IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2020, accepted March 9, 2020, date of publication April 6, 2020, date of current version April 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2986025

UAV-Aided Jamming for Secure Ground Communication With Unknown Eavesdropper Location

CHRISTANTUS OBINNA NNAMANI, MUHAMMAD R. A. KHANDAKER, (Senior Member, IEEE), AND MATHINI SELLATHURAI, (Senior Member, IEEE)
School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, U.K.

Corresponding author: Muhammad R. A. Khandaker (m.khandaker@hw.ac.uk)

This work was supported in part by the EPSRC under Grant EP/P009670/1, in part by the Petroleum Technology Development Fund, and in part by the University of Nigeria Nsukka.

ABSTRACT This paper investigates unmanned aerial vehicle (UAV)-aided jamming technique for enabling physical layer keyless security in scenarios where the exact eavesdropper location is unknown. We assume that the unknown eavesdropper location is within an ellipse characterizing the coverage region of the transmitter. By sequentially optimizing the transmit power, the flight path of the UAV and its jamming power, we aim at maximizing the average secrecy rate with arbitrary eavesdropper location. Simulation results demonstrate that the optimal flight path obtains better secrecy rate performance compared to that using direct UAV flight path encasing the transmitter and the legitimate receiver. Most importantly, even with the unknown eavesdropper location, we obtained a secrecy rate that is comparable to a scenario when the eavesdropper's location is known. However, the average secrecy rate with the unknown eavesdropper location varies depending on the proximity of the eavesdropper to the known location of the transmitter. We also observe that due to the UAV-aided jamming, the average secrecy rate stabilizes at some point even though the average received envelope power of the eavesdropper increases. This essentially demonstrates the effectiveness of the proposed scheme.

INDEX TERMS Secure communication, jamming, UAV, trajectory optimization, physical layer security.

I. INTRODUCTION

Protecting sensitive or confidential information is of paramount interest to most businesses/organizations – private, public, government, military or intelligence. In the event that such data/information is made public, these businesses/organizations may face legal or financial ramifications. At the very least, they will suffer loss of customer trust (e.g. companies, etc.); but in the worst case, it could lead to the complete annihilation of the organization (e.g. Military, etc.). Thus, secure communications are obligatory to most businesses/organizations and in this sense seen as a primordial requirement of technological and military exploits. However, as technologies continue to explode, especially with the development of modern computing technologies, the internet of things (IoT), 5G and future generation networks, adverse robust ways of information theft continue to grow [1], [2]. In practice, a total secured communication is unattainable, nevertheless, theories seem to support a measure that is acceptable [3], [4]. It is important that communication be unique in all the layers of the communication model - open system interconnection (OSI) and/or the internet model to guarantee its security. Different protocols and techniques have been developed in the literature for the security in the layers of these models [4]. Public and private key-based cryptographic security measures are most widely used in many communication systems. However, cryptographic security is heavily computation demanding in one hand, thus impractical in many IoT applications, and subject to sophisticated external attacks with the advent of modern computing facilities on the other hand. Developing novel security measures to combat such attacks is therefore of prime interest for many researchers. In this context, the notion of physical layer security has attracted significant attention due to its ability to provide information-theoretic security [4]–[7].

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

The physical layer is similar in most communication models as it deals with processing the encapsulated message for transmission via the channel [8]. In wireless communications, it deals directly with the electromagnetic waves referred to as signals. These signals can be compromised via eavesdropping and jamming of legitimate receivers. Focusing on the eavesdropping, the security in the physical layer can be subdivided into key-based and keyless security models. The primary objective of both models is to reduce the ability of an illegitimate user to gain access to the transmitted message. While the key-based models use information obscurity as its main tool, the keyless models detect the possible information leak in the presence of eavesdropper(s)[1] and attempts to decrease its intercepted information. The degree of information protection in a keyless physical layer security model is measured as the secrecy capacity for delay tolerant applications and the outage probability for delay intolerant applications. To maximize the secrecy capacity, [3] proposed an on/off algorithm that varies the power transmitted from the source especially when the eavesdropper have better channel quality. It relied on the principle that the source knows the channel state of the eavesdropper based on inherent channel monitoring. While this scheme reduces the information content received by the legitimate receiver, it also has limited practical applications as the channel information of the eavesdropper is usually unknown. Instead of reducing the transmit power, a more sophisticated approach could be to deliberately jam the eavesdropper's channel ensuring that it receives little/no information. The major limitation of this technique is that the eavesdropper will usually operate at the same band as the legitimate receiver, hence the jamming will also affect the legitimate receiver. A combination of jamming and power variation, harnessing their gains is subsequently the bedrock of modern signal jamming techniques.

Signal jamming as a physical layer protection strategy is one of the most prominent brute-force methods of limiting the information theft in keyless physical layer security exploiting the fading characteristics of the channel [8]. It entails simultaneous transmission of a signal with similar characteristics to the genuine signal but carrying no information content to cause interference to the eavesdropper's received signal. Although this technique does not guarantee that there will be no information leakage, similar to other security techniques, it reduces the probability of successful interception thereby increasing the secrecy capacity of the end-to-end communication. While jamming poses to be an effective technique for improving secrecy, there are some critical issues that affect the effectiveness of signal jamming:

(a) The degree of transmit power required to increase the secrecy capacity without adversely degrading the information content of the desired receiver,
(b) The transmitter's responses to the knowledge of the possible eavesdropper(s),
(c) The optimal location to deliver the jamming signals from.

Researchers have since investigated these requirements independently as in [10], however, the investigation of the collective effects of (a)-(c) is of practical interest due to their inter-dependency in the context of secrecy performance. While some recent studies affirm that this technique yields improvement in the secrecy capacity, they are all based on the impractical assumption that the eavesdropper(s') location is perfectly known at the transmitter [11].

With respect to the known remote eavesdropper location, mobile means of delivering the jamming signals have recently been investigated in the literature. One of the effective methods proposed is the use of an unmanned aerial vehicle (UAV) in scenarios where the nodes under consideration (the source, the main receiver and the eavesdropper) are all based on the ground. This is primarily due to its aerial radio visibility of the ground terminals, its cost efficiency and its availability for low-range applications. The applications of UAVs in communications range from their use as aerial base stations [12]–[15], as relay nodes [16], as access/user nodes [11], [12] to channel estimation [17], etc. Recently, with the advancement of the internet of things (IoT), network of UAVs for UAV-to-UAV communications as well as for general data transmission has also been considered [18].

More recently, UAVs have been deployed for assisting in secure communications between ground terminals [19], [20], and to act as both relay nodes and security agents between ground terminals [21]. In [22], the UAV is deployed with two opposing roles namely, to establish favorable and degraded channels for the legitimate and the eavesdropping links, respectively. A separate jammer UAV has been considered in [23] to degrade the eavesdropping channel in addition to the cooperative UAV for the legitimate channel. Subsequently, UAVs have also been used to deliver classified messages to ground terminals amidst the constraints of eavesdroppers and no-fly regions in [24]. Critical examination reveals that the methods used in [19]–[24] are similar in principle since they optimized the transmitted power, the UAV jamming power and its trajectory for the corresponding scenarios. However, a strong assumption made in [19]–[24] is that the location of the eavesdropper(s) is known to the source and/or the UAV(s). Although this assumption simplifies the respective problem in each scenario, it is grossly impractical. In most practical communication scenarios, even knowing the presence of an eavesdropper is often very difficult let alone knowing their exact locations or channel state information (CSI). This practical challenge motivates us to investigate secret communication with unknown eavesdropper location in this paper. We consider UAV-aided jamming technique for proactively degrading the eavesdropping channel at unknown ground point for improving the achievable secrecy rate.

