International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 1043-1054
https://doi.org/10.70917/ijcisim-2026-5237
Article

Authentication and Trust Evaluation Method for Wireless Sensor Networks

Vijay Kumar [*1], Dr. Akhtar Husain[2] , Dr. Ashwani Gupta[3]

[1]Research Scholar, CSIT Department, MJP Rohilkhand University Bareilly, India. vk2007703@gmail.com
[2]Associate Professor, CSIT Department, MJP Rohilkhand University, Bareilly, India. akhtarhusain@mjpru.ac.in
[3]Assistant Professor, CSIT Department, MJP Rohilkhand University Bareilly, India. ashwani.gupta@mjpru.ac.in

Abstract: Wireless Sensor Networks (WSNs) have emerged as a crucial technology for applications such as environmental monitoring, healthcare, and military surveillance. However, due to their decentralized architecture, limited computational resources, and open wireless medium, WSNs are highly susceptible to various security threats. The primary problem addressed in this research is the lack of efficient mechanisms for secure authentication and reliable trust evaluation to detect and mitigate malicious node behavior. To overcome this issue, this study proposes an integrated Authentication and Trust Evaluation Method that combines lightweight cryptographic authentication with a dynamic trust management framework. The proposed approach evaluates trust based on parameters such as node reliability, packet forwarding behavior, and data integrity, and updates trust scores in real time. Simulation results indicate that the proposed method significantly enhances security by improving attack detection accuracy, increasing packet delivery ratio, and reducing energy consumption compared to existing techniques. Furthermore, the system effectively isolates malicious nodes, ensuring network stability and data reliability. In conclusion, the proposed model provides a scalable, energy-efficient, and robust solution for securing WSNs against internal and external threats.
Keywords: Wireless Sensor Networks, Authentication, Trust Evaluation, Security and Energy Efficiency

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 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, wireless sensor networks face challenges including limited computational capacity, restricted energy resources, and susceptibility to node compromise, This necessitate lightweight yet robust security frameworks (Desai & Nene, 2019).

Authentication is a crucial mechanism in ensuring secure communication within wireless sensor networks. 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, there mechanisms focus 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, block chain-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).

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.

1.1. Statement of the Problem

Wireless Sensor Networks (WSNs) are increasingly deployed in mission-critical domains like environmental monitoring, military surveillance, healthcare systems, and industrial automation. Despite 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).

A number of trust evaluation models have been presented to monitor node behavior and isolate compromised nodes. These approaches are based on probabilistic models, fuzzy logic, or evidence theory, and shown potential in improving resilience against misbehaving nodes (Feng, Xu, Zhou, & Wan, 2011; Zhao, Huang, & Xiong, 2019). These models often face limitations such as high computational overhead, delayed response in dynamic network conditions, and vulnerability to collusion attacks. 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) like these models.

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. There is an urgent need for a hybrid model that ensures node legitimacy while continuously assessing behavioral trust, thereby enhancing network reliability and sustainability.

1.2. Research Objectives

1 2.1To develop an integrated authentication and trust evaluation method for secure and reliable WSN communication.

1.2.2 To design a lightweight framework that balances security robustness with energy efficiency in resource-constrained nodes.

1.2.3 To enhance malicious node detection by combining authentication mechanisms with behavioral trust metrics.

1.2..4 To evaluate the proposed method against existing models in terms of accuracy, scalability, and energy consumption.

1.3. Significance of the Study

Ensuring secure and reliable communication in Wireless Sensor Networks (WSNs) is vital for their successful deployment in critical domains like 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. It is tailored for resource-constrained WSN environments. The proposed framework combines the strengths of authentication techniques with dynamic trust evaluation. It ensures that only legitimate and trustworthy nodes participate in communication. This dual-layer security approach enhances protection for external and internal adversaries.

From a practical point, the study provides a lightweight yet robust model that balances security with energy efficiency. It makes this model 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.

1.4. Related Work

Authentication is a fundamental requirement for secure communication in WSNs, ensuring that only legitimate nodes participate in the network. Traditional approaches are based on symmetric or asymmetric cryptography, but these methods are computationally expensive for resource-constrained sensor nodes (Wang, Ding, & Wang, 2011). Lightweight authentication models have been proposed to reduce overhead with maintaining security, though they are limited in defending against insider threats where compromised nodes behave maliciously despite being authenticated (Zhu, 2018). 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). Wang et al. (2025) offer a trust models defending against Denial-of-Service (DoS) attacks **in** WSNs, pointing out how trust evaluation methods are applied to detect misbehaving nodes and detailing challenges such as trust threshold settings, evidence extraction, and integration with authentication and routing.

Trust management has emerged as a complementary security mechanism for detecting insider attacks. Early models introduced probabilistic and statistical approaches, 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 Dempster–Shafer evidence theory-based trust evaluation algorithm that integrates multiple behavioral factors. This highlights the importance of combining direct and indirect trust. 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. Clustering improves efficiency; it is still vulnerable to collusion attacks when multiple compromised nodes operate within the same cluster.

