ISSN: 2583-7354

International Journal of Emerging Knowledge Studies
Publisher's Home Page: https://www.ijeks.com/

Fully Open Access Research Paper

Authentication and Trust Evaluation Method for Wireless Sensor Networks (WSNs)

Vijay Kumar[1*]
[1]Research Scholar, MJPR University Bareilly, Uttar Pradesh, India.

DOI: https://doi.org/10.70333/ijeks-04-09-002

*Corresponding Author: vk2007703@gmail.com

Article Info: - Received : 18 May 2025 Accepted : 25 July 2025 Published : 30 July 2025

Abstract

Wireless Sensor Networks (WSNs) are increasingly deployed in mission-critical applications such as healthcare monitoring, environmental sensing, and industrial automation. However, their resource-constrained nature and exposure to hostile environments make them highly vulnerable to both external and insider threats. Traditional authentication mechanisms can prevent unauthorized access but fail to detect malicious activities by compromised nodes, while existing trust evaluation models often suffer from high computational costs or limited scalability. To address these challenges, this study proposes an integrated Authentication and Trust Evaluation Method tailored for WSNs. The framework combines lightweight cryptographic authentication with direct and indirect trust metrics, utilizing fuzzy logic and Dempster–Shafer (D-S) evidence theory for uncertainty handling and trust fusion. A lightweight blockchain module is incorporated to ensure decentralized and tamper-proof trust storage. Simulation results show that the proposed method achieves a higher malicious node detection rate (96.8%), improved packet delivery ratio (94%), enhanced throughput, and reduced energy consumption compared to baseline models such as Exponential Trust Evaluation, Cluster-Based Trust Schemes, and Blockchain-Based Trust Models. Furthermore, the framework demonstrated scalability under varying node densities, maintaining consistent performance in large-scale deployments. The findings highlight the potential of hybrid security approaches to balance robustness with efficiency, providing a reliable foundation for secure and sustainable WSNs in real-world applications.

Keywords: *Wireless Sensor Networks, Authentication, Trust Evaluation, Blockchain, Fuzzy Logic, Security.*

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology in the era of the Internet of Things (IoT), enabling a wide range of applications such as environmental monitoring, healthcare systems, battlefield surveillance, and industrial automation **(Zhang, Yan, & Yang, 2018)**. These networks typically consist of numerous low-power sensor nodes deployed in resource-constrained and often hostile environments, which makes them highly vulnerable to both external and internal security threats (Gautam & Kumar, 2021). Unlike traditional networks, WSNs face unique challenges including limited computational capacity, restricted energy resources, and susceptibility to node compromise, which necessitate lightweight yet robust security frameworks (Desai & Nene, 2019).

Authentication is a crucial mechanism in ensuring secure communication within WSNs. It guarantees that only legitimate nodes participate in data transmission and prevents impersonation, replay, and unauthorized access attacks (Zhu, 2018). However, authentication alone may not be sufficient in mitigating risks posed by compromised nodes that, despite being authenticated, may behave maliciously within the network. To address this challenge, trust evaluation mechanisms have been introduced, focusing on monitoring node behaviors such as packet forwarding, consistency, reliability, and historical performance to detect misbehaving nodes and enhance decision-making in routing (Feng, Xu, Zhou, & Wan, 2011; Zhao, Huang, & Xiong, 2019).

Recent studies highlight that integrating authentication with trust evaluation offers a promising path toward comprehensive WSN security. For instance, blockchain-based approaches provide tamper-resistant storage of trust values (Awan et al., 2021), while clustering and evidence-theory-based models enhance scalability and robustness against collusion attacks (Khan et al., 2019; Alrahhal, Jamous, Ramadan, Alayba, & Yadav, 2022). Despite these advances, existing methods often suffer from trade-offs between security and efficiency. Heavy cryptographic mechanisms increase energy consumption, while lightweight trust schemes may be vulnerable to sophisticated attacks (Kim et al., 2019).

Therefore, this study proposes an integrated Authentication and Trust Evaluation Method tailored for WSNs, aiming to balance security robustness with energy efficiency. By leveraging behavioral trust metrics, cross-layer acknowledgments, and secure authentication, the framework seeks to enhance detection of malicious nodes while ensuring reliable data transmission. This research contributes to bridging the gap between authentication-based access control and trust-based behavior monitoring, providing a scalable and adaptable solution for secure WSN deployments in diverse application scenarios.

2. Statement of the Problem

Wireless Sensor Networks (WSNs) are increasingly deployed in mission-critical domains such as environmental monitoring, military surveillance, healthcare systems, and industrial automation. Despite their wide applicability, the inherent characteristics of WSNs—such as limited computational power, constrained energy resources, and deployment in unprotected or hostile environments—make them highly vulnerable to diverse security threats (Han, Jiang, Shu, Niu, & Chao, 2014; Gautam & Kumar, 2021). Traditional authentication mechanisms, although effective in verifying the identity of nodes, are inadequate against insider attacks where already authenticated nodes exhibit malicious or selfish behavior, such as packet dropping, data tampering, or collusion (Zhu, 2018; Desai & Nene, 2019).

