IRS-Enhanced UAV Communication Networks: Securing Data with Hybrid Genetic and Gradient Descent Algorithms

Zina Chkirbene[1], Ala Gouissem[2], Ridha Hamila[1], Unal Devrim[3], Arafat Al-Dweik[4], Kaya Kuru[5]
[1] Electrical Engineering, Qatar University, Qatar,
[2] College of Computing and Information Technology, University of Doha for Science and Technology, Qatar,
[3]KINDI Center for Computing Research, College of Engineering, Qatar University, Qatar,
[4] Electrical Engineering and Computer Science at Khalifa University, UAE.
[5] School of Engineering, University of Central Lancashire, Preston, PR1 2HE, UK.

***Abstract*—In the rapidly advancing field of wireless communication, Unmanned Aerial Vehicles (UAVs) have become crucial due to their extensive coverage capabilities and ability to access remote locations. Deployed as mobile base (BSs) stations or relays, UAVs significantly enhance network throughput and reliability. Alongside UAVs, Intelligent Reflecting Surfaces (IRS) have surfaced as a cost-effective method to improve communication quality via passive modulation arrays. Despite these advances, the potential misuse of UAVs poses serious security risks, particularly in communication eavesdropping. Addressing these challenges, this paper introduces a novel communication framework that integrates a UAV equipped with an adaptive IRS. The primary aim is to boost communication secrecy BSs and multiple users, even in the presence of several UAV eavesdroppers. This goal is formulated as an optimization problem focused on maximizing the secrecy rate, while also considering UAV mobility constraints. To solve this non-convex problem, we propose a hybrid strategy that combines Genetic Algorithms and Gradient Descent techniques. This innovative approach efficiently calculates suboptimal reflection angles and UAV trajectories for IRS-equipped UAVs, thereby enhancing the security of the communication network. This method not only addresses the complexity of the optimization but also provides a practical pathway to secure communications in environments with high eavesdropping risks.**

Index UAV, IRS , secure communication, reflecting angle, secrecy rate, trajectory optimization.

I. Introduction

The rapid evolution of wireless communication systems, propelled by the transition from 5G to emerging 6G technologies, has opened up a plethora of optimization opportunities. These futuristic networks demand significantly increased bandwidth, elevated data transfer rates, reduced latency, and decreased energy consumption to support an expanding array of applications from ultra-reliable low-latency communications (URLLC) to massive machine-type communications (mMTC). Advanced methodologies like massive MIMO, Non-Orthogonal Multiple Access (NOMA), and Low Power Wide Area Network (LPWAN) have been developed to address these needs. However, their deployment faces substantial challenges, particularly at higher frequencies such as millimeter-wave bands, where system complexity and deployment costs are considerably heightened. To circumvent these hurdles, Intelligent Reflecting Surfaces (IRS) have emerged as a cost-effective approach to ensure persistent line-of-sight communications in highly dynamic environments [1], [2].

Simultaneously, the integrity of communication systems is continually challenged by a variety of risks, both malicious and accidental. Sectors as diverse as military operations, emergency response, connected automotive systems, and unmanned aerial vehicles (UAVs) depend critically on robust and secure wireless communications [3]. UAVs, for their part, have proven especially versatile, capable of providing expansive coverage over large areas and reaching remote or otherwise inaccessible locations. These attributes make UAVs ideal for roles such as mobile base stations (BSs) or communication relays, where they significantly enhance system throughput and reliability [4]. However, the innovative use of UAVs brings with it enhanced security challenges, most notably the risk of communication eavesdropping. This vulnerability has spurred a range of solutions aimed at safeguarding UAV communications. These include securing UAV-to-UAV links within large-scale fading channels [5], enhancing the detection of signals in environments with randomly positioned UAV eavesdroppers [6], and adopting a variety of tactics such as signal jamming, trajectory adjustments, and the deployment of artificial noise to improve secrecy rates [7].

In this context, the strategic deployment of IRS emerges as a particularly effective method for bolstering secure communications. By fine-tuning phase shifts, IRS enhances the Signal-to-Noise Ratio (SNR) for legitimate users without the need for increased power output, simultaneously impairing the reception quality for potential eavesdroppers [8]. This capability positions IRS as a formidable ally in UAV-centric communication systems, synergizing with UAV capabilities to elevate secrecy rates without additional energy consumption or significant resource allocation.