An attempt to introduce eavesdropper obscurity has also been made by Miao Cui, *et al.* in [25]. The authors in [25]

[1]The kind of eavesdroppers referred to in this paper are considered as passive Wyner wiretappers [9] which do not attempt to alter the transmitted message but try to overhear only.

considered the UAV as the information source and optimized its trajectory and transmitting power to a legitimate receiver amidst a group of eavesdroppers located within an independent small uncertainty region. The trajectory of the UAV has been optimized to find the best points in the space to deliver the maximum information to the legitimate receiver while the eavesdroppers receive minimum information. In contrast, we consider the UAV with an opposing role in this paper to degrade the eavesdropper's channel via cooperative jamming. Note that our work differs from [25] not just in terms of the UAV's role, but also in terms of guaranteed secrecy performance. In fact, the achievable secrecy performance in [25] cannot be guaranteed as the uncertainty region expands and overlaps with the certainty region of the legitimate receiver. Furthermore, a network of legitimate and illegitimate UAVs has been considered in [26] in which a UAV acts as the base station to transmit signal to other legitimate UAVs in altitude and the eavesdropper UAVs from unknown locations try to overhear the signal. The secrecy outage probability and the average secrecy rate performance have been analyzed. Since all the nodes are at the same altitude, the gains of aerial visibility of UAV was subdued. In this work, we intend to explore this opportunity for ground nodes (source, legitimate receiver and eavesdropper) in order to maximize the benefits of aerial visibility of the UAV while constrained by the properties of ground propagation.

We formulate the problem of maximizing the average secrecy rate under the unknown eavesdropper location assumption by jointly optimizing the source transmit power, the UAV trajectory and its jamming power. The problem is strictly non-convex due to the correlation of the optimization variables in the problem. Therefore, in this work, we sequentially optimize the flight path of a UAV, its jamming power and the transmitted power by the source node to ensure secure communication in the considered scenario. One set of variables are optimized in each step while keeping the others fixed. The main contributions in this paper can be summarized as:

(a) Developing the mathematical analysis of UAV-aided jamming applications to secure wireless communication when the location of the eavesdropper is completely unknown.
(b) Applying the block coordinate descent method and successive convex approximation (SCA) technique with the aid of the first-order Taylor series expansion.
(c) Unveiling the influence of the unknown eavesdropper's received power on the average secrecy rate between the source and the legitimate receiver.
(d) Validating the formulations and the solutions by demonstrating the performance of the proposed algorithm against existing UAV-aided secure communication schemes through extensive numerical simulations.

The rest of this paper is organized as follows: Section II describes the UAV-aided communication system model and the problem formulation. The proposed solution is developed in Section III. Simulation results are presented in Section IV before making the concluding remarks in Section V.

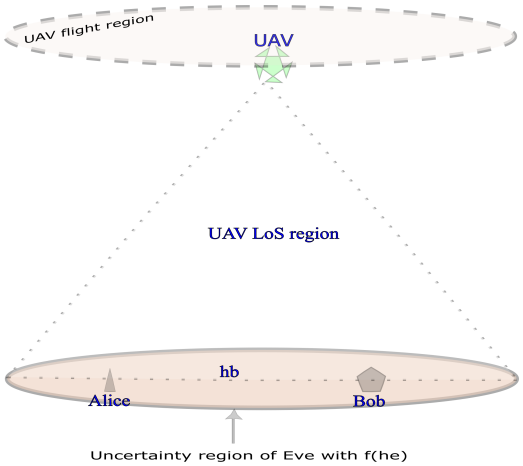

FIGURE 1. UAV-aided jamming for secure communication.

II. SYSTEM MODEL

We consider a secure wireless communication scenario between a base station (BS) acting as a transmitting source (Alice) located at an a-priori known ground point[2] $w_a = [x_a, y_a, 0]^T$ and a receiver (Bob) at an a-priori known ground point $w_b = [x_b, y_b, 0]^T$ as shown in Fig. 1. However, an eavesdropper (Eve) lurks around the area in an unknown ground location, $\tilde{\mathbf{w}}_e = [\tilde{x}_e, \tilde{y}_e, 0]^T$, but within the area where the wireless signal can be received. We denote the complex block-fading channels of Alice with Bob and Eve as g_b and g_e, respectively. Since Eve's location is unknown, Alice's transmission power P_a is a function of Bob's channel power gain $h_b = \mathbb{E}[|g_b|^2]$ alone; hence $P_a = P(h_b)$, i.e. Alice varies her transmission power depending on the channel state of Bob. Averaging through all fading realizations of the channels of Bob and Eve, the average secrecy rate and secrecy capacity derived from Shannon's information content are given respectively as [3]

$$R_s = \int\int [\underbrace{\log_2(1 + h_b P(h_b))}_{\text{information rate of Bob}} - \underbrace{\log_2(1 + h_e P(h_b))}_{\text{information rate of Eve}}]^+ \times f(h_b) f(h_e)\, \mathrm{d}h_e\, \mathrm{d}h_b, \quad (1)$$

$$C_s = \max_{P(h_b)} R_s \quad (2)$$

where R_s, C_s, and $P(h_b)$ are the average secrecy rate,[3] secrecy capacity, and transmit power from Alice, respectively, h_b, $h_e = \mathbb{E}[|g_e|^2]$, and $f(h_b)$, $f(h_e)$ are the channel power gain and probability density functions (PDF) of Bob and Eve, respectively. $[a]^+$ indicates $\max(0, a)$. Note that $[\cdot]^+$ imposes a constraint such that Eve cannot receive higher information

[2] z-coordinate represents the altitude and the ground point is located at z = 0.

[3] Nota bene: All logarithms used in this work is of base 2 since we refer to digital communications.

than Bob at any time during the communication. Hence, in the subsequent formulations, the $[\cdot]^+$ will be ignored since the value of the integral function is always non-negative. Accordingly, the limits of the integrals in (1) are defined such that when $h_e > h_b$, the mutual information between Alice and Eve is upper-bounded by $\log_2(1+h_bP(h_b))$. This ensures that averaging the secrecy rate over all possible channel realizations of Eve is upper bounded by the channel of Bob following the variable rate scheme described in [3]. Nevertheless, it is desirable that the rate of Bob be as high as possible and only limited by the power constraints of Alice (transmitter), hence, (1) reduces to

$$R_s = \int_0^{\infty}\int_0^{h_b} [\log_2(1+h_bP(h_b) - \log_2(1+h_eP(h_b] \times f(h_b)f(h_e)\,\mathrm{d}h_e\,\mathrm{d}h_b. \quad (3)$$

The objective of keyless physical layer security is to ensure that (2) is sustained at its optimal value over the duration of the communication.

Note that the achievable secrecy rate in (1) describes the secrecy rate as the difference of the average information rates of Bob and Eve over all fading realizations of Bob and Eve. The non-negativity assumption on the secrecy rate $[\cdot]^+$ requires that the location of Eve revolves around that of Bob and not beyond the coverage region of Alice. However, in practice, Eve may even be located at positions closer to Alice than Bob and thereby receive stronger signals than Bob assuming they both share the same channel model based on the proximity to the transmitter alone. In such scenarios, the achievable secrecy rate would be zero as defined in (3).

To ameliorate the aforementioned challenge, we deploy a UAV that will deliver jamming signals to reduce the information acquired by Eve while attempting to sustain that obtained by Bob. However, in UAV-aided communications, a common challenge is to optimize the UAV trajectory [12]. In secure communications, the challenge is further proliferated by the unknown eavesdropper location. We aim at addressing this challenge in the following sections. The UAV flight path will be optimized to ensure that for any location of Eve within the coverage region of Alice, its information rate will be continually below that of Bob, thereby, achieving positive secrecy rates.

