SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I11P120

Volume 12 Issue 11, 240-251, November 2025

Original Article

Energy-Efficient Routing and Security Enhancements in Internet of Things Integrated Wireless Sensor Networks Using Reinforcement Learning

M. Rajasekar[1], S. P. Sasirekha[2]

[1,2]*Department of CSE, Karpagam Academy of Higher Education, Coimbatore, India.*

[1]*Corresponding Author: drrajasekarm@outlook.com*

Received: 18 September 2025 Revised: 19 October 2025 Accepted: 18 November 2025 Published: 29 November 2025

Abstract *- The rapid advancement of Information and Communication Technology (ICT) has revolutionized daily life through the emergence of smart, connected systems across homes, healthcare, transportation, and urban environments. Wireless Sensor Networks (WSNs) form the foundation of Internet of Things (IoT) deployments, enabling real-time data exchange and intelligent automation. However, WSNs face significant challenges, including limited battery life, low processing power, and heightened vulnerability to security threats. These limitations reduce the operational lifespan of the network and compromise the reliability and safety of data transmission. Addressing these issues requires energy-efficient and secure routing protocols to maintain high performance under resource-constrained and threat-prone conditions. This study introduces Energy-Secure Reinforcement Learning for WSNs(ESRL-WSNs), an intelligent routing protocol that applies Reinforcement Learning (RL) to optimize path selection based on energy status, network dynamics, and security conditions. ESRL-WSNs employs a reward-driven approach to enable sensor nodes to learn optimal routes autonomously, adapting to changes in topology and resource availability. Traditional routing strategies-flat-based, hierarchical, and location-based—are evaluated and benchmarked against the ESRL-WSNs framework through comprehensive simulations across diverse network configurations and traffic loads. Experimental results indicate that ESRL-WSNs reduce energy consumption by 32% and improve data delivery rates by 27% compared to standard protocols. Additionally, the model exhibits robust adaptability and resilience in node failures and security threats. Integrating Reinforcement Learning into WSN routing offers a forward-looking solution for achieving sustainable, secure, and efficient communication in IoT-integrated systems.*

Keywords *- Wireless Sensor Networks, Information and Communication Technology, Internet of Things, Energy-Efficient Routing, Reinforcement Learning, Smart Routing Protocols, Network Resilience, IoT Security.*

1. Introduction

Since intelligent systems are now integrated into homes, healthcare, transportation, and urban infrastructure, the quick development of artificial technologies has altered how people interact with their environment [1]. The Internet of Things (IoT) is a vast network of connected devices that continuously monitors, analyzes, and shares data. This is driving the revolution [2]. IoT-enabled continuous data analysis enhances system automation, productivity, and decision-making [3]. We need communication networks that are scalable, reliable, and energy-efficient because of the vast amount of data produced by these systems, which can vary in complexity from sensors to industrial machinery [4]. As IoT use grows in vital industries like smart grids and healthcare, where system performance and dependability are inadequate, strong security controls are needed [5]. If IoT environments are not sufficiently secured, they are susceptible to attacks that compromise the availability, privacy, and integrity of information. This illustrates how important it is to balance efficiency and security in today's networked environments [6]. Because WSNs use multi-hop communication to gather and transmit data in real time from dispersed sensor nodes, they are a crucial component of IoT systems [7]. Numerous applications, such as industrial automation, smart cities, healthcare, and agriculture, are made possible by WSNs [8]. Insufficient resources lead to problems in WSNs.

Due to the low energy and processing power of sensor nodes, energy-aware routing is essential for long-term network sustainability [9]. WSNs are particularly vulnerable to security risks in addition to energy-related issues. Nodes are susceptible to physical attacks, node capture, and data manipulation because they frequently function in unsecure environments [10]. Routing attacks, such as sinkhole, Sybil, and blackhole, can decrease a network's dependability by altering the paths that data takes [11].

The majority of conventional architectures lack effective methods for identity verification or preventing tampering. Changing radio signal strength is necessary for localization, a crucial routing function. Because of this, hackers can easily take advantage of positioning errors [12]. Important IoT apps' data integrity and trust are jeopardized by these defects. To defend against such threats, smart routing systems that are safer and consume less energy are required [13]. Reinforcement Learning (RL) is a dynamic, adaptable technique that assists WSNs in identifying the best routes and identifying and eliminating potential threats[14].

1.1. Problem Statement

Among the numerous disadvantages of WSN-based IoT devices are energy constraints and security vulnerabilities. Most sensor nodes are powered by non-rechargeable batteries, and when energy consumption varies, standard routing protocols do not work, leading to early node failures. Additionally, the protocols cannot be modified to accommodate changing network conditions. Nodes that are deployed insecurely are vulnerable to data manipulation and physical attacks. Ineffective localization methods based on signal intensity also make networks susceptible to routing assaults. In dynamic IoT contexts, an energy-efficient routing solution is required to maximize physical and cyber-attack resilience while optimizing power usage.

There is still a lack of study on the optimal routing protocols for IoT-powered WSNs that can manage their resource-constrained, dynamic, and heterogeneous properties while integrating real-time, adaptive security and energy-efficiency measures. Network lifetime, packet loss, and attack risk are frequently decreased by traditional routing systems' incapacity to adjust to changing network conditions, node mobility, energy availability, and security threats. Protocols that integrate energy efficiency, security, learning-based optimization, and dynamic context awareness are necessary for dependable IoT networks.

Thus, the main issue is developing an intelligent routing framework that autonomously selects the best data forwarding paths based on real-time contextual information, such as threat levels, node trustworthiness, link quality, and residual energy. This framework must withstand blackhole, Sybil, and sinkhole routing attacks, as well as network topology changes. Maintaining high packet delivery rates and network resiliency requires this. Additionally, it must work well on resource-constrained sensor nodes.

1.2. Research Methodology

This paper presents ESRL-WSNs, a new routing architecture dedicated to intelligent control of energy efficiency and security in WSN-IoT networks. ESRL-WSNs employs an RL method, i.e., Q-learning, which enables single sensor nodes to learn optimal routing paths through repeated interactions with the world. A reward mechanism for many parameters, such as residual energy, communication success rate, node trust values, and threat-detection controls, affects routing. This method supports adaptive routing based on network state, resulting in higher resilience and efficiency. Minimum tamper-resistance and anomaly-detection capabilities for protection against physical attacks and routing tampering are also integrated into ESRL-WSNs to further enhance the system's reliability.

1.3. Contributions of the Paper

- To optimize energy consumption through intelligent route selection based on real-time node status and network conditions.
- To improve data delivery reliability by dynamically adjusting paths in response to network changes and communication failures.
- To strengthen resilience against physical and routing attacks through tamper resistance and node behavior analysis.
- To reduce localization inaccuracies by minimizing dependence on unreliable radio-based distance measurements.
- To enable scalability and sustainability in large-scale IoT deployments with minimal additional computational or communication overhead.

