IRIS: Propulsion Aware Secrecy Energy Optimization in Dynamic RIS Assisted UAV IoT Networks

Candida Y[1], Dr. K. Sudhaman[2], Dr. J. Ann Roseela[3], Dr. C. Sharanya[4*]

[1] Research Scholar, Department of ECE, Dr. M.G.R. Educational and Research Institute, India.
Email: candida.jenish@gmail.com

[2] Professor, Department of ECE, Dr. M.G.R. Educational and Research Institute, India.

[3] Professor, Department of ECE, Dr. M.G.R. Educational and Research Institute, India.

[4] Associate Professor, Department of ECE, Sathyabama Institute of Science and Technology, India.

Corresponding Author:

Candida Y[1]*
Email: candida.jenish@gmail.com

Abstract: The use of reconfigurable intelligent surfaces (RIS) and Unmanned Aerial Vehicles (UAVs) has started to become a viable solution for secure and energy efficient communication in IoT networks. However, most of the current approaches concentrate on the aspect of secrecy performance only and neglect the aspect of propulsion energy and the evolvable wireless environment, which have a significant impact on practical UAV system. In this work, a learning driven framework called IRIS (Intelligent Reconfigurable Integrated Security) is introduced to handle this issue through propulsion-aware secrecy-energy optimization. This research piece tackles the problem of jointly optimizing the trajectory of the UAV, the transmit power and the RIS phase configuration, with the help of reinforcement learning and enables the system to adapt continuously as the network conditions evolve. To estimate its performance IRIS is compared with PPO, TD3, SAC, DDPG, and DQN algorithms. The simulation outcomes confirm significant improvements with nearly 3.32 bits/s/Hz secrecy rate, 3.51 bits/J energy efficiency and quick convergence, without any communication delay in dynamic IoT scenarios.

Keywords: Reconfigurable Intelligent Surface (RIS); Unmanned Aerial Vehicle (UAV); Internet of Things (IoT); Physical Layer Security; Reinforcement Learning; Secrecy-Energy Optimization; Propulsion-Aware Communication; Energy Efficiency

Introduction

Unmanned aerial vehicles (UAVs) are becoming popular as flexible aerial platforms in next generation wireless communication. They can provide on demand coverage, easily change positions and immediately deploy, making them particularly well suited for Internet of Things (IoT) environments, especially in areas where the ground infrastructure is limited or unavailable. But, when UAV is used in IoT systems, there are severe security problems to be addressed because of the massive dissemination of wireless signals, particularly by passive eavesdroppers, all trying to intrude on the data. Therefore, secure communication in UAV assisted IoT networks is a crucial issue for the direction of 6G wireless networks [1] and [3].

Reconfigurable Intelligent Surfaces (RIS) are a new technology that has potential applications for enhancing the delivery of wireless signals as well as boosting the security of communications. They

work by allowing an RIS to adjust the phase of the reflected electromagnetic wave dynamically, allowing them to control a wireless channel without having to transmit an active radio frequency signal. These systems would therefore be able to amplify the signal for the authorized users while not allowing that signal to be leaked to the unauthorized users using the RIS devices. Many studies have been conducted to demonstrate that the use of RISs in the deployment of wireless networks enhances the secrecy performance of wireless networks deployed with RISs, and the spectral efficiency of the wireless networks in which RISs are deployed [11, 14].In addition the mobility of RISs and the UAVs on which they are deployed will allow for additional degrees of freedom to be used to support adaptive beamforming and trajectory optimization and providing increased reliability and security of the deployed systems.

Research interest on the combination of Reconfigurable Intelligent Surfaces (RIS) and Unmanned Aerial Vehicles (UAVs) has attracted a lot of attention recently [36]. The work done in the past has focused on aspects of joint trajectory planning of UAVs, beamforming and distributing resources in UAV-RIS enabled communication systems. The joint optimization of UAV paths and beamforming for secure communications with RIS as an enhancement was analyzed in [1].[2] used deep reinforcement learning (DRL) techniques to control the trajectory of UAV for RIS assisted Internet of Things (IoT) networks. In the same way [8] investigated multi UAV communication structures using RIS, to enhance the secure transmission of information. Combined, these literature studies show that the combination of UAV mobility and intelligent wireless environments will have a great positive impact in communication performance.

Although progress has been made there are still some major hurdles to overcome. The current security frameworks for RIS-UAV focus mainly on achieving the maximum secrecy rate, without explicitly considering reliability requirements for IoT devices. For some IoT communications, low power sensors are used for delay sensitive data, secure and reliable connections are required [37]. Moreover, UAV energy consumption is largely related to propulsion power, but most of the studies in the literature fail to consider the relationship between the mobility of the UAV and communication energy efficiency [36]. Lastly, most optimization techniques use deterministic algorithms that are not feasible in a dynamic wireless network with numerous control parameters.

Deep Reinforcement Learning (DRL) has been proposed as a potential solution to solve the complex optimization problems in wireless communication networks. It enables agents to adaptively control by interacting with the environment, which can be useful in situations where analytical solutions are hard to find. In recent reviews, several features of DRL's capabilities were recognized in various aspects of wireless resource management, trajectory planning and smart network operation in next generation systems [10],[31]. The characteristics of these qualities render DRL particularly useful for UAV communication systems supporting RIS, the channel conditions, UAV mobility and hostile conditions are subject to frequent variations.

Based on a forementioned findings, this research proposes an IoT-aware reinforcement learning framework for secure communication systems for UAVs assisted by RIS. The primary purpose is to improve secrecy energy efficiency defined as the secrecy throughput that can be achieved divided by the total power consumption of the UAV, including secrecy communication and propulsion energy. This method takes into account the reliability of IoT communication and a worst-case secrecy scenario from passive eavesdroppers, unlike the traditional approach, which only uses secrecy rate. However, the optimization problem is highly non-convex because of the complex relationship between UAV trajectory, the distribution of the transmit power and the phase adjustment of RIS [38].

To tackle these challenges, a novel learning framework called IRIS-DRL is proposed. It sees the UAV controller as an autonomous agent which observes the wireless environment and optimizes its trajectory, transmission power, RIS configuration using reinforcement learning. The design is composed of energy efficient trajectory management, reliability centred secrecy enhancement and adaptive RIS phase control in a single learning system. This framework is designed to improve the security aspect of UAV based IoT networks by optimizing both mobility and reconfigurable wireless channels.

The key findings of this study are the development of an IoT aware secrecy energy-efficiency optimization model for RIS-assisted UAV communications while taking into account both UAV propulsion energy and the reliability of IoT devices [7]. Moreover, a reinforcement learning framework is proposed to jointly optimize the RIS phase configuration, transmit power and UAV trajectory in a variable wireless environment. This study also integrates a worst case eavesdropper model into the learning process to strengthen physical layer security without requiring exact knowledge of adversarial channels. Lastly, the framework compares static and dynamic RIS deployment strategies to improve secrecy performance in UAV enabled IoT networks.

The rest of this paper is organized as follows: The related research focused on RIS assisted secure UAV communication and learning based wireless optimization techniques are summarized in Section II. The system model and the formulation of channel are described in Section III. In Section IV, the proposed reinforcement learning framework and optimization approach is introduced. The implementation of the algorithm and the learning process are explained in Section V. The results and performance evaluation of the simulation are discussed in section VI. Finally, the conclusions are presented in Section VII.

Related Work

Reconfigurable Intelligent Surfaces (RIS) are emerging as a promising technology to improve the performance of wireless communication systems and physical layer security in conjunction with the recent deployment of Unmanned Aerial Vehicles (UAVs). Through the use of UAV mobility and programmable wireless environments, RIS assisted UAV systems can dynamically adjust the propagation of the signal to get better communication reliability. Secure communication strategies, trajectory optimization and learning based resource allocation are some of the previous studies analyzed for RIS-UAV networks. However, most of the existing works focus mainly on either maximizing the secrecy rate or optimizing the trajectory while overlooking Internet of Things (IoT) traffic patterns, UAV propulsion energy usage and reliability requirements. In order to show the differences between previous studies and the proposed design, a comparison of representative studies is presented in Table I.

