American Journal of Networks and Communications
2024; 3(1): 64-74
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20241301.15
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

Trajectory Optimization and Power Allocation Scheme for a UAV Relay-aided Network in the Presence of an Eavesdropper

Jishan E Giti[1, *], Shah Ariful Hoque Chowdhury[2], Al-Hadith Moon[1]

[1]Department of Electrical and Electronic Engineering, Rajshahi University of Engineering and Technology, Rajshahi, Bangladesh
[2]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology, Rajshahi, Bangladesh

Email address:

jishan.e.giti@gmail.com (Jishan E Giti), arif.1968.ruet@gmail.com (Shah Ariful Hoque Chowdhury),
alhadithmoon2000@gmail.com (Al-Hadith Moon)
*Corresponding author

To cite this article:

Jishan E Giti, Shah Ariful Hoque Chowdhury, Al-Hadith Moon. Trajectory Optimization and Power Allocation Scheme for a UAV Relay-aided Network in the Presence of an Eavesdropper. *American Journal of Networks and Communications, 3*(1), 64-74. https://doi.org/10.11648/j.ajnc.20241301.15

Received: 22 March 2024; **Accepted:** 22 April 2024; **Published:** 27 May 2024

Abstract: The information theoretical security for a cellular network in the presence of an eavesdropper is investigated in this research. The network is single-input-single-output (SISO) in nature. A small unmanned aerial vehicle (UAV) is aiding the network as a relay that follows the decode-and-forward (DF) protocol. The relay decodes the transmitted signal and retransmits it to the destination while repositioning itself if required. The allotted power of the UAV may not be enough for long-distance and long-duration travel. This article deals with the power needed for the data transmission so that the UAV can operate as a relay with less transmit power. However, the confidential data transmission between a base station and a mobile device is being intercepted by a passive eavesdropper. The security issue affects the transmit power and the outage situation. The theory of physical layer security is employed to ensure a secure wireless transmission. The secrecy parameters, namely, the secrecy capacity and the secrecy outage probability are investigated via mathematical derivations and computer programming. Additionally, optimizing the trajectory and allocation of the transmit power budget of the UAV will increase the network's reliability. Our results show that the UAV relay can handle a secure transmission with its limited resources if a budget power allocation can be achieved along with an optimized trajectory.

Keywords: Power Allocation, Secrecy Capacity, Secrecy Outage Probability, Trajectory Optimization, UAV Relay

1. Introduction

Unmanned aerial vehicles (UAVs) have become highly popular in various sectors like military, tourism, geology and even in personal interests. In the military, they serve for surveillance, reconnaissance, and precision strikes. In the public and civil domains, they excel in tasks like environmental monitoring, disaster assessment, and efficient goods delivery [1, 2]. Recently, a growing interest has been in utilizing UAVs as communication relays. This involves using UAVs as aerial platforms to improve connectivity and data transmission, especially in remote or challenging areas where traditional communication infrastructure is lacking [3, 4].

Numerous research works can be found in wireless communications using a UAV relay. However, investigating physical layer security in those cases is found to be few. Classical security solutions may not be implementable on UAVs since they lack enough memory and CPU power to perform cryptographic approaches. Hence, physical layer security creates an interest in maintaining security and reliability in drone applications.

The authors in this paper address a UAV relay network operating on a Single-Input Single-Output (SISO) Rayleigh fading channel. The scenario falls under the category of drone to networks communication. The UAV extends the coverage range between the Base Station (BS), Mobile Device (MD),

and an eavesdropper by acting as a Decode-and-Forward (DF) relay. The system model and problem formulation are inspired by the works of Zeng et. al. [3] who worked with the power allocation and trajectory optimization problem of a UAV relay. The communication was in the uplink and no eavesdropper or attacker was included. The authors in this article added an eavesdropper in that network so that an investigation of secrecy can be done while understanding the capability of the UAV relay under the constraint of limited resources. The contributions of this article are as follows:

1. A private downlink communication is considered to be aided by a UAV relay. Simultaneously, the presence of an eavesdropper is considered which intercepts the confidential data.
2. The primary objective is to maximize secrecy capacity and minimize secrecy outage probability by optimizing the UAV's trajectory and transmit power.

The structure of this article is as follows: Section 1 consists of introductory information. Section 2 is based on the literature review. Section 3 discusses the system model and the problem to be investigated. Section 4 investigates the trajectory optimization and power allocation process for the UAV relay. Finally 5 and 6 discuss the results and concluding remarks, respectively.

Table 1. *Brief summary of previous works.*

Ref. No.	Uplink(UL) /Downlink (DL)	Relay	Eavesdropp	Investigated Parameters
[22]	DL	stationary, DF	Adaptive	Secrecy Capacity, Friendly jamming
[28]	UL	UAV	Active	Active eavesdropper detection by unsupervised learning
[26]	DL, UL	UAV	×	User scheduling at cellular border
[29]	DL	multiple UAVs	passive	Secrecy Capacity, UAV swarm collaboration, Energy efficiency
[2]	UL	single UAV, DF	×	Outage Probability, Trajectory optimization, Power allocation
Our work	DL	single UAV, DF	Passive	Secrecy Capacity, Secrecy Outage Probability, Trajectory optimization, Power allocation

2. Related Works

Secure transmission in wireless communications using cryptographic approaches was initiated by Shannon [5] in 1949. However, providing secure communication over wireless networks using a cryptographic approach with the help of encryption keys presents significant challenges since the wireless medium is open in nature and thus allows eavesdroppers and attackers to intercept information transmission or degrade the quality of transmission. The expression of secrecy capacity was derived certainly from Shannon's capacity theorem [5]. In 2006, Barros and Rodrigues [6] characterized secrecy capacity in terms of outage probability for a quasi-static Rayleigh fading SISO channel. For a transmitter unknown of the eavesdropper channel, they defined the probability of transmitting at a target secrecy rate R_s greater than the secrecy capacity C_s as the probability that the information-theoretic security is compromised.

Relays came in to help to retransmit data from transmitters to receivers, thus preventing data loss due to fading or attenuation. Many networks need relays for quality transmission thus making them a matter of interest. Proper relay precodings can help to mitigate interference and relays can be used as jammers too. Therefore, researchers investigated various relay functions such as beamforming, relay precoding, cooperative relaying, and co-operative jamming, to gain diversity and array gain [7, 8], to tackle interference [9–11], to communicate using multiple relays in cooperation [12, 13], and even to jam adversaries [14–18], respectively.

