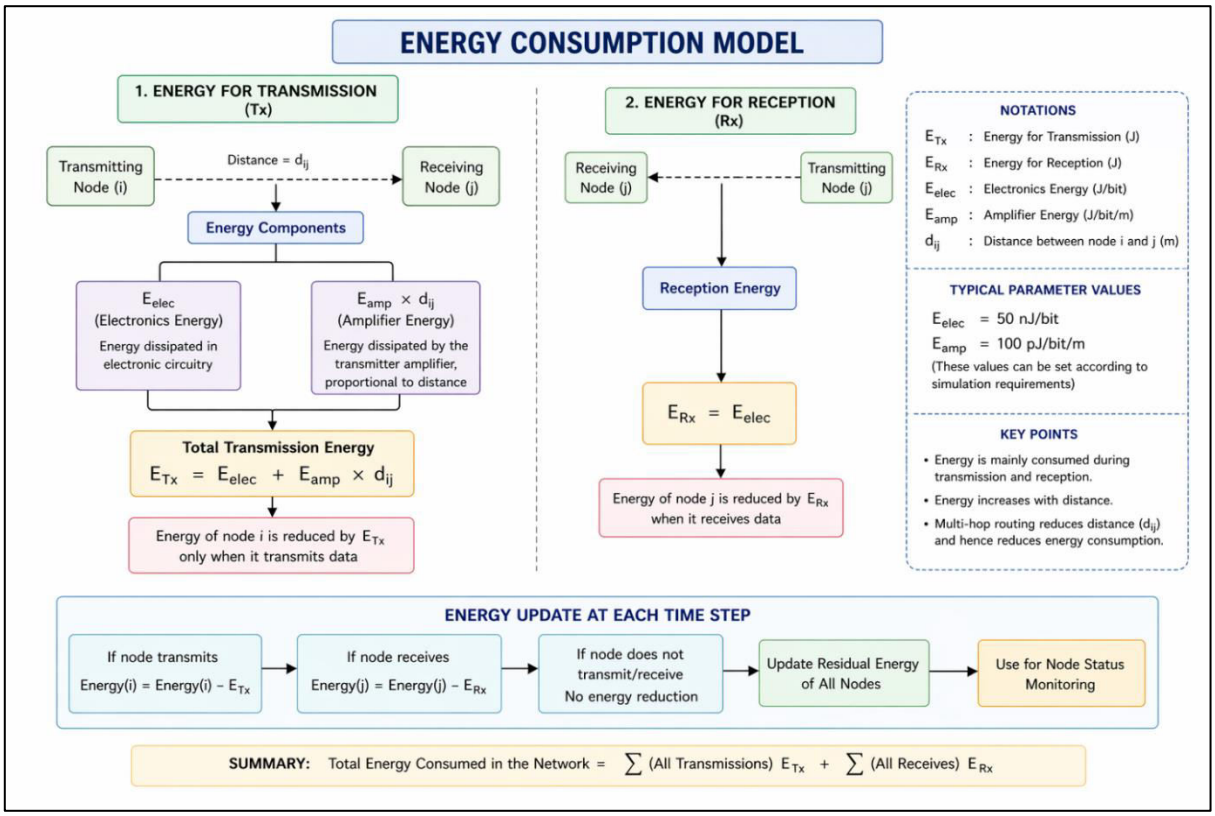


Figure 2: Energy Consumption Model

Step 8: Simulation: The proposed malicious node detection framework is implemented and simulated using MATLAB 2024a. During simulation, sensor nodes communicate dynamically while malicious nodes perform abnormal activities within the network. Trust values are continuously updated, cluster heads are selected, routing paths are established, and network behavior is analyzed over multiple communication rounds. Simulation enables the evaluation of detection performance, routing efficiency, energy consumption, and overall network reliability under different network conditions and attack scenarios.

Step 9: Performance Evaluation Metrics: Several performance metrics are used to evaluate the effectiveness of the proposed framework. These include Detection Rate (DR), False Positive Rate (FPR), Packet Delivery Ratio (PDR), residual energy, network lifetime, First Node Death (FND), Last Node Death (LND), and detection accuracy. These metrics help analyze how efficiently the framework identifies malicious nodes, preserves energy, maintains communication reliability, and improves network survivability. Performance evaluation provides quantitative evidence of the advantages of the trust-based security mechanism.

