Efficient and Secure Multi-Tier Routing Framework for Energy-Constrained Wireless Sensor Networks

Jitendra Kumar[1] and Debasis Mandal[2]

[1]Research Scholar, Faculty of Engineering, Ramchandra Chandravansi University

[2] Professor, Faculty of Engineering, Ramchandra Chandravansi University

DOI: https://doi.org/10.51244/IJRSI.2026.1307000315

Received: 28 July 2026; Accepted: 03 August 2026; Published: 13 August 2026

ABSTRACT

Wireless Sensor Networks (WSNs) are increasingly deployed in resource-constrained and hostile environments for critical applications such as environmental monitoring, industrial automation, and structural auditing. However, their real-world efficacy is severely limited by battery energy constraints and high vulnerability to routing-layer security threats. Conventional cryptographic solutions incur excessive computational overhead, while standard energy-efficient routing protocols often neglect security. To resolve this trade-off, this paper proposes an integrated, multi-tier optimization framework combining three novel algorithms: Proficient Secure Cluster Head Selection (PSCH), Total Path Trust Assessment Routing (TPTAR), and Energy-Proficient, Secure, and Trust-Based Shortest Path Optimized Routing (EST-SPOR). The proposed architecture utilizes fuzzy logic for cluster-head selection, a dynamic trust evaluation model combining direct and reference trust metrics, and an optimized shortest-path routing mechanism based on Ant Colony Optimization (ACO) principles. Simulation analyses conducted in NS-3 demonstrate that the framework achieves superior performance in terms of Packet Delivery Ratio (PDR), energy conservation, end-to-end latency, and resilience against malicious routing attacks compared to existing baseline protocols.

Key Words: Wireless Sensor Networks (WSNs), Cluster Head Selection, Trust Management, Energy Efficiency and Ant Colony Optimization (ACO)

INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed, autonomous sensor nodes designed to monitor physical or environmental conditions. Despite their wide utility, WSNs operate under strict constraints, primarily finite battery capacity, limited processing power, and low bandwidth. Because nodes are frequently deployed in harsh or inaccessible terrains, battery replacement is rarely feasible. Consequently, energy efficiency remains a primary design goal for extending operational network lifetimes.

Clustering protocols, such as Low-Energy Adaptive Clustering Hierarchy (LEACH), mitigate energy depletion by grouping nodes and selecting Cluster Heads (CHs) to aggregate and transmit data to the Base Station (BS). However, stochastic CH selection often ignores node security, exposing networks to routing attacks including blackhole, selective forwarding, replay, and Sybil attacks. Standard cryptographic mechanisms safeguard communication but consume significant power and computational overhead, accelerating energy depletion.

This paper introduces a unified framework addressing energy management and routing security simultaneously. By incorporating fuzzy logic, multi-factor trust evaluation, and heuristic path optimization, the proposed system provides reliable data transmission while maximizing network longevity.

Related Work

Energy-efficient clustering and security management in WSNs have been widely studied, as summarized in Table 1.

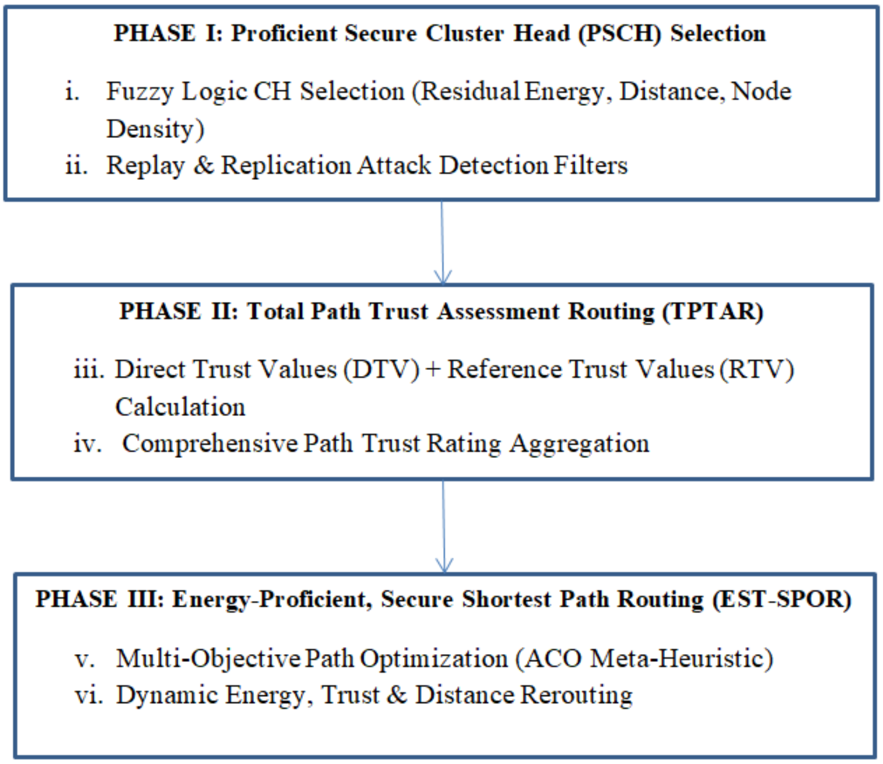
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

