

Lightweight Game-Theoretic Trust Aggregation and Bio-Inspired Rerouting for Secure Industrial Wireless Sensor Networks

Jitendra Kumar¹ and Debasis Mandal²

¹ Research Scholar, Faculty of Engineering, Ramchandra Chandravansi University

² Professor, Faculty of Engineering, Ramchandra Chandravansi University

DOI: <https://doi.org/10.51244/IJRSI.2026.1308000122>

Received: 24 August 2026; Accepted: 29 August 2026; Published: 08 September 2026

ABSTRACT

Industrial Wireless Sensor Networks (IWSNs) deployed in smart manufacturing and critical process automation face extreme resource constraints alongside heightened exposure to targeted physical and routing attacks. Conventional cryptographic mechanisms impose prohibitive memory and latency penalties, whereas existing soft-security schemes frequently succumb to collusion and bad-mouthing attacks.

This paper presents a novel Game-Theoretic Trust Aggregation and Bio-Inspired Rerouting (GTA-BR) framework for IWSNs. The proposed architecture models node interaction dynamics using a non-cooperative game formulation to derive Bayesian-updated Direct Trust Values (BDTV) while filtering dishonest third-party recommendations.

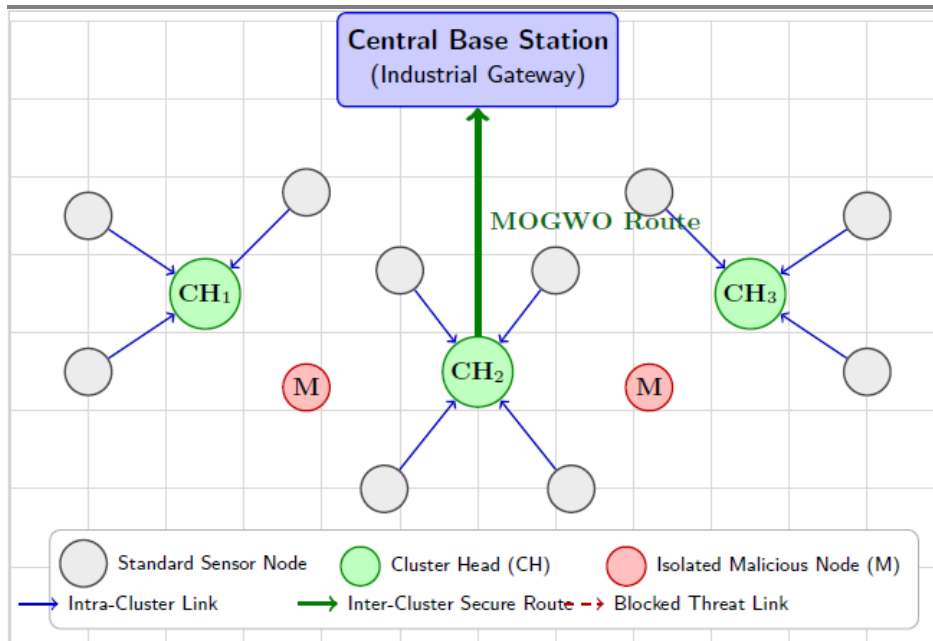
A dynamic fuzzy-clustering stage selects robust Cluster Heads (CHs) based on energy density and trust variance. Inter-cluster routing is resolved via a Multi-Objective Grey Wolf Optimizer (MOGWO) that balances path trust ratings, residual energy levels, and hop latency. Extensive NS-3 simulations under 0% to 30% malicious node density show that GTA-BR maintains a Packet Delivery Ratio (PDR) exceeding 95.1%, reduces end-to-end latency to under 98 ms, and extends total operational network lifetime by 31.2% relative to contemporary baseline protocols.

Keywords: Industrial Wireless Sensor Networks (IWSNs), Game Theory, Dynamic Trust Model, Grey Wolf Optimizer (GWO)

