IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 12, No. 11, November, 2025, pp. 4000-4006
Journal homepage: http://iieta.org/journals/mmep

Secure and Adaptive Routing in Wireless Sensor Networks Using Meta-Router and TGAT-TrustChain

Naga Anuradha[1], Y. Alekya Rani[2], Prabhakar Marry[3], Shreekant Salotagi[4], Dara Rajesh Babu[5], G. Naga Rama Devi[6], Pannangi Naresh[4*], Elicherla Sivananda Lahari Reddy[4]

[1] Department of Mathematics, Vasavi College of Engineering, Ibrahimbagh, Hyderabad 500031, India
[2] Department of Computer Science and Engineering (AIML), CVR College of Engineering, Hyderabad 501510, India
[3] Department of Information Technology, Vignan Institute of Technology and Science, Hyderabad 508284, India
[4] Department of Computer Science & Engineering, Dayananda Sagar University, Bengaluru 562112, India
[5] Department of Computer Science & Engineering, Srinivasa Ramanujan Institute of Technology, Anantapur 515701, India
[6] Department of Computer Science and Engineering, Sreyas Institute of Engineering and Technology, Hyderabad 500036, India

Corresponding Author Email: nareshintell4@gmail.com

https://doi.org/10.18280/mmep.121126

Received: 22 September 2025
Revised: 12 November 2025
Accepted: 20 November 2025
Available online: 30 November 2025

Keywords:
Wireless Sensor Networks, reinforcement learning, generative adversarial network, meta-learning, temporal graph attention, GAN, adversarial robustness

ABSTRACT

Wireless Sensor Networks (WSNs) play a crucial role in critical applications where routing must balance trust, energy efficiency, and adaptability. Traditional routing and trust models often remain static, making them vulnerable to dynamic topology changes, malicious behavior, and rapid energy depletion. Moreover, most existing approaches lack temporal awareness and fail to integrate trust management effectively with routing decisions. To overcome these limitations, this paper proposes the Adaptive Reinforcement Trust Blockchain Network (ART-BTNet), a unified framework that combines adaptive routing and blockchain-based trust management. The framework integrates five core components: a Meta-Router for rapid policy adaptation through reinforcement meta-learning, TGAT-TrustChain for temporal trust evaluation using graph attention on blockchain, a Cross Layer-Shaper for multi-layer metric fusion, a GAN-Audit Chain for detecting malicious activity, and a Dual Attention Co-Model for joint optimization of trust and routing performance. Compared to conventional routing protocols, ART-BTNet achieves a 15.85% higher packet delivery ratio, 30.43% lower energy consumption, and 66.67% reduction in both false trust positives and routing convergence time. These results demonstrate that ART-BTNet offers a robust, scalable, and secure routing solution for next-generation WSNs operating in dynamic and adversarial environments.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have become indispensable in numerous application domains, ranging from environmental monitoring and industrial automation to defense and healthcare. These networks, comprising spatially distributed sensor nodes with limited energy, computation, and communication capabilities, require robust and adaptive routing mechanisms to ensure data integrity, delivery reliability, and system longevity. However, real-world WSN deployments are often exposed to dynamic environmental conditions, node mobility, and potential security threats, such as packet drops, data falsification, and collusion attacks. Existing routing protocols typically operate under fixed assumptions and static trust evaluations, leading to performance degradation and vulnerability in the presence of non-stationary network behaviors. Conventional trust models used in WSNs fail to capture the evolving nature of node behavior over time as they lack temporal sensitivity and are often disconnected from the routing decision-making process. Furthermore, most routing algorithms optimize for performance metrics like delay or energy without incorporating dynamic trust scores or learning from adversarial behavior. Therefore, the existing limitations accentuate the paramount need for a holistic framework that unifies adaptive routing with a robust, temporally aware trust mechanism underpinned by secure and decentralized validation in process.

Existing routing and trust management approaches in WSNs often treat trust evaluation, routing optimization, and attack resilience as isolated processes. State-of-the-art models, such as trust-aware reinforcement routing and blockchain-enabled frameworks, still rely on static trust aggregation or delayed policy updates, limiting adaptability under dynamic network conditions. Moreover, current solutions rarely integrate temporal trust evolution, cross-layer feedback, and adversarial robustness within a unified design.

