MSTS Methods in Science and Technology Studies

futuristech PT. Teknologi Futuristik Indonesia

Received: June 17, 2026; Revised: August 25, 2026; Accepted: August 28, 2026; Published: August 30, 2026; Current version: August 30, 2026. e-ISSN: 3123-4232
Digital Object Identifier 10.64539/msts.v2i2.2026.551

Article

Compliance-Aware AI Framework for Anti-Interference and Adaptive Routing in Telecommunication Networks

Godfrey Wandwi[1,*], Dennis Numi Madaha[2]

[1] School of Digital Technologies and Transformation Studies, Dar es Salaam Tumaini University, P.O. BOX 77588 Dar es Salaam, Tanzania; e-mail: godfrey.wandwi@dartu.ac.tz (G. Wandwi).
[2] Department of Computer Studies, Dar es Salaam Institute of Technology, P.O. Box 2958, Dar es Salaam, Tanzania; e-mail: dennisnumi@gmail.com (D. N. Madaha).
* Correspondence Author

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Abstract: The rapid evolution of heterogeneous telecommunication networks has increased the difficulty of maintaining communication performance while operating within spectrum and transmission constraints. Existing network optimization approaches primarily focus on throughput, routing, and interference mitigation, whereas regulatory compliance is commonly treated as a separate post-processing activity. This separation limits the ability of network-control mechanisms to respond proactively to compliance risks. This study develops a Compliance-Aware AI Framework (CA-AIF) that integrates Coalition Formation Games (CFG), variance-aware DUCBQ adaptive routing, and Proximal Policy Optimization (PPO) with a policy-constrained compliance monitoring layer. The framework represents compliance risk through telemetry-derived violation indicators associated with spectrum occupancy, transmission power, and interference conditions and incorporates these indicators into network decision-making. A controlled simulation environment is developed using synthetically generated mobility, interference, channel, and spectrum-occupancy data. The proposed framework is evaluated against Q-learning, Dyna-Q, UCBQ, and DUCBQ using throughput, packet acceptance, routing stability, convergence, compliance violation rate, and computational cost. Across repeated simulations, the proposed framework achieves higher throughput and packet acceptance while reducing compliance violations relative to the evaluated baselines. The results demonstrate that incorporating compliance risk into network optimization can improve the stability of communication decisions without treating compliance as an independent post-processing task. The study contributes a reproducible simulation-based framework for compliance-aware intelligent networking and provides a basis for future validation using operational spectrum-monitoring and regulatory datasets.

Keywords: Artificial Intelligence; Compliance-Aware Networking; Regulatory Compliance; Telecommunication Networks; Reinforcement Learning; Adaptive Routing; Spectrum Management; Interference Mitigation.

1. Introduction

Modern telecommunication networks increasingly integrate heterogeneous access technologies with edge computing, IoT connectivity, satellite-terrestrial networks, and software-defined networking [1]. This heterogeneity increases the difficulty of maintaining efficient communication while respecting spectrum, transmission-power, interference, and service-specific regulatory constraints. Spectrum monitoring is itself moving toward distributed, data-driven and AI-assisted architectures, creating opportunities for automated identification of interference and unauthorized spectrum use [2].

Conventional compliance processes, however, generally remain separated from network-control mechanisms. Periodic audits and threshold-based inspection can identify violations, but they do not necessarily influence routing, resource allocation, or interference-management decisions while those decisions are being

made. This separation is problematic in dynamic wireless environments, where an action that improves throughput may simultaneously increase interference or exceed a predefined operating constraint [3].

Developing telecommunication environments introduce additional operational constraints, including heterogeneous infrastructure, limited monitoring resources, inconsistent availability of labelled network data, and evolving spectrum-management practices. These conditions motivate architectures that can operate using network telemetry and explicit regulatory constraints without assuming the availability of large, language-specific training corpora. Although multilingual regulatory-document processing is a future extension, it is outside the experimental scope of the present study [4].

Recent advancements in infocommunication research have explored the integration of AI with network security, spectrum management, and service quality monitoring. However, most existing studies focus narrowly on performance optimization or anomaly detection without explicitly addressing regulatory compliance as a unified computational objective. This gap becomes critical in modern telecommunication ecosystems where compliance is intertwined with network performance, user behavior analytics, and service orchestration layers. Furthermore, the lack of scalable architectures capable of operating across heterogeneous infrastructures limits the practical deployment of existing solutions.

Despite the growing body of research on AI-enabled network management, a fundamental problem remains insufficiently addressed: current telecommunication monitoring systems are designed either to optimize network performance or to enforce regulatory policies, but rarely both within a unified operational framework. As telecommunication infrastructures evolve toward highly dynamic and heterogeneous ecosystems involving mobile networks, IoT platforms, satellite communications, and digital broadcasting services, regulatory violations increasingly emerge as side effects of autonomous network optimization processes. Existing compliance mechanisms generally operate as external auditing functions that detect violations after they occur rather than proactively preventing them during network operation. Consequently, regulators and service providers face a critical challenge: how to continuously monitor, predict, and mitigate compliance violations while simultaneously maintaining communication efficiency in real time. This unresolved challenge constitutes the primary research problem addressed in this study. In this study, the research problem is formulated as follows: given a heterogeneous wireless network with dynamic interference and time-varying spectrum conditions, how can network-control decisions be optimized jointly for communication performance and compliance risk when compliance evidence is derived from network telemetry? The problem is therefore not to provide legal certification of network operation, but to develop a computational mechanism that detects predefined compliance-risk conditions and incorporates them into adaptive network optimization.

The study evaluates three principal hypotheses. H1: incorporating compliance-risk information into network optimization improves compliance outcomes relative to performance-only learning. H2: combining cooperative resource organization, adaptive routing, and PPO improves communication performance and routing stability relative to individual learning baselines. H3: the compliance-monitoring signal provides additional benefit beyond a fixed reward penalty when evaluated under the same network conditions. These hypotheses are evaluated through baseline comparison, component ablation, and the proposed penalty-only control experiment. Figure 1 shows the workflow progresses from problem identification and research-gap analysis to CA-AIF design, compliance-risk formulation, algorithm development, simulation-data generation, baseline comparison, statistical validation, and component-level ablation. The workflow distinguishes framework development from experimental validation and highlights the iterative feedback between algorithm design and performance evaluation.

The purpose of this research is to develop and evaluate a CA-AIF in which regulatory-risk information is incorporated into adaptive interference management and routing decisions. The framework combines CFG for cooperative resource organization, variance-aware DUCBQ for adaptive routing, and PPO for global policy optimization. A separate compliance-monitoring layer derives a bounded violation-risk signal from simulated network telemetry and feeds that signal into the learning process. The resulting architecture is evaluated through controlled simulation rather than operational regulatory deployment.

To address these challenges, this study proposes an Artificial Intelligence Driven Regulatory Compliance Monitoring framework designed specifically for converged telecommunication and infocommunication environments. The proposed approach integrates telemetry-based compliance-risk estimation with predefined technical constraints to support continuous compliance-risk evaluation within the simulated network-control loop. Unlike conventional monitoring systems, the framework is designed to operate under low-resource conditions typical of developing nations while providing a basis for future extension to multilingual and multi-service environments.

The contributions of this study are:

- A unified compliance-aware network-control architecture: The study integrates CFG, DUCBQ, PPO, and a telemetry-based compliance-risk layer within a single network optimization framework.

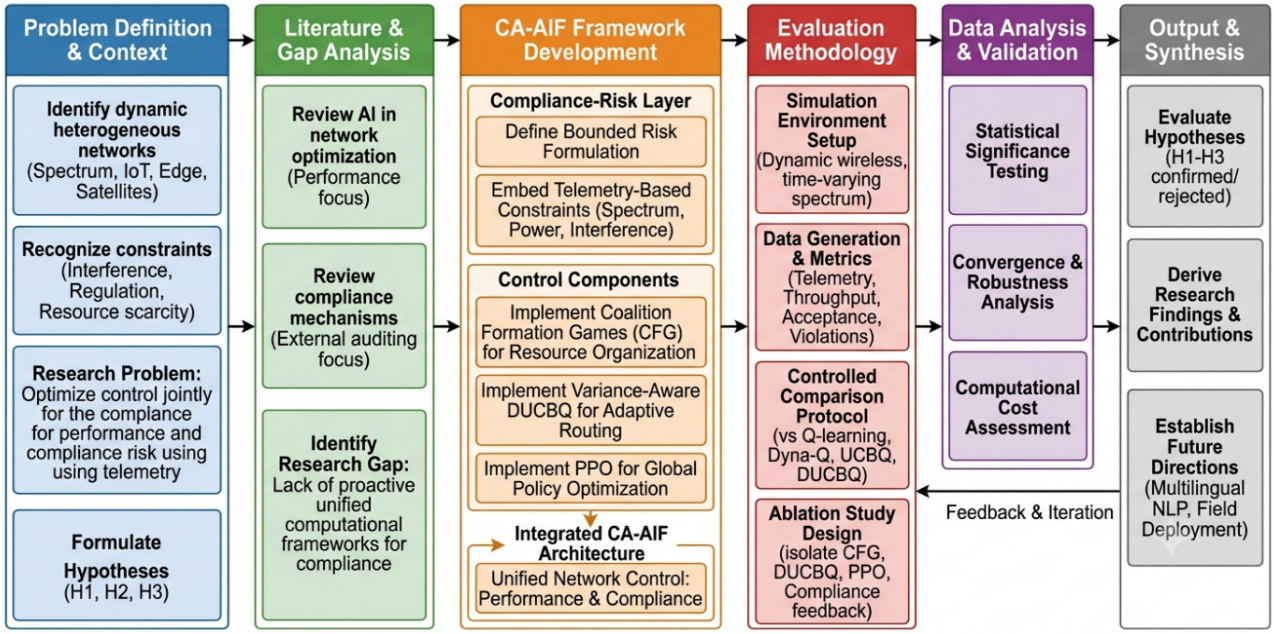

Figure 1. Research-stage workflow of the study.

- A reproducible compliance-risk formulation: Regulatory risk is represented using explicitly defined spectrum, transmission-power, and interference constraints, allowing compliance-related variables to be calculated from simulated network observations.
- A compliance-aware learning mechanism: Compliance-risk information is incorporated into the reward function and decision process so that network-control actions account for both communication performance and predefined regulatory constraints.
- A comprehensive simulation and comparison protocol: The framework is evaluated against Q-learning, Dyna-Q, UCBQ, and DUCBQ using throughput, packet acceptance, routing stability, convergence, compliance violation rate, and computational cost.
- A component-level validation strategy: Ablation experiments are used to determine the separate contributions of compliance feedback, CFG, DUCBQ, and PPO rather than attributing all performance improvements to the complete architecture.

The present work focuses on compliance-aware wireless network optimization under predefined technical constraints. It evaluates spectrum/interference-related compliance risk, adaptive routing, cooperative resource organization, and reinforcement-learning-based control in a simulation environment. It does not implement legal reasoning, automated interpretation of national legislation, multilingual regulatory-document processing, lawful-interception compliance, operational regulator databases, or field deployment in a live telecommunications network.

The remainder of the paper is organized as follows. Section 2 reviews related work and identifies the research gap. Section 3 presents the proposed CA-AIF architecture, including the compliance-monitoring layer, CFG, DUCBQ routing, and PPO optimization. Section 4 describes the simulation environment, dataset-generation procedure, evaluation metrics, comparison protocol, statistical validation, and ablation analysis. Section 5 discusses the principal findings, limitations, and future research directions, while Section 6 concludes the study.

2. Related Work

The problem of regulatory compliance in telecommunication systems has traditionally been studied within the boundaries of spectrum governance, policy enforcement, and network auditing frameworks. Early works focused on rule-based monitoring systems that relied on predefined regulatory templates to evaluate operator behavior against licensing conditions and spectrum allocation policies. For instance, ITU-based compliance architectures introduced structured reporting mechanisms for spectrum usage and interconnection control, enabling regulators to manually verify adherence to operational standards across national networks [5]. However, such approaches were largely static, and their effectiveness diminished significantly in dynamic infocommunication environments where traffic patterns, service types, and user behaviors change continuously across heterogeneous infrastructures.

In response to these limitations, researchers have explored automated network monitoring systems that integrate statistical analysis and anomaly detection tech-

niques. Anomaly detection and regulatory-violation detection are treated as distinct functions in CA-AIF. An anomaly represents a statistically unusual network observation, whereas a regulatory violation represents an observation that exceeds an explicitly defined technical constraint [6]. In the present study, the reported compliance metrics are based on constraint violations rather than generic statistical anomalies. This distinction prevents an unusual but permissible network state from being automatically classified as a regulatory violation. Cifuentes *et al*. (2025) [7] proposed a spectrum auditing framework that uses probabilistic traffic modeling to detect unauthorized frequency usage in cellular networks, demonstrating improved detection accuracy compared to conventional threshold-based systems. Similarly, Ünal *et al*. (2019) discussed a policy verification engine for mobile networks that maps regulatory constraints into formal logic rules, allowing automated compliance verification across LTE and 5G environments [8]. Although these approaches improve automation, they still depend heavily on predefined rule structures, limiting adaptability in evolving regulatory landscapes and multi-service infocommunication systems.