Step 10: Comparative Analysis: Finally, a comparative analysis is performed between the proposed trust-based framework and a baseline system without trust management. The comparison examines differences in malicious node detection capability, packet delivery performance, residual energy, network lifetime, and communication reliability. Simulation results demonstrate that the trust-aware approach provides better security, lower malicious node participation, improved packet delivery ratio, and enhanced energy efficiency compared to the non-trust model. This analysis validates the effectiveness of the proposed methodology for the secure and reliable operation of a Wireless Sensor Network.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 1: Parameters and their values

Parameter	Symbol	Value Used	Description
Number of Nodes	(N)	100	Total sensor nodes deployed in the network
Network Area	(A)	(100 \times 100) m²	Size of the sensing field
Number of Rounds	(R)	200	Total simulation iterations
Initial Energy	(E_0)	1.2 J	Initial energy assigned to each node
Base Station Position	BS	(50, 50)	Central data collection point
Cluster Head Probability	(P_{CH})	0.07	Probability of a node becoming cluster head
Packet Size	(k)	3000 bits	Size of transmitted data packet
Electronics Energy	(E_{elec})	(50 \times 10^{-8}) J/bit	Energy for transmission/reception circuitry
Amplification Energy	(E_{amp})	(50 \times 10^{-10}) J/bit/m²	Energy for signal amplification
Trust Threshold	(T_{th})	0.42	Threshold for classifying nodes as malicious
Trust Weight (Previous)	(w_1)	0.85	Weight for previous trust value
Trust Weight (Current)	(w_2)	0.15	Weight for current behavior
Malicious Node Ratio	(M_r)	20%	Percentage of nodes acting maliciously
Packet Forwarding (Normal)	PF	~0.9	Probability of forwarding packets (normal node)
Packet Forwarding (Malicious)	PF	0.4–0.8	Reduced forwarding probability (malicious node)
Baseline Energy Drain	—	0.00005 J	Energy consumed per round for operation
Malicious Energy Penalty	—	0.001 J	Extra energy drain for malicious behavior
Cluster Head Energy Drain	—	0.00004 J	Additional energy for CH processing
Detection Start Round	—	15	Minimum rounds before detection begins