We assume that the UAV is not equipped with any tracking devices. Therefore, the UAV will not be able to locate or track Eve despite having a clear line-of-sight (LoS) to all points within the coverage region of Alice due to aerial visibility. Furthermore, if the UAV flies horizontally at constant altitude from an initial point q_0 to a final point q_f, its ascent and descent flight path to the initial and final ground points can be neglected. The UAV flight duration, T, is sampled at discrete time-stamps of N equal time slots with duration of $\delta = T/N$ [16], [19]. The UAV maintains constant speed V m/s and transmits a pulse of the jamming signal within a slot δ. The channel within the slot is also assumed to vary slowly allowing for block fading within the slot. Hence, increasing the number of time slots, N, the UAV may be assumed to transmit almost continuously. For simplicity, we assume that V is constant over the entire flight duration as also assumed in [19]. If the distance covered in each sample is small enough, we can assume that the UAV is stationary at each sample point. Considering a large number of sample points, the UAV is assumed to send jamming signals continuously. These sampled points can be denoted as $\boldsymbol{q}[n] = \left[x[n], y[n], z[n]\right]^T$, $n \in \{1, \ldots, N\}$, which satisfies the following constraints:

$$\|\boldsymbol{q}[n+1] - \boldsymbol{q}[n]\|^2 \leq (V\delta)^2 \quad (4a)$$
$$\|\boldsymbol{q}[1] - \boldsymbol{q}_0\|^2 \leq (V\delta)^2 \quad (4b)$$
$$\boldsymbol{q}[N] = \boldsymbol{q}_f \quad (4c)$$
$$\|\boldsymbol{q}[n] - \boldsymbol{w}_a\| + \|\boldsymbol{q}[n] - \boldsymbol{w}_b\| \leq 2a \quad (4d)$$
$$\boldsymbol{q}(x_n, y_n, z_n) = \boldsymbol{q}(x_n, y_n, H). \quad (4e)$$

Inequalities (4a) and (4b) ensure that the distance covered by the UAV within the flight samples does not exceed the parametric distance. The velocity V m/s is chosen such that the total distance covered by the UAV through the samples will be greater than or equal to the Euclidean distance between q_0 and q_f, i.e., $(V\delta) \geq \|\boldsymbol{q}_f - \boldsymbol{q}_o\|$, otherwise the system will be intractable. This ensures that the UAV travels at least in a straight path from its initial to its final points for a given total flight duration. The equality in (4c) ensures that the final flight point of the UAV is at the a-priori final destination, while (4d) allows the UAV to remain within the uncertainty region where the eavesdropper can be found. This region is postulated as an ellipse and physically represents a cellular coverage region of Alice. a determines the size of the ellipse and satisfies {for $a > \|\boldsymbol{w}_b - \boldsymbol{w}_a\|$}, w_a and w_b are the two foci of the ellipse, ensuring that Bob is not a cell-edge user. Finally, (4e) places the UAV to fly at constant altitude denoted by H meters.

Assuming that the ground fading channel between Alice and Bob is Rayleigh distributed, the lower bound of the channel power gain (corresponding to the worst channel condition) with the jamming signal delivered by the UAV is given by [20], [22], [23]

$$h_b[n] = \frac{\overbrace{\beta_o d_{ab}^{-\psi}\mathbb{E}[\zeta]}^{\text{ground channel gain}}}{\underbrace{P_u[n]\beta_o d_{qb}^{-2}[n] + 1}_{\text{LoS jamming signal attenuation}}}, \quad (5)$$

where ψ is the ground path loss component between Alice and Bob, β_0 represents the signal-to-noise ratio (SNR) at a reference distance ($d_0 = 1m$) of the ground channels, ζ is an exponentially distributed random variable with unit mean ($\mathbb{E}[\zeta] = 1$), d_{ab} and d_{qb} are the Euclidean distance between Alice, UAV and Bob respectively and P_u is the UAV jamming signal power.

We note that (5) is the upper bound of the random complex channel g_b as expressed in [22, eq. (12)]. Thus the channel power gain of Bob (h_b) has been discretized to reflect the discrete interference caused by the UAV jamming signal as

represented by the N samples. We also note that the choice of integrals in (3) depicts averaging over all channel realizations of Bob and Eve. Clearly, $\int_0^\infty g(h_b)f(h_b)dh_b$ shows that the channel realization of Bob, h_b, is continuous over an infinite space. However, based on the discrete-time samples of the UAV trajectory, h_b is discretized as shown in (5) to represent the channel of Bob under the jamming signal delivered by the UAV at each sampled slot. Hence, assuming slow fading in between slots of the UAV flight time, it is sufficient to find the average in (3) under the discrete-time block fading samples as in [14], [19]:

$$R_s = \frac{1}{N}\sum_{n=1}^{N}\int_0^{h_b[n]} [\log(1+h_b[n]P_a[n] - \log(1+h_e[n]P_a[n]]f(h_e)dh_e. \quad (6)$$

To ensure that the power levels of the communication is within acceptable range, P_u and P_a are subjected to average and peak power constraints described as:

$$0 \le P_u[n] \le P_{umax} \quad (7a)$$

$$\frac{1}{N}\sum_{n=1}^{N} P_u[n] \le \bar{P}_{ub} \quad (7b)$$

$$0 \le P_a[n] \le P_{amax} \quad (7c)$$

$$\frac{1}{N}\sum_{n=1}^{N} P_a[n] \le \bar{P}_{ab}. \quad (7d)$$

A. PROBLEM FORMULATION

Let $\mathbf{Q} = \{q[n], n \in N\}$, $\mathbf{p}_a = \{P_a[n], n \in N\}$, and $\mathbf{p}_u = \{P_u[n], n \in N\}$ be the set of UAV sample points (representing its trajectory when connected by a straight line), the set of power transmitted by Alice as well as the UAV, respectively. We aim at solving (2) by alternating the optimization of $\mathbf{Q}$, $\mathbf{p}_a$ and $\mathbf{p}_u$.

In order to solve (6), we need to know the possible distribution of the fading channel of Eve which can be obtained via historical measurements collected over the region covered by Alice (represented in this model as an ellipse, as in (4d)). If we consider that the time-varying complex channel $g_e(t)$ of Eve is normally distributed with mean zero and known variance such that $g_e(t) = g_{e,I}(t)+ig_{e,Q}(t)$, where $g_{e,I}, g_{e,Q} \sim \mathcal{C}(0, b_0)$ are the in-phase and quadrature components of $g_e(t)$, then its magnitude, $\alpha(t) = |g_e(t)|$, will be Rayleigh distributed with average envelop power $\mathbb{E}[\alpha^2] = 2b_0 \triangleq y_e$. The instantaneous envelop power is the squared envelop $\alpha^2(t) = |g(t)|^2 \triangleq h_e$ and is exponentially distributed as

$$f(h_e) = \frac{1}{y_e}e^{-\frac{h_e[n]}{y_e}}, \quad \forall h_e \ge 0. \quad (8)$$

Considering block fading within a slot, the channel variations are negligible for the time in between slots, as N becomes very large. Substituting (8) in (6), we obtain

$$R_s = \frac{1}{N}\sum_{n=1}^{N}\log(1+h_b[n]P_a[n])(1-e^{-\frac{h_m}{y_e}}) + \int_0^{h_b[n]}\log(1+h_e[n]P_a[n])(\frac{1}{y_e}e^{-\frac{h_e}{y_e}})dh_e. \quad (9)$$

By applying integration by parts, (9) reduces to

$$R_s = \frac{1}{N}\sum_{n=1}^{N}\underbrace{\log(1+h_b[n]P_a[n])}_{\text{information rate of Bob}} - \underbrace{\int_0^{h_b[n]}\frac{P_a[n]e^{-\frac{h_e[n]}{y_e}}}{1+h_e[n]P_a[n]}dh_e}_{\text{information rate of Eve}}. \quad (10)$$