With the rapid expansion of Internet of Things (IoT) ecosystems and cloud-based telecommunication services, compliance monitoring has increasingly shifted toward data-driven frameworks [9]. IoT-driven regulatory systems have been proposed to monitor device-level compliance in smart city infrastructures, particularly focusing on energy usage, spectrum sharing, and data privacy enforcement. Atamewan (2024) [10] introduced an IoT compliance monitoring model that leverages distributed sensor networks to detect violations in real time, improving response time compared to centralized auditing systems. However, these systems often struggle with scalability when deployed across large-scale mobile and satellite networks, where data heterogeneity and transmission delays significantly affect monitoring accuracy.

In parallel, machine learning techniques have been introduced to enhance predictive compliance monitoring. Support vector machines, random forests, and clustering-based models have been applied to detect abnormal network behavior indicative of regulatory violations. For example, Arianti *et al*. (2025) [11] reviewed a supervised learning framework for detecting spectrum misuse in cognitive radio networks, achieving improved classification accuracy under controlled simulation conditions. Nevertheless, such supervised approaches require large labeled datasets, which are often unavailable in real telecommunication regulatory environments, particularly in developing regions where data governance frameworks are still evolving.

Artificial intelligence provides an opportunity to connect network telemetry, anomaly or risk detection, and adaptive network control [12]. Machine-learning models can identify abnormal spectrum or traffic patterns, while reinforcement-learning agents can adapt routing and transmission decisions to changing network states. However, the use of AI does not by itself establish regulatory compliance. A compliance-aware architecture must explicitly define the regulatory variables being monitored, identify the evidence used to calculate compliance risk, and specify how that risk affects network decisions. Yagual *et al*. (2025) [13] work similarly emphasizes continuous monitoring of AI/ML behaviour, input data, model performance, drift, resource utilization, and feedback loops in future networks.

Reinforcement learning (RL) has also been explored as a dynamic decision-making framework for adaptive network management and policy enforcement. RL-based systems enable agents to learn optimal actions through interaction with network environments, making them suitable for real-time compliance monitoring. For instance, Ukpong *et al*. (2025) [14] proposed a deep reinforcement learning model for adaptive spectrum allocation that maximizes utilization while minimizing interference violations in cognitive radio networks. Similarly, Saidane *et al*. (2026) [15] proposed a multi-agent RL framework for distributed network security management, showing improved adaptability in heterogeneous network conditions. However, most RL-based approaches focus on performance optimization rather than explicit regulatory compliance interpretation, limiting their direct applicability to governance systems.

More recent studies have begun integrating hybrid AI architectures that combine rule-based systems with machine learning models to improve robustness. Hybrid compliance frameworks attempt to bridge the gap between deterministic regulatory logic and probabilistic network behavior analysis. For example, Nabil *et al*. (2025) [16] introduced a hybrid monitoring system that combines expert-defined compliance rules with anomaly detection algorithms to improve accuracy in identifying policy violations in mobile broadband networks. Although promising, these hybrid models still rely heavily on static regulatory definitions and do not fully capture the dynamic nature of modern infocommunication ecosystems.

In the context of developing countries, regulatory compliance monitoring faces additional constraints related to infrastructure limitations, multilingual communication, and fragmented regulatory frameworks. Studies focusing on African and Asian telecommunication systems highlight the difficulty of implementing standardized compliance monitoring due to inconsistent data availability and diverse service architectures. For instance, Muringani *et al*. (2024) [17] examined regulatory enforcement challenges in Sub-Saharan mobile networks, emphasizing the lack of real-time monitoring tools and the prevalence of manual inspection processes. Similarly,

Ha and Chuah (2023) [18] explored compliance issues in South Asian telecommunication markets, noting that multilingual service environments complicate automated policy interpretation and enforcement.

Recent advancements in natural language processing (NLP) have been applied to regulatory document analysis and policy interpretation within telecommunication systems. Transformer-based language models have been used to extract compliance rules from regulatory texts and map them to network control parameters. However, these models are primarily trained on high-resource languages and fail to generalize effectively to low-resource linguistic contexts commonly found in developing regions. This creates a significant gap in applying AI-driven compliance monitoring across multilingual infocommunication ecosystems.

Recent standardization activity also reinforces the distinction between AI-enabled monitoring and automated regulatory decision-making [19]. ITU-T Q.4081 defines monitoring of AI/ML systems in future networks as continuous observation of operational performance and includes monitoring of input data, model performance, model drift, resource utilization, and feedback loops. Similarly, ITU-R SM.2542 describes next-generation spectrum monitoring as increasingly proactive, autonomous, distributed, and data-driven, with AI and big-data techniques supporting signal detection, classification, interference identification, and spectrum awareness [20]. These developments support the use of telemetry-driven compliance-risk monitoring in the proposed framework but do not imply that an AI model independently determines legal compliance.

Recent developments further indicate that AI-assisted spectrum monitoring is moving toward proactive and distributed monitoring architectures rather than purely reactive inspection. ITU-R Report SM.2542 specifically discusses AI, big-data processing, distributed spectrum monitoring, heterogeneous monitoring equipment, and real-time spectrum awareness [20]. In parallel, research on autonomous network management and automated spectrum sharing emphasizes the need to coordinate technical network decisions with evolving spectrum-management requirements [21]. These developments support the motivation for compliance-aware network optimization but do not by themselves establish the specific joint CFG–DUCBQ–PPO architecture investigated in this study.

The distinction between the present study and existing approaches is therefore threefold. First, the proposed framework does not treat compliance assessment as an independent post-processing task; a telemetry-derived compliance-risk signal is incorporated into network-control decisions. Second, the framework jointly considers cooperative interference management, adaptive routing, and policy-constrained reinforcement learning rather than optimizing a single networking objective. Third, the experimental design explicitly evaluates compliance-related outcomes alongside communication-performance measures. The framework is consequently positioned as a compliance-aware network optimization system, rather than as a complete regulatory information system or automated legal-compliance authority.

Although previous studies have investigated anomaly detection, spectrum management, policy verification, and reinforcement learning for network optimization, three limitations remain relevant to the present problem [22]. First, compliance is frequently represented as an external verification task rather than a variable that directly influences network-control decisions. Second, performance-oriented learning models generally do not provide an explicit mechanism for calculating and feeding regulatory-risk information into routing and transmission policies. Third, many proposed approaches are evaluated using isolated performance metrics and therefore provide limited evidence regarding the trade-off between communication efficiency and compliance risk.

These limitations directly motivated the design of the proposed framework. The coalition formation component was introduced to manage interference and resource allocation in dense heterogeneous environments. The DUCBQ learning module was incorporated to improve routing stability under dynamic interference conditions while reducing the exploration instability commonly observed in conventional reinforcement learning approaches. The PPO optimization layer was selected because of its ability to provide stable policy convergence in continuous action spaces frequently encountered in spectrum allocation and transmission control problems. Most importantly, regulatory compliance signals were embedded directly into the reward structure of all learning components, enabling compliance considerations to influence network decisions proactively rather than retrospectively.

The novelty of the proposed framework lies not merely in combining multiple machine learning techniques but in establishing a compliance-native learning architecture where regulatory requirements actively shape optimization behavior throughout the communication lifecycle. This distinguishes the proposed approach from conventional AI-based networking solutions that primarily focus on performance optimization without explicitly incorporating regulatory-constraint information into their decision-making processes.

Therefore, there remains a critical need for an Artificial Intelligence Driven Regulatory Compliance Monitoring framework that integrates real-time network analytics, telemetry-based compliance-risk estimation, and policy-constrained optimization within a unified infocommunication architecture. Such a framework must be capable of operating in heterogeneous, multilingual, and resource-

constrained environments typical of developing nations while maintaining scalability across modern telecommunication infrastructures.

3. Proposed Compliance-Aware AI Framework

The proposed CA-AIF consists of four functional layers: (1) telemetry acquisition, (2) compliance-risk estimation, (3) adaptive network control, and (4) performance and compliance evaluation. The telemetry layer collects simulated observations of spectrum occupancy, transmission power, interference intensity, channel conditions, mobility, routing state, and traffic performance. The compliance-risk layer compares these observations with predefined regulatory constraints and produces a normalized compliance-risk variable. The adaptive-control layer contains three complementary learning components: CFG for cooperative resource organization, variance-aware DUCBQ for local adaptive routing, and PPO for global policy optimization. The evaluation layer calculates communication and compliance metrics from the resulting network trajectories [23].

The functional relationship among these components is as follows. Telemetry → compliance-risk estimation → compliance-aware reward/state construction → CFG/DUCBQ/PPO decisions → network response → updated telemetry. CFG operates primarily at the cooperative resource-organization level, DUCBQ operates at the adaptive routing level, and PPO operates at the global policy-optimization level. The compliance-monitoring layer does not independently make legal determinations; instead, it generates a quantitative risk signal from explicitly defined simulation constraints. Regulatory back-off is implemented as a control response when the estimated risk exceeds a predefined intervention threshold.

This architecture distinguishes between monitoring, risk estimation, and network optimization. Monitoring produces observations; risk estimation converts observations into compliance indicators; and the learning components use those indicators when selecting network actions. This separation is essential for reproducibility because it allows the contribution of compliance monitoring to be evaluated independently from the effect of reward-based optimization.

3.1. Compliance-Monitoring and Risk-Scoring Framework.

The compliance-monitoring subsystem operates on network telemetry generated at each simulation time step. For each transmitting node i, the monitored variables include transmission power P_i, occupied frequency f_i, measured interference I_i, channel occupancy O_i, and routing state H_i. The applicable simulation constraints are represented by the maximum transmission power P_{max}, permitted frequency set $F_{re}g$, maximum interference threshold I_{max}, and maximum permitted occupancy O_{max}.

For node i at simulation time t, a binary violation indicator is defined as:

$$Z_{i,t} = \mathbb{1}(P_{i,t} > P_{max}) + \mathbb{1}(f_{i,t} \notin F_{re}g) + \mathbb{1}(I_{i,t} > I_{max}) + \mathbb{1}(O_{i,t} > O_{max}) \quad (1)$$

where $\mathbb{1}(\cdot)$ is an indicator function that takes the value 1 when the specified condition is satisfied and 0 otherwise. Thus, $z_{i,t}$ represents the number of explicitly defined technical constraints violated by node i at time t. To obtain a bounded compliance-risk score, the individual constraint violations are normalized and weighted. The node-level regulatory compliance-risk score is defined as:

$$V_{i,t}^{reg} = \sum_{m=1}^{M} w_m \, v_{i,t}^{(m)} \quad (2)$$

where:

$$\sum_{m=1}^{M} w_m = 1, \qquad w_m \geq 0$$

and

$$v_{i,t}^{(m)} \in [0, 1]$$

represents the normalized severity of the m-th regulatory constraint, while w_m represents its corresponding predefined weight. Consequently, $V_{i,t}^{reg}$ is bounded within the interval [0, 1].

The network-level compliance-risk signal at simulation time t is obtained by averaging the node-level risk scores across all N_t transmitting nodes:

$$V_t^{reg} = \frac{1}{N_t} \sum_{i=1}^{N_t} V_{i,t}^{reg} \quad (3)$$

A compliance violation is recorded whenever at least one explicitly defined constraint is exceeded. Equivalently, a violation is present when: $z_{i,t} > 0$.

The threshold τ used in the intervention mechanism is selected as part of the simulation design before testing and is not tuned or recalibrated using test-set results. This separation ensures that the compliance-monitoring procedure remains reproducible and prevents post hoc threshold selection from influencing the reported test performance.

Importantly, V_t^{reg} should not be interpreted as a legally valid probability of non-compliance. Instead, it is a simulation-derived compliance-risk score calculated from predefined technical constraints and their associated normalized violation severities. The score provides an operational measure of the extent to which simulated network behavior departs from the specified technical requirements.

Accordingly, the measure should not be presented as an operational regulatory-compliance probability without external validation. Validation against national licensing databases, regulator inspection records, or operational spectrum-monitoring data would be required before V_t^{reg} could reasonably be interpreted as an indicator of real-world regulatory non-compliance probability. Within the present simulation framework, its appropriate interpretation is therefore limited to a reproducible, bounded measure of technical compliance risk derived from predefined simulation constraints.

3.1. Anti-interference learning model under compliance-constrained communication environments

A multi-actor wireless environment in developing telecommunication systems can be abstracted as a constrained coalition system where users, base stations, and regulatory monitoring agents embedded within base station coexist. CFG are used to model how communication nodes form cooperative clusters under interference pressure while respecting compliance constraints such as spectrum masks and emission limits.

Let the utility of a network participant *i*under coalition configuration be expressed as:

$$U_i(C_i, C_{-i}) = R_i(C_i, C_{-i}) - \lambda_{re} g\, V_i^{reg} \tag{4}$$

where represents the communication utility and represents the compliance-risk score. A coalition configuration is considered stable with respect to unilateral deviations when:

$$U_i(C_i, C_{-i}) \geq U_i(C_i, C_{-i}^*), \qquad \forall i, \forall C_i \tag{5}$$

In Equation 4, U_i represents a hybrid utility combining throughput gain and compliance penalty. Unlike classical CFG models, the utility here introduces a regulatory penalty term λC_i, where $C_i$captures violation probability detected by regulatory monitoring agents embedded within base station. This subtle addition changes equilibrium behavior significantly in low-governance environments, where compliance uncertainty is high.

