Energy-Constrained UAV-Assisted Secure Communications with Position Optimization and Cooperative Jamming

Wei Wang, *Member, IEEE*, Xinrui Li, Miao Zhang, Kanapathippillai Cumanan, *Senior Member, IEEE*, Derrick Wing Kwan Ng, *Senior Member, IEEE*, Guoan Zhang, Jie Tang, *Senior Member, IEEE*, and Octavia A. Dobre, *Fellow, IEEE*

***Abstract*—In this paper, we consider an energy-constrained unmanned aerial vehicle (UAV)-enabled mobile relay assisted secure communication system in the presence of a legitimate source-destination pair and multiple eavesdroppers with imperfect locations. The energy-constrained UAV employs the power splitting (PS) scheme to simultaneously receive information and harvest energy from the source, and then exploits the time switching (TS) protocol to perform information relaying. Furthermore, we consider a full-duplex destination node which can simultaneously receive confidential signals from the UAV and cooperatively transmit artificial noise (AN) signals to confuse malicious eavesdroppers. To further enhance the reliability and security of this system, we formulate a worst case secrecy rate maximization problem, which jointly optimizes the position of the UAV, the AN transmit power, as well as the PS and TS ratios. The formulated problem is non-convex and generally intractable. In order to circumvent the non-convexity, we decouple the original optimization problem into three subproblems; this facilitates the design of a suboptimal iterative algorithm. In each iteration, we propose a multi-dimensional search and numerical method to handle the subproblem. Numerical simulation results are provided to demonstrate the effectiveness and superior performance of the proposed joint design versus the conventional schemes in the literature.**

***Index Terms*—Unmanned aerial vehicles (UAV) communications, physical layer security, simultaneous wireless information and power transfer (SWIPT), robust design, artificial noise (AN).**

W. Wang is with the School of Information Science and Technology, Nantong University, Nantong, China, and with Research Center of Networks and Communications, Peng Cheng Laboratory, Shenzhen, China, and also with the Nantong Research Institute for Advanced Communication Technologies, Nantong, China (e-mail: wwang2011@ntu.edu.cn).

X. Li and G. Zhang are with the School of Information Science and Technology, Nantong University, Nantong, China (e-mail:1811310045@yjs.ntu.edu.cn, gzhang@ntu.edu.cn).

M. Zhang and K. Cumanan are with the Department of Electronic Engineering, University of York, York, YO10 5DD, United Kingdom (e-mail:msczz@foxmail.com, kanapathippillai.cumanan@york.ac.uk).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, University of New South Wales, Kensington, NSW 2033, Australia (e-mail:w.k.ng@unsw.edu.au).

J. Tang is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China (e-mail: eejtang@scut.edu.cn).

O. A. Dobre is with the Faculty of Engineering and Applied Science, Memorial University, St. Johns, NL A1B 3X9, Canada (e-mail:odobre@mun.ca)

The work of W. Wang, X. Li, and G. Zhang were supported in part by the Natural Science Foundation of China under Grant 61971245, in part by the Six Categories Talent Peak of Jiangsu Province under Grant KTHY-039, in part by the Verification Platform of Multi-tier Coverage Communication Network for oceans under Grant LZC0020, and in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX19-2057. The work of K. Cumanan was supported by H2020-MSCA-RISE-2015 under Grant 690750. The work of D. W. K. Ng was supported in part by the funding from the UNSW Digital Grid Futures Institute, UNSW, Sydney, under a cross-disciplinary fund scheme and in part by the Australian Research Council's Discovery Project under Grant DP190101363. The work of J. Tang was supported by the Natural Science Foundation of China under Grant 61971194. The work of O. A. Dobre was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), through its Discovery program. *(Corresponding author: Wei Wang)*

I. Introduction

THE high mobility and flexibility of unmanned aerial vehicles (UAVs) make their deployment possible in the fifth-generation (5G) and beyond wireless networks [1]–[4]. However, in contrast to the conventional wireless communication systems, UAV-ground communications are more vulnerable to eavesdropping as they can be easily intercepted by potential eavesdroppers due to the inherent broadcast nature of the line-of-sight (LoS) dominated wireless channels. Therefore, UAV-ground communications bring up different security challenges [5]–[7], which need to be addressed to unlock the potential of UAV-based communications.

Recently, physical layer security has emerged as a promising technology to realize secrecy in wireless communications [8]–[14], while complementing the conventional encryption techniques in UAV networks. In the literature, different physical layer security-based designs have been proposed to improve the performance of UAV-assisted communication systems. For instance, a joint transceiver design for UAV-ground secure communications was proposed in [15], where the secrecy rate was maximized by jointly optimizing the UAV's trajectory and its transmit power. Later on, physical layer security was extended to both the downlink and uplink of an UAV-ground communication system in [16], where the average secrecy rate was maximized by jointly optimizing the UAV's trajectory and the transmit power of the legitimate transmitter over a given flight duration of the UAV. In [17], the authors considered a utility optimization problem to maximize the secrecy rate in UAV-enabled mobile relaying secure communications by jointly designing the transmit power of a source and a relay node. Moreover, a caching UAV-assisted secure transmission scheme was investigated in hyper-dense small-cell networks to enhance coverage and to increase the system secrecy rate in [18]. A secrecy rate maximization problem for an UAV-enabled mobile jamming system was studied in [19], which a joint design of trajectory and power control scheme was proposed. Furthermore, a secure transmission scheme for UAV wiretap channels was considered

in the presence of a full-duplex (FD) eavesdropper in [20]. However, the aforementioned works, e.g., [15]–[20], assumed that perfect knowledge of the eavesdroppers' locations is available at the transmitter for resource allocation and trajectory design, which is difficult to realize in practical scenarios. In particular, eavesdroppers may remain silent to hide their existence and obtaining their perfect location information is unrealistic. More importantly, applying the designs based on perfect location information of eavesdroppers may result in significant degradation of security performance. In addition, the works in [15]–[20] only considered the case of a single eavesdropper, which is typically an unrealistic assumption in many practical and emerging scenarios. Therefore, designing the position of an UAV taking into account the existence of multiple eavesdroppers for enhancing the secrecy performance is an utmost important set of challenges. To address these issues, a secure UAV communication system in the presence of multiple eavesdroppers with imperfect locations was considered in [21], where a joint robust trajectory design and power control scheme was proposed to maximize the average worst-case secrecy rate. However, it is noted that the sizes and weights of UAVs are usually small for enabling both high flexibility and safety [15]–[21], which results in UAVs having limited onboard energy storage with short cruising duration.

To overcome this difficulty, energy-constrained UAV-aided communications have drawn a significant increasing research interests recently. For instance, a joint design of UAV's trajectory, propulsion energy consumption, and communication throughput was proposed to maximize the energy efficiency with a simple fixed circular trajectory in [22]. In [23], the authors investigated a fundamental energy tradeoff problem in UAV-enabled data collection system with two practical fixed UAV trajectories, namely circular flight and straight flight. Furthermore, a joint sensor nodes' schedule and UAV trajectory design was studied in [24] to minimize the maximum energy consumption within all sensor nodes. However, reducing the energy consumption of UAV by adjusting either its location or power allocation does not fundamentally solve the energy shortage problem of UAV for prolonging system lifetime. Instead of reducing energy consumption, energy harvesting (EH) from surrounding environments has been considered as an emerging solution to effectively extend the operational time of energy-constrained UAVs [25]–[27]. Recently, the simultaneous wireless information and power transfer (SWIPT) technique has received considerable attention for energy-constrained UAV communications as the radio frequency (RF) signals can be exploited to carry both information and energy. For instance, in [28], the authors studied the throughput maximization problem for a typical end-to-end cooperative communication system, where an UAV was assumed to be an aerial mobile relay and its transmission was powered by the harvested energy in the RF signal from the source. Besides, an orthogonal frequency division multiplexing (OFDM) relaying-based SWIPT UAV communication system was proposed in [29], where the energy-constrained UAV exploits the power splitting (PS) scheme to simultaneously perform EH and information decoding (ID). Furthermore, in [30], a joint UAV location deployment, PS, and time switching (TS) ratio design was investigated to maximize the network throughput in an energy-constraint UAV amplify-and-forward relaying system. Despite the research efforts devoted to SWIPT in UAV-ground communications, the security issue of SWIPT-aided UAV wireless communication has drawn little attention so far. In fact, although the applications of SWIPT have brought various advantages to communication systems, it is also known that SWIPT-powered systems are more vulnerable than conventional systems in terms of security [31], [32]. More importantly, existing designs, e.g., [28]–[30], may not be applicable to the case when communication security is utmost important in SWIPT-aided UAV systems. It is worth noting that there have been some initial attempts (e.g., [33]) that address the security issues of SWIPT-powered UAV-ground communication systems. In [33], the authors investigated an UAV-assisted SWIPT system in the presence of multiple eavesdroppers, where the secrecy rate was maximized by jointly optimizing the trajectory and transmit power of the UAV. Nevertheless, the authors in [33] assumed that the locations of eavesdroppers were perfect, and results are not applicable to practical cases with imperfect location information.

Motivated by the aforementioned aspects, in this paper we consider an UAV-ground secure communication system, where a source transmits information to a legitimate destination via an energy-constrained UAV-enabled mobile relay in the presence of multiple eavesdroppers.[1] In particular, it is assumed that the imperfect locations of all potential eavesdroppers are available. As such, the energy-constrained UAV receives information and harvests energy from the source, and then forwards the secret messages to the destination. Furthermore, in order to combat multiple eavesdroppers with imperfect locations information, we employ a destination node which operates in FD mode, i.e., it can simultaneously receive confidential signals (CS) from the UAV and transmit artificial noise (AN) to confuse the eavesdroppers. We then define and evaluate the worst-case secrecy rate, which shows the performance of both communication reliability of the legitimate link (between the UAV and destination) and the communication confidentiality to the multiple eavesdroppers. We aim to maximize the minimum secrecy rate under the constraints of the position, EH at the UAV, the maximum transmit power, and AN power level at the destination node. To the best of our knowledge, the robust design for SWIPT-assisted UAV secure communications has not been reported in the literature, and our contributions are summarized as follows:

1) The proposed robust joint design enhances both security performance and battery lifetime of the considered UAV

[1]This system setting has a number of potential applications in wireless networks, e.g., in cellular systems, when a legitimate source-destination pair cannot communicate directly, and then, an aerial relay should be employed to establish this communication without the support of a fixed site and power supply.

