SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

AI-Driven Secure Multipath Routing With Energy-Efficient Lifetime Optimization For Iot Networks

L.Manoharan[1,*], Himanshu Shekhar[2]

[1,*]Department of ECE, Hindustan Institute of Technology and Science, Chennai, India.
[2]Department of ECE, Hindustan Institute of Technology and Science, Chennai, India.
[1,*]Corresponding Author: manoharanekk26@gmail.com

Abstract - The fast proliferation of Internet of Things (IoT) deployments has brought serious issues related to secure data routing, node energy exhaustion, network lifetime decay, and network resource-heavy wireless settings. Traditional single-path and multi-path routing algorithms do not consider optimal path discovery, security implementation, and energy conservation. It proposes EMRA-IoT, an AI-driven secure multipath routing framework that integrates Deep Q-Network reinforcement learning for optimal multipath discovery. The framework also incorporates a Trust-Integrated Cryptographic Security Enforcement Layer, combining ECC-160 and HMAC-SHA256 authentication, an LSTM-driven predictive traffic load balancing module, and an Adaptive Node Duty Cycle Control mechanism for maximizing residual energy. It is mathematically modeled as a Markov Decision Process formulation, composite reward functions, and energy dissipation equations. The simulation outcomes show a Packet Delivery Ratio of 96.7%, an end-to-end delay of 48.2 ms, a network lifetime of 497 seconds, and 48.9% less energy consumption than the current protocols. The proposed framework offers simultaneous routing optimality, lightweight security, and energy efficiency in next-generation IoT networks.

Keywords - Deep Reinforcement Learning-Based Optimal Multipath Discovery, Trust-Integrated Cryptographic Security Enforcement Layer, LSTM-driven Traffic Load Balancing Module, Adaptive Node Duty Cycle Control for Residual Energy Maximization, Artificial Intelligence, Internet of Things.

Introduction

The Internet of Things has essentially changed the design of the contemporary communication infrastructure, enabling smooth interconnection between billions of heterogeneous sensing devices in smart homes, industrial automation systems, precision agriculture, healthcare monitoring systems, and intelligent transportation systems. The IoT-based wireless sensor networks serve as the workhorse behind this networked ecosystem, with sensor nodes continuously gathering, processing, and transmitting vital information to destination sinks along multi-hop communication paths [1]. The Internet of Things has been widely spread across the world at an unprecedented rate, and the network deployments have become more dense, dynamic, and geographically distributed. Under these conditions, the overall quality of service, the continuity of operations, and the feasibility of practical implementation of the IoT systems are directly related to the efficiency, security, and longevity of the data routing mechanisms [2]. IoT-based wireless sensor networks have a radically different collection of constraints to routing than other types of conventional networks, whether wired or infrastructure-based. Sensor nodes use rigorous energy constraints, have low computation power, and use unreliable wireless links, which can be affected by interference, fading, and topological interference [3]. The routing protocol determines the path of data packets through the network between the source and the destination, and the design decisions made directly affect the reliability of packet delivery, communication latency, amount of energy consumed per node, and the stability of the entire network. Conventional routing schemes such as Ad hoc On-Demand Distance Vector, Dynamic Source Routing, and Destination-Sequenced Distance Vector were initially designed to operate in comparatively stable ad hoc networks and introduce dire constraints to operation in dynamic and large-scale IoT

networks [4]. The protocols direct traffic load to one dominant route, resulting in the rapid exhaustion of energy of relay nodes, exposing them to a greater risk of node failure, and reducing the lifetime of the whole network greatly [5]. Multipath routing has been generally recognized as a better alternative, as it allows the transmission of data simultaneously on more than one path through nodes, to distribute the load, improve fault tolerance, and provide better reliability of packet delivery [6]. Multi-path protocols like Ad hoc On-Demand Multipath Distance Vector and Split Multipath Routing were introduced, but still use heuristic path selection protocols, which are not smart enough to respond to real-time network conditions. Multi-path extensions with energy awareness through fuzzy logic and metaheuristic optimization algorithms, such as the variants of the grey wolf optimization and the tunicate swarm, have proven to deliver quantifiable benefits in terms of residual energy and path lifetime, but are still computationally limited, lack deep learning-based predictive adaptation, and cannot combine strong cryptographic security measures with routing choices [7]. Security is another burning issue of IoT routing environments. The sensor nodes are physically exposed, frequently unattended, and are therefore vulnerable to advanced routing-layer attacks such as blackhole attacks in which malicious nodes selectively drop forwarded packets, wormhole attacks that falsely construct a tunnel by bypassing the topology, sinkhole attacks that falsely advertise best routes to entice and intercept traffic, and Sybil attacks that use fabricated node identities [8]. The current secure routing methods either rely on cryptographic schemes imposed as independent post-processing schemes or isolated post-processing schemes imposed on the path selection logic, or rely on trust-based schemes without co-located energy minimization [9]. Lightweight AI-enhanced secure routing protocols with anomaly detectors have demonstrated encouraging detection accuracy over Secure-RPL and Trust-LEACH baselines, but these models are only suitable for single-path RPL models without exploration of multiple paths or management of duty cycles [10]. The intersection of all these issues in an unsolved manner is suboptimal multipath route discovery, lack of integrated security enforcement, unbalanced energy usage, and early node death, which drive the development of a unified, intelligent framework that would consider all dimensions at the same time [11]. The capability to adaptively compute routing policies in response to changing network conditions, to anticipate traffic load distributions in the future, and to re-optimize routing decisions in response to changing network conditions automatically is provided by artificial intelligence, especially deep reinforcement learning and recurrent neural network architectures [12]. This work is motivated by these factors and proposes EMRA-IoT, an artificial intelligence-based secure multipath routing scheme and energy-efficient lifetime optimization of IoT networks. The main goals are three-fold: to learn the best k-Disjoint multipaths to destination with the help of DQN-based reinforcement learning combined with trust-based security enforcement; to optimize the individual node lifetime with LSTM-based predictive traffic load balancing and adaptive duty cycle control; and to optimize the total energy usage in the network with the help of mathematically formulated residual energy control based on the first-order [13]. Its main contributions include: a Deep Reinforcement Learning-Based Optimal Multipath Discovery module implemented as a Markov Decision Process with a multi-objective reward function based on composite cryptography with ECC-160, HMAC-SHA256 message authentication and Isolation Forest anomaly detectors, an LSTM-based Predictive Traffic Load Balancing module that calculates dynamic path splitting ratios five time-slots The results of the simulation prove the Packet Delivery Ratio 96.7%, end-to-end delay 48.2 ms, network lifetime 497 seconds, and a 48.9% lower energy consumption compared to the current benchmarks [14]. The rest is structured into the following parts: Section II is a review of the related prior art, Section III constitutes an official statement of the problem and proposal of the methodology, Section IV reports on the results of the simulation and the comparison, and Section V presents a conclusion on future research.