Reference	**System Model**	**Optimization Objective**	**Method**	**Key Limitation**
Yang et al. [1]	UAV + STAR-RIS	Secrecy rate maximization	Joint trajectory and beamforming optimization	No IoT device modelling
Wang et al. [2]	RIS-assisted UAV IoT	UAV trajectory optimization	Deep reinforcement learning	Energy consumption is not considered
Li et al. [3]	Static vs dynamic RIS deployment	Secrecy performance comparison	Analytical evaluation	No learning-based optimization
Wu et al. [4]	Multi-UAV RIS communication	Secure communication design	Convex optimization	Limited scalability
Iqbal et al. [5]	RIS-UAV networks	Resource allocation	DRL-based optimization	The UAV energy model was ignored

Cui et al. [6]	RIS-UAV integrated sensing	Joint communication and sensing	Optimization-based control	No secrecy energy efficiency analysis
Wei et al. [8]	Multi-UAV RIS networks	Secure transmission optimization	Coordinated trajectory design	No IoT reliability consideration
Nguyen et al. [17]	UAV-RIS NOMA systems	Secure communication	Deep reinforcement learning	Simplified energy model
Liu et al. [24]	RIS-UAV communication	Energy-efficient transmission	Phase optimization	UAV mobility is not optimized
My Work	RIS-assisted UAV IoT network	Secrecy energy efficiency	IoT-aware DRL framework	Joint mobility, power, and RIS control

Table I: Comparison with Representative RIS–UAV Secure Communication Studies

Comparative Analysis and Research Gaps

Table I shows some recent advancements that have been made in developing secure communication in RIS assisted UAV networks. Several works have been directed towards joint trajectory design and beamforming optimization for increasing the secrecy rate [1, 4]. There have been other approaches to learning such as those using deep reinforcement learning to adapt UAV paths or control communication resources in dynamic environments [2, 5]. Furthermore, recent study has focused on the combination of RIS with UAV platforms for the better connectivity reliability and coverage in future wireless systems [6] and [8]. But there are some significant challenges to be addressed. Most research focuses on the problem of optimizing the secrecy rate, while reliability requirements for IoT systems are not taken into consideration. IoT systems will have to cope with low power devices that require stable and secure connections. Second, the effects of UAV propulsion energy and communication performance are rarely taken into account and have a tremendous potential to influence overall system efficiency. Finally, the mobility of UAVs, RIS settings and the reliability of IoT communication have not been fully explored.

In these developments, my study introduces an IoT aware reinforcement learning methodology that jointly optimises the UAV trajectory, transmit power and RIS phase which maximises secrecy energy efficiency. This approach incorporates reliability aware communication modelling, UAV propulsion energy factors to offer a more implementable and scalable approach to secure UAV enabled IoT networks.

System Model

The system considered here is a UAV supported communication system for multiple ground IoT devices, in the presence of possible eavesdroppers. A Reconfigurable Intelligent Surface (RIS) is used in the covered area to optimize the propagation and increase reliability of the communication. The mobile transmitter for the UAV remains at a fixed altitude, but its horizontal position varies with time depending on the mission. The configuration of the RIS at a specific time t is given by its position vector $\mathbf{q}(t) = [x(t), y(t)]$ and the diagonal $\mathbf{\Phi}(t) = \mathrm{diag}\left(e^{j\theta_1(t)}, \dots, e^{j\theta_N(t)}\right)$. where each element is a passive reflecting element with a controllable phase shift. It is assumed that the channel environment is block fading in which the channel gains are constant within a time slot and random between the time slots because of UAV motion.

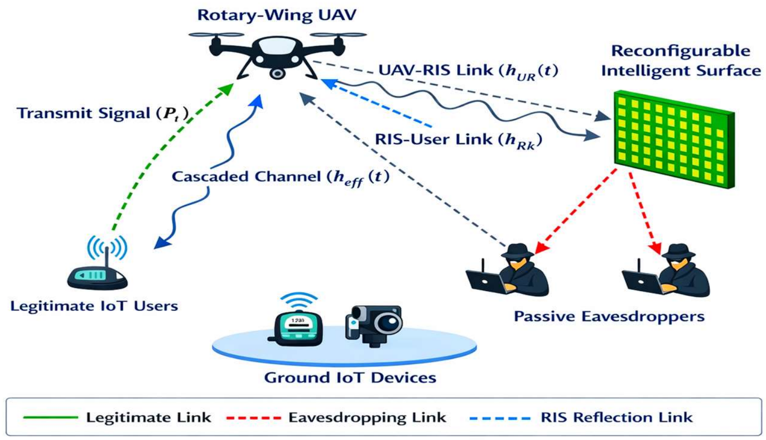

Fig 1: RIS-assisted UAV-enabled IoT communication network

The signal propagation between the UAV and each IoT device depends on the spatial separation between them. The distance between the UAV and the k- The device at the time $t$is given by

$$d_{u,k}(t) = \sqrt{(x(t) - x_k)^2 + (y(t) - y_k)^2 + h^2}, \tag{1}$$

where h denotes the UAV altitude. The corresponding channel coefficient is modeled as the product of large-scale attenuation and small-scale fading, expressed as

$$h_{u,k}(t) = \sqrt{\beta_{u,k}(t)}\, g_{u,k}(t), \tag{2}$$

where the path loss term is defined as

$$\beta_{u,k}(t) = \beta_0 / d_{u,k}(t)^{\alpha}, \tag{3}$$

and $g_{u,k}(t)$represents the random fading component. A similar formulation is used for the UAV–RIS link, where the channel is expressed as

$$\mathbf{g}_{u,r}(t) = \sqrt{\beta_{u,r}(t)}\, \mathbf{g}(t), \tag{4}$$

with path loss determined by the UAV–RIS distance. The RIS-to-IoT channel is described as $\mathbf{h}_{r,k} = \sqrt{\beta_{r,k}}\, \mathbf{h}_k$, where the fading vector captures random propagation effects between the reflecting surface and the ground device.

The overall communication link between the UAV and each IoT device comprises two components: the direct transmission path and the reflected path via the RIS. These two contributions combine to form an effective channel, expressed as

$$H_k(t) = h_{u,k}(t) + \mathbf{h}_{r,k}^H \boldsymbol{\Phi}(t) \mathbf{g}_{u,r}(t). \tag{5}$$

The same structure models the channel to an eavesdropper, considering both direct and reflected signal components. This integrated channel representation enables the RIS to manage signal propagation, enhancing signals to legitimate devices while reducing unintended exposure.

The quality of the received signal at each IoT device is characterized by the signal-to-noise ratio, defined as

$$\gamma_k(t) = \frac{P_t |H_k(t)|^2}{\sigma^2}, \tag{6}$$

where $P_t$denotes the UAV transmit power and σ^2represents the noise variance. From this, the achievable data rate is defined by

$$R_k(t) = B \log_2\left(1 + \gamma_k(t)\right) \tag{7}$$

where $B$is the system bandwidth. The eavesdropper rate is defined similarly to the legitimate communication rate, and can be expressed as

$$R_{e,m}(t) = B \log_2 \left(1+\frac{P_t |H_{e,m}(t)|^2}{\sigma^2}\right). \tag{8}$$

Given that obtaining precise channel-state information for passive eavesdroppers is typically the method that involves taking a cautious approach by assuming the worst-case scenario, interception scenario, where the eavesdropper's rate is regarded as the highest among all potential eavesdroppers, as defined by

$$R_e^{\text{worst}}(t) = \max_{m \in \mathcal{M}} \; R_{e,m}(t). \tag{9}$$

Thus, the secrecy rate is the non-negative difference between the legitimate communication rate and the maximum eavesdropper rate, and it can be expressed as

$$C_s(t) = [R_k(t) - R_e^{\text{worst}}(t)]^+, \tag{10}$$

where $[x]^+ = \max(x, 0)$. This formulation guarantees robustness despite uncertainty in interception channels.