TABLE I
LIST OF FUNDAMENTAL VARIABLES.

Symbol	Description
α	Time switching ratio
ρ	Power splitting ratio
T	Flight period of UAV
h_{ab}	Channel coefficient between a and b
f_d	Self-interference channel coefficient
β_0	Channel power gain at a reference distance
ζ	Exponentially distributed random variable
d_{ab}	Distance between a and b
η	Energy conversion efficiency
β	Amplification factor
ε	Effectiveness of SIC
$\sigma^2_{\{r,d,e\}}$	Variance of AWGN
σ^2_{ID}	Noise variance of ID
$\sigma^2_{Z_d}$	Noise variance of AN
P_s	Transmit power of S
P_r	Transmit power of UAV
P_{cr}	Circuit power consumption of UAV
$P_{r,\max}$	Maximum transmit power of UAV
$P_{AN,\max}$	Maximum transmit power of AN
$r_{\max}$	Maximum flight radius of UAV

system, which is more suitable for practical scenarios when compared to the existing works on UAV secure communications [21], [33], [34].

2) To circumvent the non-convexity issue of the formulated design problem, we first decompose the considered problem into three subproblems. Then, we propose the multi-dimensional search and numerical methods to handle the subproblems.

3) By iteratively solving the three subproblems, a suboptimal solution of the original problem is realized. In each iteration, we derive closed-form expressions for the position of the UAV, the AN transmit power vector of the destination, the PS and TS ratio, which provide important insights related to the system design.

4) Extensive simulation results are provided to demonstrate the impacts of different parameters and the superior performance of the proposed joint robust design against other four benchmark schemes in the literature.

The remainder of the paper is organized as follows. The system model and the formulation of the minimum secrecy rate maximization problem are presented in Section II, while a three-step alternating algorithm is developed in Section III to obtain a suboptimal solution of the optimization problem at hand. Section IV provides simulation results to validate the effectiveness of our proposed design, and finally, Section V concludes the paper.

Notations: $\mathbb{E}(\cdot)$ represents the statistical expectation and $|\cdot|$ denotes the absolute value of a complex number. The distribution of a circular symmetric complex Gaussian vector with mean vector $\mathbf{x}$ and covariance matrix $\mathbf{\Sigma}$ is denoted by $\mathcal{CN}(\mathbf{x}, \mathbf{\Sigma})$. The notation $(m)^+$ stands for $\max(0, m)$. A list of the fundamental variables is provided in Table I.

II. SYSTEM MODEL AND PROBLEM FORMULATION

In this paper, we consider a legitimate UAV-ground secure communication system as shown in Fig. 1, where a source S intends to transmit confidential information to a destination D through an UAV-assisted mobile relay R in the presence of multiple independent eavesdroppers $\{E_1, E_2, \cdots, E_n\}$. It is assumed that the source, the UAV and the eavesdroppers are single-antenna devices, while the FD destination is equipped with a dual antenna, one for signal transmission and the other for signal reception. Specifically, the UAV is powered by an energy-limited onboard battery which needs to harvest energy from the power-supply source. Since the propulsion energy consumption of the UAV is much larger than that of the wireless transmission in practical scenarios, we assume that the onboard battery supplies for the flight control of UAVs while the harvested energy accounts only for its information transmission and circuit power consumption, as commonly adopted in the literature [28]–[30]. The SWIPT-based EH and ID protocol is presented in Fig. 2. In the first phase αT, with $\alpha \in [0, 1]$ representing the TS ratio, the source transmits information and energy simultaneously to the UAV. In the second phase $(1-\alpha)T$, the received signal at the relay UAV is amplified and then forwarded to the destination and eavesdroppers.[2] In this phase, the FD destination also acts as a jammer to cooperatively transmit AN to reduce the received signal-to-interference plus-noise ratio (SINR) at the eavesdroppers. Without loss of generality, a three-dimensional Cartesian coordinate system is considered, where the source and destination nodes are located at $(x_S, 0, 0)$ and $(x_D, 0, 0)$, respectively. $(x_k, y_k, 0)$ denotes the exact location of the k-th eavesdropper, E_k, $k \in \{1, 2, \cdots, n\}$, which is unknown to the legitimate system. However, we assume that

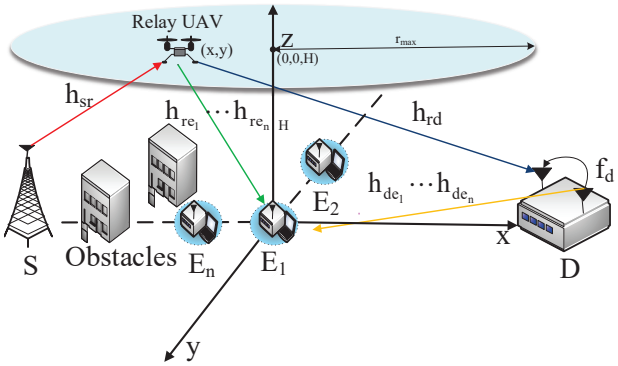


Fig. 1. System model for a SWIPT-based UAV secure relay network.

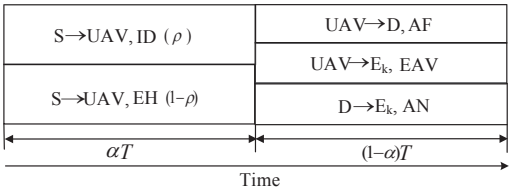


Fig. 2. Joint TS and PS-based SWIPT protocol for UAV-assisted relaying.

[2]In contrast to the decode-and-forward scheme, the amplify-and-forward scheme requires less energy consumption and provides more degrees of freedom to the UAV system design, which is more suitable for energy-constrained UAV-assisted communication scenarios [28].

the UAV and the destination have the capability to estimate the locations of E_k, i.e., $(x_{E_k}, y_{E_k}, 0)$ [21], [33]. Furthermore, it is assumed that the UAV flies at the fixed altitude H [15]–[19], [21], [33], [35], hence, the position of the UAV can be expressed by its Cartesian coordinate (x, y, H). The channels between S and the UAV as well as D are denoted by h_{sr} and h_{rd}, respectively. Besides, h_{re_k} and h_{de_k} denote the channel coefficients between E_k and the UAV as well as D, respectively. We assume that all the above channels are LoS channels.[3] Moreover, f_d denotes random self-interference channel at the destination. In addition, it is also assumed that there is no direct link between the source and destination as well as eavesdroppers, due to heavy shadowing or existence of obstacles.

Under the above setting, the channel gains h_{sr}, h_{rd}, h_{re_k}, and h_{de_k} can be respectively expressed as:

$$\begin{aligned} h_{sr}^2 &= \frac{\beta_0}{d_{sr}^2} = \frac{\beta_0}{(x-x_S)^2+y^2+H^2}, \\ h_{rd}^2 &= \frac{\beta_0}{d_{rd}^2} = \frac{\beta_0}{(x-x_D)^2+y^2+H^2}, \\ h_{re_k}^2 &= \frac{\beta_0}{d_{re_k}^2} = \frac{\beta_0}{(x-x_k)^2+(y-y_k)^2+H^2}, \\ h_{de_k}^2 &= \frac{\beta_0}{d_{de_k}^2} = \frac{\beta_0}{(x_k-x_D)^2+(y_k-y_D)^2}\zeta, \end{aligned} \tag{1}$$

where β_0 denotes the channel power gain at a reference distance of $d = 1\ m$ [15]–[21], [28]–[30], [33], and ζ is an exponentially distributed random variable with unit mean accounting for the Rayleigh fading [16]. The parameters $d_{sr} = \sqrt{(x-x_S)^2+y^2+H^2}$, $d_{rd} = \sqrt{(x-x_D)^2+y^2+H^2}$, $d_{re_k} = \sqrt{(x-x_k)^2+(y-y_k)^2+H^2}$, and $d_{de_k} = \sqrt{(x_k-x_D)^2+(y_k-y_D)^2}$ represent the distances between S-to-UAV, UAV-to-D, UAV-to-E_k and D-to-E_k, respectively.

As the locations of the eavesdroppers are imperfectly known, the relations between the actual and the estimated x, y coordinates of E_k are defined, respectively as

$$x_k = x_{E_k} + \Delta x_k, \tag{2}$$

and

$$y_k = y_{E_k} + \Delta y_k, \tag{3}$$

where Δx_k and Δy_k denote the estimation errors. These errors are assumed to be bounded within a circle, i.e., $(\Delta x_k, \Delta y_k) \in \xi \triangleq \{(\Delta x_k, \Delta y_k) | \Delta x_k^2 + \Delta y_k^2 \le \Delta Q_k^2\}$, where ΔQ_k^2 denotes the magnitude square of the maximum estimation error [21], [31].

