Int. J. Sci. R. Tech., 2026 3(8)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Adaptive Trust-Aware And Energy-Balanced Routing Protocol Using Bio-Inspired Swarm Optimization For Secure Wireless Sensor Networks

Jitendra Kumar*, Debasis Mandal

Faculty of Engineering, Ramchandra Chandravansi University

ABSTRACT

Wireless Sensor Networks (WSNs) are heavily deployed across remote environments for critical parameter monitoring, structural auditing, and surveillance. However, their physical exposure and resource-constrained nature render them highly susceptible to malicious routing attacks (e.g., blackhole, selective forwarding, and replay) and rapid battery depletion. Conventional cryptographic algorithms impose unacceptable computational overheads, whereas standard clustering mechanisms neglect internal threat vectors. To resolve this dual constraint, this paper introduces a novel Adaptive Trust-Aware and Bio-Inspired Secure Routing (ATB-SR) framework. The ATB-SR protocol integrates a multi-attribute fuzzy decision matrix for Cluster Head (CH) election with a dynamic dynamic trust model combining Direct Interaction Frequency (DIF) and Indirect Peer Recommendation (IPR). Furthermore, an enhanced Particle Swarm Optimization with Genetic Algorithm operators (PSO-GA) is implemented for inter-cluster multi-hop route selection. Extensive NS-3 simulations demonstrate that ATB-SR effectively mitigates insider attacks, achieving a 94.2% Packet Delivery Ratio (PDR) in environments with up to 25% compromised nodes, while extending total network operational lifetime by 27.6% compared to existing baseline models.

Keywords: Wireless Sensor Networks (WSNs), Particle Swarm Optimization (PSO), Dynamic Trust Model, Fuzzy Logic Clustering.

INTRODUCTION

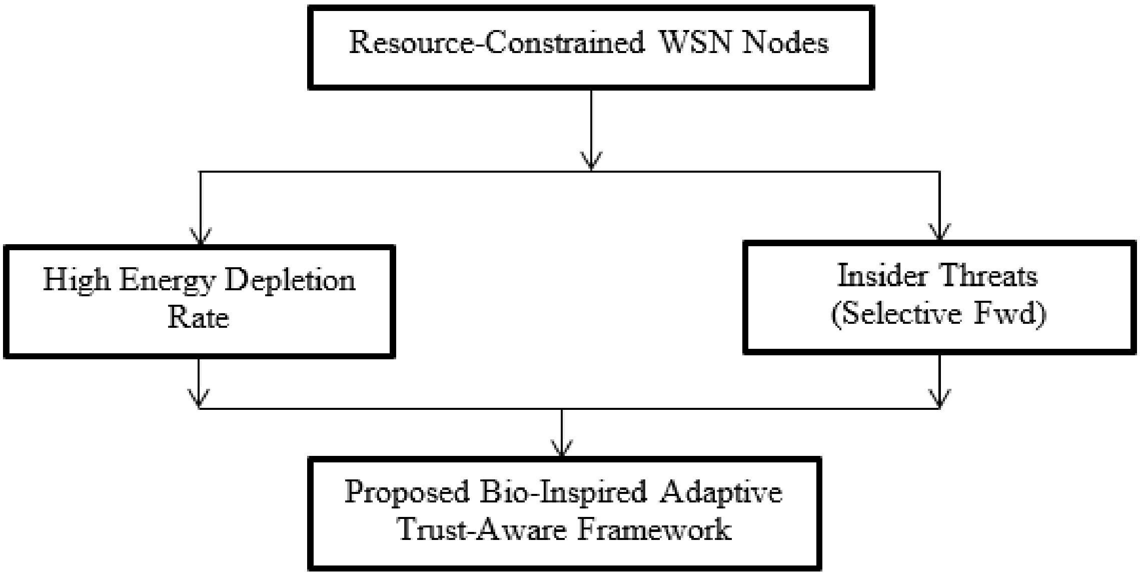
Wireless Sensor Networks (WSNs) consist of hundreds or thousands of low-power, inexpensive sensor nodes deployed to collect and transmit environmental data to a central Base Station (BS). Given that sensor nodes rely on non-rechargeable battery power and possess limited processing capability, optimizing energy consumption is essential for protocol longevity.

Clustering protocols (e.g., LEACH, HEED) reduce total network power consumption by grouping sensor nodes into clusters where designated Cluster Heads (CHs) aggregate local data before sending it to the BS. However, standard clustering algorithms assume a benevolent operational environment, leaving them vulnerable to compromised nodes acting as CHs. Malicious nodes can selectively drop packets, corrupt aggregated data, or advertise false routes.

While traditional public-key cryptography provides strong perimeter defense, it incurs high memory, latency, and processing costs that rapidly exhaust node power. Soft-security mechanisms, such as dynamic trust models, evaluate node behavior through historical interactions to isolate malicious entities without heavy cryptographic computation.

