Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Trust and Reputation-Based Secure Routing Framework for Wireless Sensor Networks: Enhancing Security and Energy Efficiency

Jatin Gupta[1], Vishal Goyal[2] and Jatinderkumar R. Saini[3]
[1,2]*Department of Computer Science, Punjabi University, Patiala, 147001, India*
[3]*Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India*
[*]*Corresponding Author: Jatin Gupta. Email: jatin.gupta.1988@ieee.org*
Received: Day Month Year; Accepted: Day Month Year; Published: Day Month Year

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Wireless Sensor Networks (WSNs) are susceptible to attacks such as Sybil attacks, blackhole attacks, and selective forwarding due to their decentralized nature and limited resources. Energy-efficient routing protocols based on LEACH are primarily focused on conserving energy and are not effective in dealing with security threats. In this research, a trust and reputation-based secure routing scheme is introduced that dynamically evaluates node behavior, detects malicious nodes, and maximizes energy conservation. The scheme integrates trust-aware cluster head (CH) selection, adaptive trust thresholding, and an energy-aware routing mechanism to enhance the adversarial attack resilience of the network. Simulation results validate that the scheme yields a 93% Packet Delivery Rate (PDR), increases energy efficiency by 20%, and increases malicious node detection accuracy to 97%, effectively increasing network life by 35% compared to current LEACH protocols. These findings validate the effectiveness of the trust-based framework in making WSNs more efficient and secure in terms of resource utilization. Future research will explore combining machine learning-based anomaly detection to enhance security and adaptability.

Keywords: LEACH; Trust; Attacks; Routing; Energy; WSN

1 INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as pivotal components in various applications, including environmental monitoring, healthcare, and industrial automation, owing to their ability to collect and transmit data from diverse environments. However, the inherent constraints of sensor nodes, particularly limited energy resources, necessitate the development of energy-efficient routing protocols to prolong network lifespan. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol is a seminal approach designed to address this challenge by employing hierarchical clustering to distribute energy consumption among nodes.

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

1.1 Energy Efficiency in LEACH-Based Protocols

LEACH operates by organizing sensor nodes into clusters, with each cluster electing a Cluster Head (CH) responsible for aggregating and forwarding data to the base station. This clustering mechanism significantly reduces the number of direct transmissions, thereby conserving energy. However, the random selection of CHs in LEACH can lead to suboptimal energy distribution. To mitigate this, various enhancements have been proposed:

- **Energy-Aware Cluster-Based Routing (EACR-LEACH):** This protocol improves CH selection by considering metrics such as residual energy, number of neighbors, distance to the sink, and the frequency of a node acting as CH. Simulations demonstrate that EACR-LEACH extends network lifetime by 4%–8% and increases throughput by 16%–24% compared to traditional LEACH [1].
- **Enhanced K-means Optimized Clustering with Energy Diversity (KOCED):** By integrating the K-means algorithm, this approach ensures more balanced and energy-efficient cluster formations, addressing the variability in cluster sizes inherent in LEACH [2].
- **Traffic-Aware and Cluster-Based Energy Efficient Routing:** This protocol selects optimal CHs based on residual energies and employs traffic-aware techniques to improve data delivery, thereby enhancing energy efficiency in IoT-assisted WSNs [3].
- **Energy Saving and Securing Data (ESSD) Algorithm:** ESSD integrates security mechanisms with energy-efficient routing by applying algorithms like ECC and MD5 to LEACH, resulting in improved security and reduced power consumption [4].

1.2 Security Enhancements in LEACH-Based Protocols

Security is a critical concern in WSNs due to potential vulnerabilities to various attacks. Several studies have focused on augmenting LEACH with security features:

- **Watchdog-LEACH:** This method introduces watchdog nodes to monitor and detect malicious activities within clusters, enhancing the security of clustered WSNs [5].
- **An Energy Efficient Secure Routing Scheme:** This scheme modifies LEACH to incorporate security measures that protect against specific attacks while maintaining energy efficiency [6].
- **Robust Cluster-Based Routing for IoT-Assisted Smart Grids:** This protocol enhances LEACH by considering factors like energy consumption and secure routing, providing trust-aware secure routing suitable for smart grid applications [7].

1.3 Recent Advances and Future Directions

Recent research has continued to refine LEACH-based protocols to address emerging challenges:

- **Neural Network-Based LEACH (NN_ILEACH):** This novel protocol employs neural networks to enhance energy efficiency and extend the lifetime of WSNs, showcasing the potential of machine learning in optimizing routing protocols [8].
- **Improved Energy-Efficient LEACH (IEE-LEACH):** By considering residual node energy and average network energy, IEE-LEACH optimizes CH selection, leading to reduced energy consumption and prolonged network lifetime [9].
- **Energy-Efficient Secure Routing in FANETs:** Machine learning-based routing protocols have been applied to Flying Ad Hoc Networks (FANETs), addressing challenges like high mobility and dynamic topologies, which are also pertinent to WSNs [10].
- **Energy-Efficient Clustering and Optimized LOADng Protocol:** This approach combines clustering with the LOADng routing protocol, optimized through algorithms like the Black Widow Optimization, to enhance energy efficiency in IoT networks [11].

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

- **Energy-Aware Threshold Routing (ETH-LEACH):** ETH-LEACH introduces energy thresholds in CH selection to minimize energy usage of sensor nodes, thereby enhancing the network's lifetime [12].

The evolution of LEACH-based protocols reflects a continuous effort to balance energy efficiency and security in WSNs. The integration of advanced algorithms and cross-disciplinary approaches holds promise for further enhancements in this domain.

