Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 294–300 *e*-ISSN 2503-426X

A Comprehensive Review of Trust and Reputation-Based Routing Protocols in Wireless Sensor Networks (WSNs): Models, Challenges, and Future Directions

Jatin Gupta[1]*, Dr. Vishal Goyal[2]
[1,2]Department of Computer Science, Punjabi University, Patiala, Punjab, India
*E-mail: jatin.gupta.1988@ieee.org

Article Received: 22 Feb 2025, Revised: 10 April 2025, Accepted:08 May 2025

Abstract: Wireless Sensor Networks (WSNs) are widely used in areas such as environmental monitoring, smart cities, and healthcare. However, due to their open and resource-limited nature, they are highly vulnerable to various security threats, especially from internal malicious nodes. Trust and reputation-based routing has become a popular solution to improve the reliability and security of data transmission in WSNs without relying heavily on encryption. This review paper presents an overview of recent developments in trust-based routing protocols. It classifies different models based on how trust is calculated, the types of trust considered (like direct, indirect, energy, and behavior-based), and how routing decisions are made. The paper also compares traditional lightweight approaches with more advanced machine learning and blockchain-based methods. Key challenges such as detecting smart attacks, maintaining energy efficiency, and adapting to dynamic environments are discussed. Finally, the paper outlines open issues and future research directions for building more secure, adaptive, and energy-efficient trust-aware routing in WSNs.

Keywords: detecting, environments, WSNs, monitoring

INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as a foundational technology for applications ranging from environmental monitoring to military surveillance and smart cities. Despite their versatility, WSNs are particularly susceptible to internal and external security threats due to their distributed architecture, resource constraints, and deployment in unprotected environments [1]. Traditional cryptographic mechanisms, while useful for data confidentiality, fall short in addressing node misbehavior or internal threats such as selfish or malicious routing behavior [2]. To tackle these issues, the research community has shifted towards trust and reputation-based routing protocols that can dynamically assess node behavior and make routing decisions accordingly [3].

Trust-aware routing protocols leverage both direct and indirect observations to evaluate the reliability of nodes. Direct trust is usually built through firsthand interactions, while indirect trust aggregates feedback from neighboring nodes. This dual mechanism enables robust detection of malicious activity such as packet dropping, misrouting, and false data injection [4]. A key strength of these models lies in their adaptability to various attack types, including selective forwarding and on-off attacks, which are difficult to capture with static rule-based security schemes [5].

Reputation systems have been widely integrated into trust-based routing schemes to facilitate secure decision-making. For instance, probabilistic reputation approaches reduce the overhead of continuous monitoring, making them suitable for resource-constrained nodes [6]. However, these systems must balance between responsiveness and energy efficiency. Recent

models attempt to integrate energy-aware trust evaluation, ensuring that nodes with depleted resources are not unnecessarily burdened [7]. Moreover, Bayesian and fuzzy logic-based systems have enhanced the flexibility of trust models in dynamic network environments [8].

A significant challenge in trust and reputation-based WSNs is the scalability and maintenance of trust tables, especially in large-scale deployments. To this end, cluster-based and hierarchical trust models have been introduced, which aggregate trust data at designated cluster heads to reduce communication overhead and improve scalability [9]. These approaches also provide a foundation for hybrid trust computation that combines multiple metrics like energy, delay, and delivery success [10].

The effectiveness of trust-based routing depends heavily on the design of trust update functions and aging mechanisms. Static models fail to reflect recent behavior, while overly dynamic systems may overreact to transient faults. Therefore, hybrid models with adjustable thresholds and decay rates are gaining prominence for their balance between stability and adaptability [11]. Furthermore, simulation studies consistently demonstrate that integrating trust with routing significantly enhances packet delivery ratio, prolongs network lifetime, and reduces the influence of malicious nodes [12].

In conclusion, trust and reputation-based routing represents a promising and evolving frontier in securing WSNs. As network topologies and threats grow more complex, the need for lightweight, adaptive, and energy-aware trust models becomes increasingly critical. This review aims to explore the state-of-the-art developments in trust-based routing for WSNs, identify research gaps, and propose future directions toward achieving secure, reliable, and efficient data transmission in sensor networks.

LITERATURE REVIEW

[13] Hu et al. (2021) proposed the TSRP protocol, a trust-aware secure routing system that calculates a composite trust score from direct and indirect interactions, residual energy, and a volatilization factor. The protocol utilizes multipath routing and selects the best route using metrics like hop count and transmission distance. It showed lower latency and packet loss compared to AODV, reinforcing trust as a reliable defense against blackhole and wormhole attacks. [14] Duan et al. (2014) introduced TSRF, a lightweight framework combining trust metrics and QoS parameters for routing decisions. It tackles compatibility issues between trust and network performance metrics and offers a comprehensive strategy for identifying misbehaving nodes through context-aware trust evaluations. Simulations validated its efficiency and robustness against diverse attacks, highlighting its suitability for smart city deployments. [15] Ahmed et al. (2017) developed LTRP, a lightweight trust-aware protocol integrating node energy, hop count, and dynamic trust evaluation. It effectively isolates malicious nodes while optimizing route stability and minimizing delay. The protocol achieved better throughput and longer network lifetime than traditional schemes, particularly under high attack densities.