In the first phase αT, the received signal at the UAV can be expressed as

$$y_r = h_{sr} x_t + n_r, \tag{4}$$

where x_t denotes the transmit signal from S with transmit power $\mathbb{E}(|x_t|^2) = P_s$ and n_r represents a circularly symmetric complex Gaussian (CSCG) additive white Gaussian noise (AWGN) at the UAV with a distribution $\mathcal{CN}(0, \sigma_r^2)$. Based on the proposed SWIPT protocol in Fig. 2, the received signal at the ID and the EH circuits can be respectively expressed as

$$y_r^{ID} = \sqrt{\rho}(h_{sr} x_t + n_r) + n_{ID}, \tag{5}$$

and

$$y_r^{EH} = \sqrt{1-\rho}(h_{sr} x_t + n_r), \tag{6}$$

where $\rho \in [0, 1]$ represents the PS ratio and n_{ID} is the noise introduced by the ID circuit, which follows a distribution $\mathcal{CN}(0, \sigma_{ID}^2)$. In general, the harvested energy is a nonlinear function with respect to the received RF power [36], [37]. However, there is no a generic EH model which can captures all practical issues [38]. Therefore, for simplicity, we consider a linear EH model which has been commonly adopted in the literature [28]–[30], [33]. Accordingly, the harvested energy at the UAV is defined as

$$E_r^{EH} = \eta \alpha T (1-\rho) P_s |h_{sr}|^2, \tag{7}$$

where $\eta \in (0, 1]$ denotes the energy conversion efficiency.

In the second phase $(1-\alpha)T$, the signal transmitted by the UAV can be written as

$$x_r = \sqrt{\beta} y_r^{ID} = \sqrt{\beta}(\sqrt{\rho} h_{sr} x_t + \sqrt{\rho} n_r + n_{ID}), \tag{8}$$

where β denotes the amplification factor adopted at the UAV [39], [40]. Then, the transmit power of the UAV is $\mathbb{E}(|x_r|^2) = P_r$, which can be defined as

$$P_r = \beta \rho P_s |h_{sr}|^2 + \beta \rho \sigma_r^2 + \beta \sigma_{ID}^2. \tag{9}$$

For the FD destination, after self-interference cancellation (SIC) [41]–[43], its received signal is given by

$$\begin{aligned} y_d &= h_{rd} x_r + n_d \\ &= \underbrace{\sqrt{\beta}\sqrt{\rho} h_{rd} h_{sr} x_t}_{\text{Relayed signal}} + \underbrace{\sqrt{\beta}\sqrt{\rho} h_{rd} n_r}_{\text{Relayed noise}} \\ &\quad + \underbrace{\sqrt{\beta} h_{rd} n_{ID}}_{\text{ID noise}} + \underbrace{f_d \sqrt{\varepsilon} z_d}_{\text{Residual AN}} + \underbrace{n_d}_{\text{AWGN}}, \end{aligned} \tag{10}$$

where $\varepsilon \in [0, 1]$ denotes the effectiveness of the adopted SIC. z_d and n_d represent the AN and AWGN at the destination, which follow the distribution $z_d \sim \mathcal{CN}(0, \sigma_{Z_d}^2)$ and $n_d \sim \mathcal{CN}(0, \sigma_d^2)$, respectively. Thus, the SINR and the achievable data rate at the destination are respectively defined as

$$\begin{aligned} &\text{SINR}_d \\ &= \frac{\beta \rho P_s |h_{rd} h_{sr}|^2}{\beta \rho \sigma_r^2 |h_{rd}|^2 + \beta \sigma_{ID}^2 |h_{rd}|^2 + \varepsilon \sigma_{Z_d}^2 |f_d|^2 + \sigma_d^2}, \end{aligned} \tag{11}$$

and

$$R_d = (1-\alpha)\log_2(1 + \text{SINR}_d). \tag{12}$$

At the same time, the received signal at the k-th eavesdropper can be expressed as

$$\begin{aligned} y_{e_k} =& h_{re_k} x_r + h_{de_k} z_d + n_{e_k} \\ =& \underbrace{\sqrt{\beta}\sqrt{\rho} h_{re_k} h_{sr} x_t}_{\text{Relayed signal}} + \underbrace{\sqrt{\beta}\sqrt{\rho} h_{re_k} n_r}_{\text{Relayed noise}} \\ &+ \underbrace{\sqrt{\beta} h_{re_k} n_{ID}}_{\text{ID noise}} + \underbrace{h_{de_k} z_d}_{\text{AN signal}} + \underbrace{n_{e_k}}_{\text{AWGN}}, \end{aligned} \tag{13}$$

[3]The LoS channel model is a reasonable approximation for UAV-ground communications in practice, which has been already adopted in many works in the literature, e.g., [15]–[21], [28]–[30], [33].

where n_{e_k} represents the AWGN at the k-th eavesdropper node with a distribution $\mathcal{CN}(0, \sigma_e^2)$. Therefore, the SINR and the achievable data rate of E_k are respectively expressed as

$$\mathrm{SINR}_{e_k} = \frac{\beta\rho P_s |h_{re_k} h_{sr}|^2}{\beta\rho\sigma_r^2 |h_{re_k}|^2 + \beta\sigma_{ID}^2 |h_{re_k}|^2 + \sigma_{Zd}^2 |h_{de_k}|^2 + \sigma_e^2}, \tag{14}$$

and

$$R_{e_k} = (1-\alpha)\log_2(1 + \mathrm{SINR}_{e_k}). \tag{15}$$

Here, we consider a max-min secrecy rate optimization problem in a SWIPT-powered UAV relaying system with multiple eavesdroppers, where the secrecy rate between S and D is maximized by jointly optimizing the AN transmit power of the destination, the TS and PS ratios of the SWIPT protocol, as well as the amplification factor and position of the UAV. This problem can be formulated as

$$\begin{aligned} \max_{\sigma_{Zd}^2, \alpha, \rho, \beta, (x,y)} \; & \left[R_d - \max_{k\in\{1,2,\ldots,n\}} \; \max_{\Delta x_k, \Delta y_k \in \xi} \; \{R_{e_k}\} \right]^+ \\ \text{s.t. } & C1: (1-\alpha)T(P_r + P_{cr}) \le E_r^{EH}, \\ & C2: (1-\alpha)T\sigma_{Zd}^2 + E_{SIC} \le E_d, \\ & C3: \sqrt{x^2+y^2} \le r_{max}, \\ & C4: P_r \le P_{r,\max}, \\ & C5: \sigma_{Zd}^2 \le P_{AN,\max}, \\ & C6: 0 \le \rho \le 1, 0 \le \alpha \le 1, 0 < \beta < 1, \end{aligned} \tag{16}$$

where $[m]^+ \triangleq \max(m, 0)$. P_{cr} in constraint C1 denotes the UAV's circuit power consumption [44] such that UAV transmission and circuit power consumption should be less than the total harvested energy. E_{SIC} and E_d represent the energy consumptions of SIC and the energy budget of the destination, respectively. C3 is the constraint on the position of the UAV, in which r_{max} denotes UAV maximum flight radius. $P_{r,\max}$ and $P_{AN,\max}$ denote the maximum transmit power of UAV and AN, respectively.

Remark 1: In this paper, only the position of the UAV is optimized. This is due to the fact that we focus on the cases when an UAV needs to steer away from the estimated location of multiple eavesdroppers while approaching its intended receiver as close as possible at the same time to enhance the secrecy rate. For this scenario, the UAV position design is particularly appealing since it can strike a balance between communication efficiency and security.

III. Joint Design of the Maximization Problem

In this section, we maximize the minimum secrecy rate by jointly designing the AN transmit power, the TS and PS ratios, as well as the UAV's position and amplification factor. It is obvious that the formulated problem in (16) is not convex and difficult to solve due to the coupling between variables σ_{Zd}^2, α, ρ, β, and (x, y) in both SINR and transmit power constraints. Furthermore, the imperfect locations of the eavesdroppers impose semi-infinite numbers of constraints, which make the optimization problem more intractable. To tackle these non-convexity issues, we first define R_e^* as the upper bound of the achieved rate of E_k in the presence of estimation errors, which is equivalent to

$$\begin{aligned} R_e^* &= \max_{k\in\{1,2,\ldots,n\}} \; \max_{\Delta x_k, \Delta y_k \in \xi} \; \{R_{e_k}\} \\ &= \max_{k\in\{1,2,\ldots,n\}} \; \max_{\Delta x_k, \Delta y_k \in \xi} \; (1-\alpha)\log_2\!\left(1 + \frac{\beta\rho P_s |h_{sr}|^2}{\beta\rho\sigma_r^2 + \beta\sigma_{ID}^2 + \frac{\sigma_{Zd}^2 |h_{de_k}|^2 + \sigma_e^2}{|h_{re_k}|^2}}\right) \\ &\qquad \text{s.t. } \Delta x_k^2 + \Delta y_k^2 \le \Delta Q_k^2, \forall k. \end{aligned} \tag{17}$$

In the following, we aim to determine the highest achievable rate of the multiple eavesdroppers with imperfect locations for a given position of the UAV, which facilitates the design of resource allocation in later sections. To efficiently solve problem (17), we introduce a new variable $g(\Delta x_k, \Delta y_k) = \frac{\sigma_{Zd}^2 |h_{de_k}|^2 + \sigma_e^2}{|h_{re_k}|^2} = \frac{\sigma_{Zd}^2 \beta_0 d_{re_k}^2 + \sigma_e^2 d_{re_k}^2 d_{de_k}^2}{\beta_0 d_{de_k}^2}$, where $d_{re_k}^2 = (x - (x_{E_k} + \Delta x_k))^2 + (y - (y_{E_k} + \Delta y_k))^2 + H^2$ and $d_{de_k}^2 = ((x_{E_k} + \Delta x_k) - x_D)^2 + ((y_{E_k} + \Delta y_k) - y_D)^2$; then, the problem defined in (17) can be equivalently reformulated as follows:

$$\begin{aligned} \min_{k\in\{1,2,\ldots,n\}} \; \min_{\Delta x_k, \Delta y_k \in \xi} \; & g(\Delta x_k, \Delta y_k) \\ \text{s.t. } & \Delta Q_k^2 - \Delta x_k^2 - \Delta y_k^2 \ge 0. \end{aligned} \tag{18}$$

The problem defined in (18) is still difficult to be solved optimally due to the coupled variables d_{re_k} and d_{de_k} in both numerator and denominator of $g(\Delta x_k, \Delta y_k)$. To tackle this issue, we propose a multi-dimensional line search to obtain an approximated optimal solution, which is summarized in Table II. As a result, the problem (16) can be simplified as

$$\begin{aligned} \max_{\sigma_{Zd}^2, \alpha, \rho, \beta, (x,y)} \; & [R_d - R_e^*]^+ \\ \text{s.t. } & C1 - C6. \end{aligned} \tag{19}$$

Remark 2: From Table II, for a given position of the UAV, due to the limitation of the estimation errors, an approximated optimal solution (Δx_k^*,Δy_k^*) can be obtained by adjusting the search interval τ, which provides a tight upper bound R_e^* to problem (17).