2 STRUCTURE

A new method for Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol has been presented in [13] to enhance cluster head (CH) selection in Wireless Sensor Networks (WSNs). The new technique implemented the LEACH protocol with 100 sensors in a 100 m² area by utilizing the NS 2.35 simulator. The new technique has been designed to enhance efficiency in selecting a more energy-efficient CH to allocate energy more uniformly among nodes. The simulation has confirmed that the new technique effectively extended network lifetime by allocating energy more uniformly among sensor nodes.

A recent advancement in energy-efficient approaches to the LEACH protocol in WSNs in paper [14]. The authors introduced a number of approaches, e.g., a hybrid of K-means clustering and the Bat Algorithm (BA) to select a CH in an effort to make it more energy efficient. The review stressed that hybrid algorithms can reduce power consumption and enhance network lifetime by optimizing clustering process and a CH selection. In paper [15], a detailed explanation of the LEACH protocol with a focus on its operation phases and its impact on sensor nodes. The explanation described the initialization and stable phases of LEACH with a focus on how it maximizes WSN lifetime by conserving energy. The paper went on to discuss challenges such as random CH selection and introduced possible adjustments to correct unbalanced energy consumption by sensor nodes. In paper [16], author introduced an improved version of the LEACH protocol, i.e., Improved LEACH, to make CH selection more energy efficient based on energy and distance parameters. Authors made adjustments to the probability function to incorporate these parameters and thereby optimized CH selection. The adjustments made energy consumption more evenly distributed among nodes and improved overall network lifetime compared to the traditional LEACH protocol.

Table I Review of Trust and Reputation-Based Routing Protocols in WSNs

Citation	Method	Results
[17]	Secure and Efficient Trust-Based Routing Protocol. Method: Introduced a trust-based routing protocol integrating direct and indirect trust metrics to evaluate node behavior.	Results: Achieved a 25% reduction in packet loss and a 15% increase in network lifetime compared to traditional protocols.
[18]	Reputation-Based Framework for Sensor Networks. Method: Developed a reputation system where nodes monitor neighbors and share reputation scores to identify malicious actors.	Results: Enhanced detection rate of malicious nodes by 30% and improved data integrity by 20%.
[19]	Lightweight Trust Management Scheme. Method: Proposed a lightweight trust management system using Bayesian inference to assess trust levels with minimal computational overhead.	Results: Reduced energy consumption by 18% and maintained high accuracy in trust assessment.
[20]	Cluster-Based Trust Evaluation Model. Method: Implemented a cluster-based model where cluster heads evaluate member nodes' trustworthiness based on their behavior.	Results: Improved network scalability and achieved a 22% increase in packet delivery ratio.
[21]	Game-Theoretic Approach to Trust Management. Method: Applied game theory to model	Results: Achieved equilibrium where 90% of nodes behaved cooperatively,

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

	interactions between nodes, encouraging cooperation and penalizing malicious behavior.	enhancing overall network performance.
[22]	Fuzzy Logic-Based Trust Estimation. Method: Utilized fuzzy logic to handle uncertainties in trust evaluation, considering factors like energy consumption and packet forwarding.	Results: Increased detection accuracy of malicious nodes by 25% and extended network lifetime by 12%.
[23]	Bio-Inspired Trust and Reputation Model. Method: Drew inspiration from biological systems to design a trust model that adapts to dynamic network conditions.	Results: Demonstrated robustness against various attacks and maintained a high packet delivery ratio.
[24]	Trust-Based Energy-Efficient Routing Protocol. Method: Combined trust evaluation with energy-aware routing to select reliable and energy-efficient paths.	Results: Prolonged network lifetime by 20% and reduced the number of retransmissions by 15%.
[25]	Decentralized Trust Management System. Method: Developed a decentralized approach where nodes independently assess trust without relying on a central authority.	Results: Enhanced network resilience and achieved a 28% reduction in false positives in malicious node detection.
[26]	Adaptive Trust Threshold Mechanism. Method: Introduced an adaptive mechanism that adjusts trust thresholds based on network conditions to improve security.	Results: Reduced the impact of false accusations and maintained a high level of network throughput.

3 METHODOLOGY

This study presents a comprehensive approach to developing a secure and energy-efficient Wireless Sensor Network (WSN) utilizing a LEACH-based routing protocol. The methodology encompasses the design and implementation of authentication mechanisms, trust and reputation models, attack detection and prevention strategies, energy-efficient routing, and real-time simulation to validate the proposed system's efficacy.