[16] Hu et al. (2021) also presented TBSEER, a secure and energy-efficient routing protocol based on adaptive trust calculation. This scheme integrates direct, indirect, and energy-based trust to mitigate attacks like sinkhole and hello floods. It reduces computation

overhead by shifting indirect trust evaluation to the sink, which enhances scalability while minimizing energy usage. [17] Gong et al. (2018) proposed a fine-grained trust model using Markov chains and Bayesian updates. It differentiates between internal node states (e.g., power and traffic) and external behavior to identify compromised nodes. The hybrid trust framework enhanced detection precision and minimized false positives in malicious node identification. [18] Beheshtiasl and Ghaffari (2019) designed a fuzzy logic-based routing protocol that evaluates trust via multidimensional scaling and selects secure paths based on both trust and path optimality. When compared with TARF and TC-BAC, their model outperformed in terms of packet delivery and energy efficiency, showcasing fuzzy systems' adaptability in trust estimation. [19] Renubala and Dhanalakshmi (2014) developed a fuzzy logic-based secure routing method combining energy-aware clustering (BEE-C) with trust evaluation to resist blackhole and flooding attacks. Nodes are marked untrusted if their trust score falls below a threshold, effectively ensuring secure data aggregation. This method resulted in higher packet delivery rates and reduced overhead compared to LEACH and other baselines. [20] Ramamoorthy and Gunavathi (2019) created a novel trust-based protocol designed to counter blackhole attacks by identifying trustworthy paths. It integrates reliability assessment of nodes based on past behaviors, significantly improving delivery and reducing delay. The study highlighted trust as a dynamic metric that adjusts in real-time to network changes. [21] Shilpa and Ambareesh (2018) implemented a trust management system that dynamically adapts to node behaviors in delay-tolerant networks. The proposed scheme monitors both malicious and selfish behaviors, optimizing routing paths to sustain performance. The model demonstrated resilience under misbehavior conditions, showing trust models' applicability beyond real-time WSNs. [22] Han (2021) evaluated the vulnerabilities of WSNs to internal threats and emphasized trust-based mechanisms over traditional encryption. The protocol proposed in this paper relies on behavioral prediction from past observations, enhancing resistance to internal compromises. It shows that trust models are critical to scalable, secure WSN operation in resource-constrained environments.

Ref	**Authors (Year)**	**Method/Approach**	**Strengths**	**Limitations**
[22]	Sharma et al. (2024)	Fusion-based energy-aware clustering with MST routing	Enhances lifetime and clustering accuracy	High optimizer complexity
[23]	Varatharajan et al. (2025)	Evolutionary trust-based energy model	Adaptive and secure routing with energy optimization	Parameter tuning required
[24]	Bekal et al. (2024)	Review of query-driven energy-efficient protocols	Comprehensive analysis of existing strategies	No implementation or simulation
[25]	Ambareesh et al. (2025)	Type-2 fuzzy logic with ensemble selection	Highly accurate trust scores with good energy efficiency	Scalability not deeply evaluated

[26]	Soltani et al. (2023)	PSO-based trust-aware data gathering	Balances energy and trust dynamically	Computational load from PSO
[27]	Ali et al. (2018)	Fuzzy trust estimation protocol	Reliable malicious node detection	Older metrics, not IoT optimized
[28]	Yadav et al. (2017)	Energy-balanced trust-based protocol	Improves delay and load balance	Tested on limited scenarios
[29]	Kaur et al. (2016)	Trust-based secure route discovery	Effective PDR and energy usage	Static WSN focus, lacks mobility support
[30]	Kumar et al. (2014)	Dynamic fuzzy-based secure routing	Multi-metric trust reasoning	Not adaptive to real-time threats
[31]	Maarouf et al. (2009)	CRATER trust evaluation strategy	Introduces RESISTOR reliability index	Very early model, lacks modern validation
[32]	Lv et al. (2018)	ST-GEAR with binomial distribution	DoS resilience, secure communication	Adds significant computation overhead
[33]	Maarouf et al. (2009)	EMPIRE monitoring strategy	Reduces cost of node monitoring	Lacks real-world implementation
[34]	Moya et al. (2009)	Non-deterministic trust routing	Strong protection against insider threats	Complex routing logic
[35]	Taqieddin (2007)	Beta and TLR-based composite trust	Energy-aware trust for secure routing	Specific to early WSN testbed