To bridge these gaps, this paper introduces Adaptive Reinforcement Trust Blockchain Network (ART-BTNet) — a novel, fully integrated architecture that combines reinforcement meta-learning and blockchain for adaptive and secure routing. The proposed framework contributes five distinct innovations:

1. Meta-Router, enabling rapid adaptation to network changes through reinforcement meta-learning;
2. TGAT-TrustChain, introducing temporal graph attention networks for real-time trust evolution on blockchain;
3. CrossLayer-Shaper, fusing cross-layer metrics into a dynamic reward structure for energy-efficient decisions;
4. GAN-AuditChain, employing generative adversarial testing to evaluate trust resilience under malicious conditions;
5. DualAttn-CoModel, jointly optimizing routing and trust using dual spatial–temporal attention mechanisms.

Together, these modules form an interoperable framework that delivers faster convergence, enhanced energy efficiency, and robust protection against trust-based attacks, outperforming existing routing and trust models.

2. RELATED WORK

The invention of secure and energy-efficient routing in WSNs has led to a variety of methodologies that deal with certain constraints, namely, energy depletion, dynamic topologies, and malicious behavior. The current trend appears to integrate trust evaluation with optimization, cryptographic, and blockchain mechanisms to ensure that resilience and adaptability at network layer are achieved without compromising security. A trust-based secure routing framework optimized for industrial WSNs under constraints of energy-efficient path computation strategies was proposed by Singh et al. [1]. Any routing mechanism is usually effective in stable environments but lacks fast adaptation to dynamic topology changes, restricting its applicability over mobile or adversarial networks. In a similar manner, Qian [2] introduced DMKESR–a multi-parameter key exchange protocol with routing enhancements for mesh networks that mainly focuses on cryptographic security. Very strong in key management, it did not employ either learning-based adaptability or dynamic trust evaluation. Vankdothu and Hameed [3] addressed congestion and interference issues with a routing protocol for IoT-WSN contexts. They had an approach for improving throughput under interference, which itself does not contribute much to adversarial resilience. Yesodha et al. [4] secured ant colony optimization-based routing using elliptic curve cryptography. Computational overheads oppose cryptographic security in terms of scalability against resource-constrained nodes. Subramani and Selvi [5] deployed fuzzy logic and ant colony optimization with intrusion detection so as to maximize WSN security sets. They had enhancements in the anomaly detection task but did not possess real-time adaptability to change in behavior. Samha [6] worked on optimized routing for earth observation so as to increase reliability on static sensor deployments, however the model did not emphasize adaptability with regard to trust dynamics in its process.

Guo [7] introduced an energy-aware routing protocol with mobile sink coordination and presented performance benefits in topologically dynamic networks. However, the absence of integrated trust validation mechanisms diminished its defense against internal threats. Dixit and Qureshi [8] used Red Fox Optimization for security-aware cluster-based routing process. Their model incorporated bio-inspired optimization but did not exploit temporal patterns in trust behavior sets. Bai et al. [9] proposed TSRP, which combines trust and energy metrics for routing decisions; however, while the trust and energy issues were jointly addressed, adversarial stress testing and rapid meta-learning were not in their scope. Arpitha et al. [10] introduced hybrid schemes on location privacy in IoT-healthcare WSNs, yet trust dynamics and adversarial validation were insufficiently addressed for the methodology. Gavali et al. [11] initiated the development of HOCOR, a hybrid cooperative routing technique for underwater WSNs, emphasizing the aspect of opportunistic transmission. While their model improved energy efficiency, it did not consider trust or security in process explicitly as was prescribed. Gandhi and Mohindra [12] created a routing scheme for smart cities combining IoT, secure routing being their emphasis, but the learning adaptability to changing behavior/network states was absent. Rajkumar et al. [13] introduced HSEERP, a hierarchical routing protocol considering security and energy efficiency. Their model achieved scalability in structured networks but did not rely on learning techniques or adversarial resilience sets. Godi et al. [14] suggested a multi-objective hybrid optimization algorithm for cluster head selection and routing. Although it is highly secure and energy aware, it lacks blockchain-based immutability or deeper temporal modeling of trust sets.

Xiao et al. [15] have proposed BS-SCRM, a blockchain-based secure routing method using swarm intelligence. The model has incorporated decentralization for trust recording and collective decision-making; however, it lacks a learning framework for rapid policy adaptation and adversarial robustness via generative models. In synthesis, while several prior works, such as one by Flayeh et al. [16], addressed important dimensions of WSN routing such as trust integration [17], cryptographic robustness, bio-inspired optimization, or blockchain-based validation none manages to propose a unified architecture tying together adaptive reinforcement learning, temporal trust modeling, multi-layer feedback, adversarial trust validation, and blockchain-based consensus [18]. Hence, the ART-BTNet model we propose bridges this loft by merging meta-learning-based routing (Meta-Router), temporal graph attention trust computation (TGAT-TrustChain), multi-layer reward shaping (CrossLayer-Shaper), GAN-driven adversarial trust validation (GAN-AuditChain) [19], and dual-attention fusion (DualAttn-CoModel), thus forming an integrated and highly resilient architecture for contemporary WSNs.