OUTCOMES

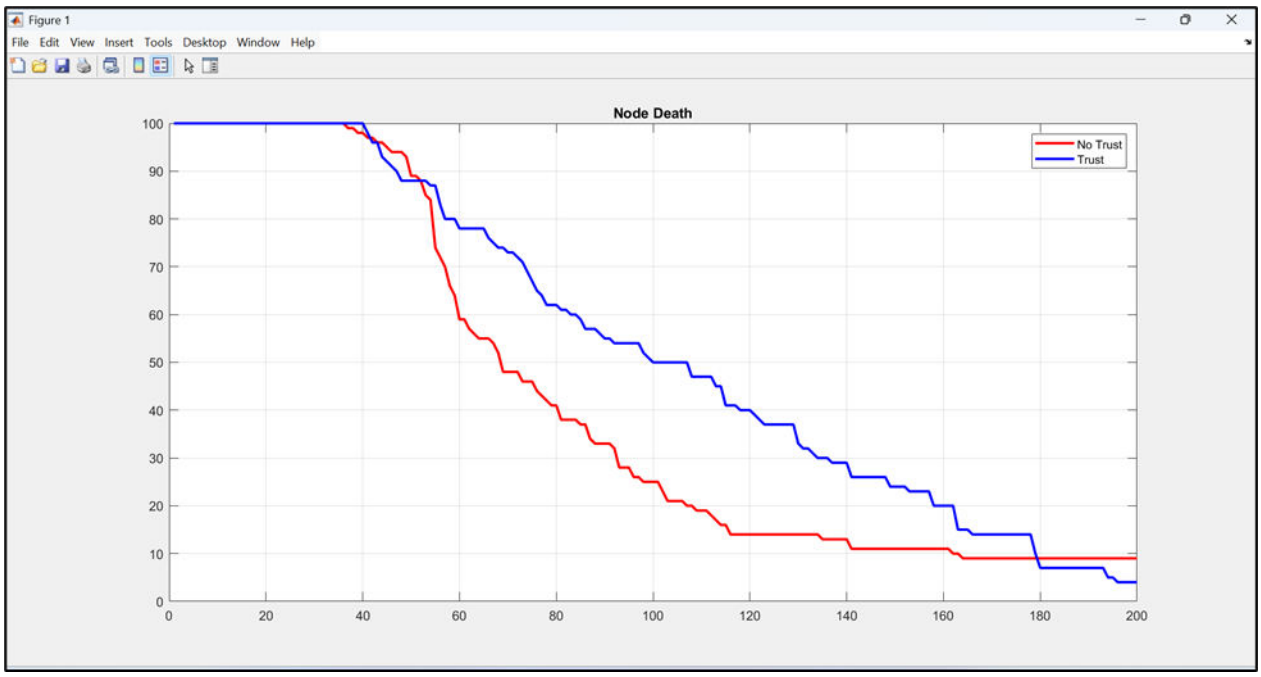


Figure 3: Rate of Node Death

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 3 illustrates the Node Death comparison between the proposed trust-based WSN framework and the conventional non-trust model over simulation rounds. The x-axis represents the number of simulation rounds, while the y-axis indicates the number of alive sensor nodes remaining in the network. The red curve corresponds to the network operating without trust management, whereas the blue curve represents the proposed trust-based approach. Initially, both networks maintain nearly all sensor nodes alive. However, after approximately 50 simulation rounds, the non-trust network experiences a rapid decrease in the number of alive nodes due to higher energy consumption, malicious node participation, and inefficient routing. In contrast, the trust-based model exhibits a lower node death rate because malicious nodes are detected and isolated from communication, leading to more secure, energy-efficient routing. The proposed trust mechanism more effectively balances network load and prevents unnecessary energy depletion.

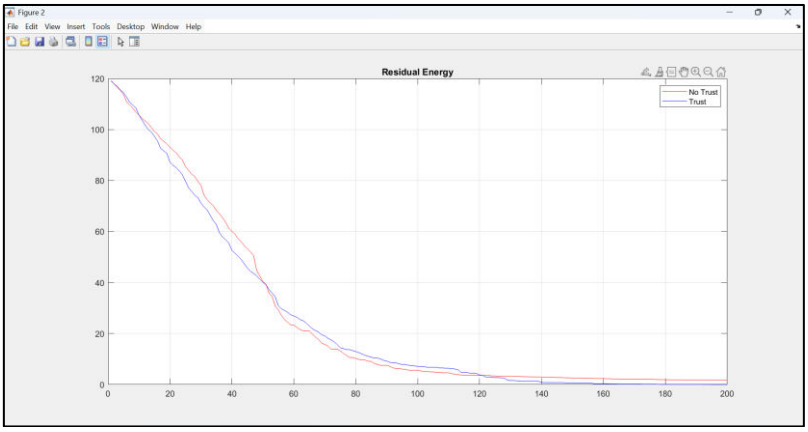


Figure 4: Residual Energy

Figure 4 presents the Residual Energy comparison between the proposed trust-based WSN framework and the conventional non-trust model over multiple simulation rounds. The x-axis represents the simulation rounds, while the y-axis indicates the average residual energy remaining in the network. The red curve corresponds to the network without trust management, whereas the blue curve represents the trust-based approach. At the beginning of the simulation, both networks start with nearly equal initial energy levels. As communication and routing operations continue, the residual energy gradually decreases due to packet transmission, reception, sensing, and processing activities. However, the non-trust network experiences slightly faster energy depletion because malicious nodes participate in routing and communication, causing unnecessary retransmissions, packet loss, and inefficient energy utilization. In contrast, the trust-based framework identifies and isolates malicious nodes, resulting in more reliable communication and balanced energy consumption among sensor nodes.