TABLE II
Proposed Multi-dimensional Search for Solving (18).

Set the search range $[-\Delta Q_k, 3\Delta Q_k]$, $k \in \{1, 2, \cdots, n\}$ and search interval $\tau = 0.05$;
Initialize $\Delta x_k^L = -\Delta Q_k$, $g_k^L = 1000$, $L = 1$;
While $\Delta Q_k > 0$ do
  While $\Delta x_k^L < 3\Delta Q_k$ do
    If $\Delta x_k^L \le \Delta Q_k$, calculate $\Delta y_k^L = \sqrt{(\Delta Q_k)^2 - (\Delta x_k^L)^2}$;
    Determine $g^L(\Delta x_k^L, \Delta y_k^L)$ and $g_k^L = \min\{g^L(\Delta x_k^L, \Delta y_k^L), g_k^L\}$;
    Else compute $\Delta y_k^L = -\sqrt{(\Delta Q_k)^2 - (\Delta x_k^L - 2\Delta Q_k)^2}$;
    Determine $g^L(\Delta x_k^L, \Delta y_k^L)$ and $g_k^L = \min\{g^L(\Delta x_k^L, \Delta y_k^L), g_k^L\}$;
    End
    Update $\Delta x_k^L = \Delta x_k^L + \tau$ and $L = L + 1$;
  Update $\Delta Q_k = \Delta Q_k - \tau$;
Return $g_k^* = g_k^L$, $\Delta x_k^* = \Delta x_k^L$, $\Delta y_k^* = \Delta y_k^L$;
Output $g^* = min\{g_1^*, g_2^*, ..., g_n^*\}$.

Then, to tackle the non-smoothness of the objective function of problem (19), the following lemma is presented.

LEMMA 1. *Problem* (19) *has the same optimal solution as that of the following problem:*

$$\begin{aligned} \max_{\sigma_{Zd}^2,\alpha,\rho,\beta,(x,y)} \; & R_d - R_e^* \\ \text{s.t. } & C1 - C6. \end{aligned} \tag{20}$$

Proof: Please refer to Appendix A. ■

Although problem (20) resolves the non-smoothness of the objective function, the optimization problem is still non-convex due to the coupling of multiple variables. As a compromise approach, we aim to design a suboptimal iterative algorithm by dividing the problem at hand into three sub-problems and solve them iteratively [45], [46]. The key idea is to optimize a subset of variables while the remaining ones are fixed to obtain the locally optimal solution.

A. Joint Optimization of AN Transmit Power σ_{Zd}^2 and TS Ratio α

For given ρ, β, and (x, y), the problem defined in (20) can be reformulated into the following form:

$$\begin{aligned} \max_{\sigma_{Zd}^2,\alpha} \; & (1-\alpha)\left[A_1 - \log_2\left(1 + \frac{A_2}{A_3 + \sigma_{Zd}^2}\right)\right] \\ \text{s.t. } & C1: \sigma_{Zd}^2(1-\alpha) + A_4 \le 0, \\ & C2: A_5 \le \alpha, \\ & C3: \sigma_{Zd}^2 \le P_{AN,\max}, \\ & C4: 0 \le \alpha \le 1, \end{aligned} \tag{21}$$

where $A_1 = \log_2(1 + \text{SINR}_\text{d})$, $A_2 = \frac{\beta\rho P_s |h_{re}^* h_{sr}|^2}{|h_{de}^*|^2}$, $A_3 = \frac{\beta\rho\sigma_r^2|h_{re}^*|^2 + \beta\sigma_{ID}^2|h_{re}^*|^2 + \sigma_e^2}{|h_{de}^*|^2}$, $A_4 = -\frac{E_d - E_{SIC}}{T}$ and $A_5 = \frac{\beta\rho P_s|h_{sr}|^2 + \beta\rho\sigma_r^2 + \beta\sigma_{ID}^2 + P_{cr}}{\beta\rho P_s|h_{sr}|^2 + \beta\rho\sigma_r^2 + \beta\sigma_{ID}^2 + P_{cr} + \eta(1-\rho)P_s|h_{sr}|^2}$.

Now, we adopt the following theorem to solve the problem defined in (21).

THEOREM 1. *The optimal solution of problem* (21) *can be obtained in the following three cases:*

- *When constraints $C1$ and $C2$ are satisfied with equality, the optimal solutions $\{{\sigma_{Zd}^2}^*, \alpha^*\}$ are given by*

$$\begin{aligned} {\sigma_{Zd}^2}^* &= -\frac{A_4}{1 - A_5}, \\ \alpha^* &= A_5. \end{aligned} \tag{22}$$

- *When constraints $C1$ and $C3$ are satisfied with equality, the optimal solutions $\{{\sigma_{Zd}^2}^*, \alpha^*\}$ can be expressed as*

$$\begin{aligned} {\sigma_{Zd}^2}^* &= P_{AN,\max}, \\ \alpha^* &= 1 + \frac{A_4}{P_{AN,\max}}. \end{aligned} \tag{23}$$

- *When constraints $C2$ and $C3$ are satisfied with equality, the optimal solutions $\{{\sigma_{Zd}^2}^*, \alpha^*\}$ can be denoted as*

$$\begin{aligned} {\sigma_{Zd}^2}^* &= P_{AN,\max}, \\ \alpha^* &= A_5. \end{aligned} \tag{24}$$

Proof: Please refer to Appendix B. ■

We compare the values of the objective function by substituting (22)−(24) into (21) and select one with the highest objective value as the optimal solution.

Remark 3: From Theorem 1, the optimal AN transmit power σ_{Zd}^2 and the TS ratio α for given ρ, β, and (x, y) can be jointly attained as a closed-formed expression. Furthermore, as can be seen from (22)−(24), only a small AN is needed when the UAV harvested energy is fully used for information relaying.

B. Optimization of PS Ratio ρ

In this subsection, we fix variables σ_{Zd}^2, α, β, and (x, y) for optimizing the PS ratio, ρ, at the UAV. Then the problem defined in (20) can be equivalently recast as follows by introducing a new variable $m = \frac{1}{\rho}$:

$$\begin{aligned} \max_{m} \; & \frac{1 + \frac{1}{B_1 + B_2 m}}{1 + \frac{1}{B_3 + B_4 m}} \\ \text{s.t. } & 1 < B_5 \le m, \\ & B_6 \le m, \end{aligned} \tag{25}$$

where $B_1 = \frac{\sigma_r^2}{P_s|h_{sr}|^2}$, $B_2 = \frac{\beta\sigma_{ID}^2|h_{rd}|^2 + \sigma_{SI}^2|f_d|^2 + \sigma_d^2}{\beta P_s|h_{rd}h_{sr}|^2}$, $B_3 = \frac{\sigma_r^2}{P_s|h_{sr}|^2}$, $B_4 = \frac{\beta\sigma_{ID}^2|h_{re}^*|^2 + \sigma_{Zd}^2|h_{de}^*|^2 + \sigma_e^2}{\beta P_s|h_{re}^* h_{sr}|^2}$, $B_5 = \frac{(1-\alpha)\beta P_s|h_{sr}|^2 + \alpha\eta P_s|h_{sr}|^2 + (1-\alpha)\beta\sigma_r^2}{\alpha\eta P_s|h_{sr}|^2 - (1-\alpha)(\beta\sigma_{ID}^2 + P_{cr})}$, and $B_6 = \frac{\beta P_s|h_{sr}|^2 + \beta\sigma_r^2}{P_{r,\max} - \beta\sigma_{ID}^2}$.

THEOREM 2. *$B_2 < B_4$ always hold and the optimal solution of the problem defined in* (25) *can be derived in the following two closed-forms:*

- *When $B_7 < \max\{B_5, B_6\}$, the optimal ρ^* can be given by*

$$\rho^* = \min\left\{\frac{1}{B_5}, \frac{1}{B_6}\right\}, \tag{26}$$

  where $B_7 = \sqrt{\frac{B_1 B_3 + B_1}{B_2 B_4}}$.
- *When $B_7 \ge \max\{B_5, B_6\}$, the optimal ρ^* can be denoted as*

$$\rho^* = \frac{1}{B_7}. \tag{27}$$

Proof: Please refer to Appendix C. ■

Remark 4: Based on Theorem 2, for given σ_{Zd}^2, α, β, and (x, y), the optimal PS ratio, ρ, can be derived as a closed-form expression. Thus, we can always split the received signal at the UAV into two optimal portions for EH and ID. Evidently, the system prefers to assign more signal power on ID with lower value of B_n, $n \in \{5, 6, 7\}$.

