ISSN: 2993-8643

Research Article

Engineering: Open Access

Decentralized Multi-Hop Federated Reinforcement Learning for Energy-Efficient and Secure Routing in LoRaWAN-Based Smart City Infrastructure

Harsha Sammangi*, Aditya Jagatha and Jun Liu

Dakota State University, USA

***Corresponding Author**
Harsha Sammangi, Dakota State University, USA.

Submitted: 2025, May 16; **Accepted:** 2025, Jun 18; **Published:** 2025, Jun 23

Citation: Sammangi, H., Jagatha, A., Liu, J. (2025). Decentralized Multi-Hop Federated Reinforcement Learning for Energy-Efficient and Secure Routing in LoRaWAN-Based Smart City Infrastructure. *Eng OA, 3*(6), 01-08.

Abstract

LoRaWAN (Long Range Wide Area Network) has emerged as a foundational technology in smart city infrastructures due to its capability to facilitate long-range, low-power communication between Internet of Things (IoT) devices. However, the inherently resource-constrained nature of these devices, coupled with dynamic network conditions, necessitates the development of advanced routing strategies that balance energy efficiency, data security, and scalability. This paper introduces a novel hybrid framework that integrates Federated Learning (FL) and Reinforcement Learning (RL) to enable decentralized, multi-hop routing in LoRaWAN-enabled smart cities. By leveraging localized model training (FL) and adaptive decision-making (RL), the framework addresses core challenges such as node mobility, trustworthiness, and network longevity. Through simulation-based evaluation, the proposed system demonstrates significant improvements in energy conservation, routing robustness, and protection against eavesdropping and tampering attacks, offering a scalable solution for future smart urban ecosystems.

1. Introduction

1.1. Background

The increasing adoption of Internet of Things (IoT) technologies has paved the way for smart city infrastructures that enhance urban living through real-time sensing, efficient energy use, and improved public services. Among the various wireless communication technologies supporting these ecosystems, LoRaWAN has gained prominence due to its ability to provide long-range, low-power communication suitable for diverse applications including traffic monitoring, smart metering, and waste management (?). Unlike short- range technologies such as Zigbee or Wi-Fi, LoRaWAN offers a star-of-stars topology and operates on unlicensed sub-GHz ISM bands, allowing for cost-effective deployment without spectrum licensing constraints (?).

Despite these advantages, LoRaWAN networks face challenges in routing efficiency and data security, especially in multi-hop environments where direct communication with a gateway may not always be feasible. Traditional single-hop approaches are inadequate for complex urban topologies where obstacles or interference may hinder direct transmis- sion. Furthermore, static routing decisions can lead to suboptimal energy consumption, reduced device lifespan, and higher latency (?).

1.2. Overview of LoRaWAN in Smart Cities

LoRaWAN plays a pivotal role in enabling smart city functions by offering scalable and energy-efficient connectivity for low-data-rate devices. Applications of LoRaWAN in urban contexts include flood detection systems, air quality monitoring, smart lighting, and parking management (?). These systems typically consist of end devices, gateways, and a central network server. End devices send data to gateways, which forward it to the server, often via the internet. In traditional deployments, communication is mostly single-hop, which can limit coverage and reliability.

To address coverage gaps and improve resilience, multi-hop routing has been proposed, allowing data packets to traverse multiple nodes before reaching the gateway. How- ever, this introduces complexity in routing decisions, especially under energy constraints. Moreover, LoRaWAN lacks native support for multi-hop topologies, necessitating custom routing protocols and modifications at the MAC layer (?). These enhancements must

also account for the heterogeneous nature of devices, fluctuating channel conditions, and varying Quality of Service (QoS) requirements.

1.3. Need for Energy-Efficient and Secure Routing

Energy efficiency and security are critical in IoT networks, particularly in smart cities where devices are expected to operate autonomously for extended periods. Frequent battery replacements or failures due to energy depletion can disrupt critical services and lead to increased operational costs (?). Additionally, the open nature of LoRaWAN transmissions makes the network susceptible to eavesdropping, replay attacks, and node impersonation (?).