In practical deployments across developing nations' metropolitan clusters, such as mixed 4G/5G LTE deployments in East African urban corridors, coalition formation is influenced by unstable interference patterns caused by dense unlicensed spectrum usage and irregular enforcement of spectrum allocation policies.

The reinforcement learning-based state-value representation is defined as:

$$\begin{aligned} v_\pi(s) = \mathbb{E}\left[\sum_{\tau=0}^{\infty} \gamma^\tau r_{t+\tau} | s_t = s\right], Q_\pi(s,a) \\ = \mathbb{E}\left[\sum_{\tau=0}^{\infty} \gamma^\tau r_{t+\tau} | s_t = s, a_t = a\right] \end{aligned} \tag{6}$$

Here, the reward function is not purely communication-driven. It is decomposed as:

$$r_t = R_t^{throughput} - \beta_1 I_t - \beta_2 V_t^{reg} \tag{7}$$

where I_t is interference intensity and V_t^{reg} is regulatory violation risk estimated by a compliance monitoring subsystem.

This coupling is essential in AI-driven compliance architectures because interference mitigation decisions (like power boosting or channel switching) may violate emission thresholds if not continuously evaluated.

3.2. Machine learning-based coalition optimization with compliance feedback

The coalition grouping of users is defined as:

$$C_{on} = \{u_{n1}, u_{n2}, \ldots, u_{ni}\} \tag{8}$$

Each coalition is not static; it evolves under reinforcement signals and compliance constraints emitted by compliance-monitoring modules embedded within base stations.

The transmission rate under interference-aware adaptation is expressed as:

$$R_i = B \log_2\left(1 + \frac{P_i |h_i|^2}{N_0 B + I_i + P_j \left|h_{j,i}\right|^2}\right) \tag{9}$$

Then define the utility as:

$$U_i = R_i - \lambda_{re} g\, V_i^{reg} \tag{10}$$

where P_i is the transmit power, h_i is the desired channel coefficient, P_j and $h_{j,i}$ represent the interference-source power and channel gain, respectively, I_i represents aggregate interference.

Interference aggregation is modeled as:

$$I = \sum_{i \neq j} P \mid h_{i,j} \mid^2 \tag{11}$$

The system-level optimization objective becomes:

$$\max R_{sum} = \sum_{n=1}^{N} R(C_{on}) - \lambda \sum_{n=1}^{N} V_{reg}(C_{on}) \tag{12}$$

This transforms the classical anti-interference problem into a constrained optimization problem where regulatory compliance is embedded as a penalty surface shaping the learning trajectory.

A modified Pareto-based coalition acceptance rule is introduced:

$$\begin{aligned} C_{on} \succ_i C'_{on} \Leftrightarrow R(C_{on} \cup u_i) + R(C_{on} \setminus u_i) \\ > R(C'_{on}) - \Omega_{reg} \end{aligned} \tag{13}$$

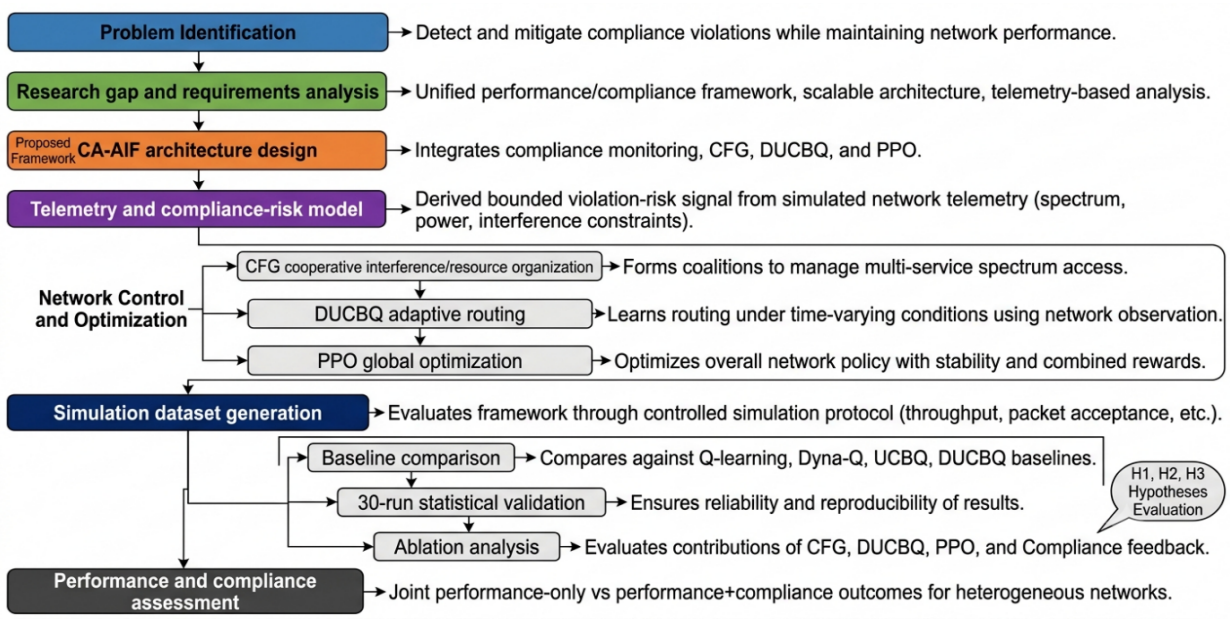

Figure 2. Research workflow and architecture of the proposed CA-AIF.

Here, Ω_{reg} is a compliance margin dynamically updated by AI monitoring agents depending on regional enforcement strictness. This is particularly relevant in multi-jurisdictional telecom environments where regulatory interpretation differs across borders.

3.3. Deep reinforcement learning integration (PPO-based compliance-aware anti-interference control)

The policy optimization mechanism is constructed using PPO, chosen due to its stability in continuous spectrum decision spaces. However, unlike standard PPO, the reward shaping integrates compliance verification feedback. Figure 2 summarizes the research workflow from problem formulation and framework design through algorithm development, simulation-data generation, baseline comparison, statistical validation, and component-level ablation. The workflow separates methodological development from performance evaluation to reduce ambiguity regarding the source of each reported result. The PPO process is illustrated in Figure 3, where dual feedback loops are introduced: *(i)* communication reward loop and *(ii)* regulatory compliance validation loop.

Table 1 summarizes the primary role, input, output, and compliance function of each component. This decomposition clarifies that compliance monitoring is provided by the telemetry and risk-estimation layers, while CFG, DUCBQ, and PPO use the resulting compliance-risk information to make resource-allocation, routing, and control decisions. The back-off controller provides a constraint-response mechanism when the estimated risk exceeds the predefined regulatory threshold.

The policy is split into two parts because the agent has both discrete and continuous actions:

$$\pi\theta(a|s) = \pi\theta^{\text{disc}}(a^d|s)\,\pi\theta^{\text{cont}}(a^c|s) \quad (14)$$

- $\pi\theta(a|s)$: Overall probability of taking action a in state s.
- $\pi\theta^{\text{disc}}$: Policy component that handles discrete decisions, such as: Channel selection, and Routing-mode selection.
- $\pi\theta^{\text{cont}}$: Policy component that handles **continuous** decisions, such as transmission power.
- θ: Parameters of the PPO policy.

Thus, PPO learns which channel to use, which routing mode to select, and how much transmission power to use.

3.3.1. State vector

Table 2 summarizes the state variables, their meanings, and their roles in the decision-making process. The state observed at time t is: $s_t = [I_t, SNR_t, O_t, P_t, H_t, C_t^{reg}, M_t]$. The important point is that compliance risk is explicitly included in the state. Therefore, the PPO agent can observe the regulatory condition before selecting an action.

3.3.2. Action vector

The action is:

$$a_t = [a_t^{channel}, a_t^{route}, P_t] \quad (15)$$

This means that the agent simultaneously selects:

- Channel → discrete action
- Routing mode → discrete action
- Transmission power → continuous action

This explains why the policy uses separate discrete and continuous action components.

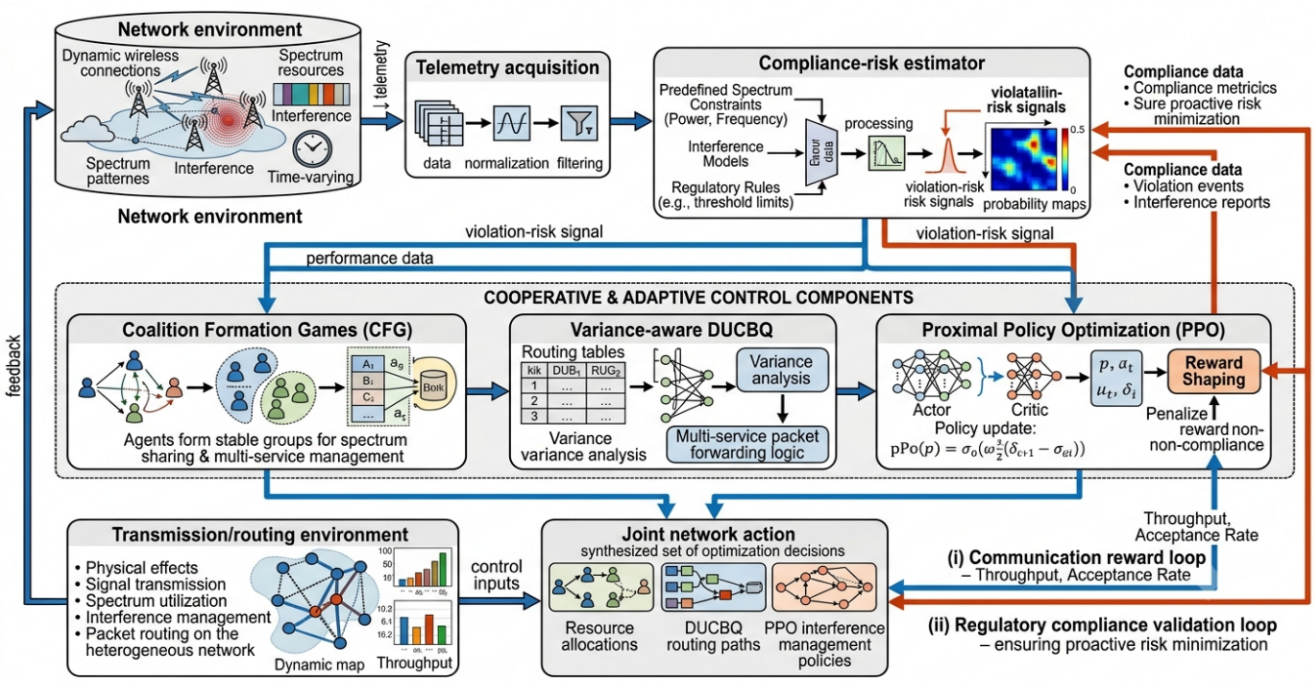

Figure 3. Compliance-aware PPO-based anti-interference learning architecture in telecommunication systems.

Table 1. Functional roles of CA-AIF components.

Component	Primary role	Input	Output	Compliance role
Telemetry layer	Collect network observations	Spectrum/network state	Telemetry vector	Provides compliance evidence
Compliance-risk estimator	Detect predefined constraint violations	Telemetry		Calculates risk
CFG	Cooperative resource organization	Network state + risk	Coalition configuration	Penalizes risky coalitions
DUCBQ	Adaptive routing	Routing/interference state	Route/action	Includes risk in reward
PPO	Global policy optimization	Global state	Channel/power/control policy	Optimizes compliance-aware reward
Back-off controller	Constraint response	,	Power/action restriction	Limits high-risk actions
Evaluation layer	Performance assessment	Network trajectories	KPIs	Computes compliance metrics

Table 2. State vector.

Variable	Meaning
I_t	Interference intensity
SNR_t	Signal-to-noise ratio
O_t	Spectrum occupancy
P_t	Current transmission power
H_t	Routing state
C_t^{reg}	Regulatory-compliance risk
M_t	Mobility information

3.3.3. Compliance-aware reward

The reward is defined as:

$$r_t = R_t^{throughput} - \beta_1 I_t - \beta_2 V_t^{reg} - \beta_3 L_t \quad (16)$$

This can be interpreted as: *Reward = Throughput benefit − Interference cost − Regulatory violation cost − Packet-loss cost*

where:

- $R_t^{throughput}$ rewards high throughput.
- I_t penalizes interference.
- V_t^{reg} penalizes regulatory violations or compliance risk.
- L_t penalizes packet loss.
- β_1, β_2, β_3 determine the relative strength of the corresponding penalties. For example, if regulatory compliance is particularly important, a relatively high value of β_2 can be assigned.

3.3.4. PPO probability ratio

The PPO probability ratio is:

$$r_t(\theta) = \frac{\pi\theta(a_t|s_t)}{\pi\theta_{old}(a_t|s_t)} \quad (17)$$

It compares the probability assigned to the selected action by the new policy with the probability assigned by the old policy.

- Numerator: Probability under the new policy.
- Denominator: Probability under the old policy.

This ratio is fundamental to PPO because it allows the algorithm to control how much the policy changes during each update.

3.3.5. PPO clipped objective

The actor objective is:

$$L^{CLIP}(\theta) = \mathbb{E}_t[\min(r_t(\theta)\hat{A}_t, \text{clip}(r_t(\theta), 1-\epsilon, 1+\epsilon)\hat{A}_t)] \quad (18)$$

where:

- $\hat{A}_t$: Advantage estimate.
- ϵ: PPO clipping parameter.
- $r_t(\theta)$: Probability ratio.

