Quantum-Infused Deep Reinforcement Learning for Intrusion Detection in Surveillance Autonomous Vehicles

Collins Izuchukwu Okafor [1], Love Allen Chijioke Ahakonye [2], Dong-Seong Kim [1] [*], Jae Min Lee [1]
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
[*] NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
(collinsokafor, loveahakonye, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—As autonomous vehicles become essential in Military operations, ensuring the security and integrity of their sensor systems is paramount. Intrusion detection is challenging due to sensor diversity, dynamic environments, and the threat of quantum-based attacks. This study introduces a GPS spoofing intrusion detection system using deep reinforcement learning (DRL) and a quantum-resilient architecture. The framework combines Recurrent Proximal Policy Optimization (RPPO), attention mechanisms (RPPO-Attention-IDS), and variational quantum circuits to process and fuse multimodal sensor data, distinguishing between spoofing and environmental changes. Evaluations in a high-fidelity vehicle simulation, using the dataset, demonstrate the framework's real-time efficiency with an inference time of 0.50 ms. A sensitivity analysis reveals that a quantum circuit with 4 layers and six (6) qubits achieves optimal performance, improving accuracy by 38%. Compared to classical RPPO (20% accuracy), our method offers enhanced feature representation, highlighting the potential of quantum-enhanced DRL for secure vehicle deployment in the post-quantum era. Further advancements in class imbalance handling are needed.**

***Index Terms*—Autonomous vehicle, Cybersecurity, IDS, GPS, Recurrent Proximal Policy Optimization, Quantum Neural Network**

I. Introduction

Autonomous vehicles (AVs) and advanced driver-assistance systems (ADAS) are revolutionizing both military and civilian sectors, enhancing safety, efficiency, and convenience [1]. This system, as demonstrated in Figure 1, depends on complex sensor arrays, including cameras, LiDAR, radar, ultrasonic sensors, inertial measurement units (IMUs), and global navigation satellite system (GNSS) receivers, for real-time perception and decision-making [1]–[3]. However, their interconnected nature exposes them to cybersecurity risks, especially GPS spoofing attacks, where adversaries manipulate navigation systems with counterfeit signals [4], [5]. Such attacks can result in incorrect positioning, compromised missions, and safety risks, highlighting the need for robust system integrity and resilience [4].

Traditional intrusion detection systems (IDS) have typically used signature-based, rule-based, or statistical anomaly detection methods [6]. These approaches often fail to address the complex sensor data in autonomous systems. To improve detection, recent research has shifted towards deep learning (DL) and reinforcement learning (RL), utilizing advanced models like convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and gated recurrent units (GRUs) for detecting sophisticated spoofing attacks [7]–[9].

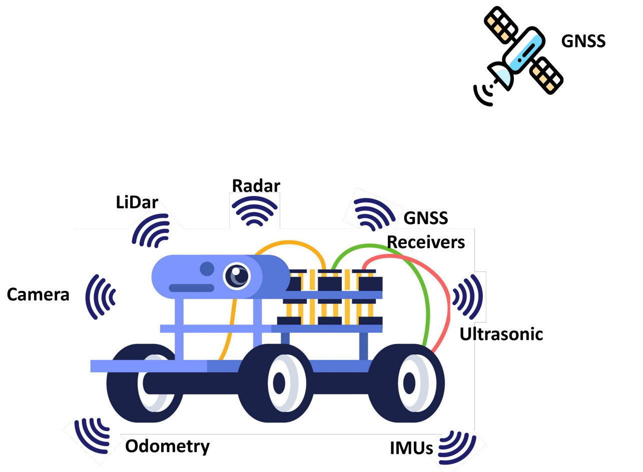

Fig. 1. Illustration of a sophisticated sensor suite in surveillance Autonomous vehicles

Despite advancements, several limitations persist in current models. One major issue is the reliance on handcrafted or shallow feature extraction, which limits the ability to capture high-dimensional and non-linear characteristics of complex GPS signals, potentially missing subtle variations and noise patterns [8]. Additionally, while recurrent models are designed for sequential data, they often struggle with long-term dependencies, particularly in autonomous systems where sensor data exhibits long-range temporal correlations and irregular intervals [1], [4]. This failure to capture extended dependencies can result in incomplete or inaccurate representations, thereby undermining the effectiveness of the detection system.