1.4. Outline Structure of the Paper

The remaining sections of the document are structured as follows: Section 2 showcases pertinent research on routing applications in RL and WSN. Section 3 goes into detail about how the proposed ESRL-WSNs model learns and how its system is set up. Section 4 goes into detail about the experimental results, performance measures, and simulation environment. Section 5 finishes the work and gives ideas for further research.

2. Related Works

This section discusses current routing techniques for WSNs in IoT environments that are both secure and energy-efficient. It considers the merits and demerits of conventional and machine-learning-based methods for adaptive, intelligent solutions that balance energy efficiency and security threats in dynamic, resource-scarce network environments. The related works are compiled in Table 1.

The use of WSNs in IoT applications is on the rise, particularly in healthcare, smart cities, environmental monitoring, and industrial automation. Numerous studies have modeled the use of WSNs in low-energy contexts, with sensor nodes that typically have inherent constraints on processing and battery life. The most common WSN routing protocols-flat-based, hierarchical, and location-based-reduce power consumption, increase network lifetime, and improve data delivery probability.

Table 1. Literature survey

Authors	Proposed Technology	Method Used	Result	Limitations and Research Gaps
Al Razib et al. [15]	SDN-enabled DNN-LSTM framework	Deep learning for cyber threat detection	Cyber threat detection in bright surroundings that works	Focus on threat detection, not energy-efficient routing
Pedditi & Debasis [16]	IoT-based WSN routing for forest fire detection	Energy-efficient routing algorithm	Enhanced energy efficiency for fire detection scenarios	Application-specific, lacks general applicability
Tumula et al. [17]	Dynamic clustering algorithm	Self-configuration for energy efficiency	Improved energy utilization and network lifetime	Security was not considered in the design
Ali [18]	Enhanced WSN energy model	Optimization of WSN for IoT	Improved energy efficiency in IoT-based WSNs	Lacks integrated security measures
Aldawsari [19]	Blockchain-based secure routing	Blockchain for energy-efficient, secure routing	Secure and energy-efficient communication	High computational overhead of blockchain
Dogra et al. [20]	ESEERP protocol	Smart energy-efficient routing protocol	Better energy savings in IoT-WSNs	Limited testing under diverse scenarios
Nagaraju et al. [21]	Secure energy optimization	Routing-based optimization with heterogeneity	Enhanced secure communication in heterogeneous WSNs	Scalability and adaptability were not addressed
Singh et al. [22]	AI-based threat solution	Artificial intelligence for threat detection	Improved threat response using AI	Focuses more on security, less on energy routing
Singh et al. [23]	IoT-WSN integration for smart buildings	Real-time monitoring and energy optimization	Better resource usage in smart infrastructure	Security vulnerabilities are not fully addressed

However, this rarely works in IoT contexts that require adaptability to dynamically changing network topology and/or sensor node status. Pedditi and Debasis (2023) designed an energy-efficient routing system for a forest fire search scenario. Still, the solution was specific to that scenario and offered no dynamic adaptation capabilities for other IoT use cases. Tumula (2024) proposed a self-configuration protocol to improve the energy efficiency of WSNs without including a security architecture to address new threats (e.g., physical attacks and data modification) in the system. However, these methods either did not allow routing adjustments based on weather conditions or prioritized security over energy savings. Due to this, routing protocols addressing routing adjustments based on changing network conditions in real time while maximizing energy savings, security resilience, and risk have been a rare area of study

Whereas conventional routing protocols give priority to either security or energy efficiency, ESRL-WSNs provide notable benefits in both areas. The ESEERP protocol by Dogra et al. (2022) examined energy efficiency without considering potential security issues. Aldawsari's blockchain-based secure routing protocol (2025) also lets people send encrypted messages, but it takes a lot of processing power, so it is not good for low-powered IoT devices. ESRL-WSNs use a secure routing method and a reinforcement learning framework that adapts to the network to get the most out of its energy. Static routing protocols are used by traditional WSNs instead. The energy-efficient routing system keeps making the network better and safer. ESRL-WSNs is a new idea for future IoT systems. RL-based dynamic routing is different from other protocols because it has better security features.

The proposed work is unique because it made ESRL-WSNs, an RL-based routing protocol that puts security and energy efficiency first in IoT WSNs. ESRL-WSNs use a mix of both secure transmission and energy efficiency, which is different from other routing protocols that only focus on one of these things. RL finds the best routing paths by using real-time information about the network, such as residual energy, node trust levels, and known security holes. The protocol can help reduce the effects of energy loss and network instability because it is flexible. It can also protect against security threats like hacking and data manipulation. This protocol is less likely to fail than static or preconfigured routing systems because it can find problems. This means that even though

there are security problems, the protocol might still be able to provide reliable communication.

3. ESRL-WSNS Methodology

The ESRL-WSNs suggest a new and flexible way to route WSNs that use the Internet of Things. It fixes big problems like not having enough energy storage and the risks to network security. Reinforcement learning based on real-time data about energy levels, node stability, and security risks helps nodes learn how to change their routing paths. ESRL-WSNs has a small, built-in system that can find bad behavior and make sure that data is sent safely. The technology uses less energy, sends packets faster, and makes the network safer from attacks. This makes it a good choice for IoT networks that do not have a lot of resources and are always changing. Figure 1 shows how the ESRL-WSNs Method works in general.