This paper proposes an optimized system architecture that integrates UAVs equipped with IRS, specifically designed to enhance secure communication under scenarios fraught with multiple legitimate users and potential eavesdroppers. We aim to maximize the secrecy rate, ensuring robust and secure

communications between UAVs (Eve) and legitimate users. The contributions of this paper are manifold:

- Introducing a novel system model that improves communication between legitimate users and a BS in the presence of eavesdroppers.
- Formulating the problem as a nonlinear optimization aimed at maximizing the secrecy rate, considering UAV (RIS) mobility constraints.
- Dynamically optimizing UAV (RIS) trajectory and IRS reflective angles to thwart eavesdropping attempts.
- Conducting extensive simulations to evaluate the system's performance across different network configurations.

The remainder of the paper is organized as follows: Section II presents our system model, while Section III formulates the problem for stationary and dynamic settings. Sections IV and V discuss IRS angle optimization and optimal UAV positioning, respectively. Section VI presents simulation results, and finally, Section VII concludes our study.

II. System Model

A. Network Topology

We consider a communication system wherein a UAV is equipped with an IRS (See Fig. 1). This system comprises a BS and multiple legitimate users, denoted by $\mathbf{U}$ with $\mathbf{U} \in \{1, 2, \ldots, u\}$, each equipped with a single antenna. Additionally, there exists a group of UAVs acting as eavesdroppers aiming to intercept the information of the legitimate users. In order to enhance communication secrecy, a dynamic IRS-equipped UAV is employed, featuring N reflecting cells with angles $\phi_1^n, \phi_2^n, \ldots, \phi_N^n$ at time n. The BS is positioned at coordinates $\mathbf{BS} = (0, 0, 0) \in \mathbb{R}^3$. Each legitimate user, denoted by u, occupies a predetermined location $\mathbf{d}_u$ units away from the BS, bearing coordinates $\mathbf{d}_u = (0, d_u, 0) \in \mathbb{R}^3$. The UAV eavesdroppers are assumed to occupy random positions within a hemisphere of radius R. Over each iteration, their positions are perturbed by Gaussian errors. Each eavesdropper, indexed by k, is positioned as described by $\mathbf{e}_k = (x_e^k, y_e^k, z_e^k) \in \mathbb{R}^3$.

Unlike the fixed BS and the legitimate users, the IRS has a time-dependent position represented by $\mathbf{IRS}(t_n) = (x_n, y_n, z_n)$ at time n, which will be optimized subsequently. We denote by $d_{A,B}^n$ (where A, B belong to $\{\text{BS, IRS, } E_k, u\}$) the distance from position A to position B at time n.

Let $h_{i,u}^n$ and $h_{i,\text{BS}}^n$ represent the small-scale unit variance Rician fading between user u and the i-th IRS, and between the i-th IRS and the BS at time n, respectively. The small-scale fading between the BS and each legitimate user at discrete time n, denoted by $h_{\text{BS},u}^n$, is modeled by a unit variance Rayleigh distribution. The noise at user u and eavesdropper k, symbolized as v_u and v_{E_k}, follows a zero-mean complex Gaussian distribution with variance $2\sigma^2$.

B. Signal Dynamics and Noise Analysis

The received signal by a legitimate user u at time n, from the IRS is formulated as:

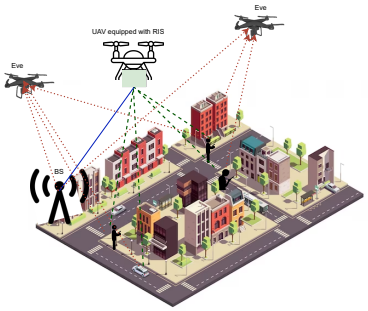

Fig. 1: Representation of the proposed system model.

$$y_u(n) = \sqrt{P}\left(\left(d_{\text{BS,IRS}}^n\right)^{-\frac{\alpha}{2}}\left(d_{\text{IRS},u}^n\right)^{-\frac{\alpha}{2}} \times \sum_{i=1}^{N} z_i^n w_{i,u}^n e^{j\phi_i^n} + \left(d_{\text{BS},u}^n\right)^{-\frac{\alpha}{2}} h_{\text{BS},u}^n\right) + v_u(n). \quad (1)$$