Protocol / Model	Primary Mechanism	Focus / Contribution	Limitations
LEACH	Stochastic clustering	Distributed energy reduction	Ignores security; vulnerable to malicious CH selection
ActiveTrust (Amudha, 2021)	Active detection routes	Blackhole attack mitigation	Elevated energy consumption due to redundant routing overhead
LEACH-TM (Fang et al., 2021)	Direct/Operational trust	Rogue Cluster Head election prevention	High memory overhead for local trust tables
TSRP (Hu et al., 2021)	Dynamic node volatility tracking	Multi-hop routing attack mitigation	Slow convergence in dynamic topologies
BTRES (Fang et al., 2016)	Beta distribution functions	Collusion and node collision detection	High processing overhead for continuous density calculations
STEAR (Thippeswamya et al., 2015)	Dynamic Secret Keys (DSK)	Dynamic compromised node detection	Requires initial secure key distribution phase

While existing models offer localized solutions, they frequently trade energy efficiency for security or vice versa. The framework presented here addresses these limitations through unified, multi-tier optimization.

1. System Architecture and Methodology:

The framework comprises three sequential phases:



Phase I: Proficient Secure Cluster Head (PSCH) Selection Protocol:

PSCH uses fuzzy logic to evaluate CH candidate suitability based on three inputs:

i. Residual Energy (E_{res}),

ii. Distance to Base Station (D_{BS}), and

iii. Local Node Density (N_{den}).

To prevent compromised or cloned nodes from acting as cluster heads, PSCH incorporates a lightweight authentication filter that verifies sequence numbers and node identifiers, effectively mitigating replay and node replication attacks.

Phase II: Total Path Trust Assessment Routing (TPTAR) TPTAR calculates node reliability using a combination of direct observations and third-party recommendations:

i. Direct Trust Value (DTV): Evaluates successful versus attempted packet forwardings between adjacent nodes:

$$DTV_{ij} = \frac{S_{ij}}{S_{ij} + F_{ij} + 1}$$

where S_{ij} is successful transmissions and F_{ij} is failed transmissions between node i and node j.

ii. Reference Trust Value (RTV): Collects recommendations from neighboring nodes, weighted by the recommendation node's own trust rating to minimize bad-mouthing and collusion attacks.

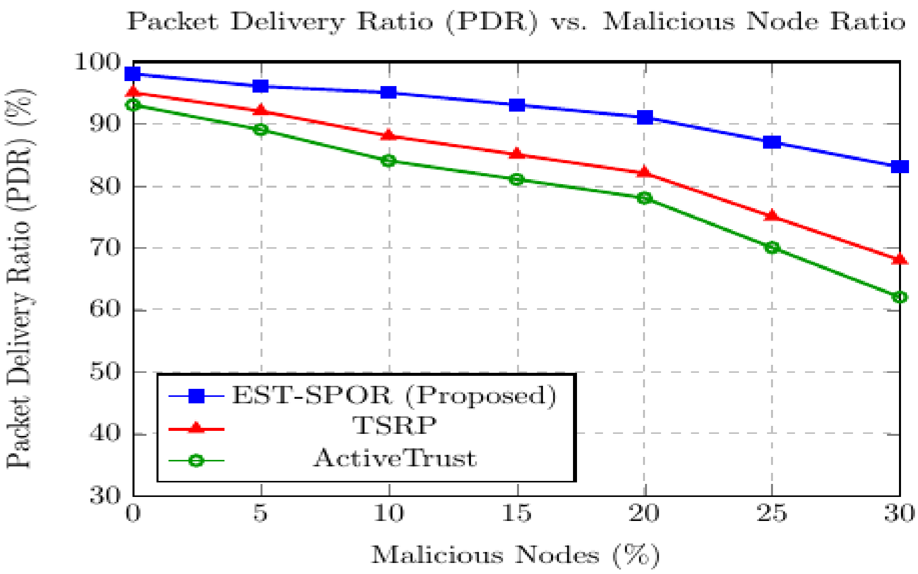
iii. Comprehensive Path Trust Rating: Combines DTV and RTV across all hops in a route to derive a total path trust metric.