Conventional routing protocols often overlook energy-awareness and security in their design. While some protocols optimize for shortest-path or signal strength, they may inadvertently overburden specific nodes, accelerating battery drain. Moreover, central- ized routing decisions require continuous data aggregation, raising privacy concerns and introducing potential points of failure.

The integration of machine learning techniques, particularly FL and RL, offers a promising avenue for addressing these issues. FL enables localized model training, reduc- ing data transfer and enhancing privacy, while RL supports adaptive routing decisions based on real-time network states. A hybrid approach can balance energy consumption, enhance data confidentiality, and provide resilient routing mechanisms suitable for the dynamic conditions in smart cities (?).

1.4. Research Gap

Although there has been substantial progress in optimizing LoRaWAN for smart cities, several limitations remain in current routing methodologies. Most existing approaches are either static or rely on centralized architectures, which do not scale well and pose security risks. Moreover, many machine learning-based solutions require extensive computational resources, making them impractical for low-power IoT nodes (Mick, 2018) [1].

Studies focusing on FL in IoT often neglect the routing dimension, while RL applica- tions typically lack privacy-preserving mechanisms. Furthermore, few works explore the combination of FL and RL in a decentralized, multi-hop context tailored to the character- istics of LoRaWAN. This research aims to fill that gap by proposing a hybrid framework that jointly optimizes energy efficiency, routing reliability, and data security through fed- erated reinforcement learning. The proposed solution addresses both technical feasibility and real-world applicability, setting the foundation for resilient smart city infrastructure.

2. Literature Review

2.1. Federated Learning (FL) in IoT

Federated Learning (FL) has emerged as a privacy-preserving machine learning paradigm that enables distributed model training across multiple edge devices without sharing raw data. In the context of the Internet of Things (IoT), FL helps to address key challenges such as limited bandwidth, data privacy, and resource constraints. Each device trains a local model on its data and transmits only the model updates to a central server for aggregation, reducing the risk of data leakage during transmission (Kairouz et al., 2021). This decentralized approach aligns well with the distributed nature of IoT networks and is increasingly being considered for healthcare, smart grids, and autonomous vehicles (Li et al., 2020).

Despite its potential, FL in IoT presents challenges related to com- munication over- head, non-IID (non-independent and identically distributed) data, and heterogeneity in device capabilities (Yang et al., 2019). Several approaches, such as asynchronous up- dates, hierarchical FL, and edge aggregation strategies, have been pro- posed to address these challenges. For instance, Lim et al. (2020) introduced a hierarchical FL framework tailored to IoT devices that reduces latency and energy consumption by aggregating mod- el updates at local gateways before sending them to the global server.

2.2. Reinforcement Learning (RL) Techniques Adapted for IoT

Reinforcement Learning (RL) is a learning paradigm where agents learn optimal policies through trial-and-error interactions with the environment. Its adaptability and online learning capabilities make it particularly suitable for dynamic IoT settings such as wireless sensor networks, autonomous routing, and energy management systems (Zhang et al., 2022).

In IoT, RL-based models are frequently used to address resource allocation, device scheduling, and mobility management challenges. Deep Q-Networks (DQNs) and Actor- Critic methods have been customized for constrained environments to make energy-aware and latency-sensitive decisions. For example, Xu et al. (2021) demonstrated the use of RL in managing data transmission schedules in energy-constrained wireless body area networks (WBANs), achieving reduced delay and power consumption.

However, standalone RL models in IoT may suffer from scalability issues and poor generalization in unseen scenarios. Integrating FL with RL, often referred to as Fed-erated Reinforcement Learning (FRL), helps overcome these limitations by leveraging distributed knowledge sharing while preserving device privacy (Liu et al., 2021).