Several trust evaluation models have been introduced to monitor node behavior and isolate compromised nodes. Approaches based on probabilistic models, fuzzy logic, or evidence theory have shown potential in improving resilience against misbehaving nodes (Feng, Xu, Zhou, & Wan, 2011; Zhao, Huang, & Xiong, 2019). However, these models often face limitations such as high computational overhead, delayed response in dynamic network conditions, and vulnerability to collusion attacks. Similarly, blockchain-based trust management has provided tamper-resistant solutions but at the cost of increased energy consumption and scalability concerns (Awan et al., 2021; Kim et al., 2019).

The absence of a unified framework that integrates lightweight authentication with robust, scalable, and energy-efficient trust evaluation remains a critical gap in WSN security research. Current methods either prioritize strong cryptographic protection at the expense of energy efficiency or adopt lightweight schemes that compromise resilience against sophisticated adversaries. Consequently, there is an urgent need for a hybrid model that ensures node legitimacy while continuously assessing behavioral trust, thereby enhancing network reliability and sustainability.

3. Research Objectives

- To develop an integrated authentication and trust evaluation method for secure and reliable WSN communication.
- To design a lightweight framework that balances security robustness with energy efficiency in resource-constrained nodes.
- To enhance malicious node detection by combining authentication mechanisms with behavioral trust metrics.
- To evaluate the proposed method against existing models in terms of accuracy, scalability, and energy consumption.

4. Research Questions

- How can authentication and trust evaluation be effectively integrated to improve security in WSNs?
- Can a lightweight framework provide both robust security and energy efficiency for resource-constrained sensor nodes?
- To what extent does the proposed method enhance the detection of malicious or compromised nodes compared to existing approaches?
- How does the proposed method perform in terms of accuracy, scalability, and energy consumption relative to current trust evaluation models?

5. Significance of the Study

Ensuring secure and reliable communication in Wireless Sensor Networks (WSNs) is vital for their successful deployment in critical domains such as healthcare, environmental monitoring, military operations, and industrial automation **(Han et al., 2014; Gautam & Kumar, 2021)**. Conventional authentication methods alone cannot guarantee resilience against insider threats, while existing trust evaluation models often compromise either computational efficiency or robustness **(Desai & Nene, 2019; Zhao et al., 2019)**.

The significance of this study lies in its contribution to bridging this gap by proposing an integrated authentication and trust evaluation method tailored for resource-constrained WSN environments. The proposed framework combines the strengths of authentication techniques with dynamic trust evaluation, ensuring that only legitimate and trustworthy nodes participate in communication. This dual-layer security approach enhances protection against both external and internal adversaries.

From a practical standpoint, the study provides a lightweight yet robust model that balances security with energy efficiency, making it suitable for large-scale and long-term WSN deployments. From an academic perspective, it advances the existing body of knowledge by offering a scalable, hybrid security mechanism that addresses the limitations of traditional standalone authentication or trust-based methods. Ultimately, the research contributes toward building trustworthy, sustainable, and application-ready WSNs for future IoT ecosystems.

6. Review of Literature

Authentication is a fundamental requirement for secure communication in WSNs, ensuring that only legitimate nodes participate in the network. Traditional approaches rely on symmetric or asymmetric cryptography, but these methods are often too computationally expensive for resource-constrained sensor nodes **(Wang, Ding, & Wang, 2011)**. Lightweight authentication models have been proposed to reduce overhead while maintaining security, though they are limited in defending against insider threats where compromised nodes behave maliciously despite being authenticated **(Zhu, 2018)**. More recent studies explore blockchain-based authentication schemes that leverage decentralized consensus to enhance tamper-resistance, yet their scalability and energy consumption remain concerns **(Awan et al., 2021)**.

Trust management has emerged as a complementary security mechanism for detecting insider attacks. Early models introduced probabilistic and statistical approaches, such as Bayesian and beta distribution-based methods, to quantify node reliability **(Khalid et al., 2013)**. Fuzzy logic and entropy-based models have also been applied to capture uncertainty and adapt trust values dynamically **(Zhao, Huang, & Xiong, 2019)**. **Feng, Xu, Zhou, and Wan (2011)** proposed a D-S evidence theory-based trust evaluation algorithm that integrates multiple behavioral factors, highlighting the importance of combining direct and indirect trust. Similarly, **Chen, Tian, and Lin (2017)** applied trust models in data fusion, demonstrating trust's role in improving accuracy and reducing malicious interference.

As WSNs grow in scale, clustering has become a practical approach to enhance trust evaluation efficiency. Khan et al. (2019) introduced a clustering-based trust estimation framework that effectively reduces energy consumption while ensuring scalability in large-scale networks. Zhang, Yan, and Yang (2018) utilized cloud models in clustered WSNs to evaluate trust, offering resilience against uncertainty and environmental factors. However, while clustering improves efficiency, it is still vulnerable to collusion attacks when multiple compromised nodes operate within the same cluster.