The secrecy rate in (10) can be further simplified as [27, eq. 3.352.1]

$$R_s = \frac{1}{N}\sum_{n=1}^{N}\log(1+h_b[n]P_a[n]) - e^{\frac{1}{y_eP_a[n]}}\left[E_i\left(-\frac{h_b[n]}{y_e}-\frac{1}{y_eP_a[n]}\right) - E_i\left(-\frac{1}{y_eP_a[n]}\right)\right], \quad (11)$$

where $E_i(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ is the exponential integral. We note that (10) is equivalent to (11) and they can be used interchangeably depending on the parameter been inferred. Thus we substitute the objective function in (2) with the elaborated form in (11) to obtain the following optimization problem[4]:

$$(P1): \max_{\mathbf{p}_a,\mathbf{p}_u,\mathbf{Q}} \sum_{n=1}^{N}\log(1+h_b[n]P_a[n]) - e^{\frac{1}{y_eP_a[n]}}\left[E_i\left(-\frac{h_b[n]}{y_e}-\frac{1}{y_eP_a[n]}\right) - E_i\left(-\frac{1}{y_eP_a[n]}\right)\right] \quad (12a)$$

$$\text{s.t. } \|\boldsymbol{q}[n+1]-\boldsymbol{q}[n]\|^2 \le (V\delta)^2 \quad (12b)$$

$$\|\boldsymbol{q}[1]-\boldsymbol{q}_0\|^2 \le (V\delta)^2 \quad (12c)$$

$$\boldsymbol{q}[N] = \boldsymbol{q}_f \quad (12d)$$

$$\|\boldsymbol{q}[n]-\boldsymbol{w}_a\| + \|\boldsymbol{q}[n]-\boldsymbol{w}_b\| \le 2a \quad (12e)$$

$$\boldsymbol{q}(x_n, y_n, z_n) = \boldsymbol{q}(x_n, y_n, H), \quad (12f)$$

$$0 \le P_u[n] \le P_{umax} \quad (12g)$$

$$\frac{1}{N}\sum_{n=1}^{N} P_u[n] \le \bar{P}_{ub} \quad (12h)$$

$$0 \le P_a[n] \le P_{amax} \quad (12i)$$

$$\frac{1}{N}\sum_{n=1}^{N} P_a[n] \le \bar{P}_{ab}. \quad (12j)$$

[4]We neglected the constant scaling factor $\frac{1}{N}$ in the objective function as this does not affect the optimal solution.

Problem (P1) entails that the secrecy capacity of the proposed system depends on the optimal transmission power of Alice, the jamming power delivered by the UAV and the UAV location. Unfortunately, (P1) is a non-convex optimization problem with respect to the optimization variables ($\mathbf{p}_a$, $\mathbf{p}_u$, $\mathbf{Q}$) and cannot be easily solved directly. However, using a sequential and iterative technique under a block coordinate approach, we can obtain suboptimal solutions that satisfy the constraints in (4) and (7).

III. PROPOSED SOLUTION

We propose solving the non-convex problem (P1) in an alternating fashion. The proposed solution involves decomposing the original problem (P1) into three sub-problems each characterizing a set of optimization variables. In each sub-problem, we optimize one set of variables while fixing the other variables in each iteration. The results obtained from each iteration step are analyzed with the objective value of (P1) and the iteration stops at the point when the objective value (P1) converges.

A. OPTIMIZING THE SOURCE POWER (P_a)

We first optimize Alice's transmit power for arbitrary initial trajectory and jamming power. Replacing the objective in problem (P1) with (10), problem (P1) can be reformulated for any given $\mathbf{Q}$ and $\mathbf{p}_u$ as problem (P2):

$$(P2): \max_{\mathbf{p}_a} \sum_{n=1}^{N} \log(1+h_b[n]P_a[n]) - \int_0^{h_b[n]} \frac{P_a[n]e^{-\frac{h_e[n]}{y_e}}}{1+h_e[n]P_a[n]}dh_e \quad (13a)$$

$$\text{s.t. (7c) and (7d).} \quad (13b)$$

Note that problem (P2) is still non-convex over the entire domain of $\mathbf{p}_a$. However, for the region under peak and average power constraints, the objective can be shown to be the sum of a concave and a convex functions. The proof is relegated to Appendix.

Since the objective function of problem (P2) is differentiable (as demonstrated in Appendix), it can be solved using the Karush-Kuhn-Tucker (KKT) conditions for non-convex problems [28, section 3.2.1]. We note that the KKT solution is the optimal solution for the non-convex problem only for very large value of N. This is because the *time-sharing* conditions for non-convex problems lead to negligible duality gap only when N is very large [29]. The KKT conditions relevant to the solution are defined as

$$\nabla f_0(x^*) + \lambda^* \nabla f_n(x^*) = 0, \quad (14a)$$

$$\lambda^* f_n(x^*) = 0, \quad (14b)$$

where f_0 is the objective in problem (P2), f_n are the constraints in (7c) and (7d) and x^* is the optimal value of P_a. Simultaneously solving (14) using [27, eq. 0.410 and 3.462.17] respectively, we obtain

$$-\left[\frac{h_b[n]}{1+h_b[n]P_a[n]} - \frac{1}{y_e(P_a[n])^2}e^{\frac{1}{y_eP_a[n]}}\left[\Gamma\left(-1,\frac{1}{y_eP_a[n]}\right) - \Gamma\left(-1,\frac{h_b[n]}{y_e}+\frac{1}{y_eP_a[n]}\right)\right]\right] \times \sum_{n=1}^{N} P_a[n] - \frac{1}{N}\bar{P}_{ab} = 0, \quad (15)$$

where $\Gamma(-i,z) = \frac{(-1)^i}{i!}(E_1(z) - e^{-z}\sum_{k=0}^{i-1}\frac{(-1)^k k!}{z^{k+1}})$ [30, eq. 8.4.15]). Solving (15) with a non-linear solver produces the suboptimal values of P_a.

B. OPTIMIZING THE UAV JAMMING POWER (P_u)

To optimize the jamming power $\mathbf{p}_u$ delivered by the UAV, we consider $\mathbf{p}_u$ as the optimization variable while fixing the values of $\mathbf{p}_a$ and $\mathbf{Q}$. Problem (P1) is then reformulated while substituting for $h_b[n]$ as

$$(P3): \max_{\mathbf{p}_u} \sum_{n=1}^{N} \log\left(1+\frac{\beta_o d_{ab}^{-\psi}P_a[n]}{P_u[n]\beta_o d_{qb}^{-2}[n]+1}\right) - e^{\frac{1}{y_eP_a[n]}} \times \left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{P_u[n]\beta_o d_{qb}^{-2}[n]+1}}{y_e} - \frac{1}{y_eP_a[n]}\right) - E_i\left(-\frac{1}{y_eP_a[n]}\right)\right] \quad (16a)$$

$$\text{s.t. (7a) and (7b).} \quad (16b)$$

Under the constraints, the objective of Problem (P3) is a non-convex function with respect to $\mathbf{p}_u$ due to the non-convexity of the information rate of the Eve. However, the information rate of Bob is concave with respect to $\mathbf{p}_u$. Hence, problem (P3) can be solved using successive convex approximation (SCA) approach [31], [32]. Note that SCA (also known as majorization minimization) is a popular optimization approach for solving this type of problems by iteratively solving a locally tight approximation of the original optimization problem, subject to a tight convex restriction of the constraint sets [32]. Given an initial UAV jamming power in the k-th iteration as $\mathbf{p}_u^k = \{P_u^k[n], n \in N\}$; we have using first order Taylor expansion that

$$e^{\frac{1}{y_eP_a[n]}}\left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{P_u[n]\beta_o d_{qb}^{-2}[n]+1}}{y_e} - \frac{1}{y_eP_a[n]}\right) - E_i\left(-\frac{1}{y_eP_a[n]}\right)\right] \le G_k[n] + T_k[n](P_u[n] - P_u^k[n]), \quad (17)$$

where

$$G_k[n] = e^{\frac{1}{y_eP_a[n]}}\left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{P_u^k[n]\beta_o d_{qb}^{-2}[n]+1}}{y_e} - \frac{1}{y_eP_a[n]}\right)\right.$$

$$- E_i\left(-\frac{1}{y_e P_a[n]}\right)\Bigg]$$

and $T_k[n] = \frac{P_a[n]\beta_o^2 d_{ab}^{-\psi} d_{qb}^{-2}[n] e^{-\left(\frac{\beta_o d_{ab}^{-\psi}}{y_e \beta_o d_{qb}^{-2}[n] P_u^k[n] + y_e}\right)}}{(\beta_o d_{qb}^{-2}[n] P_u^k[n]+1)(P_a[n]\beta_o d_{ab}^{-\psi} + \beta_o d_{qb}^{-2}[n] P_u^k[n]+1)}$.