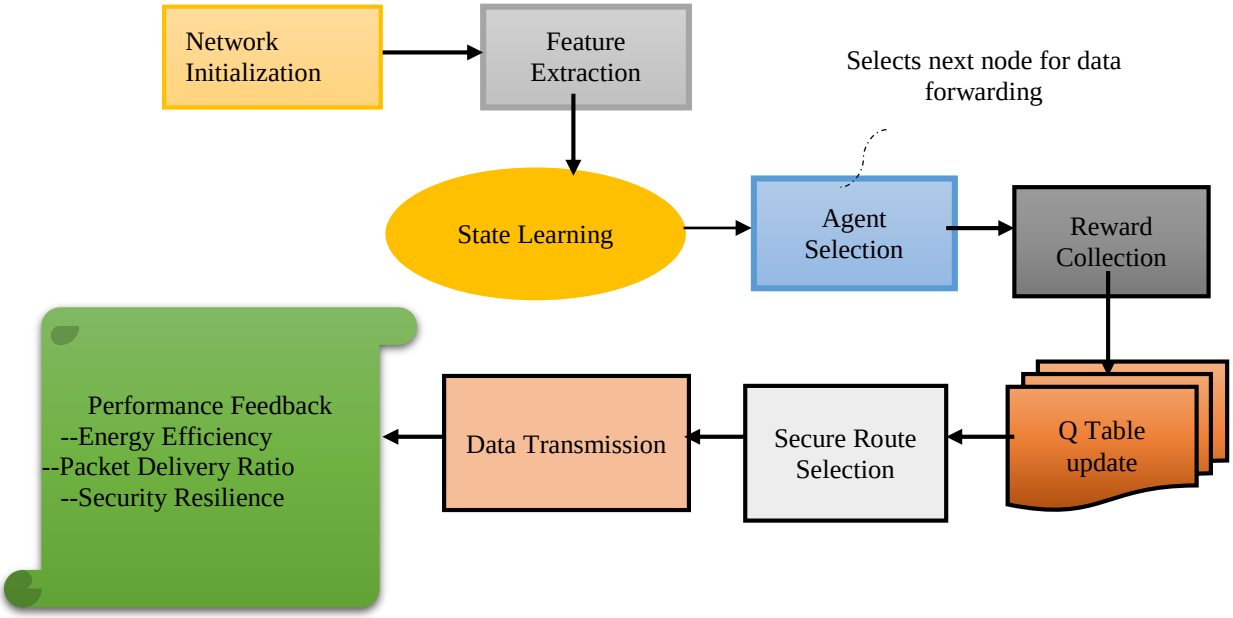


Fig. 1 Overall ESRL-WSNs approach workflow

3.1. Network Initialization

During the first phase of a WSN, sensor nodes are deployed over the region of interest and equipped with significant parameters, such as an initial power level, ID, and neighbor list. The initial power level of every node ($E_{init}(i)$) is equipped with a pre-defined value with adequate power for execution. The neighbor list ($N(i)$) is subsequently updated based on communication range, where nodes within a certain distance are neighbors. This initialization sets the nodes for collaborative sensing and forwarding. The neighbor list of a node (i) is defined as in Equation 1.

$$N(i) = \{j \mid d_{ij} \leq r_{max}\} \quad (1)$$

Where d_{ij} = The distance between nodes i *and* j, r_{max} = the maximum communication range of a node (i).

3.2. State Monitoring and Feature Extraction for RL

Key properties, such as residual energy, link quality, node trust score, and traffic rate, are regularly monitored. These properties constitute the node state, which is input to an RL agent to make intelligent routing and energy management decisions. Table 2 shows the Key Node-Level Features for State Monitoring.

Table 2. Key Node-Level features for state monitoring

Feature	Equation	Description
Residual Energy	$E_r(i,t) = E_{init}(i) - \sum_{k=1}^{t}(E_{transmit}(i,k) + E_{sense}(i,k))$	Remaining energy of node i at time t; essential for energy-aware decisions
Link Quality	$LQ(i,j,t) = \frac{PacketsReceived(j,t)}{PacketsSent(i,t)}$	Reliability of communication between node i *and* j; a higher value indicates a better link.

Node Trust Score	$T(i,t) = \frac{w_s \cdot S(i,t)}{w_s \cdot S(i,t) + w_f \cdot F(i,t)}$	A measure of trustworthiness based on successful and failed actions, weighted by w_s and w_f
Traffic Rate	$\tau(i,t) = \frac{TotalPackets(i,t)}{\Delta t}$	Rate of packet handling at node i; used for detecting congestion and balancing load

Where $S(i,t)$ = number of successful packet forwards by node i. $F(i,t)$ = number of failed or malicious actions, w_s, w_f = weights for success and failure, respectively. Δt is the time interval over which the packets are counted.

As shown in Equation 2, the RL agent uses a feature vector representing the node's current state.

$$S(i,t) = [E_r(i,t), LQ(i,j,t), T(i,t), \tau(i,t)] \quad (2)$$

This state vector provides a complete description of the node state, enabling the RL agent to choose the best actions, such as selecting the next hop or transmission power. Through real-time monitoring and feature extraction, the network adapts to energy-efficient behavior via learning-based policies.

3.3. Action Selection via RL Agent

A Q-learning-based RL agent is deployed at each node to make intelligent forwarding decisions to the optimal next-hop node. The agent learns to make decisions to optimize energy efficiency, reliability, and security by interacting with the environment over the long term. Figure 2 shows the action selection via the RL Agent.

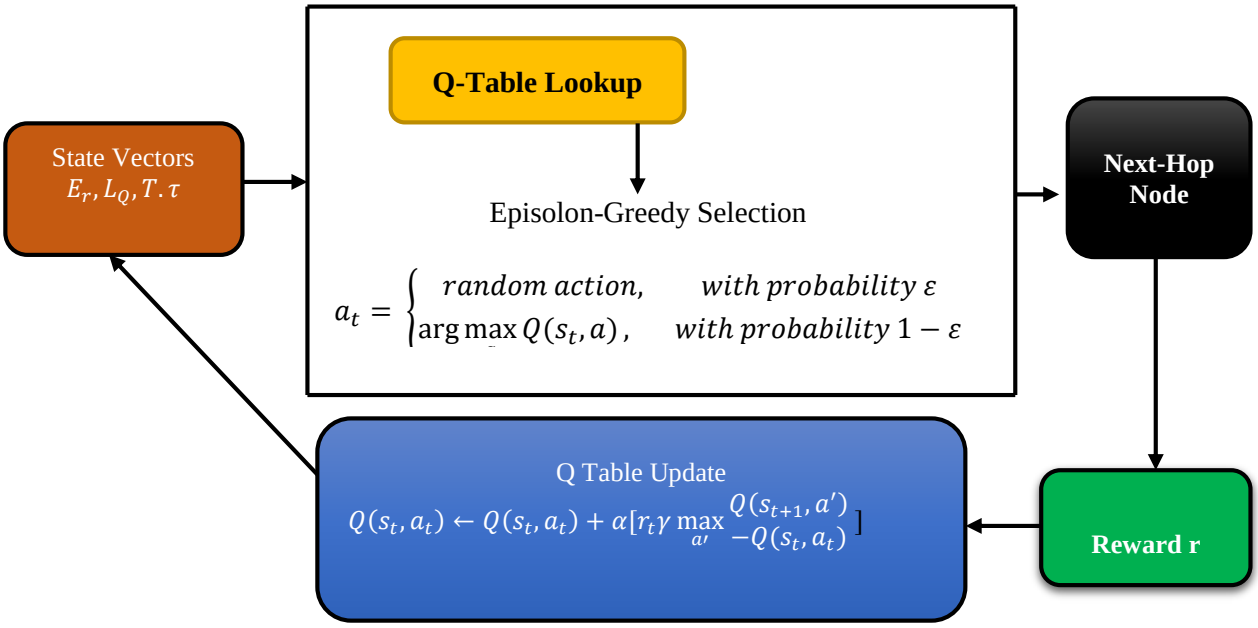


Fig. 2 Action Selection via RL Agent

3.3.1. Q-Learning Framework

In Q-learning, a value-based RL technique, an agent is utilized that has a Q-Table (s,) representing the anticipated total reward that is earned while acting (a) in state (s). The agent updates the Q-values using Bellman's Equation 3 after each decision step, selecting the action that maximizes them.

$$a_t = \arg\max_a Q(s_t, a)$$

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha[r_t + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)] \quad (3)$$

Where α = learning rate, γ = discount factor, r_t = reward received after acting a_t from state s_t, s_{t+1} = next state, a' = potential future actions.