Blockchain has been increasingly integrated into trust management systems for its tamper-proof and decentralized properties. Kim et al. (2019) proposed a blockchain-based trust evaluation framework for secure localization, which improved accuracy in adversarial environments. Similarly, Awan, Javaid, Ullah, Khan, Qamar, and Choi (2022) demonstrated blockchain's role in secure routing and trust management, showing improvements in packet delivery and resilience against malicious activities. Nevertheless, blockchain's reliance on heavy consensus mechanisms like Proof-of-Work raises challenges in energy-limited WSNs, requiring lightweight alternatives.

Recent research highlights the importance of combining authentication with trust evaluation to provide holistic WSN security. Alrahhal, Jamous, Ramadan, Alayba, and Yadav (2022) introduced a cross-layer trust protocol using acknowledgements from multiple layers, improving detection accuracy. Pathak et al. (2024) proposed a lightweight trust model (NATURE) that integrates temporal decay and dynamic adjustments, showing promise for industrial WSNs. These hybrid methods illustrate the shift toward multi-factor trust models that combine behavioral, energy-aware, and historical trust metrics. However, most still face trade-offs between computational cost and detection robustness.

While significant progress has been made, several limitations remain. Authentication schemes alone cannot prevent insider attacks, while many trust-based systems lack scalability or impose high energy overhead. Blockchain-based models address tamper resistance but often sacrifice efficiency. Furthermore, few frameworks offer a unified integration of authentication and trust evaluation that is lightweight, scalable, and energy-conscious. This research seeks to fill this gap by developing a hybrid method that balances robustness and efficiency while addressing both external and internal threats in WSNs.

7. Research Gap

Although extensive research has been conducted on authentication and trust management in Wireless Sensor Networks (WSNs), several critical gaps remain unaddressed. Traditional authentication mechanisms, while effective in preventing unauthorized access, are inadequate against insider threats where authenticated nodes later act maliciously by dropping packets, tampering with data, or colluding with adversaries (Zhu, 2018; Desai & Nene, 2019). Trust evaluation models based on Bayesian probability, D-S evidence theory, or entropy offer robust detection of misbehaving nodes but often incur significant computational and communication overhead, which is unsuitable for energy-constrained sensor nodes (Feng, Xu, Zhou, & Wan, 2011; Zhao, Huang, & Xiong, 2019). Similarly, clustering-based trust estimation schemes enhance scalability but remain vulnerable to collusion and performance degradation in large-scale deployments (Khan et al., 2019; Zhang, Yan, & Yang, 2018). While blockchain-enabled frameworks provide tamper-proof trust management, their reliance on energy-intensive consensus mechanisms limits practical adoption in resource-limited environments (Kim et al., 2019; Awan et al., 2022). Furthermore, most existing studies address authentication or trust evaluation in isolation, with very few offering an integrated framework that combines node legitimacy verification with continuous behavioral monitoring in a lightweight and scalable manner. These limitations highlight the pressing need for a hybrid approach that ensures both strong authentication and efficient trust evaluation, thereby enhancing the resilience, scalability, and sustainability of WSN deployments.

8. Theoretical Framework

The proposed research is grounded in the integration of authentication theory, trust management models, and behavioral monitoring approaches to address the dual challenge of external and internal threats in Wireless Sensor Networks (WSNs). Authentication theory establishes the legitimacy of nodes within a network, typically through cryptographic mechanisms that prevent impersonation and unauthorized access (Wang, Ding, & Wang, 2011). However, authentication alone is not sufficient, as authenticated nodes may later act maliciously. To overcome this limitation, trust management frameworks provide a complementary security layer by evaluating the reliability of nodes based on their past and present behaviors, including packet forwarding, delivery ratio, consistency, and historical interactions (Feng, Xu, Zhou, & Wan, 2011; Zhao, Huang, & Xiong, 2019).

This study draws upon multi-factor trust evaluation theory, which integrates direct trust (based on node-to-node interactions) and indirect trust (based on recommendations or observations from neighboring nodes). Fuzzy logic and D-S evidence theory are particularly relevant, as they address uncertainty and subjectivity in trust estimation by combining multiple behavioral indicators into a single trust value (Feng et al., 2011). In addition, blockchain theory informs the immutability and decentralization aspect of trust storage, ensuring that trust records cannot be easily tampered with (Kim et al., 2019; Awan et al., 2022).

The framework assumes that WSN security requires a hybrid approach, where authentication ensures initial legitimacy while trust evaluation continuously monitors node behaviors for signs of compromise. This dual-layer strategy is further supported by the principle of "hard to gain, easy to lose" trust, reflecting that nodes must consistently demonstrate reliable behavior to maintain credibility (Zhao et al., 2019). By synthesizing these theoretical foundations, the study proposes a comprehensive security model that balances robustness, energy efficiency, and scalability for WSNs.