Robustness remains a challenge, with many deep learning (DL) and reinforcement learning (RL) models still vulnerable to adversarial perturbations, which exploit system weaknesses and hinder real-world generalization [4]. Models that perform well in controlled environments often struggle when exposed to real-world conditions, such as sensor noise, environmental factors, and unforeseen attacks [5]. To address these issues, we propose the Quantum-Enhanced RPPO-Attention-IDS framework [10], integrating recurrent proximal policy optimization (RPPO), a feature attention module, and quantum neural networks (QNNs) for robust and adaptive GPS spoofing intrusion detection.

Our key contributions are as follows:

1) We propose a novel DRL framework integrating QNN-based policy and value networks within an RPPO architecture for GPS spoofing detection in autonomous systems.
2) We develop a feature attention module that enhances GPS feature extraction by dynamically re-weighting and fusing the pre-processed feature vector.
3) We design a vectorized variational quantum circuit that processes batched input data, applying parameterized gates and entangling Controlled-NOT (CNOT) operations for quantum-enhanced feature extraction.
4) We apply transfer learning to adapt pre-trained QNN models to new datasets, improving the framework's generalization and robustness across different operational scenarios.
5) Extensive evaluation on the GPS spoofing dataset shows our framework's superior detection accuracy and robustness compared to traditional deep learning and machine learning approaches.

The remainder of this paper is organized as follows: Section II reviews related literature and outlines existing challenges, Section III details our proposed methodology, Sections IV and V present the analysis, discussion, and conclusions.

II. Background and Related Works

Machine learning (ML) algorithms have improved real-time decision-making in adversarial settings. Devkota et al. [11] introduced a GPS spoofing detection system using a random forest multiclass classifier, which offers interpretability and effectiveness on real-world data but lacks adaptability due to its fixed feature sets. To address evolving threats, self-supervised deep learning approaches have emerged as a solution. Alanazi et al. [7] and Alzahrani et al. [12] proposed LSTM-GRU and ConvLSTM-based models, respectively, for learning representations from unlabeled GPS signals. These models capture spatiotemporal patterns and achieve high accuracy in controlled settings, but their generalizability and scalability remain limited in real-world and resource-constrained UAV environments.

Raghad et al. [13] reviewed ML-based IDSs for UAVs, noting high accuracy but limited adaptability to quantum-era threats and the lack of integration of quantum computing to manage large state spaces. Abreu et al. [14] introduced a hybrid IDS combining classical and quantum computing using QML for binary and multiclass attack detection. While it benefits from quantum-enhanced feature spaces, performance is hindered by NISQ limitations. Sudharson et al. [15] proposed a quantum-resistant IDS using ML and lattice-based hash trapdoor cryptography, offering strong post-quantum security but challenged by computational overhead, legacy system integration, and real-time performance trade-offs.

Fowler et al. [16] present a testbed integrating free-space optical quantum key distribution (FSO-QKD) for secure vehicle-to-infrastructure (V2I) communications. They introduce a novel zero-trust authentication protocol (ZAP), which replaces traditional public key encryption that is vulnerable to quantum attacks. However, the FSO-QKD link's performance is limited by environmental factors, affecting its operational range and reliability. Despite these advancements, challenges such as data scarcity, real-time processing limits, adversarial robustness, and interpretability persist. The proposed RPPO method focuses on GPS spoofing detection, enhancing temporal modeling and improving real-time performance. By integrating quantum-enhanced deep reinforcement learning with adaptive strategies, RPPO surpasses fixed feature sets and static models, offering a scalable and robust solution for addressing evolving cyber threats in vehicular and UAV environments.

III. System Methodology

A. Problem Statement

This section models GPS spoofing detection for autonomous vehicles and UAVs as a Markov Decision Process (MDP) within a quantum-enhanced deep reinforcement learning (DRL) framework. It defines the environment, state/action spaces, and reward function. The focus is real-time spoofing detection, where attackers manipulate GPS signals, endangering navigation [8], [9]. In light of emerging quantum-enabled threats to classical cryptography [4], [5], [16], [17], the system must handle high-dimensional GPS data, detect anomalies precisely, and maintain low false-positive and false-negative rates to ensure a robust, future-proof defense.

