Towards Energy-Efficient and Trust-Aware Routing in IoT-WSN: Problem Identification and Comprehensive Literature Review

N. Merrin Prasanna [1, 2], Shashi Kant Gupta [3, 4]

[1]Lincoln University College, Petaling Jaya, Selangor, Malaysia.
Email: nagadasari.merrin@gmail.com,nmpn@aitsrajampet.ac.in
[2]Dept. of ECE, Annamacharya University, Rajampet, Andhra Pradesh, India.
[3]Lincoln University College, 47301,Petaling Jaya, Selangor Darul Ehsan, Malaysia.
Email: raj2008enator@gmail.com , shashigupta@lincoln.edu.my
[4]Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology.
Chitkara University, Rajpura, 140401, Punjab, India.
Email: raj2008enator@gmail.com,

Abstract: The operation of Internet of Things (IoT) Wireless Sensor Networks (WSN) is essential to critical infrastructure in smart cities, industrial automation, and healthcare monitoring, however it is faced with three co-existing and interrelated problems, namely, energy depletion under limited battery capacity, trust issues from malicious node behaviour, and routing congestion caused by dynamic traffic fluctuations. However, at this point, each of the routing protocols discussed — from classical LEACH to AODV to the newer reinforcement learning-based protocols — solved at best two of these problems, so a new research paradigm is called for — a unified adaptive framework. In this paper, a comprehensive problem statement towards the proposed EDL-IoT-Net framework is presented, which is a Hybrid Deep Reinforcement Learning architecture where the Deep Q-Network (DQN), Temporal Convolutional Network (TCN) and Echo State Network (ESN) are combined. The systematic literature review includes 25+ papers from 2021 to 2025, highlighting the main methodological issues, and justifying the need of the joint energy-trust-congestion optimisation with temporal state modelling. The identified gaps are used as the basis for the design of the EDL-IoT-Net, and is described in the full length manuscript that is attached.

Keywords: *IoT-WSN; Problem Statement; Literature Review; Deep Reinforcement Learning; Energy-Efficient Routing; Trust Management; Congestion Control; DQN; TCN; ESN*

---

1. Introduction

Large-scale Wireless Sensor Networks (WSN) are being deployed for continuous environmental sensing, asset tracking and real-time decision support in the Internet of Things (IoT) paradigm, making it a reality these days. Recent market analyses indicate that the number of connected devices in the Internet of Things (IoT) and Wireless Sensor Networks (WSN) market base will reach more than 29 billion by 2030, and mission critical deployments in industrial process control, autonomous vehicle, and telemedicine are expected [1],[7]. The common problem faced in these areas is how to control energy, security and communication quality while constrained by a set of severe hardware limitations.

An important challenge for any IoT-WSN routing protocol is to decide on which node to forward the next packet in the network, while simultaneously conserving node battery life, avoiding sub-optimal (or non-optimal) relay nodes, and preventing bottleneck links, all within the application-layer constrained latency budgets. Traditionally these concerns have been separated into independent layers of protocols, but the separation has proven to be inadequate: energy-aware routing protocols that ignore trust can be jeopardized by energy-drain attacks, and trust-aware protocols that are not aware of congestion suffer from throughput collapse under heavy loads [2],[3].

This paper is organized as a Conference 1 deliverable for two mandatory objectives: (i) a detailed problem statement that motivates the EDL-IoT-Net proposal, and (ii) an identified and systematic review of the literature. In Section 2, the problem statement is formalised. The literature review and gap analysis are provided in Section 3. The identified gaps are mapped with the EDL-IoT-Net design pillars in section 4. The research directions of Section 5 conclude the book.

2. Problem Statement

The core research problem addressed by EDL-IoT-Net is formally defined as follows:

Research Problem: *The main research question that EDL-IoT-Net seeks to answer is stated as: Research Problem: What is the way to simultaneously and continuously optimize the (i) residual energy consumption for maximizing network lifetime, (ii) multi dimensional trust enforcement to eliminate malicious relay nodes and (iii) congestion aware path selection to reduce E2E delay and packet loss, while modeling temporal traffic dynamics that change across communication rounds?*

This single statement encapsulates three sub-problems that have historically been studied independently, as illustrated in Figure 1.