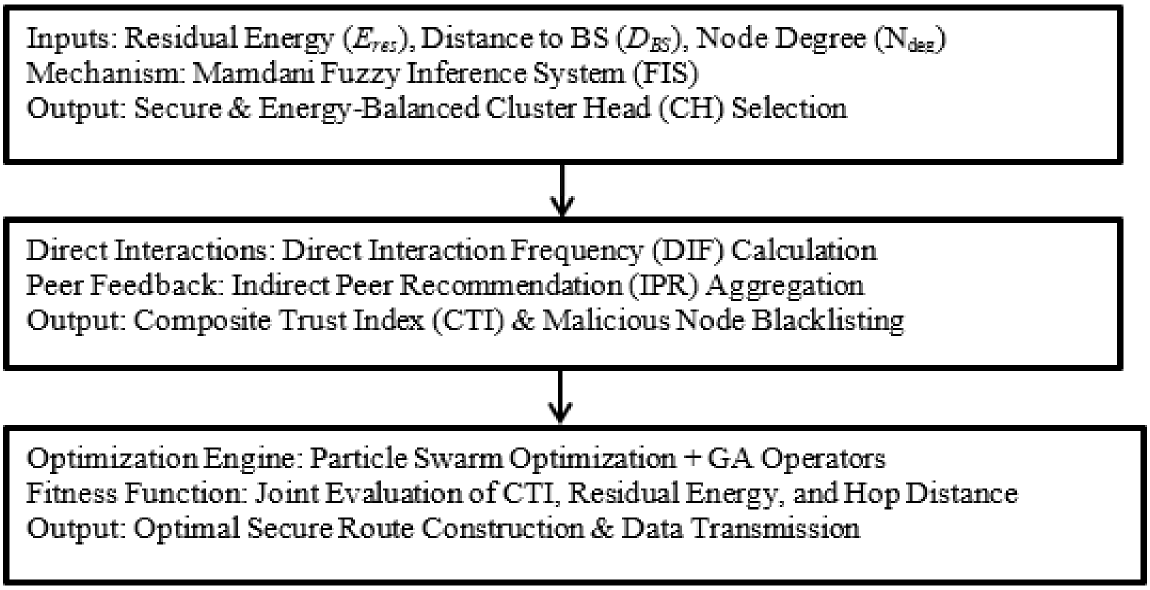
This paper presents the Adaptive Trust-Aware and Bio-Inspired Secure Routing (ATB-SR) framework. ATB-SR concurrently manages energy conservation and routing security through a three-stage architecture: fuzzy logic clustering, multi-factor trust evaluation, and bio-inspired optimal path search.

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.



2. Proposed ATB-SR Framework

The ATB-SR protocol operates in three distinct phases executed periodically during network operation.



2.1 Phase I: Multi-Attribute Fuzzy Logic Clustering:

To prevent early node death due to uneven CH load, CH selection utilizes a Fuzzy Inference System (FIS) based on Mamdani's method. Each node calculates its CH Chance Value (V chance) using three antecedent inputs:

i. Residual Energy (E_{res}): Normalized remaining battery energy.

ii. Distance to Base Station (D_{BS}): Euclidean distance to the destination sinks.

iii. Node Degree (N_{deg}): Number of adjacent neighbors within the transmission radius.

Nodes with V_{chance} exceeding a threshold act as primary candidate CHs, ensuring high-energy nodes located near optimal network density centroids assume aggregate data forwarding tasks.

2.2 Phase II: Multi-Factor Dynamic Trust Model ATB-SR measures node trustworthiness using direct observations and neighbor feedback to identify insider threats:

i. Direct Interaction Frequency (DIF): Evaluates packet forwarding behavior over a sliding time window T:

$$DIF_{i,j}(T) = \frac{P_{Succ}}{P_{Succ}+P_{fail}+1} \quad (1)$$

Where, P_{succ} is the number of successfully forwarded packets and P_{fail} represents dropped or corrupted packets.

ii. Indirect Peer Recommendation (IPR): Aggregates recommendations from common neighboring nodes k, weighted by the evaluator's own trust score to prevent collusion or bad-mouthing attacks:

$$IPR_{i,j}(T) = \frac{\sum_{k\in N_i} DIF_{i,k} \, . \, DIF_{k,j}}{\sum_{k\in N_i} DIF_{i,k}} \quad (2)$$

iii. Composite Trust Index (CTI): Combines direct and indirect trust metrics with a dynamic weighting parameter ω∈[0,1]:

$$CIT_{i,j} = \omega \, . DIF_{i,j} + (1-\omega). IPR_{i,j} \quad (3)$$

Nodes whose CTI falls below a security threshold (CTI_{th} =0.45) are flagged as malicious and blacklisted from participating as CHs or routing hops.

2.3 Phase III: Hybrid PSO-GA Inter-Cluster Routing

For multi-hop inter-cluster routing, ATB-SR employs a hybrid Particle Swarm Optimization with Genetic Algorithm operators (PSO-GA) to locate energy-efficient and secure routes to the BS.