B. Reinforcement Learning Formulation

To address the challenge of GPS spoofing detection, we formulate the task as an MDP and apply quantum-enhanced deep reinforcement learning. The environment simulates a vehicle's GNSS sensor operating under dynamic and realistic conditions. It includes a GNSS data stream with real-world noise, a spoofing injection module capable of introducing classical and quantum-style attacks (e.g., signal deviation, timestamp manipulation), and high-fidelity driving scenarios encompassing urban, highway, and rural environments.

1) Acronyms and Feature Definitions: IMU denotes *Inertial Measurement Unit*, GNSS denotes *Global Navigation Satellite System*, and CNOT denotes the *Controlled-NOT* gate. The 13 GNSS receiver-derived features are: PRN (satellite ID), DO (Doppler), PD (pseudorange), RX (receiver timing), TOW (time-of-week), CP (carrier phase), EC/LC (early/late correlators), PC (prompt correlator), PIP/PQP (prompt I/Q), TCD (tracking-loop metric), and CN0 (C/N_0). [18]

2) State: At each time step t, the state $s_t \in \mathbb{R}^d$ is defined as a feature vector containing pre-processed GPS signal characteristics. These features include, but are not limited to, PRN, DO, PD, RX, TOW, CP, EC, LC, PC, PIP, PQP, TCD, and CN0. The preprocessing involves normalization and temporal windowing to preserve spatial and temporal information essential for spoofing detection.

3) Action: The action $a_t \in \{0, 1\}$ represents the DRL agent's classification of the current GPS signal: $a_t = 0$ for *normal* and $a_t = 1$ for *spoofed*. This discrete action space lets the agent focus on binary classification for intrusion detection.

4) Reward Function: The reward function $R(s_t, a_t)$ in Equation 1 is designed to maximize detection accuracy by rewarding correct classifications and penalizing misclassifications, especially false negatives (missed spoofing instances). This encourages the agent to prioritize accurate spoofing detection in diverse, dynamic driving scenarios.

$$R(s_t, a_t) = \begin{cases} +R_{TP} & \text{if } a_t = 1 \text{ and Intrusion Detected (TP)} \\ -R_{FP} & \text{if } a_t = 1 \text{ and No Intrusion (FP)} \\ -R_{FN} & \text{if } a_t = 0 \text{ and Intrusion Present (FN)} \\ +R_{TN} & \text{if } a_t = 0 \text{ and No Intrusion (TN)} \end{cases} \tag{1}$$

To emphasize the critical nature of detecting spoofing, we set $R_{FN} > R_{FP}$ and typically $R_{TP} > R_{TN}$. To counteract class imbalance, we apply class-frequency weighting (larger penalties for minority-class misses) to discourage convergence to the majority-class policy.

C. Scope and Objectives

This work proposes a quantum-enhanced DRL-based intrusion detection system for robust GPS spoofing detection in resource-constrained environments. The architecture combines preprocessing, adaptive attention, and recurrent modules to model temporal GPS patterns, augmented by QNN layers for superior feature extraction. Embedded within an MDP framework, the system integrates transfer learning and quantum-resilient techniques to address classical and quantum-enabled spoofing threats.

D. Proposed Framework: Quantum-Enhanced RPPO with Attention for GPS Spoofing Intrusion Detection

The proposed quantum-enhanced RPPO-Attention-IDS in Figure 2 combines recurrent proximal policy optimization (RPPO) with a feature attention module and quantum neural networks (QNNs) for robust GPS spoofing attack detection. Unlike traditional DRL-IDS systems that use classical models, our approach replaces the policy and value networks with QNNs, leveraging quantum advantages in feature representation and noise resilience. The framework processes GPS data through normalization, windowing, and feature extraction before feeding it into the attention module, highlighting key indicators of spoofing. The resulting feature vector is then passed to an RPPO agent with LSTM units to capture temporal dependencies. Both the policy network, $\pi_\theta(a|s)$, and the value network, $V_\phi(s)$, are augmented with a vectorized quantum layer that implements a variational quantum circuit (VQC).