Taking only the non-constant terms in (17), problem (P3) can be reformulated as

$$(P3b): \max_{\mathbf{p}_u} \sum_{n=1}^{N}\left[\log\left(1+\frac{\beta_o d_{ab}^{-\psi} P_a[n]}{P_u[n]\beta_o d_{qb}^{-2}[n]+1}\right) - T_k[n]P_u[n]\right] \tag{18a}$$

$$\text{s.t. (7a) and (7b).} \tag{18b}$$

Note that (P3b) maximizes the lower bound of the original objective problem, (P3a). Hence, it suffices that the objective value obtained by solving (P3b) is at least equal to the solution obtained by solving (P3a) using the updated P_u^k. As we iterate over k iterations, the Taylor expansion of (P3b) ensures that its objective value is the same as that of (P3a). Problem (P3b) is a convex problem within the constrained region and can be efficiently solved using interior-point method or a convex solver such as CVX [33], [34].

C. OPTIMIZING THE UAV TRAJECTORY (Q)

In this sub-problem, the problem (P1) is recast to ensure that only the UAV trajectory, $\mathbf{Q}$ is the optimization parameter. However, the reformulated problem is non-convex in Q. Hence, to reduce computational complexity, we introduce a slack variable $\boldsymbol{M} = \{m[n] = \|q[n] - w_b\|^2, n \in N\}$ such that $d_{qb}^{-2}[n] = \frac{1}{m[n]}$. Thus we obtain the following optimization problem:

$$(P4): \max_{\mathbf{Q},\mathbf{M}} m \sum_{n=1}^{N}\log\left(1+\frac{\beta_o d_{ab}^{-\psi} P_a[n]}{\frac{P_u[n]\beta_o}{m[n]}+1}\right) - e^{\frac{1}{y_e P_a[n]}} \times\left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{\frac{P_u[n]\beta_o}{m[n]}+1}}{y_e} - \frac{1}{y_e P_a[n]}\right) - E_i\left(-\frac{1}{y_e P_a[n]}\right)\right] \tag{19a}$$

$$\text{s.t. } m[n] - \|q[n] - w_b\|^2 \le 0, \tag{19b}$$

$$\text{and} \quad (4). \tag{19c}$$

Due to the non-convexity of problem (P4) with respect to the trajectory, $q[n]$, we reformulate the problem using successive approximation with the first order Taylor expansion. Let $Q_k[n] = \{q^k[n], n \in N\}$ denote the initial UAV trajectory for the kth iteration. Then the objective function of problem (P4) can be rewritten as

$$e^{\frac{1}{y_e P_a[n]}}\left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{\frac{P_u[n]\beta_o}{m[n]}+1}}{y_e} - \frac{1}{y_e P_a[n]}\right) - E_i\left(-\frac{1}{y_e P_a[n]}\right)\right] \le O_k[n] + W_k[n](q[n] - q^k[n]) \tag{20}$$

$$- \|q[n] - w_b\|^2 \le S^k[n], \tag{21}$$

where

$$O_k[n] = e^{\frac{1}{y_e P_a[n]}}\left[E_i\left(-\frac{\frac{\beta_o d_{ab}^{-\psi}}{\frac{P_u[n]\beta_o}{m_k[n]}+1}}{y_e} - \frac{1}{y_e P_a[n]}\right) - E_i\left(-\frac{1}{y_e P_a[n]}\right)\right]$$

$$W_k[n] = \frac{\beta_o^2 d_{ab}^{-\psi} P_u[n] e^{-\frac{\beta_o d_{ab}^{-\psi}}{y_e\left(1+\frac{\beta_o P_u[n]}{m_k[n]}\right)}}}{y_e\left(-\frac{1}{y_e P_a[n]} - \frac{\beta_o d_{ab}^{-\psi}}{y_e\left(1+\frac{\beta_o P_u[n]}{m_k[n]}\right)}\right)\left(1+\frac{\beta_o P_u[n]}{m_k[n]}\right) m_k^2[n]},$$

and $S^k[n] = \|q_k[n]\|^2 - 2[q_k[n] - w_b]^T q[n] - \|w_b\|^2$. Under similar conditions as of problem (P3), (P4) can be reformulated as

$$(P4b): \max_{\mathbf{Q},\mathbf{M}} \sum_{n=1}^{N}\log\left(1+\frac{\beta_o d_{ab}^{-\psi} P_a[n]}{\frac{P_u[n]\beta_o}{m[n]}+1}\right) - W_k[n]m[n]$$

$$\text{s.t. } m[n] + S^k[n] \le 0, \tag{22a}$$

$$\text{and} \quad (4). \tag{22b}$$

Problem (P4b) is a convex problem in $\mathbf{Q}$ under the specified constraints and can be solved using interior-point methods or with a convex solver. The overall procedure has been summarized in Algorithm 1.

Algorithm 1 Iterative Algorithm for Solving $\mathbf{p}_a$, $\mathbf{p}_u$, and $\mathbf{Q}$

1: Initialize $\mathbf{p}_u$ and $\mathbf{Q}$ such that the constraints in (7a), (7b) and (4) are satisfied.
2: $m \leftarrow 1$.
3: **repeat**
4: Compute and update $\mathbf{p}_a$ in (15) with given $\mathbf{p}_u$ and $\mathbf{Q}$.
5: Using updated $\mathbf{p}_a$ and current $\mathbf{Q}$, solve (18) for $\mathbf{p}_u$.
6: With given $\mathbf{p}_a$ and $\mathbf{p}_u$, find $\mathbf{Q}$ by solving problem (22).
7: Compute R_s as defined in (11).
8: $e = \frac{R_s^{new} - R_s^{old}}{R_s^{new}}$.
9: $m \leftarrow m + 1$.
10: **until** $e < \theta$ OR $m \ge m_{max}$.
11: **Output:** $\mathbf{p}_a$, $\mathbf{p}_u$, and $\mathbf{Q}$.

IV. SIMULATION RESULTS AND ANALYSIS

In this section, we evaluate the performance of the proposed solution approach through numerical simulations. We implement the solution discussed in Section III following the procedure described in Algorithm 1. The optimization parameters are initialized by solving the feasibility problem such that the the initial values just satisfy their respective constraints. The feasibility problem can be formulated by setting the objective of problem (12) to zero, with all the primary constraints unchanged. Then, by iteratively optimizing each parameter with the knowledge of the others, we obtain the suboptimal

TABLE 1. Simulation parameters.