Where P and α denote the BS transmit power and the path loss exponent, respectively. Also, $w_{i,u}^n$ refers to the small-scale fading between user u and the i-th IRS (UAV), z_i^n defines the small-scale fading between the IRS and the BS, and $h_{\text{BS},u}^n$ elucidates the small-scale fading between the BS and user u. For the k-th eavesdropper, considering both the reflected and direct links, the received signal is expressed as:

$$y_{E_k}(n) = \sqrt{P}\left(\left(d_{\text{BS,IRS}}^n\right)^{-\frac{\alpha}{2}}\left(d_{\text{IRS},E_k}^n\right)^{-\frac{\alpha}{2}} \times \sum_{i=1}^{N} z_i^n v_{k,i}^n e^{j\phi_i^n} + \left(d_{\text{BS},E_k}^n\right)^{-\frac{\alpha}{2}} h_{\text{BS},E_k}(n)\right) + v_{E_k}(n), \quad (2)$$

where $h_{\text{BS},E_k}(n)$ outlines the small-scale fading between the BS and eavesdropper E_k at time n. Consequently, the instantaneous SNR for a legitimate user u at time n is expressed as:

$$\gamma_u(n) = \frac{P}{\sigma^2}\left|\left(d_{\text{BS,IRS}}^n\right)^{-\frac{\alpha}{2}}\left(d_{\text{IRS},u}^n\right)^{-\frac{\alpha}{2}} \times \sum_{i=1}^{N} z_i^n w_{i,u}^n e^{j\phi_i^n} + \left(d_{\text{BS},u}^n\right)^{-\frac{\alpha}{2}} h_{\text{BS},u}^n\right|^2, \quad (3)$$

The SNR received at the eavesdropper k at time n, is:

$$\gamma_k(n) = \frac{P}{\sigma^2}\left|\left(\left(d_{\text{BS,IRS}}^n\right)^{-\frac{\alpha}{2}}\left(d_{\text{IRS},E_k}^n\right)^{-\frac{\alpha}{2}} \times \sum_{i=1}^{N} z_i^n v_{k,i}^n e^{j\phi_i^n} + \left(d_{\text{BS},E_k}^n\right)^{-\frac{\alpha}{2}} h_{\text{BS},E_k}^n\right|^2. \quad (4)$$

III. Problem Formulation

In this section, we start by calculating the secrecy rate for multiple legitimate users, denoted by $u \in U = \{1, \ldots, u\}$. This metric is crucial for evaluating the security dynamics of our framework. After establishing the secrecy rate, we then proceed to formulate the optimization problem.

A. Secrecy Rate

Considering the time-dependent SNRs $\gamma_u(n)$ for each legitimate user u, and $\gamma_k(n)$ for each eavesdropper k, as defined in the revised equations (3) and (4), the secrecy rate R_s at time n is defined as [9]:

$$R_s(n) = \max\left(\min_{u\in U} R_u(n) - R_E^+(n), 0\right) \tag{5}$$

where $R_u(n)$, the rate for a legitimate user u at time n, is expressed by:

$$\begin{aligned} R_u(n) &= \log_2(1+\gamma_u(n)) \\ &= \log_2\left(1+\frac{P}{\sigma^2}\left|\left(d^n_{\text{BS,IRS}}\right)^{-\frac{\alpha}{2}}\left(d^n_{\text{IRS},u}\right)^{-\frac{\alpha}{2}}\sum_{i=1}^{N} z_i^n w_{i,u}^n e^{j\phi_i^n}\right.\right. \\ &\quad \left.\left. + \left(d^n_{\text{BS},u}\right)^{-\frac{\alpha}{2}} h^n_{\text{BS},u}\right|^2\right). \end{aligned} \tag{6}$$

For the eavesdroppers, R_E^+, the maximum rate among all the eavesdroppers at time n, is given by

$$\begin{aligned} R_E^+(n) &= \max_k \log_2(1+\gamma_k(n)) \\ &= \max_k \log_2\left(1+\frac{P}{\sigma^2}\left|\left(d^n_{\text{BS,IRS}}\right)^{-\frac{\alpha}{2}}\left(d^n_{\text{IRS},E_k}\right)^{-\frac{\alpha}{2}}\sum_{i=1}^{N} z_i^n v_{k,i}^n e^{j\phi_i^n}\right.\right. \\ &\quad \left.\left. + \left(d^n_{\text{BS},E_k}\right)^{-\frac{\alpha}{2}} h^n_{\text{BS},E_k}\right|^2\right). \end{aligned} \tag{7}$$