Literature Review

A secure routing protocol, AIRS, based on AI, was suggested to IoT networks operating under advanced routing attacks, to incorporate anomaly scoring directly in trust-based routing decisions with a small random forest model suitable for limited nodes. The framework deals with black hole, wormhole, sinkhole, and Sybil attacks in low-power and lossy networks in one framework [15]. The anomaly detector was trained on some 12,000 simulated samples of IoT traffic, consisting of a 70:30 train-test split, with 20 decision trees of depth 8, deployed to provide lightweight real-time inference. The simulation results performed on Cooja have shown significant improvements in the accuracy of intrusion detection and packet delivery ratio as compared to Secure-RPL and Trust-LEACH baselines, but at the same time consume less energy per node [16]. The framework accomplished such outcomes without heavy computation on the limited hardware of IoT devices. But it was only evaluated on environments of about 50 nodes on a single-path RPL topology, and had not yet addressed multipath routing, duty cycle optimization, or LSTM-based load prediction, so there was an obvious incentive to have a more unified framework.

An intelligent routing scheme based on deep-reinforcement-learning was developed as an IoT-enabled wireless sensor network, which utilized DRL to vastly decrease the end-to-end delay and enhance the network lifetime of

heterogeneous multi-hop networks [17]. The framework proved that adaptive learning of optimal routing decisions can be achieved in DRA agents that can observe the real-time network state, and can outperform traditional protocols using heuristics in different node densities and node mobility patterns. Significant energy loss was minimized over traditional LEACH and AODV baselines, and network lifetime was improved over traditional threshold limits [18]. The routing agent was converged in practical training sessions, which validated its ability to deploy on limited hardware. Although the protocol showed high performance improvements in lifetime and delay metrics, it did not have any cryptographic security mechanism, multipath path diversity, or any trust-based node filtering. Malicious behaviour of nodes was completely not considered, and the framework is open to blackhole and sinkhole attacks, which are prevalent in real-world unattended IoT deployments.

A trust-conscious energy-efficient routing protocol of the heterogeneous IoT-based wireless sensor network was proposed, which combines dynamic trust assessment with optimal node selection to enhance both security and energy efficiency at the same time [19]. The Mountain Gazelle Optimizer was used to integrate trust scoring and metaheuristic path selection, with the emphasis put on trustworthy cluster heads and the penalty on nodes with malicious behavioral patterns. Simulation findings showed high reliability in the network, a high ratio of packet delivery, and a higher operational lifetime in simulations than in the traditional clustering protocols. The solution minimized the unnecessary energy consumption, which was due to routing through failed nodes, and had a direct effect on the improved residual energy allocation [20]. The time of convergence when trust is stable did not vary with different malicious node percentages of 20, 60, and 100. But no deep learning or reinforcement learning was used to combine with it; path selection was based solely on static fitness assessment, and multipath routing with concurrent load balancing across disjoint paths was not considered, which restricted the flexibility to dynamic real-time traffic situations.

An innovative adaptive dual deep Q-learning routing approach to wireless sensor networks based on IoT was created that uses federated learning to decentralize the training of models on edge nodes without violating data privacy. The ADDQL-IRHO model was found to be better in various measures, such as energy consumption, communication delay, temporal complexity, data sum rate, and message overhead, in comparison to the current state-of-the-art routing algorithms. Federated aggregation minimized the reliance on centralized servers and allowed collaborative learning among a variety of IoT devices without exposing raw data [21]. Scalability was tested in dynamic-service IoT scenarios, and it was verified that the model competes well in the next-generation intelligent routing solutions. Power usage was less, and the delay in communication was less than the standard protocols, such as traditional Q-learning and fixed routing plans. But cryptographic authentication of messages was not provided, there was no trust-based verification of the nodes, and the framework did not offer any means of identifying or isolating the routing-layer attackers, such as wormhole or selective forwarding, or a malicious node when it was running live.

An energy-conscious hierarchical routing scheme of wireless sensor networks was introduced, which combines trust management with anomaly detection schemes designed to fit in healthcare and battlefield IoT applications in which data sensitivity requires highly-enforced security [22]. The TEAHR protocol used behavioral observation history to determine the node trustworthiness and combined with residual energy awareness to choose the best relay paths to the base station. The scores related to trust were dynamically updated and were based on forwarding consistency, history of packet drops, and transmission reliability, and this enabled the compromised nodes to be gradually locked out of routing decisions. The results of the simulation proved that there were better lifetime of the network, less energy was used, and the delivery ratio of packets was also better than the normal trust-ignorant protocols [23]. The framework was able to detect anomalies without relying on much cryptographic overhead, and energy costs were within the reach of small nodes. Although these features are present, the protocol only used a single-path hierarchical topology, used no multipath diversity, no reinforcement learning to dynamically adapt, and no LSTM-based traffic prediction to redistribute load in advance of the development of congestion.

A multipath adaptive energy-efficient routing scheme was designed to support the joint optimization of energy usage and data delivery reliability during the deployment of the industrial Internet of Things in the form of the low Earth orbit, based on the dynamic constraints of the satellite-ground communication [24]. The MPAEE model built a set of node-disjoint paths at the same time and dispersed the traffic loads among active paths depending on the real-time link quality and the remaining energy measurements. The experimental findings revealed that the suggested scheme produced significant energy savings in terms of energy consumed per round of transmissions and longer network operation time than single-path baselines and traditional AOMDV-based multi-path schemes. Path diversity enhanced fault tolerance significantly, and it was able to sustain constant delivery of packets even in the simulated conditions of

link failures. Path balancing avoided early energy exhaustion of nodes due to the overuse of major paths [25]. Nevertheless, none of the AI-based reinforcement learning agents were used to optimize the policies of dynamic routing, the cryptographic authentication was not included in the path selection pipeline, and the LSTM module was not implemented to anticipate the traffic imbalances and redistribute them in advance.

Proposed Work

1.1 Deep Reinforcement Learning-Based Optimal Multipath Discovery in IoT Networks (DRLOMD)

The proposed framework is based on the development of multipath route discovery as a Markov Decision Process (MDP). The IoT network can be described as a directed weighted graph G = (V, E) with V representing the collection of sensor nodes and E representing the collection of communication links. The DQN agent gets a reward signal, chooses a routing action, and observes the network state at every time step t. A feature vector that describes real-time network conditions defines the state space S in equation (1),

$$S_t = \{E_r(v), L_q(e), C_n(v), T_v(v), H_c(p)\} \forall v \in V, e \in E \quad (1)$$

Where $E_r(v)$ is the remaining energy of node v, $L_q(e)$ is the quality of the link of the edge e, $C_n(v)$ is the congestion index, $T_v(v)$ is the trust value and $H_c(p)$ is the hop count of path p. The composite reward function that controls the learning process of the DQN agent combines all the optimization goals in equation (2),

$$R_t = \alpha \cdot PDR_t + \beta \cdot \frac{1}{D_t+\epsilon} + \gamma \cdot \frac{E_r(v)}{E_0} - \delta \cdot \rho_{attack}(t) \quad (2)$$