Simulation parameter	Symbol	Value
Alice location	$\boldsymbol{w}_a$	$[0, 0, 0]$
Bob location	$\boldsymbol{w}_b$	$[300, 0, 0]$
Eve location	$\boldsymbol{w}_e$	$[150, 250, 0]$, $[350, 0, 0]$, $[300, 20, 0]$, $[300, 70, 0]$
Initial UAV location	$\boldsymbol{q}_o$	$[-100, 100, H]$
Final UAV location	$\boldsymbol{q}_f$	$[500, 100, H]$
UAV height(when fixed)	H	100m [19]
Velocity per sample(when fixed)	V	3m/s [19]
Duration per sample(when fixed)	δ	0.5s [19]
Signal-to-noise ratio	β_o	90dB [19]
Average received envelop power	y_e	20dBm
Average UAV transmit power	$\bar{P}_{ub}$	10dBm [19]
Maximum UAV power	P_{umax}	4Pub [19]
Average Source power	P_{ab}	30dBm [19]
Maximum source power	P_{amax}	36dBm [19]
Radius of uncertainty region (when fixed)	a	450m
Path loss for ground communication (urban area cellular radio)	u	3.4

solution to problem (P1) when the error (e) between steps is less than θ (where $\theta = 10^{-5}$) or the maximum number of iterations is reached (where $m_{max} = 200$).

Similar to the convergence analysis in [20], Algorithm 1 is guaranteed to converge for all feasible initial points. This is shown in Fig. 2 where a fast convergence is observed for different scenarios of the UAV flight time. In Fig. 2, the ProW algorithm represents the proposed solution to the unknown Eve problem while the associated numbers represent the UAV flight time. In all the simulations, we used the parameters as described in Table 1 unless otherwise specified.

We then analyze the secrecy rate performance of the proposed scheme as compared with the existing schemes. In Fig. 3, the performance of the unknown Eve location scenario using the proposed joint trajectory and power optimization algorithm (referred to as ProW) is compared the known Eve location scenario considered in [19] (referred to as JT&P). We also compare the performance with the baseline scheme without optimizing the UAV trajectory referred to as Straight), in which the UAV flies straight to the location above the eavesdropper. The associated numbers in the legends represent the respective Euclidean distances from Alice (source) to Bob for the ProW algorithm (recall unknown Eve location) and from Alice to Eve for the JT&P algorithm based on the locations specified in Table 1. Nevertheless, from Fig. 4 to Fig. 8, the numbers attached to the acronyms depict the UAV flight time in seconds. Results in Fig. 3 illustrate that the direct flight path with constant power (Straight) scheme performs the worst in terms of the average secrecy rate. Due to the jamming signals delivered by the UAV, the average secrecy rate of the JT&P scheme is zero when the Eve is at the same location as Bob. As Eve moves away from Bob,

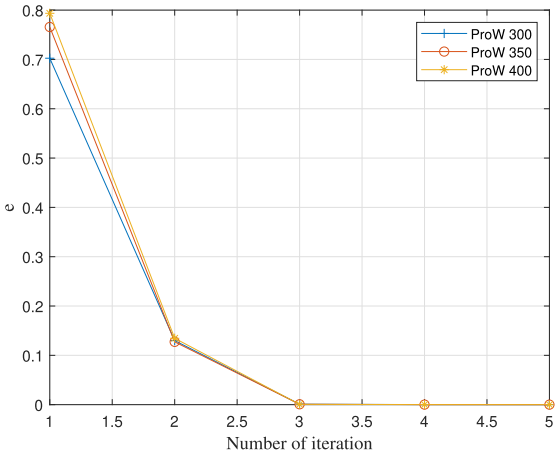

FIGURE 2. Convergence performance of Algorithm 1.

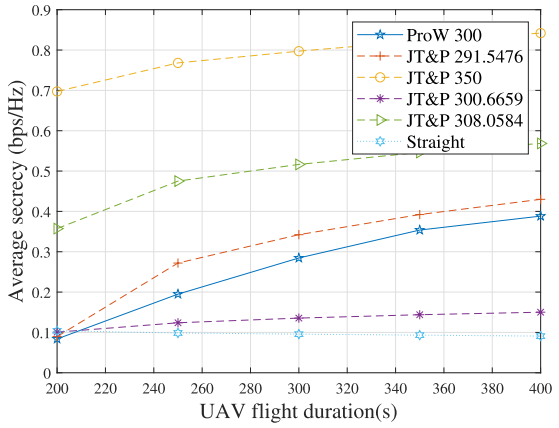

FIGURE 3. Average secrecy rate with 'unknown' as well as 'known' eavesdropper locations, and direct UAV flight path.

the average secrecy rate increases since the UAV locates Eve and stays at an optimum location to jam her signal. Nevertheless, since the location of Eve is unknown (as in ProW 300), the average secrecy rate is shown to be close to the JT&P scheme when Eve is closer to Alice and is supposed to receive more information content without the UAV jamming. However, considering that ProW 300 is near to a practical scenario, this marginal decrease in performance may be considered as the near practical trade-off to the scheme.

Also, it is important to note that the information rate of both Bob and Eve is affected by the jamming signal of the UAV. However, Eve is affected more, even when it has better channel condition (measured in terms of its average received envelope power), as the UAV regularly finds paths such that it stays further from Bob and estimates as close to Eve as possible until it flies to its final point. This allows for positive average secrecy rates shown in Fig. 3.

The flight trajectory of the UAV with respect to Alice and Bob is shown in Fig. 4. The 2D plot shows that from an aerial view, the trajectory of the UAV follows a given pattern bound by the uncertainty region of Eve (ellipse) provided it flies at a

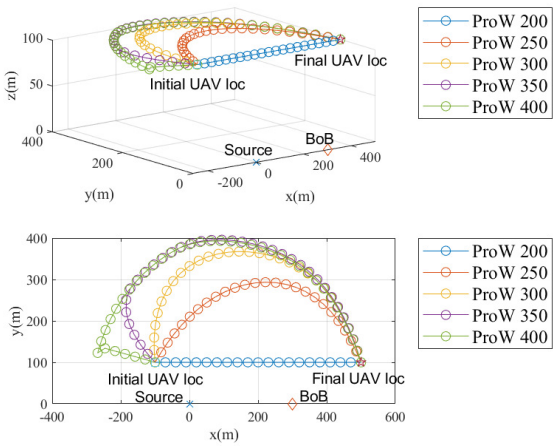

FIGURE 4. UAV flight trajectory in 2D and 3D view while Eve location is unknown (For clarity, we use $\delta = 10$).

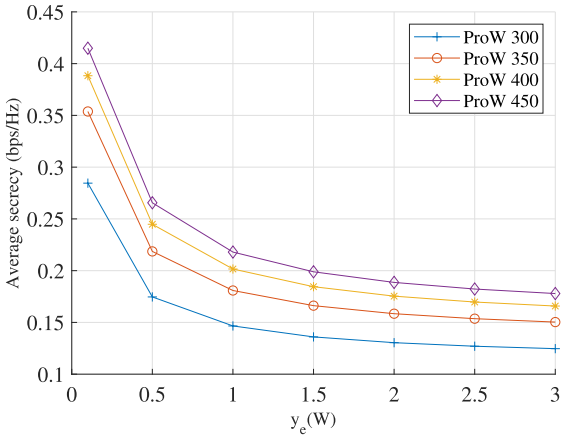

FIGURE 5. Effect of average received envelop power of Eve on average secrecy rate.

constant altitude. However, to demonstrate the effectiveness of the proposed approach in practice, we also plot a 3D view of the trajectory in Fig. 4. The 3D plot shows that the UAV trajectory moves towards the opposite of Bob while ensuring that the jamming signal is still delivered to all points within the constrained region of Eve.