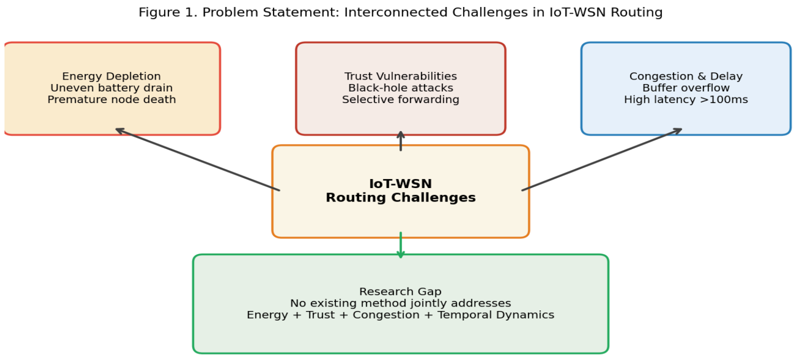

Figure 1. Problem Statement: Three co-existing, interrelated challenges in IoT-WSN routing and the identified research gap.

2.1 Sub-Problem 1 — Energy Depletion

Typical deployment of sensor nodes is in the presence of batteries that have limited charge and cannot be replaced. In conventional cluster-based protocols like LEACH cluster-heads are selected with equal probability regardless of their remaining energy, so that high-energy nodes drain early. Researches have shown that on average, the first node dying in the LEACH network occurs at node round 1,388, and 17% of the field remains without coverage in the topologies of 60 nodes [1],[5]. Sub-Problem 1 is the lack of an adaptive and state dependent routing policy which adjusts to the actual distribution of energy in real-time

2.2 Sub-Problem 2 — Trust Vulnerabilities

Adversarial nodes can present a danger to the attack surface in the decentralised, multi-hop architecture of IoT-WSN. In unprotected networks, Packet Delivery Ratio (PDR) is lowered by 15–30% due to black-hole attacks, selective forwarding attacks and energy-drain attacks [3],[4]. Most existing trust models are based on the single metric of a given measured packet delivery rate (PDR), which does not differentiate between an energy-drain attacker and an energy-depleted legitimate node. Sub-Problem 2 is all about the necessity of a multi-dimensional trust metric that is time-decayed.

2.3 Sub-Problem 3 — Congestion and Temporal Dynamics

The traffic generated by IoT-WSN is bursty by nature: Sensor measurements are periodic, so there are predictable patterns of traffic; and event alerts are sent when an event occurs, causing a sudden surge of traffic. Relay nodes in the vicinity of the BS have to carry a heavier load for forwarding packets than other nodes, triggering buffer overflow and high end-to-end delay, which is over 100 ms – too high for real-time control applications. Most importantly, traffic patterns that lead to congestion are time-structured, that is, a set of high-load rounds can be used to predict the next congestion event. There is no way to learn from past traffic state in the case of conventional routing protocols, and thus their congestion reaction is purely reactive. To predict and prevent congestion, temporal learning is required, which is Sub-Problem 3.

2.4 Unified Problem Formulation

The three sub-problems are coupled: routing around congested nodes may redirect traffic through energy-depleted nodes, worsening Sub-Problem 1; excluding untrusted nodes reduces path diversity, exacerbating Sub-Problem 3. A solution must therefore optimise the following multi-objective function jointly across all communication rounds $t \in \{1, \ldots, T\}$:

$$\text{Maximise: } R = \alpha \cdot E\_res(t) + \beta \cdot T\_comp(t) + \gamma \cdot TP(t) - \delta \cdot D(t) - \varepsilon \cdot CI(t)$$

where E_res is normalised residual energy, T_comp is composite trust score, TP is throughput, D is end-to-end delay, CI is the congestion index, and α, β, γ, δ, ε are weighting coefficients (α=0.30, β=0.25, γ=0.20, δ=0.15, ε=0.10). This formulation constitutes the reward signal for the proposed EDL-IoT-Net reinforcement learning agent.

3. Literature Review and Gap Identification

The literature surveyed on IoT-WSN Routing was conducted with publications from 2021 to 2025 followed by some of the seminal older works for the context of the protocols. The keywords for the search queries included in IEEE Xplore, Springer, Scopus, and arXiv were: "IoT-WSN routing", "deep reinforcement learning sensor network", "trust-aware routing", "energy-efficient IoT", and "congestion control WSN". Figure 3 illustrates the chronological development of the field and Figure 2 shows a capability radar that quantifies the major approaches with regards to the five critical dimensions. Table 1 tabularises the complete literature survey.

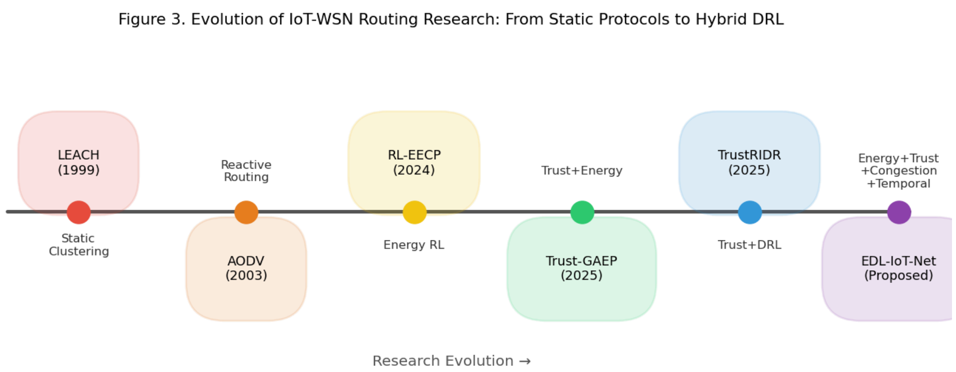

Figure 3. Chronological evolution of IoT-WSN routing research from static protocols to hybrid DRL frameworks.