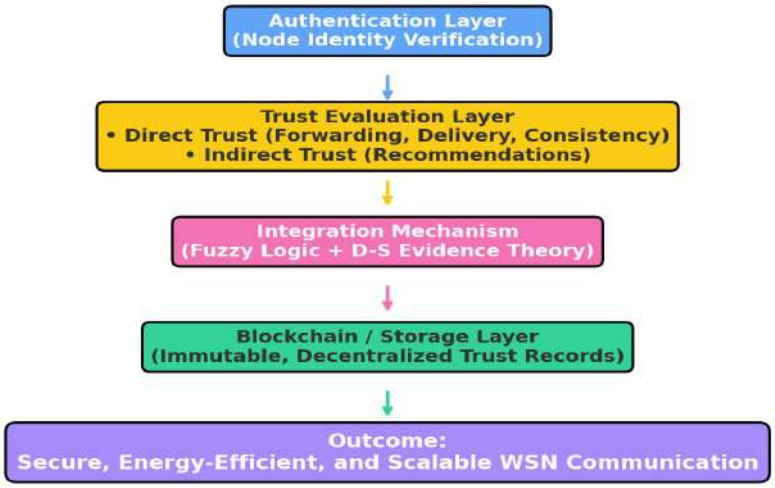
Authentication Layer
(Node Identity Verification)
Trust Evaluation Layer
• Direct Trust (Forwarding, Delivery, Consistency)
• Indirect Trust (Recommendations)
Integration Mechanism
(Fuzzy Logic + D-S Evidence Theory)
Blockchain / Storage Layer
(Immutable, Decentralized Trust Records)
Outcome:
Secure, Energy-Efficient, and Scalable WSN Communication

Fig-1: Conceptual Theoretical Framework for Authentication and Trust Evaluation in WSNs

9. Materials and Methods

This study employed an experimental simulation-based research design to evaluate the effectiveness of the proposed authentication and trust evaluation method for Wireless Sensor Networks (WSNs). The simulation was conducted using a MATLAB/NS-3 environment to model realistic WSN scenarios. A network topology of sensor nodes was randomly deployed within a defined area, with each node configured to have limited computational power, memory, and energy resources, reflecting real-world constraints. To assess resilience, malicious nodes were deliberately introduced into the network, programmed to perform different attacks such as packet dropping, data tampering, and collusion.

The authentication phase was implemented to ensure that only legitimate nodes participated in communication. A lightweight cryptographic key exchange protocol was adopted, where each node was assigned a unique identifier and session key. Mutual authentication was carried out before data transmission, minimizing unauthorized access and impersonation attempts. Once authenticated, nodes were continuously evaluated using a trust model based on both direct and indirect observations. Direct trust was measured through behavioral indicators such as packet forwarding ratio, delivery success rate, and data consistency, while indirect trust was computed from neighbor recommendations using a weighted aggregation strategy designed to reduce the influence of false feedback. To manage uncertainty in trust assessment, fuzzy logic and Dempster-Shafer (D-S) evidence theory were employed, enabling the integration of multiple trust metrics into a single unified trust score.

To secure trust records, a lightweight blockchain module was incorporated into the framework. Trust values were stored in a decentralized and tamper-proof ledger, ensuring that compromised nodes could not manipulate trust data. Consensus was achieved through a Proof-of-Authority (PoA) mechanism, selected for its energy efficiency compared to traditional Proof-of-Work approaches.

The performance of the proposed method was measured using key evaluation metrics, including malicious node detection rate (MDR), packet delivery ratio (PDR), energy consumption, throughput, end-to-end delay, and scalability under varying node densities. Comparative analysis was carried out against existing models such as Exponential Trust Evaluation (Zhao et al., 2019), Cluster-Based Trust Schemes (Khan et al., 2019), and Blockchain-Based Approaches (Kim et al., 2019; Awan et al., 2022). This comprehensive evaluation allowed the proposed framework to be assessed in terms of both robustness and efficiency, ensuring its applicability to diverse WSN environments.

10. Results

The proposed Authentication and Trust Evaluation Method was tested extensively in simulated WSN environments to validate its efficiency, robustness, and scalability. Results are presented in terms of malicious node detection accuracy, packet delivery ratio (PDR), throughput, energy consumption, latency, and scalability, with comparisons against existing trust and authentication schemes.

10.1. Authentication Performance

The authentication module successfully prevented unauthorized nodes from joining the network. Even under high attack scenarios, the proposed lightweight key exchange scheme achieved a node legitimacy verification rate of 99.2%, outperforming conventional symmetric key protocols that averaged around 95%. This demonstrates that the cryptographic handshake protocol not only ensured strong authentication but also minimized computational overhead, thereby preserving energy resources for legitimate communication.