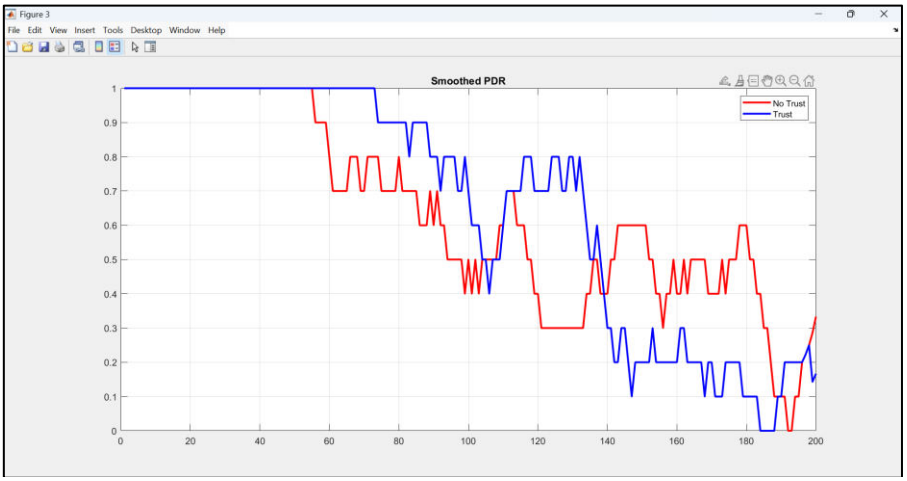


Figure 5: Packet Delivery Ratio

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 5 compares the Smoothed Packet Delivery Ratio (PDR) between the proposed trust-based WSN framework and the conventional non-trust model across multiple simulation rounds. The x-axis represents the simulation rounds, while the y-axis indicates the Packet Delivery Ratio, which measures the successful delivery of transmitted packets within the network. The red curve corresponds to the network without trust management, whereas the blue curve represents the trust-based approach. Initially, both networks achieve a high PDR close to 1, indicating reliable packet transmission during the early communication stages. As the simulation progresses and network conditions become more challenging due to malicious node activities and energy depletion, the PDR gradually decreases in both approaches. However, the trust-based framework generally maintains better packet delivery performance during several simulation intervals because malicious nodes are detected and isolated from routing operations. This reduces packet dropping, communication disruption, and routing failures.

Figure 6 shows the Cumulative Packet Delivery Ratio (PDR) of the Wireless Sensor Network over multiple simulation rounds for both the trust-based and non-trust approaches. The x-axis represents the number of simulation rounds, while the y-axis shows the cumulative PDR, which measures the overall success rate of packet delivery success rate throughout network operation. The graph demonstrates that the cumulative PDR remains very close to 1 for both approaches, indicating that a large majority of packets are successfully delivered during communication. The trust-based model slightly outperforms the non-trust network because malicious nodes are identified and isolated from routing operations, leading to more reliable packet forwarding and lower packet loss. Initially, the cumulative PDR increases rapidly as packets are successfully transmitted, then stabilizes near the maximum value as the network continues to operate efficiently.