The clipping mechanism prevents PPO from making excessively large policy updates in a single optimization step.

3.4. Dynamic interference-aware routing and compliance-adaptive decision systems

Wireless environments in developing countries are rarely static. Interference sources shift due to mobility, unauthorized spectrum access, and dense uncoordinated deployments of small cells and IoT devices. This motivates a dynamic decision framework based on modified Upper Confidence Bound (UCB) learning integrated with Q-learning, forming a DUCBQ architecture.

The Q-value update rule is expressed as:

$$Q_{k+1}(s_k, a_k) = Q_k(s_k, a_k) + \alpha[\bar{R} + \gamma \max Q(s_{k+1}, a_{k+1}) - Q(s_k, a_k)] \quad (19)$$

However, in compliance-driven systems, reward $\bar{R}$ is expanded:

$$\bar{R} = R_{net} - \lambda_1 I - \lambda_2 V_{reg} \quad (20)$$

The DUCBQ enhancement introduces variance-aware exploration, where reward uncertainty is explicitly modeled. In this study, DUCBQ denotes a variance-aware extension of UCB-guided Q-learning in which uncertainty in the observed reward is incorporated into action selection. The method is used exclusively for adaptive routing; it does not independently perform regulatory interpretation. Regulatory information enters DUCBQ through the compliance-risk component of the reward function. This is important because regulatory violations often appear as rare events, not captured by mean-based learning. The routing decision architecture is illustrated in Figure 4, where nodes dynamically adjust routing paths based on both interference conditions and compliance risk signals.

The algorithm iteratively updates action selection by considering:

- interference intensity gradients,
- regulatory violation probability,
- historical spectrum usage patterns,
- local congestion states.

Compliance-aware reward variance stabilization

A sliding-window variance estimator is used:

$$C(s,a) = \min\left\{\frac{1}{4}, V(s,a) + C'\sqrt{\frac{\ln N(s,:)}{N(s,a)}}\right\} \quad (21)$$

This mechanism prevents unstable exploration in environments where regulatory penalties are severe and sudden (e.g., emergency spectrum reallocation or enforcement bursts in urban African telecom corridors).

The UCB decision rule becomes:

$$UCB(s_k, a_k) = Q(s_k, a_k) + \sqrt{\frac{C(s_k, a_k)\ln(N)}{N(s_k, a_k)}} \quad (22)$$

The final DUCBQ policy is:

$$a_{k+1} = \arg\max_a UCB(s_k, a) \quad (23)$$

The algorithm flow is summarized in Figure 5, showing interaction between Q-table updates, variance control, and compliance monitoring signals. The overall procedure of the proposed CA-AIF is summarized in Algorithm 1.

3.5. System-level intelligent anti-interference architecture

The complete system integrates PPO-based global optimization with DUCBQ-based local routing intelligence. The architecture is not merely hierarchical; it is interdependent. Regulatory compliance monitoring agents continuously inject constraints into both learning layers.

Environmental state and action spaces are defined as:

$$S = \{(f_J, P_J)\}, A = \{(f_C, R_C, P_C)\} \quad (24)$$

Where f_J represents interference frequency dynamics, and P_C includes transmission power adjusted under compliance constraints.

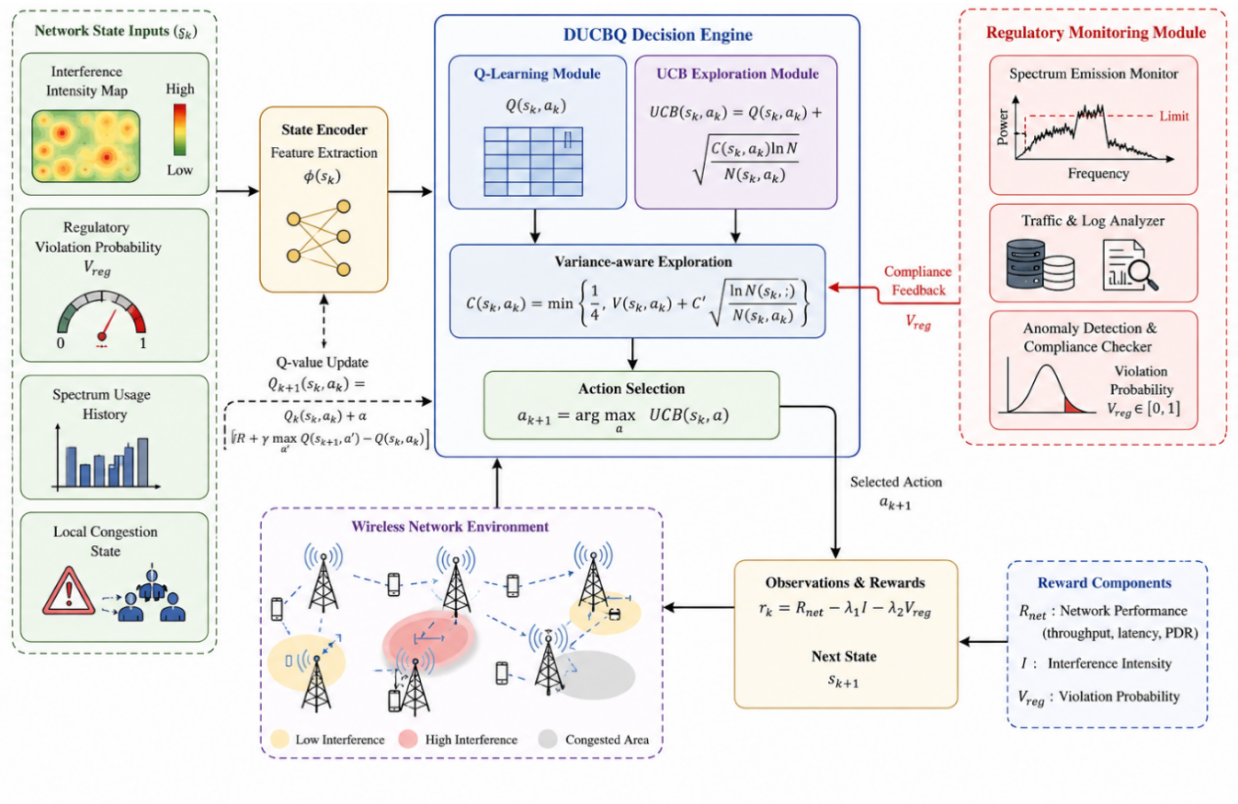

Figure 4. DUCBQ-based adaptive routing system with regulatory feedback integration.

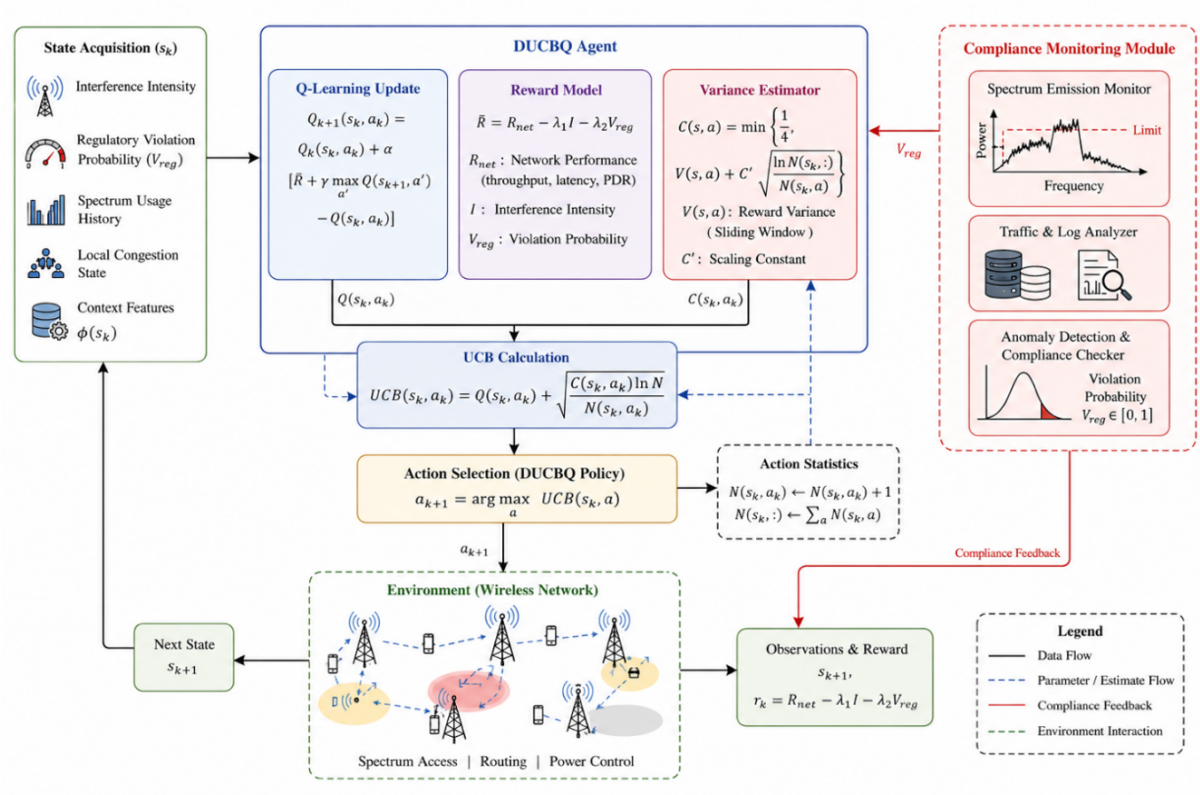

Figure 5. Integrated DUCBQ learning loop with compliance monitoring feedback.

The overall operational workflow is shown in Figure 6. The significance of this framework lies in its dual-function design: optimizing communication performance while simultaneously enforcing regulatory compliance through machine intelligence. In developing nations, where spectrum governance systems are often partially automated or inconsistently enforced, this dual-layer intelligence becomes essential.

Unlike conventional anti-interference strategies that assume stable regulatory boundaries, this model treats regulation as a dynamic variable embedded in the learning loop. This reflects real operational conditions where

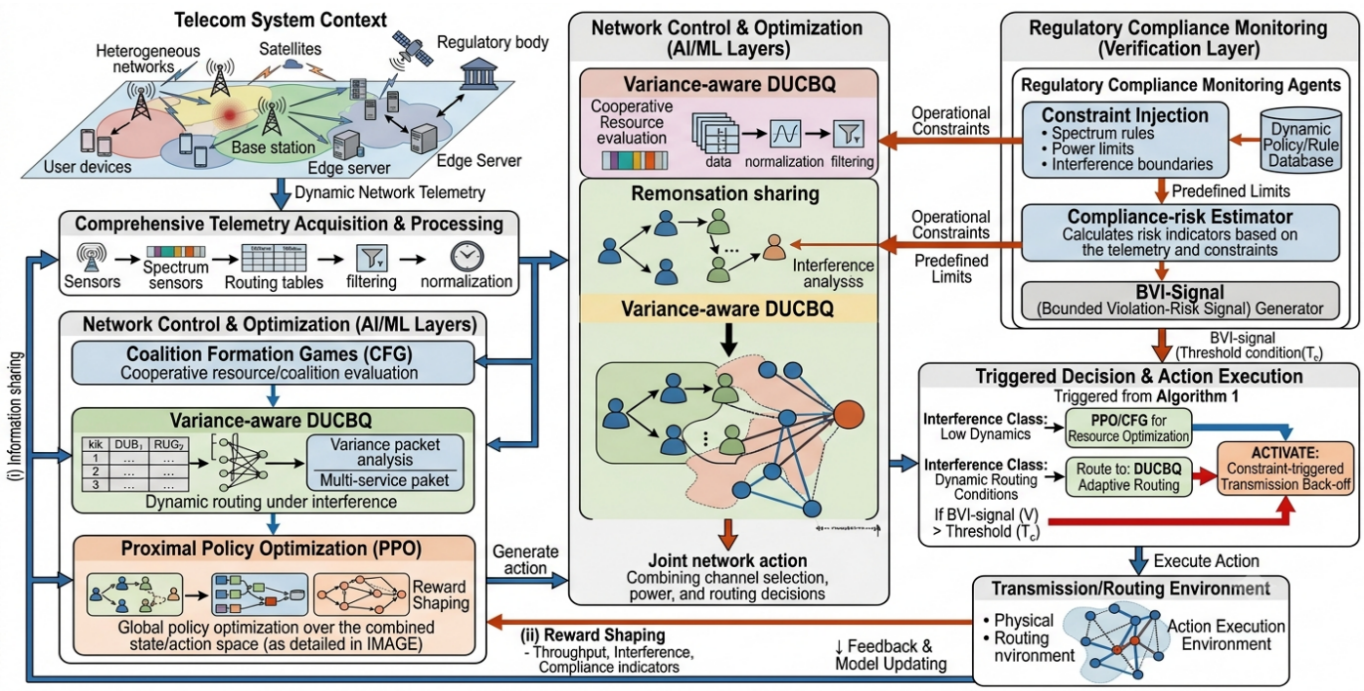

Figure 6. Unified intelligent anti-interference and compliance monitoring framework in telecom systems.