C. Joint Optimization of UAV's Position (x, y) and Amplification Factor β.

With fixed variables σ_{Zd}^2, α, and ρ, the problem defined in (20) can be reformulated as

$$\begin{aligned} \max_{\beta,(x,y)} \; & \frac{1 + \frac{\beta\rho P_s|h_{rd}h_{sr}|^2}{\beta\rho\sigma_r^2|h_{rd}|^2 + \beta\sigma_{ID}^2|h_{rd}|^2 + \sigma_{SI}^2|f_d|^2 + \sigma_d^2}}{1 + \frac{\beta\rho P_s|h_{re}^* h_{sr}|^2}{\beta\rho\sigma_r^2|h_{re}^*|^2 + \beta\sigma_{ID}^2|h_{re}^*|^2 + \sigma_{Zd}^2|h_{de}^*|^2 + \sigma_e^2}} \\ \textit{s.t. } & C1, C3, C4. \end{aligned} \tag{28}$$

TABLE III
PROPOSED MULTI-DIMENSIONAL SEARCH FOR SOLVING (28).

1: **Set** the search radius $r\epsilon[0, r_{max}]$, the search range $[-r, 3r]$ and search interval $\tau = 0.05$;
2: **Initialize** $x = -r$, $r = 0$, $R = 0$;
3 **While** $r \leq r_{max}$ do
4: **While** $x < 3r$ do
5: **If** $x \leq r$, calculate $y = \sqrt{r^2 - (x)^2}$;
6: **Else** compute $y = -\sqrt{r^2 - (x - 2r)^2}$;
7: **End**
8: **If** $D_7 < \max\{D_5, D_6\}$, Determine $\beta^* = \min\{\frac{1}{D_5}, \frac{1}{D_6}\}$;
9: **Else** Determine $\beta^* = \frac{1}{D_7}$;
10: **End**
11: Determine $R_{WSCR} = R_d - R_e$ and $R = \max\{R_{WSCR}, R\}$;
12: Update $x = x + \tau$;
13: Update $r = r + \tau$.

By substituting (1) into (28), the problem defined in (28) is still a non-convex problem due to the coupled variables β, x, and y in both the objective function and the constraints. To tackle this issue, we introduce a new variable $u = \frac{1}{\beta}$, then, the problem defined in (28) reduces to the following problem with a given position of the UAV (x, y):

$$\begin{aligned} \max_{u} \ & \frac{1 + \frac{1}{D_1 + D_2 u}}{1 + \frac{1}{D_3 + D_4 u}} \\ \textit{s.t.} \ & D_5 \leq u, \\ & D_6 \leq u, \end{aligned} \tag{29}$$

where $D_1 = \frac{\rho\sigma_r^2 + \sigma_{ID}^2}{\rho P_s |h_{sr}|^2}$, $D_2 = \frac{\sigma_{SI}^2 |f_d|^2 + \sigma_d^2}{\rho P_s |h_{rd} h_{sr}|^2}$, $D_3 = \frac{\rho\sigma_r^2 + \sigma_{ID}^2}{\rho P_s |h_{sr}|^2}$, $D_4 = \frac{\sigma_{Zd}^2 |h_{de}^*|^2 + \sigma_d^2}{\rho P_s |h_{re}^* h_{sr}|^2}$, $D_5 = \frac{(1-\alpha)\rho P_s |h_{sr}|^2 + (1-\alpha)\rho\sigma_r^2 + \rho\sigma_{ID}^2}{\eta\alpha(1-\rho) P_s |h_{sr}|^2 - (1-\alpha) P_{cr}}$, and $D_6 = \frac{P_s |h_{sr}|^2 + \sigma_r^2 + \sigma_{ID}^2}{P_{r,max}}$.

Following this transformation, it is easy to verify that problem (29) is similar to problem (25). Thus, according to Theorem 2, the optimal solutions of the problem defined in (29) can be easily derived. Then, we propose a multi-dimensional search to obtain the approximate optimal solutions of the problem defined in (28), which is summarized in Table III. Based on Theorem 2 and Table III, the UAV position $\{x, y\}$ and amplification factor β can be expressed respectively as

- When $D_7 < \max\{D_5, D_6\}$, the optimal $\{x^*, y^*, \beta^*\}$ are given by

$$x^* = x, \quad y^* = y, \quad \beta^* = \min\{\frac{1}{D_5}, \frac{1}{D_6}\}, \tag{30}$$

  where $D_7 = \sqrt{\frac{D_1 D_3 + D_1}{D_2 D_4}}$.
- When $D_7 \geq \max\{D_5, D_6\}$, the optimal $\{x^*, y^*, \beta^*\}$ can be denoted as

$$x^* = x, \quad y^* = y, \quad \beta^* = \frac{1}{D_7}. \tag{31}$$

Table III shows that when variables σ_{Zd}^2, α, and ρ are given, the UAV position $\{x, y\}$ and amplification factor β can be easily found by the proposed line search. Then, we select the variable set that corresponds to the maximum objective value as the optimal solutions.

TABLE IV
THE PROPOSED ITERATIVE OPTIMIZATION ALGORITHM.

1: **Set** $n_{max} = 100$, $n = 0$, $\gamma = 10^{-5}$, $R_0^n = 0$, $R_f^n = 100$;
2: **Initialize** P_s, ρ, x, y, and β;
3: **While** $R_f^n > \gamma$ and $n < n_{max}$ do;
4: Calculate R_e^* of (17) based on Table II;
5: Calculate ${\sigma_{Zd}^2}^*$ and α^* by substituting (22)−(24) into (21);
6: Calculate ρ^* of (25) based on (26) or (27);
7: Calculate (x^*, y^*) and β^* of (28) by using (30) or (31);
8: Determine $R_{WCSR}^n = R_d^n - R_e^{*n}$;
9: Update $R_f^n = |R_0^n - R_{WCSR}^n|$, $R_0^{n+1} = R_{WCSR}^n$ and $n = n + 1$.

D. Iterative Optimization Algorithm

In this subsection, we combine the proposed solution approaches in subsections A, B, and C to develop an iterative algorithm, which is summarized in Table IV. Specifically, a suboptimal solution of the problem defined in (16) can be found by the proposed iterative algorithm when its convergence is guaranteed. Therefore, the convergence analysis of our proposed algorithm is given in the following.

LEMMA 2. *The convergence of the proposed iterative optimization algorithm in Table IV is guaranteed.*

Proof: Please refer to Appendix D. ■

E. Computational Complexity Analysis

We define the computational complexity for the proposed algorithm in Table IV as presented in the following: In each iteration of Table IV, the main contributions to the computational complexity of the proposed algorithm arise from the complexities introduced by solving problems defined in (17) and (28) in steps 4 and 7. In particular, the complexity of solving (17) is $O(n_1 N_1)$, where n_1 is the number of eavesdroppers and N_1 is the range of the k-th eavesdropper' imperfect locations. Furthermore, the complexity of solving (28) is $O(n_2 N_2)$, where n_2 and N_2 denote the numbers of search radius and search steps, respectively. Thus, the total complexity of the proposed algorithm in Table IV is $O[(n_1 N_1 + n_2 N_2) N_{ite}]$, where N_{ite} is the number of required iterations, which will be illustrated in the following simulations.

IV. SIMULATION RESULTS

In this section, we provide numerical simulation results to validate the performance of the proposed scheme. The setting of simulation is discussed in the following. The channels h_{sr}, h_{rd}, h_{re_k}, and h_{de_k} are assumed to be LoS channels and the power gain β_0 is 50 dBm [21], [28]. The channel f_d is modeled as Rayleigh fading distribution, following $\mathcal{CN}(0, 1)$ [20]. The coordinates of the source and destination are set to $(x_S, 0, 0) = (-100, 0, 0)$ m and $(x_D, 0, 0) = (100, 0, 0)$ m, respectively. It is assumed that there exists three eavesdroppers, which are randomly and uniformly distributed within a 2D area of 150×150 m. The following results are obtained based on one random realization of the eavesdroppers estimated coordinates as $(x_{E_1}, y_{E_1}, 0) = (0, 0, 0)$

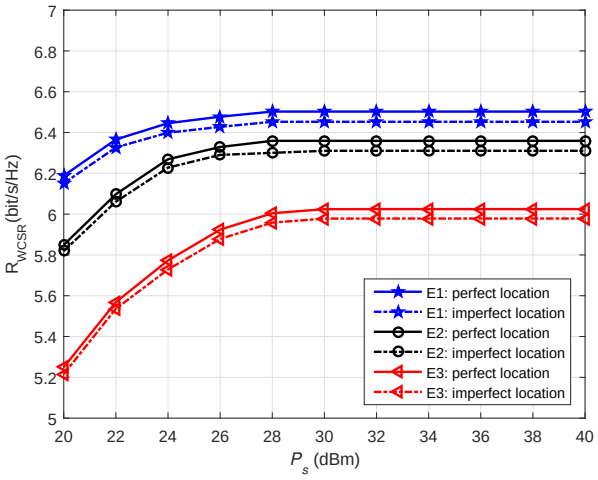


Fig. 3. The achieved secrecy rates at different eavesdroppers versus P_s. Solid curves present the scenarios with perfect location information, while dashed curves are for imperfect location information.