Besides communication performance, the UAV's energy consumption is also important, especially for practical uses. For rotary-wing UAVs, most energy is used for propulsion, which depends on the UAV's flight speed. The propulsion power is modeled as a nonlinear function of velocity and can be expressed as

$$P_{\text{prop}}(t) = P_0 \left(1+\frac{3v(t)^2}{U_{\text{tip}}^2}\right) + P_i \left(\sqrt{1+\frac{v(t)^4}{4v_0^4}} - \frac{v(t)^2}{2v_0^2}\right)^{\frac{1}{2}} + \frac{1}{2} d_0 \rho s A v(t)^3, \tag{11}$$

which models the impact of blade profile, power, induced power, and aerodynamic drag. The total power consumption at each time interval is then calculated by summing propulsion power with communication transmit power, expressed as

$$P_{\text{total}}(t) = P_{\text{prop}}(t) + P_t. \tag{12}$$

To assess the system's overall efficiency, secrecy energy efficiency is described as the ratio of the total secrecy throughput accumulated to the total energy used during the operation period, expressed as

$$SEE = \frac{\sum_{t=1}^{T} C_s(t)}{\sum_{t=1}^{T} P_{\text{total}}(t)}. \tag{13}$$

This metric captures the trade off between ensuring secure communication and reducing energy consumption, which is especially crucial in UAV assisted IoT networks with limited onboard energy resources.

Optimization Problem

The objective is to create a transmission scheme that will allow securing of the communication in an energy efficient manner in the face of dynamic environment within the existing system model. The effective channel conditions due to the trajectory of the UAV transmit power and RIS phase settings affect the secrecy rate and energy consumption. These variables are closely correlated with each other via the wireless channel and the motion of the UAV and cannot be optimized by optimizing one variable at a time. Thus, the interaction of UAV mobility and flexible wireless propagation will necessitate joint optimization approach to reap the benefits from such flexibility.

For this purpose, the system performance is tested in terms of secrecy energy efficiency, defined as the compromise between secure communication throughput and energy consumed. The objective of optimization is to maximize this value, where the UAV trajectory $\mathbf{q}(t)$, transmit power P_t, and RIS phase configuration $\mathbf{\Phi}(t)$ are optimized jointly over the entire operational period. We can write this problem as

$$\max_{\{\mathbf{q}(t),P_t,\mathbf{\Phi}(t)\}_{t=1}^{T}} SEE \tag{14}$$

subject to practical system constraints. The transmit power is limited by

$$0 \leq P_t \leq P_{\max}, \forall t, \tag{15}$$

ensuring that the UAV stays within its hardware limits. The UAV's mobility is constrained by its maximum speed, given by

$$\| \mathbf{q}(t+1) - \mathbf{q}(t) \| \leq V_{\max}\Delta t, \forall t, \tag{16}$$

which indicates the physical constraints on UAV movement. The RIS phase shifts are limited to specific discrete values because of hardware limitations, represented as

$$\theta_n(t) \in \left\{0, \frac{2\pi}{2^b}, \dots, \frac{(2^b-1)2\pi}{2^b}\right\}, \forall n, t, \tag{17}$$

were b represents the number of quantization bits. Additionally, the UAV's total energy consumption throughout the mission must adhere to the specified requirements.

$$\sum_{t=1}^{T} P_{\text{total}}(t)\Delta t \leq E_{\max}, \qquad 18)$$

which guarantees that the UAV stays within its energy limits.

The optimization problem defined above is extremely nonconvex for several reasons. The secrecy rate depends on the difference between the legitimate and eavesdropper channels, thereby introducing nonlinearity. Additionally, the interaction among UAV trajectories, RIS phase shifts, and channel gains results in complex coupling among variables. The fractional form of the secrecy energy efficiency objective further complicates the issue. These factors make traditional optimization techniques challenging, particularly in dynamic settings. Therefore, a learning based approach is employed, capable of managing high-dimensional decision spaces and adjusting to changing system conditions.

Intelligent Learning-Based Control Framework for Secure UAV–RIS Communications

The optimization problem for secure communication outlined earlier involves jointly managing the UAV trajectory, transmission power, and RIS phase settings. These factors influence the wireless environment and impact the system's secrecy performance. Finding the optimal control method is difficult because wireless channels fluctuate dynamically due to UAV movement, environmental scattering, and interference. Moreover, the RIS's programmable features introduce many controllable elements greatly increasing the complexity of the optimization task.

This research presents an adaptive learning framework, IRIS (Intelligent Reconfigurable Integrated Security), designed to address these challenges. The primary concept of IRIS is to enable unmanned aerial vehicles (UAVs) to develop secure communication strategies by interacting with the wireless environment and continuously monitoring communication performance. Rather than solving a deterministic optimization problem at each juncture the UAV incrementally learns how variations in trajectory, transmit power, and RIS phase configurations influence the secrecy rate and energy consumption. Recent developments demonstrate that reinforcement learning is effective for managing such sequential decision-making tasks in wireless systems [10]. The IRIS framework consolidates environmental observation, decision-making, and policy training within a single control loop that continuously improves the communication strategy.

A. System Interaction Architecture

The IRIS framework operates through the interaction of the UAV agent, the RIS controller, and the wireless communication environment. The UAV acts as the decision-maker, assessing the network's current state and choosing control actions. These actions affect the communication environment by adjusting the UAV's position, transmission power, and RIS reflection settings. Figure 4 illustrates the overall system architecture. In this configuration, the UAV communicates with ground IoT devices and legitimate users, while potential eavesdroppers try to intercept signals. The RIS enhances the communication link by tuning its reflection coefficients to improve signal propagation toward the intended receiver.

The reinforcement learning module receives system-state information, including UAV position, channel state, and received signal quality. Using this data, the IRIS learning engine generates control actions that jointly determine UAV trajectory, transmission power, and RIS phase configuration. This interaction between the learning agent and the wireless environment enables the system to refine its communication strategy and improve secure transmission performance continuously. Similar RIS-assisted UAV architectures have been explored in recent studies to enhance communication reliability and coverage [1], [4].

B. Markov Based IRIS Framework

The dynamic control problem is represented as a Markov Decision Process (MDP), offering a mathematical framework for solving sequential decision-making issues. In this model, the communication system progresses through a series of states, actions, and rewards.