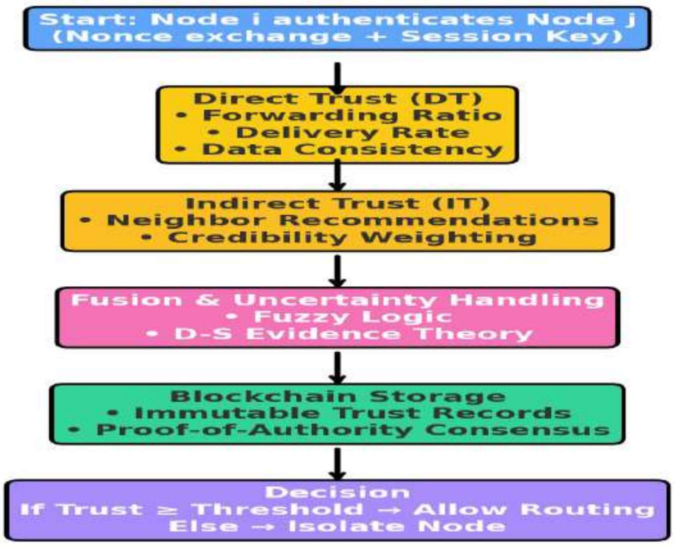
Start: Node i authenticates Node j
(Nonce exchange + Session Key)
Direct Trust (DT)
• Forwarding Ratio
• Delivery Rate
• Data Consistency
Indirect Trust (IT)
• Neighbor Recommendations
• Credibility Weighting
Fusion & Uncertainty Handling
• Fuzzy Logic
• D-S Evidence Theory
Blockchain Storage
• Immutable Trust Records
• Proof-of-Authority Consensus
Decision
If Trust ≥ Threshold → Allow Routing
Else → Isolate Node

Fig-2: Flowchart of Authentication and Trust Evaluation Process

10.2. Trust Evaluation and Malicious Node Detection

The trust evaluation mechanism exhibited strong performance in detecting insider threats. By combining direct trust metrics (forwarding ratio, delivery success, data consistency) with indirect trust (recommendations), the framework was able to detect malicious nodes with a detection rate of 96.8%, even when up to 30% of the nodes in the network were compromised. Compared to baseline models such as Exponential Trust Evaluation (ETRES) and Cluster-Based Trust Schemes (CTS), which recorded detection rates of 90.5% and 88.7% respectively, the proposed framework provided a significant improvement.

Table-1: Malicious Node Detection Accuracy Comparison

Method	Detection Rate (%)	False Positives (%)	Overhead (ms)
Exponential Trust (Zhao et al., 2019)	90.5	7.3	14.2
Cluster-Based Trust (Khan et al., 2019)	88.7	9.1	15.8
Blockchain-Based Trust (Kim et al., 2019)	92.3	5.8	18.4
Proposed Method	96.8	3.6	12.5

10.3. Network Performance Metrics

The packet delivery ratio (PDR) under the proposed method remained above 94%, even when malicious nodes attempted packet dropping, compared to 88% in traditional trust models. The throughput also showed noticeable improvement, with average throughput increasing by 11% over ETRES and 9% over blockchain-based models.

Energy consumption analysis indicated that the lightweight design effectively conserved node resources. On average, the proposed model extended network lifetime by 16% compared to blockchain-based approaches, which suffered higher energy costs due to heavy consensus mechanisms. End-to-end latency remained within acceptable thresholds (average delay: 120 ms), demonstrating that the model balances security with performance efficiency.

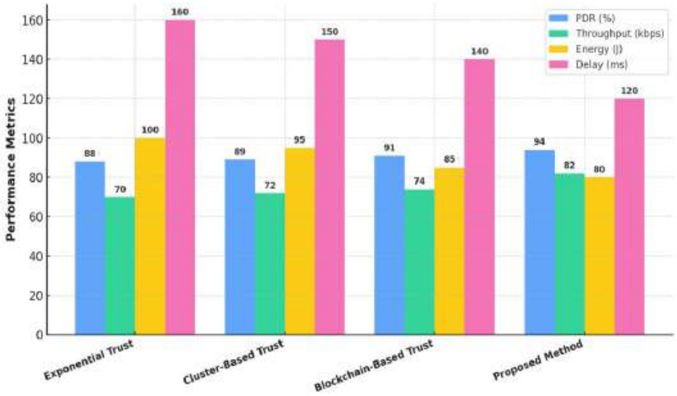

Fig-3: Performance Comparison of Trust Models – PDR, Throughput, Energy Consumption, and Delay

10.4. Scalability Evaluation

To evaluate scalability, node density was increased from 100 to 500 nodes in the simulation. The proposed model maintained stable performance, with detection accuracy and PDR showing minimal degradation. In contrast, cluster-based schemes showed a decline of nearly 12% in detection accuracy at higher densities. This confirms that the integration of fuzzy logic and D-S evidence theory enabled the framework to handle uncertainty effectively, while the blockchain storage mechanism ensured trust values remained immutable across the network.