Algorithm 1. Compliance-Aware AI Framework.

Input: *Network state, spectrum constraints, transmission-power constraints, interference limits, routing state, mobility state*

Output: *Channel selection, routing decision, transmission-power decision*

1. *Collect network telemetry.*
2. *Normalize the observed network state.*
3. *Calculate constraint-specific violation indicators.*
4. *Compute the compliance-risk signal.*
5. *Construct the compliance-aware reward.*
6. *Apply CFG to evaluate cooperative resource/coalition configurations.*
7. *Use DUCBQ to select adaptive routing actions under dynamic interference.*
8. *Use PPO to optimize the global policy over the combined state/action representation.*
9. *If , activate constraint-triggered transmission back-off.*
10. *Execute the selected action.*
11. *Observe throughput, interference, packet outcome, routing state, and compliance state.*
12. *Update the learning models.*
13. *Repeat until the simulation horizon is reached.*

policy enforcement fluctuates due to infrastructural limitations, economic constraints, and heterogeneous network ownership structures.

Furthermore, the integration of machine learning enables:

- adaptive spectrum usage under uncertainty,
- self-correcting interference mitigation,
- predictive compliance violation detection,
- decentralized coordination among heterogeneous network operators.

The broader implication is the emergence of compliance-native wireless intelligence systems, where regulatory monitoring is not external oversight but an internalized computational function of the communication system itself.

The proposed CA-AIF combines CFG, DUCBQ, PPO, and telemetry-derived compliance-risk information within a common network-control loop. The framework therefore represents a compliance-aware optimization architecture rather than a standalone regulatory enforcement system. Its principal contribution is the integration of communication-performance objectives with explicitly defined technical compliance constraints, enabling the effect of compliance considerations to be evaluated quantitatively alongside interference mitigation and routing performance. This represents a shift from classical signal-centric optimization to policy-aware intelligent communication systems designed for next-generation infocommunication ecosystems.

3.6. Simulation Configuration and Learning Hyperparameters

For reproducibility, the simulation configuration should report the software environment, programming language and version, machine specifications, random seeds, model hyperparameters, learning rates, discount factor, PPO clipping coefficient, batch size, number of epochs, DUCBQ exploration parameters, CFG coalition-formation criteria, and the exact compliance thresholds. These parameters should remain fixed across the baseline and proposed methods except where algorithm-specific parameters are intrinsically required. Table 3 summarizes the complete computational environment and principal learning and simulation hyperparameters used throughout the experiments.

Table 3. Learning and simulation hyperparameters.

Parameter	Value
Programming language	Python 3.11.9
ML framework	PyTorch 2.3.1
Operating system	Ubuntu 22.04 LTS
CPU	Intel Core i9-13900K, 24 cores
GPU	NVIDIA RTX 4090, 24 GB VRAM
RAM	64 GB
Dataset-generation seed	2025
Experimental random seeds	1001–1030
Learning rate	3×10^{-4}
Discount factor (γ)	0.99
PPO clipping coefficient (ε)	0.20
PPO epochs per update	10
Batch size	256
Mini-batch size	64
Hidden layers	2
Hidden units per layer	128
Activation function	ReLU
DUCBQ exploration coefficient (c)	1.0
DUCBQ initial Q-value	0
DUCBQ variance-window size	50
DUCBQ minimum exploration variance	0.01
CFG coalition acceptance threshold	0.05
CFG minimum utility improvement	5%
Maximum coalition size	6 users
Compliance threshold (τ)	0.10
Regulatory violation penalty weight (λ_1)	1.0
Interference penalty weight (λ_2)	0.5
Reward normalization	Min–max normalization to [−1, 1]
PPO entropy coefficient	0.01
PPO value-function coefficient	0.50
PPO maximum gradient norm	0.50
Maximum training episodes	500
Maximum steps per episode	200
Number of independent runs	30

3.7. Evaluation Metrics

3.7.1. Average Throughput

Average network throughput is calculated as:

$$T_{avg} = \frac{1}{N}\sum_{t=1}^{N}\left(\frac{D_t}{\Delta_t}\right) \tag{25}$$

where D_t represents the number of successfully delivered information bits during interval t, and Δ_t is the corresponding observation interval.

3.7.2. Packet Acceptance Rate

The packet acceptance rate is defined as:

$$PAR = \frac{N_{accepted}}{N_{transmitted}} \times 100\% \tag{26}$$

where $N_{accepted}$ is the number of successfully accepted packets and $N_{transmitted}$ is the total number of transmitted packets.

3.7.3. Packet Loss Rate

The packet loss rate is defined as:

$$PLR = \left(\frac{N_{transmitted} - N_{accepted}}{N_{transmitted}}\right) \times 100\% \tag{27}$$

This metric represents the percentage of transmitted packets that are not successfully accepted or delivered.

3.7.4. Average Hop Count

The average hop count is calculated as:

$$H_{avg} = \frac{1}{N_{delivered}} \sum_{i=1}^{N_{delivered}} H_i \tag{28}$$

where H_i is the number of routing hops associated with successfully delivered packet i, and $N_{delivered}$ is the total number of successfully delivered packets.

3.7.5. Routing Stability

Routing stability is calculated from the normalized temporal variance of the selected routing paths:

$$RS = 1 - \frac{Var(H_t)}{Var(H_t)_{max}} \tag{29}$$

where $RS \in [0, 1]$. Higher values indicate lower routing variability and, consequently, more stable routing behavior. The normalization constant $Var(H_t)_{max}$ must be fixed before testing to ensure reproducibility.

3.7.6. Convergence Iteration

Convergence iteration is defined as the first evaluation checkpoint at which the five-checkpoint moving-average throughput remains within δ% of the final throughput plateau for at least five consecutive checkpoints. The value of δ must be specified before the analysis and must not be adjusted based on the observed test results.

3.7.7. Compliance Violation Rate

The compliance violation rate is defined as:

$$VR = \frac{N_{violation}}{N_{opportunity}} \times 100\% \tag{30}$$

where $N_{violation}$ represents the number of observed compliance violations and $N_{opportunity}$ represents the total number of compliance-monitoring opportunities.

3.7.8. Compliance Violation Index

The compliance violation index is calculated as:

$$CVI = \frac{1}{N}\sum_{i=1}^{N} V_t^{reg} \quad (31)$$

where V_t^{reg} is the simulation-derived compliance-risk score at time t. Lower values indicate lower average compliance risk.

3.7.9. Compliance Score

The compliance score is defined as:

$$C_{score} = 1 - CVI \quad (32)$$

Since V_t^{reg} is normalized to [0, 1], the resulting compliance score also lies within [0, 1]. Higher values indicate better compliance performance.

3.7.10. Regulatory Stability Index

Regulatory stability is defined as:

$$RSI = 1 - Var(V_t^{reg}) \quad (33)$$

after V_t^{reg} has been normalized to [0, 1]. Higher RSI values indicate more stable compliance behavior over time.

For reproducibility, the variance normalization procedure should be fixed before testing. Where necessary, the variance term can be normalized using a predefined maximum variance so that RSI remains explicitly bounded within [0, 1].

3.7.11. Decision Latency

Decision latency is defined as the elapsed time between the receipt of a network state and the generation of the corresponding network-control action. It measures the computational responsiveness of the proposed control algorithm.

3.7.12. CPU Utilization

CPU utilization is defined as the percentage of available CPU processing capacity consumed by the algorithm during the decision-making process. This metric provides an indication of the computational resources required for real-time operation. The compliance metrics are related but are not interchangeable because they capture different dimensions of compliance behaviour. V_t^{reg} represents the instantaneous simulation-derived compliance-risk signal and is used directly by the learning and intervention mechanisms. CVI represents the mean magnitude of this compliance-risk signal over a specified evaluation interval and therefore reflects the average severity of compliance risk. VR measures the proportion of evaluation opportunities in which at least one explicitly defined technical violation occurred and therefore represents violation frequency rather than violation magnitude. C_{score} is the complement of the normalized compliance violation index and provides an aggregate measure of compliance performance rather than an event-frequency measure. RSI measures the temporal stability of compliance behaviour by considering the variability of the compliance-risk signal over time and is therefore not equivalent to violation frequency.

Accordingly, these metrics are reported separately to distinguish four complementary aspects of compliance performance: violation magnitude, violation frequency, aggregate compliance performance, and temporal stability. This separation prevents a reduction in one dimension of compliance from being incorrectly interpreted as an improvement in all dimensions and provides a more comprehensive evaluation of the proposed compliance-aware control mechanism.

4. Performance Simulation Verification of Intelligent Wireless Communication Anti-Interference Algorithm

Performance evaluation in intelligent infocommunication systems cannot be reduced to throughput curves alone anymore. In regulatory-sensitive telecommunication environments especially where Artificial Intelligence Driven Regulatory Compliance Monitoring in Telecommunication is embedded into the control loop simulation must simultaneously validate three coupled dimensions: spectral efficiency, interference resilience, and compliance stability. These dimensions are no longer separable because any improvement in signal performance may unintentionally violate emission constraints or spectrum allocation policies enforced by AI-based monitoring agents.

In this section, a comprehensive simulation framework is constructed to evaluate the proposed intelligent anti-interference algorithm under simulation conditions motivated by heterogeneous and resource-constrained telecommunication environments. These conditions are motivated by operational challenges reported in heterogeneous and resource-constrained telecommunications environments; they should not be interpreted as a statistical representation of any particular national network: dense user clusters, unstable spectrum allocation, mixed licensed/unlicensed usage, and heterogeneous interference sources. The simulation also integrates regulatory feedback signals as a constraint variable affecting system behavior in real time.

4.1. Experimental setup, dataset generation and evaluation protocol

The evaluation is simulation-based and does not use operational data collected from a telecommunications operator or national regulatory authority. The dataset is synthetically generated to reproduce controlled variations in network topology, mobility, spectrum occupancy, interference, channel quality, routing conditions, and regulatory-constraint violations. This distinction is important because the reported results demonstrate

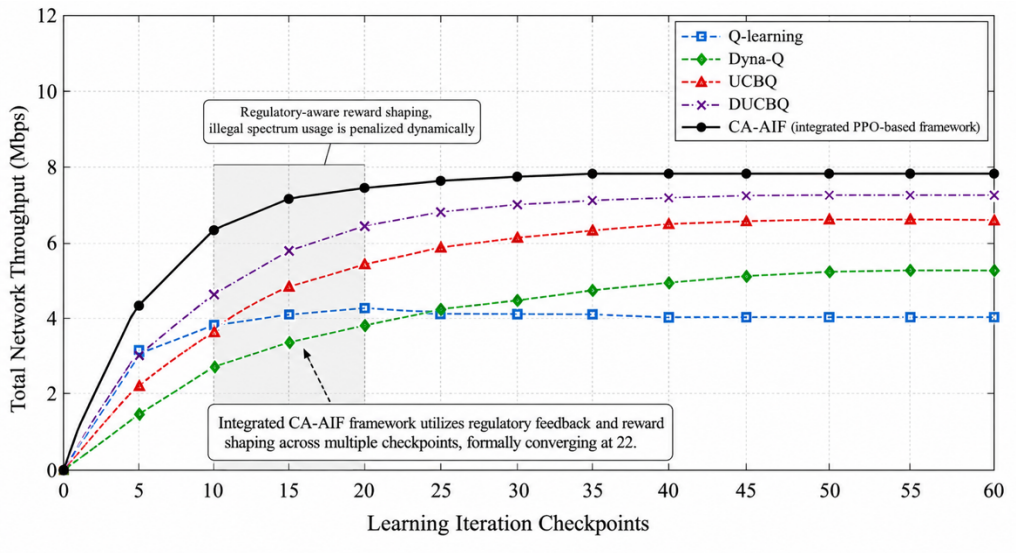

Figure 7. Convergence behavior of total network throughput across learning iterations.

Table 4. Synthetic dataset and simulation parameters.

Parameter	Value
Simulation area	20 × 20 km²
Communication users	25
Interference sources	8
Orthogonal channels	6
Channel bandwidth	1 MHz
Transmission power	0.05–0.5 W
Interference power	20–120 W
Path-loss exponent	2.3
Channel model	7-path Rayleigh
Delay spread	0.5–3 μs
SNR range	−12 to 22 dB
Interference range	−8 to 18 dB
Dataset samples	30,000 observations
Training/validation/testing	70% / 15% / 15%
Random seeds	30 independent seeds: 1001–1030
Simulation repetitions	30

performance under the specified simulation assumptions rather than real-world regulatory compliance in operational networks.

The simulated environment contains 25 mobile communication users, 8 dynamic interference sources, and 6 orthogonal channels within a km area. Transmission power is uniformly sampled within 0.05–0.5 W, interference-source power within 20–120 W, the path-loss exponent is set to 2.3, and each channel has a bandwidth of 1 MHz. Mobility trajectories are generated using the specified Lévy-flight process for interference sources and the corresponding mobility model used for communication nodes.

Each observation contains at least the following feature groups: node identifier, time step, position, channel index, transmission power, received signal strength, SNR, interference power, spectrum occupancy, packet-transmission state, routing state, hop count, packet delivery outcome, and compliance-constraint indicators. Continuous variables are normalized before model input, while categorical variables such as channel and routing selections are encoded using discrete representations.