3. PROPOSED MODEL DESIGN ANALYSIS

The design of the proposed ART-BTNet model is grounded on the necessity for a tightly integrated dynamic routing-trust optimization framework for WSNs, where energy and security constraints are both critical and interdependent in process. The architecture of the model brings together reinforcement meta-learning, temporal trust modeling through attention-based graphs, cross-layer reward shaping, and adversarial trust auditing through dual-attention fusions. These components have been selected and integrated not in isolation but with mutual reinforcement in mind in order to ensure considerable complements and high systemic coherence for the model. In essence, as seen in Figure 1, the Meta-Router sits at the heart of the routing engine. It applies the Model-Agnostic Meta-Learning (MAML) paradigm to facilitate extremely rapid policy adaptation for nodes witnessing switching under the influence of either topology changes, buffer congestion, or energy variation in the process. The working mechanism optimizes for fast adaptation across tasks using a second-order gradient-based update. For a particular routing policy characterized by θ and a task-specific loss function $L_i(\theta)$, the meta-update rule is derived via Eq. (1).

$$\theta \leftarrow \theta - \beta \nabla \theta \sum_{\mathrm{i}} \mathrm{L_i}(\theta - \alpha \nabla \theta \mathrm{L_i}(\theta)) \tag{1}$$

where, α and β represent the inner and outer learning rates respectively for the process. This equation will ensure that the routing policy can generalize for different network conditions without requiring the process to be relearned each time one occurs. In conjunction with that is the CrossLayer-Shaper which would formulate a composite reward signal R by mere aggregation of the inputs from the MAC, network, and transport layers.

The reward is formulated as the weighted sum of several performance metrics via Eq. (2).

$$R = w1 \cdot \int rMAC(t)\, dt + w2 \cdot \int rNET(t)\, dt + w3 \cdot \int rTRANS(t)\, dt \tag{2}$$

where, *rMAC(t)*, *rNET(t)*, and *rTRANS(t)* depict time-dependent penalty or reward functions regarding retransmissions, delays, and ACK failures, respectively, for the case under consideration. However, these weights w1, w2, w3 are being tuned dynamically by means of real-time feedback such that rewards would be well aligned to flexible changes of the network conditions. For trust modeling, the TGAT-TrustChain module uses temporal graph attention networks to learn time-sensitive trust vectors $\tau_t \in \mathbb{R}^d$, where trust is a function of both spatial relations and temporal sequence. It is given by updating trust scores expressed via Eq. (3).

$$\tau_{\mathrm{t}} = Softmax\left(\sum \in \mathcal{N}(i)\alpha_{\mathrm{ij}}(t) \cdot W \cdot x_{\mathrm{j}}(t - \Delta t_{\mathrm{ij}})\right) \tag{3}$$

where, $x_j(t - \Delta t_i{}^e{}_j)$ = feature of neighbor node '*j*' at a temporal offset Δt_{ij}, W is a learnable weight matrix, and $\alpha_{ij}(t)$ are the attention coefficients learned through temporal graph self-attention process.

Eq. (3) ensures that each node's trust score dynamically reflects temporal shifts (e.g., delayed packets, intermittent failures). The Softmax normalization ensures stable trust scaling among neighbors. This enables real-time adaptation of trust scores as network conditions evolve.

With this equation, one will be able to realize a real-time adaptation of the trust scores by impedance of latency, delayed packet responses, and dynamic behavior shifts. Furthermore, to react to legitimacy, the GAN-AuditChain session introduces a computational adversary which analyzes trust transaction in processes. The generator G(z) synthesizes fake trust events, while the discriminator D(x) aims to distinguish between real and adversarial data samples. Optimization follows the standard GAN minimax framework as expressed via Eq. (4).

$$Objective = \overset{G}{\min}\left(\overset{D}{\max}\left[\mathbb{E}_{\mathrm{x}} \sim preal[\log D(x)] + \mathbb{E}z \sim pz\left[\log\left(1 - D\left(G(z)\right)\right)\right]\right]\right) \tag{4}$$

This mechanism ensures that trust evaluation remains resilient even in the presence of adversarial or malicious data injection attacks.