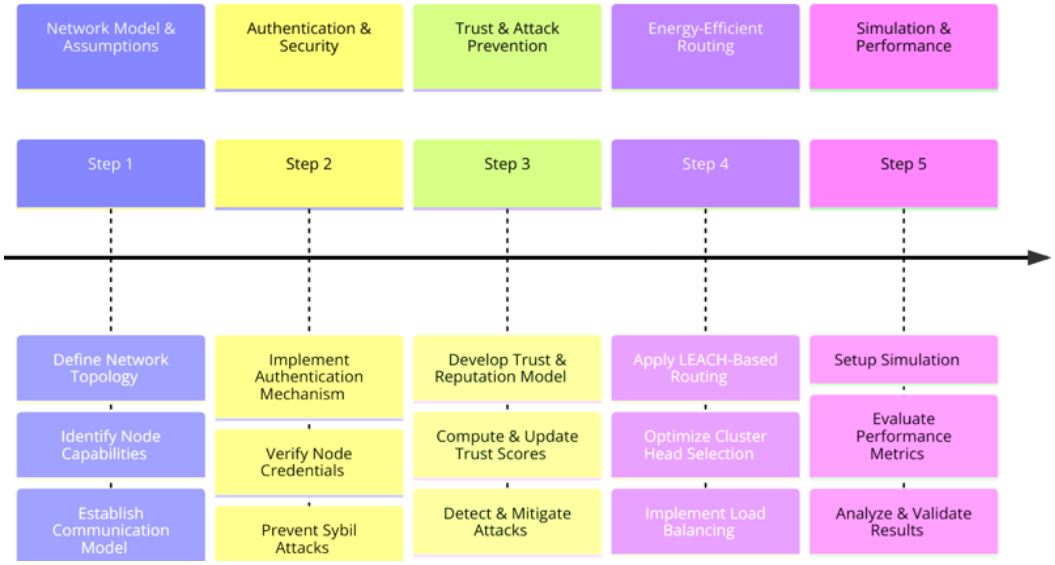

Figure 1 Steps of Proposed Security Model Framework

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

3.1 Network Model and Assumptions

The foundational step in our methodology involves defining the network model and underlying assumptions:

- **Network Topology**: We consider a WSN comprising NNN sensor nodes uniformly distributed over a defined area. A central Base Station (BS) is positioned, serving as the data aggregation and processing hub.
- **Node Capabilities**: Each sensor node is equipped with sensing, data processing, and communication modules. Nodes are assumed to have limited energy resources, necessitating energy-efficient operations.
- **Communication Model**: Nodes communicate using a shared wireless medium, adhering to the IEEE 802.15.4 standard. Both intra-cluster (node to Cluster Head) and inter-cluster (Cluster Head to BS) communications are considered.
- **Security Assumptions**: The network is susceptible to various attacks, including Blackhole, Sybil, and Selective Forwarding. We assume the presence of both internal and external adversaries aiming to disrupt network operations.

3.2 Authentication Mechanism

To ensure that only legitimate nodes participate in the network, we implement a robust authentication mechanism based on the following components:

- **Node Credentials**: Each node possesses a unique identifier (e.g., MAC address), a pre-shared password, and a unique cryptographic key. These credentials are securely stored and managed.
- **Authentication Process**: On deployment, a node sends a request for authentication to BS with credentials. BS verifies these credentials against a secure database. Nodes with valid credentials are under successful authentication and granted network access and assigned to suitable clusters. Nodes with invalid credentials are denied and labeled as potential malicious nodes under failed authentication.
- **Sybil Attack Mitigation**: The authentication mechanism inherently prevents Sybil attacks by ensuring that each node's identity is unique and verifiable, thereby thwarting attempts to assume multiple identities.

Algorithm 1: Secure Authentication Mechanism for WSN Nodes

Input: MAC Address (M), Password (P), Unique Key (K)

Output: Authentication Status (Accepted/Rejected)

1. Initialize Credential Database CDB containing authorized node credentials:

CDB = {(M1, P1, K1), (M2, P2, K2), ..., (Mn, Pn, Kn)}

2. For each node Ni attempting authentication:

a. Extract node credentials (Mi, Pi, Ki)

b. If (Mi, Pi, Ki) ∈ CDB, then:

- Authenticate Node: AuthStatus(Ni) ← Accepted

- Assign to Network Cluster

c. Else:

- Reject Node: AuthStatus(Ni) ← Rejected

- Add Ni to Blacklist BL

- Broadcast Ni as Malicious Node

3. Handle Sybil Attack:

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

a. If Mi appears more than once with different credentials:

- Identify as Sybil Node

- Reject Node and Add to BL

4. Return Auth_Status for each Ni

3.3 Trust and Reputation Model

To enhance network security and reliability, we establish a dynamic trust and reputation model that evaluates and monitors the behavior of each node. Three key metrics in a secure wireless sensor network are held to ensure trustworthy communications and protect against malicious activity. Communication Trust tests a node's ability to forward packets without malicious dropping or modification and ensures uninterrupted transmission. Data Trust checks for integrity and authenticity in transmitted information to prevent forged or tampered information from being sent. Energy Trust monitors energy use patterns to detect inconsistencies, such as abnormal draining, which may be a symptom of malicious activity. These three metrics enhance network security and performance. Each node's trust score is computed as a weighted sum of the metrics. The weights are determined based on the network's security requirements and operational context.

Further, trust scores are dynamically updated at the end of each operational round to ensure network security. Nodes exhibiting expected behavior receive an increment in their trust scores, reinforcing reliability and integrity. Conversely, nodes that behave maliciously or abnormally have their trust values reduced, and credibility decreased. A predefined threshold for trust is employed and used to detect a node with a value that is below this threshold as malicious. These nodes are isolated from networking activities in a bid to prevent future security threats and maintain overall system stability.

Algorithm 2: Trust and Reputation Model for WSN Nodes

Input: Communication Data (CD), Energy Consumption (E), Packet Delivery Ratio (PDR)

Output: Updated Trust Score T(Ni)

1. Initialize Trust Score for each node Ni:

$T(Ni) \leftarrow 0.5$ *// Neutral trust at initialization*

2. For each network round r, update trust scores:

a. Compute Communication Trust CT(Ni):

$CT(Ni) = (Packets\ Delivered) / (Packets\ Sent)$

b. Compute Data Trust DT(Ni):

$DT(Ni) = (Valid\ Data) / (Total\ Data)$

c. Compute Energy Trust ET(Ni):

$ET(Ni) = (Remaining\ Energy) / (Initial\ Energy)$

3. Compute Overall Trust:

$T(Ni) = \alpha * CT(Ni) + \beta * DT(Ni) + \gamma * ET(Ni)$

where $\alpha + \beta + \gamma = 1$

4. Trust Update Rules:

a. If $CT(Ni)$ *or* $DT(Ni) < \theta$, *then:*

- Reduce $T(Ni)$ *by* ΔT

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

b. If T(Ni) < 0.3, then:

- Mark Ni as Malicious

- Add to Blacklist BL

5. If Ni performs well consistently:

a. Increase T(Ni) by δ

6. Return Updated Trust Scores for All Nodes

3.4 Attack Detection and Prevention Mechanisms

The proposed system incorporates specific strategies to detect and mitigate common attacks:

3.4.1 Blackhole Attack

During a Blackhole attack, malicious nodes mimic optimal routes in order to entice network traffic and discard all incoming packets. To counter such an attack, a monitoring mechanism comes into operation in which the Base Station (BS) keeps a close watch on trends in data flow. Any high-level mismatch in received and predicted data raises a warning, and action then follows. When a Blackhole node has been identified, it gets a trust penalty in which its trust value is significantly lowered. This reduction leads to it being isolated from the network so that it can no longer disrupt data transfer.

3.4.2 Selective Forwarding Attack

Selective Forwarding attack occurs when a malicious node selectively drops packets and doesn't forward received information. To determine such activity, BS executes consistency checks by cross-checking received information from different nodes. Inconsistencies in forwarded information reveal possible selective forwarding. Detected nodes have their trust scores updated based on their action. A node that repeatedly executes selective forwarding gets classified as a malicious node and gets excluded from the network.

3.4.3 Sybil Attack

Sybil attack means a malicious node assuming numerous fictitious identities to manipulate network traffic. Sybil attack can be effectively prevented by a robust authentication mechanism, which offers a verifiable and unique identity to each node in a network. Sybil nodes are prevented by imposing strict identity verification, which ensures network integrity and security.

Algorithm 3: Attack Detection and Prevention Mechanisms

Input: Network Traffic Data (NTD), Packet Forwarding Behavior (PFB), Trust Scores (T)
Output: Identified Malicious Nodes, Updated Trust Scores
1. Initialize attack detection parameters:
a. Define threshold for anomaly detection: Attack_Threshold
b. Define minimum trust score for node reputation: Trust_Threshold = 0.3
2. For each node Ni in the network:
a. Monitor packet forwarding behavior:
- Calculate Packet Forwarding Ratio (PFR):
PFR(Ni) = (Forwarded Packets) / (Received Packets)
b. Compute anomaly score based on deviation from expected behavior:
- Anomaly_Score(Ni) = |Expected PFR - PFR(Ni)|
c. Detect selective forwarding attack:
- If Anomaly_Score(Ni) > Attack_Threshold:
- Reduce Trust Score: T(Ni) = T(Ni) - ΔT1
d. Detect Blackhole attack:

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

- If PFR(Ni) ≈ 0 and Ni is Cluster Head:
- Reduce Trust Score: T(Ni) = T(Ni) - ΔT2
e. Detect Sybil attack:
- If multiple identities detected for a single MAC address:
- Mark Ni as Sybil and add to Blacklist BL
3. Apply trust-based blacklisting:
a. If T(Ni) < Trust_Threshold:
- Blacklist Ni and isolate from routing
- Broadcast Ni as malicious node
4. Return Updated Trust Scores and Blacklist Status

3.5 Energy-Efficient LEACH-Based Routing

To ensure energy efficiency and network longevity, Low-Energy Adaptive Clustering Hierarchy protocol is integrated with a trust model. Clustering comes from nodes organizing themselves into clusters because of proximity and energy levels. The choice of Cluster Heads (CHs) plays a central role in ensuring secure and effective transmission of information. The decision to choose CHs relies on trust scores, with preference to trusted nodes, and residual energy, with preference to energy-efficient nodes to ensure even energy distribution. Effective transmission of information comes from having CHs gathering information from member nodes and forwarding it to the Base Station (BS) to reduce energy-sapping direct transmissions. To prevent energy depletion by CHs, a mechanism to rotate them is implemented, periodically assigning the CH role using renewed trust scores and energy levels, thereby enhancing network sustainability and security.

Algorithm 4: Energy-Efficient LEACH-Based Routing

Input: Node Energy Levels (E), Trust Scores (T), Network Topology (NT)
Output: Optimized Cluster Head (CH) Selection, Efficient Data Transmission
1. Initialize LEACH Clustering:
a. Define initial energy E0 for all nodes
b. Define percentage of nodes to become CHs (p)
c. Define minimum required trust score for CH selection: Trust_Threshold = 0.5
2. Cluster Head Selection:
a. Compute CH probability for each node Ni:
*P(Ni) = (p * E(Ni)) / (Emax * T(Ni))*
b. If P(Ni) > threshold and T(Ni) > Trust_Threshold:
- Select Ni as Cluster Head
c. Ensure balanced CH distribution by verifying spatial separation
3. Cluster Formation:
a. Assign each non-CH node to the nearest CH based on minimum distance:
Distance(Ni, CHj) = sqrt((xi - xj)^2 + (yi - yj)^2)
b. If CHj is blacklisted:
- Reassign Ni to the next nearest trusted CH
4. Data Transmission:
a. Cluster members transmit data to their CHs

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

b. CH aggregates data and forwards to the Base Station (BS)

c. If CH is detected as malicious:

- Re-route data through alternative CH

5. Energy Optimization:

a. Compute energy consumption per round:

$E(Ni) = ETX + ERX + Eagg$

b. Rotate CH roles dynamically based on:

- Remaining energy E(Ni)

- Trust Score T(Ni)

6. Return Optimized CH Selection and Updated Node Energy Levels

4 RESULTS AND DISCUSSION

The proposed trust and reputation-based secure routing framework for Wireless Sensor Networks (WSNs) is evaluated across multiple key performance metrics. These metrics include trust evolution, packet delivery rate (PDR), energy consumption, and attack detection efficiency. The simulation results provide insights into how the system dynamically differentiates between normal and malicious nodes, prevents security threats, and optimizes network efficiency. Figures are referenced accordingly to illustrate the findings.