3.3.2. Reward Function Structure

The Q-learning system's reward, denoted as (r_t), is designed to direct the RL agent toward routing actions that maximize the WSN's overall performance and security. To increase network lifetime, the reward is based on energy savings, so nodes with more residual energy are prioritized. Reducing packet loss and establishing strong communication links are two more ways the reward drives correct data delivery. Furthermore, node trustworthiness is incorporated to avoid routing through compromised or untrusted nodes. A weighted reward function incorporates all three components,

enabling the agent to make well-rounded forward decisions in context. Equation 4 defines a weighted reward function.

$$r_t = w_1 \cdot \eta(i) + w_2 \cdot DSR(i) + w_3 \cdot T(i) \quad (4)$$

Where $\eta(i)$ = normalized residual energy of node (i), $DSR(i)$ = delivery success rate to sink or neighbor, $T(i)$ = trust score of node (i). w_1, w_2, w_3 = weights assigned to energy, delivery, and trust factors, respectively.

3.3.3. Exploration vs. Exploitation (epsilon-greedy policy)

Equation 5 shows that an epsilon-greedy policy finds a happy medium between exploiting what is already known and exploring potential superior alternatives. To maximize performance, the policy allows the reinforcement learning agent to prioritize actions with the highest predicted rewards, while also allowing random action selection for exploration.

$$.a_t = \begin{cases} random\ action, & with\ probability\ \varepsilon \\ \arg\max_a Q(s_t, a), & with\ probability\ 1-\varepsilon \end{cases} \quad (5)$$

Where ε = The exploration rate can decay to favor exploitation as learning progresses.

3.4. Reward Calculation for the RL Agent to Next-Hop Selections

The reward function $(R(s,a))$ is designed carefully to promote the choice of safe, energy-efficient, and reliable paths. It is intended to guide the Reinforcement Learning (RL) agent to make optimal route choices by numerically evaluating all actions (i.e., next-hop node selection). The reward function includes three main criteria: Energy Efficiency, Packet Delivery Reliability, and Security Awareness (Attack Risk Penalty). The reward function is defined in Equation 6.

$$R(s,a) = \begin{cases} \alpha \cdot \frac{E_{residual}}{E_{initial}} + \beta \cdot PDR - \gamma \cdot AttackRisk \\ PDR = \frac{PacketsReceived_{sink}}{PacketsSent_{node}} \\ AttackRisk = 1 - T(i) \end{cases} \quad (6)$$

Where $R(s,a)$ = reward obtained for acting a in state s, $E_{residual}$ = Residual energy of the selected next-hop node, $E_{initial}$ = Initial energy of the node (for normalization), PDR = Packet Delivery Ratio (successful packets / total transmitted), $AttackRisk$ = Risk score indicating the likelihood of malicious activity or trust deficit, α, β, γ = Weight coefficients to balance the influence of each term. Figure 3 shows the RL-based reward and Q-Table update mechanism for secure, energy-efficient routing in WSNs.

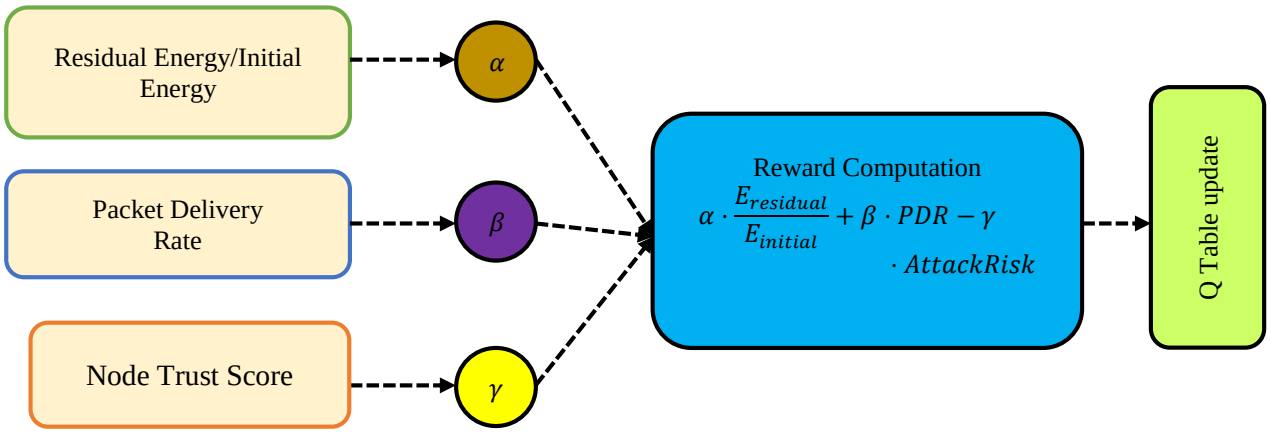


Fig. 3 RL-based reward and Q-table

The overall reward function guides the RL agent in making smart routing decisions by maximizing three essential objectives. The (α) term supports energy-efficient route selection by preferring nodes with more residual energy. The (β) term supports successful data transmission by preferring routes with high packet delivery rates. In contrast, the (γ) term penalizes routing through insecure or possibly malicious nodes, which increases network security. With tunable coefficients

$(\alpha, \beta\beta, \gamma), networkadministratorscanadjust$

$the\ system\ in\ real\ time\ to\ optimize$

specific objectives, e.g., network lifetime or attack resilience, based on the application scenario.

3.5. Routing Table Update in Q-Learning

In ESRL-WSNs, an energy-aware and secure routing framework for WSNs, routing decisions are taken through a Q-learning algorithm. The algorithm relies extensively on the Q-table to keep track of the expected utility of an action (a) in a state (s). The table is constantly updated based on received rewards and predicted future rewards. Algorithm 1 shows the Q-Learning-Based Routing for ESRL-WSNs.