B. Optimization Problem

Given the updated secrecy rate expressions with multiple users, the objective is to devise an optimization framework for the UAV's IRS phase shifts and trajectory to enhance the secrecy rate. This involves adapting the IRS phase shifts and UAV's path to maximize the overall secrecy rate, represented by R_s, while ensuring secure communication in the presence of eavesdroppers. For solving the problem efficiently, the optimization formulation is relaxed and represented as:

$$\begin{aligned} \underset{\phi^n, x_n, y_n, z_n}{\text{maximize}} \quad & \sum_{u=1}^{U}\left[\log_2\left(1+\frac{P}{\sigma_u^2}\left|\left(d^n_{\text{BS,IRS}}\cdot d^n_{\text{IRS},u}\right)^{-\frac{\alpha}{2}}\right.\right.\right. \\ & \left.\left.\left.\times\sum_{i=1}^{N} z_i^n w_{i,u} e^{j\phi_i^n} + \left(d^n_{\text{BS},u}\right)^{-\frac{\alpha}{2}} h^n_{\text{BS},u}\right|^2\right)\right] \\ & - \max_k\left[\log_2\left(1+\frac{P}{\sigma_k^2}\left|\left(d^n_{\text{BS,IRS}}\cdot d^n_{\text{IRS},E_k}\right)^{-\frac{\alpha}{2}}\right.\right.\right. \\ & \left.\left.\left.\times\sum_{i=1}^{N} z_i^n w_{i,k} e^{j\phi_i^n} + \left(d^n_{\text{BS},E_k}\right)^{-\frac{\alpha}{2}} h^n_{\text{BS},E_k}\right|^2\right)\right]^+ \end{aligned} \tag{8}$$

subject to

$$\sqrt{(\Delta x_n)^2+(\Delta y_n)^2+(\Delta z_n)^2} \le \Delta_{\max}, \tag{9}$$

$$\sqrt{x_n^2+y_n^2+z_n^2} \le R, \tag{10}$$

$$z_{\min} \le z_n \le z_{\max}, \tag{11}$$

$$0 \le \phi_i^n \le 2\pi, \forall i \in \{1,\ldots,N\}, \tag{12}$$

The optimization variables include the IRS phase shifts for each element ϕ_i^n, and the UAV's Cartesian coordinates x_n, y_n, and z_n at each time slot n. Here, $w_{i,u}$ denotes the IRS beamforming weight for the i-th element and u-th user. The noise variance for user u is denoted by σ_u^2, while the notation $[\cdot]^+$ ensures that the secrecy rate remains non-negative by taking the positive part. The displacement constraints are expressed as:

$$\begin{aligned} &\Delta x_n = x_n - x_{n-1}, \quad \Delta y_n = y_n - y_{n-1}, \\ &\Delta z_n = z_n - z_{n-1}. \end{aligned}$$

These equations define the changes in position along the x, y, and z coordinates. Each constraint in the above optimization problem mirrors real-world considerations for scenarios involving multiple legitimate users:

- **UAV Movement Limitations** (9): This constraint ensures the UAV stays within its maximum displacement between time slots, reflecting speed and energy limits for a feasible trajectory.
- **Operational Radius** (10): Keeps the UAV within a predefined radius R, ensuring it stays within operational zones for regulatory or communication coverage purposes.
- **Altitude Boundaries** (11): The altitude range between $z_{\min}$ and $z_{\max}$ ensures regulatory compliance and optimizes communication performance.
- **Phase Shift Limits** (12): Ensures IRS phase shifts remain within achievable limits to optimize signal quality and counter eavesdropping.

These constraints ensure practical UAV and IRS operations within regulatory, safety, and communication requirements, making the optimization problem realistic for multi-user environments.

C. Proposed Iterative Solution

The optimization problem (13) is inherently non-convex, making it challenging to find a globally optimal solution using traditional techniques. Hence, in this paper, we introduce a novel approach tailored to address this complexity and provide a viable solution. As detailed in Alg. 1, our proposed optimization solution adopts an iterative sequential approach by alternating between optimizing the IRS angles and the UAV positions, considering the multi-user environment until convergence is achieved. This recursive strategy is designed to incrementally improve the solution, addressing the problem's non-convex nature and rendering it more tractable in scenarios with multiple legitimate users.

In the scenario with multiple legitimate users, the UAV's trajectory and positioning (x_n, y_n, z_n) are optimized considering the coverage and quality of service for all users. The iterative detailed in Alg. 1 takes into account the aggregate communication requirements and seeks to balance the overall network performance. The UAV's position is strategically determined to provide optimal signal strength and secrecy rates, mitigating the risk from potential eavesdroppers. While the UAV's physical coordinates are not directly altered by the number of users, the optimization criteria are indeed influenced, necessitating a comprehensive approach that ensures effective service to each user within the network's operational constraints.