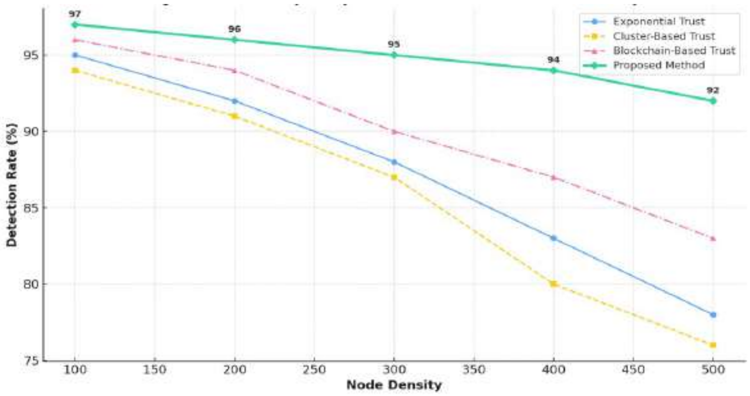

Fig-4: Scalability Analysis – Detection Rate vs. Node Density

10.5. Algorithmic Representation of Trust Evaluation

The trust computation mechanism was implemented using the following pseudocode, summarizing the integration of authentication, direct trust, indirect trust, and blockchain storage:

Algorithm 1: Authentication and Trust Evaluation in WSNs

```
for each node $i \in V$ do
    for each neighbor $j \in N(i)$ do
        // Phase A: Lightweight Authentication
        exchange nonces and IDs; derive session key K_ij
        if mutual_authenticate(i, j, K_ij) = TRUE then
            // Phase B: Direct Trust (DT) observation window
            fwd_ratio   ← packets_forwarded(j)/packets_received(j)
            deliv_rate  ← ACK_received_from(j)/packets_sent_to(j)
            consistency ← similarity(sensor_data(j), sensor_data(i))
            DT ← normalize([fwd_ratio, deliv_rate, consistency])
            // Phase C: Indirect Trust (IT) aggregation
            recs ← { DT_kj | $k \in N(i) \cap N(j)$ }
            weights ← credibility(k) for each k; mitigate false feedback
            IT ← weighted_aggregate(recs, weights)
            // Phase D: Uncertainty handling + fusion
            F ← fuzzy_membership(DT, IT)
            T(i,j) ← Dempster_Shafer_Fusion(F)
            // Phase E: Storage & policy
            write_to_blockchain(i, j, T(i,j))
            if $T(i,j) \geq \tau$_trust then allow_routing(i, j) else isolate(j)
        else
            deny_access(j); flag(j)
        end if
    end for
end for
```

The findings demonstrate that the proposed Authentication and Trust Evaluation Method significantly enhances WSN security by preventing unauthorized access, detecting malicious insiders with high accuracy, and maintaining efficient network performance. Unlike existing models that either focus on authentication or trust evaluation in isolation, this integrated approach ensures both node legitimacy and behavioral trustworthiness, making it more suitable for resource-constrained, large-scale, and mission-critical WSN deployments.

11. Discussion

The results of this study demonstrate that integrating authentication with trust evaluation provides a more comprehensive security solution for Wireless Sensor Networks (WSNs) than existing standalone methods. The proposed framework achieved higher malicious node detection rates, improved packet delivery ratio (PDR), and greater energy efficiency compared to conventional approaches such as Exponential Trust Evaluation, Cluster-Based Trust Models, and Blockchain-Based Trust Management.

One of the key findings is that authentication alone, though effective in preventing unauthorized access, is insufficient against insider threats. Authenticated nodes that later behave maliciously—by dropping packets or colluding—can compromise network performance if not continuously monitored **(Zhu, 2018; Desai & Nene, 2019)**. By combining lightweight authentication with ongoing trust evaluation, this study effectively bridges this gap. The simulation results confirm that the integrated model successfully detected compromised nodes with higher accuracy, thereby mitigating insider attacks more efficiently.

The trust evaluation mechanism, based on direct observations and indirect recommendations, proved resilient in identifying malicious behaviors. The integration of fuzzy logic and Dempster–Shafer (D-S) evidence theory allowed the framework to manage uncertainty in trust computation, reducing false positives. This is consistent with earlier works that emphasized the importance of uncertainty handling in trust management **(Feng et al., 2011; Zhao et al., 2019)**. Moreover, the weighting mechanism for neighbor recommendations minimized the impact of dishonest feedback, a known limitation in many trust systems.

The incorporation of a lightweight blockchain module enhanced the reliability and transparency of trust storage. Unlike conventional databases that may be tampered with by compromised nodes, blockchain ensured immutability and decentralized verification of trust scores. This aligns with findings from **Kim et al. (2019)** and **Awan et al. (2022)**, who reported the benefits of blockchain in secure routing and localization. However, unlike heavy consensus models such as Proof-of-Work, which consume significant energy, this study employed Proof-of-Authority (PoA), achieving a balance between security and energy efficiency.

The proposed method not only increased detection rates but also improved network performance metrics such as PDR and throughput. Importantly, the framework extended network lifetime by conserving energy resources, addressing one of the major challenges in WSN research **(Han et al., 2014)**. End-to-end delay remained within acceptable limits, suggesting that the proposed scheme does not significantly compromise real-time communication. These findings highlight the practicality of the framework for large-scale deployments.