Block chain has been increasingly integrated into trust management systems due to its tamper-proof and decentralized properties. Kim et al. (2019) proposed a block chain-based trust evaluation framework for secure localization, which improved accuracy in adversarial environments. Similarly, Awan, Javaid, Ullah, Khan, Qamar, and Choi (2022) demonstrated block chain role in secure routing and trust management, showing improvements in packet delivery and resilience against malicious activities. Nevertheless, block chain 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. Block chain-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.

1.5. Research Gap

Although a large 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, Dempster–Shafer evidence theory, or entropy offer robust detection of misbehaving nodes but often incur significant computational and communication overhead. This 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). Block chain-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). 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.

1.6. Theoretical Frame Work

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 insufficient, above 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 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 Dempster–Shafer 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 proposed 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.

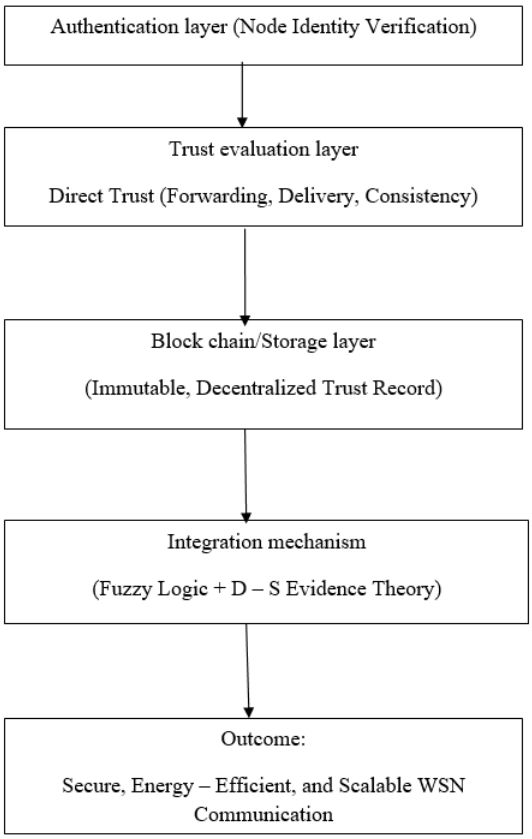

Fig-1: framework for authentication and trust evaluation in WSNs

2. 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 Python reference 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 block chain 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 Block chain-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 WSNs environments.

3. Results

The proposed authentication and trust evaluation method is tested extensively in simulated WSNs environments to validate its efficiency, robustness, and scalability. Results are presented in terms of malicious node (it is a bad node (fake information) in the network that tries to harm the network or other nodes) detection accuracy it shows how accurately the system can find bad nodes in the network.

Detection Accuracy=(Number of correctly detected malicious nodes)/(Total number of actual malicious node s) ×100%

Packet delivery ratio (PDR) - It is the ratio of the number of packets successfully received by destination nodes to the number of packets sent by source nodes.

PDR = (Packets received successfully)/ (Packets sent)×100%

Throughput - Throughput is the amount of data successfully transmitted over a network per unit time.

Energy consumption - Energy consumption is the total amount of energy used by a system or device to perform its operations.

Latency - Latency is the time delay between sending data and receiving it at the destination.

Scalability - Scalability is the ability of a system or network to handle an increasing number of users or nodes without performance degradation with comparisons against existing trust and authentication schemes.

3.1 Authentication Performance

The authentication module successfully prevents unauthorized nodes from joining the network. Even under high attack scenarios, the proposed lightweight key exchange scheme achieves a node legitimacy verification rate of 99.2%, outperforming conventional symmetric key protocols that average 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.

3.2. 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 is able to detect malicious nodes with a method detection rate of 96.8%, even when up to 30% of the nodes in the network are compromised. Compared to baseline models such as An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks (Zhao, et al 2019) and Cluster-Based Trust Schemes (Khan et. al, 2019) and block chain based trust (Kim, et. al 2019) 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 (5)	False position (%)	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
Block chain based trust (Kim et al 2019)	92.3	5.8	18.4
Proposed Method	96.8	3.6	12.5

3.3. Network Performance Matrices

The packet delivery ratio (PDR) under the proposed method remained above 94%, even when malicious nodes attempts packet dropping, compared to 88% in traditional trust models. The throughput also shows noticeable improvement, with average throughput increasing by 11% over ETRES and 9% over block chain-based models. Energy consumption analysis indicates that the lightweight design effectively conserved node resources. On average, the proposed model extends network lifetime by 16% compared to block chain-based approaches, which suffers higher energy costs due to heavy consensus mechanisms. End-to-end latency remains within acceptable thresholds (average delay: 120 ms), demonstrating that the model balances security with performance efficiency.