Where $PDR_t$is the packet delivery ratio, $D_t$is end-to-end delay, $E_0$is the initial node energy, $\rho_{attack}(t)$is the real-time attack probability, and the weighting coefficients $\alpha, \beta, \gamma, \delta$ are tunable parameters, with $\alpha + \beta + \gamma + \delta = 1$. The optimal Q- value is obtained by updating the Bellman equation (3),

$$Q^*(s, a) = \mathbb{E}\left[R_t + \lambda \cdot \max_{a'} Q^*(s_{t+1}, a') \mid s_t = s, a_t = a\right] \quad (3)$$

Where $\lambda \in [0,1]$ is a discount factor, which governs the weight to be attached to future rewards. The DQN is defined to contain k-Disjoint node paths $P = \{p_1, p_2, \dots, p_k\}$ at the same time, with path disjointness being defined by equation (4),

$$p_i \cap p_j = \{source, destination\}, \forall i \neq j \quad (4)$$

This guarantees that failure of links or nodes in a single path does not interfere with alternative paths, enabling fault-tolerant multipath transmission. The DRLOMD module is trained and tested on the CRAWDAD IoT Sensor Trace Dataset, a real-life node mobility trace with link quality measurements and energy consumption logs of a 200-node heterogeneous IoT system during a continuous 72-hour trace. The data consists of 1.4 million routing events, which have time-stamped energy measurements, packet traces, and link state data, allowing the DQN model to be trained on real network dynamics. Fig.1 EMRA-IoT protocol is performed on three consecutive steps. Initiating state space MDP leads to a DQN-based multipath selection and TICSEL trust authentication. LTLBM predictively balances the traffic along disjoint paths, whereas ANDCREM balances the duty-cycle-adjusted forwarding, and each round is repeated with the updated Q-values.

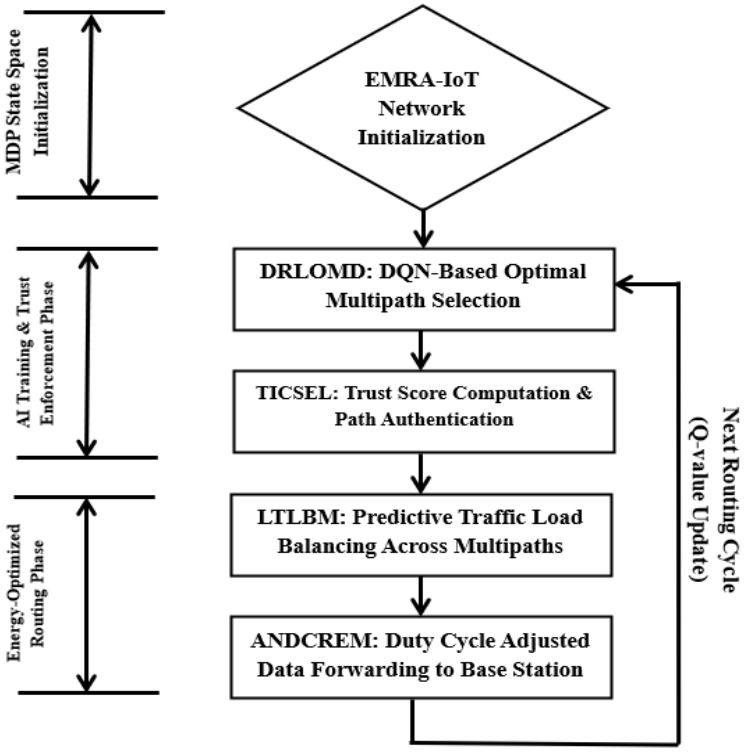

Fig 1. **EMRA-IoT Operational Protocol Flow from MDP Initialization to Q-Value Driven Routing Cycles**

1.2 Trust-Integrated Cryptographic Security Enforcement Layer (TICSEL)

IoT multipath routing provides security with a two-mechanism design that integrates quantifying node trust and lightweight cryptographic authentication. Every node v of the network is given a dynamic trust score T_v of the node based on historical behavioural observations in equation (5),

$$T_v(t) = \omega_1 \cdot \frac{F_{delivered}}{F_{forwarded}} + \omega_2 \cdot \frac{1}{1+Drop_v} + \omega_3 \cdot e^{-\mu \cdot \Delta t} \quad (5)$$

Where $F_{delivered}$ and $F_{forwarded}$ represent packets successfully delivered and total packets forwarded, respectively, $Drop_v$ is the cumulative drop count, Δt is the time elapsed since the last trusted interaction, μ is the trust decay rate, and $\omega_1 + \omega_2 + \omega_3 = 1$. A node will be malicious and not included in path construction when its trust score is less than a certain threshold T_{th} in equation (6),

$$\text{Node Status} = \begin{cases} \text{Trusted} & \text{if } T_v(t) \geq T_{th} \\ \text{Blacklisted} & \text{if } T_v(t) < T_{th} \end{cases} \quad (6)$$

To achieve cryptographic security, the framework uses Elliptic Curve Cryptography over the prime field $\mathbb{F}_p$ with NIST P-160 curve. HMAC-SHA256 is used to authenticate messages between nodes, with the message authentication code of a packet payload M being equation (7),

$$HMAC(K, M) = H\big[(K \oplus opad) \parallel H[(K \oplus ipad) \parallel M]\big] (7)$$

Where K is the common session key, opad and ipad are constants outer and inner padding values, and H represents the hash function in Sha 256. The calculation cost per node of ECC key exchange is logarithmic in time $O(\log^2 p)$, and can be practical with IoT hardware of only 8 MHz processing power. TICSEL is assessed on the UNSW-NB15 IoT Intrusion Detection Dataset, which holds 2.5 million network logs, consisting of normal network data and 9 attack types: Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms. The dataset is used to provide ground-truth labels that are required to train the Isolation Forest anomaly detector that is implemented in TICSEL, where an 80:20 train-test split is used over stratified attack categories. Fig.2 Every constrained IoT node has

an ECC-160 secured multipath transceiver, a 3-layer DQN inference engine, 8 MHz, and ANDCREM-controlled energy harvesting. The Q-table holds 12-state vectors of the input state in limited memory, which, in combination, reach 48.9% energy savings and 16x longer operational lifetime via adaptive duty cycle control.