Existing literature includes lots of works about stationary relays and their usefulness in regular wireless transmission [10, 19, 20], and playing a role in enhancing security [18, 21, 22]. Recently, a growing interest has been in utilizing UAVs as communication relays since they are lightweight and mobile.

Due to the increasing use of UAVs, some issues also arose. The security, privacy and reliability of data, along with the regulation, and ownership of the UAV relays became the matters of concern. Various security-critical applications may observe a failure by the relays to provide complete security of data, and that results in a great loss. A cyber attack on the UAVs may introduce life-threatening risks. Since UAVs may not handle many computation complexities, physical layer security is a great alternative to enhance security.

Extensive research has been conducted in the literature to explore the potential of UAV relays in enhancing communication coverage. A network architecture deploying UAV relay platforms was presented by Ayyagari et al. [23]. The architecture mimicked cellular towers in the sky for implementing rapidly deployable broadband wireless networks. The authors try to optimize the UAV's flight path and communication settings to achieve a balance between energy conservation and effective relay performance in [24]. Another study emphasizes integrating UAVs into public safety communications to supplement conventional technologies, enabling dependable and high-speed data transmission during crucial situations [25]. Optimizing UAV trajectory to enhance the sum rate of edge users of multiple cells was investigated by Cheng et al [26]. Authors introduces a novel method for optimizing UAV flight paths and communication resource allocation in two-way relaying setups, focusing on enhancing channel secrecy capacity by considering eavesdroppers in [27]. Detection of active eavesdroppers using machine learning is

the topic of [28]. Recently, Sun et al. studied a collaboration of UAV swarms to employ a virtual antenna array for an energy-efficient secure system [29]. A similar concept can be found in a conference paper by Shi et al. [30].

We highlighted some of the previous works in the literature in Table 1 to draw some comparisons with our works. As we can see some of these have stationary relays, and others have UAVs as relays. Our work includes the presence of both a UAV relay and an eavesdropper which is found in very few articles.

3. System Model and Problem Formulation

The system model is illustrated in Figure 1. The communication occurs between a Base Station (BS) and a Mobile Device (MD). The MD is located beyond the BS's coverage area. A UAV serves as a Decode-and-Forward (DF) relay, adjusting its position and transmit power to enhance transmission quality. The whole system is considered single-input-single-output (SISO), and the channel fadings follow the Rayleigh distribution considering there is no line-of-sight (LoS) between the source (BS) and the destination (MD). However, there's a challenge due to the presence of an eavesdropper (Eve) capable of intercepting the data.

The primary goal is to optimize UAV power allocation and trajectory to achieve two objectives: maximize the MD's channel capacity for improved communication quality while minimizing Eve's channel capacity to prevent unauthorized data access. The UAV is a battery-powered multi-rotor drone usually used for civilian applications. Therefore, the weight of the battery is an overhead for the system. These battery-powered UAVs tend to have a short endurance, they cannot operate for more than 90 minutes with Li-ion batteries [31, 32]. Therefore a joint trajectory optimization and power allocation (JTO-PA) scheme is also necessary.

The transmission duration covers N time slots, denoted as $\mathcal{N} = 1, ..., N$. Each slot consists of two phases namely, the broadcasting phase and then the relaying phase. In the first phase, the antenna transmits signal x_s^t to the UAV relay. In the second phase, the UAV decodes the signal and re-encodes it as x_r^t. After that, the UAV simultaneously transmits it to both MD and Eve. For the sake of simplicity, throughout the paper, the parameters relating to BS, UAV, MD and EVE can be found having subscripts as S, R, D and E, respectively. We have the BS located at $(0, 0, H)$, the MD located at $(D, 0, 0)$, and the Eve located at $(E, 0, 0)$. The antenna is elevated H meters above the ground and is positioned at a distance of D meters from the receiver (MD). The matrix $\mathbf{L}$ represents the UAV's trajectory from time slots 2 to N. Each row in matrix $\mathbf{L}$ indicates the UAV's location in time slot $t + 1$, denoted by coordinates $(x_{t+1}, y_{t+1}, z_{t+1})$. To calculate distances, we use the following formulas:

Distance between BS and UAV: $D_{SR}^t = \sqrt{(x_t^2 + y_t^2 + (z_t - H)^2)}$ Distance between UAV and MD: $D_{RD}^t = \sqrt{((x_t - D)^2 + y_t^2 + z_t^2)}$ Distance between UAV and Eve: $D_{RE}^t = \sqrt{((x_t - E)^2 + y_t^2 + z_t^2)}$

The variable $s_{t+1,t}$ represents the UAV's travel distance during the time period t. There's a fundamental constraint that the UAV cannot cover a distance greater than v within a single time period, where v is significantly less than D. The condition $s_{t+1} \leq v$ restricts the UAV's movement, ensuring it doesn't exceed this distance in each time slot. A list of notations used in this article is shown in the table 2.

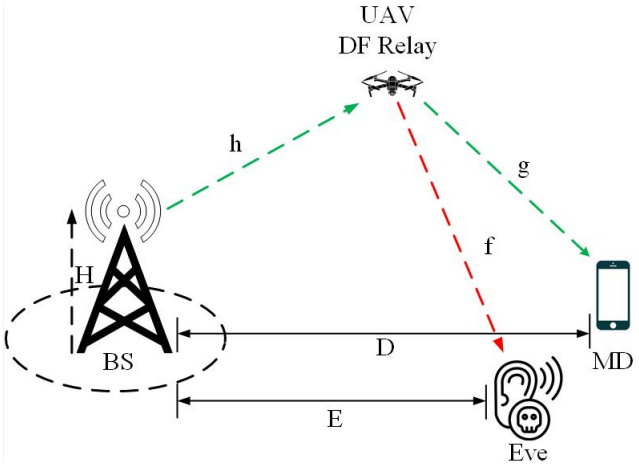

Figure 1. *UAV DF Relay networking system model.*

Table 2. *List of Notations.*

Notation	Description
h, g and f	Channel coeff. of BS-UAV,UAV-MD and UAV-Eve links, respectively.
P_s and P_u	The transmit power of the Base station and UAV relay, respectively.
N_{0D} and N_{0E}	The noise variance of destination (MD) and Eavesdropper (Eve), respectively.
S, R, D and E	Used as subscripts for some parameters denoting the entities, source (BS), Relay (UAV), Destination (MD), and Eavesdropper (Eve), respectively.
γ_{XY}	$=\frac{\lvert\omega\rvert^2 P_X}{N_{0Y}}$, instantaneous SNR of X-Y link with channel coefficient equals to ω.
$\overline{\gamma}_{XY}$	$=\frac{P_X \Lambda_{XY}}{N_{0Y}}$, average SNR of X-Y link
ξ_{th}	SNR threshold of a link, below which a signal degradation may happen.
C_s	Secrecy capacity.
P_{out}	Outage probability.
N	Total number of time slots for data transmission.
α	Path-loss coefficient.