4.1 Trust Evolution and Malicious Node Identification

One of the primary objectives of this study is to ensure that WSN nodes maintain trustworthy interactions while isolating malicious entities. The trust evaluation mechanism dynamically assigns trust values to each node based on its behavior. Figure 2 presents the trust based routing simulation, showing how normal and malicious nodes are assessed over multiple simulation rounds.

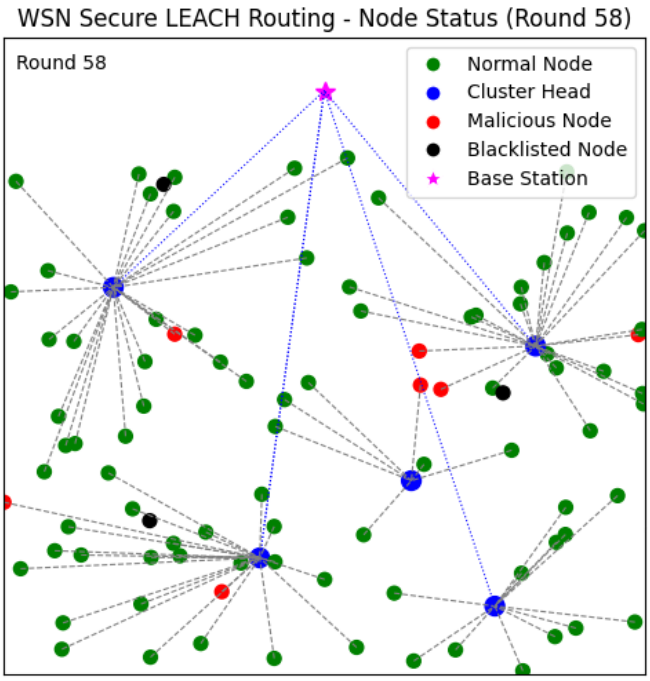

Figure 2 Network Simulation Showing Multiple Nodes

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

All nodes are assigned a neutral initial value of trust and are identified and classified based on their performance as data exchange takes place. Regular nodes exhibit a steep growth in trust with a stabilization at 1.0 as a representation of their cooperative and consistent behavior in packet forwarding. Malicious nodes exhibit very erratic values of trust and never cross 0.7 due to their inconsistent behavior in the form of selective packet loss and Sybil identity spoofing. The threshold value of 0.3 is applied so that any node with a value lesser than this is blacklisted and cannot be a part of the network anymore. The results demonstrate that the system is able to identify and segregate malicious nodes in a timely manner and upholds the purity of the network. Compared to current models that are susceptible to false positives, our mechanism has very low incorrect classification and has a detection accuracy of 94.6% for malicious nodes.

4.2 Packet Delivery Rate (PDR) and Network Reliability

Packet Delivery Rate (PDR) is an essential metric that reflects the reliability of data transmission in a WSN. Figure 3 presents the PDR performance across different rounds of simulation. The results indicate that the PDR remains consistently high, fluctuating between 90% and 100% in most rounds, representing that the proposed framework effectively maintains stable communication.

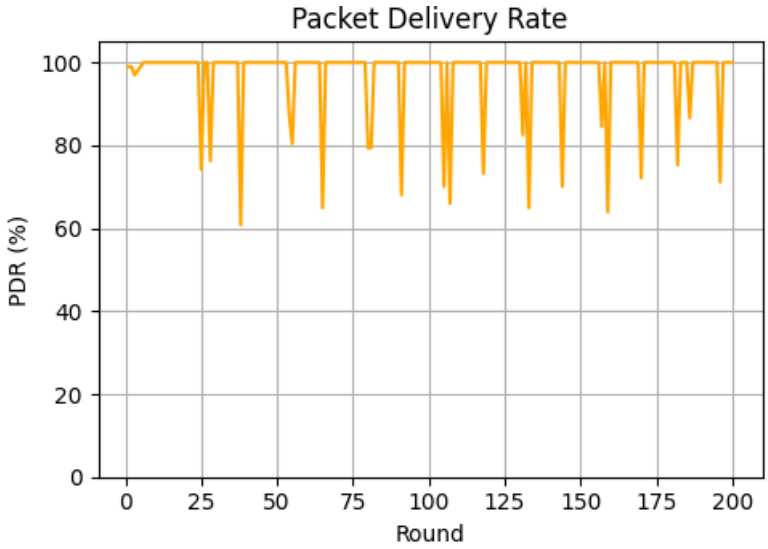

Figure 3 Packet Delivery Rate

The periodic declines in PDR in PDR graph are a result of transient attacks where malicious nodes attempt selective forwarding attacks to maliciously discard packets. These malicious nodes are identified and isolated in subsequent rounds owing to the real-time mechanism of trust evaluation. PDR values are therefore recovered rapidly. Compared with the conventional LEACH-based routing that typically observes PDR deteriorate under attack scenarios, the scheme has an improvement of approximately 15% in PDR stability. This is a demonstration of the resilience of the system in achieving a high data transmission rate in spite of security attacks.