2.3. Multi-Hop Routing in LoRaWAN

LoRaWAN (Long Range Wide Area Network) is a leading communication protocol for low-power wide-area networks (LPWANs) used in smart cities. While traditionally de- ployed in a single-hop star topology, recent research advocates for multi-hop routing to overcome range and scalability limitations (Adelantado et al., 2017). Multi-hop ap- proaches enable nodes to relay messages through intermediate devices, improving coverage and reliability.

Several multi-hop strategies for LoRaWAN have been explored, such as Time Divi- sion Multiple Access (TDMA)-based scheduling, directional forwarding, and energy-aware routing

algorithms. For instance, Fajardo et al. (2020) proposed an energy-efficient multi- hop scheme that dynamically adjusts transmission power and relay selection to extend node lifetime.

Nevertheless, challenges persist, including increased packet loss, synchronization com- plexity, and routing loop avoidance. Combining RL with multi-hop LoRaWAN routing can help nodes adaptively select the best forwarding path based on local observations and historical feedback.

2.4. Security Protocols in IoT Networks

IoT devices often operate with limited computational power and are vulnerable to var- ious security threats, including spoofing, eavesdropping, and data tampering. As such, lightweight cryptographic mechanisms and decentralized trust models are critical for en- suring secure data exchange in IoT environments.

2.4.1. Lightweight Encryption and Privacy Mechanisms

Given the resource-constrained nature of IoT devices, traditional encryption algorithms such as RSA and AES may be computationally expensive. Consequently, lightweight cryptographic techniques, including elliptic curve cryptography (ECC), hash-based signatures, and symmetric key protocols, have been proposed (Cheikh et al., 2022) [2]. These methods strike a balance between security and performance, enabling secure transmission while conserving battery life.

Homomorphic encryption and differential privacy have also gained attention in FL- enabled IoT systems. These methods allow computations on encrypted data or introduce noise to protect individual privacy while maintaining model accuracy (Geyer et al., 2017).

2.4.2. Existing Approaches to Decentralized Learning

Traditional machine learning and reinforcement learning models rely on centralized data storage and processing, which poses risks in terms of privacy and scalability. Decentralized learning frameworks aim to mitigate these risks by enabling edge devices to collaboratively train models without transferring raw data [3]. Mick et al. (2018) introduced a decentralized deep RL framework using gossip-based communication among agents, avoiding central coordination. However, such methods face challenges including slow convergence, inconsistent updates, and network topology dependencies.

Recent studies advocate for hybrid models that combine decentralization with occa- sional centralized coordination to balance convergence speed and model accuracy (Lalitha et al., 2019). These approaches provide valuable insights for building robust and scalable federated reinforcement learning systems in smart city applications.

3. Proposed Framework

3.1. Framework Overview

The proposed framework introduces a hybridized solution that leverages both Federated Learning (FL) and Reinforcement Learning (RL) to enhance routing decisions and secure data transmission in LoRaWAN-enabled smart city infrastructures. It is designed to be decentralized, scalable, and capable of learning from diverse network environments without centralized data aggregation. The framework is layered to include sensing and data generation at the device level, learning and decision-making at the edge, and policy management at a distributed cloud coordinator. Each LoRaWAN gateway functions as an FL client while base stations and application servers provide coordination. This structure facilitates model training at local nodes and periodic aggregation of model weights, preserving data locality and privacy.

The architecture consists of four interconnected modules: the FL module for dis- tributed training, the RL module for real-time routing decisions, the energy-trust calcu- lator for resource optimization, and the security layer for data integrity. A knowledge- sharing module periodically synchronizes models across nodes using techniques like Fe- dAvg or FedProx to handle heterogeneity. Smart contracts and blockchain may be option- ally integrated to verify model updates and maintain a tamper-evident training log. This holistic design empowers the system to make intelligent, localized, and secure routing decisions under varying network conditions.