Matrix $\mathbf{P}$ is utilized to prevail transmit powers of both the UAV and the transmitter across N time slots. Each row in matrix $\mathbf{P}$ represents the transmit powers of the source antenna and the UAV during time slot t, denoted as (p_s^t, p_u^t). To increase power efficiency, the total transmit power in each time slot is constrained, i.e., $p_U^t + p_s^t \leq P_{max}$.

Since it is assumed that the channel is Rayleigh faded, path-loss and small-scale fading both affect the channel gain. As a result, the received signal at the UAV during the first phase of time slot t is represented mathematically as follows:

$$y_{UAV}^t = \sqrt{P_s^t (D_{SR}^t)^{-\alpha}} h x_s^t + z_R,$$

$$y_{MD}^t = \sqrt{P_u^t (D_{RD}^t)^{-\alpha}} g x_r^t + z_D,$$

$$y_{Eve}^t = \sqrt{P_u^t (D_{RE}^t)^{-\alpha}} f x_r^t + z_E,$$

where, x_s^t, x_r^t, = transmit unit energy of the source and relay, respectively, α = path loss coefficient, channel coefficients $[(BS \to UAV), (UAV \to MD), (UAV \to Eve)]$: f, g, h = $\sim \mathcal{CN}(0,1)$, z_R, z_D and z_E = noise received at UAV, MD and Eve respectively.

According to the above equations, the signal-to-noise ratio (SNR) at the UAV, destination (MD) and Eavesdropper(Eve) channel in time slot t can be given as, respectively,

$$\gamma_{UAV}^t = (p_s^t (D_{SR}^t)^{-\alpha} |h|^2)/N_0$$

$$\gamma_{MD}^t = (p_u^t (D_{RD}^t)^{-\alpha} |g|^2)/N_0$$

$$\gamma_{Eve}^t = (p_u^t (D_{RE}^t)^{-\alpha} |f|^2)/N_0$$

For complex Gaussian distribution channel capacity

$$C_{main}^t = \log_2(1 + \min(\gamma_{UAV}^t, \gamma_{MD}^t)) \text{ bits/s/Hz} \quad (1)$$

$$C_{Eve}^t = \log_2(1 + \gamma_{Eve}^t) \text{ bits/s/Hz} \quad (2)$$

The secrecy capacity will be as given by (3).

$$C_S = [C_{main}^t - C_{Eve}^t]^+ = \log_2 \left[\frac{1 + \min(\gamma_{UAV}^t, \gamma_{MD}^t)}{1 + \gamma_{Eve}^t} \right]^+ \text{ bits/s/Hz.} \quad (3)$$

The secrecy capacity is the security measure that on this transmission rate, no eavesdropper will be able to intercept the confidential data.

The outage probability represents the chance of signal degradation due to insufficient Signal-to-Noise Ratio (SNR) values falling below a specified threshold (ξ_{th}). It applies to the links between the Base Station (BS) and the UAV, as well as between the UAV and the Mobile Device (MD). Similarly, it applies to the likelihood that the SNR at Eve drops below ξ_{th}. These outage probabilities estimate the risk of signal deterioration caused by low SNR values in each link.

$$P_{out}^t(BS \to UAV) = Pr(\gamma_{UAV}^t < \xi_{th}) \quad (4)$$

$$P_{out}^t(UAV \to MD) = Pr(\gamma_{MD}^t < \xi_{th}) \quad (5)$$

$$P_{out}^t(UAV \to Eve) = Pr(\gamma_{Eve}^t < \xi_{th}) \quad (6)$$

For the Rayleigh Faded SISO channel, we consider the probability density function (PDF) to is $f(\phi) = exp(\frac{-\phi/2}{2})$ To achieve successful communication from the Base Station (BS) to the Mobile Device (MD), two consecutive links must have successful transmissions: from BS to the UAV $(BS \to UAV)$ and from the UAV to the MD $(UAV \to MD)$. The outage probability for the communication from the BS to the MD during time slot t, denoted as P_{out}^t, can be expressed as:

P_{out}^t for the legitimate channel:

$$\begin{aligned} P_{out}^t(main) &= 1 - (1 - P_{out}^t(BS \to UAV)) \times (1 - P_{out}^t(UAV \to MD)) \\ &= 1 - \exp\left(\left(-\frac{N_{0D}\xi_{th}}{2} \right) \left(\frac{1}{P_s^t (D_{SR}^t)^{-\alpha}} + \frac{1}{P_u^t (D_{RD}^t)^{-\alpha}} \right) \right) \end{aligned} \quad (7)$$

and also for the eavesdropper channel:

$$\begin{aligned} P_{out}^t(Eve) &= 1 - (1 - P_{out}^t(BS \to UAV)) \times (1 - P_{out}^t(UAV \to Eve)) \\ &= 1 - \exp\left(\left(-\frac{N_{0E}\xi_{th}}{2} \right) \left(\frac{1}{P_s^t (D_{SR}^t)^{-\alpha}} + \frac{1}{P_u^t (D_{RE}^t)^{-\alpha}} \right) \right) \end{aligned} \quad (8)$$

Our main goal is to minimize the overall outage probability by optimizing both the UAV's trajectory and power allocation. Considering that power and location factors in each time slot have an impact on the outage probability for that slot, we can simplify the optimization by focusing on minimizing the outage probability for a single time slot. To achieve this, we formulate the problem as follows:

$$\begin{aligned} &\min_{\mathbf{P,L}} \sum_{t\in\mathcal{N}} P_{out}^t \\ &s.t. \quad P_s^t + P_u^t \le P_{max}, \quad \forall t \in \mathcal{N}, \\ &P_s^t > 0, \quad P_u^t > 0 \quad \forall t \in \mathcal{N}, \\ &\qquad s_{t,t-1} \le v, \quad \forall t \in \mathcal{N} \setminus \{1\}, \end{aligned} \tag{9}$$

Equation (9) represents the power constraints and mobility constraints. The first three equalities relate to the power constraints while the last equality denotes the mobility constraints.