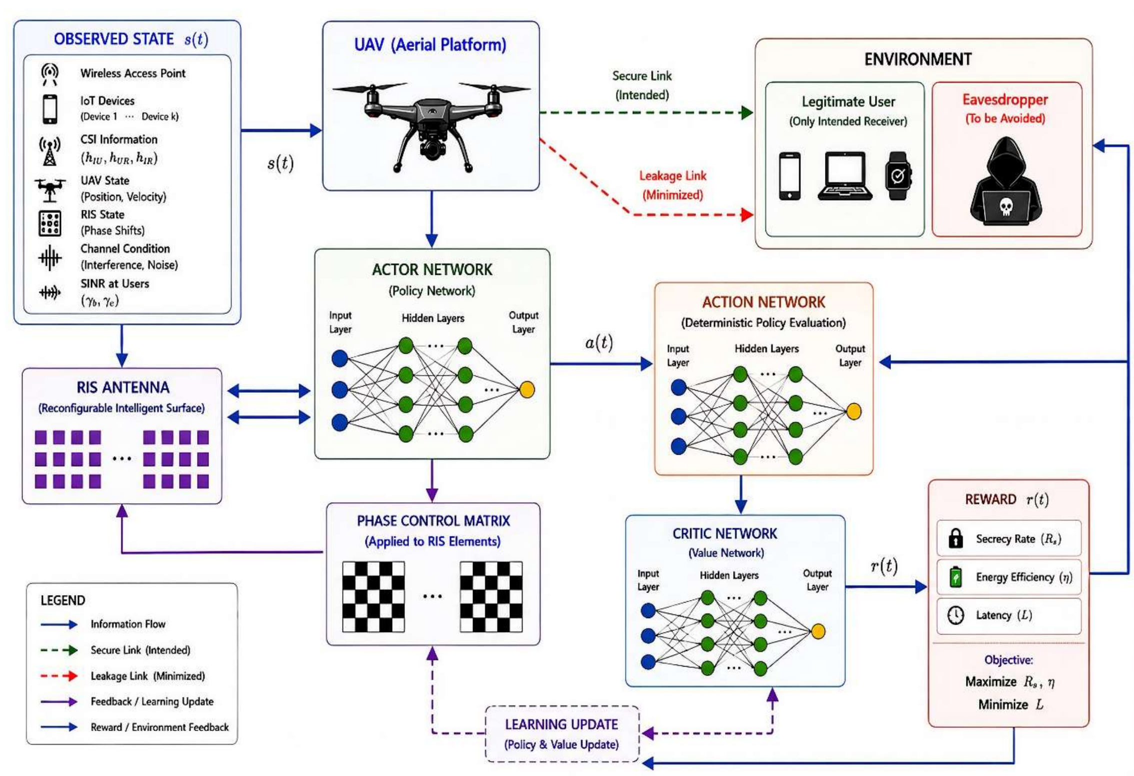

Fig. 4: IRIS System Architecture

The tuple defines the MDP

$$\mathcal{M} = (S, A, P, R, \gamma)$$
(19)

Were S denotes the state space, A represents the action space, $P(s_{t+1} \mid s_t, a_t)$represents the state transition probability, $R(s_t, a_t)$denotes the reward function, and $\gamma \in (0,1)$is the discount factor. At time step t, the UAV observes the system state $s_t$and selects an action a_t. The environment then transitions to a new state $s_{t+1}$and provides a reward r_t. The objective of the learning agent is to determine a policy π that maximizes the expected cumulative reward

$$J(\pi) = \mathbb{E}\left[\sum_{t=0}^{T} \gamma^t r_t\right] \quad (20)$$

This approach allows the UAV to develop long-term communication tactics that enhance secrecy while conserving energy.

To enable effective decision-making, the state vector must include essential information for assessing communication performance and guiding control decisions. In the UAV–RIS network under consideration, the system state comprises spatial data, channel conditions, and received signal quality.

The system state at time step t is defined as

$$s_t = [\mathbf{p}_u(t), \mathbf{h}_{IU}(t), \mathbf{h}_{UR}(t), \mathbf{h}_{IR}(t), \gamma_b(t), \gamma_e(t)] \quad (21)$$

Were $\mathbf{p}_u(t)$represents the three-dimensional position of the UAV, $\mathbf{h}_{IU}(t)$denotes the IoT-to-UAV channel vector, $\mathbf{h}_{UR}(t)$represents the UAV-to-RIS channel vector, $\mathbf{h}_{IR}(t)$represents the RIS-to-user channel vector. The signal-to-interference-plus-noise ratio (SINR) at the legitimate user is expressed as

$$\gamma_b(t) = \frac{P_t |h_b(t)|^2}{\sigma^2 + I_b} \quad (22)$$

while the SINR at the eavesdropper is expressed as

$$\gamma_e(t) = \frac{P_t |h_e(t)|^2}{\sigma^2 + I_e} \quad (23)$$

To capture real-world wireless conditions, imperfect channel estimation is considered. The estimated channel coefficient can be modeled as $\hat{h} = h + \epsilon$ where $\epsilon \sim \mathcal{CN}(0, \sigma_\epsilon^2)$ represents the channel estimation error.

The learning agent's control action dictates how the communication environment changes. In this framework, the action encompasses UAV trajectory adjustment, transmission power allocation, and RIS phase configuration. The action vector is defined as:

$$a_t = [\Delta x_t, \Delta y_t, P_t, \boldsymbol{\theta}_t] \quad (24)$$

Were $\Delta x_t$and Δy_trepresent UAV displacement in the horizontal plane, $P_t$denotes the transmission power, $\boldsymbol{\theta}_t = [\theta_1, \theta_2, \dots, \theta_N]$represents RIS phase shifts.

The UAV position evolves according to

$$x_u(t+1) = x_u(t) + \Delta x_t$$
$$y_u(t+1) = y_u(t) + \Delta y_t \quad (25)$$

subject to the mobility constraint

$$\sqrt{(\Delta x_t)^2 + (\Delta y_t)^2} \le V_{max} \Delta t \quad (26)$$

were V_{max}denotes the maximum UAV velocity.

Besides controlling mobility, the RIS improves wireless communication by modulating the phase of incoming electromagnetic waves. Its reflection characteristics can be described using a diagonal phase matrix.

$$\Phi = \mathrm{diag}\left(e^{j\theta_1}, e^{j\theta_2}, \dots, e^{j\theta_N}\right) \quad (27)$$

The effective channel between the transmitter and receiver through the RIS becomes

$$h_{eff} = h_d + \mathrm{h}_{UR}^T \Phi \mathrm{h}_{IR} \quad (28)$$

were $h_d$denotes the direct communication channel.

In practical RIS hardware, phase shifts are limited to discrete values due to circuit constraints. Each reflecting element supports a specific set of phase states, determined by the hardware resolution [11]. Consequently, the phase shift is constrained by this limitation.

$$\theta_n \in \left\{0, \frac{2\pi}{2^b}, \dots, \frac{(2^b-1)2\pi}{2^b}\right\} \tag{29}$$

were b denotes the number of quantization bits.

The reward function, based on SINR expressions, guides the learning process by assessing the quality of each control decision. It must account for both secrecy performance and energy efficiency.

The achievable secrecy rate is defined as

$$R_s(t) = \left[\log_2\left(1+\gamma_b(t)\right) - \log_2\left(1+\gamma_e(t)\right)\right]^+ \tag{30}$$

Beyond the UAV's energy consumption, it also includes communication power and propulsion energy.

$$E_t = P_t + P_{prop}(t) \tag{31}$$

The instantaneous reward is therefore defined as

$$r_t = \alpha R_s(t) - \beta E_t \tag{32}$$

were $\alpha$and βrepresent weighting coefficients that balance secrecy performance and energy efficiency.

The UAV agent interacts with the communication environment through an iterative learning process. In each cycle, it observes the system state, determines a control action, and updates its policy based on the feedback.

C. Algorithm Implementation

The IRIS framework uses an actor–critic reinforcement learning architecture to jointly optimize UAV trajectory, transmit power, and RIS phase configuration. The actor network has three fully connected layers with 256, 128, and 64 neurons, each followed by ReLU activation. The output layer produces continuous control actions for UAV movement, transmit power, and RIS phase shifts.

The critic network uses a similar structure and takes both state and action as input to estimate the Q value function. Both networks are trained using the Adam optimizer with a learning rate of 10−410^{-4}10−4 for the actor and 10−310^{-3}10−3 for the critic.

Key hyperparameters include a discount factor $\gamma = 0.99$, mini-batch size of 64, replay buffer size of 10^5, and Gaussian exploration noise with decaying variance.