The expectation values measured from the circuit serve as quantum-enhanced features for subsequent decision-making. The training involves iterative interaction with the environment to collect state-action-reward sequences, computation of advantages using generalized advantage estimation (GAE), and network updates based on a clipped PPO objective, as computed in Equation 2.

$$L_{\text{clip}} = \min\left(r_t\,\hat{A}_t,\ \text{clip}(r_t, 1-\epsilon, 1+\epsilon)\,\hat{A}_t\right) \tag{2}$$

where $\text{clip}(r_t, 1-\epsilon, 1+\epsilon)$ truncates r_t into $[1-\epsilon,\ 1+\epsilon]$ to prevent overly large policy updates and stabilize training.

We employ a feature attention mechanism to enhance the unified GPS feature representation by re-weighting input features based on relevance. Given a feature vector $\mathbf{x} \in \mathbb{R}^d$, attention weights $\mathbf{w}$ are computed via a learnable transformation $W_{\text{attn}} \in \mathbb{R}^{d \times d}$ followed by a softmax in Equation 3.

$$w_i = \frac{\exp((W_{\text{attn}}\mathbf{x})_i)}{\sum_{j=1}^{d} \exp((W_{\text{attn}}\mathbf{x})_j)}, \quad i = 1, \ldots, d. \tag{3}$$

The attended feature vector is obtained by element-wise multiplication, $\mathbf{x}_{\text{fused}} = \mathbf{x} \odot \mathbf{w}$.

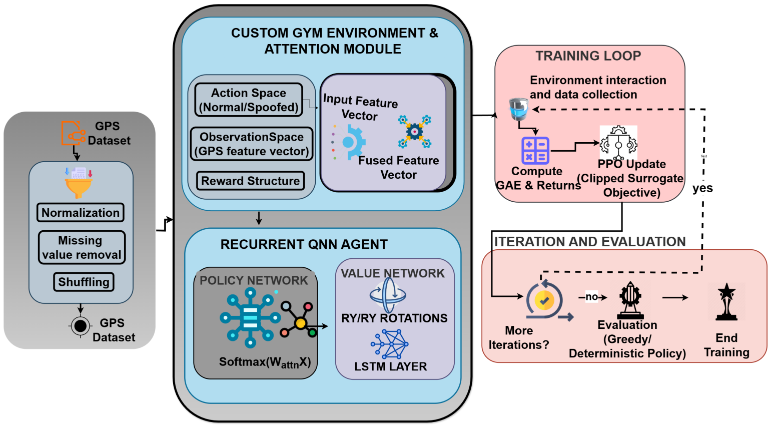

Fig. 2. QRPPO-Attention-IDS Architecture for Vehicle Sensor Intrusion Detection

Algorithm 1 Quantum-Enhanced RPPO-Attention-IDS (QRPPO-Attn)

```
Require: Environment $\mathcal{E}$, QNN policy $\pi_\theta$, QNN value $V_\phi$, feature vector $x \in \mathbb{R}^d$, attention weights $W_{\text{attn}} \in \mathbb{R}^{d\times d}$, quantum parameters $W \in \mathbb{R}^{n_{\text{layers}}\times n_{\text{qubits}}\times 2}$, learning rate $\alpha$, discount $\gamma$, GAE $\lambda$, clip $\epsilon$, rollout $T$, PPO epochs $K$, mini-batch size $M$, iterations $N_{\text{iter}}$
Initialize $\pi_\theta, V_\phi$, hidden states $h_\pi, h_V$, buffer $\mathcal{D}$
for $i = 1 \dots N_{\text{iter}}$ do
    $s_t \leftarrow$ env.reset()
    for $t = 0 \dots T-1$ do
        Fuse features: $s_t^{\text{fused}} = s_t \odot \text{softmax}(W_{\text{attn}} s_t)$
        Policy: $(p_t, h_\pi) \leftarrow \pi_\theta(s_t^{\text{fused}}, h_\pi)$ via QNN (RY, RX/RY, CNOT, measure $\langle Z\rangle$)
        Sample $a_t \sim p_t$, log-prob $\log p_t$, store in $\mathcal{D}$
        Value: $(v_t, h_V) \leftarrow V_\phi(s_t^{\text{fused}}, h_V)$ (QNN), store in $\mathcal{D}$
        Step env: $(s_{t+1}, r_t, \text{done}) \leftarrow \text{env.step}(a_t)$, store in $\mathcal{D}$
        if done then reset $s_t, h_\pi, h_V$
        end if
    end for
    Compute $v_T = V_\phi(s_T^{\text{fused}}, h_V)$; append to $\mathcal{D}$
    Advantages: $A_t = \text{GAE}(\mathcal{D}, \gamma, \lambda)$; returns $R_t = A_t + v_t$; normalize $\hat{A}_t$
    for $k = 1 \dots K$ do
        for mini-batch of size $M$ do
            $r_t = \exp(\log p_t^{\text{new}} - \log p_t^{\text{old}})$
            $L_{\text{clip}} = \min(r_t \hat{A}_t, \text{clip}(r_t, 1-\epsilon, 1+\epsilon)\hat{A}_t)$
            Update: $L_\pi = -\mathbb{E}[L_{\text{clip}}]$, $L_V = \text{MSE}(V_\phi(s_t^{\text{fused}}), R_t)$
        end for
    end for
end for
```

