TrustRIDR-Net: A Hybrid Trust-Aware Routing Framework Using RFO and DRL for Scalable IoT Networks

Shaik Shafiuddin
Department of Computer Science and Engineering, School of Computing, Mohan Babu University, Tirupati, Andhra Pradesh, India
shafiuddin111@gmail.com (corresponding author)

Konda Hari Krishna
Department of Computer Science and Engineering, School of Computing, Mohan Babu University, Tirupati, Andhra Pradesh, India
khk396@gmail.com

Received: 22 May 2025 | Revised: 4 August 2025 | Accepted: 11 August 2025

 DOI: https://doi.org/10.48084/etasr.12294

ABSTRACT

This paper presents TrustRIDR-Net, a novel hybrid trust-based routing framework for Internet of Things (IoT) networks that intelligently integrates biologically-inspired optimization and adaptive machine learning for secure, energy-efficient, and scalable communication. TrustRIDR-Net achieves a throughput of 17,560 kbps, a Packet Delivery Ratio (PDR) of 98.9%, and reduces energy consumption to 68%, significantly outperforming state-of-the-art models. The proposed model combines Rider Foraging Optimization (RFO) for trust-aware clustering and Deep Reinforcement Learning (DRL) for dynamic routing decisions, while incorporating a comprehensive trust metric based on seven behavioral and energy-related factors: Direct Trust, Indirect Trust, Forwarding Rate, Integrity, Availability, Consistency, and Energy Trust. The model dynamically computes trust scores and routing policies, while ensuring energy-aware transmission using a scalable power control formula. Extensive simulations conducted in a 200×200 m virtual IoT environment with 100 nodes and a centrally placed base station showed that TrustRIDR-Net outperformed existing models such as LSTM, GRU, LEACH, BFA, LOA, and AODV-based techniques. These results validate TrustRIDR-Net's capacity to support resilient, intelligent communication in large-scale, trust-sensitive IoT networks, setting the stage for its deployment in critical applications such as smart cities, healthcare monitoring, and industrial automation.

Keywords-IoT networks; metric; integrity; energy; trust; lifetime; machine learning; optimization

I. INTRODUCTION

The Internet of Things (IoT) has transformed modern communication by interconnecting billions of smart devices across diverse sectors, including smart cities, healthcare, agriculture, and industrial automation [1-3]. These networks consist of resource-constrained sensor nodes that collaboratively collect, process, and transmit data to central servers or cloud platforms [2]. As IoT ecosystems continue to scale, ensuring secure, reliable, and energy-efficient communication becomes increasingly critical [3-5]. The decentralized and dynamic nature of these networks makes them particularly vulnerable to issues such as malicious attacks, unreliable node behavior, and rapid energy depletion, all of which degrade overall system performance and reliability [6-9]. Traditional routing protocols in IoT networks often prioritize energy minimization or shortest-path routing without considering the behavioral aspects of the participating nodes [10-12]. Although these models may perform well under static or ideal conditions, they falter under dynamic and adversarial scenarios where nodes may behave selfishly or maliciously [12-17]. Moreover, most existing trust-based models use limited trust metrics or rely on fixed routing strategies, making them less adaptable to changing environments [18-19]. This creates a significant gap in the design of intelligent routing systems that are both trust-aware and adaptively optimized [20].

The main contributions of this work are summarized as follows:

- Integrates Rider Foraging Optimization (RFO) with Deep Reinforcement Learning (DRL) for adaptive and secure routing.
- Designs a comprehensive 7-dimensional trust metric combining behavioral and energy factors.

- Introduces an energy-aware transmission model to reduce consumption and extend network lifetime.
- Extensive simulation demonstrated superior performance, achieving 17,560 kbps throughput, 98.9% PDR, and a lifetime of 1250 rounds.

II. RELATED WORKS

In [21], the Cluster and Optimal Routing Assisted Cryptograph (CORAC) model was introduced, intended for cluster-based networks. However, despite its high PDR, the reliance on static cluster formation has limitations in highly dynamic or mobile network environments. In [22], the Bacteria Foraging Algorithm (BFA) was employed to improve routing in wireless sensor networks. Despite its effectiveness, BFA has slow convergence times and is sensitive to initial parameter selection, making it inefficient in highly dynamic networks. In [23], the SGPL model was proposed, which is an intelligent game-based secure collaborative communication scheme for metaverse environments through 5G and beyond networks. However, the SGPL model is highly dependent on precise and consistent network parameters. In [24], the Sand Cat Swarm Optimization Algorithm (SCSOA) was developed for IoT-based WSN security and routing. However, this model struggles to identify malicious nodes effectively, making the network vulnerable to potential security breaches and reducing its overall integrity in adversarial environments. In [25], the Lion Optimization Algorithm (LOA) was introduced, achieving a PDR of 94.24%, which, despite its strong routing performance, suffers from local optimization issues in complex network topologies.

In [26], graph-based deep learning models used in communication networks were reviewed. Complexity limits real-time applicability, and integrating GNNs with existing network protocols remains difficult due to compatibility issues. In [27], a data fusion trust model was introduced, which assesses trust using temporal attributes and behavioral analysis. In [28], a trust model was proposed for opportunistic routing, relying on node behavior to assess trust. This model performed well in detecting malicious nodes and improving network reliability.

III. PROPOSED SYSTEM

Figure 1 outlines the proposed method, which aims to build a trust-centric, energy-aware, and intelligent communication system for IoT networks. At its core lies the TrustRIDR-Net framework, which blends Rider Foraging Optimization (RFO) for trust-aware clustering with Deep Reinforcement Learning (DRL) for adaptive and resilient routing.