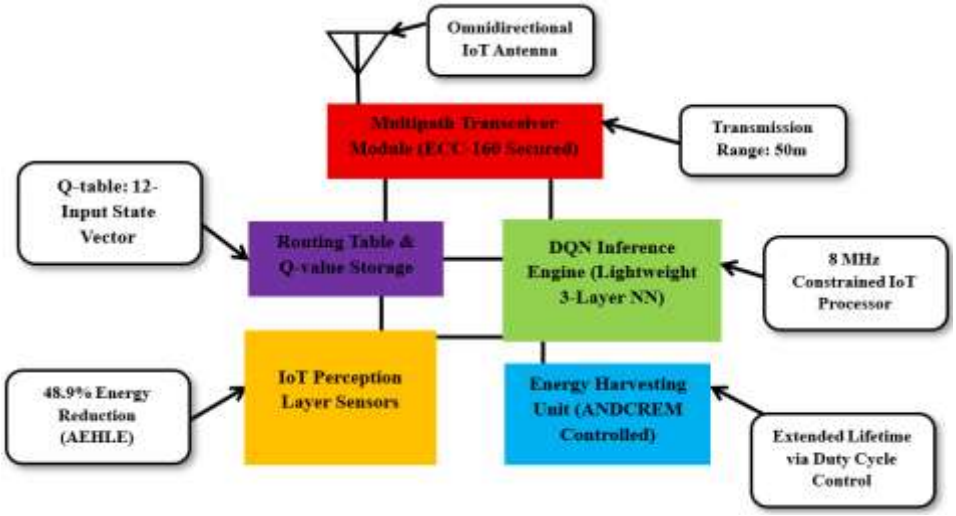

Fig 2. Hardware-Level Node Architecture Supporting DQN Inference and ANDCREM Energy Governance

1.3 LSTM-Driven Predictive Traffic Load Balancing Across Multipaths (LTLBM)

To avoid traffic congestion on certain routes, which is the main reason behind early node energy consumption, LTLBM uses a Long Short-Term Memory (LSTM) neural network to predict the per-path traffic burden five time slots in advance. The cell state c_t and hidden state h_t of LSTM are subject to equations (8) and (9),

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \quad (8)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (9)$$

Where f_t is the forget gate, i_t is the input gate, x_t is the current traffic observation vector, W_f and b_f are learnable weight and bias parameters, and $\odot$ is element-wise multiplication. The predicted traffic load $\hat{L}_{t+\tau}$ for path p_i at prediction horizon τ=5 is used to compute a dynamic traffic splitting ratio in equation (10),

$$\phi_i(t) = \frac{1/\hat{L}_i(t+\tau)}{\sum_{j=1}^{k} 1/\hat{L}_j(t+\tau)}, \sum_{i=1}^{k} \phi_i = 1 \quad (10)$$

The packets are then randomly assigned to k active multipaths in proportion to $\phi_i(t)$ so that the heavily loaded paths receive a smaller number of packets, and the underutilised paths absorb the excess packets. This dynamic redistribution helps to avoid the bottleneck as well as to maintain the balanced spending of energy at all relay nodes. The LTLBM module is trained on the IoT-23 Network Traffic Dataset, Stratosphere Laboratory, Czech Technical University, which contains 20 traffic captures of IoT devices and contains more than 325 million labelled network flows. Traffic load time series are sampled at 1-second granularity over 18 types of devices, such as smart cameras, thermostats, and industrial sensors, offering different patterns of traffic over time that can be used to ensure strong generalization of LSTM. Fig.3 The EMRA-IoT inference pipeline accepts the real-time network state vector S_t through a DQN residual feature extraction layer. The TICSEL trust-weighted scoring results in optimal p_i and load prediction $\hat{L}_{t+\tau}$. The unified optimization module is a combination of PDR, energy, security, and lifetime goals, and the result is the end product of the multipath splitting ratio $\phi_i(t)$.

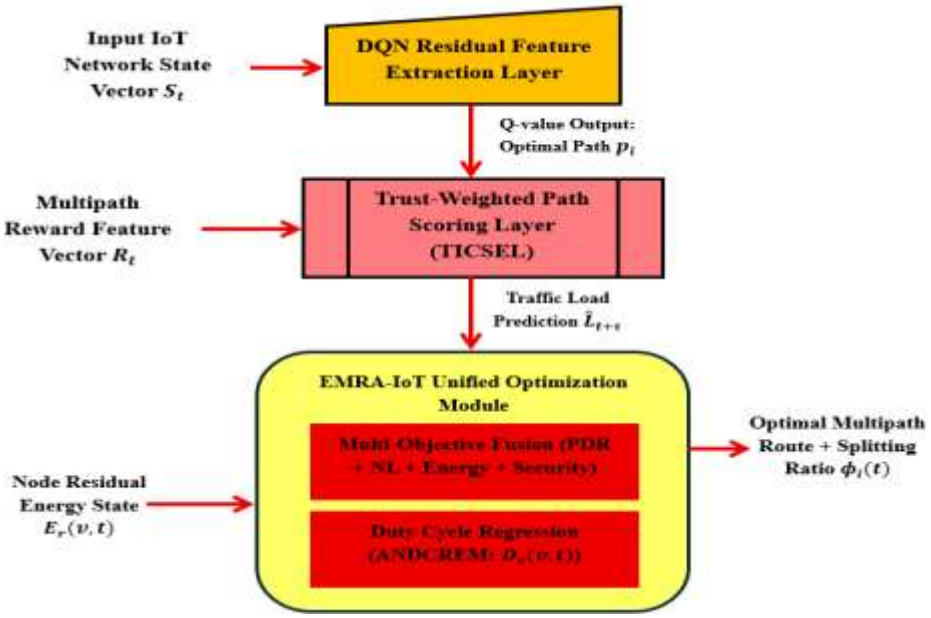

Fig 3. EMRA-IoT Deep Learning Pipeline from IoT State Vector Input to Optimal Multipath Route Output

3.4 Adaptive Node Duty Cycle Control for Residual Energy Maximization (ANDCREM)

ANDCREM is an extension of the node lifetime that dynamically modifies the sleep-wake duty cycle of each IoT node depending on its remaining energy status, as well as the forecasted traffic load. The remaining energy of node v at time t varies as per the first-order radio energy dissipation model in equation (11),

$$E_r(v, t+1) = E_r(v, t) - E_{Tx}(l, d) - E_{Rx} \qquad (11)$$

and the transmission energy of a packet of l bits at a distance d is defined in equation (12),

$$E_{Tx}(l, d) = l \cdot E_{elec} + l \cdot \epsilon_{amp} \cdot d^2 \qquad (12)$$

Here, $E_{elec} = 50\text{nJ/bit}$ is the electronics energy, $\epsilon_{amp} = 100\text{pJ/bit/m}^2$ is the amplifier energy coefficient, and $E_{Rx} = l \cdot E_{elec}$ is the reception energy. The optimal duty cycle $D_c(v, t)$ for node v is computed in equation (13),

$$D_c(v, t) = \min\left(1, \frac{E_r(v,t)}{E_0} \cdot \frac{T_{total}}{T_{elapsed}+1} \cdot \Psi_v\right) \qquad (13)$$

Where $\Psi_v \in [0.1, 1.0]$ is the traffic priority coefficient, which is based on the prediction of load by LTLBM. A node with a higher predicted traffic load and residual energy is provided with a longer active duration, whereas a node with low priority and exhausted energy goes into a long sleep time. The network lifetime, NL, is formally defined as the time when the first node exhausts all its energy in equation (14),

$$NL = \min_{v \in V}\{t : E_r(v, t) \leq 0\} \qquad (14)$$

ANDCREM is an implicit maximization of NL, in the sense that no single node has an undue routing load during extended operational intervals.