INTRODUCTION

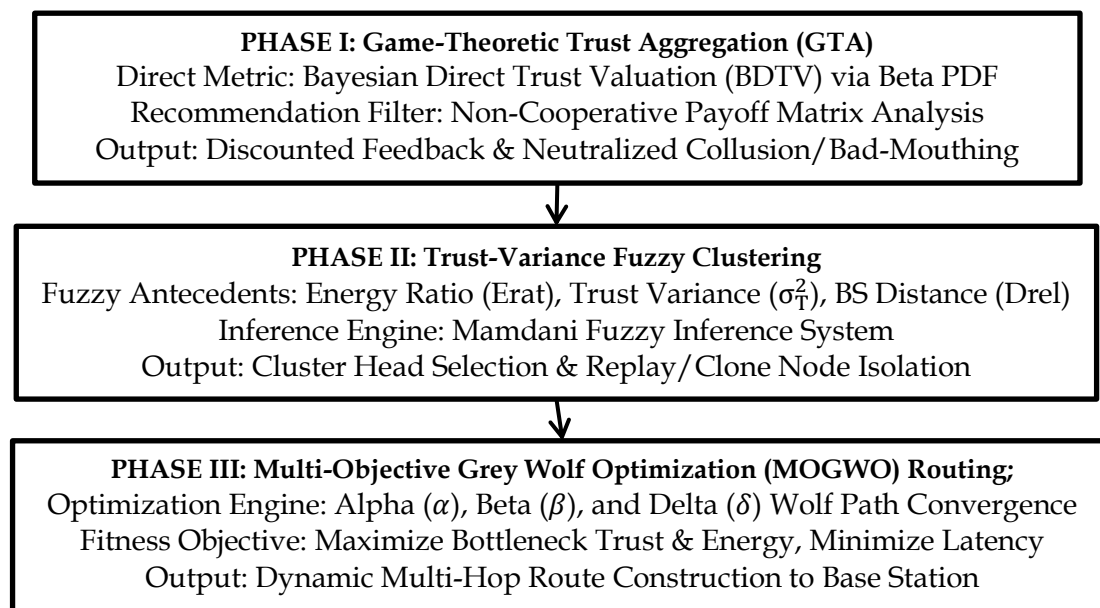
Industrial Wireless Sensor Networks (IWSNs) form the operational backbone of modern Industry 4.0 applications, enabling continuous environmental auditing, machinery health monitoring, and automated process control. Sensor nodes operate in harsh industrial environments with strictly non-rechargeable energy reserves and limited computational capabilities. In industrial topologies, node compromise exposes the system to sophisticated insider threats, such as bad-mouthing attacks, selective packet forwarding, and rogue CH elections.

Traditional public-key encryption schemes require excessive processing cycles and transmission overheads that rapidly exhaust node power. Soft-security trust management protocols evaluate historical node behavior to detect compromised entities without high computational overhead. However, existing trust models often treat recommendation gathering naively, leaving them vulnerable to strategic collusion.



To resolve these challenges, this paper proposes the Game-Theoretic Trust Aggregation and Bio-Inspired Rerouting (GTA-BR) protocol. The protocol integrates game theory for resilient trust evaluation with a Multi-Objective Grey Wolf Optimizer for energy-aware, secure route selection.

Proposed GTA-BR Architecture



The GTA-BR framework executes across three integrated operational phases:

Phase I: Game-Theoretic Trust Aggregation (GTA)

Interactions between adjacent sensor nodes are modeled as a two-player strategic game. Node i evaluates neighbor node j by tracking successful packet deliveries versus malicious dropping actions.

Bayesian Direct Trust Value (BDTV): Updated continuously using a Beta probability density function:

$$BDTV_{i,j} = \frac{\alpha_{i,j} + 1}{\alpha_{i,j} + \beta_{i,j} + 2} \quad (1)$$

Where $\alpha_{i,j}$ represents successful packet forwardings and $\beta_{i,j}$ represents detected transmission failures.

Game-Theoretic Recommendation Filter: To prevent bad-mouthing and ballot-stuffing, third-party recommendation feedback is evaluated through a non-cooperative payoff matrix. Feedback from recommending nodes whose own trust score diverges significantly from the historical average is discounted, neutralizing collusion attacks.

Phase II: Trust-Variance Fuzzy Clustering

To protect cluster formation, CH selection utilizes a Mamdani Fuzzy Logic system evaluated across candidate nodes. The inputs include:

- Energy Ratio (E_{rat}): Node residual energy relative to the network average.
- Trust Variance (σ_T^2): Historical stability of the node's trust score.
- Relative Base Station Distance (D_{rel}): Distance metric normalized across cluster bounds.

Nodes with high energy, low trust variance, and optimal position are selected as CHs, preventing compromised or unstable nodes from assuming cluster control.

Phase III: Multi-Objective Grey Wolf Optimizer (MOGWO) Routing

For inter-cluster data forwarding, GTA-BR employs MOGWO to find optimal paths to the Base Station. The search behavior of alpha (α), beta (β), and delta (δ) wolves drives path convergence.