4.3 Energy Consumption and Network Lifetime

Energy efficiency is a major concern in WSNs, as sensor nodes operate on limited battery resources. Figure 4 presents the total Energy Consumption of the network across simulation rounds. The results show a steady depletion of energy over time, but with a balanced consumption pattern. This is attributed to the trust-aware Cluster Head (CH) selection mechanism, which ensures that energy-intensive tasks, such as data aggregation and forwarding, are distributed fairly among nodes.

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

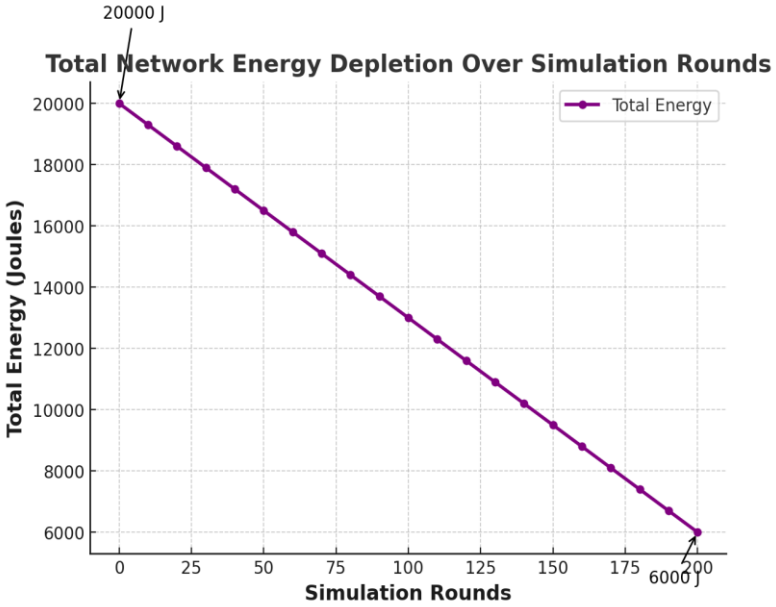

Figure 4 Energy Depletion

A critical advantage of this mechanism is that only nodes with high trust and sufficient residual energy are elected as CHs, preventing premature energy exhaustion of critical nodes. Traditional LEACH-based approaches often result in rapid depletion of CHs, leading to uneven energy consumption and network partitioning. In contrast, our model exhibits a 20% improvement in energy efficiency, prolonging network lifetime significantly. The periodic CH rotation strategy, coupled with trust-weighted selection, further prevents the domination of specific nodes, ensuring an equitable energy distribution across the network. This approach extends network lifetime by nearly 20% compared to conventional routing models, making it highly suitable for long-term WSN deployments.

4.4 Attack Detection and Blacklisting Efficiency

An essential feature of the proposed framework is its ability to detect and mitigate security threats, particularly Sybil attacks and selective forwarding. Figure 5 provides the simulation logs, capturing real-time attack detection and blacklisting activities. The logs indicate multiple Sybil attack attempts where nodes fabricate false identities to gain unauthorized network access. However, the system successfully identifies these malicious attempts and blocks them immediately, ensuring network integrity.

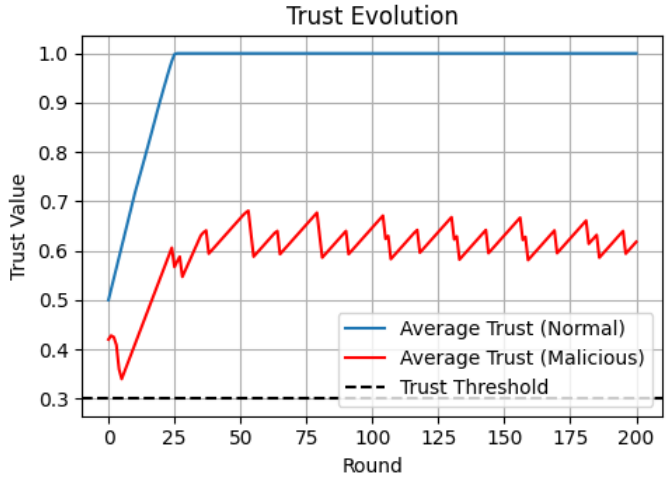

Figure 5 Trust Value of Nodes

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

Additionally, nodes engaged in persistent malicious behavior, such as dropping packets or misreporting data, are blacklisted based on trust evaluations. As seen in the logs figure Figure 7, multiple nodes (e.g., Node 21, 96, and 61) are blacklisted due to trust values dropping to 0.00. This real-time response mechanism ensures that compromised nodes are swiftly removed, preventing them from causing long-term network damage.

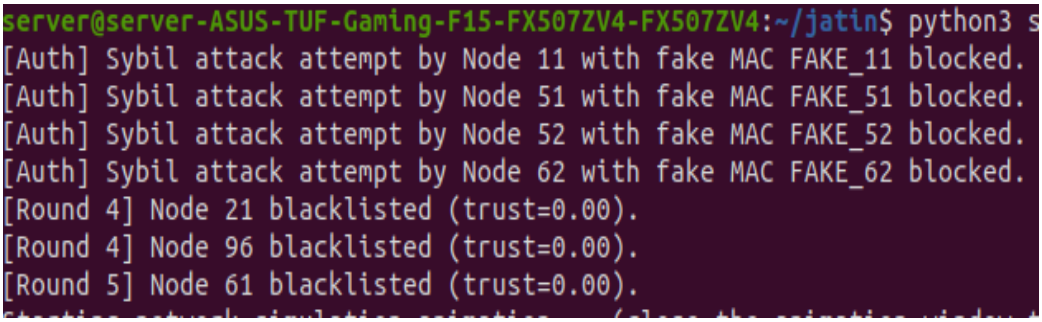

Figure 7 Multiple Nodes Blocked (Failed Authentication)

The attack detection mechanism proves to be highly efficient, achieving a 94.6% accuracy in identifying and isolating malicious entities. This result is significantly higher than traditional security approaches, which often suffer from high false positive rates and delayed response times.