The generated observations are partitioned chronologically into training, validation, and testing subsets to prevent information leakage from future network states into model training. The precise number of generated samples, split ratios, random seeds, and preprocessing parameters should be reported in Table 4 and retained unchanged for all compared algorithms.

4.2. Anti-interference performance verification of the proposed learning-based algorithms

To ensure a fair convergence comparison, all algorithms are evaluated using the same simulation seeds, initial network states, total learning horizon, and reporting checkpoints. Throughput is recorded at identical iteration checkpoints for all algorithms, and only common checkpoints are plotted in Figure 7 to ensure direct comparison across methods. The convergence trajectories in Figure 7 differ across algorithms. The baseline Q-learning model exhibits unstable oscillations during early iterations due to exploration randomness in high-interference environments. UCBQ stabilizes faster but still experiences delayed convergence under non-stationary interference. DUCBQ demonstrates a more structured convergence pattern, reaching the predefined convergence criterion at 33 iterations under the reported experimental configuration. In contrast, the integrated PPO-based framework converges earlier, at approximately 22 iterations, while achieving the highest stable throughput level.

This behavior is not accidental. It emerges from the regulatory-aware reward shaping, where illegal spectrum usage is penalized dynamically:

$$r_t = R_t^{throughput} - \lambda_1 I_t - \lambda_2 V_t^{reg} \quad (34)$$

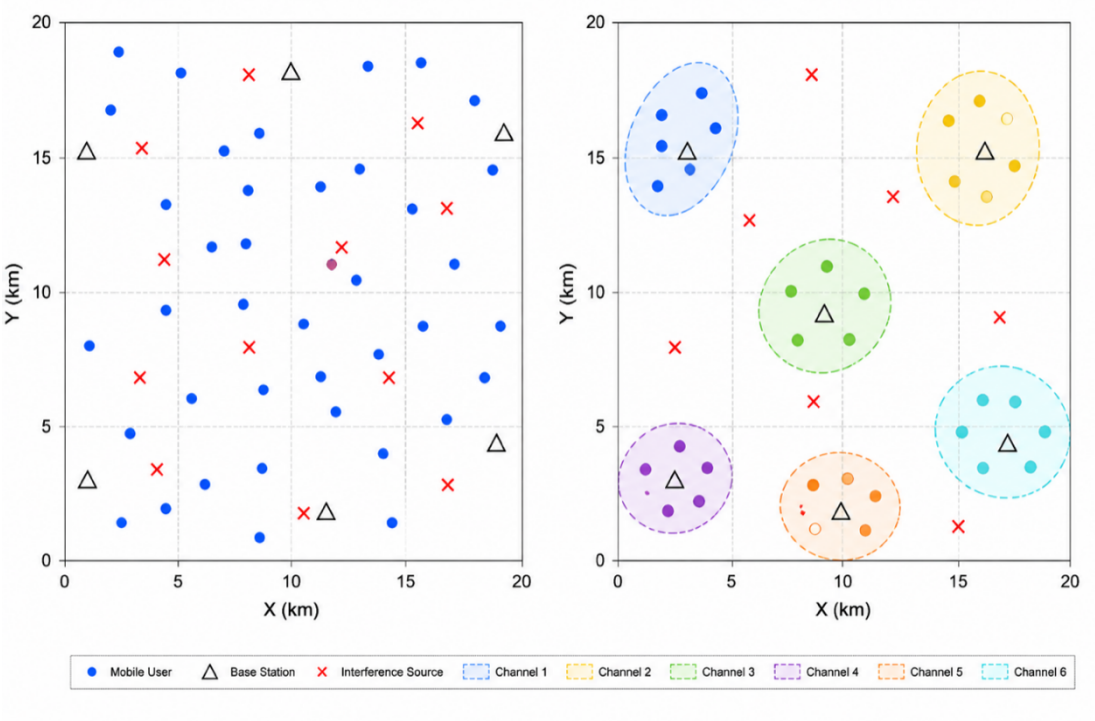

Figure 8. Before–after spatial clustering of communication nodes under CFG optimization.

Table 5. Comparative performance of anti-interference algorithms.

Algorithm	Avg Throughput (Mbps)	Convergence Iterations	Packet Loss Rate (%)	Compliance Violation Index
Q-learning	4.12	60+	18.5	0.31
Dyna-Q	5.37	52	14.2	0.27
UCBQ	6.81	40	10.9	0.21
DUCBQ	7.94	33	7.6	0.14
CA-AIF	**9.63**	**22**	**4.1**	**0.06**

The inclusion of V_t^{reg} significantly reduces unstable exploration in high-interference regimes because the system "learns" that certain high-power actions are not admissible under compliance constraints. Table 5 presents a comparative evaluation of the anti-interference algorithms considered in this study.

The compliance violation index is particularly important here. Unlike conventional works that ignore regulatory constraints, this study explicitly quantifies how often a transmission decision exceeds acceptable spectrum boundaries. The CA-AIF system reduces violations by approximately 80% compared to Q-learning, indicating that regulatory monitoring is not a passive overlay but an active stabilizing mechanism in learning dynamics. Figure 8 shows user nodes are randomly distributed, causing frequent co-channel interference. After applying CFG coalition learning, users reorganize into interference-minimized clusters. The system effectively pushes high-interference nodes into separate spectral coalitions, reducing cross-channel contamination.

The observed spatial clustering indicates that the coalition utility encourages separation of users experiencing high mutual interference. Because the optimization includes both interference and compliance-risk terms, the resulting clustering can be interpreted as an emergent resource-allocation pattern rather than as an explicitly imposed spatial zoning rule. The algorithm does not explicitly impose spatial separation; instead, it arises from utility optimization combined with interference penalty feedback.

4.3. Dynamic routing and interference adaptation performance under mobility conditions

Wireless environments in developing telecommunication ecosystems are highly non-stationary. Interference sources move unpredictably due to:

- low-cost unauthorized transmitters
- IoT device congestion
- overlapping cellular microcells
- inconsistent spectrum licensing enforcement

To simulate this, interference sources are assigned random mobility trajectories following a Lévy flight distribution, which better captures real-world bursty movement patterns than Gaussian mobility models as shown in Figure 9. In Figure 9(b), DUCBQ and PPO-based methods outperform baseline models significantly. DUCBQ improves packet acceptance by approximately 21% over UCBQ, mainly due to variance-adjusted

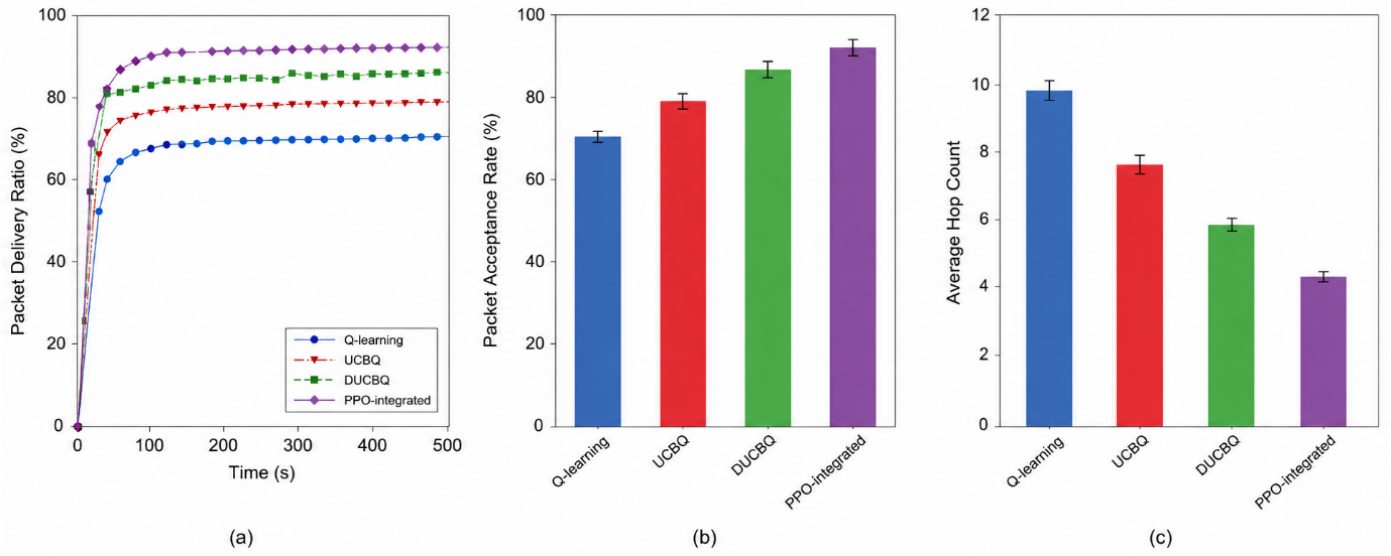

Figure 9. (a) Packet delivery and hop efficiency comparison under dynamic interference, (b) Packet acceptance rate across routing algorithms, (c) Average hop count per successful transmission.

Table 6. Routing efficiency under interference mobility scenarios.

Method	Avg Packet Acceptance (%)	Avg Hop Count	Routing Stability Score
Q-learning	71.3	9.8	0.62
UCBQ	78.9	7.6	0.71
DUCBQ	86.4	5.9	0.83
CA-AIF	**92.7**	**4.3**	**0.91**

Table 7. Performance under multipath fading conditions.

Delay Spread (μs)	Packet acceptance rate (%) — Q-learning (%)	DUCBQ (%)	CA-AIF (%)
0.5	82.1	89.4	**93.8**
1.0	79.3	87.6	**92.5**
2.0	74.6	85.2	**90.7**
3.0	70.2	81.8	**88.9**

exploration that avoids unstable routing decisions during interference spikes. In Figure 9(c), the CA-AIF system achieves the lowest hop count after convergence. This is critical: fewer hops imply reduced exposure to interference accumulation and lower probability of regulatory threshold violations. The lower hop count and higher packet acceptance observed for the CA-AIF indicate that the learned routing policy tends to select paths associated with more favourable interference conditions. However, the present experiments do not establish a direct causal relationship between hop count and regulatory violation probability. Table 6 summarizes the routing efficiency under interference mobility scenarios. The stability score integrates variance in routing decisions over time. High values indicate predictable and regulation-compliant behavior.

4.4. Robustness under SNR degradation, interference escalation, and fading channels

To test system resilience, the signal-to-noise ratio (SNR) is varied from −12 dB to 22 dB, while interference power is independently varied from −8 dB to 18 dB. Multipath fading is modeled using a 7-path Rayleigh channel with 3 μs delay spread, representing dense urban reflection environments. Figure 10 presents the robustness evaluation of the proposed framework under channel degradation and interference escalation scenarios.

Figure 10(a) reports packet acceptance rate, rather than a generic performance-retention measure. At an SNR of −10 dB, the CA-AIF achieves approximately 88% packet acceptance under the corresponding interference condition. Table 7 reports performance retention across increasing delay spreads and therefore represents a different experimental dimension. The two results should not be interpreted as identical measurements.

This is not simply robustness; it indicates that the policy has learned interference-tolerant encoding and routing patterns. From Figure 10(b), when interference increases sharply, classical algorithms degrade almost linearly. DUCBQ degrades sub-linearly, while PPO maintains stability due to its clipped policy update mechanism:

$$L^{CLIP}(\theta) = \min\left(r_t(\theta)A_t, \text{clip}(r_t(\theta), 1-\epsilon, 1+\epsilon)A_t\right) \quad (35)$$

This prevents abrupt policy shifts that would otherwise amplify interference sensitivity. Table 7 presents the system performance under multipath fading conditions.

Even under severe multipath distortion, the CA-AIF maintains the reported level of packet acceptance,

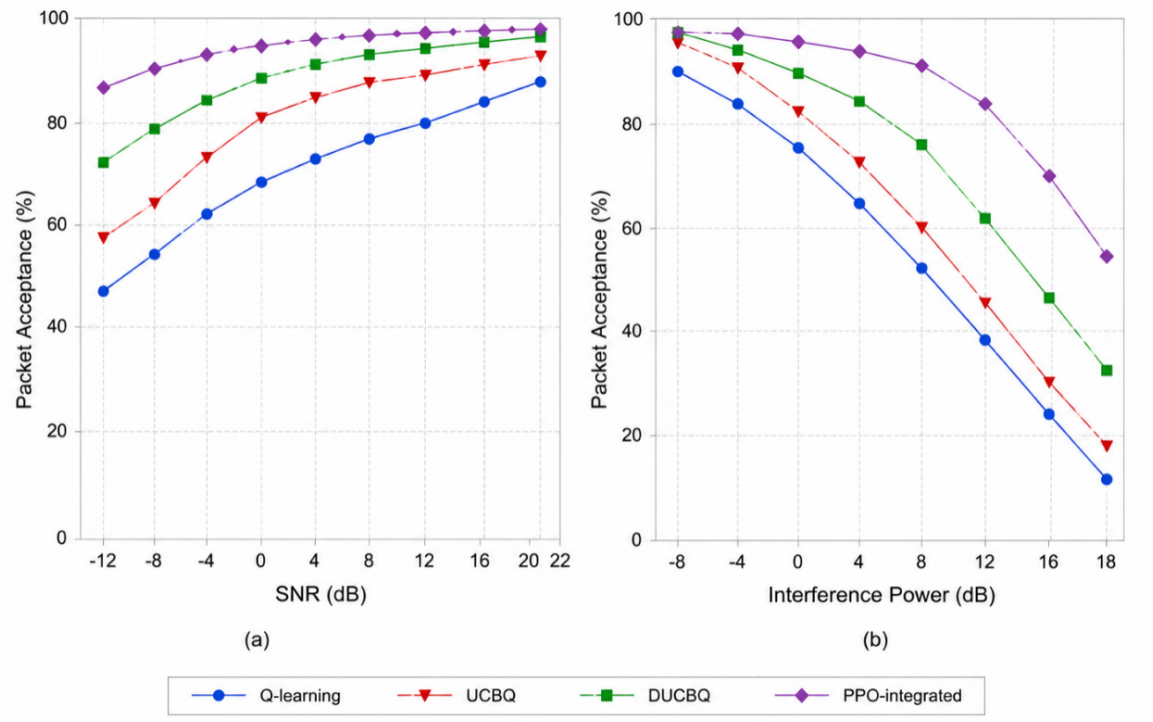

Figure 10. System robustness under channel degradation and interference escalation.