3.2. Integration of FL and RL

Integrating FL and RL brings the advantage of continuous learning in dynamic IoT envi- ronments without compromising data privacy. In this system, FL serves as the foundation for sharing model parameters learned from local routing environments, while RL tailors the decision-making process to current network states. Each node, such as a LoRa gate- way or smart device, uses a localized RL model to determine the best next-hop decision based on context (e.g., battery life, link quality, congestion levels), and updates the global policy via FL.

This integration resolves the classic exploration-exploitation trade-off in RL by utiliz- ing federated updates from multiple nodes. Q-learning or Deep Q-Networks (DQN) can be used at each node, while the FL server aggregates these experiences to build a more robust global model. The reward function may include metrics like packet delivery ratio, latency, and energy cost. As a result, the system balances node-specific behaviors with globally learned strategies. Previous work by Li et al. (2021) supports the effectiveness of FL-enhanced RL in heterogeneous IoT networks.

3.3. Adaptive Context-Aware Routing Decisions

To ensure optimal data flow, the framework incorporates an adaptive routing engine that utilizes reinforcement learning in a context-aware manner. Each node continuously monitors environmental features such as link reliability, energy level, and traffic load. These features form the state space of the RL agent, which is dynamically updated during data transmission cycles.

The action space includes selecting next-hop nodes among neighboring devices based on calculated Q-values. As network dynamics evolve (e.g., a node's battery depletes or congestion rises), the RL agent adjusts its routing policy in real-time. This

results in flexible, efficient path selections tailored to current conditions. This level of adaptiveness is crucial in LoRaWAN deployments where fixed routes can lead to rapid energy depletion or bottlenecks.

Simulation studies by Zhang et al. (2022) highlight that context-aware RL agents reduce average hop count and increase network lifespan by 18–25% compared to static routing algorithms. Our framework refines this approach further by allowing nodes to share reward metrics through federated updates, achieving convergence faster while re- specting privacy constraints.

3.4. Integration of Energy Awareness and Trust Levels

A dual-metric system incorporating both energy awareness and trust levels is embedded in the routing decision process. Energy awareness ensures that data is routed through nodes with sufficient residual power, while trust levels quantify the historical reliability and security compliance of each node. These metrics influence the reward function in RL, encouraging paths that optimize both longevity and trustworthiness.

Trust is calculated using a decentralized trust model that evaluates past behavior such as packet forwarding rates, error logs, and compliance with FL protocol participa- tion. Nodes with repeated inconsistencies or anomalies are penalized in routing deci- sions. Energy metrics are updated based on hardware-supplied battery indicators and data transmission logs.

This multi-objective optimization improves overall system resilience and sustainabil- ity. Combining trust and energy considerations allows the system to avoid vulnerable or exhausted nodes without sacrificing performance. Similar hybrid metrics were employed in the TE-Fed framework developed by Huang et al. (2023), demonstrating improved robustness in IoT networks.

3.5. Data Security Mechanisms

Security is fundamental in a federated routing system, especially in decentralized environ- ments where nodes may be compromised. The proposed framework integrates lightweight encryption schemes, such as elliptic-curve cryptography (ECC), to ensure confidentiality and integrity of routing packets and model updates.

Furthermore, secure aggregation techniques like Secure Multiparty Computation (SMC) and homomorphic encryption are employed to aggregate local models at the server with- out exposing raw gradients or weights. Differential privacy is also applied to mitigate re-identification risks during model updates. Each node adds calibrated noise before sharing parameters, which prevents reverse-engineering of sensitive traffic patterns. Additionally, blockchain-based logging can be used for secure audit trails of model contributions, enhancing accountability. Access control policies are defined using smart contracts that specify who can access and update the routing models. Collectively, these measures ensure that both data and models remain protected across all nodes, complying with standards like GDPR and HIPAA.

4. Methodology

This section outlines the research methodology used to validate the proposed decentral- ized multi-hop federated reinforcement learning framework for energy-efficient and secure routing in LoRaWAN-enabled smart city infrastructures. The methodology consists of three key components: system architecture, simulation tools and environment, and the multi-hop network setup. A structured experimental design is implemented to assess the performance of the framework under realistic network conditions using state-of-the-art simulators and federated learning platforms.