The complete learning procedure of the IRIS framework is summarized in **the algorithm.**

Algorithm 1: IRIS Secure Communication Learning Framework

Input:

Environment parameters

RIS configuration

UAV mobility constraints

Learning rate α

Discount factor γ

```
   Replay memory capacity D
Output:
   Optimized secure communication policy μ*
Initialize actor network μ(s|θμ)
Initialize critic network Q(s,a|θQ)
Initialize target actor network μ′
Initialize target critic network Q′
Initialize replay memory D
Initialize UAV position pu(0)
Initialize RIS phase matrix Φ(0)
for episode = 1 to N do
    Reset wireless environment
    Observe initial state st
    for each time step t do
        Generate action using actor policy
        at = μ(st|θμ) + Nt
        Update UAV trajectory
        Update RIS phase shifts
        Adjust transmission power
        Compute legitimate user SINR γb(t)
        Compute eavesdropper SINR γe(t)
        Compute secrecy rate
        Rs(t)=[log2(1+γb(t))−log2(1+γe(t))]+
        Compute total energy consumption Et
        Compute energy efficiency
        η(t) = Rs(t) / Et
        Evaluate communication latency L(t)
        Compute reward
        rt = αRs(t) + βη(t) − λL(t)
        Observe next state st+1
        Store transition
        (st, at, rt, st+1) → D
        Sample mini-batch from replay memory
        Compute target value
        yt = rt + γQ′(st+1, μ′(st+1))
        Update critic network by minimizing
        L = E[(yt − Q(st,at))^2]
        Update actor network using
```

36: deterministic policy gradient

37: Update target networks

38: st ← st+1

39: end for

40: end for

41: Return optimized policy μ*

The IRIS framework continuously interacts with the wireless environment, gradually learning communication strategies that improve secure transmission while preserving energy efficiency.

D. Policy Optimization and Learning Framework of IRIS

To link the optimization problem described in Section IV with the IRIS learning framework, the policy parameters are tuned to enhance the system's long-term secrecy and energy efficiency.

Let the policy be parameterized by θ. The learning objective can be written as

$$J(\theta) = \mathbb{E}_{s_t, a_t \sim \pi_\theta}\left[\sum_{t=0}^{T} \gamma^t r_t\right] \tag{33}$$

Were r_t represents the reward defined in the previous subsection, γ denotes the discount factor, T represents the decision horizon.

The optimal policy parameters are obtained by solving.

$$\theta^* = \arg\max_{\theta} \quad J(\theta) \tag{34}$$

Because the transition dynamics of the wireless environment are unpredictable and evolve, expected outcomes are estimated from trajectories obtained through interaction. To address this, the IRIS framework employs an actor–critic learning approach to determine the optimal policy. The actor network then generates the control action.

$$a_t = \mu(s_t \mid \theta^\mu) \tag{35}$$

while the critic network estimates the value of each state–action pair

$$Q(s_t, a_t \mid \theta^Q) \tag{36}$$

The critic network is trained by minimizing the temporal-difference loss.

$$L(\theta^Q) = \mathbb{E}[(y_t - Q(s_t, a_t \mid \theta^Q))^2] \tag{37}$$

were the target value is computed as

$$y_t = r_t + \gamma Q\big(s_{t+1}, \mu(s_{t+1} \mid \theta^\mu)\big) \tag{38}$$

The actor network parameters are updated using the deterministic policy gradient.

$$\nabla_{\theta^\mu} J = \mathbb{E}[\nabla_a Q(s, a) \nabla_{\theta^\mu} \mu(s)] \tag{39}$$

These gradients direct the learning policy toward control actions that enhance the secrecy-energy efficiency of the communication system. To promote thorough exploration of the action space during training, exploration noise is added to the actor's output, encouraging the agent to try various control strategies.

Therefore, the action performed within the environment is

$$a_t = \mu(s_t \mid \theta^{\mu}) + \mathcal{N}(0, \sigma_t) \quad (40)$$

were $\mathcal{N}(0, \sigma_t)$represents Gaussian exploration noise.

The exploration variance steadily decreases over time.

$$\sigma_t = \sigma_0 e^{-\lambda t} \quad (41)$$

Were $\sigma_0$represents the initial exploration variance, λcontrols the decay rate.

This mechanism enables the agent to explore extensively during initial training phases, then progressively shift towards exploiting the learned policy. The primary source of computational complexity in the IRIS framework comes from training the actor and critic networks.

Let $N_a$and N_c represent the number of parameters in the actor and critic networks, respectively. The computational complexity per training iteration is approximately.

$$\mathcal{O}(N_a + N_c) \quad (42)$$

In a system with N number of RIS elements and M number of $With$ UAVs, the dimensionality of the action space becomes

$$\mid A \mid = 2M + M + N \quad (43)$$

which grows linearly with the number of controllable system components. While this increase in dimensionality can lead to extra computational overhead, the modular design of the IRIS framework enables its extension to larger networks. For large-scale deployments with multiple UAVs or RIS panels, approaches like distributed learning or multi-agent reinforcement learning can help ensure scalability.

Simulation Results and Performance Assessment

In this section, we analyze the performance of the developed IRIS framework for secure communication in RIS enabled UAV-IoT networks. MATLAB simulations are used, where the UAV acts as a transmitter receiving information collected from several IoT nodes that are uniformly placed within the covered area. In order to provide secure communication, an intelligent reconfigurable surface (RIS) helps enhance the transmission by reflecting signals towards intended users and restricting them from being leaked to the passive eavesdropper. All parameters used in the simulations are listed. They are provided in Table 2.

Parameter	**Value**
UAV Initial Position	(0, 0, 200) m
RIS Location	(200, 0, 50) m
IoT Deployment Area	Radius = 500 m
Number of IoT Devices (N)	10
UAV Type	Rotary-wing
UAV Altitude Range	100 – 300 m
Maximum UAV Speed	20 m/s
Time Slot Duration	1 s
Carrier Frequency	2 GHz
Transmit Power Range	1 – 5 W
System Bandwidth (B)	1 MHz

Noise Power Spectral Density	-90 dBm
Path Loss Exponent	2.2
Number of RIS Elements	64
RIS Phase Resolution	2-bit discrete (4 levels)
DRL Framework	Actor–Critic (IRIS)
Discount Factor ((\gamma))	0.99
Number of Episodes	2000
Replay Buffer Size	(10^5) samples
Mini-batch Size	64
Exploration Strategy	Gaussian noise
Monte Carlo Runs	100
Evaluation Metrics	Secrecy Rate, Energy Efficiency, Latency
Benchmark Algorithms	PPO, TD3, DDPG, DQN, SAC

Table 2: Simulation Parameters

A. Convergence behavior of the Learning Algorithms

The figure below demonstrates how the considered learning algorithms converge and shows secrecy energy efficiency as a function of the number of training episodes.