Before initiating optimization or trust evaluation, the IoT network must be initialized. This includes setting up nodes, defining base station location, assigning initial energy, and establishing the communication model. Let N denote the total number of sensor nodes. The Base Station (BS) is located at coordinates $BS(x_{bs}, y_{bs})$. Each node i is initialized with energy E_0.

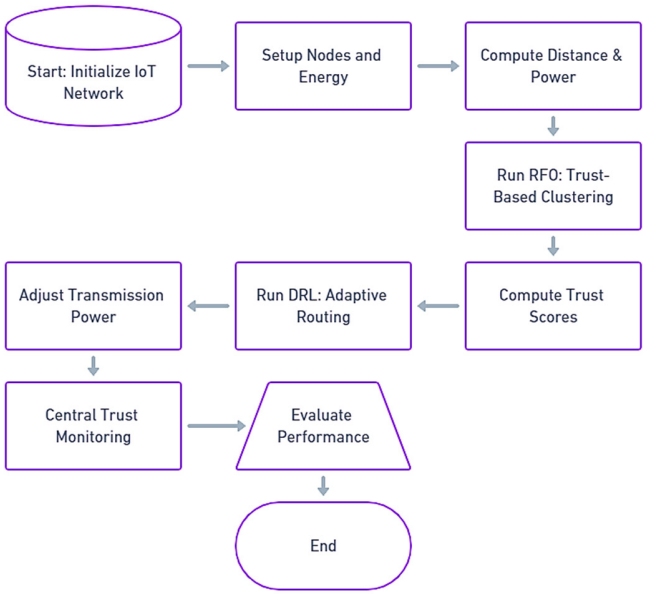

Fig. 1. Block diagram of the proposed method.

The Euclidean distance between any two nodes i and j is calculated as:

$$d(i,j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (1)$$

To model energy consumption, the transmit power for a node i to communicate with the BS is given by:

$$P_{tx}(i) = P_0 + P_{amp} \cdot [d(i, BS)]^n \quad (2)$$

where P_0 is the base transmission power , P_{amp} is the amplifier constant, and n is the path-loss exponent

TrustRIDR-Net comprises two intelligent modules: Rider Foraging Optimization (RFO) for initial trust-aware clustering and path selection, and Deep Reinforcement Learning (DRL) for dynamic policy-driven routing adaptation. Each node i computes a composite trust score T_i based on seven trust factors:

$$T_i = w_1 DT_i + w_2 IT_i + w_3 FT_i + w_4 IF_i + w_5 AF_i + w_6 CF_i + w_7 ET_i \quad (3)$$

subjected to:

$$\sum_{j=1}^{7} w_j = 1 \quad (4)$$

Direct Trust (DT) is based on past interactions:

$$DT_i = \frac{1}{|N_i|} \sum_{j \in N_i} C_{ij} \quad (5)$$

Indirect Trust (IT) is based on neighbor recommendations:

$$IT_i = \frac{1}{|N_i|} \sum_{j \in N_i} T_j \quad (6)$$

Forwarding Rate (FT) is the packet forwarding behavior:

$$FT_i = \frac{P_{fwd}(i)}{P_{recv}(i)} \quad (7)$$

Integrity Factor (IF) denotes the validity of forwarded packets:

$$IF_i = \frac{P_{valid}(i)}{P_{total}(i)} \quad (8)$$

Availability Factor (AF) is the node uptime:

$$AF_i = \frac{T_{active}(i)}{T_{obs}(i)} \quad (9)$$

Consistency Factor (CF) is a comparison with neighbors:

$$CF_i = \frac{1}{|N_i|}\sum_{j\in N_i}\left(1 - \frac{|D_i - D_j|}{D_i}\right) \quad (10)$$

Energy Trust (ET) is the remaining energy ratio:

$$ET_i = \frac{E_i^{curr}}{E_i^{init}} \quad (11)$$

The final trust score is calculated as a weighted sum of seven factors, where behavioral metrics (Direct, Indirect, Forwarding, Integrity, Availability, Consistency) collectively hold higher weights compared to Energy Trust to prioritize secure and reliable behavior. However, the inclusion of Energy Trust ensures that nodes with low residual energy are deprioritized to prolong network lifetime.

Once RFO initializes the topology, DRL refines routing through policy learning. The DRL agent learns from environmental feedback and updates its routing decisions to maximize trust, minimize energy use, and reduce hop counts.

State S_t includes $T_i, E_i, d(i, BS)$, and H_i.

Action A_t is the selection of the next-hop node.

The reward function is:

$$R_t = \alpha_1 \cdot \Delta T + \alpha_2 \cdot \Delta E - \alpha_3 \cdot D_{hop} \quad (12)$$

where ΔT is the improvement in trust, ΔE is the energy saved, D_{hop} is the hop distance, and $\alpha_1, \alpha_2, \alpha_3$ are reward weights. DRL algorithms like DQN or PPO are used to learn and optimize the routing policy over time.