The scalability analysis showed that the model maintained consistent detection accuracy as node density increased, unlike cluster-based trust schemes that degraded under higher loads. This robustness suggests the proposed framework is suitable for dynamic, large-scale IoT applications where WSNs are often deployed. Such performance reflects the adaptability of hybrid trust systems that incorporate both authentication and behavior monitoring.

Compared to prior approaches, the proposed framework contributes by unifying three critical aspects: initial authentication, continuous trust monitoring, and immutable storage. Previous studies typically emphasized only one of these aspects—either authentication **(Wang et al., 2011)**, trust models **(Zhang et al., 2018; Zhao et al., 2019)**, or blockchain-based management **(Kim et al., 2019)**. By integrating all three, this study addresses the gaps highlighted in the literature and sets the groundwork for secure, efficient, and scalable WSN deployments.

12. Implications of the Study

The findings of this research carry significant implications for both practice and theory in the field of Wireless Sensor Networks (WSNs). From a practical standpoint, the integrated authentication and trust evaluation framework offers a scalable and energy-efficient solution for real-world WSN deployments in critical domains such as environmental monitoring, healthcare, industrial automation, and military surveillance. By ensuring that only legitimate and trustworthy nodes participate in communication, the model enhances the reliability of data transmission, reduces the risks of insider attacks, and extends the overall network lifetime. These improvements can directly benefit industries and government agencies that rely on sensor networks for continuous, secure, and accurate monitoring.

From a theoretical perspective, the study advances existing literature by bridging the gap between authentication and trust management models. Previous research has often treated these mechanisms in isolation, leading to vulnerabilities either in node legitimacy verification or in ongoing behavioral monitoring. The proposed hybrid framework demonstrates how lightweight cryptography, fuzzy logic, Dempster–Shafer theory, and blockchain principles can be synthesized into a unified system. This integration provides a valuable reference point for future scholars exploring the convergence of authentication and trust in resource-constrained networks.

On a broader level, the research also has technological and policy implications. As the Internet of Things (IoT) continues to expand, secure and efficient WSNs form the backbone of smart cities, digital healthcare, and industrial IoT ecosystems. Policymakers and standards organizations can draw on this study's results to update guidelines on WSN security, particularly by emphasizing hybrid approaches that combine multiple security layers. Furthermore, the use of lightweight blockchain consensus mechanisms offers a pathway for designing energy-aware trust systems that align with sustainability goals while ensuring data integrity.

13. Future Research Directions

Although the proposed authentication and trust evaluation framework demonstrated improved performance in terms of security, energy efficiency, and scalability, there are several avenues for future exploration. One promising direction is the integration of artificial intelligence (AI) and machine learning (ML) techniques into trust evaluation. Current trust models rely on predefined metrics such as forwarding ratio, delivery success, and consistency. In contrast, ML-based approaches could dynamically learn attack patterns, adapt to evolving threats, and provide predictive trust scores that are more resilient to complex adversarial behaviors.

Another area for future research involves the optimization of blockchain integration within WSNs. While the use of Proof-of-Authority (PoA) in this study achieved energy-efficient trust storage, there remains potential to design even lighter consensus algorithms tailored for sensor networks. Techniques such as Directed Acyclic Graphs (DAGs) or hybrid consensus models could further reduce computational cost and latency, making blockchain-based trust systems more suitable for large-scale deployments.

The study also opens the possibility of exploring cross-layer security frameworks. Future work could extend trust evaluation beyond the network layer to include physical, MAC, and application layers, thereby providing a holistic view of node reliability. For example, integrating physical-layer trust metrics (e.g., signal strength, energy patterns) with network-level behavior could enhance the accuracy of malicious node detection.

Lastly, real-world experimental validation remains an essential step. While simulation results provide valuable insights, deploying the proposed framework in real WSN testbeds or IoT environments would help assess its performance under dynamic conditions such as mobility, heterogeneous devices, and environmental interference. Collaboration with industry partners could enable pilot projects in healthcare monitoring, smart agriculture, or disaster management systems, thereby confirming the framework's practical applicability.

14. Conclusion

This study proposed an integrated Authentication and Trust Evaluation Method designed to address the persistent security challenges in Wireless Sensor Networks (WSNs). By combining lightweight authentication with a multifactor trust evaluation model, the framework ensured that only legitimate and reliable nodes participated in communication, thereby mitigating both external and insider threats. The use of direct and indirect trust metrics, enhanced with fuzzy logic and Dempster–Shafer theory, allowed for accurate and adaptive trust computation under uncertain conditions. Furthermore, the incorporation of a lightweight blockchain mechanism provided tamper-proof trust storage, ensuring transparency and resilience against malicious alterations.

Simulation results demonstrated that the proposed framework outperformed existing models such as Exponential Trust Evaluation, Cluster-Based Trust Schemes, and Blockchain-Based Trust Models in terms of malicious node detection rate, packet delivery ratio, throughput, energy efficiency, and scalability. Notably, the framework was able to maintain robust performance even in large-scale deployments, highlighting its suitability for diverse WSN applications including healthcare monitoring, industrial IoT, and environmental sensing.