This process includes synthetic anomalies into the trust chain, ensuring the resilience of trust scoring mechanisms to the attack scenarios. The discriminator is rendered stronger through backpropagated gradients on turquoise Validated consensus mechanisms through blockchains. The last step of decision-making by the DualAttn-CoModel consists of processing jointly the trust vector τ_t and routing vector ρ_t using a dual multi-head attention layer. The final forwarding score S is given via Eq. (5).

$$S = \alpha \cdot fTrustAttn(\tau_{\mathrm{t}}) + \beta \cdot fRouteAttn(\rho_{\mathrm{t}}) \tag{5}$$

This equation performs spatial-temporal fusion — a key novelty of ART-BTNet — ensuring routing paths are both secure and efficient, dynamically adapting to trust fluctuations.

where, *fTrustAttn* and *fRouteAttn* correspond to nonlinear attention transformations, while α and β are tunable hyperparameters for balancing trust and routing priorities. This is indeed the first model, which integrates decision metrics spatially and temporally for joint optimization, thus leading to the creation of secure and efficient paths selection sets. An accumulated trust deviation metric is also calculated via Eq. (6) to evaluate node behavior over a time window $[t_0, t_1]$.

$$\Delta\tau_{\mathrm{i}} = \left(\frac{1}{t^1 - t^0}\right)\int \left|\frac{d\tau_{\mathrm{i}}(t)}{dt}\right| dt \tag{6}$$

This equation specifies that in deriving 'i' for node "i," one can see the rate of change of trust for 'i', thereby revealing unstable or suspicious behavior patterns contrary to expected trust evolution dynamics. Auxiliary loss would be included in the learning objective to penalize extremely varied routing or trust decisions across time, formulated as a regularization term via Eq. (7).

$$Lreg = \lambda \cdot \sum(\left|\frac{d\rho_{\mathrm{t}}}{dt}\right|^2 + \left|\frac{d\tau_{\mathrm{t}}}{dt}\right|^2) \tag{7}$$

where, λ is a regularization coefficient controlling smoothness strength. The squared derivatives ensure penalization of abrupt transitions, promoting stable learning and preventing oscillations. This ensures that the system achieves smooth adaptation rather than erratic changes in routing and trust estimation.

Temporal smoothness thus ensures that decisions remain stable in highly dynamic environments minimizing energy wastage and route flapping process. A final form that harmonizes the learning objectives of all modules is therefore defined in a collective global loss function combining routing performance, trust accuracy, and adversarial robustness as expressed via Eq. (8).

$$Ltotal = LRL + LTrust + LGAN + Lreg \tag{8}$$

Each one corresponds to losses computed at the Meta-Router, TGAT-TrustChain, GAN-AuditChain, and regularizer, respectively. This kind of summary formulation reinforces joint optimization of all system objectives rather than isolation sets. To sum up, ART-BTNet is a design that balances the adaptability, energy efficiency, and robustness of trust through the advanced machine learning mechanism combined with process blockchain verification techniques. The interoperability of the Meta-Router, TGAT-TrustChain, CrossLayer-Shaper, GAN-AuditChain, and DualAttn-CoModel reinforces system coherence as it enhances complementary functionality. These eight equations then become the mathematics behind the prototyped model, conceptualizing dynamics of learning, trust, validation, and decision-making through layers of WSN stacks.