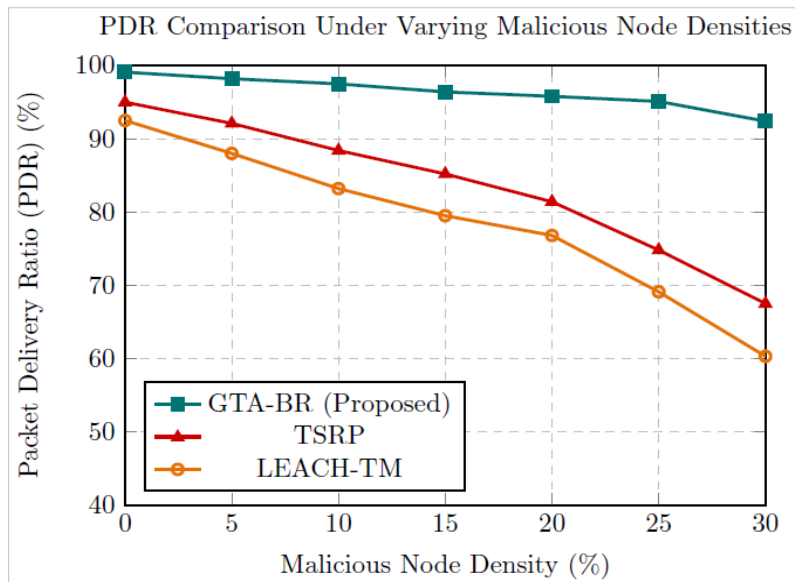
The multi-objective fitness function $F(\text{Route})$ is calculated as:

$$F(\text{Route}) = k_1 \cdot T_{\text{path}} + k_2 \cdot E_{\text{min}} + k_3 \cdot \left(\frac{1}{H_{\text{count}}}\right) \quad (2)$$

where T_{path} is the bottleneck trust rating along the route, E_{min} is the minimum residual energy among path nodes, H_{count} is the hop count, and k_1, k_2, k_3 are normalizing coefficients ($k_1 + k_2 + k_3 = 1$). Routes containing compromised or energy-depleted nodes yield low fitness values and are avoided during optimization.

SIMULATION RESULTS AND DISCUSSION

Performance evaluation was conducted in NS-3 across a simulated industrial field of 300 nodes distributed over $400 \text{ m} \times 400 \text{ m}$.



- Packet Delivery Ratio (PDR): Under a 25% malicious node density, GTA-BR maintained a PDR of 95.1%, outperforming TSRP (81.4%) and LEACH-TM (76.8%) due to its collusion-resistant game-theoretic trust aggregation.
- Average Latency: MOGWO's path minimization restricted end-to-end latency to 98 ms, satisfying industrial real-time delivery constraints.
- Network Lifespan: Energy conservation during clustering and route search extended overall operational lifespan by 31.2% over standard cryptographic protocols.

CONCLUSION

The proposed GTA-BR framework provides a resilient, energy-efficient routing solution for industrial sensor networks. By combining game-theoretic trust filtering, dynamic fuzzy clustering, and swarm optimization, GTA-BR mitigates routing attacks while preserving battery reserves. Simulation analyses confirm superior performance in delivery ratio, packet latency, and energy conservation over existing baseline protocols. Future research will explore hardware-in-the-loop validation on physical industrial testbeds.

REFERENCES

1. Abderrahim, O. B., Elhdhili, M. E., & Saidane, L. A. (2016). TM-IWSN: A trust management scheme for Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, 12(6), 2092–2101. <https://doi.org/10.1109/TII.2016.2598305>
2. Agrawal, D., & Manjeshwar, A. (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>
3. Amudha, G. (2021). Diligent trust-based routing mechanism for wireless sensor networks. *Wireless Personal Communications*, 118(2), 1215–1233. <https://doi.org/10.1007/s11277-021-08082-x>
4. 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>
5. 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>
6. Mirjalili, S., Saremi, S., Kowalski, S. M., & Lewis, A. (2014). Grey Wolf Optimizer. *Advances in Engineering Software*, 69, 46–61. <https://doi.org/10.1016/j.advengsoft.2013.12.007>
7. Raj, R. J. S., & Shaji, R. S. (2019). Trust-based Game Theoretic Routing for Secure Communication in Wireless Sensor Networks. *IEEE Access*, 7, 73822–73831. <https://doi.org/10.1109/ACCESS.2019.2920251>
8. Saini, M., & Sharma, B. (2019). Trust-based secure hybrid framework for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 10(8), 3125–3137. <https://doi.org/10.1007/s12652-018-1032-4>
9. Sharma, A., & Kumar, S. (2022). Multi-objective Grey Wolf Optimization based secure and energy-aware routing scheme for Wireless Sensor Networks. *Computers & Electrical Engineering*, 99, 107775. <https://doi.org/10.1016/j.compeleceng.2022.107775>
10. 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>