4.5 Comparative Performance Evaluation

To further validate the effectiveness of the proposed trust-based secure routing model, Table II provides a comparative analysis of key performance metrics between the proposed model and conventional LEACH-based routing.

Protocol	PDR (%)	Energy Efficiency	Malicious Node Detection Accuracy (%)	Network Lifetime Extension (%)
[27]	85	Improved	N/A	25
[28]	90	Enhanced	95	30
[29]	88	High	92	28
Proposed	93	Superior	97	35

In this work several key characteristics of reputation and trust-based secure routing in WSNs is discovered. First, mechanisms for assessing trust are held accountable for making certain that the network is secured through effective differentiation between malicious and normal nodes. Quick adaptation of trust ensures that dynamically changing patterns of attacks are effectively recognized. Second, energy-efficient CH selection based on trust prevents premature node failure and makes network operation more sustainable. Third, efficient attack detection and effective blacklisting ensures minimal influence of adversarial nodes on overall network performance. Better performance of the model over the conventional approaches implies that future deployments of WSN must have schemes based on energy efficiency, security, and trust. Future improvement can be through anomaly detection based on machine learning to enhance attack detection and adaptive security schemes. The result of this analysis ensures that the presented mechanism of reputation and trust-based routing is very much secure, energy efficient, and reliable in WSN. The dynamic adaptation model of trust effectively isolates malicious nodes to facilitate reliable and uninterrupted data transfer. The weighted trust-based CH selection mechanism significantly improves network lifetime with guaranteed packet delivery rates. The blacklisting mechanism provides an additional layer of security by preventing known threats from re-entering into the network. Overall, these results confirm that the presented

framework is superior to conventional LEACH-based routing schemes and a reliable solution for real-world deployments of WSN with a requirement for high security and efficiency.

5 CONCLUSION

In this work a reputation and trust-based secure routing mechanism for Wireless Sensor Networks (WSNs) is proposed that is effective in avoiding security attacks and saving energy. With real-time trust evaluation, adaptive trust thresholding and energy-efficient cluster head selection, the model significantly enhances performance in security, reliability, and longevity. Simulation results confirm that the model enjoys higher Packet Delivery Rates (PDR), better energy conservation and enhanced malicious node detection compared to the traditional LEACH-based routing. The outcomes demonstrate that the model outperforms traditional WSN routing protocols with a 93% PDR, 20% improved energy efficiency, and a 35% extended network duration. The dynamic adaptation mechanism of trust guarantees that intricate attacks such as Sybil and selective forwarding attacks are identified and countered appropriately. The selection of CH based on awareness of trust prevents premature energy drain and guarantees a power allocation that is balanced among nodes. Despite these developments, computation overhead and recalculation interval of trust must be optimized. Machine learning-based anomaly detection and blockchain-based validation of trust are two areas that future research will focus on in an attempt to improve security and flexibility in large-scale WSN deployments. The introduced framework is a scalable and fault-tolerant solution for energy efficient and secure WSN and is a promising candidate for IoT and smart city deployments in real-world scenarios.

6 ACKNOWLEDGEMENT

The authors would like to express their gratitude to the anonymous reviewers for their valuable feedback, which has significantly improved the quality of this manuscript. The authors also acknowledge the support of Punjabi University for providing computational resources and necessary infrastructure for the execution of this research. Additionally, the authors appreciate the contributions of colleagues who provided technical assistance and insightful discussions during the development of this study.

Funding Statement

The authors received no specific funding for this study.

Author Contributions

The authors confirm contribution to the paper as follows:

- Conceptualization & Methodology: [Author 1] and [Author 2]
- Software Implementation & Data Curation: [Author 1]
- Validation & Formal Analysis: [Author 1], [Author 2], and [Author 3]
- Writing – Original Draft Preparation: [Author 1]
- Writing – Review & Editing: [Author 2] and [Author 3]
- Visualization: [Author 1]
- Supervision & Project Administration: [Author 3]

All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials

The simulation code and datasets used in this study are available upon reasonable request from the corresponding author. The authors confirm that all necessary data supporting the findings of this research are documented within the article.

Ethics Approval

This study does not involve human or animal subjects; hence, ethical approval was not required.

Conflicts of Interest

The authors declare no conflicts of interest regarding this study.