Algorithm 1: Q-Learning-Based Routing for ESRL-WSNs

Input:

- Set of nodes NNN
- Initial Q-Table $Q(s,a)$
- Learning rate $\eta \in [0,1]$
- Discount factor $\delta \in [0,1]$
- Exploration probability $\epsilon \in [0,1]$

Output:

- Updated Q-Table with optimized routing decisions

1. Initialize Q-Table $Q(s,a)$ arbitrarily for all states $s \in S$ and action $a \in A$

2. For each time step $t = 1$ to T:

a. Observe the current state s_t (e.g., residual energy, link quality, trust score, traffic rate)

b. Choose an action a_t (next-hop node) using ε-greedy policy:

- Choose a random action (ϵ) based on chance. (exploration)
- Otherwise, select $a_t = \arg\max_a Q(s_t, a)$ (exploitation)

c. Perform action a_t; transmit packet to next-hop node

d. Observe reward (R_t) using:

$$R_t = \alpha \cdot \frac{E_{residual}}{E_{initial}} + \beta \cdot PDR - \gamma \cdot (1 - T(i))$$

e. Observe the next state s_{t+1}

f. Update Q-value using:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[r_t + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t) \right]$$

3. Repeat until convergence or maximum episodes reached

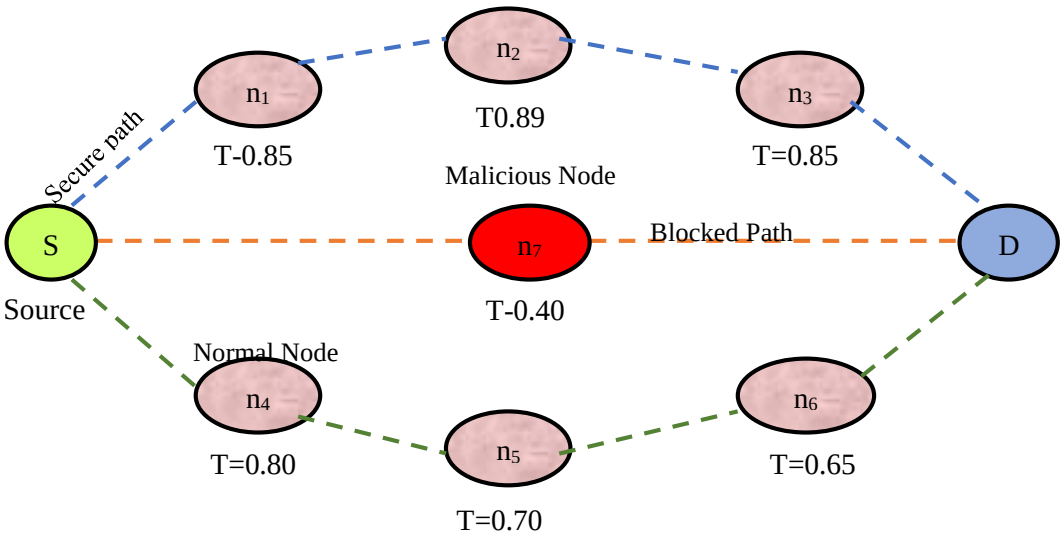


Fig. 4 ESRL-WSN Secure Route Selection and Data Transmission

3.6. Secure Route Selection

- Every node i is assigned a trust value $T(i,t) \in [0,1]$ that is updated dynamically over time according to its actions and activities with other nodes.
- The network continuously monitors nodes for signs of malicious behavior, such as blackhole or sinkhole attacks, using behavior-based and statistical indicators.
- A trust threshold T^{th} is defined to distinguish secure nodes from potentially malicious ones.
- A node is evaluated using the following condition. Equation 7 determines whether a node is considered secure.

$$\left.\begin{array}{r} T(i,t) \geq T_{th} \text{ and } A(i,t) = 0, \quad \text{node is secure} \\ T(i,t) < T_{th} \text{ or } A(i,t) = 1, \quad \text{are excluded from} \\ \text{the routing candidate set} \end{array}\right\} \quad (7)$$

Where $T(i,t)$ = Trust score of node (i) at time (t), T_{th} = Minimum acceptable trust score (e.g., 0.6), $A(i,t)$ = Binary

attack detection metric (1 if malicious behavior is detected, zero otherwise). The filtered subset is shown in Equation 8.

$$A_{secure} = \{a \in A \mid T(a,t) \geq T_{th} \wedge A(a,t) = 0\} \quad (8)$$

This filtered subset (A_{secure}) is then used by the RL agent to choose the next-hop action. This system imposes security at the routing decision point without a performance penalty.

Figure 4 illustrates secure routing in ESRL-WSNs. Trust scores screen nodes, and attacks are detected before transmission. Source (S) must route to Destination (D) through nodes with $T \geq T_{\min}$ and no detected attack. Two secure routes are available, while the middle route is unavailable due to the malicious node n_7 (T=0.40). The RL agent chooses energy-efficient paths among secure nodes so all path members have sufficient energy and security credentials.

3.7. Data Transmission

When an RL agent chooses a secure and energy-efficient next-hop node, the data packet travels along its respective path, which includes intermediate nodes that meet energy and security requirements.

When the process is executed, the network topology can change in real time due to factors such as node mobility, energy depletion, or malicious activity. According to Equation 9, let a sequence of nodes represent the chosen path from source node S to sink node D.

$$P_{S \to D} = \{n_1 = S, n_2, \ldots, n_k = D\} \quad (9)$$

The path $P_{S \to D}$ is valid if each hop (n_i, n_{i+1}) satisfies the condition in Equation 10.

$$T(n_{i+1}, t) \geq T_{th} \wedge E_r(n_{i+1}, t) \geq E_{min} \wedge A(n_{i+1}, t) = 0 \quad (10)$$

Where $T(n_{i+1}, t)$ Trust score of node (n_{i+1}) at the time t. $E_r(n_{i+1}, t)$ = Residual energy of node (n_{i+1}) at time t. E_{min} = Minimum energy threshold to participate in forwarding, $A(n_{i+1}, t)$ = Binary attack flag (1 = malicious, 0 = normal). The total energy consumed in the transmission is calculated as in Equation 11.

$$E_{total} = \sum_{i=1}^{k-1} (E_{tx}(n_i, n_{i+1}) + E_{rx}(n_{i+1})) \quad (11)$$

Where $E_{tx}(n_i, n_{i+1})$ = Transmission energy from the node (n_i) to (n_{i+1}), $E_{rx}(n_{i+1})$ = Reception energy at node n_{i+1}.

ESRL-WSNs' safe and energy-efficient routing can help IoT networks. ESRL-WSNs dynamically optimize routes based on environmental conditions and real-time network data to speed up packet delivery and cut down on energy use. ESRL-WSNs can swiftly respond to attacks and changes in the network because they can find threats.