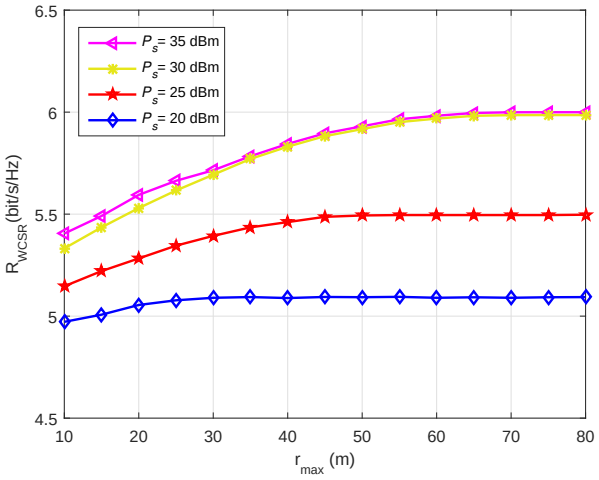


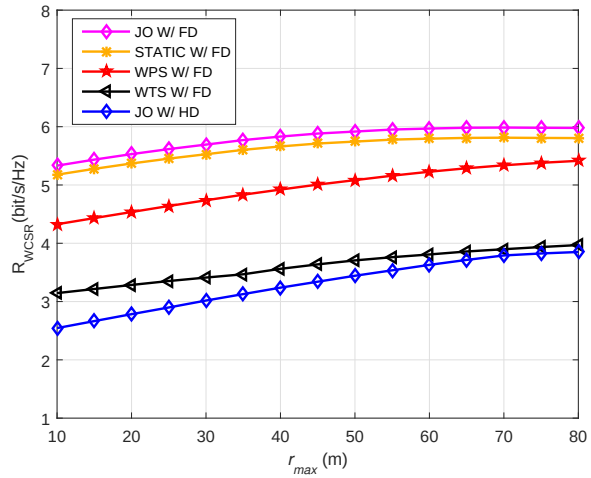
Fig. 4. The achieved secrecy rate with different source transmit powers P_s at various UAV flight radii.

m, $(x_{E_2}, y_{E_2}, 0) = (0, -40, 0)$ m, and $(x_{E_3}, y_{E_3}, 0) = (-40, 0, 0)$ m, respectively. Furthermore, the noise variances are assumed to be $\sigma_r^2 = \sigma_{ID}^2 = \sigma_d^2 = \sigma_e^2 = -30$ dBm [48]. Moreover, unless otherwise specified, $\eta = 0.8$ is the energy conversion efficiency, $P_{cr} = 10$ dBm is the circuit power consumption [44], $P_s = 30$ dBm is the transmit power at the source, $P_{AN,\max} = 20$ dBm and $P_{r,\max} = 25$ dBm are the maximum transmit power of AN and UAV, respectively [49]. In addition, $E_d = 100$ mW is the energy budget of the destination, $E_{SIC} = 50$ mW is the energy consumption of SIC, $\Delta Q_k = 5$ m is the estimation error, $H = 80$ m is the flight altitude, and $r_{max} = 80$ m is the maximum flight radius, respectively.

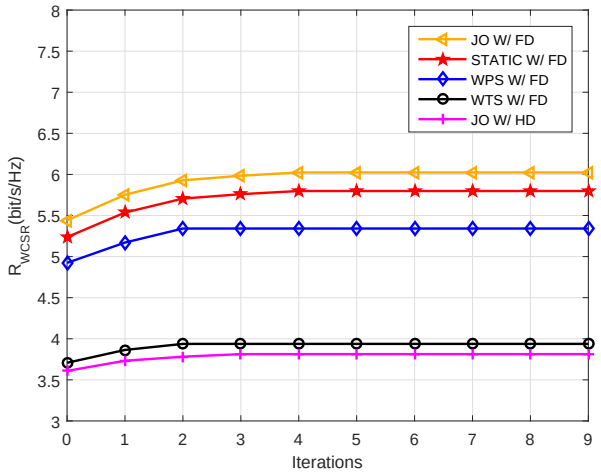
Fig. 3 compares the secrecy rate of the proposed scheme received at different eavesdroppers with the case of perfect locations information (solid curves) and the imperfect locations information (dashed curves), respectively. As can be seen in Fig. 3, the achieved secrecy rates first increase and then become saturated as the available transmit power (P_s) at the source increases in all cases. The reason behind this behavior is that the harvested energy increases with the increasing source transmit power, which provides perpetual energy for the UAV to relay the desired information. However, when P_s is sufficiently large, the UAV cannot fully exhaust all the harvested energy for transmission as there is a maximum transmit power constraint at the UAV. As expected, the achievable secrecy rate performance of the eavesdropper with imperfect location information is worse than that of perfect locations information due to the location estimation errors. However, it is obvious that our proposed robust scheme (imperfect locations) could achieve a similar performance with the perfect scheme (perfect locations). Moreover, compared to the achieved secrecy rate between the destination and eavesdroppers $E1$ and $E2$, the secrecy rate between the destination and eavesdropper $E3$ has the worst performance. The reason is that eavesdroppers $E1$ and $E2$ are closer to the destination node D than E_3, and hence, the AN jamming is more effective on $E1$ and $E2$ to improve the secrecy rate.

Fig. 4 presents the max-min secrecy rate versus different maximum flight radii r_{max} and source transmit powers P_s, respectively. As can be seen in Fig. 4, the achieved secrecy rate first increases and then saturates as the source transmit power P_s increases for all considered values of the maximum flight radius r_{max}, which has been explained in detail in the previous paragraph. Moreover, with different P_s, the achieved secrecy rate also first increases and then saturates as r_{max} increases. This is because when the harvested energy meets the energy consumption requirements at the UAV, increasing r_{max} would result in a higher SINR at the destination due to the UAV's optimal position closer to the destination. However, when r_{max} is sufficiently large, the UAV needs to harvest more energy from the signal received from the source to satisfy the EH constraints, which results in less information received at the UAV. Thus, the UAV will keep the optimal position unchanged with r_{max} increasing to obtain the best system performance.

Fig. 5(a) compares the performance of our proposed robust joint design with FD destination (denoted as JO W/FD) with other four benchmark schemes, namely: 1) Robust FD design without optimizing the UAV's position (STATIC W/FD), i.e., $(x, y, H) = (-r_{max}, 0, 80)$ m, where $r_{max} = 10 : 5 : 80$; 2) Robust FD design without optimizing the PS ratio (WPS W/FD), i.e., $\rho = 0.2$; 3) Robust FD design without optimizing the TS ratio (WTS W/FD), i.e., $\alpha = 0.7$; 4) Robust joint design with half-duplex (HD) destination (JO W/HD). From the simulation results illustrated in Fig. 5(a), it is observed that the max-min secrecy rate of all schemes first increases and then saturates as the maximum flight radius r_{max} increases, showing trends similar to Fig. 4. Furthermore, as expected, the proposed algorithm achieves a superior performance when compared with the other three FD schemes. The reason is that the proposed joint design can exploit effectively more



(a)



(b)

Fig. 5. Achieved secrecy rates and convergence of different algorithms: (a) The achieved secrecy rates versus r_{max}. (b) The achieved secrecy rates versus the iteration number.

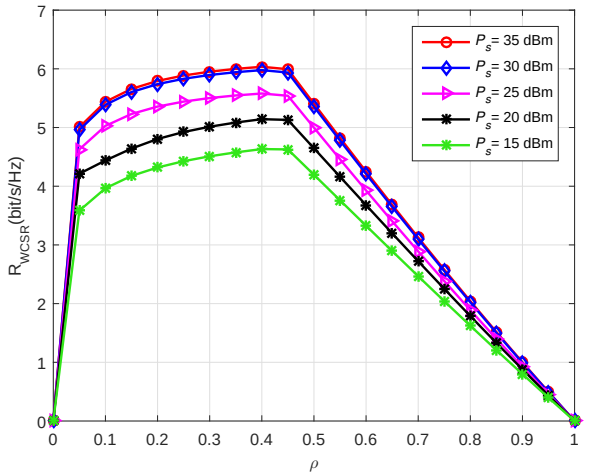


Fig. 6. The effect of the PS ratio, ρ, on the max-min secrecy rates with different source transmit powers.

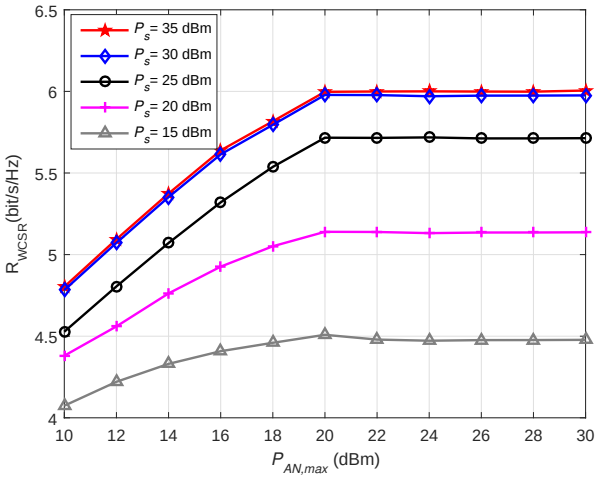


Fig. 7. The effect of AN on the max-min secrecy rates with different source transmit powers.

degrees of freedom of the UAV's position, PS, and TS ratio. In addition, compared with the joint HD scheme, the proposed joint FD scheme significantly improves the secrecy rate since it can transmit malicious AN signal to confuse the eavesdroppers.

Fig. 5(b) illustrates the convergence performance comparison of our proposed algorithm and other four benchmark algorithms. As can be seen in Fig. 5(b), the max-min secrecy rate of all algorithms first increases with the number of iterations in Table IV, and then converges to a constant within a few iterations. In addition, it is also observed that our proposed joint FD scheme has a similar convergence rate as the other benchmark algorithms. From Fig. 5(b), it is noticed that only about 4 iterations are required on average for the convergence of the proposed algorithm.

Fig. 6 presents the achievable max-min secrecy rates versus different PS ratios ρ and source transmit powers P_s, respectively. As shown in Fig. 6, the achieved secrecy rate increases with the PS ratio until it reaches the maximum for all considered P_s values. However, when the PS ratio ρ is sufficiently large, the achieved secrecy rate of all curves decreases dramatically. The reason is that when the PS ratio ρ is large enough, a larger TS ratio α needs to be allocated for the EH to satisfy the energy consumption requirements at the UAV relay, which results in less time allocated for the information forwarding within the entire communication time. In addition, with different P_s values, it is seen that the best performance for all considered scenarios is achieved when $\rho = 0.45$. This implies that splitting the received signal at the UAV into two unequal portions, as $\sqrt{0.45}\, y_r$ for ID and $\sqrt{0.55}\, y_r$ for EH, appears to be the best choice.