4. Trajectory Optimization and Power Allocation

To address the non-convexity of (9), we split the problem into two parts: power allocation and trajectory optimization. These subproblems are solved iteratively. In the power allocation subproblem, we optimize UAV power subject to constraints. In the trajectory optimization subproblem, we determine the best UAV path to minimize outage probability. The joint trajectory optimization and power allocation (JTOPA) algorithm alternates between these subproblems until convergence, ensuring an efficient solution is reached.

4.1. Trajectory Optimization

When the transmit power values for the UAV, MD, and Eavesdropper are known for each time slot, we can express problem (3) as an optimization task to minimize the outage probability based on the given power allocations for all parties involved.

$$\begin{aligned} &\min_{\mathbf{L}} \sum_{t\in\mathcal{N}} P_{out}^t \\ &\text{s.t.} \quad s_{t,t-1} \le v, \quad \forall t \in \mathcal{N} \setminus \{1\} \end{aligned} \tag{10}$$

To efficiently tackle the non-convexity of problem (10) related to **L**, we adopt a sequential approach by dividing it into $N-1$ subproblems. Each subproblem focuses on independently minimizing the outage probability for a specific time slot. This means that we optimize the UAV trajectory (**L**) for each time slot separately, taking into account the specific conditions and constraints of that particular time slot. The subproblem for time slot t can be represented as:

$$\begin{aligned} &\min_{x_t,y_t,z_t} \sum_{t\in\mathcal{N}} P_{\text{out}} \\ &\text{s.t.} \quad s_{t,t-1} \le v \end{aligned} \tag{11}$$

P_{out}^t is the function of $q(x) = 1 - \exp\left(-\frac{\xi_{th} N_0}{2} x\right)$ and $\delta(x_t, y_t, z_t) = (\frac{\sqrt{((x_t-D)^2+y_t^2+z_t^2)^\alpha}}{P_s^t} + (\frac{\sqrt{(x_t^2+y_t^2+(z_t-H)^2)^\alpha}}{P_u^t} + \frac{\sqrt{((x_t-E)^2+y_t^2+z_t^2)^\alpha}}{P_u^t}$. The function $\delta(x_t, y_t, z_t)$ is linked to the UAV's performance, increasing as it nears its destination. This results in the derived function $q(x)$ also being monotonically increasing. Leveraging the UAV's improved performance as it approaches its target can help reduce the outage probability P_{out}, as defined in (11).

The subproblem (11) is a convex optimization problem satisfying Slater's condition, ensuring a zero duality gap [33]. Thus, we can efficiently solve it by tackling its dual problem. Using the Lagrange multiplier λ for the moving distance constraint, the Lagrangian function $L(x_t, y_t, z_t, \lambda)$ combines the objective function $\delta(x_t, y_t, z_t)$ and the Lagrange term for distance constraints $(s_{t,t-1} - v)$. Solving the dual problem helps find the optimal UAV trajectory effectively. So, the Lagrangian of subproblem (11) is

$$L(x_t, y_t, z_t, \lambda) = \delta(x_t, y_t, z_t) + \lambda(s_{t,t-1} - v). \tag{12}$$

and the objective is

$$q(\lambda) = \inf_{x_t,y_t,z_t} L(x_t, y_t, z_t, \lambda) \tag{13}$$

Thus the problem explained in (11) can be explained by

$$\begin{aligned} &\max_{\lambda} q(\lambda) \\ &s.t. \lambda \ge 0 \end{aligned} \tag{14}$$

Since the function $q(\lambda)$ lacks differentiability, we employ the subgradient method to solve the dual problem (14). This method involves searching for feasible solutions by following selected subgradient directions. At the p-th iteration, we define the subgradient M^p as follows:

$$M^p = \sqrt{(x_t^p - x_{t-1})^2 + (y_t^p - y_{t-1})^2 + (z_t^p - z_{t-1})^2} - v \tag{15}$$

Here, (x_t^p, y_t^p, z_t^p) corresponds to the values that minimize the Lagrangian $L(x_t, y_t, z_t, \lambda^p)$ at the p-th iteration [34]. To put it simply, we compute the subgradient M^p of the dual function $q(\lambda)$ at the λ^p iteration. This iterative approach helps us systematically explore feasible solutions along the subgradient direction, ultimately providing an effective solution to the non-differentiable dual problem.

With the aid of the Karush-Kuhn-Tucker (KKT) conditions, we ascertain the optimal trajectory by taking partial derivatives of equation (12) with respect to x_t, y_t, and z_t. These derivatives establish crucial conditions that guide us in finding the best values for the UAV's trajectory, as shown below:

$$I(x_t - D - E) + Jx_t + K(x_t - x_{t-1}) = 0 \tag{16}$$

$$Iy_t + Jy_t + K(y_t - y_{t-1}) = 0 \tag{17}$$

$$Iz_t + J(z_t - H) + K(z_t - z_{t-1}) = 0 \tag{18}$$

Where

$$I = \frac{\alpha}{P_s^t}\left((x_t - D)^2 + y_t^2 + z_t^2\right)^{\frac{\alpha}{2}-1}$$

$$J = \frac{\alpha}{P_u^t}\left(x_t^2 + y_t^2 + (z_t - H)^2\right)^{\frac{\alpha}{2}-1}$$

$$K = \lambda^p\left((x_t - x_{t-1})^2 + (y_t - y_{t-1})^2 + (z_t - z_{t-1})^2\right)^{-0.5}$$

We calculate the optimum trajectory from (16) to (18). For updating λ^p we may use this formula for every iteration

$$\lambda^{p+1} = [\lambda^p + \alpha^p M^p]^+ \tag{19}$$

where, $[z]^+$=max$(z, 0)$, step size $\alpha^p = \frac{c}{d+p}$, where $c > 0$ and $d \geq 0$. The Lagrange multiplier λ increases when the flying distance constraint $d_{t,t-1}$ exceeds the allowed distance v and decreases when not violated. This helps enforce the constraint. The iteration stops when $|q(\lambda^{p+1}) - q(\lambda^p), | < \mu_1$, where μ_1 is the error tolerance.