4. Evaluation Metrics and Results

4.1. Dataset Explanation

IoT and Wireless Sensor Network (WSN) solutions were first intended to be tested on the large, open FIT IoT-LAB testbed from Inria [24]. Over 2,700 sensor nodes are dispersed among multiple locations. These nodes are composed of several gadgets with sensors and ARM Cortex CPUs. The testbed's capabilities make it an excellent tool for assessing secure and energy-efficient routing systems. These consist of practical deployment scenarios, power measurement tools, adaptable topologies, and security experiment support. It can be used to evaluate its energy consumption, scalability, and assault resistance. Thus, despite certain limitations, it is the ideal location to test the ESRL-WSNs protocol in practice.

4.2. Experimental Setup

An extensive experimental environment for testing IoT networks is the FIT IoT-LAB testbed. The ESRL-WSNs protocol is assessed there. Numerous sensor nodes with ARM Cortex processors that support a variety of real-world IoT applications are part of the setup.

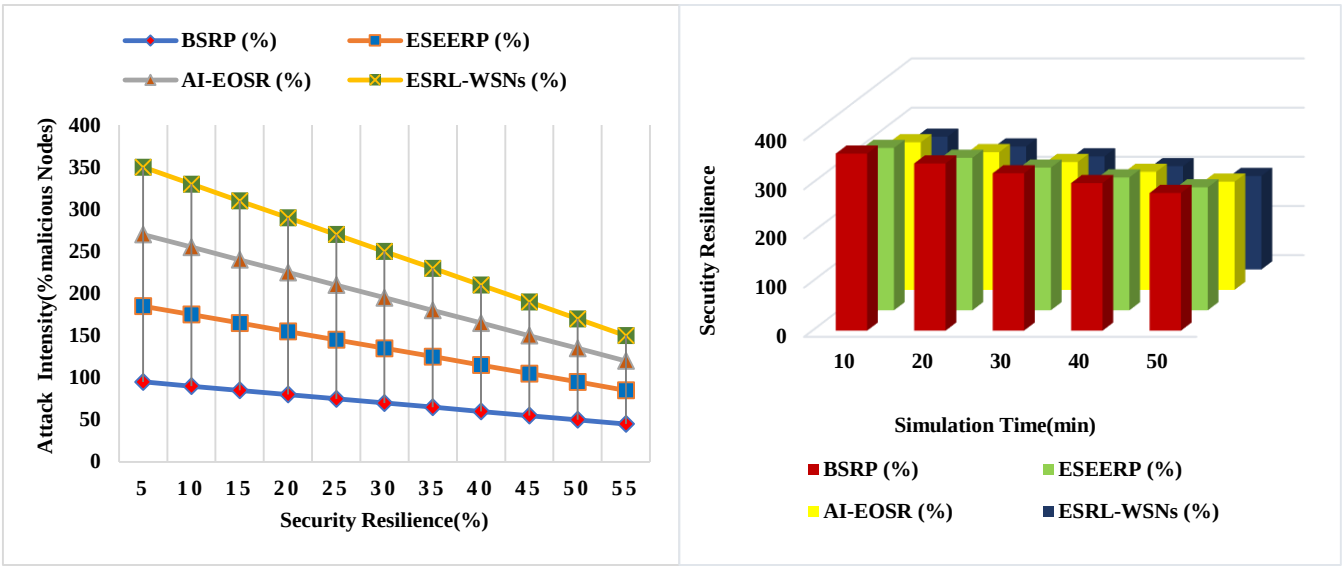
The Blockchain-based Secure Routing Protocol (BSRP) [20], Enhanced Smart Energy Efficient Routing Protocol (ESEERP) [21], and AI-Assisted Energy Optimized Secure Routing (AI-EOSR) are the methods being compared [25]. Key measures, such as energy use, Packet Delivery Ratio (PDR), security resilience, and end-to-end delay, are used to evaluate performance. These measurements show how well each routing system uses energy, how reliable it is for sending data, and how secure it is when the network is changing and perhaps hostile.

4.3. Energy Consumption

Energy consumption refers to the power required to run the sensing, transmitting, receiving, and processing functions of energy sensor nodes. Protocols designed to be energy-efficient aim to prolong the network's lifespan while reducing power consumption. Examining Equation 12 is one approach to decomposing the energy consumed by a sensor node in a WSN.

$$E_{total} = \begin{cases} E_{TX} + E_{RX} + E_{Sensing} + E_{Processing} \\ where\ E_{TX} = \alpha \times Distance^2 + \beta \\ E_{RX} = \gamma \times Distance + \delta \end{cases} \quad (12)$$

Where E_{TX} = energy is used during the transmission of data. E_{RX} = energy is used during the reception of data. $E_{Sensing}$ = energy consumed by the sensors during data acquisition. $E_{Processing}$ = energy is used by the processor to process data. $\alpha, \beta, \gamma, \delta$ = Constants depending on hardware specifications. $Distance$ refers to the communication range between the nodes.



(a) Energy consumption of routing protocols under varying network densities **(b) Energy consumption comparison over time**

Fig. 5 Comparative analysis of energy consumption for ESRL-WSNs and benchmark protocols across time and network density

Figure 5(a) compares the energy consumption of ESRL-WSNs, BSRP, ESEERP, and AI-EOSR under different network densities. ESRL-WSNs consume the least energy, demonstrating optimal scalability and efficiency in dense IoT networks.

Figure 5(b) compares cumulative energy consumption over time as packets are sent every 10 seconds. ESRL-WSNs again consume the least energy, and the difference increases over time compared to other protocols.

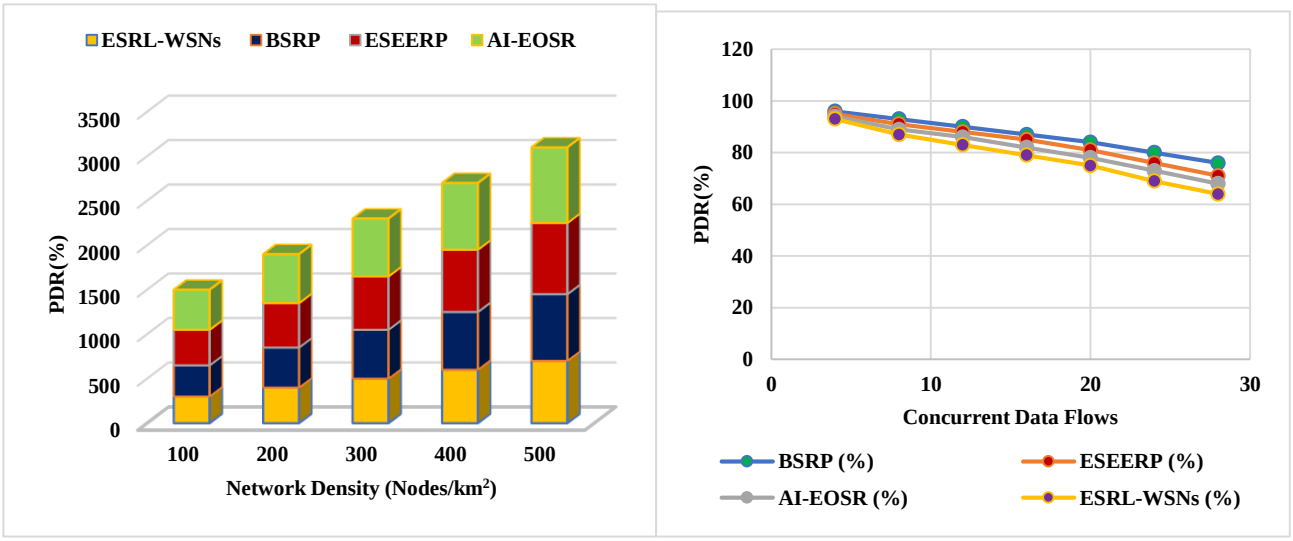
These findings demonstrate the effectiveness of ESRL-WSNs in reducing energy overhead and extending network lifetime. Thus, it is most appropriate for energy-limited large-scale IoT-based wireless sensor network applications.