Algorithm 1 Iterative Optimization for IRS Angles and UAV Positions

Initialize: IRS angles, UAV positions, and previous objective value $O_{\text{prev}} = -\infty$
Set convergence threshold $\epsilon = 0.01$
while not converged **do**
  Optimize IRS angles with respect to all users using methods in Section IV.
  Optimize UAV positions based on determined IRS angles and multi-user distribution using methods in Section V.
  Compute current objective value O_{current} (13)
  if $\frac{|O_{\text{current}} - O_{\text{prev}}|}{|O_{\text{prev}}|} \leq \epsilon$ **then**
    Break
  end if
  Update $O_{\text{prev}} = O_{\text{current}}$
end while
End

IV. IRS Angles Optimization Using Genetic Algorithm

During the first phase of Alg. 1, the objective is to optimize the IRS angles, denoted by $\phi_1, \ldots, \phi_N$ (with the time index n omitted for simplicity), to maximize the aggregate secrecy rate over all legitimate users, assuming a fixed UAV position.

A. Objective Function and Constraints

With the IRS-equipped UAV's position held constant, the optimization problem in Eq. 13 can be redefined to focus on the IRS phase angles as follows:

$$\max_{\phi_1,\ldots,\phi_N} \left[\sum_u f_u(\phi_1, \ldots, \phi_N) - \max_k g_k(\phi_1, \ldots, \phi_N) \right] \quad (13)$$

$$\text{Subject to:} \quad 0 \leq \phi_i \leq \Delta_\phi \quad \forall i \in \{1, \ldots, N\}, \quad (14)$$

where f_u and g_k are the legitimate user u's rate and the eavesdropper k's rate, respectively, given by:

$$f_u(\phi_1, \ldots, \phi_N) = \log_2 \left(1 + \frac{P}{\sigma^2} \left| B_{0,u} \sum_{i=1}^{N} z_i^n w_{i,u} e^{j\phi_i} + B_{1,u} \right|^2 \right), \quad (15)$$

$$g_k(\phi_1, \ldots, \phi_N) = \log_2 \left(1 + \frac{P}{\sigma^2} \left| D_{0,k} \sum_{i=1}^{N} z_i^n v_{k,i} e^{j\phi_i} + D_k \right|^2 \right). \quad (16)$$

The parameters B_0, B_1, D_0, and D_1 are computed based on the distances and channel gains from the base station (BS) to the legitimate users (B) and eavesdroppers (E) as:

$$B_0 = \left(d_{BS,IRS}^n \; d_{IRS,u}^n \right)^{-\frac{\alpha}{2}}, \quad D_0 = \left(d_{BS,IRS}^n \; d_{IRS,E_k^n} \right)^{-\frac{\alpha}{2}}, \quad (17)$$

$$B_1 = \left(d_{BS,u}^n \right)^{-\frac{\alpha}{2}} h_{BS,u}^n, \qquad D_1 = \left(d_{BS,E_k}^n \right)^{-\frac{\alpha}{2}} h_{BS,E_k}^n. \quad (18)$$

The fitness function $F(\phi_1, \ldots, \phi_N)$, which serves as a metric to evaluate the quality of each solution, is given by:

$$F(\phi_1, \ldots, \phi_N) = \sum_u f_u(\phi_1, \ldots, \phi_N) - \max_k g_k(\phi_1, \ldots, \phi_N). \quad (19)$$

B. Genetic Algorithm for Optimization

For phase optimization with multiple legitimate users, the Genetic Algorithm (GA) remains an apt choice due to its proficiency in navigating complex search landscapes. GA leverages adaptive mutation rates to strike a balance between exploring the search space and exploiting promising solutions. In the context of multiple users, the fitness function is tailored to evaluate the collective performance across all legitimate users, enhancing the secrecy rate optimization. Alg. 2 outlines the GA's implementation for this multi-user phase optimization problem.

Algorithm 2 Optimization via Genetic Algorithm for Multiple Users

Initialization: Generate random solutions within $0 \leq \phi_i \leq \Delta_\phi$. Let N be the size of each solution.
repeat
  Evaluate fitness $F(\phi_1, \ldots, \phi_N) = \sum_u f_u(\phi_1, \ldots, \phi_N) - \max_k g_k(\phi_1, \ldots, \phi_N)$ for each solution.
  Apply elitism to retain top-performing solutions.
  Perform `tournament_selection` from a subset S of T individuals to select parent ϕ^p.
  if random value r ¡ crossover rate ρ **then**
    Execute `crossover` at a random point c to produce offspring ϕ^o.
    Ensure ϕ^o adheres to $0 \leq \phi \leq \Delta_\phi$.
  else
    Carry forward parents to the next generation.
  end if
  for each ϕ_i^o in ϕ^o **do**
    if random value s ¡ mutation rate μ **then**
      Mutate ϕ_i^o by adding δ within $[-\epsilon, \epsilon]$.
      Confirm ϕ_i^o complies with $0 \leq \phi_i^o \leq \Delta_\phi$.
    end if
  end for
  if there is stagnation **then**
    Escalate mutation rate μ to promote diversity.
  else
    Revert mutation rate μ to its original value.
  end if
until Convergence or maximum generation limit is reached

Alg. 2 employs genetic operations, such as crossover and mutation, fine-tuned with rates μ and ρ. This ensures progressive evolution towards the optimal IRS phase angles for all users, guided by a comprehensive fitness function that reflects the aggregated communication secrecy across the network.