3.4. Algorithmic Representation of Trust Evaluation

The trust computation mechanism was implemented using the following pseudo code, summarizing the integration of authentication, direct trust, indirect trust, and block chain storage:

Algorithm 1: Authentication and Trust Evaluation in WSNs

Parameters Used

- N → Total number of nodes
- Ti → Trust value of node i
- DS → Direct Success (successful interactions)
- DF → Direct Failure (failed interactions)
- RS → Recommended Success
- RF → Recommended Failure
- α , β → Weight factors ($0 \leq \alpha, \beta \leq 1, \alpha + \beta = 1$)
- Tth → Trust Threshold

Algorithm: Trust Evaluation

Step 1: Initialization

For each node i in N:

Ti = 0.5 (initial neutral trust)

Step 2: Direct Trust Calculation

For each interaction of node i:

Direct Trust (i) = DS / (DS + DF)

Step 3: Indirect (Recommendation) Trust

Indirect Trust (i) = RS / (RS + RF)

Step 4: Total Trust Computation

$Ti = \alpha \times \text{Direct Trust (i)} + \beta \times \text{Indirect Trust (i)}$

Step 5: Node Classification

If $Ti \geq Tth$:

Node is TRUSTED

Else:

Node is MALICIOUS

Step 6: Trust Update (Dynamic)

After every time interval:

Recalculate DS, DF, RS, RF

Update Ti.

4. 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 achieves 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 Block chain-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 reduces 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).

The incorporation of a lightweight block chain module enhances the reliability and transparency of trust storage. Unlike conventional databases that may be tampered with by compromised nodes, block chain 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 block chain 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 increases detection rates but also improves network performance metrics such as PDR and throughput. Importantly, the framework extends network lifetime by conserving energy resources, addressing one of the major challenges in WSN research (Han et al., 2014). End-to-end delay remains 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 shows that the model maintains consistent detection accuracy as node density increases, unlike cluster-based trust schemes that degrade under higher loads. This robustness suggests the proposed framework

is suitable for dynamic, large-scale IoT applications where WSNs are often deploy. 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 emphasizes only one of these aspects—either authentication (Wang et al., 2011), trust models (Zhang et al., 2018; Zhao et al., 2019), or block chain-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 WSNs deployments.

5. 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 block chain 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 Block chain 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 block chain 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.

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 block chain 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 block chain-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.

7.1 Acknowledgement

I would like to express my sincere gratitude to my supervisor, **Dr. Ashwani Gupta**, Department of CSIT, **MJP Rohilkhand University**, Bareilly, India, for his invaluable guidance, continuous encouragement, and insightful suggestions throughout the course of this research work on Authentication and Trust Evaluation Method for Wireless Sensor Networks. His expertise, constructive feedback, and constant motivation greatly contributed to the successful completion of this study.

I am also thankful for **Dr. Karan Singh** SCSS Jawaharlal Nehru University, New Delhi, India and the faculty members and research scholars of the Department of CSIT for their support and cooperation. Their academic discussions and technical inputs have been instrumental in shaping the direction of this work.

I extend my heartfelt appreciation to my family and friends for their unwavering support, patience, and encouragement during the entire research process.

Finally, I acknowledge all those researchers and authors whose scholarly work in the field of Wireless Sensor Networks and trust management has provided a strong foundation for this research.

5.2 Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the publication of this research work entitled "Authentication and Trust Evaluation Method for Wireless Sensor Networks." The research was conducted independently, and no financial, commercial, or personal relationships have influenced the design, analysis, interpretation, or reporting of the study.

No funding agency, organization, or third party had any role in the development of the proposed authentication framework, trust evaluation model, data analysis, or manuscript preparation. The authors confirm that the results presented in this work are original and free from any bias or competing interests.

Appendices

A. System Model

The proposed Authentication and Trust Evaluation scheme is designed for a clustered Wireless Sensor Network (WSN) consisting of sensor nodes (SNs), cluster heads (CHs), and a base station (BS). Sensor nodes are randomly deployed and communicate using multi-hop routing. Due to limited energy and computational resources, lightweight security mechanisms are employed. The base station is assumed to be secure and computationally powerful. The network may contain malicious nodes performing packet dropping or false reporting attack

Appendix B: Mathematical Model for Trust Evaluation

The proposed trust model is based on **Direct Trust (DT)** and **Indirect Trust (IT)**.

1. Direct Trust (DT)

$DTij = Sij / (Sij+Fij)$

Where Sij = Successful interactions between node i and j, Fij = Failed interactions

2. Indirect Trust (IT)

$ITij = 1/n \sum^{n}_{k=1} Tik \times Tkj$

Where: Tik= Trust of node i on recommender k and Tkj= Trust of recommender k on node j

3. Total Trust (TT)

$TTij = \alpha DTij + (1-\alpha)\, ITij$

Where $\alpha \in [0, 1]$ is weight factor

If $TTij < T_{threshold}$ node j is considered malicious.

REFERENCES

1. 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.
2. 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.
3. Wang et al. (2025). A trust models defending against Denial-of-Service (DoS) attacks in WSNs. *Appl.*, 15(6), 3075. https://doi.org/10.3390/app15063075.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.