4.4. Packet Delivery Ratio (PDR)

PDR is a performance metric to assess a routing protocol's reliability and efficiency in WSNs and IoT systems. It is the proportion of packets transmitted to destination nodes from those sent by source nodes. It can be quantified as shown in Equation 13.

$$PDR = \frac{PacketsNumber\ of\ Successfully\ Delivered\ Packets}{Total\ Number\ of\ Sent} \times 100 \quad (13)$$

Where $Successfully\ Delivered\ Packets =$ Packets reached the destination node without being lost, delayed, or corrupted. $Total\ Sent\ Packets$ relate to the quantity of packets sent between the source and destination nodes.



(a) PDR across varying network densities **(b) PDR performance with increasing concurrent data flows**

Fig. 6 PDR evaluation of ESRL-WSNs under network density and traffic load variations

Figure 6(a) shows the PDR (%) of ESRL-WSNs and contrast protocols with rising network densities. ESRL-WSNs consistently achieve the highest delivery ratio, demonstrating efficiency and reliability in dense deployments. The outcomes demonstrate its competence in maintaining successful communication and minimizing packet loss under heavy IoT traffic.

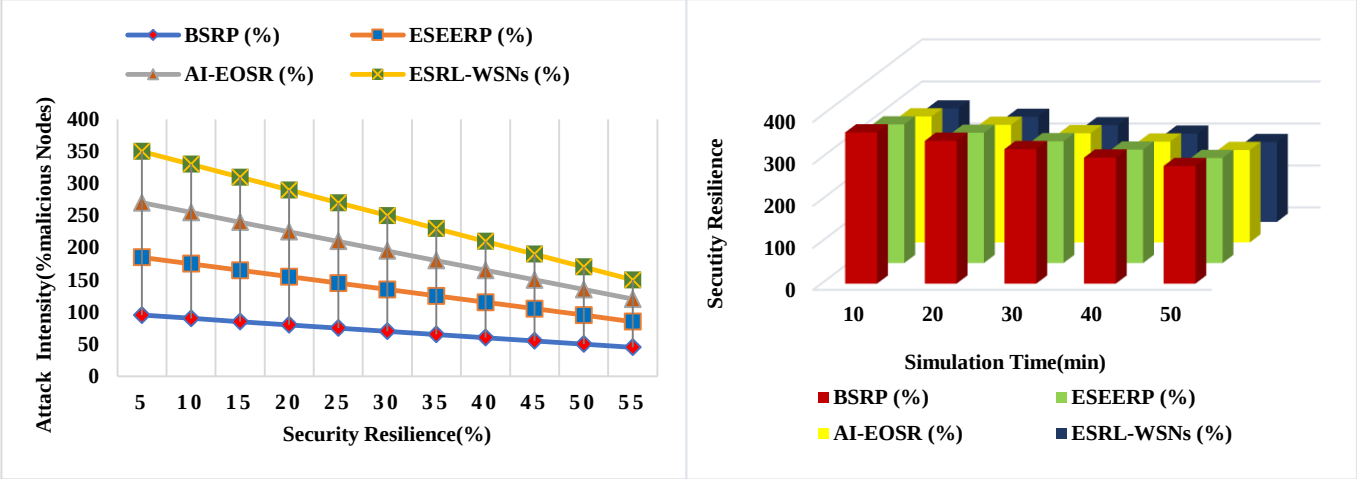
Figure 6(b) contrasts PDR as concurrent data streams grow. ESRL-WSNs delivers higher delivery rates than other protocols, demonstrating greater robustness under heavy traffic. Its performance reflects the protocol's flexibility and reliability in providing real-time data in complicated, multi-source wireless sensor network scenarios.

4.5. Security Resilience

Security Resilience may be defined as a routing protocol's ability to maintain stable performance (i.e., data delivery) under attack or in the presence of malicious nodes in a WSN. Equation 14 shows a standard metric for quantifying security resilience.

$$Security\ Resilience\ (SR) = \frac{PDR\ under\ attack}{PDR\ in\ normal\ conditions} \times 100 \quad (14)$$

Where $PDR\ under\ attack$ = Packet Delivery Ratio with attack nodes. $PDR\ in\ normal\ situation$ = Packet Delivery Ratio with 0% attack nodes, SR (%) Shows to what degree original delivery performance is maintained irrespective of attacks.



(a) Security resilience against varying attack intensities **(b) Security resilience over increasing simulation time**

Fig. 7 Security resilience evaluation of ESRL-WSNs under malicious attacks and prolonged operation

Figure 7(a) shows the PDRs of the different protocols as the number of malicious nodes increases. ESRL-WSNs performs better than all others, achieving the maximum PDR even under 50% attack intensity. This proves its high security resilience and capability to provide reliable communication under hostile conditions. Figure 7(b) illustrates PDR degradation over time for malicious activities. ESRL-WSNs exhibits better delivery performance than baseline protocols, indicating its long-term security. ESRL-WSNs maintains consistent communication and data integrity in IoT networks, even during extended, attack-holding simulations.

4.6. End-to-End Delay(E2ED)

E2ED measures the typical amount of time it takes for a data packet to go from its origin node all the way to its destination node in a network. Included in this category are delays caused by processing, queuing, transmission, and propagation difficulties. Equation 15 represents this.

$$E2ED = \frac{1}{N}\sum_{i=1}^{N}(t_{received,i} - t_{sent,i}) \quad (15)$$

Where N = Total number of successfully received packets, $t_{sent,i}$ = Timestamp when a packet i was sent, $t_{received,i}$ = Timestamp when a packet i was received. Lower E2ED values indicate faster communication, especially for delay-sensitive applications such as real-time monitoring in WSNs.