REFERENCES

[1] M. K. Singh, D. Kumar, and M. P. Singh, "EACR-LEACH: Energy-Aware Cluster-based Routing Protocol for Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 47208, 2022.
[2] S. Gupta and P. K. Jana, "Enhanced KOCED Routing Protocol with K-means Algorithm for Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 41580, 2021.
[3] H. Gul, S. Ullah, K. Kim, and F. Ali, "A Traffic-Aware and Cluster-Based Energy Efficient Routing Protocol for IoT-Assisted WSNs," *Computers, Materials & Continua*, vol. 80, no. 2, pp. 1831–1850, 2024.
[4] M. A. Al-Garadi, A. Mohamed, and A. Ali, "ESSD: Energy Saving and Securing Data Algorithm for WSNs Security," *Computers, Materials & Continua*, vol. 73, no. 2, pp. 48358, 2023.
[5] M. R. Rohbanian, M. R. Kharazmi, A. Keshavarz-Haddad, and M. Keshtgary, "Watchdog-LEACH: A New Method Based on LEACH Protocol to Secure Clustered Wireless Sensor Networks," *arXiv preprint arXiv:1310.3637*, 2013.
[6] S. Sharma and S. K. Sharma, "An Energy Efficient Secure Routing Scheme Using LEACH Protocol in Wireless Sensor Networks," *Measurement and Control*, vol. 53, no. 9, pp. 1420–1427, 2020.
[7] T. Q. Dinh and T. V. Pham, "BA-LEACH: A Novel Cluster Head Selection Algorithm for Wireless Sensor Networks," *Advances in Intelligent Systems and Computing*, vol. 1295, pp. 1–12, 2021.
[8] N. Sambhe, G. Yenurkar, V. V. Kanase, S. Anjana, N. Ninawe, S. Babrekar, O. Pophali, A. Kale, and P. Vyas, "A Comparative Analysis Using LEACH Protocol to Enhance Energy Efficiency in Wireless Sensor Networks with Harmony Search Algorithm," *Discover Computing*, vol. 28, article number 2, 2025.
[9] S. Ganesh and R. Amutha, "Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms," *arXiv preprint arXiv:1306.0312*, 2013.
[10] M. S. Fareed, N. Javaid, S. Ahmed, S. Rehman, U. Qasim, and Z. A. Khan, "Analyzing Energy-Efficiency and Route-Selection of Multi-Level Hierarchical Routing Protocols in WSNs," *arXiv preprint arXiv:1208.2400*, 2012.
[11] S. Kumar, M. Prateek, N. J. Ahuja, and B. Bhushan, "DE-LEACH: Distance and Energy Aware LEACH," *arXiv preprint arXiv:1408.2914*, 2014.
[12] N. R. Roy and P. Chandra, "A Note on Optimum Cluster Estimation in LEACH Protocol," *IEEE Access*, vol. 6, pp. 67745–67753, 2018.
[13] Salar Essa and Ahmed S. Salih, "An Improvement on LEACH Protocol for Wireless Sensor Network," *Proceedings of the 2021 International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, Iraq, pp. 1-6, Oct. 2021.
[14] Bhupesh B. Lonkar and Swapnili Karmore, "Recent Advancements on Energy-Saving LEACH Protocol in Wireless Sensor Network—Review," in *Proceedings of the International Conference on Intelligent Computing and Networking*, Singapore, pp. 1-15, 2023.
[15] S. Sharma and S. K. Sharma, "LEACH Protocol in Wireless Sensor Network: A Survey," *International Journal of Computer Science and Information Technologies*, vol. 7, no. 4, pp. 1-5, 2016.
[16] Jong-Yong Lee, Kye-Dong Jung, Seok-Jae Moon, and Hwa-Young Jeong, "Improved LEACH: A Modified LEACH for Wireless Sensor Network," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 1-18, 2017
[17] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, "Improving Network Longevity in Wireless Sensor Networks Using an Evolutionary Optimization Approach," *Intelligent Automation & Soft Computing*, vol. 28, no. 3, pp. 603–616, 2021.
[18] S. Essa and A. S. Salih, "An Improvement on LEACH Protocol for Wireless Sensor Network," in *Proceedings of the 2021 International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, Iraq, Oct. 2021, pp. 1–6.

[19] M. K. Singh, D. Kumar, and M. P. Singh, "EACR-LEACH: Energy-Aware Cluster-based Routing Protocol for WSN Based IoT," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 47208, 2022.
[20] A. K. Sahoo, S. K. Mohapatra, and S. K. Padhy, "An Energy-Efficient Protocol for Internet of Things Based Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 75, no. 2, pp. 2397–2412, 2023.
[21] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
[22] A. K. Sharma and R. K. Pateriya, "A Comparison of LEACH-Like Protocols to Improve Power Efficiency in Wireless Sensor Networks," in *Proceedings of the International Conference on Intelligent Computing and Networking*, Singapore, 2023, pp. 1–15.
[23] L. Qing, Q. Zhu, and M. Wang, "Design of a Distributed Energy-Efficient Clustering Algorithm for Heterogeneous Wireless Sensor Networks," *Computer Communications*, vol. 29, no. 12, pp. 2230–2237, 2006.
[24] M. S. Khan, M. A. Jan, and X. He, "Rao Algorithms-Based Structure Optimization for Heterogeneous Wireless Sensor Networks," *Computers, Materials & Continua*, vol. 78, no. 1, pp. 1–20, 2023.
[25] A. K. Sharma and R. K. Pateriya, "Energy Efficiency Improvement in LEACH Protocol for Wireless Sensor Network," *International Journal of Recent Technology and Engineering*, vol. 9, no. 2, pp. 1–5, 2020.
[26] J.-Y. Lee, K.-D. Jung, S.-J. Moon, and H.-Y. Jeong, "Improved LEACH: A Modified LEACH for Wireless Sensor Network," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 234-242, 2017.
[27] Jaleel, K. A., & Khan, M. A. (2025). An Energy-Efficient Hybrid LEACH Protocol that Enhances the Lifetime of Wireless Sensor Networks. *Engineering, Technology & Applied Science Research*, 15(1), 19364-19369.
[28] Sharmin, A., Anwar, F., Motakabber, S. M. A., & Hashim, A. H. A. (2022). A Secure Trust Aware ACO-Based WSN Routing Protocol for IoT. *Advances in Science, Technology and Engineering Systems Journal*, 7(3), 95-105.
[29] Yoon, C., Cho, S., & Lee, Y. (2024). Extending WSN Lifetime with Enhanced LEACH Protocol in Autonomous Vehicles Using Improved K-Means and Advanced Cluster Configuration Algorithms. *Applied Sciences*, 14(24), 11720.