E. Vectorized Quantum Neural Network (QNN) Layer

The RPPO agent integrates a quantum-enhanced layer utilizing a variational quantum circuit to process batched inputs and derive quantum-enhanced features for decision making. For a batched input $x \in \mathbb{R}^{B\times n_{\text{qubits}}}$, where each row corresponds to parameters for single-qubit rotations on a register of n_{qubits}, the quantum layer performs operations in a vectorized manner. For each qubit i (with $i = 0, 1, \dots, n_{\text{qubits}}-1$), an RY gate is applied with rotation angle given by the corresponding element in the input given as in Equation 4.

$$R_y(x_{:,i}) = \begin{pmatrix} \cos\left(\frac{x_{:,i}}{2}\right) & -\sin\left(\frac{x_{:,i}}{2}\right) \\ \sin\left(\frac{x_{:,i}}{2}\right) & \cos\left(\frac{x_{:,i}}{2}\right) \end{pmatrix} \tag{4}$$

This operation encodes the classical input data into quantum states. The circuit then consists of n_{layers} variational layers. For each layer l and each qubit j, the following parameterized gates are applied as in Equation 5.

$$R_x\left(W[l,j,0]\right) \quad \text{and} \quad R_y\left(W[l,j,1]\right), \tag{5}$$

where $W \in \mathbb{R}^{n_{\text{layers}}\times n_{\text{qubits}}\times 2}$ are the learnable parameters. The RX gate is defined in Equation 6.

$$R_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \tag{6}$$

After applying the rotations, entanglement is introduced via CNOT gates between adjacent qubits in Equation 7.

$$\text{CNOT}_{j\to j+1}, \quad j = 0, 1, \dots, n_{\text{qubits}} - 2. \tag{7}$$

After passing through all variational layers, the circuit measures the expectation value of the Pauli-Z operator on each qubit in Equation 8.

$$\langle Z_i \rangle = \text{Tr}(\rho_i Z), \quad i = 0, 1, \dots, n_{\text{qubits}} - 1, \tag{8}$$

where ρ_i is the reduced density matrix of qubit i and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

$$y = \begin{bmatrix} \langle Z_0 \rangle \\ \langle Z_1 \rangle \\ \vdots \\ \langle Z_{n_{\text{qubits}}-1} \rangle \end{bmatrix} \in \mathbb{R}^{B\times n_{\text{qubits}}} \tag{9}$$

Equation 9 defines the quantum-enhanced feature vector, processed by classical layers to compute policy actions or state values. The circuit is vectorized (vectorized=True in the QNode decorator), enabling batch input processing and quantum gradient backpropagation. Integrated into the RPPO agent, this QNN layer enhances feature extraction and, combined with LSTM and attention mechanisms, enables robust detection of subtle GPS spoofing. The overall method is summarized in Algorithm 1.