Furthermore, Fig. 5 examines the constraints posed by the assumptions on the property of Eve's channel. We recall that the only known property of Eve is its average received envelop power, y_e. Hence Fig. 5 presents the effect of varying y_e on the average secrecy rate. It can be observed that increase in y_e decreases the average secrecy rate via a positive exponential path. Hence, for large values of y_e characterizing Eve having better reception equipment and channel state as compared to Bob, the decrement in average secrecy rate with respect to increasing y_e becomes negligible. The optimized UAV path ensures that even when the location of Eve is unknown, the average secrecy rate of the communication between Alice and Bob can be guaranteed despite Eve supposedly receiving signals with high envelope power. While

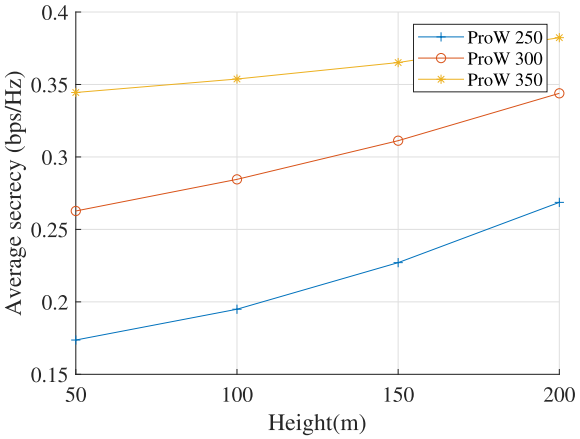

FIGURE 6. Influence of UAV altitude (height) on average secrecy rate under the proposed scheme.

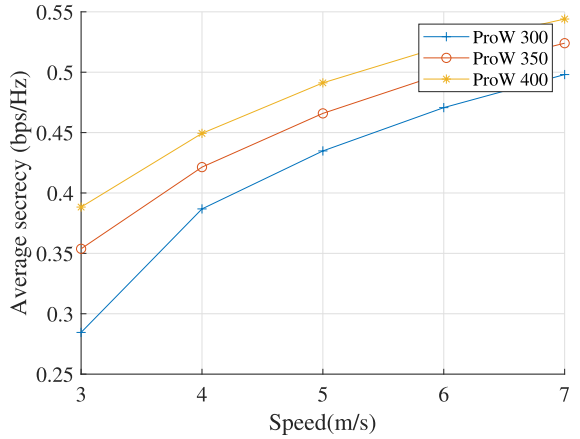

FIGURE 7. Influence of UAV flying speed on average secrecy rate with obscure Eve.

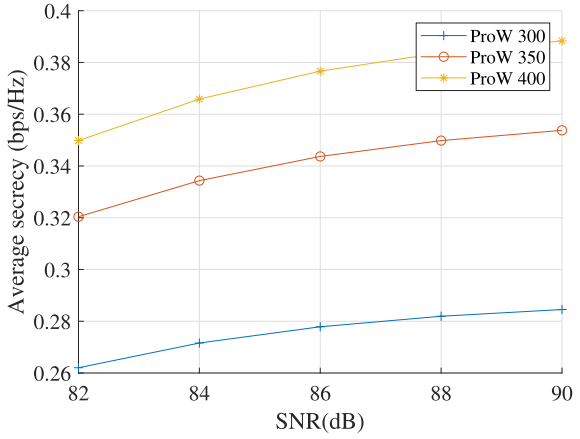

FIGURE 8. Average secrecy rate versus signal-noise-ratio (SNR) with obscure Eve.

this average secrecy rate is low, it can be improved by increasing the time of flight of the UAV or allowing the UAV to fly throughout the communication duration as shown in Figs. 3 and 5.

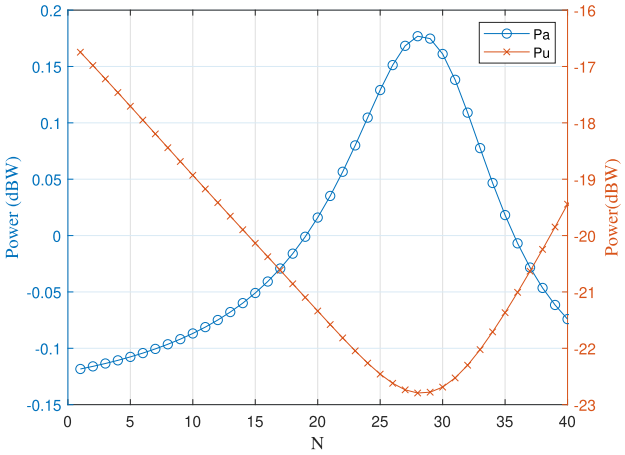

FIGURE 9. Comparing transmitted power between Alice and UAV.

Other factors that affect the average secrecy rate in the considered scenario of unknown eavesdropper location include the UAV height and speed, and the SNR of the environment. Figs. 6, 7 and 8 show the average secrecy rate of the proposed system compared to the UAV altitude, speed and ground node SNR, respectively. It can be observed that the impact of flying the UAV at higher altitude is minimal in terms of average secrecy rate, compared to allowing it to fly at longer duration. The trend in Fig. 6 suggests that the average secrecy rate increases with increase in the UAV altitude/height. However, we observed from our simulations that for large values of UAV flight altitude, the trajectory optimization problem (P4) becomes infeasible. Increasing the UAV speed and ground nodes SNR tend to increase the average secrecy rate with a logarithmic path. Nevertheless, the rate of increase is higher with the UAV speed than the SNR. As the UAV speed increases, its sample points increase allowing it to deliver more jamming signal to Eve within its flight time. Similar to results observed in [26], increasing the ground SNR improves the secrecy, however, this parameter is subject to characteristics of the outdoor environment which cannot be easily controlled.

The optimized transmitting power of Alice (P_a) and the optimized UAV jamming power (P_u) are plotted in Fig. 9. While Alice transmits at its maximum power when the UAV is close to Bob, the UAV transmits minimum jamming signal. This ensures that the UAV interference to Bob is minimal and Bob continues to receive the information sent by Alice.

V. CONCLUSION

In this paper, we have exploited UAV-aided jamming technique in reducing the information rate received by an eavesdropper in an unknown location. We solved the achievable secrecy rate maximization problem using sequential block coordinate optimization method. While we were constrained by the elusive nature of the eavesdropper location, we obtained a secrecy rate that is comparable to a scenario when the eavesdropper's location is known. We also showed that the UAV speed and flight duration are amongst the main parameters to consider while using UAV to increase physical layer security. Most importantly, we have demonstrated that the average received envelope power of the eavesdropper cannot guarantee better information content as the secrecy rate tends to stabilize with large envelope power. We propose that future works investigate predicting the eavesdropper location with the aid of deep learning techniques in order to update the UAV flight path in real-time. This could reduce the latency in continuously solving the optimization problem for each communication block.

APPENDIX

In this section, we show that the non-convexity of (10) is the sum of a concave and a convex functions in terms of P_a. From (10), we obtain

$$R_s = \sum_{n=1}^{N} \underbrace{\log(1 + h_b[n]P_a[n])}_{f_1(P_a)} - \underbrace{\int_0^{h_b[n]} \frac{P_a[n]e^{-\frac{h_e[n]}{y_e}}}{1 + h_e[n]P_a[n]} dh_e}_{f_2(P_a)}. \quad (23)$$

We consider (23) in two parts, showing their convexity with the second derivative method. In general, the convexity of a function is defined as [28]

$$f''(x) = \begin{cases} Convex & :> 0 \\ Concave & :< 0 \\ Affine & := 0. \end{cases}$$

Thus we have from (23) that

$$f_1''(P_a) = -\left(\frac{h_b}{1 + h_b P_a}\right)^2.$$

We then show the convexity of the $f_2(P_a)$ using the principle that the nonnegative weighted-sum of a convex (concave) function is a convex (concave) [28, Section 3.2.1]. The second part can be rewritten as

$$\int_0^{h_b[n]} e^{-\frac{h_e[n]}{y_e}} \frac{P_a[n]}{1 + h_e[n]P_a[n]} dh_e \equiv \int_0^{h_b[n]} w(h_e) f(P_a, h_e) dh_e.$$

It has been shown in [28] that if $f(P_a, h_e)$ is convex (concave), then $f_2(P_a)$ is convex (concave). Thus, we have that the second derivative of $f_2(P_a)$ as

$$f_2''(P_a) = -\frac{2h_e}{(1 + h_e P_a)}.$$

Thus both parts of (23) are concave functions independently under the constraint of $h_b \geq 0$ and $P_a \geq 0$. These are the positive semi-definite constraints that guarantees communication between the source and the destination. If $h_b < 0$ and/or $P_a < 0$ then no information could be transmitted

successfully. Therefore, we have that (23) is the sum of a concave and a convex function ($-f(x) =$ convex if $f(x) =$ concave) in terms of P_a.