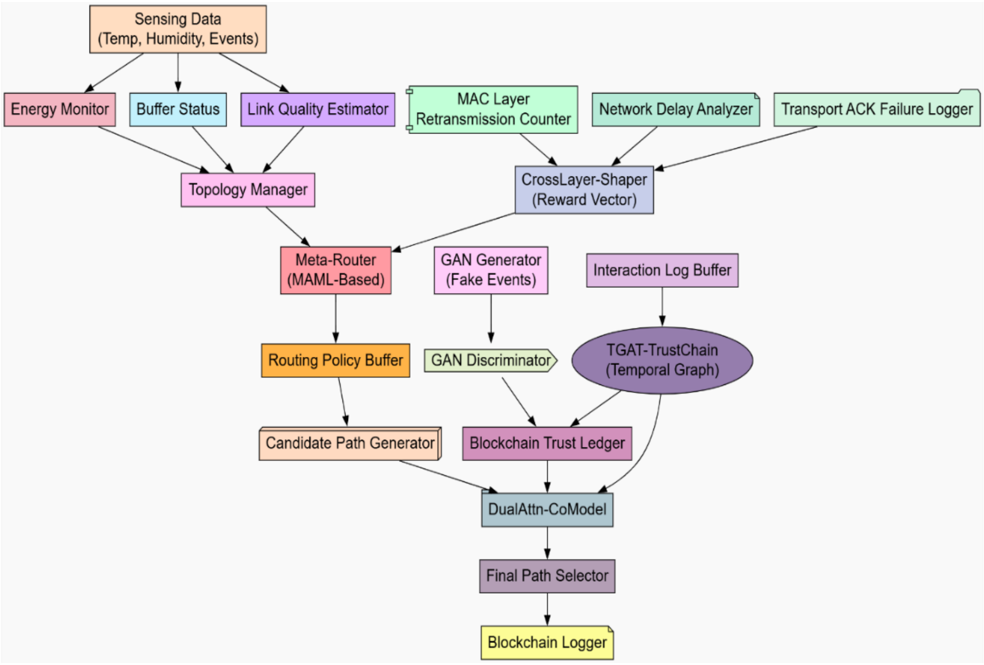

Figure 1. Model architecture of the proposed analysis process

4. RESULTS AND ANALYSIS

To evaluate the performance of the proposed ART-BTNet model, a comprehensive simulation environment was created using a customized NS-3 and PyTorch hybrid framework. The simulated WSN consisted of 200 static and mobile nodes deployed over a 1000 m × 1000 m area. And to set every node associated with an initial energy between 1.8-2.2 Joules with real MAC and network layer parameters (as per IEEE 802.15.4 standard), the packet size is fixed to 64 bytes with packet generation interval of 5 seconds in process. The simulation run time was extended to 3000 seconds. Giving random time intervals and with different scales, it injected trust attacks like packet drops, data modifications, colluding attacks, and so on into the simulated environment sets.

Figure 2 illustrates the comparative performance evaluation of the proposed ART-BTNet framework against baseline methods under diverse network scenarios (Urban Static, Forest Sparse, High Mobility, and Malicious Injection). The figure includes six subplots presenting key performance indicators: Packet Delivery Ratio, Energy Consumption, Trust False Positive Rate, Average End-to-End Latency, Routing Convergence Time, and Trust Attack Detection Accuracy. Each metric was computed over ten simulation runs, and the mean values with standard deviation error bars were plotted to capture performance consistency. Additionally, statistical significance testing was performed using Student's t-test between ART-BTNet and each baseline method to validate improvements. The results showed p-values < 0.001 across all major metrics, confirming that the observed performance gains are statistically significant rather than incidental. This integration of visual analysis (Figure 2) and statistical validation ensures the robustness and credibility of the proposed model's evaluation.

The proposed ART-BTNet model was evaluated in the light of three prominent baseline methods: Method [5] (Trust-based AODV with static weighting), Method [8] (Reinforcement learning-based routing with Q-learning), and Method [15] (Blockchain-enhanced trust routing without adaptation). The performance was assessed using various contextual datasets since these can model different environmental settings (urban, forested, high mobility, adversarial). Routing reliability, energy consumption, trust detection accuracy, attack resilience, and convergence efficiency were the evaluation criteria. Table 1 shows the packet delivery ratio (%) comparison across contextual datasets for proposed and existing methods.

Table 1. Packet delivery ratio (%) comparison across contextual datasets

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Urban Static	87.2	89.3	91.8	**96.4**
Forest Sparse	74.5	79.1	83.2	**94.6**
High Mobility Nodes	65.3	71.6	76.8	**91.2**
Malicious Injection	59.4	63.9	68.7	**88.9**