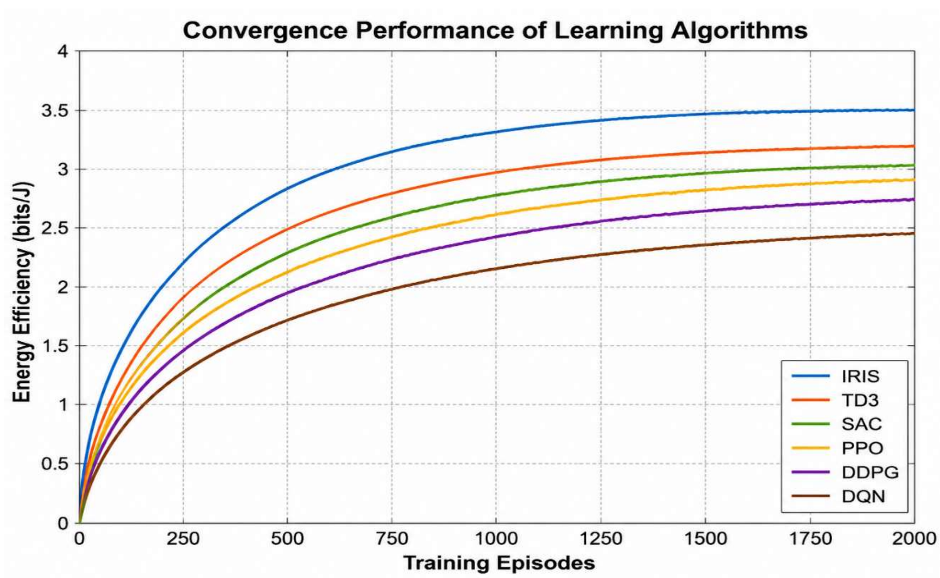

Fig 3: Convergence Performance Comparison Graph

Initially, while the training process begins, all models show some level of fluctuations while exploring different strategies for UAV movement and RIS phase shifts through reinforcement learning. The period during which all learning models explore different possibilities is seen until 200 episodes, after which all models show a steady increase in their performance levels. The proposed IRIS framework reaches the state of convergence faster than other algorithms, taking around 1100 episodes to achieve convergence. On the other hand, both PPO and TD3 require almost 1500 episodes, while DDPG and DQN need more than 1700 episodes because of their lower capability for dealing with continuous control variables. After achieving convergence, the IRIS model achieves a secrecy-energy efficiency level of 3.5 bits/J, which is almost 13% better than TD3 and 18% better than PPO.

Table II summarizes the overall performance comparison of the considered algorithms. The proposed IRIS framework attains the highest secrecy rate and energy efficiency, while also offering faster convergence and lower latency than the benchmark reinforcement learning algorithms.

Performance comparison of different learning algorithms

Algorithm	**Secrecy Rate (bits/s/Hz)**	**Energy Efficiency (bits/J)**	**Latency (ms)**	**Convergence Episodes**
IRIS (Proposed)	**3.32**	**3.51**	**18.6**	**1100**
TD3	3.05	3.12	21.4	1500
SAC	2.98	3.04	22.8	1450
PPO	2.92	2.97	23.6	1500
DDPG	2.85	2.83	25.2	1700
DQN	2.63	2.71	27.5	1800

Table 3: Overall performance comparison with TD3, SAC, PPO, DDPG, and DQN

B. Secrecy Rate Performance

The secrecy rate performance of the algorithms analyzed is shown in the following figure. At the same time, the number of IoT devices is fixed at **N = 10**.

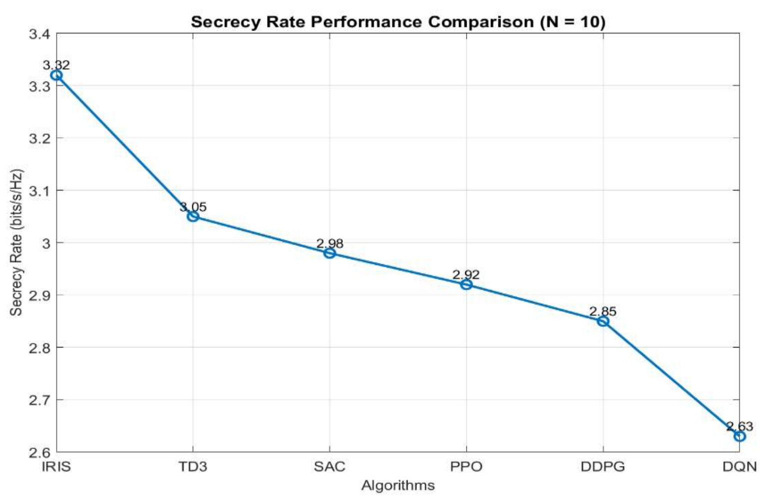

Fig 4: Secrecy rate performance comparison when the number of IoT devices is 10

In terms of secrecy rate, the IRIS scheme performs better than the other considered algorithms with a secrecy rate of about 3.32 bits/Hz. On the other hand, the secrecy rates of TD3 and SAC amount to 3.05 and 2.98 bits/Hz, respectively. The secrecy rates for PPO and DDPG equal 2.92 bits/Hz and 2.85 bits/Hz, whereas that of DQN is about 2.63 bits/Hz. In this regard, there is an improvement of about 9% for TD3 with respect to IRIS, while the increase for PPO is close to 14%.

C. Energy Efficiency Analysis

The performance of the energy efficiency for the studied algorithms can be seen in the figure below. Energy efficiency can be described as the ratio between the possible throughput of communications and the total energy consumption of the communication network of unmanned aerial vehicles (UAV). Since UAV systems are energy-limited devices, increasing energy efficiency becomes a necessary target for the system design. It should be noted that IRIS outperforms all other algorithms in terms of energy efficiency. For example, the energy efficiency of the IRIS framework reaches the value of 3.51 bits/J on average, while for TD3 and SAC, it is approximately 3.12 bits/J and 3.04 bits/J. In turn, PPO and DDPG produce the values of 2.97 bits/J and 2.83 bits/J, respectively, while DQN results in the energy efficiency of 2.71 bits/J.

Thus, IRIS demonstrates a higher level of energy efficiency than TD3 by approximately 12%, and almost 18% more than PPO. The higher energy efficiency of the algorithm is achieved due to joint optimization of the UAV trajectory and phase configuration of the reconfigurable intelligent surface (RIS).

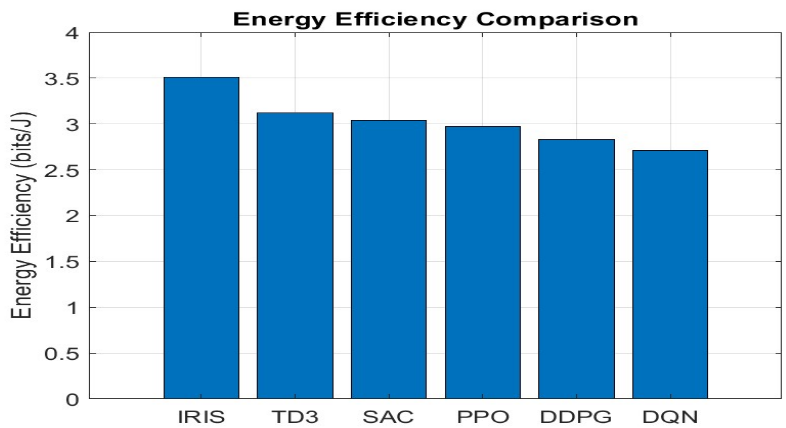

Fig 5: Energy efficiency comparison of IRIS with other benchmarking algorithms

D. Latency Performance

The communication latency of the considered algorithms is illustrated in Fig. 6.

Latency is defined as the time needed for an Unmanned Aerial Vehicle (UAV) to create a successful connection and acquire information from IoT devices. Reducing latency is necessary for real-time applications of IoT technologies for emergencies and disaster management purposes. The IRIS algorithm is found to have the lowest communication latency among all evaluated algorithms. For instance, IRIS provides an average communication latency of about 18.6 m/s, whereas, on the other hand, TD3 and PPO provide a delay of about 21.4 m/s and 23.6 m/s, respectively. DDPG and DQN algorithms take even more time owing to inefficient convergence and decision-making processes.

In summary, communication latency using IRIS is about 13% lower than that using TD3 and about 21% lower than that using PPO.