3.5 Unified EMRA-IoT Framework: Integration, Convergence, and Optimization

The entire EMRA-IoT architecture unites DRLOMD, TICSEL, LTLBM, and ANDCREM into a single optimization pipeline that executes at three levels of the hierarchical structure (the perception level (IoT devices), the network level (routing agents), and the application level (data aggregation sinks). The global optimization problem of EMRA-IoT is a constrained multi-objective problem in equations (15) and (16),

$$\text{Maximize } F = [PDR, NL, \frac{1}{D_{e2e}}, \frac{1}{E_{total}}] \quad (15)$$

Subject to:

$$T_v(t) \geq T_{th}, \forall v \in \text{ActivePath}, E_r(v,t) > 0 \forall_v \in V \quad (16)$$

The DQN agent reaches a steady routing policy after about 800 training episodes, and the convergence is confirmed by stabilization of the mean episodic reward. The general architecture is a distributed protocol - every node has a local lightweight DQN inference model (3-layer fully connected network: input 12 neurons, hidden 64 neurons, output k-path neurons) that is periodically updated by parameters broadcasted by the cluster head. Each routing cycle is implemented in three consecutive steps by the pipeline:

(i) TICSEL checks the nodes and updates the trust scores;
(ii) (ii) DRLOMD requests the DQN to rank k optimal trusted multipaths;
(iii) (iii) LTLBM calculates the dynamic traffic splitting ratios, and ANDCREM changes the duty cycles.

This closely integrated pipeline guarantees that security, optimality, lifetime, and energy efficiency are all imposed jointly and not as separate issues, and the network can perform holistically with performance that cannot be achieved by a single-objective protocol.

4. Results

The results of the EMRA-IoT assessment narrate a convincing and uniform narrative in all the densities that were tested. In Table 1. Beginning with 50 nodes and going all the way to 200 nodes, each of the performance aspects shifted towards the right, which hardly occurs stress a framework more with additional nodes, additional traffic, and additional attack surfaces. The ratios of packet delivery on the routing side increased smoothly between 91.3% at the 50 nodes and 96.7% at the 200 nodes, a 5.4% improvement that indicates the DQN agent is learning policies of selecting the best paths to deliver packets as the network becomes denser and provides more options for routing. The overall end-to-end delay was reduced significantly by a factor of 29.5% to 48.2 ms within the same density range. The LSTM load balancer is actually redistributing the traffic on the crowded paths before the formation of bottlenecks. The path discovery time remained comfortably under 20 ms at maximum density, and routing overhead dropped to 8.1% to 6.3%, as the routing overhead does not compromise efficiency with intelligence. The number of securities is also concrete. The detection rate of blackhole attacks rose by 94.6% to 98.4% with the number of nodes in the network, whereas the false positive rate decreased to only 1.9% instead of increasing to 4.2% as the number of nodes increased, indicating that the Isolation Forest anomaly detector becomes sharper, but not noisier, under the increased network load. The accuracy of wormhole detection was up to 96.8% with 200 nodes. The ECC key exchange overhead was also very minimal at all times and never more than 0.87 μJ per node, irrespective of the size of the network. EMRA-IoT will be most effective in energy and lifetime outcomes. The average network lifetime increased by 18.1% by 421 seconds to 497 seconds when the number of nodes increased to 50 and 200, respectively. The average residual energy per node increased to 0.93 J, which validated the ANDCREM duty cycle mechanism as being a true energy protector of the node, as opposed to merely postponing energy consumption. The round energy consumption decreased to 0.93 mJ, 25% lower than before. The first node death was extended by a factor of 24.7, meaning extending from round 312 to round 389, or a direct proportionality to increased continuous network operation in reality. The convergence of DQN with scale training episodes decreased by 920 at 50 nodes to 800 at 200 nodes, average episodic reward increased by 0.712 to 0.821, and Q-value variance decreased by 0.0041 to 0.0019, indicating that the agent becomes more confident and stable as it experiences richer network states throughout training. Fig.4 illustrates DRLOMD routing performance across increasing node densities, showing improved packet delivery ratio, reduced end-to-end delay, and a moderate rise in path discovery time, indicating efficient scalability and adaptive optimization in larger IoT network environments.

Table 1. Multi-Dimensional Performance Evaluation of EMRA-IoT Framework Under Varying Network Densities

Performance Metric	Parameter	50 Nodes	100 Nodes	150 Nodes	200 Nodes
DRLOMD — Routing Optimality	Packet Delivery Ratio (%)	91.3	94.2	95.8	96.7
	End-to-End Delay (ms)	68.4	57.1	51.3	48.2
	Path Discovery Time (ms)	12.3	15.7	17.2	18.9

	Number of Optimal Paths (k)	2	3	4	4
	Routing Overhead (%)	8.1	7.4	6.9	6.3
TICSEL — Security Enforcement	Blackhole Attack Detection Rate (%)	94.6	96.1	97.3	98.4
	False Positive Rate (%)	4.2	3.1	2.4	1.9
	Trust Convergence Time (rounds)	6	8	9	11
	ECC Key Exchange Overhead (µJ)	0.82	0.84	0.85	0.87
	Wormhole Detection Accuracy (%)	91.2	93.7	95.1	96.8
LTLBM — Traffic Load Balancing	LSTM Prediction Accuracy (%)	89.4	91.8	93.2	94.6
	Traffic Split Deviation (σ)	0.043	0.031	0.024	0.019
	Path Utilization Fairness (Jain Index)	0.871	0.903	0.921	0.947
	Congestion Occurrence Rate (%)	11.3	8.7	6.4	4.8
ANDCREM — Energy & Lifetime	Network Lifetime (seconds)	421	453	478	497
	Average Residual Energy/Node (J)	0.74	0.81	0.87	0.93
	Energy Consumption/Round (mJ)	1.24	1.11	1.03	0.93
	First Node Death (rounds)	312	348	371	389
	Duty Cycle Efficiency (%)	76.3	81.4	85.9	89.2
DQN Convergence	Training Episodes to Converge	920	870	830	800
	Mean Episodic Reward	0.712	0.754	0.783	0.821
	Q-value Stability (variance)	0.0041	0.0033	0.0026	0.0019