Fig. 7 presents the achievable max-min secrecy rates versus the AN transmit power, $\sigma^2_{Z_d}$, for different source transmit powers P_s. As seen from this figure, the achieved secrecy rate first increases and then saturates as the AN power $\sigma^2_{Z_d}$

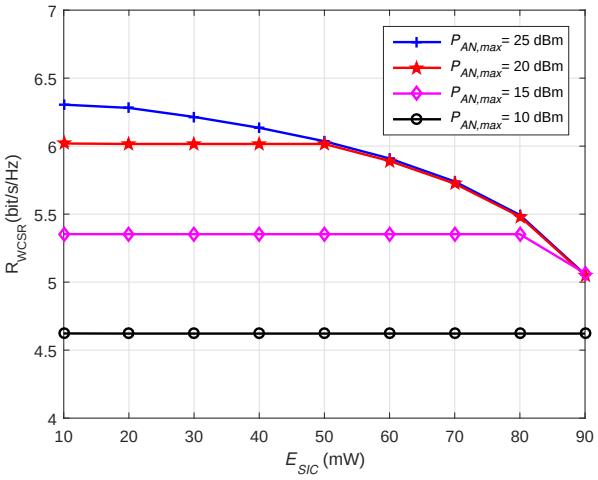


Fig. 8. The effect of energy consumption of SIC on the max-min secrecy rates with different AN transmit powers.

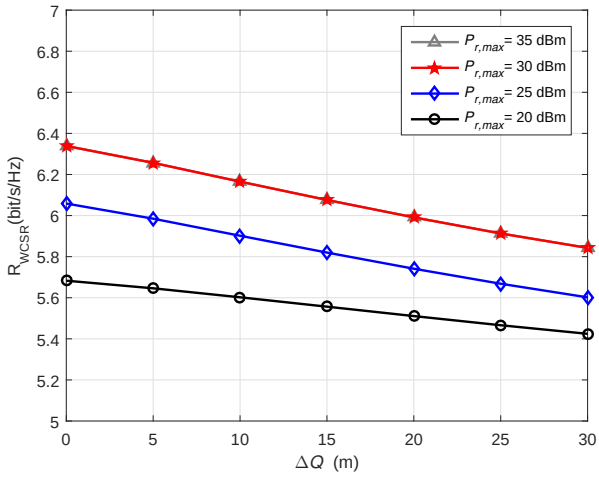


Fig. 9. The effect of the estimated errors on the max-min secrecy rates with different maximum transmit power at UAV.

increases, regardless of the P_s value. This is because when $P_{AN,max}$ is small, increasing the AN can deteriorate the instantaneous SINR at the eavesdropper quickly. However, when $P_{AN,\max}$ is large enough, the destination cannot fully use the maximum available power to transmit AN due to the fact that there is an energy budget constraint at the destination. Furthermore, the system performance will also be affected by E_d and E_{SIC}, which will be discussed in the following simulations.

Next, we show the achievable max-min secrecy rates versus the energy consumption of SIC, E_{SIC}, and for different maximum available AN transmit power, $P_{AN,\max}$. From the simulation results illustrated in Fig. 8, when $P_{AN,\max}$ is large, the achieved secrecy rate decreases as E_{SIC} increases. The reason is that increasing E_{SIC} results in less transmission power allocated for AN jamming at destination. Moreover, it is worth noting that when $P_{AN,\max}$ is small, i.e., $P_{AN,\max} = 10$ dBm, the achieved secrecy rate remains constant for different E_{SIC} values. The reason is that the destination can always use the maximum available power to transmit AN when the energy budget is sufficiently large.

Fig. 9 illustrates the achievable max-min secrecy rate versus the estimation error radius ΔQ_k and for different maximum transmit power $P_{r,\max}$ at UAV. As presented in Fig. 9 and as expected, the achieved secrecy rate steadily decreases as ΔQ_k increases for all considered values of $P_{r,\max}$. This is because the uncertainty of eavesdroppers' locations is larger for a larger ΔQ_k, and the resource allocation and position design would be more conservative, in turn, this leads to a less efficient utilization of system resources. In addition, as can be seen in Fig. 9, when the maximum available transmit power at the UAV is large, i.e., $P_{r,\max} = 30$ dBm and $P_{r,\max} = 35$ dBm, the achieved secrecy rate remains the same with different ΔQ_k. The reason is that the achieved secrecy rate is mainly limited by EH at the UAV when the source transmit power is small, and increasing the maximum transmit power allowance of the UAV does not necessarily help to enhance the secrecy rate performance.

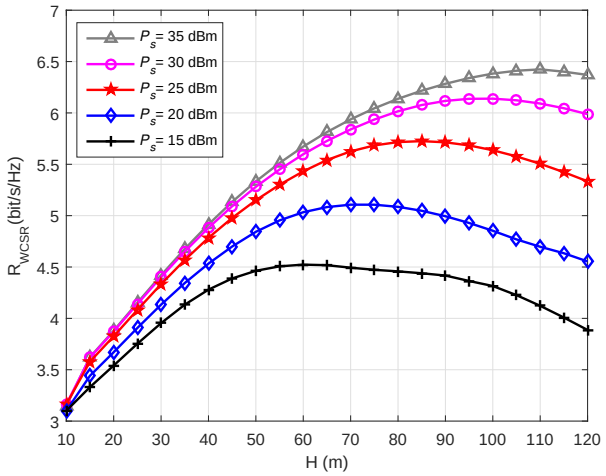


Fig. 10. The effect of the flight height of UAV on the max-min secrecy rates with different source transmit powers.

Finally, we present the achieved max-min secrecy rate versus the UAV flight height, H, and for different source transmit power, P_s. As shown in Fig. 10, the achievable secrecy rate increases with increasing H before a saturation point for all the source transmit power P_s assumptions. However, when the flight height H is larger than the saturation point, the achieved secrecy rates decrease dramatically. The reason is that when H is sufficiently large, the UAV needs to harvest more energy from the signal received from the source to satisfy the EH constraints, which results in less information received at the UAV. Moreover, as seen in Fig. 10, the achievable secrecy rate finally reaches the saturation point when P_s is sufficiently large. The reason behind this behavior is that the total harvested energy increases as P_s increases, which enables a higher transmission power available for the UAV.

V. Conclusions

This paper studied the robust joint design for an energy-constrained UAV secure communication system with imperfect eavesdropper locations. In the proposed scheme, with the help of an FD destination transmitting artificial noise to confuse the eavesdroppers, the position of the UAV, the PS and TS ratios as well as the AN power at the FD destination were jointly designed to maximize the minimum secrecy rate under the EH requirement and transmit power constraints. Due to the non-convexity of the design problem, a three-step iterative algorithm was developed to obtain a suboptimal solution of the considered problem. Furthermore, the system performance was evaluated for different system parameters and practical implementation issues were discussed. Finally, numerical results demonstrated that for the case of multiple eavesdroppers with imperfect location information, adopting the proposed FD jamming-based joint design can achieve a significant improvement in the max-min secrecy rate compared to the benchmark schemes.

Appendix A
Proof of Lemma 1

Suppose $\{R_1^*, R_2^*\}$ and $\{f_1, f_2\}$ denote the optimal values and the objective functions of problem (19) and (20), respectively. First, based on $[m]^+$ defined in (16) and due to the fact that problems (19) and (20) have the same constraints, we have $f_1 \geq f_2$ and $R_1^* \geq R_2^*$. Next, we prove that $R_2^* \geq R_1^*$ also holds. Denote $\{{\sigma_{Zd}^2}^*, \alpha^*, \rho^*, \beta^*, (x,y)^*\}$ as the optimal solution of the problem defined in (19). Moreover, we also construct a feasible solution to problem (20), denoted by $\{{\sigma_{Zd}^2}^\dagger, \alpha^\dagger, \rho^\dagger, \beta^\dagger, (x,y)^\dagger\}$, such that ${\sigma_{Zd}^2}^\dagger = {\sigma_{Zd}^2}^*$, $\alpha^\dagger = \alpha^*$, $\rho^\dagger = \rho^*$, and $\beta^\dagger = \beta^*$. When $f_1({\sigma_{Zd}^2}^*, \alpha^*, \rho^*, \beta^*, (x,y)^*) \geq 0$, we have $(x,y)^\dagger = (x,y)^*$; otherwise $(x,y)^\dagger = 0$. By substituting $\{{\sigma_{Zd}^2}^\dagger, \alpha^\dagger, \rho^\dagger, \beta^\dagger, (x,y)^\dagger\}$ into (20), we obtain the objective value $f_2({\sigma_{Zd}^2}^\dagger, \alpha^\dagger, \rho^\dagger, \beta^\dagger, (x,y)^\dagger) = R_2^\dagger$. Thus, the newly constructed solution $\{{\sigma_{Zd}^2}^\dagger, \alpha^\dagger, \rho^\dagger, \beta^\dagger, (x,y)^\dagger\}$ ensures that $R_2^\dagger = R_1^*$. Due to the fact that $\{{\sigma_{Zd}^2}^\dagger, \alpha^\dagger, \rho^\dagger, \beta^\dagger, (x,y)^\dagger\}$ is a feasible solution to problem (20), it follows that $R_2^* \geq R_2^\dagger$. As a result, we have $R_2^* \geq R_1^*$. Therefore, combining both parts above, the relationship $R_1^* = R_2^*$ holds. This completes the proof of Lemma 1. ■

Appendix B
Proof of Theorem 1

Suppose problem (21) is feasible and let $\{\alpha^*, {\sigma_{Zd}^2}^*\}$ represent its optimal solution. First, let us define f as the objective function of the problem defined in (21), then we obtain the first-order partial derivative of f with respect to α and σ_{Zd}^2, respectively:

$$\frac{\partial f}{\partial \alpha} = -\left[A_1 - \log_2\left(1 + \frac{A_2}{A_3 + \sigma_{Zd}^2}\right)\right], \tag{32}$$

and

$$\frac{\partial f}{\partial \sigma_{Zd}^2} = \frac{A_2(1-\alpha)}{\ln 2\left[(A_3 + \sigma_{Zd}^2)^2 + A_2(A_3 + \sigma_{Zd}^2)\right]}. \tag{33}$$

Based on f defined in (21) and due to the fact that $\{A_1, A_2, A_3\} > 0$, we have $\frac{\partial f}{\partial \alpha} < 0$ and $\frac{\partial f}{\partial \sigma_{Zd}^2} > 0$.