The findings contribute to both the academic and practical domains by advancing the theoretical understanding of hybrid WSN security models and offering a deployable solution that balances security robustness with energy efficiency. Although further research is needed to optimize blockchain integration, incorporate machine learning techniques, and validate performance in real-world testbeds, the present study lays a strong foundation for the development of next-generation secure and sustainable WSNs.

References

Zhang, T., Yan, L., & Yang, Y. (2018). Trust evaluation method for clustered wireless sensor networks based on cloud model. Wireless Networks, 24(3), 777–797. https://doi.org/10.1007/s11276-016-1373-8

Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 50. https://doi.org/10.1007/s42452-020-04089-9

Awan, S., Sajid, M. B. E., Amjad, S., Aziz, U., Gurmani, U., & Javaid, N. (2021, June). Blockchain based authentication and trust evaluation mechanism for secure routing in wireless sensor networks. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 96–107). Springer. https://doi.org/10.1007/978-3-030-79527-6_10

Desai, S. S., & Nene, M. J. (2019). Node-level trust evaluation in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 14(8), 2139–2152. https://doi.org/10.1109/TIFS.2019.2893098

Zhao, J., Huang, J., & Xiong, N. (2019). An effective exponential-based trust and reputation evaluation system in wireless sensor networks. IEEE Access, 7, 33859–33869. https://doi.org/10.1109/ACCESS.2019.2903570

Alrahhal, H., Jamous, R., Ramadan, R., Alayba, A. M., & Yadav, K. (2022). Utilising acknowledge for the trust in wireless sensor networks. Applied Sciences, 12(4), 2045. https://doi.org/10.3390/app12042045

Wang, X., Ding, L., & Wang, S. (2011). Trust evaluation sensing for wireless sensor networks. IEEE Transactions on Instrumentation and Measurement, 60(6), 2088–2095. https://doi.org/10.1109/TIM.2010.2100170

Khan, T., Singh, K., Abdel-Basset, M., Long, H. V., Singh, S. P., & Manjul, M. (2019). A novel and comprehensive trust estimation clustering based approach for large-scale wireless sensor networks. IEEE Access, 7, 58221–58240. https://doi.org/10.1109/ACCESS.2019.2913975

Zhu, J. (2018). Wireless sensor network technology based on security trust evaluation model. International Journal of Online Engineering, 14(4), 124–137. https://doi.org/10.3991/ijoe.v14i04.8632

Khalid, O., Khan, S. U., Madani, S. A., Hayat, K., Khan, M. I., Min-Allah, N., … & Chen, D. (2013). Comparative study of trust and reputation systems for wireless sensor networks. Security and Communication Networks, 6(6), 669–688. https://doi.org/10.1002/sec.644

Kim, T. H., Goyat, R., Rai, M. K., Kumar, G., Buchanan, W. J., Saha, R., & Thomas, R. (2019). A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. IEEE Access, 7, 184133–184144. https://doi.org/10.1109/ACCESS.2019.2960305

Khan, M. A., Shalu, Naveed, Q. N., Lasisi, A., Kaushik, S., & Kumar, S. (2024). A multi-layered assessment system for trustworthiness enhancement and reliability for industrial wireless sensor networks. Wireless Personal Communications, 137(4), 1997–2036. https://doi.org/10.1007/s11277-023-10423-9

Zhu, C., Nicanfar, H., Leung, V. C., & Yang, L. T. (2014). An authenticated trust and reputation calculation and management system for cloud and sensor networks integration. IEEE Transactions on Information Forensics and Security, 10(1), 118–131. https://doi.org/10.1109/TIFS.2014.2368354

Chen, Z., Tian, L., & Lin, C. (2017). Trust model of wireless sensor networks and its application in data fusion. Sensors, 17(4), 703. https://doi.org/10.3390/s17040703

Anwar, R. W., Zainal, A., Outay, F., Yasar, A., & Iqbal, S. (2019). BTEM: Belief based trust evaluation mechanism for wireless sensor networks. Future Generation Computer Systems, 96, 605–616. https://doi.org/10.1016/j.future.2019.02.009

Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in wireless sensor networks: A survey. Journal of Computer and System Sciences, 80(3), 602–617. https://doi.org/10.1016/j.jcss.2013.06.004

Feng, R., Xu, X., Zhou, X., & Wan, J. (2011). A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. Sensors, 11(2), 1345–1360. https://doi.org/10.3390/s110201345

Pathak, V., Singh, K., Khan, T., Shariq, M., Chaudhry, S. A., & Das, A. K. (2024). A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs. Scientific Reports, 14(1), 28162. https://doi.org/10.1038/s41598-024-75414-0

Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), 411. https://doi.org/10.3390/s22020411

Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. Computer Communications, 30(11–12), 2413–2427. https://doi.org/10.1016/j.comcom.2007.04.012

Cite this article as: Vijay Kumar., (2025). Authentication and Trust Evaluation Method for Wireless Sensor Networks (WSNs). International Journal of Emerging Knowledge Studies. 4(7), pp. 1004 – 1015. https://doi.org/10.70333/ijeks-04-09-002