Following [2], Algorithm 1 for solving the trajectory design subproblem is shown below.

Algorithm 1: Algorithm for trajectory optimization (TO)

Input: Signal's transmit power **P**
Output: The trajectory **L**
Begin
  For $t = 2 : N$;
  do
    Initialize $p = 0, \lambda^0 = 1$
    repeat
      Find the optimal trajectory for the UAV
      using (16) to (18): (x_t^p, y_t^p, z_t^p);
      Update λ according to (19);
      $p = p + 1$;
    until $|q(\lambda^p) - q(\lambda^{p-1})| < \mu 1$;
  end
end

4.2. Power Allocation

Till now we optimize the trajectory of the UAV with the transmit power. Now for a given trajectory, we optimize the power allocation. For this problem (9) can be divided into N subproblems. The subproblems can be solved simultaneously since the transmit power for each time slot is the only factor affecting the outage probability while the other constraints are independent. The subproblem for time slot t is formulated as follows:

$$\begin{aligned} &\min_{P_s^t, P_u^t} \sum_{t\in\mathcal{N}} P_{out}^t \\ &s.t. \quad P_s^t + P_u^t \leq P_{max}, \quad \forall t \in \mathcal{N}, \\ &P_s^t > 0, \quad P_u^t > 0 \quad \forall t \in \mathcal{N} \end{aligned} \tag{20}$$

Theorem 1. When the minimum outage probability is attained, the transmit power of both the MD and UAV will satisfy the constraint $P_s^t + P_u^t = P_{max}$. [2]

By substituting $P_u^t = P_{max} - P_s^t$ into (20), the optimization problem is transformed into a new problem with a single variable, P_s^t, i.e.,

$$\begin{aligned} &\min_{P_s^t} \quad P_{out}^t \\ &\text{subject to} \quad 0 \leq P_s^t \leq P_{\max}, \quad \forall t \in \mathcal{N} \end{aligned} \tag{21}$$

where,

$$P_{out}^t(main) = 1 - \exp\left(\frac{N_0\xi_{th}}{2}\right) \times \left(\frac{\left[(x_t - D - E)^2 + y_t^2 + z_t^2\right]^{\frac{\alpha}{2}}}{P_s^t} + \frac{\left[x_t^2 + y_t^2 + (z_t - H)^2\right]^{\frac{\alpha}{2}}}{P_{max} - P_s^t}\right) \tag{22}$$

4.3. JTO-PA Algorithm

We introduce the joint trajectory optimization and power allocation (JTO-PA) algorithm, which effectively addresses the problem (9) through an iterative approach. Initially, it optimizes the power allocation matrix **P** by solving the power allocation subproblem (20) using results from trajectory optimization in matrix **L**. Subsequently, it focuses on optimizing the trajectory matrix **L** by solving the trajectory optimization subproblem (10), using outcomes from the power allocation matrix **P**. This iterative process continues until convergence, providing an optimal solution for the problem (9).

By iteratively refining both power allocation and trajectory, JTO-PA aims to balance and enhance overall system performance. We use $sum^i = \sum_{t\in\mathcal{N}} (P_{out}^t)^i$ to represent the total outage probability in the i_{th} iteration. It's defined as the sum of individual outage probabilities P_{out}^t for all time instances t in the set N. Convergence of the JTO-PA algorithm is achieved when $\left|\frac{Sum^i - Sum^{i-1}}{Sum^{i-1}}\right| < \mu_2$, where μ_2 is a predefined error tolerance.

Theorem 2. The JTO-PA algorithm is ensured to reach convergence[34].

Algorithm 2: JTO-PA algorithm

Begin

Initialize $i = 0, P_u^t = P_s^t = P_{max}/2, \forall t \in \mathcal{N}$

For the provided power allocation, solve the trajectory optimization subproblem (16)-(18)

repeat

$i = i + 1$

For the given trajectory, solve the power allocation subproblem (20);

For the provided power allocation, solve the trajectory optimization subproblem (16)-(18);

until $\left|\frac{Sum^i - Sum^{i-1}}{Sum^{i-1}}\right| < \mu_2$.

end

It is worth noting that a significant number of drones rely on batteries as their primary power source. To ensure a continuous and reliable power supply for UAVs, a viable approach is to integrate a small solar power system with the UAV. This solar power system incorporates the Maximum Power Point Tracking (MPPT) technique that continuously tracks the maximum power output while maintaining a constant voltage. The employment of a solar cell on the UAV can be helpful to optimize the trajectory at the same time dissipating minimum power. The project is, however, out of the scope of this article.

5. Numerical Results

In this section, we evaluate the JTO-PA algorithm's performance through simulations adhering to 3GPP specifications. The setup comprises a base station (BS) at a 30m height and a UAV capable of moving up to 0.5m per time slot. We set the maximum total transmit power, $P_{\max}$, to 26 dBm and vary the noise variance, N_0, from -84 dBm to -100 dBm. In some simulations, we vary the transmit power from 0.2 to 1.6W. The SNR threshold, ξ_{th}, ranges from 0 dB to 4.77 dB, and the path loss exponent, α, varies from 2 to 4.

Simulations run for 400 time slots ($N = 400$). For the JTO-PA algorithm, we use error tolerances of $\mu_2 = 10^{-3}$ for the outer iteration and $\mu_1 = 10^{-3}$ for the subgradient method. The subgradient method's step size, α^p, is determined as $\alpha^p = \frac{c}{d+p}$, with c and d set to 1 and 2, respectively. Our analysis considers 400 time slots and a distance D of 500m between the BS and MD. Initially, the BS-UAV and UAV-MD are positioned at distances d_{SR}^1 and d_{RD}^1, both of which are $\frac{3}{5}$ times the value of D.

Figure 2 depicts the relationship between secrecy capacity and the average signal-to-noise ratio (SNR) under varying path loss conditions.

This study investigates the impact of path loss on secure wireless data transmission. We analyze the effect of path loss on data transmission and calculate secrecy capacity at different SNR levels.