To reduce energy waste and improve longevity, each node adjusts its transmission power based on distance:

$$P_{tx}(i) = P_0 \cdot \left(\frac{d(i,BS)}{d_{max}}\right)^{\gamma} \quad (13)$$

where $d(i, BS)$ is the distance of node i to the BS, d_{max} is the maximum distance in the network, and γ is the path-loss exponent. This ensures that nodes use only the necessary power for reliable communication. A centralized controller periodically evaluates trust and helps in activating reliable relay nodes and preventing routing through untrusted or malicious nodes. The relay selection probability is given by:

$$P_{relay}(i) = \frac{T_i}{\sum_{j\in N_i} T_j} \quad (14)$$

Comprehensive Neighborhood Trust is given by:

$$CT_i = \frac{1}{n}\sum_{k=1}^{n} T_k \quad (15)$$

A. *Performance Evaluation Metrics*

The following key performance metrics are used To validate the effectiveness of TrustRIDR-Net:

Network lifetime:

$$T_{life} = min(T | E_i(t) = 0) \quad (16)$$

Alive nodes over time:

$$N_{alive}(t) = \sum_{i=0}^{N} 1(E_i(t) > 0) \quad (17)$$

Throughput:

$$Throughput(t) = \sum_{i=1}^{N} P_{sucess}(i, t) \quad (18)$$

Total energy consumption:

$$E_{total}(t) = \sum_{i=1}^{N}[E_{tx}(i, t) + E_{rx}(i, t)] \quad (19)$$

B. *Proposed Model*

The TrustRIDR-Net architecture integrates two intelligent modules, RFO and DRL, into a unified, trust-centric routing framework for IoT networks. The process begins with the RFO module, which performs trust-aware clustering by identifying suitable cluster heads and evaluating nodes based on trust, energy, and stability. This results in a secure, organized topology of trusted relay nodes. Next, the DRL module refines routing paths dynamically, using environmental feedback to select optimal routes that balance trustworthiness, energy efficiency, and hop count.

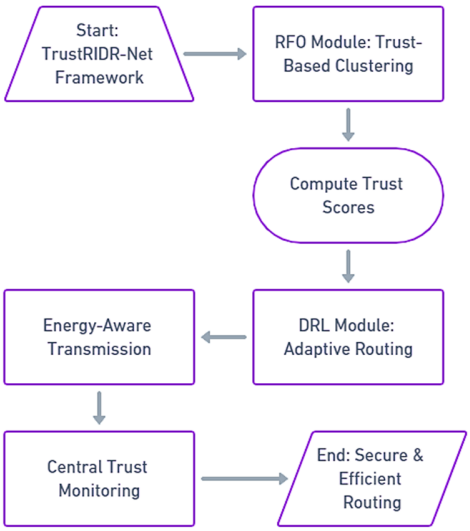

Fig. 2. Proposed model architecture.

The core novelty of TrustRIDR-Net lies in its dual-layer optimization strategy. The RFO module performs trust-aware clustering by selecting cluster heads based on trust and energy, ensuring secure and stable topology formation. The DRL module dynamically learns optimal routing policies, enabling adaptive decision-making in real-time. This synergy surpasses conventional models that rely on static clustering or heuristic routing, as it combines bio-inspired exploration with learning-based exploitation for improved throughput, PDR, and network lifetime.

C. Algorithm of the Proposed Model

Algorithm 1 describes the TrustRIDR-Net smart routing framework for IoT networks.

```
Algorithm: TrustRIDR-Net Model
1: Start the TrustRIDR-Net Framework
2: Execute the RFO Module
3: Calculate trust scores for all nodes
4: Execute the DRL Module
5: Apply Energy-Aware Transmission
6: Perform Centralized Trust
   Monitoring
7: End with secure, energy-efficient, and
   adaptive routing across the network
```

IV. RESULTS AND DISCUSSION

The parameters in Table I define the virtual IoT environment for the TrustRIDR-Net simulation. A total of 100 nodes are randomly deployed in a 200×200 m area, with each node having an initial energy of 2 J. Figure 3 illustrates the spatial layout of the IoT network, where 100 sensor nodes are randomly deployed within a 200×200 m field. Each blue dot represents an individual IoT node, while the red square at the center marks the base station located at coordinate (100, 100).

TABLE I. SIMULATION PARAMETERS

Parameter	Symbol	Value/Range
Number of nodes	N	100
Initial energy	E_0	2 J
BS position	BS	(100, 100)
Transmission range	–	25 meters
Path loss exponent	n	2 (Free Space Model)
Simulation area	–	200m × 200m
Amplifier constant	P_{amp}	0.0013 pJ/bit/m⁴
Base transmit power	P_0	50 nJ/bit

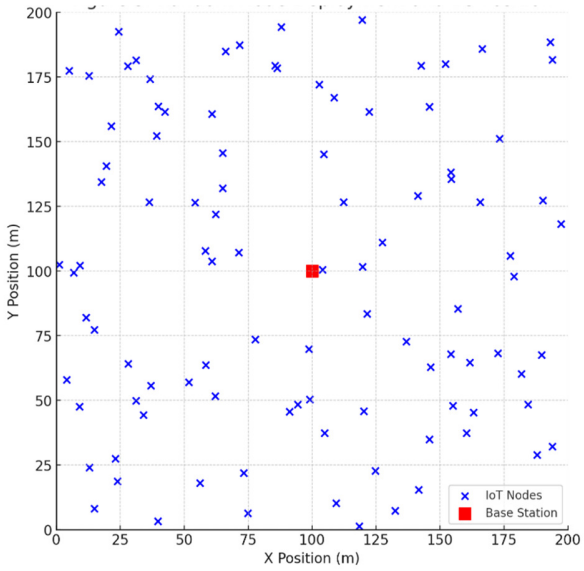

Fig. 3. Layout of random node deployment.

Table II outlines the configuration used for the Rider Foraging Optimization (RFO) algorithm during trust-aware clustering.

TABLE II. RFO CONFIGURATION PARAMETERS

Parameter	Value
Number of riders (Solutions)	50
Maximum iterations	100
Trust threshold	0.6
Step size adjustment (ROA)	Adaptive
BFO chemotactic steps	20
Cluster head selection bias	High trust and energy
Clustering radius	25 meters

Figure 4 demonstrates the outcome of cluster formation using the RFO mechanism. The network consists of 100 randomly deployed nodes, grouped into five clusters based on trust, proximity, and energy levels.