REFERENCES

[1] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun. Mag.*, 2019. [Online]. Available: https://arxiv.org/pdf/1902.06700.pdf

[2] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[3] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[5] M. R. A. Khandaker and K.-K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, Jan. 2015.

[6] M. R. A. Khandaker and K.-K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 10–13, Feb. 2015.

[7] A. A. Okandeji, M. R. A. Khandaker, K.-K. Wong, G. Zheng, Y. Zhang, and Z. Zheng, "Secure full-duplex two-way relaying for SWIPT," *IEEE Wireless Commun. Lett.*, vol. 7, no. 3, pp. 336–339, Jun. 2018.

[8] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[10] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over Non-Small-Scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

[11] F. Cheng, S. Zhang, Z. Li, Y. Chen, N. Zhao, F. R. Yu, and V. C. M. Leung, "UAV trajectory optimization for data offloading at the edge of multiple cells," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6732–6736, Jul. 2018.

[12] S. Zhang, Y. Zeng, and R. Zhang, "Cellular-enabled UAV communication: A connectivity-constrained trajectory optimization perspective," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2580–2604, Mar. 2019.

[13] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Jun. 2017.

[14] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, "UAV-enabled secure communications: Joint trajectory and transmit power optimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, Apr. 2019.

[15] Q. Wu and R. Zhang, "Common throughput maximization in UAV-enabled OFDMA systems with delay consideration," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6614–6627, Dec. 2018.

[16] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.

[17] A. Ahmed, S. Zhang, and Y. D. Zhang, "Multi-target motion parameter estimation exploiting collaborative UAV network," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*. Brighton, U.K: IEEE, May 2019, pp. 4459–4463.

[18] H. Wang, J. Wang, J. Chen, Y. Gong, and G. Ding, "Network-connected UAV communications: Potentials and challenges," *China Commun.*, vol. 15, no. 12, pp. 111–121, Dec. 2018.

[19] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 181–184, Feb. 2019.

[20] Z. Li, M. Chen, C. Pan, N. Huang, Z. Yang, and A. Nallanathan, "Joint trajectory and communication design for secure UAV networks," *IEEE Commun. Lett.*, vol. 23, no. 4, pp. 636–639, Apr. 2019.

[21] L. Shen, N. Wang, and X. Mu, "Iterative UAV trajectory optimization for physical layer secure mobile relaying," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*. Zhengzhou, China: IEEE, Oct. 2018, pp. 19–23.

[22] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.

[23] A. Li and W. Zhang, "Mobile jammer-aided secure UAV communications via trajectory design and power control," *China Commun.*, vol. 15, no. 8, pp. 141–151, Aug. 2018.

[24] Y. Gao, H. Tang, B. Li, and X. Yuan, "Joint trajectory and power design for UAV-enabled secure communications with no-fly zone constraints," *IEEE Access*, vol. 7, pp. 44459–44470, 2019.

[25] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 9042–9046, Sep. 2018.

[26] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 564–567, Apr. 2019.

[27] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed., A. Jeffrey and D. Zwillinger, Eds. New York, NY, USA: Academic, 2007.

[28] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U. K.: Cambridge Univ. Press, 2004.

[29] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1322, Jul. 2006.

[30] F. W. J. Olver, W. Lozier, F. B. Daniel, and W. C. C. Ronald, Eds., *NIST Handbook of Mathematical Functions*. Cambridge, U.K.: Cambridge Univ. Press, Jul. 2010. [Online]. Available: https://dlmf.nist.gov/8.4

[31] Y. Yang, M. Pesavento, S. Chatzinotas, and B. Ottersten, "Successive convex approximation algorithms for sparse signal estimation with non-convex regularizations," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 6, pp. 1286–1302, Dec. 2018.

[32] M. Razaviyayn, "Successive convex approximation: Analysis and applications," Ph.D. dissertation, Univ. Minnesota, Minneapolis, MN, USA, 2014.

[33] M. Grant and S. Boyd, *Recent Advances in Learning and Control* (Lecture Notes in Control and Information Sciences). Springer-Verlag, Mar. 2008, pp. 95–110.

[34] *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: http://cvxr.com/cvx

CHRISTANTUS OBINNA NNAMANI received the B.Eng. degree in electronic engineering and the M.Eng. degree in telecommunication engineering from the University of Nigeria Nsukka, in 2011 and 2015, respectively. He is currently pursuing the Ph.D. degree with the School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, U.K., under the sponsorship of the Petroleum Technology Development Fund (PTDF), Nigeria.

He was an Erasmus Mobility Student (under the DREAM Project ACP-18) with the Universita degli studi di Cagliari, Italy, from 2015 to 2016. He is an academic staff of the Department of Electronic Engineering, University of Nigeria Nsukka. He has authored and/or coauthored several academic papers and proceedings. His research interests include UAV, network security, resource allocation, and network modeling.

Dr. Nnamani is a member of the European Association for Signal Processing (EURASIP) and a corporate member of the Council for the Regulation of Engineering in Nigeria (COREN). He is also a member of the review panel to the IEEE Wireless Communication Letters and Elsevier's *Cogent Engineering* journals.

MUHAMMAD R. A. KHANDAKER (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer science and engineering from Jahangirnagar University, Dhaka, Bangladesh, in 2006, the M.Sc. degree in telecommunications engineering from East West University, Dhaka, in 2007, and the Ph.D. degree in electrical and computer engineering from Curtin University, Australia, in 2013.

He was a Postdoctoral Researcher with the Department of Electronic and Electrical Engineering, University College London, U.K., from 2013 to 2018. He is currently an Assistant Professor with the School of Engineering and Physical Sciences, Heriot-Watt University, U.K.

Dr. Khandaker received the Curtin International Postgraduate Research Scholarship for the Ph.D. degree, in 2009. He was a recipient of the Best Paper Award in the 16th IEEE Asia–Pacific Conference on Communications, Auckland, New Zealand, in 2010. He served as the Lead Guest Editor for EURASIP JWCN special issue on Heterogeneous Cloud Radio Access Networks as well as the Managing Guest Editor for *Physical Communication* (Elsevier), Special Issue on Self-Optimizing Cognitive Radio Technologies. He is currently serving as an Editor for the IEEE COMMUNICATIONS LETTERS, IEEE ACCESS, and *EURASIP Journal on Wireless Communications and Networking* (JWCN).

MATHINI SELLATHURAI (Senior Member, IEEE) is currently a Full Professor in signal processing and intelligent systems with Heriot-Watt University, Edinburgh, U.K. In her 15-year research on signal processing for communications, she has made seminal contributions on MIMO wireless systems. She has published 200 IEEE entries, given invited talks, and has written a book and several book chapters in topics related to this project. She is a Fellow of the Higher Education Academy. She is also member of the IEEE SPCOM Technical Strategy Committee, from 2014 to 2018, and an Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, from 2009 to 2014 and from 2015 to 2018. She received the IEEE Communication Society Fred W. Ellersick Best Paper Award, in 2005, Industry Canada Public Service Awards for contributions in science and technology, in 2005, and a Best PhD thesis medal from NSERC, Canada, in 2002. She was also the General Co-Chair of IEEE SPAWC2016 in Edinburgh.