Our findings show that at high path loss ($\alpha = 4$), secrecy capacity consistently remains lower, particularly between 10 dB and 40 dB SNR. This suggests that maintaining secure data transmission becomes challenging due to significant signal attenuation because of high path loss. Conversely, lower path loss values (2 and 3) result in increased secrecy capacity, even at lower SNR levels, enabling more effective and secure data transmission under less favourable conditions.

Figure 3, shows a plot of outage probability against time slots while considering variable noise power, with specific parameters set as follows: N = 400, D = 500 m, and Pmax = 26 dBm. In this JTO-PA analysis, the plot reveals that the outage probability initially decreases sharply with time, eventually, the curve becomes flatter around 200^{th} time slots.

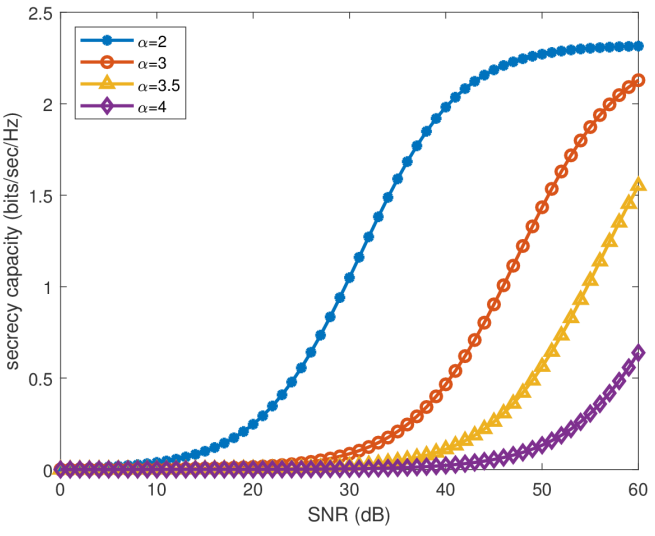

Figure 2. *Secrecy capacity vs average SNR of the channel for the selected values of path-loss coefficient (α).*

The increase in time slots also indicates the linear movement of the UAV up to 0.5m per time slot. This decreasing trend suggests an improving channel stability or reduced interference, indicating enhanced communication reliability. We consider three noise power values: -84 dB, -90 dB, and -96 dB. Notably, the scenario with -96 dB noise power exhibits the lowest outage probability throughout the communication.

Of course, a proper antenna beamforming can minimize the noise power. This observation underscores the significance of antenna beamforming and noise power in shaping the reliability of channel communication. For a UAV relay, the beamforming greatly depends on trajectory optimization. An optimized trajectory sets the line of sight communication between the relay and the destination properly.

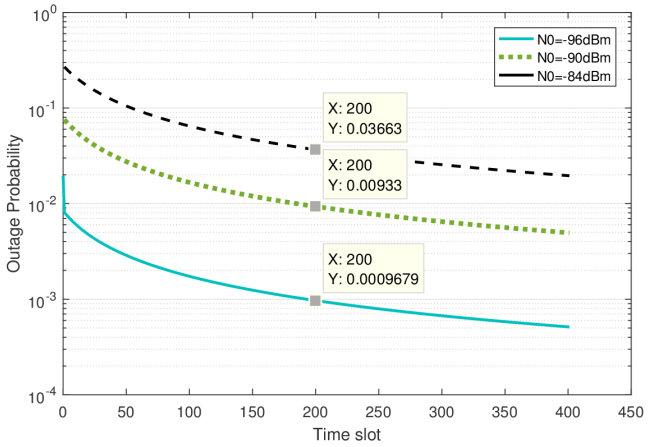

Figure 3. *Outage probability as a function of Time slot of the channel for the selected values of noise variance (N_0).*

In Figure 4, we present the comprehensive outage probability vs. distance relationship for the communication link between BS and MD, with different values of maximum transmit power.

As distance (D) increases, the path loss becomes more pronounced, causing a decrease in received power. Consequently, the outage probability exhibits a consistent upward trend with increasing distance. Our analysis explores the impact of different transmit power levels, including 0.1W, 0.8W and 1.4W. From the figure, it is seen that higher transmit power levels are associated with lower outage probability variation over the distance. As shown in the figure, when the distance between BS and MD increases from 250m to 325m, with the transmit power of 1.4W, the network observes a rise in the outage for only 0.00527. The outage probability still lies in the range of 10^{-2}.

Figure 5 shows the relationship between outage probability and maximum transmit power under various path loss scenarios (path loss exponents $\alpha = 3, 3.5$ and 4.). An outage indicates the scenario when the received power falls below the threshold at the destination, i.e., MD receiver. Because of the presence of the eavesdropper, this outage relates to the security outage when the confidentiality of the information is compromised.

Increasing transmit power improves system reliability, leading to lower outage probabilities. Initially, higher path loss exponents result in higher outage probabilities, but these decrease as transmit power increases. This underscores the importance of adjusting transmit power based on path loss conditions for dependable wireless communication. From the results, we can choose an optimum total transmit power of 0.8 W since the outage probabilities in each case of path-loss seem reasonably under control (approximately at the range of 10^{-3}).

From figures 4 and 5, a transmit power level of 0.8 W to 2 W can be chosen under the budget constraint. The rest of the power allocated to the UAV can be used to maintain its trajectory over a longer duration. Most of the battery power is used to maneuver the UAV and maintain power to circuits. If the power needed for the data transmission can be lowered then the relay can operate with less power allocation.

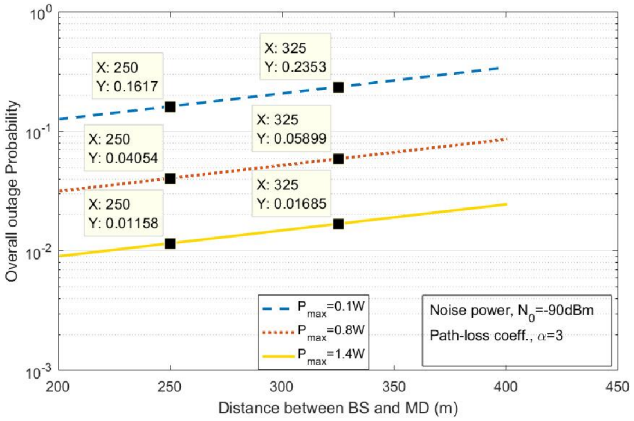

Figure 4. *Outage probability vs Distance with various transmit power (P_{max}).*