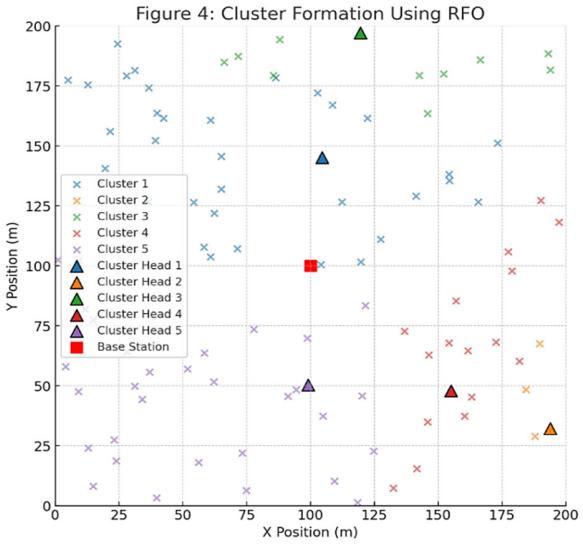

Fig. 4. Cluster formation.

Table III shows the configuration of the DRL module used in the TrustRIDR-Net framework.

TABLE III. DRL CONFIGURATION

DRL component	Configuration/Details
State space	Ti,Ei,d(i,BS),Hi
Action space	Selection of the next-hop node from the neighborhood
Reward function	$R_t = \alpha_1 \cdot \Delta T + \alpha_2 \cdot \Delta E - \alpha_3 \cdot D_{hop}$
Algorithm	Deep Q-Network (DQN)
Learning rate	0.001
Discount factor (γ)	0.95
Replay buffer size	10,000 transitions
Exploration strategy	Epsilon-Greedy (ε decays from 1.0 to 0.01)
Episodes	**1000**
Batch size	**64**

Table IV summarizes the parameters used in the energy-aware transmission strategy of the TrustRIDR-Net model. The base transmit power P_0 represents the minimum energy needed per bit. The path-loss exponent γ models how power increases

with distance, depending on the communication environment, with lower values for free-space conditions and higher values for harsh or obstructed scenarios.

TABLE IV. ENERGY-AWARE TRANSMISSION PARAMETERS

Parameter	Symbol	Value/Description
Base transmit power	P_0	50 nJ/bit
Path-loss exponent	Γ	2 (Free Space), up to 4 (Harsh)
Max distance to BS	d_{max}	200 m
Transmission power equation	–	$P_{tx}(i) = P_0 \cdot (d(i,BS)d_{max})\gamma$

Figure 5 shows how the transmit power varies with the distance to the BS under different path-loss conditions. As the distance increases, the required transmission power increases non-linearly based on the value of the path-loss exponent γ.

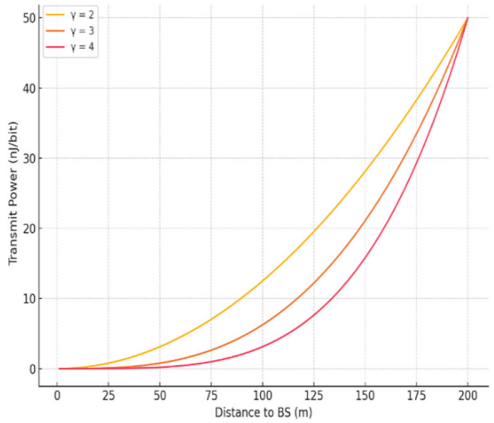

Fig. 5. Power scaling curve.

Table V displays node-level trust scores, their average neighborhood trust values (CT_i), and their computed relay selection probabilities $P_{relay}(i)$ based on (13). Nodes with higher individual trust and close alignment with neighborhood trust averages are more likely to be selected as relays. Figure 6 presents a multi-line chart that effectively compares the number of relay nodes and inactive nodes over five simulation snapshots. Table VI compares the TrustRIDR-Net model against several baseline protocols, including LSTM, GRU, PSO, GA, LEACH, and RF-based routing, demonstrating its superior performance in all key metrics. Figure 7 provides a comparative visualization of the network lifetime across various models, where TrustRIDR-Net distinctly outperforms all baseline protocols, sustaining the network for 1250 rounds, while the closest contenders, PSO and GA, plateau at 1015 rounds.

TABLE V. NODE STATUS AND RELAY PROBABILITY

Node ID	Trust score T_i	Neighborhood Avg CT_i	Relay probability $P_{relay}(i)$	Status
N1	0.85	0.79	0.21	Relay
N2	0.43	0.60	0.11	Inactive
N3	0.76	0.79	0.18	Relay
N4	0.33	0.55	0.09	Inactive
N5	0.88	0.79	0.22	Relay
N6	0.65	0.68	0.14	Conditional relay

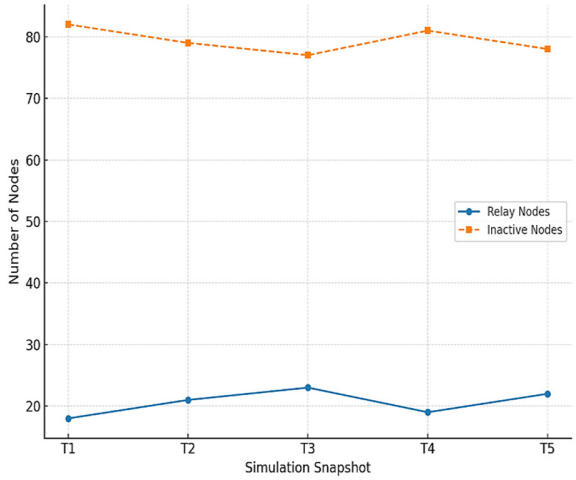

Fig. 6. Relay vs inactive nodes.