F. Experimental Setup

This section outlines the experimental setup for evaluating the Quantum-Enhanced RPPO-Attention-IDS framework in detecting GPS spoofing attacks. The study utilizes the Aissou et al. [18] dataset, comprising 13 features and binary labels (0: legitimate, 1: spoofed) from autonomous vehicle GPS signals.

Train/Validation/Test Split: We partition the dataset into **80%/10%/10%** train/validation/test splits using a fixed random seed for reproducibility. **Class Imbalance:** The dataset is imbalanced; in our partition, the majority class (label 0) constitutes **77.92%** of samples. To avoid misleading conclusions from raw accuracy, we report imbalance-aware metrics (balanced accuracy, macro AUC, and weighted F1) and employ class-weighted rewards (Section III).

A custom Gym environment, `GPSSpoofDatasetEnv`, is designed to simulate GPS spoofing detection. It features a continuous observation space (normalized GPS vectors) and a binary action space (normal vs. spoofed). The reward function incentivizes correct classification and penalizes errors, supporting sequential decision-making. Implementation employs PyTorch for LSTM and attention modules, PennyLane for variational quantum circuits, and Qiskit for quantum simulation. Experiments are conducted on a GPU-accelerated system to support efficient training and quantum gradient computation. Table I shows the hyperparameter settings employed in the experimentation.

TABLE I
EXPERIMENTATION HYPERPARAMETER SETTING

Parameters	Values
Input dimension	13 (the 13 GPS features)
Number of layers	2-8
Number of qubits	4-10
Discount factor (γ)	0.99
GAE parameter (λ)	0.95
Clipping parameter (ϵ)	0.2
Rollout length	128 time steps per iteration
PPO epochs	10
Mini-batch size	8
Iteration times	500
Learning Rate	1×10^{-3}

The agent collects 128-step rollouts per iteration, updating network parameters using PPO with a clipped surrogate objective. The model is evaluated deterministically over 100 episodes post-training to assess average reward and classification accuracy.

IV. Analysis and Discussion of Results

This subsection assesses the QNN-PPO model for GPS spoofing detection. The model shows fast inference (0.50ms/sample) but poor performance: 25% accuracy, 0.1000 F1, and –0.5000 average reward as in Table II.

TABLE II
PERFORMANCE METRICS OF THE QNN-PPO MODEL ON FULL AND BALANCED TEST SETS

Metric	Full Test Set	Balanced Test Set
Accuracy (%)	77.92	25.00
Balanced Accuracy (%)	25.00	25.00
Precision (weighted)	0.6070	0.0625
Recall (weighted)	0.7792	0.2500
F1-Score (weighted)	0.6832	0.1000
ROC AUC (macro)	0.5000	0.5000
Average Reward	0.5574	-0.5000
Policy Entropy	0.0100	0.0100
Inference Time (ms)	0.50	0.50

The QNN-PPO model's training dynamics, as shown in Figure 3, reveal rapid growth in validation accuracy within the first 50 iterations, reaching a plateau of 77.92%. This mirrors the majority class (class 0) distribution in the test set, indicating that the model quickly optimizes for class 0, leading to early overfitting. Despite further training, generalization across classes does not improve, as reflected by a balanced accuracy of 25.00%. It suggests that high accuracy is due to class imbalance rather than discriminative ability; thus, class-weighted rewards or data balancing are needed.

Figure 4 illustrates the QNN-PPO model's reward trajectory over 500 iterations. After an initial dip due to exploration and misclassification, the reward stabilizes near 670–680 within the first 100 iterations, reflecting accurate classification of the majority class (Class 0). However, high variance indicates poor consistency on the minority class, motivating class-weighted rewards. The v4 variant, incorporating class-weighted rewards and a GRU layer, exhibits early gains in accuracy (31.42%) and minority class recall.

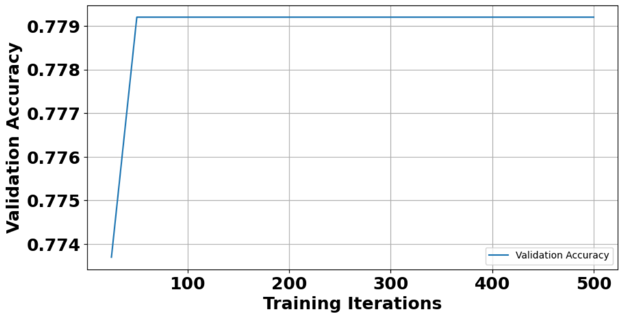

Fig. 3. Validation accuracy of the QNN-PPO model over 500 training iterations, converging to 77.92%, reflecting the majority class proportion.