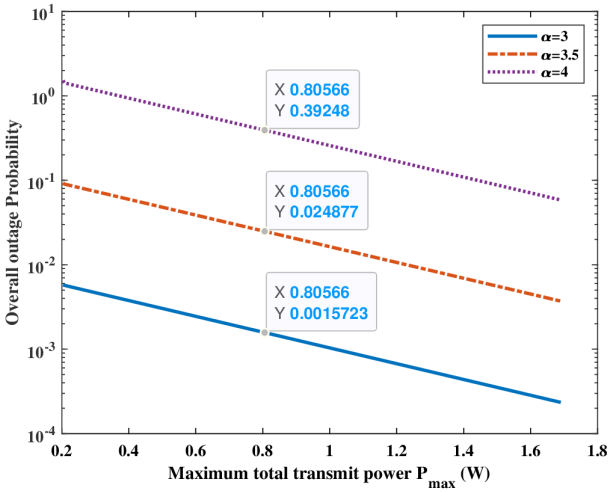

Figure 5. *Overall outage probability as a function of P_{max} for the selected values of path loss coefficient (α).*

6. Conclusions

This paper examines a SISO network with a small multirotor UAV relay employing the DF protocol where a legitimate receiver and eavesdropper are present. Our target is to find

an optimum power budget with a reasonable trajectory to maintain secure communication. We apply the physical layer security approach to investigate the security of the network. Then we apply algorithms to maintain a joint trajectory and power optimization process. Firstly we calculate the equation of secrecy capacity for the legitimate channel receiver in the presence of the eavesdropper. Secondly, we optimize the transmit power and trajectory of the UAV by using the JTO-PA algorithm. We vary different parameters like path loss coefficient, total transmit power, noise power etc. to find the best optimization for the UAV relay network. The mathematical expressions for secrecy capacity and outage probability are derived and numerical results present us with increasing non-zero positive secrecy capacity and decaying outage probability with respect to SNR or transmit power. The outage increases due to path loss and the distance between BS and MD, but the numerical results show that a power budget can be maintained for the constant maneuver of the UAV while enhancing network secrecy.

Further studies can be performed on end-to-end latency, and the source of power consumption for the UAV. The use of solar cells can be an alternative to maintain the power budget for the UAV. Other future works may include the use of UAV swarms as a collaborative body to enhance beamforming and the study on the duration of transmission phases by the base stations as an attempt to improve communication. Also, the characteristics of frameworks using machine learning make it suitable for drone applications. Therefore, several machine-learning approaches can be employed for the detection of drones and attackers, the detection of faults, the recovery of UAV data, collision avoidance and so on.

Abbreviations

BS	Base Station
DF	Decode-and-Forward
JTO-PA	Joint Trajectory Optimization and Power Allocation
MD	Mobile Device
TO	Trajectory Optimization
SISO	Single-Input-Single-Output
SNR	Signal-to-Noise ratio
UAV	Unmanned Aerial Vehicle

ORCID

https://orcid.org/0000-0001-5286-5450 (Jishan E Giti)
https://orcid.org/0000-0003-2597-156X
(Shah Ariful Hoque Chowdhury)
https://orcid.org/0000-0001-5286-5450 (Al-Hadith Moon)

Author Contributions

Jishan E Giti: Conceptualization, Data curation, Supervision, Funding acquisition, Investigation, Writing - original draft, Methodology

Shah Ariful Hoque Chowdhury: Conceptualization, Funding acquisition, Methodology, Writing - review & editing

Al-Hadith Moon: Investigation, Methodology

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] B. Li, Z. Fei and Y. Zhang. (2018). UAV Communications for 5G and Beyond: Recent Advances and Future Trends. IEEE Internet of Things Journal, pp. 1. https://doi.org/10.1109/JIOT.2018.2887086

[2] S. Zeng, H. Zhang, K. Bian and L. Song. (2018). UAV relaying: Power allocation and trajectory optimization using decode-and-forward protocol. 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-6. https://doi.org/10.1109/ICCW.2018.8403625

[3] S. Zeng, H. Zhang, Q. He, K. Bian and L. Song. (2017). Joint trajectory and power optimization for UAV relay networks. IEEE Communications Letters, vol. 22, no. 1, pp. 161-164. https://doi.org/10.1109/LCOMM.2017.2763135

[4] Y. Zeng, R. Zhang and T. J. Lim. (2016). Throughput maximization for UAV-enabled mobile relaying systems. IEEE Transactions on Communications, vol. 64, no. 12, pp. 4983-4996. https://doi.org/10.1109/TCOMM.2016.2611512

[5] C. Shannon. (1949). Communication theory of secrecy systems. Bell System Technical Journal, vol. 29, pp. 656-715.

[6] J. Barros and M. Rodrigues. (2006). "Secrecy capacity of wireless channels", in Proc. IEEE Intl. Symposium on Information Theory, July, pp. 356-360. https://doi.org/10.1109/ISIT.2006.261613

[7] Z. Yuan, C. Chen, L. Bai, Y. Jin, and J. Choi. (2016). Secure relay beamforming with correlated channel models in dual-hop wireless communication networks. In Proc. of IEEE Global Commun. Conf. (GLOBECOM), December 4-8, pp. 1-6. https://doi.org/10.1109/GLOCOM.2016.7842252

[8] Y. Jing and H. Jafarkhani (2008). Beamforming in wireless relay networks. In Proc. IEEE Inf. Theory and Applications Workshop, January 27-February 1, pp. 1-9. https://doi.org/10.1109/ITA.2008.4601040

[9] C. Masouros and T. Ratnarajah. (2012). Interference as a source of green signal power in cognitive relay-assisted co-existing MIMO wireless transmissions. IEEE Trans. on Commun., vol. 60, no. 2, pp. 525-536. https://doi.org/10.1109/TCOMM.2011.112811.100734

[10] J. E. Giti, M. Z. I. Sarkar, S. A. H. Chowdhury, M. M. Ali, and T. Ratnarajah. (2014). Secure wireless multicasting through co-existing MIMO radio systems. In Proc. of The 9^{th} International Forum on Strategic Technology (IFOST), October 21-23, pp. 195-198. https://doi.org/10.1109/IFOST.2014.6991103

[11] W. Liu, M. Z. I. Sarkar, T. Ratnarajah, and H. Du. (2016). Securing cognitive radio with a combined approach of beamforming and cooperative jamming. IET Commun., vol. 11, no. 1, pp. 1-9, December 22.