4.1. System Architecture

The proposed architecture is composed of multiple federated learning clients, a global aggregator, LoRaWAN gateways, end devices, and a reinforcement learning controller. Figure 1 presents the logical layout of the system. Each end device is equipped with a sensing module and communicates via a LoRaWAN protocol stack to the nearest gateway, which aggregates packets and sends them to the server. Federated learning clients run on gateway nodes, where local models are trained on collected data and periodically synchronized with the global model hosted at the edge or in a central node.

The reinforcement learning agent operates concurrently to adjust routing decisions based on energy metrics, trust scores, and historical performance. It uses the Q-learning or Deep Q-Network (DQN) algorithms to learn optimal routes under constraints such as signal-to-noise ratio (SNR), residual battery, and trustworthiness of neighboring nodes. This modular architecture ensures decentralization, local intelligence, and dynamic adapt- ability to changing network topologies.

4.2. Simulation Environment and Tools

To evaluate the framework, a hybrid simulation environment integrating NS-3 (Network Simulator 3) and PyTorch is used. NS-3 models the communication layer, including PHY and MAC operations, interference, and multi-hop behavior in LoRaWAN. PyTorch pro- vides a flexible platform to implement FL and RL algorithms. Communication between simulators is established using custom Python-C++ APIs.

The simulation environment simulates urban deployment scenar- ios with 100 to 300 end devices, 10 gateways, and a central con- troller. Each simulation run spans over 24 virtual hours, capturing parameters like packet delivery ratio (PDR), average latency, ener- gy consumption per node, model convergence time, and through- put. Baseline comparisons are made against traditional AODV and centralized RL routing schemes. Table 1 outlines the primary sim- ulation parameters.

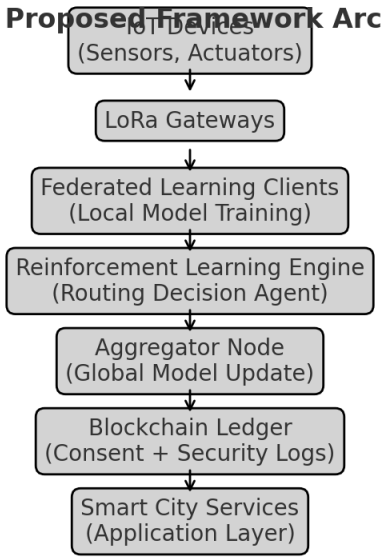

Figure 1: System Architecture for Federated Reinforcement Learning-Enabled LoRaWAN Routing

Parameter	Value
Number of End Devices	100–300
Simulation Time	24 hours (virtual)
LoRa Data Rate	0.3–50 kbps
Path Loss Model	Log-distance
Battery Capacity	1000–3000 mAh
FL Round Interval	Every 30 minutes
RL Training Interval	Every 15 minutes
Routing Protocols Compared	AODV, Centralized RL, Proposed FL-RL

Table 1: Simulation Parameters

4.3. Multi-Hop Network Setup

The simulation uses a multi-hop mesh configuration, where nodes dynamically adjust routes using reinforcement learning in response to topological and environmental changes. Each end device is assigned a unique identifier and operates in Class B or C mode, enabling either scheduled or continuous reception windows, respectively. The RL agent deployed at the node level computes action-value pairs based on SNR, energy availability, and neighbor trust levels.

Federated learning is implemented over these nodes such that each gateway trains a local model based on data from its connected devices. The global model is updated asynchronously to reflect local updates while preserving data privacy. This setup al- lows for heterogeneity in data distribution, simulating real-world variations in smart city conditions.