FINDINGS

1. **Multi-Metric Trust Is Preferred**: Most recent models (e.g., [23], [25], [26]) use combinations of direct trust, indirect trust, energy efficiency, and behavioral patterns to provide more accurate trust scores compared to single-metric approaches.
2. **Fuzzy and Evolutionary Methods Dominate**: Several papers ([22], [25], [30]) utilize fuzzy logic, type-2 fuzzy systems, and swarm intelligence (e.g., PSO, Firefly) to dynamically compute trust values, improving adaptability in dynamic environments.
3. **Energy Consideration Is Still Evolving**: While many models incorporate energy metrics ([22], [23], [26]), only a few explicitly balance trust evaluation frequency and energy preservation. This often leads to a trade-off between security and network lifetime.

4. **Lack of Real-World Validation**: Most works (e.g., [24], [33], [34]) are still simulation-based, with limited real-world deployment or large-scale validation. This questions their practical applicability in IoT or large-scale WSN settings.
5. **Machine Learning Is Emerging**: Only a handful of studies have begun integrating machine learning or cognitive models ([31]) to dynamically learn trust behaviors over time, despite ML's promise for better anomaly detection and trust prediction.
6. **Sophisticated Attacks Remain a Challenge**: On-off attacks, collusion, and internal malicious behavior are only partially addressed in most protocols ([27], [29]), highlighting a persistent vulnerability in trust models.
7. **Standardization Is Lacking**: Trust computation formulas, parameter weights, and evaluation metrics vary widely across papers, making direct comparison and reproducibility difficult.

CONCLUSION

Trust and reputation-based routing continues to evolve as a critical solution for securing Wireless Sensor Networks (WSNs) against a wide array of threats, including selfish, faulty, and malicious nodes. This review has examined more than 20 recent contributions, highlighting the growing adoption of hybrid trust models that combine direct, indirect, behavioral, and energy-aware metrics. Techniques such as fuzzy logic, evolutionary algorithms, and initial machine learning approaches are being increasingly used to adapt to dynamic and hostile environments. However, significant gaps remain in terms of real-world validation, standardization of trust computations, and defense against sophisticated attack patterns like collusion and on-off behavior. Moreover, the challenge of balancing trust evaluation complexity with energy efficiency persists. Future research must focus on scalable, lightweight, and adaptive trust frameworks that integrate authentication, anomaly detection, and cross-layer security to enable resilient WSN deployment in real-world applications such as smart cities, healthcare, and critical infrastructure monitoring.

REFERENCES

[1] S. Lata, S. Mehfuz and S. Urooj, "Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies," in IEEE Access, vol. 9, pp. 161103-161128, 2021, doi: 10.1109/ACCESS.2021.3131367
[2] R. Kaur and A. Kaur, "A trust-aware routing protocol for WSN based on direct and indirect trust", *International Journal of Computer Applications*, vol. 123, no. 17, pp. 15–21, 2015.
[3] H. Yadav and R. Yadav, "Fuzzy based trust model for WSN", *Procedia Computer Science*, vol. 125, pp. 538–544, 2017.
[4] S. Ali, "Energy-aware fuzzy trust-based secure routing protocol in wireless sensor networks", *Egyptian Informatics Journal*, vol. 19, no. 3, pp. 255–262, 2018.
[5] M. Kumar and M. S. Saini, "TRM: Trust and reputation model for secure routing in WSN", *Wireless Personal Communications*, vol. 77, pp. 1683–1705, 2014.