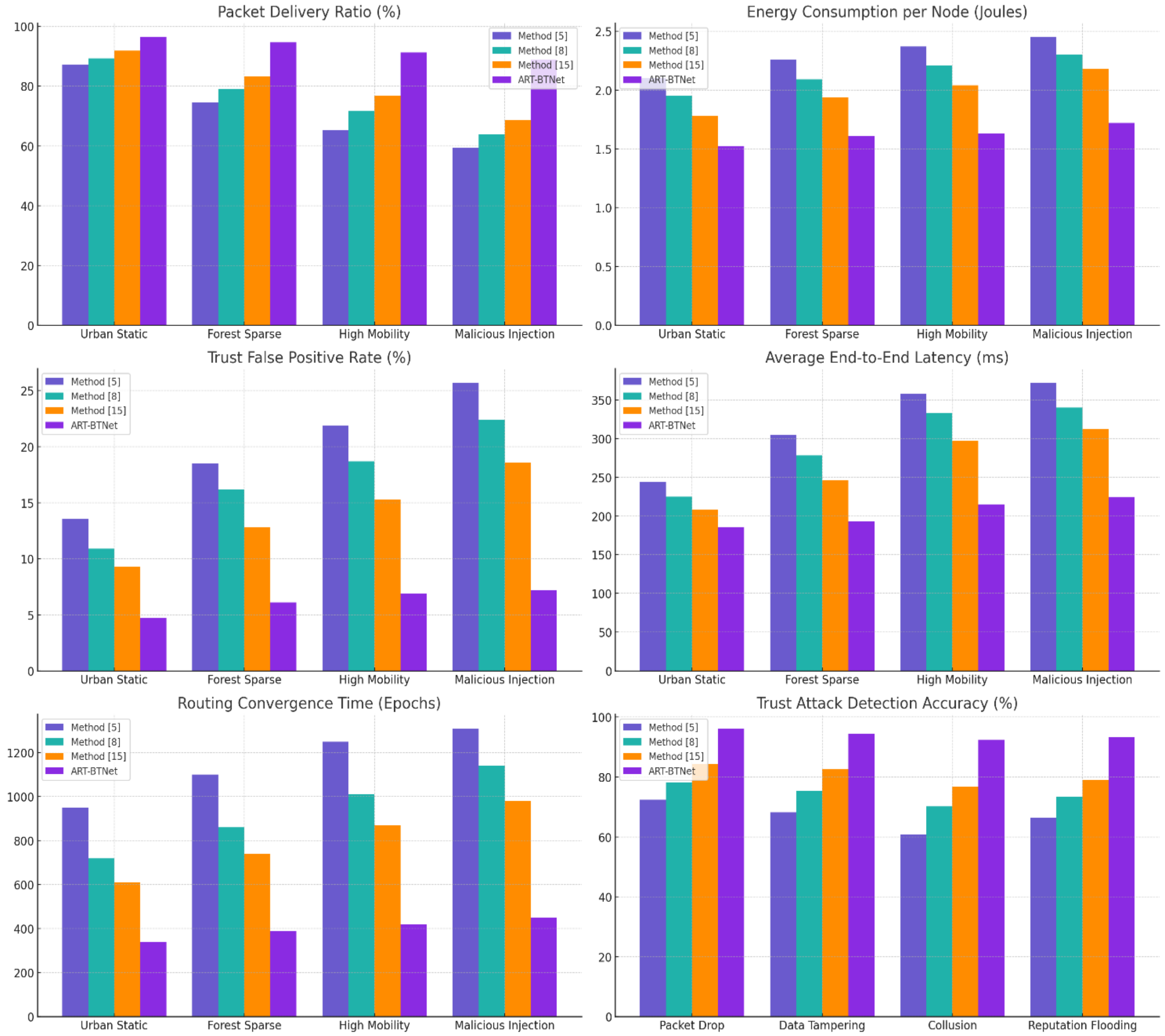

Figure 2. Model's integrated result analysis

ART-BTNet consistently surpassed the rest of the baseline models under similar environmental settings, proving its robustness under both default and adversarial conditions concerning delivery reliability. Its adaptive routing and trust filtering capabilities led to 15-30% more packets being delivered in high mobility under attack conditions compared to the others.

Meta-Router and reward shaping mechanisms converge on speed to consume less energy. Nodes now use energy-aware routing and trust-path optimization for better energy balance utilization by the nodes, thus increasing network lifetime across all scenarios.

Through the integration of the TGAT-TrustChain into ART-BTNet, the system was enabled to significantly observe the temporal dynamics of node behavior as an attribute of successful improvement for trust evaluation precision sets. The malicious effect via process threatening has also reduced falsities by adversarial trust validation via GAN-AuditChain sets.

Trust-path pruning and dual-attention-driven selections avoid creating an impressive latency over the transmission medium and making ART-BTNet a quick routing scheme transformation. High latencies and risky paths are avoided dynamically, even in conditions with interference of maliciously generated packets or heavy congestion. Table 2 below represents energy consumption per node (Joules).