V. UAV Position Optimization

Once an optimal or near-optimal set of IRS angles ϕ is identified, the next step is to optimize the UAV's position, treating the obtained ϕ as fixed. With these optimal reflection angles, it becomes possible to position the UAV towards maximizing the secrecy rates for all users. By considering that the angles are now fixed, the optimization problem for user u in Eq (13) becomes:

$$\max_{x_n,y_n,z_n} R_s(n) = \max_{x_n,y_n,z_n} \max\left(\min_{u\in U} R_u(n) - R_E^+(n), 0\right) \tag{20}$$

$$\text{s.t.} \quad \sqrt{\Delta x_n^2 + \Delta y_n^2 + (\Delta z_n)^2} \leq \Delta_{\max}, \tag{21}$$

$$\sqrt{x_n^2 + y_n^2 + z_n^2} \leq R, \tag{22}$$

$$z_{\min} \leq z_n \leq z_{\max}, \tag{23}$$

At high SNR, and given that the IRS angles are fixed, the objective function can be simplified as follows:

$$Q(x_n, y_n, z_n) = \log_2 \left| \frac{\min_{u\in U}(\alpha_1 d_{BS,IRS}^n \; {d_{IRS,u}^n}^{-\frac{\alpha}{2}} + \alpha_2)}{\max_k(\beta_1 d_{BS,IRS}^n \; {d_{IRS,E_k}^n}^{-\frac{\alpha}{2}} + \beta_2)} \right|^2. \tag{24}$$

Where α_1, α_2, β_1, and β_2 for each user u and eavesdropper E_k can be written as:

$$\begin{aligned} \alpha_1 &= \tfrac{\sqrt{P}}{\sigma} \textstyle\sum_{i=1}^N z_i^n w_{i,u}^n e^{j\phi_i^n}, \quad \alpha_2 = \tfrac{\sqrt{P}}{\sigma} {d_{BS,u}^n}^{-\frac{\alpha}{2}} h_{BS,u}^n \\ \beta_1 &= \tfrac{\sqrt{P}}{\sigma} \textstyle\sum_{i=1}^N v_{k,i}^n w_{i,k}^n e^{j\phi_i^n}, \quad \beta_2 = \tfrac{\sqrt{P}}{\sigma} {d_{BS,E_k}^n}^{-\frac{\alpha}{2}} h_{BS,E_k}^n \end{aligned} \tag{25}$$

Maximizing the objective function in Eq (24), is equivalent to maximizing:

$$\begin{aligned} M(x_n, y_n, z_n) &= \left| \frac{\alpha_1 (d_{BS,IRS}^n \; d_{IRS,B}^n)^{-\frac{\alpha}{2}} + \alpha_2}{\max_k(\beta_1 (d_{BS,IRS}^n \; d_{IRS,E_k}^n)^{-\frac{\alpha}{2}} + \beta_2)} \right|^2. \\ &= \frac{u(x_n, y_n, z_n, \alpha_1, \alpha_2, BS, B)}{u(x_n, y_n, z_n, \beta_1, \beta_2, BS, E_{k_m})}, \end{aligned} \tag{26}$$

where

$$u(x_n, y_n, z_n, \alpha_1, \alpha_2, A_1, A_2) = \alpha_1 (d_{A_1,IRS}^n \; d_{IRS,A_2}^n)^{-\frac{\alpha}{2}} + \alpha_2 \tag{27}$$

and k_m denotes the index k that maximizes the denominator expression in M. It can be proven that the gradient of $u(x_n, y_n, z_n, \alpha_1, \alpha_2, A_1, A_2)$ with reference to x_n is given by

$$\frac{du}{d_{x_n}} = -\alpha \left({\alpha_1}^2 t^{-\frac{\alpha}{2}} + Re(\alpha_1 \alpha_2^*) \right) \left(\frac{x - x_{A_1}}{d_{IRS,A_1}} + \frac{x - x_{A_2}}{d_{IRS,A_2}} \right) t^{-\frac{\alpha}{2}-1} \tag{28}$$

where $t = d_{IRS,A_1} d_{IRS,A_2}$. Consequently, the derivative of M can be obtained by applying the ratio derivative property. Similarly, the full gradient with reference to y_n and z_n can be also computed. Solving the optimization problem is non-convex and challenging. To address this optimization problem, an iterative approach is proposed and detailed in Alg. 3 where the distances are computed, and then used to determine k_m, which is subsequently used to compute the gradients.