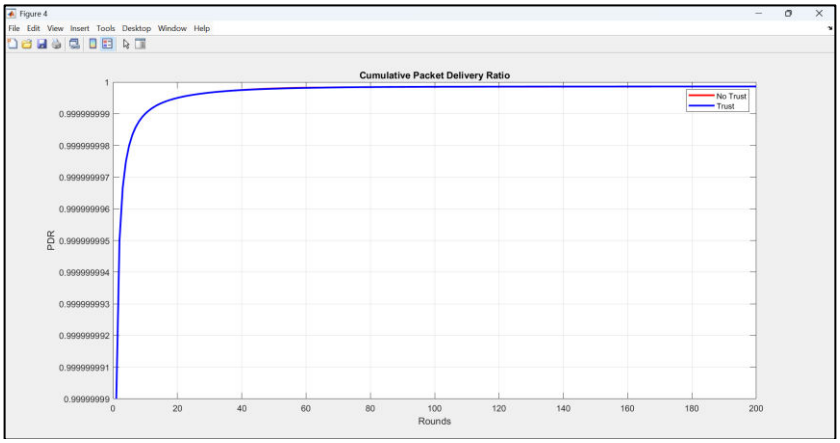


Figure 6: Cumulative PDR

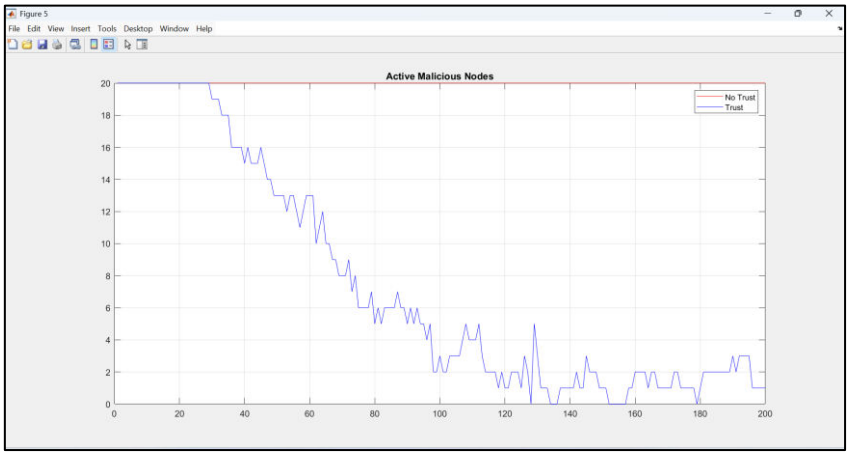


Figure 7: Active Malicious Node

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405057

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 7 presents the comparison of Active Malicious Nodes in the Wireless Sensor Network for both the trust-based framework and the non-trust model over multiple simulation rounds. The x-axis represents the simulation rounds, while the y-axis indicates the number of active malicious nodes participating in network communication. The red line corresponds to the network without trust management, whereas the blue line represents the proposed trust-based approach. In the non-trust network, the number of malicious nodes remains constant throughout the simulation because no detection or isolation mechanism is applied. As a result, malicious nodes continue to participate in routing and communication, negatively affecting network performance and security. In contrast, the trust-based framework gradually reduces the number of active malicious nodes over time. This reduction occurs because the proposed trust calculation mechanism continuously evaluates node behavior and isolates nodes with low trust values from network operations.