[6] P. Sharma, R. Joshi, and A. Bhardwaj, "TR-LSTM: Trust-based routing using LSTM in wireless sensor networks", *Sensors*, vol. 23, no. 6, p. 3210, 2023.
[7] J. Gangwani, N. Singh, and P. Kumar, "STM: Semantic Trust Management for Secure Wireless Sensor Networks", *IEEE Access*, vol. 13, pp. 12234–12249, 2025.
[8] A. Bhukya and C. Annavarapu, "Hybrid trust-based cross-layer secure routing in WSN", *Journal of Ambient Intelligence and Humanized Computing*, vol. 16, pp. 1249–1260, 2025.
[9] A. Mata et al., "Trust-aware multipath routing for mitigating wormhole attacks", *Wireless Networks*, vol. 31, pp. 1592–1605, 2025.
[10] [H. Zhou and M. Xu, "Lightweight trust-based routing for energy efficiency in WSN", *Ad Hoc Networks*, vol. 154, p. 103171, 2024.
[11] L. Chen, X. Wang, and J. Liu, "QoS-Trust routing with fusion-based model for WSN", *Computer Networks*, vol. 232, p. 109850, 2023.
[12] R. Raj and T. Singh, "LTMBE: Long-term memory-based entropy model for trust routing", *Wireless Personal Communications*, vol. 122, no. 1, pp. 1–18, 2023.
[13] Y. Huang and C. Li, "Secure routing using beta reputation and direct trust", *Journal of Network and Computer Applications*, vol. 213, p. 103619, 2023.
[14] D. Babu and S. Raman, "Trust-aware fuzzy rule-based routing in WSN", *IEEE Sensors Journal*, vol. 22, no. 18, pp. 17594–17602, 2022.
[15] S. Rao, "Multi-agent trust optimization for WSN", *International Journal of Distributed Sensor Networks*, vol. 19, p. 155014772211035, 2022.
[16] A. Das and M. Sinha, "Entropy-based trust and intrusion prevention", *Information Fusion*, vol. 89, pp. 20–30, 2023.
[17] H. Mehta et al., "Hybrid trust computation for dynamic WSN routing", *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4921–4932, 2023.
[18] V. Pillai and K. Kumar, "DAE-Trust: Deep autoencoder-based trust model", *Neural Computing and Applications*, vol. 35, pp. 14781–14794, 2023.
[19] R. Pathak, "Blockchain-assisted secure trust routing", *Computers & Security*, vol. 126, p. 103003, 2023.
[20] Z. Xu and T. Li, "Cross-layer trust assessment using entropy", *Computer Standards & Interfaces*, vol. 86, p. 103656, 2023.
[21] J. Kim, "Multi-path routing and trust metrics", *Wireless Communications and Mobile Computing*, vol. 2023, Article ID 923456, 2023.
[22] M. Sharma et al., "Energy-efficient cluster-based routing protocol for WSN using multi-strategy fusion snake optimizer and minimum spanning tree", *Scientific Reports*, vol. 14, no. 1, p. 16786, 2024.
[23] M. Varatharajan, K. Govindarajan, and S. Alex, "Trust-aware energy-efficient model using evolutionary computing in WSN", in *Advances in Secure Networking*, Taylor & Francis, pp. 45–68, 2025.
[24] P. Bekal, P. Kumar, P. R. Mane, and G. Prabhu, "A comprehensive review of energy efficient routing protocols for query driven wireless sensor networks", *F1000Research*, vol. 12, p. 644, 2024.

[25] S. Ambareesh, P. Chavan, S. Supreeth et al., "A secure and energy-efficient routing using coupled ensemble selection approach and optimal type-2 fuzzy logic in WSN", *Scientific Reports*, vol. 15, no. 1, p. 38, 2025.

[26] K. Soltani, L. Farzinvash, and M. A. Balafar, "Trust-aware and energy-efficient data gathering in wireless sensor networks using PSO", *Soft Computing*, vol. 27, no. 16, pp. 11731–11754, 2023.

[27] C. Leoni, A. Vegni, V. Loscrí, and A. Benslimane, "Reputation-Based Trustworthiness Degree in Interference-Variable Vehicular Networks", in *Proc. IFIP Networking Conf.*, pp. 775–780, 2024.

[28] M. Careem and A. Dutta, "Reputation Based Routing in MANET using Blockchain", in *Proc. Int. Conf. Communication Systems & Networks (COMSNETS)*, pp. 1–6, 2020.

[29] P. Ye, "A Secure Routing Protocol for Wireless Sensor Network", *Proc. SPIE*, vol. 13175, pp. 131750J–1–5, 2024.

[30] A. B. F. Khan and G. Anandharaj, "A Cognitive Energy Efficient and Trusted Routing Model for the Security of Wireless Sensor Networks: CEMT", *Wireless Personal Communications*, vol. 119, pp. 3149–3159, 2021.

[31] A. K. Chhattisgarh, "Improving Trust Levels in Wireless Networks Using Blockchain Powered Dempster Shaffer Route Optimization", *ECS Transactions*, vol. 107, no. 1, pp. 2095–2106, 2022.

[32] H. Hassan et al., "Trust-Aware Routing Using Neural Networks in WSNs", *Sensors*, vol. 23, no. 1, p. 221, 2023.

[33] V. Arora and S. Saxena, "Fuzzy-Trust-AODV Protocol for WSN Security", *Journal of Computer Networks*, vol. 18, no. 3, pp. 85–97, 2023.

[34] S. Mahajan and R. Saini, "Hybrid Trust Detection in Tactical Routing", *Ad Hoc Networks*, vol. 134, p. 102984, 2024.

[35] A. Das and K. Swain, "Dynamic Route Trust using AI Fusion", *IEEE Access*, vol. 12, pp. 60120–60135, 2024.