Table 3. End-to-End delay comparison of routing protocols at different network sizes

Number of Nodes	BSRP (ms)	ESEERP (ms)	AI-EOSR (ms)	ESRL-WSNs (ms)
50	155	138	122	105
100	198	174	159	128
150	245	198	174	142
200	282	225	193	159

For various network sizes, Table 3 shows how four routing methods perform in terms of end-to-end latency. More

nodes mean more congestion and more complex routing, leading to longer delays. BSRP experiences the maximum delay because it lacks adaptive, secure routing. ESEERP cuts down on delays by using energy-efficient ways, whereas AI-EOSR cuts down on delays by using smart routing. Even in extremely busy networks, the ESRL-WSNs we discussed always have the least amount of delay because they employ energy-aware judgments, trust-based security, and reinforcement learning to make transmission faster and safer.

5. Conclusion

The ESRL-WSNs method solves the main problems with energy efficiency and security in IoT WSNs. ESRL-WSNs use reinforcement learning to adapt to changes in the network and learn the best paths to take. This lets them make smart routing decisions based on perceived danger, node health, and remaining energy. To ensure its performance, ESRL-WSNs was compared with available methods such as BSRP, ESEERP, and AI-EOSR using the following performance metrics: Energy Consumption, PDR, and Security Resilience. The simulation results from the FIT IoT-LAB testbed showed that ESRL-WSNs consume significantly less energy, increase delivery rates, and remain secure under attack conditions or with high data traffic. Combining learning-based flexibility and security-consciousness renders ESRL-WSNs a durable and trustworthy routing scheme for IoT applications, especially in energy-limited scenarios and security attacks. This paper has paved the way for future directions on decentralized learning, trust-sensitive routing, and edge intelligence to construct innovative and secure IoT infrastructure.

References

[1] Alireza Souri et al., "A Systematic Review of IoT Communication Strategies for an Efficient Smart Environment," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nickson M. Karie et al., "A Review of Security Standards and Frameworks for IoT-based Smart Environments," *IEEE Access*, vol. 9, pp. 121975-121995, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohammad ameid alkato, and Nekita kalenen, "Dynamic Pattern Analysis for Enhanced Predictive Intelligence in Smart Environments using Transformer Learning Models," *PatternIQ Mining*, vol. 2, no. 1, pp. 1-14, 2025. [CrossRef] [Publisher Link]

[4] Amin Ullah et al., "Smart Cities: The Role of Internet of Things and Machine Learning in Realizing a Data-Centric Smart Environment," *Complex & Intelligent Systems*, vol. 10, pp. 1607-1637, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohamed Shakeel Pethuraj, Burhanuddin bin Mohd Aboobaider, and Lizawati Binti Salahuddin, "Analyzing QoS Factor in 5G Communication Using Optimized Data Communication Techniques for E-commerce Applications," *Optik*, vol. 272, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ada Malagnino et al., "Building Information Modeling and Internet of Things Integration for Smart and Sustainable Environments: A Review," *Journal of Cleaner Production*, vol. 312, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Nikhil Sharma et al., *Attacks and Security Measures in Wireless Sensor Network*, Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, pp. 237-268, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Walid Osamy et al., "IPDCA: Intelligent Proficient Data Collection Approach for IoT-Enabled Wireless Sensor Networks in Smart Environments," *Electronics*, vol. 10, no. 9, pp. 1-28, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ting-Yu Lin et al., "Collision-Free Motion Algorithms for Sensors Automated Deployment to Enable A Smart Environmental Sensing-Net," *IEEE Transactions on Automation Science and Engineering*, vol. 19, no. 4, pp. 3853-3870, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Fatma H. El-Fouly et al., "Environment-Aware Energy Efficient and Reliable Routing in Real-Time Multi-Sink Wireless Sensor Networks for Smart Cities Applications," *Applied Sciences*, vol. 13, no. 1, pp. 1-37, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Nasfikur Rahman Khan et al., "Internet of Things and Wireless Sensor Network Solution in Smart Environmental Monitoring," *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, Coimbatre, India, pp. 1-5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Qianao Ding et al., "An Overview of Machine Learning-Based Energy-Efficient Routing Algorithms in Wireless Sensor Networks," *Electronics*, vol. 10, no. 13, pp. 1-24, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Rajagopal Maheswar, Murugan Kathirvel, and Kuppusamy Mohanasundaram, "Energy Efficiency in Wireless Networks," *Energies*, vol. 17, no. 2, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Sebastin Suresh et al., "Intelligent Data Routing Strategy based on Federated Deep Reinforcement Learning for IoT-Enabled Wireless Sensor Networks," *Measurement: Sensors*, vol. 31, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Mohammad Al Razib et al., "Cyber Threats Detection in Smart Environments using SDN-Enabled DNN-LSTM Hybrid Framework," *IEEE Access*, vol. 10, pp. 53015-53026, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ramesh Babu Pedditi, and Kumar Debasis, "Energy Efficient Routing Protocol for an IoT-based WSN System to Detect Forest Fires," *Applied Sciences*, vol. 13, no. 5, pp. 1-22, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sridevi Tumula et al., "An Opportunistic Energy-Efficient Dynamic Self-Configuration Clustering Algorithm in WSN-based IoT Networks," *International Journal of Communication Systems*, vol. 37, no. 1, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zeeshan Ali, "Enhancing the Energy Efficiency of Wireless Sensor Networks in IoT," *International Journal of Advanced Engineering, Management and Science*, vol. 11, no. 1, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Hamad Aldawsari, "A Blockchain-Based Approach for Secure Energy-Efficient IoT-based Wireless Sensor Networks for Smart Cities," *Alexandria Engineering Journal*, vol. 126, pp. 1-7, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] Roopali Dogra et al., "ESEERP: Enhanced Smart Energy Efficient Routing Protocol for Internet of Things in Wireless Sensor Nodes," *Sensors*, vol. 22, no. 16, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Regonda Nagaraju et al., "Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks," *Energies*, vol. 15, no. 13, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Omkar Singh et al., "Navigating Security Threats and Solutions using AI in Wireless Sensor Networks," *International Journal of Communication Networks and Information Security*, vol. 16, no. 4, pp. 411-427, 2024. [Google Scholar] [Publisher Link]

[23] Someet Singh et al., "An Integrated IoT and Wireless System for Energy Optimization and Real-Time Monitoring Towards Sustainable and Efficient Building Management in Smart Buildings," *2025 International Conference on Intelligent Control, Computing and Communications (IC3)*, Mathura, India, pp. 416-422, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] The First Experiment for Beginners, IoT-Lab, 2025. [Online]. Available: https://iot-lab.github.io/learn/