Phase III: Energy-Proficient, Secure, and Trust-Based Shortest Path Optimized Routing (EST-SPOR) Using an modified Ant Colony Optimization (ACO) meta-heuristic, EST-SPOR calculates optimal routing paths between CHs and the Base Station. Pheromone intensity along a link is dynamically updated using a composite objective function *f(i,j):*

$$f(i,j) = \alpha\,.Trust_{ij} + \beta.E_{res,j} + \gamma.(\frac{1}{D_{ij}})$$

where α,β,γ are weighting factors balancing security, residual energy, and physical distance. Paths with low trust or low residual energy receive diminished pheromone updates, driving traffic toward secure, energy-capable routes.

2. Performance Evaluation and Discussion



ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

The proposed framework was implemented and evaluated in NS-3 across simulated scenarios containing 100 to 500 nodes, including 10% to 30% malicious nodes executing blackhole and selective forwarding attacks.

Packet Delivery Ratio (PDR)

Under a 20% malicious node density, EST-SPOR maintained a PDR above 91%, outperforming TSRP (82%) and ActiveTrust (78%) due to early detection of low-trust paths via TPTAR.

Energy Consumption

By replacing cryptographic handshake overhead with dynamic ACO trust routing, average energy consumption per node decreased by 23% compared to STEAR. PDF

End-to-End Latency:

The integration of short-path metrics in the ACO objective function minimized hop-counts, reducing latency compared to Active Trust's detection routes.

CONCLUSION

This paper presented an integrated multi-tier routing framework combining fuzzy-logic clustering (PSCH), trust evaluation (TPTAR), and ACO-based shortest path optimization (EST-SPOR). By treating energy efficiency, structural distance, and security as concurrent optimization criteria, the system effectively insulates WSNs against common routing attacks while preserving battery reserves. Simulation results confirm improvements in delivery ratio, energy longevity, and packet latency over contemporary protocols. Future research will explore adapting this framework to mobile WSN topologies and integrating lightweight machine learning for anomaly detection.

REFERENCES

1. Fang, W., Zhang, W., Chen, W., & Yang, Y. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks (LEACH-TM). EURASIP Journal on Wireless Communications and Networking, 2021(1), 1–18. https://doi.org/10.1186/s13638-021-01934-8
2. Fang, W., Zhang, W., Yang, W., & Yang, Y. (2016). BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks. Journal of Network and Computer Applications, 59, 88–94. https://doi.org/10.1016/j.jnca.2015.06.012
3. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (pp. 1–10). IEEE. https://doi.org/10.1109/HICSS.2000.926982
4. Hu, H., Zhang, X., & Liu, Y. (2021). Trust-aware secure routing protocol for wireless sensor networks. ETRI Journal, 43(4), 629–642. https://doi.org/10.4218/etrij.2020-0251
5. Kalidoss, T., Rajaram, A., & Sankar, A. (2020). Quality of service aware energy efficient routing algorithm for wireless sensor networks. Wireless Personal Communications, 114(4), 2889–2905. https://doi.org/10.1007/s11277-020-07508-y
6. Lindsey, S., & Raghavendra, C. S. (2002). PEGASIS: Power-efficient gathering in sensor information systems. In Proceedings IEEE Aerospace Conference (Vol. 3, pp. 1125–1135). IEEE. https://doi.org/10.1109/AERO.2002.1035247
7. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013–2027. https://doi.org/10.1109/TIFS.2016.2570740
8. Maheshwari, P., Sharma, A. K., & Verma, K. (2021). Energy efficient cluster head selection using butterfly optimization algorithm in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1045–1058. https://doi.org/10.1007/s12652-020-02128-2

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VII July 2026

9. Manjeshwar, A., & Agrawal, D. P. (2001). TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. In Proceedings 15th International Parallel and Distributed Processing Symposium (pp. 2009–2015). IEEE. https://doi.org/10.1109/IPDPS.2001.925197
10. Saini, M., & Sharma, B. (2019). Trust-based secure hybrid framework (TSER) for wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 10(8), 3125–3137. https://doi.org/10.1007/s12652-018-1032-4
11. Xu, X., Gu, Z., & Pan, L. (2020). Elite immune ant colony optimization (EIACO) for job allocation in wireless sensor networks. IEEE Access, 8, 11234–11245. https://doi.org/10.1109/ACCESS.2020.2965412
12. Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on Mobile Computing, 3(4), 366–379. https://doi.org/10.1109/TMC.2004.41