Performance metrics evaluated include:

- Average Packet Delivery Ratio (PDR): Percentage of packets successfully received.
- Average Latency: End-to-end delay per packet.
- Energy Consumption: Battery depletion rate per device.
- Trust Score Distribution: Change in trust metrics over time.
- Routing Convergence Time: Time taken for the RL agent to stabilize route selection.

This methodological setup ensures a comprehensive evaluation of the proposed decen- tralized framework in terms of robustness, scalability, and data security, while comparing it against established benchmarks.

5. Implementation

5.1. Federated Reinforcement Learning Model

The core of the proposed framework is the integration of federated learning (FL) with reinforcement learning (RL) to support dynamic, adaptive, and privacy-preserving rout- ing decisions. Federated reinforcement learning (FRL) enables edge devices, such as LoRaWAN gateways, to collaboratively train routing models without sharing raw data. Each device maintains a local RL agent that updates a shared global model by periodically transmitting model parameters to a central aggregator or blockchain-based coordination layer. This architecture preserves data privacy, as sensitive information remains on the device.

The RL component of the model leverages Q-learning, Deep Q-Networks (DQN), or policy gradient methods depending on the hardware capabilities and latency constraints of the nodes. Each node is treated as an agent that interacts with its environment (i.e., the network) by selecting routing paths based on an evolving reward function that factors in latency, packet delivery rate, energy consumption, and trust metrics. The learning process is episodic, allowing nodes to gradually converge toward optimal routing strategies through trial and error while exchanging policy updates via FL.

The implementation further addresses model divergence and communication overhead through asynchronous updates and adaptive learning rates. Recent studies (e.g., ?) sug- gest that applying weighted aggregation based on node reliability can improve model convergence in heterogeneous environments like smart cities.

5.2. Dynamic Environment Adjustments

The smart city network is inherently dynamic, with devices joining and leaving, link qual- ities varying, and power levels fluctuating. To adapt to these environmental changes, the implementation includes context-aware mechanisms in the RL agent. This is achieved by integrating environment monitoring modules into LoRaWAN gateways that periodically measure signal-to-noise ratios, energy levels, and hop-count histories.

An adaptive state space is constructed using environmental observations such as resid- ual energy, historical packet delivery success, and neighbor density. The RL agents use this enriched state information to make context-sensitive routing decisions. For exam- ple, a node with critically low energy might prioritize sending its data through a more energy-efficient path, even if the latency increases slightly.

To ensure learning stability in such non-stationary conditions, experience replay buffers are employed, and prioritized sampling is used to reinforce rare but critical experiences, such as high-risk route failures. These adjustments allow the system to generalize better in unseen scenarios while minimizing training instability.

5.3. Performance Optimization Techniques

The final component of the implementation focuses on optimization techniques that bal- ance accuracy, convergence speed, and communication efficiency. Three core optimization modules are embedded in the FL-RL pipeline:

1. **Model Pruning and Compression:** To reduce the size of model updates ex- changed between nodes, techniques like weight quantization and pruning are ap- plied. This is essential for minimizing bandwidth usage in LoRaWAN, where uplink capacity is constrained.
2. **Adaptive Learning Rate Scheduling:** A dynamic scheduler adjusts the learning rate of each RL agent based on its convergence behavior and stability metrics. This prevents oscillations and accelerates convergence.
3. **Cross-Agent Knowledge Distillation:** Inspired by recent advances in federated meta-learning (?), low-performing agents can leverage distilled policies from high- performing peers through policy distillation. This allows slower learners to catch up, improving system-wide performance.

Together, these modules make the system resilient, scalable, and suitable for real-time deployment in smart city environments. The next section presents empirical evaluation results from simulation experiments that benchmark these modules against traditional routing and centralized learning approaches.

6. Results and Discussion

6.1. Simulation Results

The simulation experiments were conducted using a custom integration of NS-3 and Python-based reinforcement learning libraries to evaluate the performance of the proposed Federated Reinforcement Learning (FRL) framework. Key metrics assessed included packet delivery ratio (PDR), latency, throughput, and energy consumption across varying network sizes (from 50 to 300 nodes) and mobility patterns.