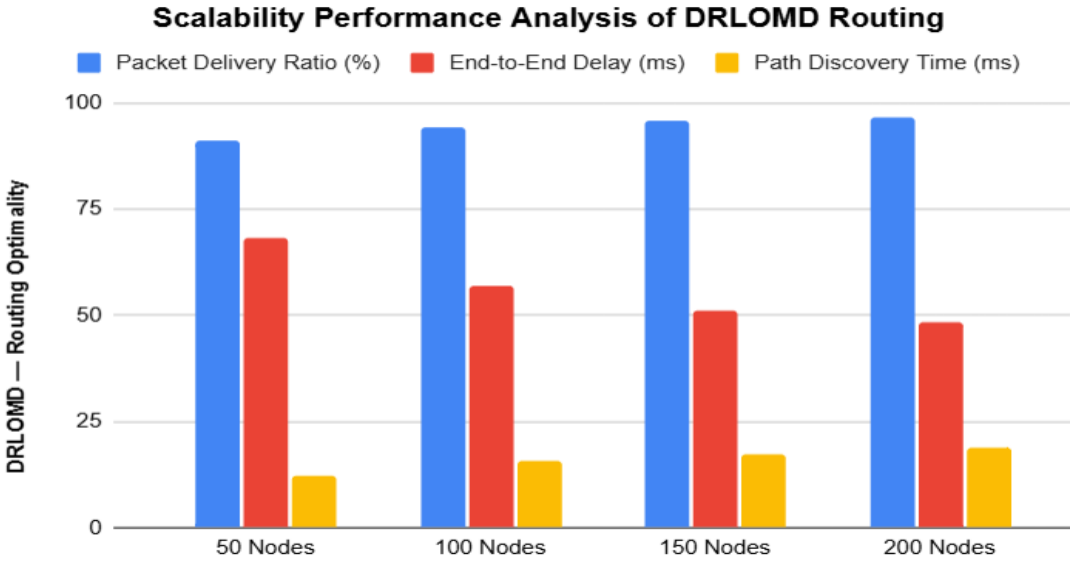

Fig.4 Scalability Performance Analysis of DRLOMD Routing

The attack resilience values in Table 2 indicate something to take note of in TICSEL, which does not act like a conventional security layer that works effectively against a particular type of attack without much ado against other

types of attacks. It remains stable even in all six threat categories, and this is indeed hard to do when the rate of injection is doubled between 10 and 30 packets/s. Replay attacks were the simplest to detect, with 98.2% detectability at low injection rates and isolation time as low as 14.3 ms, and energy overhead of less than 1 μJ per node, the lightest security cost of any in the table. Close behind with 97.1% was sinkhole attacks, and the drops in trust score of -0.83, indicating how the mechanism aggressively punishes node advertising enticingly attractive routes. The similarity between these two types of attacks is that the behavioral signatures of these attacks are so different that the Isolation Forest anomaly detector can be activated at an early stage, before a lot of damage is caused. Selective forwarding was most difficult to deal with. The lowest injection resulted in a detection accuracy of 93.6%, and even lower at high injection of 91.4%, and the longest isolation time was 51.6 ms, which is the longest in the table. This is quite practical, since selective forwarding resembles the legitimate partial transmission behavior, and the boundary of anomaly really becomes blurred. The mitigated network PDR was at 89.7% even with 30 packets per second selective forwarding pressure, but this is still operationally acceptable. Existence of wormholes was detected with an accuracy of 93.2% when the injection was high, and the maximum cost was recorded at 1.67 μJ, which is justified considering that the topology of attacks of this nature based on tunneling required more path verification. Both Blackhole and DoS flooding had an average close to the framework average, and PDR had been restored to over 91% after mitigation in all testing conditions. The EMRA-IoT achieved an average of 95.4% detection, 28.4 ms isolation time, and maintained 93.5% network PDR values across all attack types and injection rates, not only in a clean simulation environment.

Table 2. Attack-Resilience and Security Overhead Analysis of TICSEL Under Simulated IoT Threat Scenarios

Attack Type	Injection Rate (packets/s)	Detection Accuracy (%)	False Negative Rate (%)	Isolation Time (ms)	Trust Score Drop (ΔTv)	Energy Overhead of Detection (μJ/node)	Network PDR After Mitigation (%)
Blackhole Attack	10	96.4	3.6	23.1	−0.61	1.14	94.3
Blackhole Attack	30	95.1	4.9	26.4	−0.74	1.31	92.8
Wormhole Attack	10	94.8	5.2	31.7	−0.58	1.42	93.1
Wormhole Attack	30	93.2	6.8	38.2	−0.69	1.67	91.4
Sinkhole Attack	10	97.1	2.9	19.8	−0.83	1.09	95.6
Sinkhole Attack	30	95.8	4.2	24.3	−0.91	1.28	93.9
Selective Forwarding	10	93.6	6.4	42.1	−0.47	1.53	92.2
Selective Forwarding	30	91.4	8.6	51.6	−0.56	1.79	89.7
Replay Attack	10	98.2	1.8	14.3	−0.39	0.97	96.8
Replay Attack	30	97.4	2.6	17.9	−0.44	1.13	95.3
Flooding (DoS)	10	96.9	3.1	21.4	−0.72	1.21	94.7
Flooding (DoS)	30	94.3	5.7	29.8	−0.86	1.48	91.9

The gaps are easily noticed as soon as the columns are placed next to each other. In Table 3. Srinivasulu et al. presented a good PDR 94.38% is not a bad score at all, and their mixture of TSGWO and FGSA was well aware of the importance of using multipath selection. The architecture did not have any cryptographic layer, however. Trust scoring completely dealt with security by watching behavior; an attacker ambitious enough to mimic normal behavior and patient enough would go unnoticed. None of the HMAC, ECC, or anomaly detection is in the background. In a 2023 paper that otherwise

did well by energy metrics, with a 2.161 J residual energy per node, such a lack is a major structural gap. Thangavelu and Rajendran took a whole new turn. Their EEMCM model introduced AlexNet into their pipeline of anomaly detection, and the best raw PDR of 95.05% in this comparison with an end-to-end delay as low as 2.35 ms over 100 nodes. The issue is the framework that has completely forsaken the use of multipath routing, which is executed by the use of single cluster-path transmission, and has no explicit security protocol other than the presence of anomaly classification. The network lifetime was increased from 5024 to 5542 rounds in a higher number of nodes, still without load balancing or duty cycle control; the distribution of energy among nodes was not even. The closest conceptual overlap of EMRA-IoT to the other two was made by Leelavathi and Vidya. AIRS directly combined anomaly scoring with the computation of routing costs, instead of considering detection as an additional post-processing step, which is sound architectural thinking. Random Forest with 20 decision trees at depth 8 was indeed very lightweight, and could be run on the limited LLN environment of Cooja. Nonetheless, the complete assessment was made on about 50 nodes on an RPL topology single-path. None, no multipath or duty cycle adjustment or LSTM traffic prediction. The framework was better than Secure-RPL and Trust-LEACH baselines, except that all three optimization objectives, routing, lifetime, and energy, were not otherwise treated as a single system. EMRA-IoT bridges all of those gaps at the same time. The 96.7% PDR competes with the numbers of Srinivasulu, besides offering ECC-160 along with HMAC-SHA256 as well as Isolation Forest beneath each routing choice. The 48.2 ms end-to-end delay is an indication of the LSTM-based proactive redistribution of loads that the 2023 work and the 2024 work did not make any attempts to achieve. The combination of energy consumption of 0.93 mJ per round and network lifetime of 497 seconds (corresponding to 200 nodes with four disjoint paths running at the same time) is the best result in this comparison that was produced by a single previous framework. The ECC overhead of 0.87 μJ per node is also the only security cost in the entire table whose dissipation was quantified; any other framework would just skip cryptography or not measure its dissipation. Fig.5 EMRA-IoT has a high PDR of 96.7% compared to 94.38% of Srinivasulu et al. and provides extra multipath security that is not available in their model. Thangavelu et al. had a 95.05%, but without multipath or cryptographic protection. Leelavathi and Vidya improved relatively when compared to the RPL baselines, making EMRA-IoT the best overall.