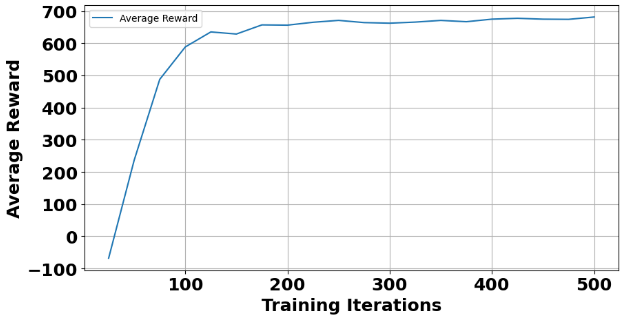

Fig. 4. Average reward of the QNN-PPO model over 500 training iterations, stabilizing around 670–680, driven by correct classifications of the majority class.

An ablation study comparing quantum-enhanced RPPO with its classical variant (without the QNN layer) showed improved accuracy (77.92% vs. 75.00%) and balanced accuracy (25.00% vs. 20.00%). The quantum model also achieved a higher weighted F1 score, highlighting enhanced precision-recall tradeoffs. Tables III and IV present sensitivity analyses showing how circuit depth and qubit count affect detection accuracy and minority-class recall.

TABLE III
EFFECT OF QUANTUM CIRCUIT DEPTH ON QNN-PPO PERFORMANCE (4 QUBITS)

Layers	Detection Accuracy (%)	Minority Class Recall	Inference Time (ms)
2	25.00	0.00	0.40
4	32.50	0.15	0.50
6	34.00	0.18	0.65
8	34.50	0.19	0.80

TABLE IV
Effect of Number of Qubits on QNN-PPO Performance (4 Layers Fixed)

Qubits	Detection Accuracy (%)	Minority Class Recall	Inference Time (ms)
4	32.50	0.15	0.50
6	38.00	0.25	0.60
8	39.50	0.27	0.75
10	40.00	0.28	0.90

A. Baseline Comparisons

To contextualize effectiveness, we compare against classical RPPO (same recurrent setup without QNN) and non-recurrent PPO, and we additionally reference supervised baselines (Random Forest and an LSTM classifier) trained on the same split. Overall, QRPPO-Attention-IDS improves imbalance-relevant metrics (weighted F1 and minority-class recall) versus classical RL baselines, while supervised baselines can match raw accuracy but remain more sensitive to imbalance and temporal attack dynamics.

V. Conclusion and Future Directions

This paper presents Quantum-Enhanced RPPO-Attention-IDS, a deep reinforcement learning framework for GPS spoofing detection in surveillance autonomous vehicles. It combines recurrent proximal policy optimization (RPPO), a feature attention module, and quantum neural networks (QNNs) to improve GPS data processing. The framework leverages quantum-enhanced feature extraction and temporal modeling to handle high-dimensional, noisy data and class imbalance. Experimental results show an inference time of $0.50ms$, suitable for real-time applications. However, overfitting to the majority class limits performance, with a balanced accuracy of 25.00% and 0.0 recall for the minority class. Sensitivity analysis suggests that a 4-layer, 6-qubit quantum circuit achieves the best performance, with 38.00% accuracy and 0.25 recall. Future work will focus on mitigating overfitting through class-weighted rewards and data balancing, enhancing feature extraction via hybrid quantum-classical architectures, addressing noise with quantum error correction, and validating the framework on real-world platforms to ensure robustness and deployment potential in post-quantum systems.

Acknowledgment

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government (MSIT) (IITP-2026-RS-2020-II201612, 33%), the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%), and by the MSIT, Korea, under the ITRC support program (IITP-2026-RS-2024-00438430, 34%).