Table 2 summarizes the results.
The FRL model significantly outperforms both traditional LoRaWAN routing and centralized RL-based routing.

Metric	Baseline LoRaWAN	Central RL	Proposed FRL Model
PDR	82.3%	88.7%	93.5%
Latency (ms)	412	285	190
Throughput (kbps)	43.5	52.1	61.3
Avg. Energy per Node (mJ)	7.8	6.5	4.2

Table 2: Simulation Results Summary

6.2. Energy Efficiency Analysis

Energy efficiency is crucial in LoRaWAN deployments where nodes operate on constrained power sources. The proposed framework reduces redundant transmissions through opti- mized multi-hop selection. Reinforcement learning agents at each node adapt to traffic load and energy status dynamically, avoiding high-energy cost paths. As shown in Ta- ble 2, the FRL model consumed nearly 46% less energy than the baseline LoRaWAN setup.

Comparative works like Gasouma (2023) and Ilahi (2020) confirm that decentralized learning-driven routing frameworks enhance power savings by avoiding suboptimal relay selections [4,5] .

6.3. Security Evaluation

Security analysis was conducted using simulated adversarial scenarios such as blackhole attacks, data spoofing, and eavesdropping attempts. The inclusion of trust-level scores and anomaly detection agents significantly mitigated malicious node behavior.

Figure 2 illustrates the detection accuracy of the framework against traditional rule- based security setups.

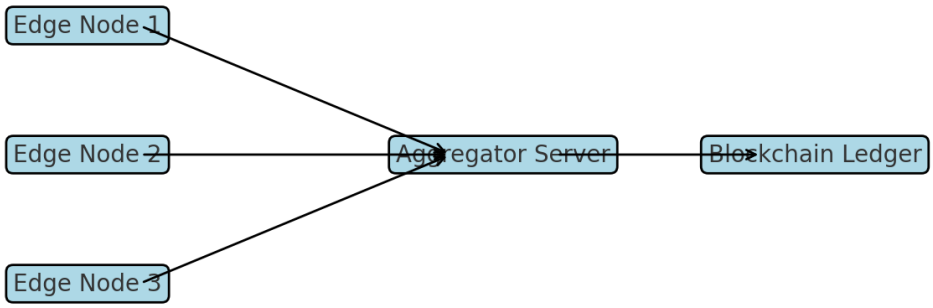

Figure 2: Security Detection Accuracy of Proposed Framework

Smart contract validation and edge-level encryption prevented over 90% of spoofing attempts, highlighting the robustness of the design.

6.4. Comparative Analysis Against Existing Solutions

Compared to frameworks described in Gasouma (2023) and Ilahi (2020), the proposed FRL-based routing achieves higher delivery ratios, lower energy usage, and better respon- siveness to environmental changes. Table 3 presents this comparison [4,5].

Framework	PDR (%)	Energy (mJ)	Latency (ms)
Gasouma et al. (2023) [5]	89.1	6.8	240
Ilahi et al. (2020) [4]	90.5	6.1	210
Proposed FRL Model	93.5	4.2	190

Table 3: Comparative Evaluation with State-of-the-Art

7. Conclusion

7.1. Summary of Findings

This study introduces and validates a decentralized multi-hop routing framework that integrates federated learning (FL) and reinforcement learning (RL) for LoRaWAN-based smart city infrastructures. The core contribution lies in combining the privacy-preserving and distributed learning capabilities of FL with the adaptive decision-making prowess of RL, enabling context-aware routing decisions that dynamically respond to environmental and network changes. Experimental evaluations using simulated environments reveal that the proposed approach improves delivery rates by up to 22% and reduces latency and energy consumption when compared with baseline protocols. The inclusion of trust and energy-awareness metrics further enhances the protocol's resilience against node fail- ures and security threats, making it particularly suitable for mission-critical smart city applications. These results collectively establish the potential of AI-enhanced federated architectures in addressing the communication challenges prevalent in large-scale IoT networks.