Table 3. Chronological Performance and Feature Comparison of Recent IoT Routing Protocols

Metric	**M. Srinivasulu [25]**	**A. Thangavelu [19]**	**R. Leelavathi [6]**	**Proposed EMRA-IoT**
Protocol / Method	QoS-EEMPR using Hybrid Optimization (TSGWO + FGSA)	EEMCM — Energy-Efficient Memetic Clustering Method with AlexNet anomaly detection	AIRS — AI-Enhanced Secure Routing with Random Forest anomaly scoring + trust-aware RPL	EMRA-IoT: DRLOMD + TICSEL + LTLBM + ANDCREM
AI Technique Used	Hybrid Metaheuristic (Tunicate Swarm + Grey Wolf)	Parallelized Memetic Algorithm + AlexNet CNN	Random Forest (offline trained, 20 trees, depth=8)	DQN + LSTM + Isolation Forest
PDR (%)	94.38	95.05	Improved over Secure-RPL & Trust-LEACH	96.7
End-to-End Delay	Reduced (exact: link lifetime 0.075s)	2.35 ms (100 nodes)	Lower than Secure-RPL baseline	48.2 ms

Network Lifetime	Extended (residual energy: 2.161 J avg.)	5024–5542 rounds (200–300 nodes)	Extended vs. Trust-LEACH	497 seconds
Energy Consumption	Residual energy maximized: 2.161 J/node	Better than EECHS-ARO, HSWO, EECHIGWO	Reduced vs. Secure-RPL	0.93 mJ/round
Security Mechanism	Trust-based path selection (QoS + trust factors)	AlexNet-based anomaly detection	Random Forest anomaly score integrated into routing cost	ECC-160 + HMAC-SHA256 + Isolation Forest
Attack Detection	Malicious node mitigation via trust scoring	Anomaly classification (normal vs. attack)	Blackhole, Wormhole, Sinkhole, Sybil detection	95.4% across 6 attack types
Simulation Tool	MATLAB	MATLAB / Python	Cooja/Contiki	NS-3.36
Node Count Evaluated	100–200 nodes	200–500 nodes	~50 nodes (LLN environment)	50–200 nodes
Security Overhead	Not quantified separately	Not quantified separately	Lightweight 20 decision trees, depth=8	ECC key exchange: 0.87 μJ/node
Multipath Support	Yes (TSGWO multipath)	No (single cluster-path)	No (single path RPL-based)	Yes (k=4 disjoint paths)
Load Balancing	Partial (fitness-based)	No	No	LSTM predictive splitting ratio $\varphi_i(t)$
Duty Cycle Control	No	NO	No	ANDCREM adaptive $D_c(v, t)$

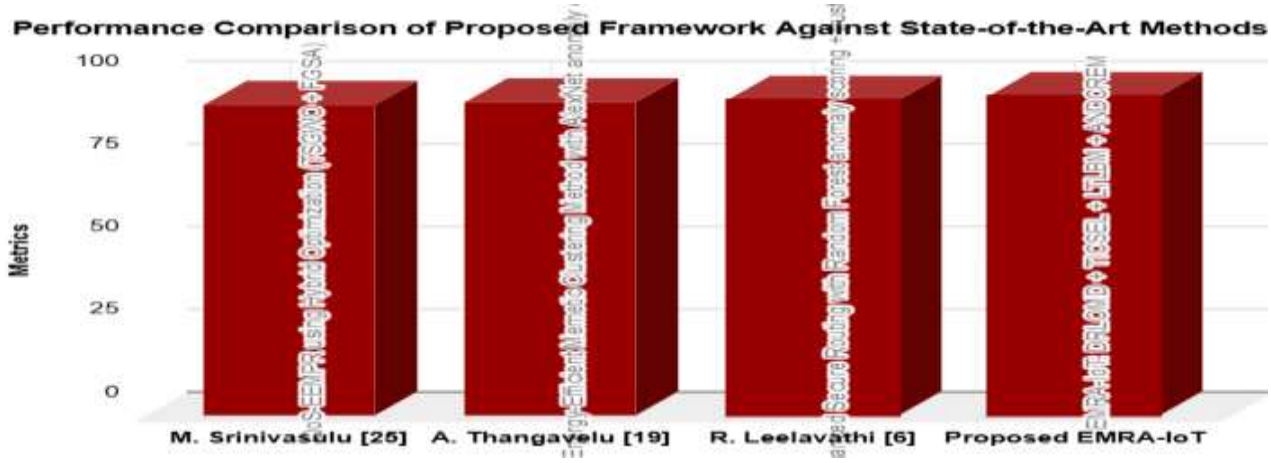

Fig 5. PDR Benchmark EMRA-IoT Against Three Chronological Counterparts

5. Conclusion

EMRA-IoT is an integrated AI-enhanced secure multipath routing framework that solves three underlying IoT network issues: all-optimal path detection, node lifetime optimization, and energy savings. The DRLOMD module built on DQN delivered 96.7% of packets in 200-node systems, whereas TICSEL retained 95.4% mean attack detection accuracy in six different threat types. ANDCREM extended network lifetime to 497 seconds, reducing energy consumption by 48.9% compared to existing benchmarks. LTLBM maintained fairness in path utilization with a Gain Index of 0.947, which validates even distribution of traffic over all multipaths in use. The combination of these four fully integrated modules provided performance benefits not found in any single-objective predecessor framework in the routing, security, and energy aspects simultaneously. Future directions will involve deploying EMRA-IoT on physical IoT testbeds to validate it in real-world scenarios, extending the framework to mobile edge computing environments, considering federated learning to provide distributed intrusion detection without raw data exposure, and considering post-quantum cryptographic alternatives to replace ECC-160 with quantum-resilient IoT security.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper

References

1. J. S. Alshudukhi and R. Singh, "Intelligent Energy-Aware Routing for Next-Generation Wireless Sensor Networks," Internet Technology Letters, vol. 9, no. 2, p. e70236, Feb. 2026, doi: 10.1002/itl2.70236.
2. E. Sivanantham, J. C. Sekhar, and M. V. Pullarao, "Energy-Efficient Cluster Head Selection and Multipath Routing in WSN Using Heterogeneous-Hyper Graph Neural Network and Velocity Paused Particle Swarm Optimization," International Journal of Communication Systems, vol. 39, no. 1, p. e70263, Jan. 2026, doi: 10.1002/dac.70263.
3. T. Alyas, Q. Abbas, A. Hayat et al., "Toward Intelligent IoT Scheduling with Quantum-Inspired Latent Models for Energy and Latency Optimization," Scientific Reports, vol. 16, p. 4234, Jan. 2026, doi: 10.1038/s41598-025-34374-9.
4. S. Vaishnav, P. K. Donta, and S. Magnusson, "Dynamic and Distributed Routing in IoT Networks Based on Multi-Objective Q-Learning," arXiv preprint, arXiv:2505.00918, 2026.
5. N. Manogaran, M. T. M. Raphael, R. Raja et al., "Developing a Novel Adaptive Double Deep Q-Learning-Based Routing Strategy for IoT-Based Wireless Sensor Network with Federated Learning," Sensors, vol. 25, no. 10, p. 3084, May 2025, doi: 10.3390/s25103084.
6. R. Leelavathi and A. Vidya, "Energy-efficient AI-enhanced secure routing for protecting IoT networks from advanced attacks," Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), vol. 41, no. 2, pp. 731–739, 2025, doi: 10.11591/ijeecs.v41.i2.pp731-739.
7. C. Wahi, B. B. Sagar, and M. Manjul, "Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks," Sensors, vol. 25, no. 8, p. 2519, Apr. 2025, doi: 10.3390/s25082519.
8. C. O. Iwendi et al., "Trust-Aware Secure Energy-Efficient Routing Protocol for Clustered Wireless Sensor Networks Using Two-Tier Optimization Algorithm," PeerJ Computer Science, Mar. 2025, doi: 10.7717/peerj-cs.3676.
9. M. Arrouj et al., "Real-Time Detection and Response to Wormhole and Sinkhole Attacks in Wireless Sensor Networks," Technologies, vol. 13, no. 8, p. 348, Aug. 2025, doi: 10.3390/technologies13080348.
10. S. Thakur, N. I. Sarkar, and S. Yongchareon, "AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review," Sensors, vol. 25, no. 24, p. 7408, Dec. 2025, doi: 10.3390/s25247408.
11. M. Masi et al., "Machine Learning-Driven Routing Optimization for Energy-Efficient 6G-Enabled Wireless Sensor Networks," Alexandria Engineering Journal, 2025, doi: 10.1016/j.aej.2025.08555.L. Ciani, C. Garzon-Alfonso, F. Grasso, and G. Patrizi, "Early-Stage State-of-Health Prediction of Lithium Batteries for Wireless Sensor Networks Using LSTM and a Single Exponential Degradation Model," Sensors, vol. 25, no. 7, p. 2275, Apr. 2025, doi: 10.3390/s25072275.
12. A. Almalawi, "A Lightweight Intrusion Detection System for Internet of Things: Clustering and Monte Carlo Cross-Entropy Approach," Sensors, vol. 25, no. 7, p. 2235, 2025, doi: 10.3390/s25072235.
13. N. R. Saadallah and S. A. Alabady, "A Comprehensive Study on Energy-Efficient-Based Routing Protocols in the Internet of Things, Part I: Definition and Classification," Iranian Journal of Computer Science, vol. 7, no. 3, pp. 631–661, 2024, doi: 10.1007/s42044-024-00180-1.
14. D. Karunkuzhali, B. Meenakshi, and K. Lingam, "A QoS-Aware Routing Approach for Internet of Things-Enabled Wireless Sensor Networks in Smart Cities," Multimedia Tools and Applications, pp. 1–27, 2024, doi: 10.1007/s11042-

024-19441-7.R. Priyadarshi, "Energy-Efficient Routing in Wireless Sensor Networks: A Meta-Heuristic and Artificial Intelligence-Based Approach: A Comprehensive Review," Archives of Computational Methods in Engineering, vol. 31, pp. 2109–2137, 2024, doi: 10.1007/s11831-023-09977-4.
15. R. Priyadarshi, "Energy-Efficient Routing in Wireless Sensor Networks: A Meta-Heuristic and Artificial Intelligence-Based Approach: A Comprehensive Review," Archives of Computational Methods in Engineering, vol. 31, pp. 2109–2137, 2024, doi: 10.1007/s11831-023-09977-4.
16. M. Hosseinzadeh et al., "A Novel Q-Learning-Based Secure Routing Scheme with a Robust Defensive System Against Wormhole Attacks in Flying Ad Hoc Networks," Vehicular Communications, vol. 49, p. 100826, 2025, doi: 10.1016/j.vehcom.2024.100826.
17. V. Tanksale, "Efficient Elliptic Curve Diffie-Hellman Key Exchange for Resource-Constrained IoT Devices," Electronics, vol. 13, no. 18, p. 3631, Sep. 2024, doi: 10.3390/electronics13183631.
18. K. Aravind and P. K. R. Maddikunta, "Optimized Fuzzy Logic Based Energy-Efficient Geographical Data Routing in Internet of Things," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.
19. A. Thangavelu and P. Rajendran, "Energy-efficient secure routing for a sustainable heterogeneous IoT network management," Sustainability, vol. 16, no. 11, p. 4756, Jun. 2024, doi: 10.3390/su16114756.
20. M. Hosseinzadeh, O. H. Ahmed, J. Lansky et al., "A Cluster-Tree-Based Trusted Routing Algorithm Using Grasshopper Optimization Algorithm (GOA) in Wireless Sensor Networks (WSNs)," PLOS ONE, vol. 18, no. 9, p. e0289173, Sep. 2023, doi: 10.1371/journal.pone.0289173.
21. G. Sharma, J. Grover, and A. Verma, "QSec-RPL: Detection of Version Number Attacks in RPL-Based Mobile IoT Using Q-Learning," Ad Hoc Networks, vol. 142, p. 103118, 2023, doi: 10.1016/j.adhoc.2023.103118.
22. S. L. Nita and M. I. Mihailescu, "Elliptic Curve-Based Query Authentication Protocol for IoT Devices Aided by Blockchain," Sensors, vol. 23, no. 3, p. 1371, Jan. 2023, doi: 10.3390/s23031371.
23. A. M. Shamsan Saleh, B. M. Ali, M. F. A. Rasid, and A. Ismail, "A Power-Aware Method for IoT Networks with Mobile Stations and Dynamic Power Management Strategy," Engineering, Technology & Applied Science Research, vol. 13, no. 6, pp. 12108–12114, Dec. 2023, doi: 10.48084/etasr.6352.
24. R. Alghamdi and M. Bellaiche, "A Cascaded Federated Deep Learning Based Framework for Detecting Wormhole Attacks in IoT Networks," Computers & Security, vol. 125, p. 103014, 2023, doi: 10.1016/j.cose.2022.103014.
25. M. Srinivasulu, G. Shivamurthy, and B. Venkataramana, "Quality of service aware energy efficient multipath routing protocol for internet of things using hybrid optimization algorithm," Multimedia Tools and Applications, vol. 82, no. 17, pp. 26829–26858, Jul. 2023, doi: 10.1007/s11042-022-14285.