Algorithm 3 UAV Position Optimization

Require: Optimal or near-optimal IRS angles ϕ
Ensure: Optimal UAV position (x_n, y_n, z_n)
Fix IRS angles ϕ
Simplify the objective function at high SNR
while not converged **do**
  Step 1: Compute Distances
  $d_{IRS,B}^n \leftarrow$ Compute distance to B
  $d_{\text{IRS},E_k^n}(n) \leftarrow$ Compute distance to E_k
  Step 2: Determine k_m
  $k_m \leftarrow$ Determine entity with max weighted path loss
  Step 3: Compute Gradients
  Compute gradients w.r.t. x_n, y_n, z_n
  Step 4: Update the Position
  Update Q using gradients and learning rate η
  Step 5: Position Projection and Constraint Enforcement
  Project and enforce constraints on position
  Step 6: Update Q
  Update Q and optimize the IRS angle
end while
return (x_n, y_n, z_n)

VI. Simulation Results

This section evaluates the performance of the proposed technique in ensuring the security of network communication using MonteCarlo simulation. The secrecy rate is used as the primary evaluation metric.The secrecy rate is evaluated with the following simulation parameters: path loss exponent $\alpha = 2$, region radius $R = 1000$ m, IRS cells $N_c = 10$, transmit power $P = 50$ dBm, noise level $\sigma_E^2 = \sigma_B^2 = -80$ dBm, and the number of eavesdroppers $K = 10$.

The proposed "Optimized IRS Optimized Position" (OIOP) technique is compared to several benchmark schemes to assess its efficiency. First, it is evaluated against Exhaustive Search (ES), which explores all possible solutions but is computationally impractical, leading to the introduction of Accelerated Exhaustive Search (A-ES). A-ES narrows the search space iteratively for greater efficiency. Additionally, OIOP is compared with three other benchmarks: Random IRS with Fixed Position Phase (RIFP), Optimized IRS with Fixed Position Phase (OIFP), and Random IRS with Optimized Position Phase (RIOP).

Fig. 2 compares the secrecy rates of the Optimized IRS Optimized Position (OIOP) with other benchmark schemes as the operational radius R increases. The results show that OIOP consistently outperforms the other methods in enhancing secrecy. RIFD, which lacks both phase and position optimization, performs the worst, while OIFP, with only phase optimization, is limited by its static position. RIOP, optimizing only position, fares better than RIFD but falls short of OIOP, which achieves the highest secrecy rates by optimizing both phase and position. The analysis also indicates that as the operational radius R increases, the secrecy rate tends to decrease. This decrement can be attributed to the increased exposure area, which potentially offers eavesdroppers more

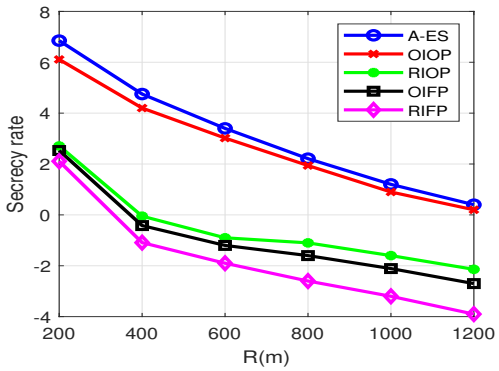

Fig. 2: The effect of the zone radius R on OIOP secrecy rate when compared to A-ES, RIFP, OIFP, and RIOP.

vantage points for interception. Larger operational radii may also lead to weakened signal strengths at the outer boundaries of the radius, reducing the effectiveness of signal optimization strategies and making communications more vulnerable to eavesdropping. This relationship between the increased radius and decreased secrecy rate highlights the critical balance needed between extending operational coverage and maintaining secure communications. Furthermore, the comparison reveals insights into the computational trade-offs inherent in optimization methods. Although the A-ES method offers superior performance, its computational intensity, stemming from the exhaustive examination of all possible combinations, necessitates careful consideration of the trade-off between computational complexity and optimality.