[12] Q. F. Zhou, F. C. M. Lau, and S. F. Hau. (2009). Asymptotic analysis of opportunistic relaying protocols. IEEE Trans. on Wireless Commun., vol. 8, no. 8, pp. 3915-3920. https://doi.org/10.1109/TWC.2009.080783

[13] K. Elkhalil, M. E. Eltayeb, H. Shibli, H. R. Bahrami, and T. Y. Al-Naffouri. (2014). Opportunistic relay selection in multicast relay networks using compressive sensing. In Proc. of IEEE Global Commun. Conf. (GLOBECOM), December 8-12.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. (2009). Cooperative jamming for wireless physical layer security. In Proceedings of IEEE/SP 15^{th} Workshop on Statistical Signal Processing, 2009 (SSP'09), Cardiff, Wales, UK, 31 Aug.-03 Sept., pp. 417-420. https://doi.org/10.1109/SSP.2009.5278549

[15] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin (2013), Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI. IEEE Signal Processing Letters, vol. 20, no. 1, pp. 39-42. https://doi.org/10.1109/LSP.2012.2227725

[16] X. Guan, Y. Cai, Y. Wang, and W. Yang. (2011). Increasing secrecy capacity via joint design of cooperative beamforming and jamming. In Proc. of the 22^{nd} Annual IEEE International Sym. on Personal, Indoor and Mobile Radio Commun. (PIMRC): Fundamentals and PHY, September 11-14. https://doi.org/10.1109/PIMRC.2011.6139705

[17] E. R. Alotaibi and K. A. Hamdi. (2015). Optimal cooperative relaying and jamming for secure communication. IEEE Wireless Commun. Letts., vol. 4, no. 6, pp. 689-692.

[18] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, and R. Gaire. (2020). Friendly jammer against an adaptive eavesdropper in a relay-aided network. In Proc. 2020 International Wireless Communications and Mobile Computing (IWCMC), June 15-19, pp. 1707-1712.

[19] J. E. Giti, S. A. H. Chowdhury, and M. M. Ali. (2015). Enhancing security in wireless multicasting with selective precoding. International Journal of Systems, Control and Commun., vol. 6, no. 3.

[20] A. Kuhestani, A. Mohammadi, and M. Mohammadi. (2018). Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers. IEEE Trans. on. Inf. Forensic. Sec., vol. 13, no. 2, pp. 341-355. https://doi.org/10.1109/TIFS.2017.2750102

[21] W. Liu, M. Sarkar, and T. Ratnarajah. (2014). On the security of cognitive radio networks: Cooperative jamming with relay selection. In Proc. of European Conf. on Netw. and Commun. (EuCNC), June 23-26. https://doi.org/10.1109/EuCNC.2014.6882674

[22] J. E. Giti, B. Srinivasan, and J. Kamruzzaman. (2017). Impact of friendly jammers on secrecy multicast capacity in presence of adaptive eavesdroppers. In Proc. IEEE GLOBECOM Workshops (GC Wkshps), December 4-8, pp. 1-6. https://doi.org/10.1109/GLOCOMW.2017.8269226

[23] A. Ayyagari, J. Harrang, and S. Ray. (1996). Airborne information and reconnaissance network. In Proc. of IEEE Military Commun. Conf. (MILCOM), December 1-3, pp. 230-234 https://doi.org/10.1109/MILCOM.1996.568619

[24] D. H. Choi, S. H. Kim, and D. K. Sung. (2014). Energy-efficient maneuvering and communication of a single UAV-based relay. IEEE Transactions on Aerospace and Electronic Systems, vol. 50, no. 3, pp. 2320-2327. https://doi.org/10.1109/TAES.2013.130074

[25] A. Merwaday and I. Guvenc. (2015). UAV assisted heterogeneous networks for public safety communications. In proceedings of 2015 IEEE wireless communications and networking conference workshops (WCNCW), pp. 329-334. https://doi.org/10.1109/WCNCW.2015.7122576

[26] F. Cheng, S. Zhang, Z. Li, Y. Chen, N. Zhao, F. R. Yu, and V. C. M. Leung. (2018). UAV trajectory optimization for data offloading at the edge of multiple cells. IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6732-6736. https://doi.org/10.1109/TVT.2018.2811942

[27] Y. Liang, L. Xiao, D. Yang and K. Lu. (2020). Joint trajectory and resource allocation optimization for two-way UAV-aided relaying network. In Proceedings of 2020 International Conference on Wireless Communications and Signal Processing (WCSP), pp. 376-381. https://doi.org/10.1109/WCSP49889.2020.9299837

[28] T. M. Hoang, N. M. Nguyen, and T. Q. Duong. (2020). Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and K-means clustering. IEEE Wireless Commun. Letts., vol. 9, no. 2, pp.139-142. https://doi.org/10.1109/LWC.2019.2945022

[29] G. Sun, J. Li, A. Wang, Q. Wu, Z. Sun, and Y. Liu. (2022). Secure and energy-efficient UAV relay communications exploiting collaborative beamforming. IEEE Trans. on Commun., vol. 70, no. 8, pp. 5401-5416. https://doi.org/10.1109/TCOMM.2022.3184160

[30] X. Shi, A. Wang, G. Sun, J. Li, and X. Zheng. (2022). Air to air communications based on UAV-enabled virtual antenna arrays: A multi-objective optimization approach. in 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 878-883. https://doi.org/10.1109/WCNC51071.2022.9771817

[31] S. Elouarouar and H. Medromi. (2022). Multi-rotors unmanned aerial vehicles power supply and energy management. E3S Web Conf., vol. 336, p. 00068. https://doi.org/10.1051/e3sconf/202233600068

[32] L. Cwojdziński and M. Adamski. (2014). Power units and power supply systems in UAV. Aviation, vol. 18, no. 1, pp. 1-8. https://doi.org/10.3846/16487788.2014.865938

[33] S. P. Boyd and L. Vandenberghe. (2004). Convex optimization. Cambridge University Press.

[34] D. P. Bertsekas. (1997). Nonlinear programming. Journal of the Operational Research Society, Taylor & Francis, vol. 48, no. 3, pp. 334-334.