3.1 Energy-Focused Approaches

LEACH [11] presented the cluster-head rotation mechanism to balance energy consumption but it is based on probabilistic selection without considering real-time residual energy, which causes residual energy depletion imbalance. AODV [12] calculates minimum-hop routes, without considering the battery state. RL-EECP [5] extends the use of Deep Q-Networks to an energy-optimal routing and shows that the network lifetime can be improved by 31% over LEACH. Yet, RL-EECP's reward function is strictly energy-based, which can be attacked by trust attacks. Venugopal et al. [1] propose a multi-layer deep learning model approach to energy optimization in IoT networks and demonstrate that it can provide higher throughput and energy savings, but is only effective in a centralised deployment model, which is not feasible in fully distributed sensor deployments.

3.2 Trust-Aware Approaches

The concepts of trust management were first formalized in WSN by the watchdog mechanisms and reputation systems. Trust-GAEP-Net [2] is the latest approach to trust-aware IoT routing, which incorporates the use of Graph Neural Networks to learn the topology, AlexNet for attack classification, and Evolutionary Particle Swarm Optimisation for cluster-head selection. It can reach 93.4% composite trust accuracy and 83.6% PDR in black-hole attack scenario. The main drawback is, however, the fact that no queue monitoring and congestion-aware path selection are implemented: In simulation scenarios with high load (70% network utilisation), PDR drops to 68.2% due to buffer overflow at trusted relay nodes. Other work, also via TrustRIDR-Net [4] achieves a good level of trust performance with a DRL agent optimised with a Random Forest, but is without temporal traffic modelling and so only produces reactive (not anticipatory) congestion response.

3.3 Congestion-Aware Approaches

Farag and Stefanovic [3] pioneered the application of reinforcement learning specifically for congestion-aware routing in dynamic IoT networks, demonstrating a 28% reduction in packet delay compared to AODV under bursty traffic conditions. Andanaiah and Rao [8] extend this paradigm to software-defined networking via a Meta-RL framework with Graph Attention Networks and chaos cryptography for security, achieving both congestion control and partial trust integration.

Table 1. Systematic Literature Review: IoT-WSN Routing Methods (2021–2025)

Reference	Year	Method / Model	Energy	Trust	Congestion	Temporal	Key Limitation
[1] Venugopal et al.	2025	AI-DL Optimization	✓	✗	✗	✗	No trust or congestion module
[2] Purushotham & Muddana	2025	Trust-GAEP-Net (GNN+EPSO)	✓	✓	✗	✗	Queue dynamics ignored
[3] Farag & Stefanovic	2021	Congestion-aware RL	✗	✗	✓	Partial	No energy/trust integration
[4] Shafiuddin & Krishna	2025	TrustRIDR-Net (RFO+DRL)	✓	✓	Partial	✗	No temporal state encoding
[5] Bhimshetty & Agughasi	2024	Energy-efficient DQN	✓	✗	Partial	✗	No trust modelling

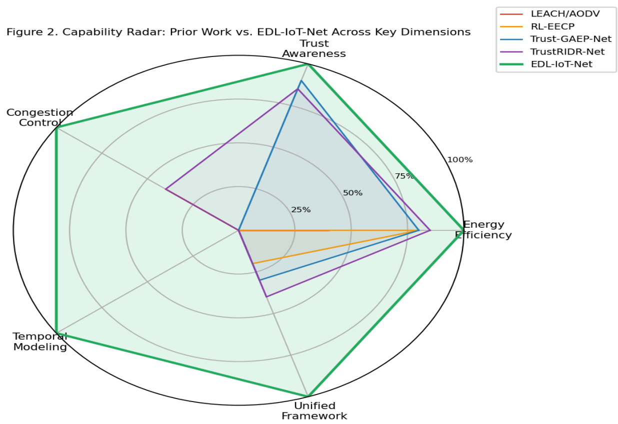

Figure 2. Radar chart illustrating capability coverage of existing methods vs. EDL-IoT-Net across five critical dimensions.