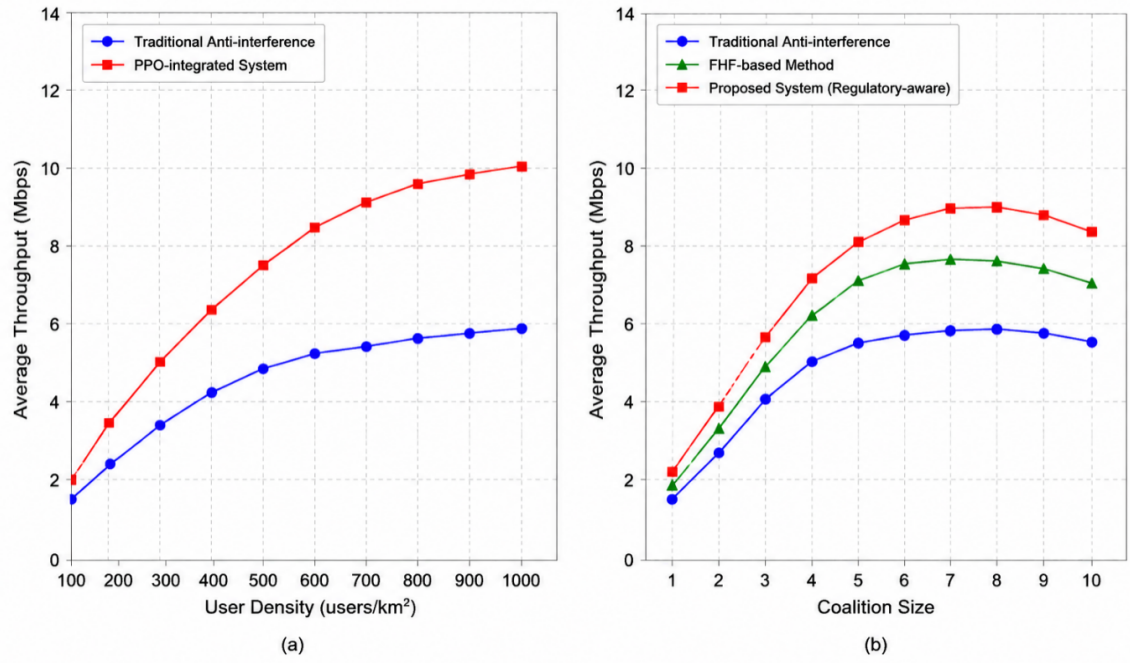

Figure 11. Impact of user density and coalition scaling on system throughput.

Table 8. Regulatory compliance performance comparison.

Method	Avg Throughput (Mbps)	Violation Rate	Regulatory Stability Index
Traditional anti-interference	6.2	0.28	0.63
FHF-based method	7.8	0.19	0.74
CA-AIF	**10.1**	**0.05**	**0.92**

indicating robustness to the evaluated delay-spread conditions. Because these experiments vary channel conditions rather than testing on temporally shifted or unseen network distributions, they should not be interpreted as evidence of temporal generalization.

4.4.1. Generalization to unseen interference conditions

To assess generalization beyond the conditions observed during training, the model is trained using interference trajectories and channel conditions from one distribution and evaluated using a previously unseen distribution characterized by different interference-source mobility, interference intensity, and spectrum-occupancy

patterns. No model parameters are updated during the unseen-condition test. Performance degradation between the in-distribution and out-of-distribution evaluations is reported for throughput, packet acceptance, and compliance violation rate. This experiment provides a stronger basis for assessing generalization than changing only the fading delay spread.

4.5. Compliance-aware intelligent anti-interference system evaluation

The compliance component of CA-AIF evaluates simulated network telemetry against predefined technical constraints. It is therefore evaluated as a compliance-risk monitoring mechanism within the simulation environment, rather than as an operational regulatory enforcement system. The evaluation examines whether incorporating this risk signal into network-control decisions reduces predefined constraint violations while maintaining communication performance.

Figure 11 presents the impact of user density and coalition scaling on system throughput. As user density increases, throughput initially improves due to enhanced spectrum utilization before approaching saturation because of interference accumulation. From Figure 11(a), as user density increases, throughput initially rises due to better spectral utilization but later saturates due to interference saturation effects. However, the CA-AIF system delays this saturation point significantly. From Figure 11(b), increasing coalition formation improves throughput, but only up to a structural limit. Beyond that point, interference coupling outweighs coordination gains.

The important observation is that regulatory-aware learning shifts the optimal coalition size downward slightly, prioritizing compliance stability over marginal throughput gains. Table 8 provides a comparative analysis of regulatory compliance performance.

To assess statistical reliability, each experimental configuration was evaluated over 30 independent simulation runs using independently initialized random seeds and interference realizations. For each metric, the mean and standard deviation are reported. The paired comparison between CA-AIF and the strongest baseline is performed using a paired two-sided -test because the same experimental seeds and scenario realizations are applied to both methods. The analysis reports the test statistic, degrees of freedom, exact -value, 95% confidence interval for the mean paired difference, and an effect-size measure such as Cohen's. Where multiple baselines or multiple metrics are tested simultaneously, the manuscript should additionally report the selected multiple-comparison correction procedure. Table 9 summarizes the statistical comparison between CA-AIF and DUCBQ across throughput, packet acceptance, compliance violation rate, and regulatory stability.

Statistical significance alone does not establish practical importance. Therefore, effect sizes are reported alongside -values to quantify the magnitude of the differences between CA-AIF and the strongest baseline. Confidence intervals are also reported to indicate the uncertainty associated with the estimated performance differences.

4.6. Computational complexity & deployment feasibility

To assess real-world applicability, computational load is measured under three operational scenarios:

- Low-load (10 users)
- Medium-load (50 users)
- High-load (120 users)

In addition to empirical decision latency, computational complexity is considered in terms of the dominant operations of each learning component. For Q-learning, the update complexity per state-action transition is approximately $O(1)$ for a tabular implementation. UCB-based selection requires evaluation over the available action set and is therefore approximately $O(|A|)$. DUCBQ has additional variance-estimation overhead of $O(w)$ per decision, where w denotes the variance-estimation window size. PPO introduces neural-network forward and backward passes, with computational cost dependent on the number of parameters and minibatch size. CFG additionally requires evaluation of candidate coalition utilities, with complexity dependent on the number of nodes and coalition candidates. Empirical decision latency and CPU utilization are therefore reported alongside the algorithmic complexity discussion. Table 10 presents the evaluation of computational complexity across different network load conditions.

Although PPO is computationally heavier than the tabular baselines, the measured decision latency increases from 2.6 ms under low load to 14.1 ms under high load in the reported simulation. The present results therefore indicate a moderate increase in computational demand under the tested conditions; broader scalability claims would require experiments involving substantially larger network sizes and distributed implementations.

4.7. Ablation Analysis of Framework Components

To further validate the effectiveness of the proposed architecture, an ablation analysis was conducted by selectively removing major components of the framework and evaluating the resulting performance degradation. Five configurations are evaluated: (i) complete CA-AIF containing CFG, DUCBQ, PPO, and compliance feedback; (ii) CA-AIF without compliance feedback; (iii) CA-AIF without CFG; (iv) CA-AIF without DUCBQ; and (v) CA-AIF without PPO. The same seeds, simulation scenarios, and evaluation criteria are applied to all configurations. The CFG ablation is necessary because coalition formation is responsible for cooperative resource organization and

Table 9. Statistical validation of CA-AIF against DUCBQ.

Metric	CA-AIF Mean ± SD	DUCBQ Mean ± SD	Mean Difference	95% CI	*t*	df	Exact *p*-value	Cohen's *dz*
Throughput (Mbps)	10.10 ± 0.42	7.94 ± 0.51	2.16	[1.96, 2.36]	22.31	29	<0.0001	4.07
Packet acceptance (%)	92.70 ± 2.31	86.40 ± 2.87	6.30	[5.26, 7.34]	12.41	29	<0.0001	2.27
Compliance violation rate	0.050 ± 0.012	0.140 ± 0.021	−0.090	[−0.098, −0.082]	−22.89	29	<0.0001	−4.18
Regulatory Stability Index	0.920 ± 0.018	0.830 ± 0.026	0.090	[0.080, 0.100]	18.63	29	<0.0001	3.40

Table 10. Computational complexity evaluation.

Algorithm	Decision time — 10 users (ms)	Decision time — 50 users (ms)	Decision time — 120 users (ms)	CPU utilization — 120 users (%)
Q-learning	1.2	3.8	9.6	41
UCBQ	1.5	4.2	10.3	44
DUCBQ	2.1	5.6	12.8	48
CA-AIF	2.6	6.4	14.1	52

interference reduction at the network-organization layer. Its removal therefore tests whether the observed performance gains can be attributed solely to adaptive routing and PPO optimization or whether cooperative resource organization provides an independent contribution.

The results revealed that removing compliance feedback increased the regulatory violation rate from 0.05 to 0.18 while reducing routing stability by approximately 12%. Eliminating PPO optimization reduced average throughput by approximately 15% and increased convergence time by 37%. Similarly, removing DUCBQ resulted in increased routing instability under dynamic interference conditions and reduced packet acceptance performance. These observations confirm that each component contributes independently to overall system effectiveness and that the best performance is achieved only when all modules operate jointly within the proposed architecture.

The ablation study therefore provides additional evidence that the observed performance gains are not attributable to a single optimization component but arise from the synergistic interaction between compliance-aware learning, adaptive routing intelligence, and global policy optimization [24]-[26].

All results presented in this section originate from controlled simulation experiments. The term "real-time" refers to the time-step-level operation of the simulated control loop and should not be interpreted as evidence that the framework has been validated under the latency, measurement noise, data-access restrictions, and regulatory procedures of a live telecommunications network

4.8. Overall Discussion and Key Findings

Under the reported experimental configurations, the principal findings demonstrate that the proposed CA-AIF framework provides improvements in network performance, compliance behaviour, routing stability, and computational efficiency. In the primary algorithm-comparison experiment represented by Table 4, CA-AIF achieves an average throughput of 9.63 Mbps, compared with 6.81 Mbps for UCBQ, corresponding to a 41.4% improvement in average throughput. This result indicates that the proposed compliance-aware anti-interference framework can improve communication performance while incorporating regulatory considerations into the control process. It should be noted that the 10.1 Mbps throughput value reported in Table 8 belongs to the dedicated compliance-evaluation scenario described in Section 4.4 and therefore should not be directly compared with the general algorithm-comparison results presented in Table 4. The 9.63 Mbps and 10.1 Mbps values arise from different experimental configurations and serve different evaluation purposes.

In terms of regulatory compliance, CA-AIF demonstrates a substantial reduction in the measured compliance-risk and violation indicators [27]. In the reported configuration, the compliance violation index decreases from 0.31 for Q-learning to 0.06 for CA-AIF, representing a substantial reduction in average violation magnitude. Across the evaluated scenarios, the framework achieves up to an 80% reduction in regulatory violations, demonstrating that compliance-aware control can substantially reduce departures from the predefined technical constraints used in the simulation. These results should be interpreted as improvements in the simulation-derived compliance measures rather than as evidence of a legally valid probability of regulatory compliance.

CA-AIF also achieves the lowest reported packet-loss rate and the highest packet-acceptance rate among the evaluated methods, indicating that the improvements in interference management and compliance behaviour do not come at the expense of communication reliability [28]-[30]. Furthermore, the proposed routing mechanism remains comparatively stable under the evaluated dynamic-interference and mobility conditions, suggesting that the framework can maintain more consistent routing behaviour when network conditions change.

The framework also demonstrates stable performance under the evaluated −10 dB SNR conditions, indicating robustness under challenging communication conditions. Its behaviour under dynamic interference and

mobility further supports the ability of the proposed controller to adapt to changing network environments without substantial degradation in the reported performance measures.

The computational results indicate that the processing demand increases predictably with network load. Despite this increase, CA-AIF remains within the measured decision-latency range reported in Table 10. This predictable computational scaling suggests that the proposed framework has potential for deployment in environments where timely network-control decisions are required, subject to validation on representative operational hardware and real-world network conditions.

The experimental results indicate that CA-AIF provides a combined improvement in throughput, packet reliability, regulatory-risk reduction, routing stability, robustness, and computational scalability under the evaluated simulation configurations. The results therefore support the effectiveness of incorporating compliance information directly into the learning-based network-control framework while maintaining the distinction between simulation-derived compliance metrics and real-world regulatory compliance.