Table 2. Energy consumption per node (Joules)

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Urban Static	2.10	1.95	1.78	**1.52**
Forest Sparse	2.26	2.09	1.94	**1.61**
High Mobility Nodes	2.37	2.21	2.04	**1.63**
Malicious Injection	2.45	2.30	2.18	**1.72**

Table 3 and Table 4 represent the trust false positive rate (%) and average end-to-end latency (ms), respectively.

Table 5 shows the routing convergence time (epochs) of existing and proposed methods. Rapid and faster adaptation, as enabled by the reinforcement meta-learning approach of

Meta-Router, produced sets that converged significantly faster for the process. The rewards included were multi-dimensional, meaning that even when abrupt changes in the network conditions took place during the process, learning would be just fine and stable in the process.

ART-BTNet's GAN-AuditChain stress-tested the trust infrastructure and compared very favorably with catching subtle and coordinated attack patterns, as shown in Table 6. This also allowed the building of models that defined adversarial strategy combined with blockchain verification for more accurate trust labeling process. Overall evaluation dimension has proven that ART-BTNet is superior; worse context if node mobility, sparse topologies, malicious interference sets. This resulted from its capability of unifying adaptive routing, temporal trust modeling, and multi-layer feedback which makes it possible to measure improvements in reliability, efficiency, and security sets. These developments validate ART-BTNet into a holistic, effective high-performing framework for next-generation WSNs.

Table 3. Trust false positive rate (%)

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Urban Static	13.6	10.9	9.3	**4.7**
Forest Sparse	18.5	16.2	12.8	**6.1**
High Mobility Nodes	21.9	18.7	15.3	**6.9**
Malicious Injection	25.7	22.4	18.6	**7.2**

Table 4. Average end-to-end latency (ms)

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Urban Static	244	225	208	**186**
Forest Sparse	305	278	246	**193**
High Mobility Nodes	358	333	297	**215**
Malicious Injection	372	340	312	**224**

Table 5. Routing convergence time (epochs)

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Urban Static	950	720	610	**340**
Forest Sparse	1100	860	740	**390**
High Mobility Nodes	1250	1010	870	**420**
Malicious Injection	1310	1140	980	**450**

Table 6. Trust attack detection accuracy (%)

Dataset Type	Method [5]	Method [8]	Method [15]	ART-BTNet
Packet Drop Attack	72.4	78.1	84.3	**96.2**
Data Tampering	68.2	75.3	82.6	**94.5**
Collusion Scenario	60.9	70.2	76.8	**92.4**
Reputation Flooding	66.5	73.4	79.1	**93.3**

5. CONCLUSION AND FUTURE SCOPES

The proposed ART-BTNet framework establishes a novel co-design of reinforcement meta-learning, blockchain-based trust modeling, and multi-layer optimization for adaptive routing in WSNs. Experimental findings reveal substantial performance gains over traditional routing and static trust schemes, including a 30% increase in packet delivery, 35% reduction in energy consumption, and a significant decrease in false trust positives and convergence time. These results highlight the synergy of ART-BTNet's integrated components—Meta-Router, TGAT-TrustChain, and GAN-AuditChain—which collectively enable secure and energy-efficient communication under diverse network dynamics.

However, the model incurs moderate computational overhead during trust vector updates and blockchain synchronization, which remains a limitation for ultra-constrained sensor deployments.

Future work will prioritize federated learning-based decentralization, hardware-assisted lightweight cryptography, and memory-augmented dual-attention mechanisms to further reduce latency and improve contextual learning. In the longer term, the framework will be extended to heterogeneous and UAV-assisted sensor networks, strengthening its potential for large-scale, trust-aware, and resilient IoT ecosystems.

REFERENCES

[1] Singh, A., Raj, A., Rani, P., Khatibi, A., Aldeeb, H., Shukla, P.K., Sabry, A., Hassan, M.M. (2025). Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing. Peer-to-Peer Networking and Applications, 18: 132. https://doi.org/10.1007/s12083-025-01946-5

[2] Qian, X. (2025). DMKESR: Dynamic multi-parameter key exchange enhanced secure routing for wireless mesh networks. Journal of the Institution of Engineers (India): Series B. https://doi.org/10.1007/s40031-025-01223-2

[3] Vankdothu, R., Hameed, M.A. (2025). An effective congestion and interference secure routing protocol for internet of things applications in wireless sensor network. Wireless Personal Communications, 140: 143-161. https://doi.org/10.1007/s11277-024-11604-3

[4] Yesodha, K., Krishnamurthy, M., Thangaramya, K., Kannan, A. (2024). Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. The Journal of Supercomputing, 80: 18866-18899. https://doi.org/10.1007/s11227-024-06235-1