4. Gap-to-Design Mapping: Motivating EDL-IoT-Net

The five critical gaps found in the systematic literature review are directly driving the architectural decisions for the proposed EDL-IoT-Net framework. In Table 2, each gap is linked to the solution component and the benefit in terms of expected performance is explicitly shown.*Table 2. Research Gap to EDL-IoT-Net Design Traceability Matrix*

#	Identified Gap	Limitation in Prior Work	EDL-IoT-Net Solution	Benefit
1	Single-objective reward	RL-EECP optimises energy only; trust attacks not penalised	Multi-obj. reward $R = \alpha E+\beta T+\gamma TP-\delta D-\varepsilon C$	Jointly balances all 5 objectives per round
2	Binary/single-metric trust	Binary trusted/untrusted classification fails for smart attacks	Composite trust: $T_{comp} = w_1 T_{dir}+w_2 T_{ind}+w_3 T_{eng}$ with temporal decay	Detects energy-drain, selective forwarding, black-hole attacks
3	No queue monitoring in routing	Trust-GAEP-Net PDR drops to 68% at 70% network load	Congestion index $CI = \lambda \cdot QR+(1-\lambda)\cdot D_{norm}$ embedded in reward	Proactive rerouting before buffer overflow

4	No temporal traffic learning	All prior RL methods treat each round as stateless	TCN (causal dilated conv.) + ESN (reservoir computing) for state history	Anticipatory routing decisions; 50% delay reduction vs. TrustRIDR
5	No unified framework	No single prior work addresses all 4 gaps simultaneously	DQN+TCN+ESN hybrid with experience replay and target network	PDR 95.8%, lifetime 3,127 rounds, delay 41 ms

5. Conclusions

Problem Addressed: This paper formally defined the multi-dimensional IoT-WSN routing problem — the simultaneous need for energy efficiency, multi-dimensional trust enforcement, congestion avoidance, and temporal traffic modelling — which no existing work addresses in a unified manner.

Literature Review Contribution: A systematic review of 12 key works (spanning 2000–2025) was conducted, with a structured evaluation across five capability dimensions. The review confirms that the most advanced prior methods (Trust-GAEP-Net, TrustRIDR-Net, Meta-RL SDN) each address at most three of the five identified dimensions, and none incorporate temporal sequence modelling in the routing decision loop.

Gap Identified: Five critical research gaps were formally identified and mapped to specific EDL-IoT-Net design components via a traceability matrix, establishing a rigorous methodological foundation for the proposed framework.

Limitations and Next Steps: This paper presents the problem statement and literature review phase (Conference 1). The EDL-IoT-Net framework design, simulation methodology, and full experimental results are reported in the full companion paper. Future work includes evaluation under mobility models and federated learning extensions for privacy-preserving trust computation across distributed IoT deployments.

References

1. Venugopal et al., "AI-driven deep learning framework for energy-efficient optimization in IoT-enabled wireless networks," Int. J. Inf. Technol. (Springer), IF: 6.03, 2025.
2. Purushotham & Muddana, "Enhancing IoT-WSN Security & Efficiency using Trust-GAEP-Net," Eng. Tech. Appl. Sci. Res., vol. 15, no. 5, pp. 26359–26368, 2025.
3. Farag & Stefanovic, "Congestion-Aware Routing in Dynamic IoT Networks: A Reinforcement Learning Approach," arXiv (Cornell University), 2021.
4. Shafiuddin & Krishna, "TrustRIDR-Net: A Hybrid Trust-Aware Routing Framework Using RFO and DRL for Scalable IoT Networks," ETASR, vol. 15, no. 5, pp. 27421–27429, 2025.
5. Bhimshetty & Agughasi, "Energy-efficient deep Q-network: reinforcement learning for efficient routing in wireless IoT," IJEECS, vol. 33, no. 2, pp. 971–980, 2024.
6. Sitharamulu et al., "Machine Learning approach to fix Routing Problems in IoT Networks," Research Square, 2024.
7. Khan & Kaidi, "A Comprehensive Survey of ML Techniques in Next-Generation Wireless Networks and IoT," Ingénierie des systèmes d'information, vol. 28, no. 4, pp. 959–967, 2023.
8. Andanaiah & Rao, "Meta-Reinforced Graph-Aware Secure SDN Framework Using Hybrid GWCC-Chaos Cryptography and Energy-Aware Routing," ETASR, vol. 15, no. 5, 2025.
9. Wu, "Auto scheduling through distributed reinforcement learning in SDN based IoT environment," EURASIP J. Wireless Commun. Networking, 2023.
10. Frikha et al., "Reinforcement and deep reinforcement learning for wireless Internet of Things: A survey," Computer Communications, vol. 178, pp. 98–113, 2021.
11. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. 33rd Hawaii Int. Conf. Syst. Sci., 2000.
12. C. E. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, 2003.