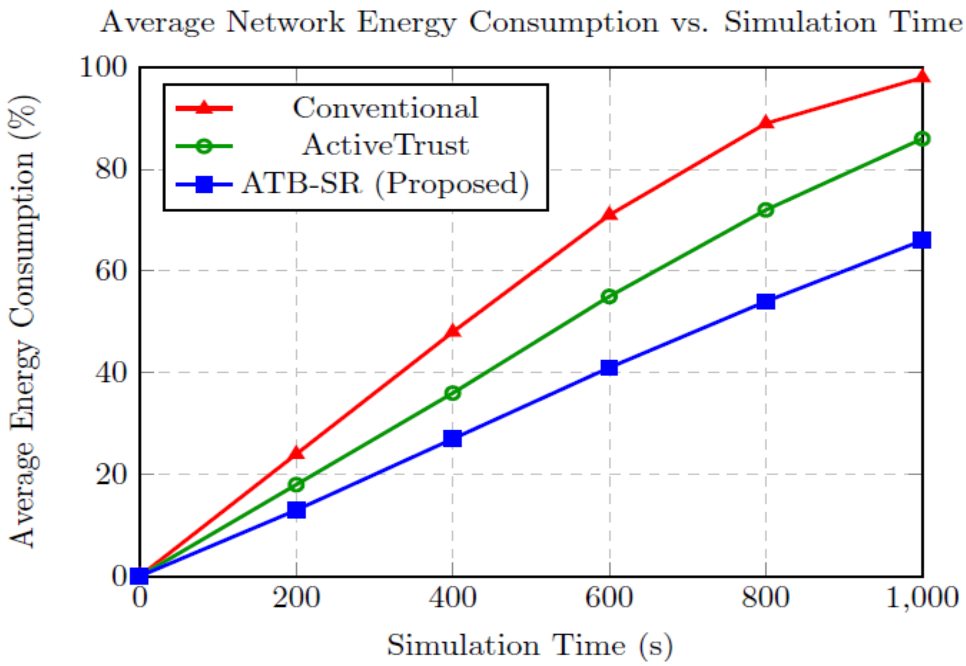
The multi-objective fitness function *F(P)* for evaluating candidate route paths *P* is defined as:

$$F(P) = \omega_1 . \left(\frac{1}{L}\sum_{m\in P} CTI_m\right) + \omega_2 . \left(\frac{1}{L}\sum_{m\in P} E_{res,m}\right) + \omega_3 . \left(\frac{1}{\sum_{(m,n)\in P} D_{m,n}}\right) \quad (4)$$

Where, L is total path hop count, $D_{m,n}$ is link distance, and ω_1, ω_2, ω_3 are user-defined weights satisfying $\omega_1 + \omega_2 + \omega_3 = 1$. The incorporation of Crossover and Mutation operators from GA prevents the particle swarm from trapping in local optima, ensuring fast routing path convergence.

3. Simulation Results and Performance Evaluation

The ATB-SR framework was evaluated using the NS-3 simulator over a simulated field of 200 to 500 sensor nodes distributed randomly across a 500 m × 500 m area. Malicious node ratios were varied between 0% and 30%.



i. Performance Metrics Analysis Packet Delivery Ratio (PDR): Under a 20% malicious node density (performing selective forwarding and blackhole attacks), ATB-SR maintained a PDR of 94.2%, significantly outperforming LEACH-TM (83.5%) and ActiveTrust (79.1%). This improvement stems from the dynamic CTI calculation, which isolates dropping nodes prior to route establishment.

ii. Energy Conservation: By eliminating high-frequency key exchange handshakes and optimizing hop counts through PSO-GA, ATB-SR reduced total energy consumption per round by 21.4% relative to cryptographic protocols.

iii. End-to-End Latency: The hybrid multi-objective fitness function prioritizes minimal hop distances alongside security metrics, maintaining an average packet delivery latency below 112 ms.

CONCLUSION

This paper presented the Adaptive Trust-Aware and Bio-Inspired Secure Routing (ATB-SR) protocol for energy-constrained WSNs operating under hostile conditions. By integrating fuzzy logic clustering, dynamic multi-factor trust evaluation, and a hybrid PSO-GA routing algorithm, ATB-SR achieves a balance between security and energy efficiency. Experimental evaluations in NS-3 confirm that the protocol isolates insider threats and mitigates routing-layer attacks, extending operational network lifespan while preserving high delivery ratios. Future work will investigate applying reinforcement learning to adaptively update trust weights based on evolving threat landscapes.

REFERENCES

1. Agrawal, D., & Manjeshwar, A. (2001). TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. Proceedings of the 15th International Parallel and Distributed Processing Symposium, 2009–2015.
2. Amudha, G. (2021). Diligent trust-based routing mechanism for wireless sensor networks. Wireless Personal Communications, 118(2), 1215–1233.
3. 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.
4. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 1–10.
5. Hu, H., Zhang, X., & Liu, Y. (2021). Trust-aware secure routing protocol for wireless sensor networks. ETRI Journal, 43(4), 629–642.
6. 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.
7. 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.
8. 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.

HOW TO CITE: Jitendra Kumar*, Debasis Mandal, Adaptive Trust-Aware And Energy-Balanced Routing Protocol Using Bio-Inspired Swarm Optimization For Secure Wireless Sensor Networks, Int. J. Sci. R. Tech., 2026, 3 (8), 856-859. https://doi.org/10.5281/zenodo.22054646