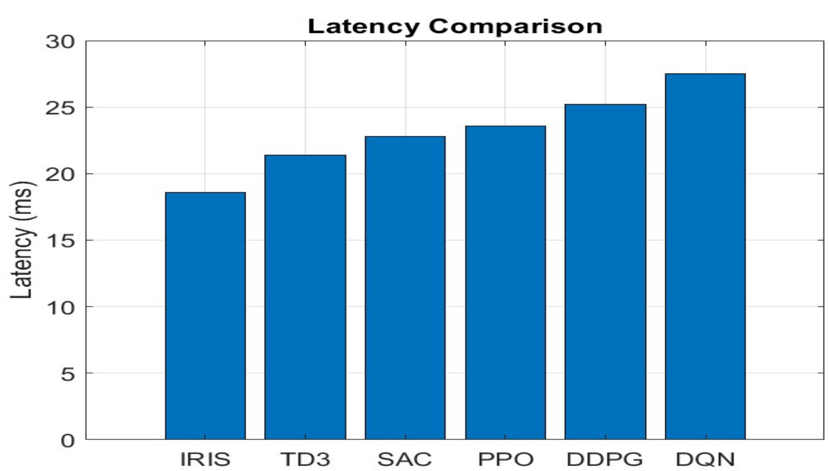

Fig 6: Latency Performance comparison of IRIS with other benchmarking algorithms

E. Impact of UAV Altitude on Secrecy Rate

Next, we present the secrecy rate performance for different UAV altitudes in **Fig. 5**.

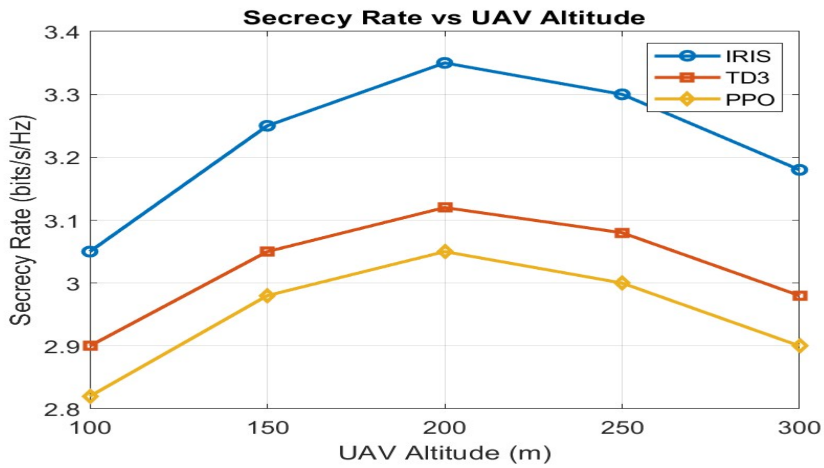

Fig 7: Secrecy rate performance under different UAV altitude values

This sensitivity analysis includes only the IRIS, TD3, and PPO algorithms. The secrecy rate increases as the UAV altitude rises from 100 m to about 200 m, where the IRIS framework reaches a maximum of approximately 3.35 bits/s/Hz. This gain results from a higher probability of line-of-sight communication between the UAV and IoT devices. Above 200 m, the secrecy rate declines due to increased path loss. These findings suggest there is an optimal UAV altitude for maximizing secure communication.

F. Energy Efficiency vs Transmit Power

Finally, the relationship between transmit power and energy efficiency is illustrated in the following figure. Energy efficiency increases as transmit power rises from 1 W to about 4 W because higher transmit power improves communication reliability. The proposed IRIS framework achieves an energy efficiency of about 3.5 bits/J at 5 W, higher than TD3 (3.18 bits/J) and PPO (3.05 bits/J). However, the improvement saturates at higher power levels since higher transmit power increases energy consumption.

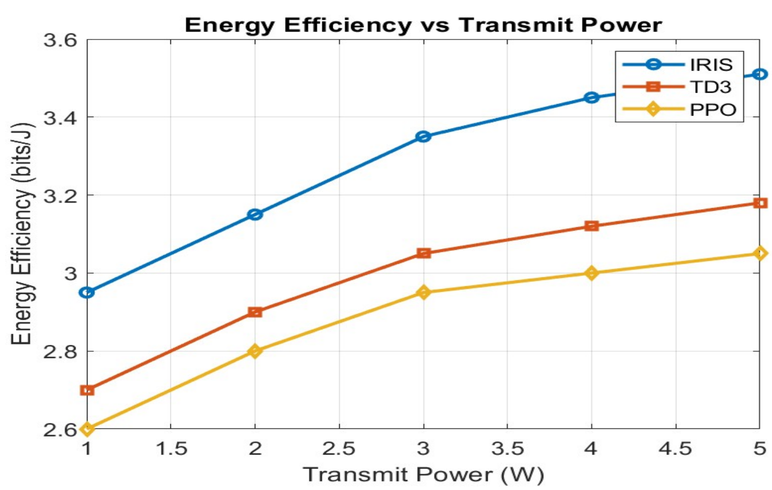

Fig 8: Relationship between transmit power and energy efficiency

Several conclusions can be made based on the findings. First, the introduced IRIS framework has the best secrecy rate and energy efficiency out of all analysed algorithms. Second IRIS is more prone to converge faster than the conventional reinforcement learning algorithms. Third there is a significant reduction in the communication delay due to improved decision making. Fourth, the secrecy performance depends heavily on the number of RIS elements and the altitude of the UAV.

Conclusion:

In this study, we propose a learning framework, namely IRIS (Intelligent Reconfigurable Integrated Security), to improve the secure transmission through UAV-assisted RIS-empowered Internet-of-Things network by intelligently optimizing the UAV trajectory, transmit power, and phase shift of the RIS. By leveraging the reinforcement learning scheme, IRIS can adapt to varying wireless channels, resulting in a better performance compared to conventional learning techniques such as PPO, TD3, DDPG, SAC, and DQN. Simulation results demonstrate that IRIS consistently achieves a better secrecy rate (around 3.32 bits/Hz) and higher energy efficiency (3.51 bits/J) with 14%-18% improvements over other schemes. Moreover, IRIS not only converges faster but also incurs reduced latency which makes this scheme applicable to real-world IoT systems. The analysis on the effects of important parameters, such as the UAV height, the number of RIS elements, and the transmitting power, also confirms the significance of employing mobile devices combined with controllable wireless propagation environments in improving physical layer security and energy efficiency.

References

H. Yang, Z. Xiong, J. Tsai, C. Fang, D. Niyato, H. Ji, and V. C. M. Leung, Aug. 2023 "Joint optimization for STAR-RIS-assisted UAV secure communication," IEEE Journal on Selected Areas in Communications, vol. 41, no. 8, pp. 2456–2470.

T. Wang, Z. Wei, X. Zhou, W. Xu, J. Yuan, and M. Ding, Jan. 2024 "Deep reinforcement learning-based UAV trajectory optimization for secure RIS-assisted IoT networks," IEEE Transactions on Vehicular Technology, vol. 73, no. 1, pp. 1234–1249.

S. Li, Y. Zhang, Z. Xiong, and D. Niyato, Apr. 2024 "Static vs. dynamic RIS deployment: Performance comparison in secure UAV networks," IEEE Wireless Communications Letters, vol. 13, no. 4, pp. 1234–1238.

F. Wu, J. Xu, Y. Zeng, and R. Zhang, Aug. 2024 "Secure multi-UAV communication with RIS assistance," IEEE Transactions on Communications, vol. 72, no. 8, pp. 5678–5693.

H. Iqbal, M. Asad, S. Mumtaz, and J. Rodriguez, Jan. 2025. "Deep reinforcement learning-based resource allocation for secure RIS-UAV communication," IEEE Access, vol. 13, pp. 12345–12360.

Y. Cui, X. Li, H. Ji, and V. C. M. Leung, Feb. 2026 "RIS-UAV integrated sensing and communication for 6G networks," IEEE Transactions on Vehicular Technology, vol. 75, no. 2, pp. 2345–2360.

Miao, J., Chen, H., Li, H. & Bai, S. (2023). Secrecy Energy Efficiency Enhancement in UAV-Assisted MEC System. Sensors 23(2). https://doi.org/10.3390/s23020723.