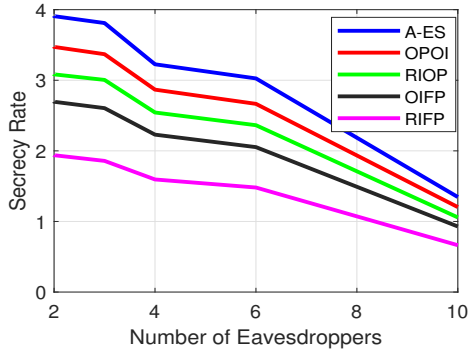

Fig. 3: The effect of the number of eavesdroppers on OIOP secrecy rate when compared to A-ES, RIFP, OIFP, and RIOP.

Additionally, Fig. 3 delves into the impact of the number of eavesdroppers on the secrecy rate of OIOP in comparison with A-ES, RIFP, OIFP, and RIOP. This analysis elucidates the resilience of different strategies in the face of escalating eavesdropping threats. Notably, as the number of eavesdroppers escalates, the secrecy rate across all schemes experiences a decline. Nevertheless, OIOP consistently outperforms other schemes, especially in scenarios with a relatively low number of eavesdroppers. However, as the eavesdropper count approaches ten, a convergence of secrecy rates among all techniques becomes apparent. This convergence suggests that the proliferation of eavesdroppers diminishes the efficacy of optimization strategies, posing challenges in sustaining high secrecy rates amidst escalating eavesdropping threats.

VII. Conclusion

This paper introduces an advanced system to enhance secure wireless communication by utilizing a UAV equipped with an IRS. Serving as a relay, the UAV improves secrecy performance in IRS-aided wireless networks, despite the ongoing threat of eavesdropping. Our approach optimizes both the IRS's reflective angles and the UAV's positioning to maximize secrecy rates. Simulations reveal that this method outperforms conventional techniques, particularly in dynamic scenarios with varying eavesdropping conditions. The study provides valuable insights into system parameters and presents a promising approach for developing robust wireless networks amidst evolving security challenges. However, the approach encounters challenges with computational complexity and adaptability in rapidly changing environments. Future work will aim to improve efficiency, enhance real-time adaptability, and reduce energy consumption. Furthermore, real-world testing will be essential to validate the system's performance under practical conditions, paving the way for further advancements in secure wireless communication.

Acknowledgment

This work was supported by Qatar University Internal Grant IRCC-2023-237. The statements made herein are solely the responsibility of the author[s].

References

[1] Junghoon Kim, Seyyedali Hosseinalipour, Andrew C Marcum, Taejoon Kim, David J Love, and Christopher G Brinton, "Learning-based adaptive irs control with limited feedback codebooks," *IEEE Transactions on Wireless Communications*, vol. 21, no. 11, pp. 9566–9581, 2022.

[2] Ming Zeng, Ebrahim Bedeer, Xingwang Li, Quoc-Viet Pham, Octavia A Dobre, Paul Fortier, and Leslie A Rusch, "Irs-empowered wireless communications," *6G Wireless: The Communication Paradigm Beyond 2030*, p. 15, 2023.

[3] Tamim M Al-Hasan, Aya N Sayed, Faycal Bensaali, Armstrong Nhlabatsi, and Ridha Hamila, "Security-driven performance analysis of lightweight cryptography for energy efficiency applications," in *2024 IEEE 8th Energy Conference (ENERGYCON)*. IEEE, 2024, pp. 1–6.

[4] Zina Chkirbene, Ala Gouissem, Ridha Hamila, and Devrim Unal, "The future of aerial communications: A survey of irs-enhanced uav communication technologies," in *2024 IEEE 8th Energy Conference (ENERGYCON)*. IEEE, 2024, pp. 1–6.

[5] Jia Ye, Chao Zhang, Hongjiang Lei, Gaofeng Pan, and Zhiguo Ding, "Secure uav-to-uav systems with spatially random uavs," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 564–567, 2018.

[6] Kezhi Wang, Hongjiang Lei, Gaofeng Pan, Cunhua Pan, and Yue Cao, "Detection performance to spatially random uav using the ground vehicle," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 16320–16324, 2020.

[7] Zina Chkirbene, Ridha Hamila, and Aiman Erbad, "Secure wireless sensor networks for anti-jamming strategy based on game theory," in *2023 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2023, pp. 1101–1106.

[8] Wen Wang, Hui Tian, and Wanli Ni, "Secrecy performance analysis of irs-aided uav relay system," *IEEE Wireless Communications Letters*, vol. 10, no. 12, pp. 2693–2697, 2021.

[9] Lai Wei, Kezhi Wang, Cunhua Pan, and Maged Elkashlan, "Secrecy performance analysis of ris-aided communication system with randomly flying eavesdroppers," *IEEE Wireless Communications Letters*, vol. 11, no. 10, pp. 2240–2244, 2022.