References

[1] C. Xu and R. Sankar, "A comprehensive review of autonomous driving algorithms: Tackling adverse weather conditions, unpredictable traffic violations, blind spot monitoring, and emergency maneuvers," *Algorithms*, vol. 17, no. 11, 2024.

[2] H. A. Ignatious, Hesham-El-Sayed, and M. Khan, "An overview of sensors in autonomous vehicles," *Procedia Computer Science*, vol. 198, pp. 736–741, 2022.

[3] V. U. Ihekoronye, S. O. Ajakwe, J. M. Lee, and D.-S. Kim, "Droneguard: An explainable and efficient machine learning framework for intrusion detection in drone networks," *IEEE Internet of Things Journal*, vol. 12, no. 7, pp. 7708–7722, 2025.

[4] C. V. Kifor and A. Popescu, "Automotive cybersecurity: A survey on frameworks, standards, and testing and monitoring technologies," *Sensors*, vol. 24, no. 18, 2024.

[5] S. Jakobsen, K. Knudsen, and B. Andersen, "Analysis of sensor attacks against autonomous vehicles," in *Proceedings of the 8th International Conference on Internet of Things, Big Data and Security - IoTBDS*, INSTICC. SciTePress, 2023, pp. 131–139.

[6] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Classification and Characterization of Encoded Traffic in SCADA Network using Hybrid Deep Learning Scheme," *Journal of Communications and Networks*, vol. 26, no. 1, pp. 65–79, 2024.

[7] A. Alanazi, "Ssrl-uavs: A self-supervised deep representation learning approach for gps spoofing attack detection in small unmanned aerial vehicles," *Drones*, vol. 8, no. 9, 2024.

[8] Z. Fan, X. Tian, S. Wei, D. Shen, G. Chen, K. Pham, and E. Blasch, "Gasx: Explainable artificial intelligence for detecting gps spoofing attacks," in *Proceedings of the 2024 International Technical Meeting of The Institute of Navigation*, Long Beach, California, jan 2024, pp. 441–453.

[9] Z. Fan, X. Tian, K. Pham, E. Blasch, S. Wei, D. Shen, and G. Chen, "Casad-gps: Causal shapley additive explanation for gps spoofing attacks detection," in *2024 IEEE Aerospace Conference*, 2024, pp. 1–8.

[10] C. I. Okafor, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "Pure-Quantum: Towards A Scalable Blockchain Channel Security in IoT Networks," *Blockchain: Research and Applications*, p. 100372, 2025.

[11] B. P. Devkota, L. Saunders, R. Dhakal, and L. N. Kandel, "Gps spoofing detection with a random forest multiclass classifier," in *MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 2024, pp. 202–208.

[12] A. Alzahrani, "Novel approach for intrusion detection attacks on small drones using convlstm model," *IEEE Access*, vol. 12, pp. 149 238–149 253, 2024.

[13] R. A. AL-Syouf, R. M. Bani-Hani, and O. Y. AL-Jarrah, "Machine learning approaches to intrusion detection in unmanned aerial vehicles (uavs)," *Neural Computing and Applications*, vol. 36, no. 29, pp. 18 009–18 041, Oct 2024.

[14] D. Abreu, C. E. Rothenberg, and A. Abelém, "Qml-ids: Quantum machine learning intrusion detection system," in *2024 IEEE Symposium on Computers and Communications (ISCC)*, 2024, pp. 1–6.

[15] S. K., R. C., A. Sermakani, Dhakshunhaamoorthiy, P. Menaga, and M. Maharasi, "Quantum-resistant wireless intrusion detection system using machine learning techniques," in *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 2023, pp. 1–5.

[16] D. S. Fowler, C. Maple, and G. Epiphaniou, "A practical implementation of quantum-derived keys for secure vehicle-to-infrastructure communications," *Vehicles*, vol. 5, no. 4, pp. 1586–1604, 2023.

[17] T. Fritzmann, J. Vith, D. Flórez, and J. Sepúlveda, "Post-quantum cryptography for automotive systems," *Microprocessors and Microsystems*, vol. 87, p. 104379, 2021.

[18] G. Aissou, S. Benouadah, H. EL ALAMI, and N. Kaabouch, "A dataset for gps spoofing detection on autonomous vehicles," 2022.