Z. Wei, F. Gao, W. Xu, and A. Nallanathan, Feb. 2025 "Coordinated multi-UAV RIS deployment for secure communication," IEEE Journal on Selected Areas in Communications, vol. 43, no. 2, pp. 456–472.

X. Mu, Y. Zhang, J. Xu, and R. Zhang, Jan. 2025. "Joint trajectory and beamforming optimization for UAV secure communications with passive coupled phase-shift/active STAR-RIS," Digital Signal Processing, vol. 152, Art. no. 104567.

L. G. Jaimes, S. Bhattacharjee, A. K. Gupta, and T. Q. S. Quek, Second Quarter 2023. "Deep reinforcement learning for wireless communications: An overview," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1234–1278.

H. V. Cheng, C. Huang, H. Wang, H. Zhang, E. Björnson, A. L. Swindlehurst, and C. Yuen, Mar. 2023. "Practical deployment of reconfigurable intelligent surfaces: Principles, challenges, and future perspectives," IEEE Transactions on Antennas and Propagation, vol. 71, no. 3, pp. 2345–2359.

Z. Xiao, L. Zhu, Y. Choi, P. Xia, and X.-G. Xia, May 2023 "Joint power allocation and passive beamforming design for IRS-assisted UAV-enabled MEC," IEEE Transactions on Antennas and Propagation, vol. 71, no. 5, pp. 4567–4581.

A. Liu, Y. Zhang, Z. Xiong, J. Gao, Y. Zhang, and D. Niyato, Apr. 2023. "RIS-assisted UAV for fresh data collection in IoT networks," IEEE Transactions on Communications, vol. 71, no. 4, pp. 2345–2360.

S. Hu, F. Rusek, and O. Edfors, Dec. 2023. "Beyond massive MIMO: The potential of positioning with large intelligent surfaces," IEEE Journal on Selected Areas in Communications, vol. 41, no. 12, pp. 3789–3804.

J. Li, X. Chen, Y. Liu, and D. Niyato, May 2025 "Secure communication of UAV-mounted STAR-RIS under phase uncertainty," IEEE Transactions on Wireless Communications, vol. 24, no. 5, pp. 3456–3471.

M. Zhang, H. Yang, Z. Xiong, and D. Niyato, Jun. 2025"Enhancing reliable and energy-efficient UAV communication with RIS," IEEE Transactions on Vehicular Technology, vol. 74, no. 6, pp. 4567–4582.

K. Nguyen, T. Q. Duong, and Ö. Özdagoglu, Feb. 2025. "RIS-assisted UAV NOMA secure communication based on deep reinforcement learning," Physical Communication, vol. 62, Art. no. 102234.

P. Zhang, W. Xu, and M. Ding, Apr. 2025 "Intelligent beamforming for UAV-RIS communication systems," IEEE Transactions on Communications, vol. 73, no. 4, pp. 2345–2360.

Q. Wu, Y. Zeng, and R. Zhang, Mar. 2025 "STAR-RIS-assisted secure UAV communication: Joint trajectory and beamforming design," IEEE Journal on Selected Areas in Communications, vol. 43, no. 3, pp. 567–582.

L. You, X. Mu, and H. V. Poor, Feb. 2025 "Active STAR-RIS for secure UAV-ground user communication," IEEE Transactions on Information Theory, vol. 71, no. 2, pp. 1234–1250.

F. Liu, Z. Wei, and A. Nallanathan Jul. 2025, "Multi-agent DRL for secure multi-UAV STAR-RIS networks," IEEE Transactions on Wireless Communications, vol. 24, no. 7, pp. 4567–4582.

H. Yang, J. Tsai, and V. C. M. Leung, Apr. 2025 "Joint sensing, communication, and security optimization for UAV-STAR-RIS-ISAC," IEEE Journal on Selected Areas in Communications, vol. 43, no. 4, pp. 789–804.

X. Zhou, T. Wang, and J. Yuan, Aug. 2025 "Trajectory optimization for secure UAV communication with discrete RIS phase shifts," IEEE Transactions on Vehicular Technology, vol. 74, no. 8, pp. 6789–6804.

M. Asad, H. Iqbal, and S. Mumtaz, May 2025 "Imperfect CSI-aware secure resource allocation for RIS-UAV networks," IEEE Access, vol. 13, pp. 23456–23471.

Y. Liu, S. Li, and Z. Xiong, May 2025 "Dynamic RIS phase configuration for energy-efficient UAV communication," IEEE Wireless Communications Letters, vol. 14, no. 5, pp. 1234–1239.

R. Zhang, J. Xu, and Y. Zeng, Jul. 2025 "Secure multi-user UAV communication with STAR-RIS: A game-theoretic approach," IEEE Transactions on Communications, vol. 73, no. 7, pp. 4567–4582.

E. Björnson, Ö. T. Demir, and H. V. Cheng, Oct. 2025 "Channel estimation for STAR-RIS-assisted UAV networks," IEEE Transactions on Signal Processing, vol. 73, no. 10, pp. 5678–5693.

D. Niyato, Z. Xiong, and Y. Zhang, Jun. 2025 "Federated learning for secure RIS-UAV resource management," IEEE Communications Magazine, vol. 63, no. 6, pp. 123–130.

W. Saad, M. Bennis, and H. Ji, Jul. 2025 "6G vision: STAR-RIS and UAV integration for secure IoT," IEEE Network, vol. 39, no. 4, pp. 234–245.

M. Di Renzo, E. Basar, and M.-S. Alouin , Aug. 2025 "STAR-RIS field trials: Practical deployment insights," Proceedings of the IEEE, vol. 113, no. 8, pp. 1567–1585.

T. Q. S. Quek, L. G. Jaimes, and A. K. Gupta, Third Quarter 2025 "AI-native wireless networks: DRL for UAV-RIS systems," IEEE Communications Surveys & Tutorials, vol. 27, no. 3, pp. 3456–3500.

C. Huang, G. C. Alexandropoulos, and A. L. Swindlehurst, Sep. 2025 "Energy-constrained RIS optimization for UAV networks," IEEE Transactions on Wireless Communications, vol. 24, no. 9, pp. 6789–6804.

J. Yuan, X. Zhou, and M. Ding, Oct. 2025 "Robust secure communication under UAV mobility constraints," IEEE Transactions on Vehicular Technology, vol. 74, no. 10, pp. 7890–7905.

V. C. M. Leung, H. Ji, and H. Yang, Oct. 2025 "Integrated sensing, communication, and security for 6G UAV networks," IEEE Journal on Selected Areas in Communications, vol. 43, no. 10, pp. 2345–2360.

A. Nallanathan, Z. Wei, and F. Gao, Dec. 2025. "Scalable multi-UAV coordination with RIS for 6G IoT," IEEE Transactions on Wireless Communications, vol. 24, no. 12, pp. 8901–8916.

Goh, C. Y., Leow, C. Y. & Nordin, R. (2023). Energy Efficiency of Unmanned Aerial Vehicle with Reconfigurable Intelligent Surfaces: A Comparative Study. Drones 7(2). https://doi.org/10.3390/drones7020098

Silva, C., Cunha, V. A., Barraca, J. P. & Aguiar, R. L. (2024). Analysis of the Cryptographic Algorithms in IoT Communications. Information Systems Frontiers 26. https://doi.org/10.1007/s10796-023-10383-9

Qin, X., Song, Z., Hou, T., Yu, W., Wang, J. & Sun, X. (2023). Joint Optimization of Resource Allocation, Phase Shift and UAV Trajectory for Energy-Efficient RIS-Assisted UAV-Enabled MEC Systems. IEEE Transactions on Green Communications and Networking 7, pp. 1778-1792.