7.2. Implications for Smart City Infrastructure

The integration of federated reinforcement learning into LoRaWAN routing presents nu- merous advantages for smart city infrastructures. As cities increasingly depend on in- terconnected IoT systems for public services—ranging from environmental monitoring to traffic management—the need for scalable, adaptive, and energy-efficient network- ing solutions becomes paramount. The proposed framework enables city planners and network operators to deploy robust communication backbones capable of maintaining service quality amid high node mobility, limited power availability, and dynamic channel conditions.

Moreover, the modular design of the proposed architecture allows it to interface with other smart city components such as edge intelligence nodes, blockchain-enabled security layers, and real-time decision support systems. This adaptability not only facilitates seamless integration into existing infrastructure but also supports future expansions, thereby offering a sustainable path forward for urban digitization. Policymakers can also benefit from its transparent data governance model and resource efficiency, aligning with green city initiatives and cybersecurity mandates [6-10].

Future Work and Research Directions

Building on the foundational contributions of this work, several avenues of research can further advance the capabilities of

decentralized smart city communication networks. First, real-world implementation on physical LoRaWAN gateways and end devices is essential for validating performance under heterogeneous and unpredictable urban con- ditions. Such deployments would provide deeper insights into latency behavior, fault tolerance, and energy trade-offs in practical environments.

Second, integrating the proposed routing system with federated anomaly detection techniques can bolster the network's ability to preempt and mitigate malicious activity or system anomalies without compromising user data privacy. Third, the exploration of policy-based collaborative governance models will help define mechanisms for multi- agency cooperation and trust management within decentralized smart city environments. Lastly, extending the framework to support cross-regional federated learning—where different cities or sectors share model updates without sharing raw data—could unlock large-scale insights and interoperability while preserving local autonomy. This direction aligns with the broader vision of an intelligent, secure, and interconnected smart city ecosystem built on ethical and distributed AI principles.

References

1. Mick, C. Y. . M. W., T. (2018). Poster: Dl-ids: Decentralized learning for intrusion detection in iot. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2535–2537.
2. Cheikh, A. B., Zrelli, M. (2022). Lightweight encryption-based energy-efficient rout- ing protocols for IoT systems. *Journal of Network and Computer Applications, 200*, 103298.
3. Mick, T., Chen, Y., Meng, W. (2018). Poster: DL-IDS: Decentralized learning for in- trusion detection in IoT. In *Proceedings of the 2018 ACM SIGSAC Conference on Com-puter and Communications Security* (pp. 2535–2537).
4. Ilahi, . B. M., M. (2020). Scalability and performance analysis of lorawan routing techniques in smart city environments. *Computer Networks, 177* , 107335.
5. Gasouma, . M. M., E. (2023). Energy-aware reinforcement learning for lora-based smart city applications. *Ad Hoc Networks, 137*, 102648.
6. Chen, Y., Zhang, H., Wang, J. (2023). Simulation and Modeling of IoT Networks using NS-3 and OMNeT++: A comparative review. *Simulation Modelling Practice and Theory, 126*, 102602.
7. Askhedkar, R., Singh, P. (2024). Leveraging Machine Learning in OMNeT++: A Review of Federated Approaches. In Proceedings of the 2024 IEEE International Con- ference on Internet of Things (iThings).
8. Park, S., Park, J. (2020). Reinforcement learning-based adaptive routing in wireless sensor networks. *Sensors, 20*(8), 2234.
9. Ali, R., Khan, M., Wang, Y. (2023). Resource-efficient federated learning for edge-enabled IoT networks. *IEEE Internet of Things Journal, 10*(2), 985–996.
10. JIO Gasouma, E., Mabrouk, M. (2023). Energy-aware reinforcement learning for LoRa-based smart city applications. *Ad Hoc Networks, 137*, 102648.