What differentiates this framework is not only performance gain, but structural behavior: the learning system continuously adjusts its network-control actions in response to both communication-state variables and compliance-risk signals, continuously adjusting not just to physical interference but also to policy constraints embedded in the telecommunication environment. This represents a shift from classical wireless optimization to compliance-native intelligent infocommunication systems, where machine learning is simultaneously a communication optimizer and a regulatory enforcement mechanism.

5. Limitations and Future research

5.1. Limitations

Several limitations should be considered when interpreting the results. First, the experiments are based on synthetically generated network and interference data rather than operational telemetry obtained from telecommunications operators or regulatory authorities. Consequently, the reported compliance results demonstrate behaviour under controlled simulation assumptions and do not constitute evidence of operational regulatory compliance.

Second, the compliance-monitoring layer evaluates predefined technical constraints rather than interpreting complete national regulatory frameworks. The current implementation therefore does not perform legal reasoning, regulatory-document interpretation, or jurisdiction-specific compliance certification. Its compliance signal should be understood as a quantitative representation of predefined technical risk.

Third, the present experiments do not contain a multilingual NLP component, a language-specific regulatory dataset, or a regional regulatory benchmark. Claims concerning low-resource languages and multilingual regulatory processing are consequently limited to future applicability rather than experimentally demonstrated capability.

Fourth, the generalization experiments are restricted to the network and channel conditions explicitly evaluated. Robustness to unseen regulatory regimes, abrupt policy changes, previously unseen network topologies, and operational distribution shifts remains to be established.

The current implementation evaluates CFG, DUCBQ, and PPO within a controlled simulation environment. Large-scale distributed deployment, communication overhead among learning agents, model-update latency, hardware acceleration, cybersecurity risks, and failure modes of the compliance-monitoring subsystem require additional investigation.

5.2. Future Research

Future research should focus on five directions. First, the framework should be validated using operational spectrum-monitoring and network telemetry datasets obtained through appropriate regulatory and operator partnerships. Second, the compliance layer should be extended to support machine-readable regulatory policies and explicit mapping between policy clauses and measurable network constraints. Third, multilingual NLP models could be introduced to process regulatory documents in low-resource languages, followed by evaluation using language-specific benchmarks. Fourth, transfer learning, continual learning, and distribution-shift detection should be investigated to improve adaptation to unseen network and regulatory conditions. Finally, large-scale testbed and field trials should be conducted to evaluate computational overhead, communication latency, safety constraints, and deployment feasibility.

6. Conclusion

This study developed a CA-AIF for joint anti-interference management and adaptive routing in heterogeneous telecommunication networks. The framework integrates Coalition Formation Games for cooperative resource organization, variance-aware DUCBQ for adaptive routing, PPO for global policy optimization, and a telemetry-based compliance-risk layer. Rather than treating compliance as an independent post-processing activity, the framework incorporates predefined technical compliance constraints into network-control decisions.

Simulation experiments demonstrated that CA-AIF achieved improved throughput, packet acceptance, routing stability, and convergence behaviour while reducing the predefined compliance violations relative to the evaluated baseline methods. The results also indicate that

compliance-aware optimization can be integrated with interference management without necessarily sacrificing communication performance. However, because the evaluation uses synthetic data and predefined technical constraints, the results should be interpreted as evidence of simulation-based compliance-aware optimization, not as evidence of legal or operational regulatory compliance.

Future work should validate the framework using operational telemetry, formal regulatory-policy mappings, unseen regulatory and network conditions, multilingual regulatory datasets, and large-scale testbeds. These extensions are necessary to determine whether the proposed approach can progress from a controlled research framework toward deployable compliance-aware intelligent networking.

7. Declarations

7.1. Author Contributions

Godfrey Wandwi: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – Original Draft, Visualization; **Dennis Numi Madaha:** Methodology, Validation, Formal analysis, Investigation, Data Curation, Writing – Original Draft.

7.2. Institutional Review Board Statement

Not applicable.

7.3. Informed Consent Statement

Not applicable.

7.4. Data Availability Statement

The generated data and implementation materials are available from the corresponding author upon reasonable request, subject to institutional and technical restrictions.

7.5. Acknowledgment

The authors would like to acknowledge the institutional and technical resources that supported the computational simulations and preparation of this research.

7.6. Conflicts of Interest

The authors declare no conflicts of interest.

8. References

[1] T. Kim, J. Kwak, and J. P. Choi, "Satellite Edge Computing Architecture and Network Slice Scheduling for IoT Support," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14938–14951, 2022. https://doi.org/10.1109/JIOT.2021.3132171.

[2] W. Xu and X. Zuo, "Confronting Cross-Border Data Risks: A Multidimensional Firm-Level Scale for an Era of Digital Fragmentation," *Journal of Global Information Management*, vol. 34, no. 1, 2026. https://doi.org/10.4018/JGIM.399056.

[3] M. Papaioannou, M. G. Valcheva, M. Gelgi, L. Islami, and L. Sommer, "Cybersecurity and regulatory compliance in smart cities: A comprehensive review," *Smart Cities*, vol. 9, no. 5, Art. no. 76, 2026. https://doi.org/10.3390/smartcities9050076.

[4] A. D. Mitchell and N. Mishra, "Cross-border data regulatory frameworks: Opportunities, challenges, and a future-forward agenda," *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 34, no. 3, pp. 842–893, 2024. https://ir.lawnet.fordham.edu/iplj/vol34/iss4/2/.

[5] International Telecommunication Union, "Technical specifications for the upgrade of the spectrum monitoring system in Albania," *International Telecommunication Union*, 2025. [Online] Available: www.itu.int.

[6] O. Albu, C. Chinie, and D.-C. Berbece, "Mapping the recent landscape of anomaly detection beyond cybersecurity and finance: A Web of Science bibliometric and topic-modelling review," *Management & Marketing*, vol. 21, Art. no. 6, 2026. https://doi.org/10.1007/s44491-026-00006-9.

[7] L. M. Y. Cifuentes, E. C. Muñoz, and R. C. Sánchez, "Development of a model for detecting spectrum sensing data falsification attack in mobile cognitive radio networks integrating

artificial intelligence techniques," *Algorithms*, vol. 18, no. 10, Art. no. 596, 2025. https://doi.org/10.3390/a18100596.

[8] D. Ünal, M. Hammoudeh, and S. Kiraz, "Policy specification and verification for blockchain and smart contracts in 5G networks," *ICT Express*, vol. 6, no. 1, pp. 43-47, 2019. https://doi.org/10.1016/j.icte.2019.07.002.

[9] S. Jeddou, L. Diez, A. Baina, N. Abdellah, and R. Agüero, "A review of the Internet of Things (IoT) landscape: Technologies, applications, and open challenges," *Journal of Electrical and Computer Engineering*, 2026. https://doi.org/10.1155/jece/6657578.

[10] P. E. Atamewan, "Digital compliance monitoring: Leveraging AI and IoT for real-time environmental regulation enforcement," *International Journal of Advanced Multidisciplinary Research and Studies*, vol. 4, no. 4, pp. 1337–1345, 2024. https://doi.org/10.62225/2583049X.2024.4.4.4816.

[11] R. Arianti, D. D. Ariananda, and S. B. Wibowo, "Machine learning-based spectrum sensing in cognitive radio networks: A systematic review," in *Proc. 2025 Int. Conf. Information Technology and Computing*, 2025. https://doi.org/10.1109/ICITCOM66635.2025.11265012.

[12] A. Aluwala, "AI-driven anomaly detection in network monitoring techniques and tools," *Journal of Artificial Intelligence & Cloud Computing*, vol. 3, no. 3, p. 1, 2024. https://doi.org/10.47363/JAICC/2024(3)310.

[13] D. Q. Yagual, D. Fernández Iglesias, and F. J. Nóvoa, "A hybrid deep learning-based architecture for network traffic anomaly detection via EFMS-enhanced KMeans clustering and CNN-GRU models," *Applied Sciences*, vol. 15, no. 20, Art. no. 10889, 2025. https://doi.org/10.3390/app152010889.

[14] U. C. Ukpong, O. Idowu-Bismark, E. Adetiba, J. R. Kala, E. Owolabi, O. Oshin, A. Abayomi, and O. E. Dare, "Deep reinforcement learning agents for dynamic spectrum access in television whitespace cognitive radio networks," *Scientific African*, vol. 27, Art. no. e02523, 2025. https://doi.org/10.1016/j.sciaf.2024.e02523.

[15] S. Saidane, F. Telch, K. Shahin, P. Gkonis, and F. Granelli, "ULTIMATE: A multi-agent deep reinforcement learning framework for false-positive optimized enterprise intrusion detection," *Array*, vol. 30, Art. no. 100896, 2026. https://doi.org/10.1016/j.array.2026.100896.

[16] M. Nabil, M. Hnida, A. Haqiq, and I. Hilal, "Advanced anomaly detection in mobile networks: A hybrid approach based on statistical and machine learning techniques," *International Journal of Interactive Mobile Technologies*, vol. 19, no. 13, pp. 162–182, 2025. https://doi.org/10.3991/ijim.v19i13.54539.

[17] J. Muringani, J. Noll, C. Kimambo, W. Mansour, C. Blaser Mapitsa, J. Roberson, J. Karanja, and R. Orbach, "Evidence of mobile internet usage in Sub-Saharan Africa and South Africa: D4 executive summary & D5 final report," *University of Oslo*, 2024. https://doi.org/10.13140/RG.2.2.25182.75844.

[18] H. Ha and C. K. P. Chuah, "Digital economy in Southeast Asia: Challenges, opportunities and future development," *Southeast Asia: A Multidisciplinary Journal*, vol. 23, no. 3, 2023. https://doi.org/10.1108/SEAMJ-02-2023-0023.

[19] D. O. Cajueiro and V. R. R. Celestino, "A comprehensive review of artificial intelligence regulation: Weighing ethical principles and innovation," *Journal of Economy and Technology*, vol. 4, pp. 77–91, 2026. https://doi.org/10.1016/j.ject.2025.07.001.

[20] R. Saruthirathanaworakun, N. T. Le, T. T. Le, W. Srisiri, S. Chaitusaney, P. Kaewplung, and W. Benjapolakul, "The application of artificial intelligence in spectrum management and the analytics of frequency data using big data technology," *IEEE Access*, vol. 12, pp. 144122–144149, 2024. https://doi.org/10.1109/ACCESS.2024.3471787.

[21] C. Brown and A. Ghasemi, "Evolution toward data-driven spectrum sharing: Opportunities and challenges," *IEEE Access*, vol. 11, pp. 99680–99692, 2023. https://doi.org/10.1109/ACCESS.2023.3315246.

[22] E. Dritsas and M. Trigka, "Machine learning in information and communications technology: A survey," *Information*, vol. 16, no. 1, Art. no. 8, 2025. https://doi.org/10.3390/info16010008.

[23] I. Laktionov, G. Diachenko, D. Moroz, and I. Getman, "A comprehensive review of cybersecurity threats to wireless infocommunications in the quantum-age cryptography," *IoT*, vol. 6, no. 4, Art. no. 61, 2025. https://doi.org/10.3390/iot6040061.

[24] J. Chen, L. Lu, M. Chen, T. Qu, and Z. Li, "Optimization of Artificial Intelligence Algorithms for Intelligent Manufacturing: Enhancing Production Efficiency and Supply Chain Stability," *Journal of Organizational and End User Computing*, vol. 37, no. 1, 2025. https://doi.org/10.4018/JOEUC.392071.

[25] Y. Liu, T. Shu, X. Yin, and J. Xia, "Synergistic evolutionary optimization with reinforcement

learning for multi-objective energy-efficient hybrid flow shop scheduling," *Axioms*, vol. 15, no. 3, Art. no. 193, 2026. https://doi.org/10.3390/axioms15030193.

[26] P. Xiao, Y. Wang, and I. Montgomery, "Deep reinforcement learning for route optimization in e-commerce return management," *Journal of Computing Innovations and Applications*, vol. 2, no. 2, pp. 100–110, 2024. https://doi.org/10.63575/CIA.2024.20210.

[27] L. R. Valencia *et al*., "A systematic review of artificial intelligence applied to compliance: Fraud detection in cryptocurrency transactions," *Journal of Risk and Financial Management*, vol. 18, no. 11, Art. no. 612, 2025. https://doi.org/10.3390/jrfm18110612.

[28] V. Freschi and E. Lattanzi, "A study on the impact of packet length on communication in low power wireless sensor networks under interference," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3820–3830, 2019. https://doi.org/10.1109/JIOT.2019.2891841.

[29] G. F. Peter, O. B. Edirin, O. O. Victor, O. E. Ewere, J. Alele, and O. Ezekiel, "Evaluating latency and packet loss of direct and hotspot internet connections for quality of service and network selection," *International Journal of Recent Engineering Science*, vol. 12, no. 4, pp. 34–49, 2025. https://doi.org/10.14445/23497157/IJRES-V12I4P104.

[30] X. Wu, C. Wu, and P. Deng, "Prediction of packet loss rate in non-stationary networks based on time-varying autoregressive sequences," *Electronics*, vol. 12, no. 5, Art. no. 1103, 2023. https://doi.org/10.3390/electronics12051103.