TABLE VI. COMPARATIVE PERFORMANCE METRICS

Model/Protocol	Network lifetime (Rounds)	Avg. trust score	Energy consumed (%)	Throughput (kbps)	PDR (%)
TrustRIDR-Net	1250	0.89	68%	17,560	98.9
LSTM	1010	0.73	76%	1586	94.2
GRU	940	0.69	80%	1467	91.5
PSO	1015	0.75	73%	1522	92.8
GA	1015	0.74	74%	1540	93.0
LEACH	940	0.66	82%	1394	89.6
RF-based routing	980	0.70	79%	1448	90.3

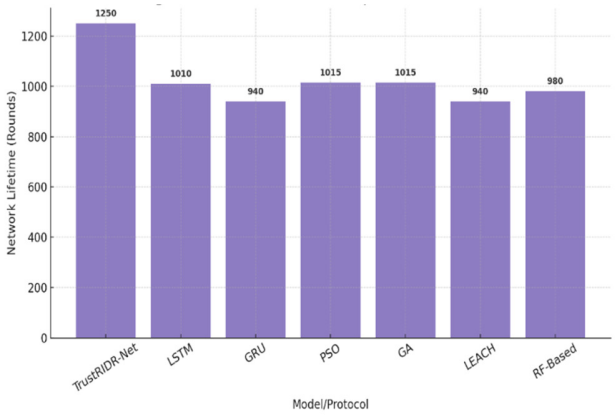

Fig. 7. Network lifetime comparison.

Figure 8 illustrates the throughput performance of various models in kbps. The TrustRIDR-Net model achieves a dramatic lead with a throughput of 17,560 kbps, clearly outperforming all other techniques. Figure 9 presents a comparison of the PDR across different models. TrustRIDR-Net achieves a PDR of 98.9%, significantly outperforming all other techniques.

Table VII compares energy consumption across TrustRIDR-Net, GRU, and LEACH at selected simulation rounds. TrustRIDR-Net consistently consumes less energy at every stage.

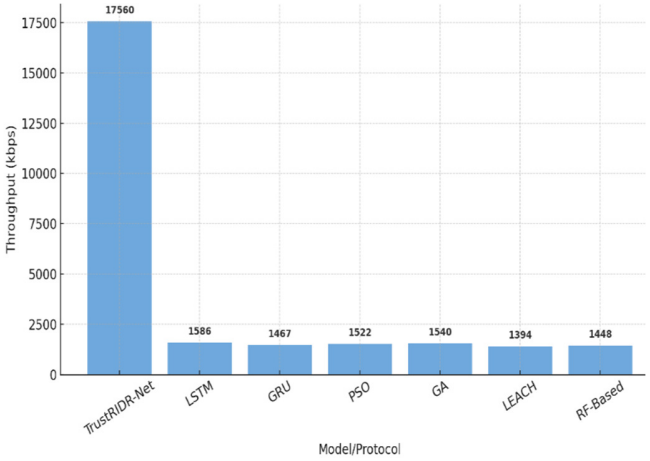

Fig. 8. Throughput comparison plot.

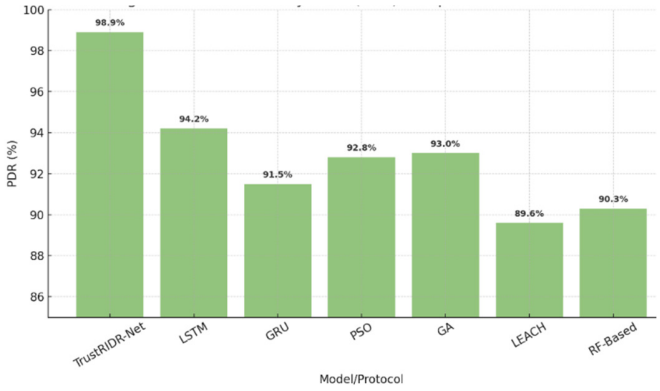

Fig. 9. PDR comparison.

TABLE VII. ENERGY CONSUMPTION OVER TIME

Round	TrustRIDR-Net	GRU (%)	LEACH (%)
250	12	18	22
500	27	38	44
750	46	60	68
1000	61	82	91
1250	68	100	100

As shown in Figure 10, the energy consumption trend of TrustRIDR-Net is slower compared to GRU and LEACH over increasing simulation rounds. Figure 11 shows the number of alive nodes over time during the simulation, where TrustRIDR-Net maintains a high node survival rate.

Figure 12 displays the evolution of the trust scores for three representative nodes (A, B, and C) over simulation rounds. Figure 13 illustrates a sample routing path selected by the TrustRIDR-Net model within a simulated IoT environment, where the estimations closely match the actual or expected values. Table VIII compares the PDR of the proposed TrustRIDR-Net model with existing techniques in the recent literature.

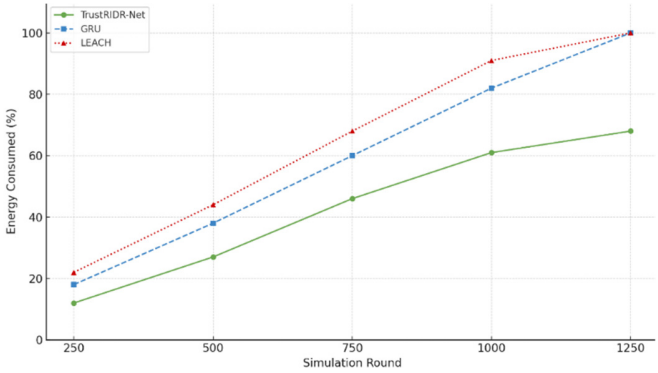

Fig. 10. Energy consumption trend over time.