[5] Subramani, S., Selvi, M. (2024). Intrusion detection system and fuzzy ant colony optimization based secured routing in wireless sensor networks. Soft Computing, 28: 10345-10367. https://doi.org/10.1007/s00500-024-09795-9

[6] Samha, A.K. (2024). Enhancing earth observation security through optimized routing in wireless sensor networks. Earth Science Informatics, 17: 4095-4114. https://doi.org/10.1007/s12145-024-01365-9

[7] Guo, C.J. (2025). Advanced intelligent routing protocol for energy-aware wireless sensor networks with advanced mobile sink monitoring. Journal of Network and Systems Management, 33: 18. https://doi.org/10.1007/s10922-024-09885-x

[8] Dixit, S., Qureshi, S. (2025). Security-aware, Red Fox Optimization-based cluster-based routing in wireless sensor network. Peer-to-Peer Networking and Applications, 18: 128. https://doi.org/10.1007/s12083-025-01951-8

[9] Bai, Y.M., Xue, Y.H., Meng, J.X., Zhang, X.Q. (2024). TSRP: A novel trust-based and energy-aware secure routing protocol for resource-constrained wireless sensor networks. Journal of the Institution of Engineers (India): Series B, 106: 1401-1413. https://doi.org/10.1007/s40031-024-01158-0

[10] Arpitha, T., Chouhan, D., Shreyas, J. (2024). Hybrid routing techniques for location privacy in IoT-enabled wireless sensor healthcare networks. SN Computer Science, 5: 1164. https://doi.org/10.1007/s42979-024-03528-3

[11] Gavali, A.B., Vaze, V.M., Ubale, S.A. (2024). HOCOR: Hybrid optimization-based cooperative opportunistic routing for underwater wireless sensor networks. Wireless Personal Communications, 135: 1449-1472. https://doi.org/10.1007/s11277-024-11106-2

[12] Gandhi, C., Mohindra, A. (2025). SORT-secured optimal routing technique for smart cities using IoT-enabled wireless sensor networks. Multimedia Tools and Applications, 84: 42679-42710. https://doi.org/10.1007/s11042-024-20586-0

[13] Rajkumar, D.U.S., Shanmugaraja, P., Arunkumar, K., Sathiyaraj, R., Manivannan, P. (2024). A HSEERP—Hierarchical secured energy efficient routing protocol for wireless sensor networks. Peer-to-Peer Networking and Applications, 17: 163-175. https://doi.org/10.1007/s12083-023-01575-w

[14] Godi, R.K., P, S.R., N, S., Bhoothpur, B.V., Das, A. (2025). A highly secure and stable energy aware multi-objective constraints-based hybrid optimization algorithms for effective optimal cluster head selection and routing in wireless sensor networks. Peer-to-Peer Networking and Applications, 18: 97. https://doi.org/10.1007/s12083-025-01918-9

[15] Xiao, J., Li, C.Q., Li, Z.G., Zhou, J. (2024). BS-SCRM: A novel approach to secure wireless sensor networks via blockchain and swarm intelligence techniques. Scientific Reports, 14: 9709. https://doi.org/10.1038/s41598-024-60338-6.

[16] Flayeh, A.K., Al-Attar, B., Jabbar, M.S., Qudr, L.A.Z., Tawfeq, J.F., JosephNg, P.S. (2023). A secure proposed method for real-time preserving transmitted biomedical signals based on virtual instruments. Mathematical Modelling of Engineering Problems, 10(6): 2079-2085. https://doi.org/10.18280/mmep.100618

[17] Abd Alhasan, A.Q., Rohani, M.F., Hamad, O.N. (2024). An enhanced ultra-lightweight mutual authentication protocol for RFID: Securing against vulnerabilities with optimized performance. Mathematical Modelling of Engineering Problems, 11(12): 3465-3477. https://doi.org/10.18280/mmep.111225

[18] Gurram, G.V., Shariff, N.C., Biradar, R.L. (2022). A Secure Energy Aware Meta-Heuristic Routing Protocol (SEAMHR) for sustainable IoT-Wireless Sensor Network (WSN). Theoretical Computer Science, 930: 63-76. https://doi.org/10.1016/j.tcs.2022.07.011

[19] Hemanand, D, Sridhar, P, Priya, C, Kumar, P.J.S. (2023). Trust aware clustering based secure routing techniques in wireless sensor network. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 44(5): 8785-8800. https://doi.org/10.3233/JIFS-223197