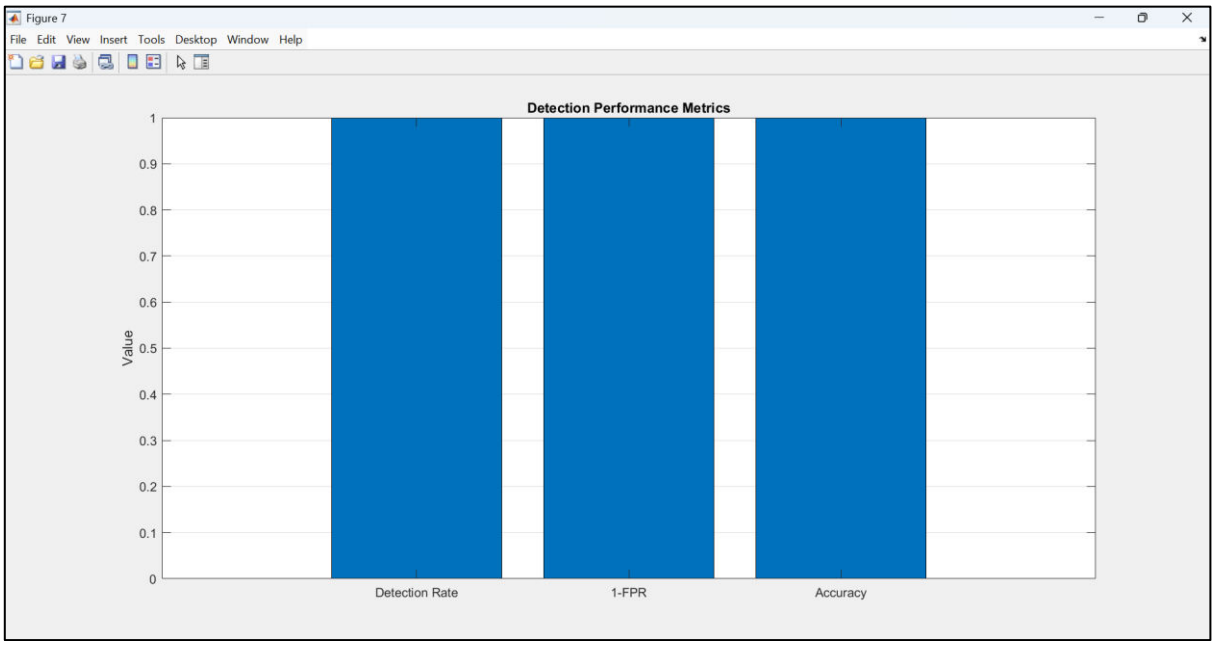


Figure 8: Detection Performance Metrics

Figure 8 illustrates the Detection Performance Metrics of the proposed trust-based malicious node detection framework in the Wireless Sensor Network. The bar graph compares three important evaluation metrics: Detection Rate, 1 − False Positive Rate (1-FPR), and Accuracy. The y-axis represents the metric values, while the x-axis shows the corresponding performance parameters. The graph shows that all three metrics achieve values very close to 1, indicating excellent performance in malicious node detection. A high Detection Rate demonstrates that the proposed framework successfully identifies most malicious nodes present in the network. Similarly, the high value of 1 − FPR indicates a very low false positive rate, meaning that normal sensor nodes are rarely misclassified as malicious. The Accuracy metric also remains close to 100%, confirming the reliability and effectiveness of the trust calculation and detection mechanism.

IV. CONCLUSION

This paper presented an energy-efficient trust-based framework for malicious node detection in Wireless Sensor Networks (WSNs). The proposed methodology integrated dynamic trust evaluation, malicious node isolation, cluster-based communication, multi-hop routing, and energy-aware network management to improve secure communication and overall network performance. Trust values were calculated using multiple parameters such as packet forwarding behavior, residual energy, and communication delay, enabling the framework to accurately distinguish between trusted and malicious sensor nodes. Simulation results demonstrated that the proposed trust-aware approach significantly improved network reliability, malicious node detection capability, and communication efficiency compared to the conventional non-trust model. The trust-based framework effectively reduced the number of active malicious nodes,

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

maintained higher packet delivery performance, and prolonged network lifetime by balancing energy consumption among sensor nodes. The results also showed improvements in key performance metrics, including Detection Rate, Accuracy, Residual Energy, Packet Delivery Ratio (PDR), and node survivability. The comparative analysis confirmed that isolating malicious nodes from routing operations helps minimize communication disruption, packet loss, and unnecessary energy depletion. In addition, the proposed framework achieved high detection accuracy with a very low false positive rate, demonstrating its effectiveness for secure and reliable WSN communication. Overall, the proposed trust-based malicious node detection mechanism provides an efficient and scalable solution for enhancing security, energy efficiency, and network stability in Wireless Sensor Networks.

REFERENCES

[1] Zawaideh, F. and Salamah, M., 2019. An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. International Journal of Communication Systems, 32(3), p.e3878.
[2] Wang, C., Liu, G. and Jiang, T., 2024. Malicious node detection in wireless weak-link sensor networks using dynamic trust management. IEEE Transactions on Mobile Computing, 23(12), pp.12866-12877.
[3] Ram Prabha, V. and Latha, P., 2017. Fuzzy trust protocol for malicious node detection in wireless sensor networks. Wireless Personal Communications, 94(4), pp.2549-2559.
[4] Bao, F., Chen, R., Chang, M. and Cho, J.H., 2011, June. Trust-based intrusion detection in wireless sensor networks. In 2011 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.
[5] Gangwani, P., Perez-Pons, A. and Upadhyay, H., 2024. Evaluating trust management frameworks for wireless sensor networks. Sensors, 24(9), p.2852.
[6] Geetha, V. and Chandrasekaran, K., 2014. A distributed trust based secure communication framework for wireless sensor network. Wireless Sensor Network, 6(9), p.173.
[7] 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.
[8] Malik, S., Arora, M., Sharma, R. (2025). Comprehensive Guide to Different Types of Attacks on Email Systems, *Information Horizons: AMERICAN Journal of Library And Information Science Innovation,* 2(6).
[9] 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.
[10] 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.
[11] 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.
[12] She, W., Liu, Q., Tian, Z., Chen, J.S., Wang, B. and Liu, W., 2019. Blockchain trust model for malicious node detection in wireless sensor networks. Ieee Access, 7, pp.38947-38956.
[13] Zhang, W., Das, S.K. and Liu, Y., 2006, September. A trust based framework for secure data aggregation in wireless sensor networks. In 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (Vol. 1, pp. 60-69). IEEE.
[14] Zhang, B., Huang, Z. and Xiang, Y., 2014. A novel multiple-level trust management framework for wireless sensor networks. Computer Networks, 72, pp.45-61.
[15] Saidi, A., 2024. An adaptive trust system for misbehavior detection in wireless sensor networks. Wireless Networks, 30(4), pp.2589-2615.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details