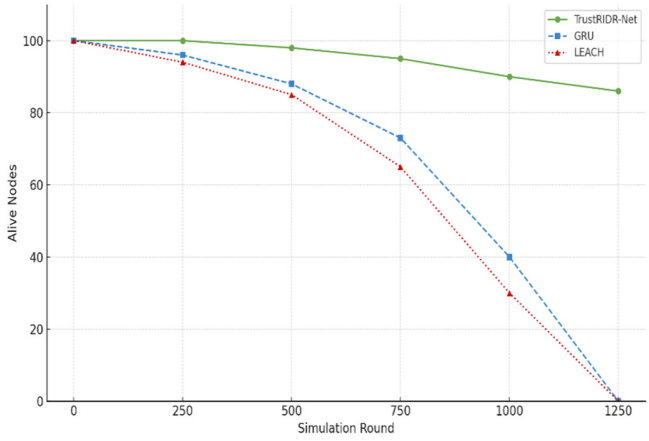

Fig. 11. Number of alive nodes.

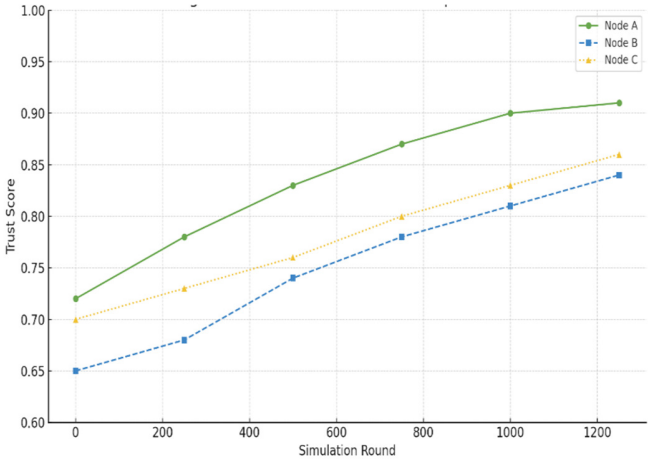

Fig. 12. Trust score trend.

TABLE VIII. PDR COMPARISON

Model	PDR
CORAC [21]	98%
BFA [22]	91%
SCSOA [24]	95%
LOA [26]	94.24%
Proposed TrustRIDR-Net	98.9%

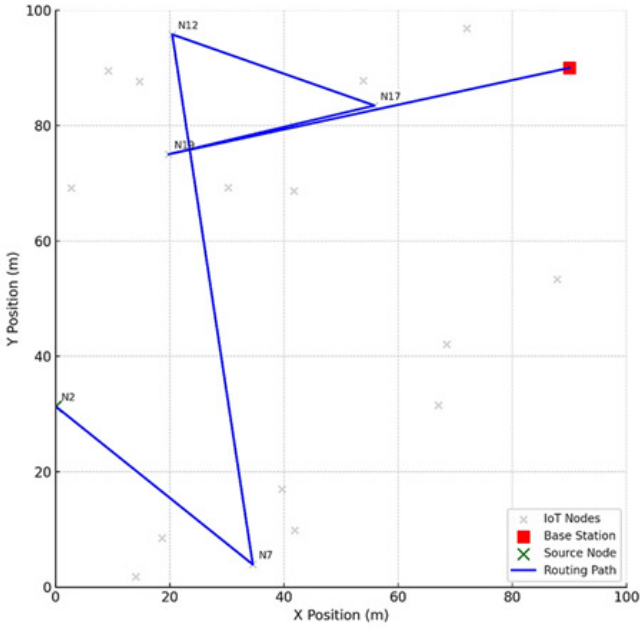

Fig. 13. Routing path visualization.

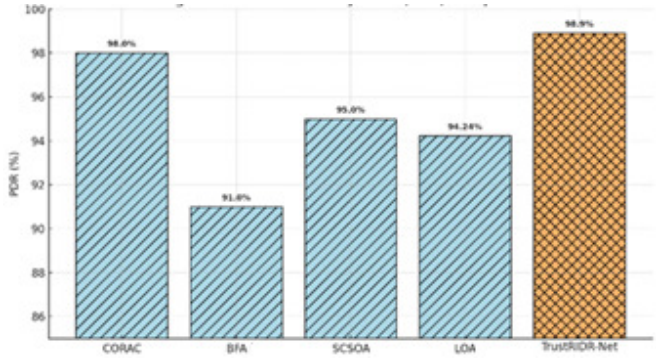

Fig. 14. PDR comparison with existing works.

Figure 14 compares the PDR of various models, including CORAC, BFA, SCSOA, LOA, and the proposed TrustRIDR-Net. Figure 15 presents a comprehensive comparison of throughput performance across a range of node counts for various routing techniques. The TrustRIDR-Net model consistently leads, achieving the highest throughput across all scenarios, reaching up to 17,560 kbps at 300 nodes. Table IX clearly demonstrates that TrustRIDR-Net outperforms all baseline models across key metrics, confirming its effectiveness in trust-aware and energy-efficient IoT routing.

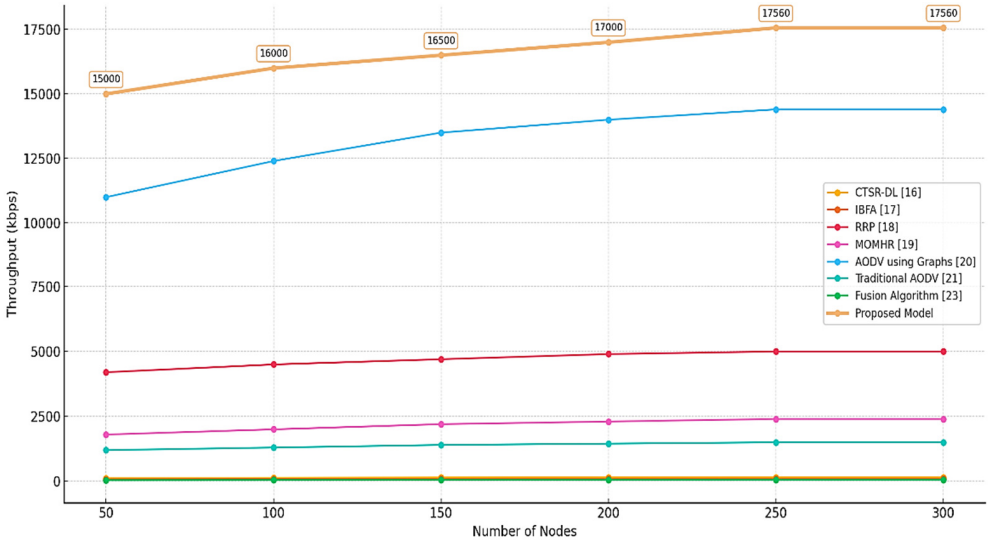

Fig. 15. Throughput comparison with existing methods

TABLE IX. PERFORMANCE COMPARISON BETWEEN TRUSTRIDR-NET AND BASELINE MODELS

Model	PDR (%)	Energy consumed (%)	Through-put (kbps)	Network lifetime (Rounds)	Avg. trust score
TrustRIDR-Net	98.9	68	17,560	1250	0.89
LEACH	89.6	82	1,394	940	0.66
AODV	91.0	79	1,452	960	0.70
GRU	91.5	80	1,467	940	0.69

All performance metrics are averaged over 10 independent simulation runs with random node placements to reduce bias and capture variability in trust dynamics. The standard deviation between runs was consistently below 2%, confirming the statistical significance of the reported results.

To evaluate the contribution of each module, an ablation study was conducted by selectively disabling components. Removing the RFO clustering reduced the PDR from 98.9% to 93.1%, while excluding DRL routing decreased throughput by nearly 74%. Similarly, omitting energy-aware control shortened network lifetime by 21%. These results confirm that each module significantly influences overall system performance, and their combined effect is essential for achieving the reported efficiency and scalability.

During experimentation, one challenge was maintaining the stability of the trust metric in fluctuating traffic, which was addressed by adaptive weight adjustments. Another difficulty was ensuring convergence of the DRL agent, requiring fine-tuning of the learning rate and the exploration decay. Additionally, parameter sensitivity emerged in heterogeneous networks, particularly in balancing clustering radius and trust threshold, which was mitigated through iterative optimization.

V. CONCLUSION

This study presented TrustRIDR-Net, a comprehensive routing framework for IoT networks that integrates trust evaluation, energy awareness, and intelligent route learning into a unified, adaptive system. The model innovatively combines RFO for trust-aware clustering and DRL for dynamic routing path refinement. A multi-factor trust computation mechanism enables accurate relay node selection based on behavioral patterns and energy metrics. The energy-aware transmission model further ensures efficient power utilization, improving overall network longevity. Through extensive simulation, TrustRIDR-Net demonstrated superior performance over state-of-the-art models, achieving 17,560 kbps throughput, 98.9% PDR, and a network lifetime of 1250 rounds. It maintained high node survival and accurate trust prediction, even under growing network loads. These results confirm the framework's ability to support secure, scalable, and energy-efficient communication in modern IoT scenarios.

Future work will explore the extension of TrustRIDR-Net to heterogeneous and mobile IoT environments, ensuring adaptability under dynamic topologies. In addition, blockchain-based trust verification will be investigated to provide decentralized immutability of trust data.

REFERENCES

[1] W. Wang, V. Srinivasan, and K. C. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking*, May 2005, pp. 270–283, https://doi.org/10.1145/1080829.1080858.

[2] X. Liu, "Atypical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5372–5383, Jul. 2015, https://doi.org/10.1109/JSEN.2015.2445796.

[3] A. Vijaya Krishna and A. Anny Leema, "ETM-IoT: Energy-Aware Threshold Model for Heterogeneous Communication in the Internet of Things," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1815–1827, 2022, https://doi.org/10.32604/cmc.2022.018455.

[4] P. M. Urs, A. T. N. Reddy, S. Mallikarjunaswamy, and U. M. Lakshminarayan, "An Innovative IoT Framework using Machine Learning for Predicting Information Loss at the Data Link Layer in Smart Networks," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 20904–20911, Apr. 2025, https://doi.org/10.48084/etasr.9597.

[5] S. S. S. Paulraj and T. Deepa, "Energy-efficient data routing using neuro-fuzzy based data routing mechanism for IoT-enabled WSNs," *Scientific Reports*, vol. 14, no. 1, Dec. 2024, Art. no. 30081, https://doi.org/10.1038/s41598-024-79590-x.

[6] J. Guo, A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, "ITCN: An Intelligent Trust Collaboration Network System in IoT," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 203–218, Jan. 2022, https://doi.org/10.1109/TNSE.2021.3057881.

[7] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, "Trust-aware and cooperative routing protocol for IoT security," *Journal of Information Security and Applications*, vol. 52, Jun. 2020, Art. no. 102467, https://doi.org/10.1016/j.jisa.2020.102467.

[8] Q. Jing, L. Y. Tang, and Z. Chen, "Trust Management in Wireless Sensor Networks," *Journal of Software*, vol. 19, no. 7, pp. 1716–1730, 2008.

[9] W. Jianping and L. Ming, "Study on Reputation and Trust Group-based Wireless Sensor Network Entity Authentication," *Chinese Journal of Sensors and Actuators*, 2008.

[10] K. Jaiswal and V. Anand, "An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks," in *2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, Jun. 2019, pp. 857–860, https://doi.org/10.1109/ICECA.2019.8822173.

[11] M. S. Abdalzaher and O. Muta, "A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness in IoT Applications," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11250–11261, Aug. 2020, https://doi.org/10.1109/JIOT.2020.2996671.

[12] D. Praveen Kumar, T. Amgoth, and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion*, vol. 49, pp. 1–25, Sep. 2019, https://doi.org/10.1016/j.inffus.2018.09.013.

[13] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia Computer Science*, vol. 131, pp. 1156–1163, Jan. 2018, https://doi.org/10.1016/j.procs.2018.04.289.

[14] S. Karimullah, D. Vishnuvardhan, V. K. Gunjan, and F. Shaik, "Improved Spectral Efficiency Using Vehicular Visible Light Communication with 16-Bit DCO in OFDM," in *Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough: Volume 4*, V. K. Gunjan, J. M. Zurada, and N. Singh, Eds. Springer International Publishing, 2024, pp. 159–168.

[15] A. Srivastava and R. Paulus, "CTSR-DL: Cluster based trusted secure aware routing for WSN Assisted IoT using deep learning technique," *African Journal of Biological Sciences*, vol. 6, no. 5, pp. 9549–9597, 2024.

[16] D. Siddy and M. S. Islam, "Energy and Trust-Aware Routing in Wireless Networks for Multimedia Applications," *Advances in Image and Video Processing*, vol. 12, no. 3, pp. 127–150, Mar. 2024, https://doi.org/10.14738/aivp.123.16994.

[17] A. H. Wheeb *et al.*, "Improvised Spectral Efficiency and Channel Estimation Parameters in Visible Light Vehicular Communication by Integrating Simulation of Urban Mobility Data," *IEEE Access*, vol. 13, pp. 70828–70848, 2025, https://doi.org/10.1109/ACCESS.2025.3558697.

[18] R. Vinodhini and C. Gomathy, "MOMHR: A Dynamic Multi-hop Routing Protocol for WSN Using Heuristic Based Multi-objective Function," *Wireless Personal Communications*, vol. 111, no. 2, pp. 883–907, Mar. 2020, https://doi.org/10.1007/s11277-019-06891-0.

[19] L. A. Maglaras and D. Katsaros, "Distributed clustering in vehicular networks," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Barcelona, Spain, Oct. 2012, pp. 593–599, https://doi.org/10.1109/WiMOB.2012.6379136.

[20] M. R. Ghori, A. S. Sadiq, and A. Ghani, "VANET Routing Protocols: Review, Implementation and Analysis," *Journal of Physics: Conference Series*, vol. 1049, no. 1, Apr. 2018, Art. no. 012064, https://doi.org/10.1088/1742-6596/1049/1/012064.

[21] D. Annalakshmi and C. Jayanthi, "A secured routing algorithm for cluster-based networks, integrating trust-aware authentication mechanisms for energy-efficient and efficient data delivery," *The Scientific Temper*, vol. 15, no. 03, pp. 2672–2682, Aug. 2024, https://doi.org/10.58414/SCIENTIFICTEMPER.2024.15.3.35.

[22] C. E. Singh, S. S. Priya, B. M. Kumar, K. Saravanan, A. Neelima, and B. Gireesha, "Trust aware fuzzy clustering based reliable routing in Manet," *Measurement: Sensors*, vol. 33, Jun. 2024, Art. no. 101142, https://doi.org/10.1016/j.measen.2024.101142.

[23] M. Chen, A. Liu, N. N. Xiong, H. Song, and V. C. M. Leung, "SGPL: An Intelligent Game-Based Secure Collaborative Communication

Scheme for Metaverse Over 5G and Beyond Networks," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 3, pp. 767–782, Mar. 2024, https://doi.org/10.1109/JSAC.2023.3345403.

[24] G. Muneeswari, A. Ahilan, R. Rajeshwari, K. Kannan, and C. John Clement Singh, "Trust And Energy-Aware Routing Protocol for Wireless Sensor Networks Based on Secure Routing," *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 9, pp. 1015–1022, Nov. 2023, https://doi.org/10.32985/ijeces.14.9.6.

[25] G. Sudha and C. Tharini, "Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks," *Automatika*, vol. 64, no. 3, pp. 634–641, Jul. 2023, https://doi.org/10.1080/00051144.2023.2208462.

[26] W. Jiang, "Graph-based deep learning for communication networks: A survey," *Computer Communications*, vol. 185, pp. 40–54, Mar. 2022, https://doi.org/10.1016/j.comcom.2021.12.015.

[27] S. Baskar, R. Selvaraj, V. M. Kuthadi, and P. M. Shakeel, "Attribute-based data fusion for designing a rational trust model for improving the service reliability of internet of things assisted applications in smart cities," *Soft Computing*, vol. 25, no. 18, pp. 12275–12289, Sep. 2021, https://doi.org/10.1007/s00500-021-05910-2.

[28] B. Su, C. Du, and J. Huan, "Trusted Opportunistic Routing Based on Node Trust Model," *IEEE Access*, vol. 8, pp. 163077–163090, 2020, https://doi.org/10.1109/ACCESS.2020.3020129.