Next, we prove that the optimal solutions α^* and ${\sigma_{Zd}^2}^*$ must satisfy the constraints $C1$ or $C2$ and $C1$ or $C3$ with equality, respectively. This can be proved by contradiction. Namely, if the above conditions are not satisfied, we can find another solution of problem (21), denoted by $\{\alpha^\dagger, {\sigma_{Zd}^2}^\dagger\}$, which achieves a higher objective value. In this case, for any given σ_{Zd}^2, constraints $C1$ and $C2$ can be equivalently rewritten as

$$\alpha \geq 1 + \frac{A_4}{\sigma_{Zd}^2}, \tag{34}$$

and

$$\alpha \geq A_5. \tag{35}$$

Due to the fact that $\frac{\partial f}{\partial \alpha} < 0$, the objective function f is strictly monotonically decreasing with respect to α, and it can be observed that when $\alpha^* = \max\{1 + \frac{A_4}{\sigma_{Zd}^2}, A_5\}$, the objective value $f(\alpha^*) > f(\alpha^\dagger)$. Similarly, for a given α, constraints $C1$ and $C3$ can be expressed respectively as:

$$\sigma_{Zd}^2 \leq -\frac{A_4}{1-\alpha}, \tag{36}$$

and

$$\sigma_{Zd}^2 \leq P_{AN,\max}. \tag{37}$$

As a result, when ${\sigma_{Zd}^2}^* = \min\{-\frac{A_4}{1-\alpha}, P_{AN,\max}\}$, we can easily obtain $f({\sigma_{Zd}^2}^*) > f({\sigma_{Zd}^2}^\dagger)$ based on the fact that the objective function f is a strictly increasing function with respect to σ_{Zd}^2. Thus, these contradict our assumption. In conclusion, the optimal solution $\{\alpha^*, {\sigma_{Zd}^2}^*\}$ must satisfy EH or transmit power constraint with equality.

Moreover, for given $\{\alpha^*, {\sigma_{Zd}^2}^*\}$, we can prove that at least two constraints of problem (21) are satisfied with equality. This can also be proved by contradiction. Firstly, suppose optimal solutions $\{\alpha^*, {\sigma_{Zd}^2}^*\}$ can be obtained when only constraint $C2$ is satisfied with equality. In this case, for a given α, the objective function value increases as σ_{Zd}^2 increases due to $\frac{\partial f}{\partial \sigma_{Zd}^2} > 0$. Therefore, the objective function can achieve a higher value when constraint $C1$ or $C3$ are satisfied with equality. Thus, this assumption is not valid. Secondly, for the other assumptions where only one constraint is satisfied with equality, we can easily prove that these assumptions are not valid either. Combining both parts above, the optimal solution $\{\alpha^*, {\sigma_{Zd}^2}^*\}$ of problem (21) can be obtained as the three cases provided in (22)−(24). This completes the proof of Theorem 1. ■

APPENDIX C
PROOF OF THEOREM 2

Due to the fact that $B_1 = B_3$, the problem (25) can be equivalently rewritten as

$$\begin{aligned} \max_{m} \ & \frac{(B_4 - B_2)m}{m^2 + \frac{B_1B_4+B_2B_3+B_2}{B_2B_4}m + \frac{B_1B_3+B_1}{B_2B_4}} \\ s.t. \ & 1 < B_5 \leq m, \\ & B_6 \leq m. \end{aligned} \tag{38}$$

Suppose $f(\cdot)$ denotes the objective function of (38) and then $f(m) = \frac{(B_4-B_2)m}{m^2+\frac{B_1B_4+B_2B_3+B_2}{B_2B_4}m+\frac{B_1B_3+B_1}{B_2B_4}}$. First, we calculate the first-order derivative of f with respect to m as

$$\frac{df}{dm} = \frac{-(B_4 - B_2)(m^2 - B_7^2)}{\left(m^2 + \frac{B_1B_4+B_2B_3+B_2}{B_2B_4}m + \frac{B_1B_3+B_1}{B_2B_4}\right)^2}, \tag{39}$$

where $B_7 = \pm\sqrt{\frac{B_1B_3+B_1}{B_2B_4}}$. If $B_2 < B_4$, based on $m \geq \max\{B_5, B_6\}$ from (25), we can derive that the relationship $B_7 < m$ holds when $B_7 < \max\{B_5, B_6\}$, i.e., $\sqrt{\frac{B_1B_3+B_1}{B_2B_4}} < \max\{B_5, B_6\}$. Then, substituting into (39), we have $\frac{df}{dm} < 0$, which shows that the objective function value decreases as m increases. Therefore, there must exist a maximum value of the objective function $f(m^*)$ when the two constraints of the problem defined in (38) are satisfied with equality. The optimal solution m^* of problem (38) can be expressed as

$$m^* = \max\{B_5, B_6\}. \tag{40}$$

Hence, based on $m = \frac{1}{\rho}$, we can obtain the optimal solution as in (26).

Similarly, when $B_2 < B_4$, if $B_7 \geq m$, due to the fact that $m \geq \max\{B_5, B_6\}$, we can derive that the inequality $\frac{df}{dm} \geq 0$ holds when $\sqrt{\frac{B_1B_3+B_1}{B_2B_4}} \geq m \geq \max\{B_5, B_6\}$. As a result, the objective function $f(m^*)$ is strictly monotonically increasing with respect to m. Hence, the optimal solution m^* of problem (38) can be derived as

$$m^* = B_7. \tag{41}$$

Next, if $\sqrt{\frac{B_1B_3+B_1}{B_2B_4}} \geq \max\{B_5, B_6\}$ and $\sqrt{\frac{B_1B_3+B_1}{B_2B_4}} \leq m$, we have $\frac{df}{dm} \leq 0$, which shows that the value of the objective function decreases as m increases. Thus, the optimal solution m^* of the problem defined in (38) can be attained as in (41). Combining both parts above, we show that the optimal solution can be expressed as in (27).

Finally, we show that $B_2 \geq B_4$ is not possible at the optimal solution ρ^*. We prove this result by contradiction. In this case, for given $B_2 \geq B_4$, the objective function $f(m)$ of problem (38) is negative, i.e., $f(m) \leq 0$. It is easy to verify that the above condition does not hold due to the worst-case secrecy rate determined in problem (16). In conclusion, the optimal solution ρ^* of (25) can be only obtained when $B_2 < B_4$. This completes the proof of Theorem 2. ■

APPENDIX D
PROOF OF LEMMA 2

At the n_{th} iteration, due to the limitation of the estimation errors ΔQ_k, the approximation optimal solution R_e^* of the problem defined in (17) must be firstly obtained by adjusting the search interval τ. Since the other three subproblems (21), (25), and (28) can be optimally solved through steps 5, 6, and 7 in Table IV, respectively, the value of the objective function in problem (16) must be monotonically nondecreasing for this step. Because of that, if the objective value R_{WCSR}^n decreases, we could keep the same optimal solutions ${\sigma_{Zd}^2}^{(n-1)*}$, $\alpha^{(n-1)*}$, $\rho^{(n-1)*}$, $(x, y)^{(n-1)*}$ or $\beta^{(n-1)*}$ unchanged. In addition, the constraints of all subproblems form a compact set, and thus, the objective value of problem (16) is bounded. The monotonicity and bound guarantee that the iterative optimization algorithm converges to a stationary point [47]. This completes the proof of Lemma 2. ■

REFERENCES

[1] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123-1152, Secondquarter 2016.

[2] 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.

[3] M. Mozaffari, W. Saad, M. Bennis, Y. Nam and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334-2360, thirdquarter 2019.

[4] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. G.Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417-3442, Fourthquarter 2019.

[5] Y. Zeng, R. Zhang, and J. Teng, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36-42, Oct. 2016.

[6] H. Shakhatreh, A. H. Sawalmeh, A. A. Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access,* vol. 7, pp. 48572-48634, Apr. 2019.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773-1828, Jun. 2019.

[8] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603-3611, Mar. 2017.

[9] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027-1053, Nov. 2017.

[10] K. Cumanan, Z. Ding, B. Sharif, Y. G. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, pp. 1678-1690, May 2014.

[11] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417-1432, Dec. 2016.

[12] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495-7505, Aug. 2017.

[13] M. Zhang, K. Cumanan, J. Thiyagalingam, W. Wang, A. G. Burr, Z. Ding, and O. A. Dobre, "Energy efficiency optimization for secure transmission in MISO cognitive radio network with energy harvesting," *IEEE Access*, vol. 7, pp. 126234-126252, Sep. 2019.

[14] X. Li, W. Wang, M. Zhang, F. Zhou, and N. AI-Dhahir, "Robust secure beamforming for SWIPT-aided relay systems with full-duplex receiver and imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1867-1878, Feb. 2020.

[15] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, Singapore, Singapore, Dec. 2017.

[16] 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.

[17] Q. Wang, Z. Chen, and W. Mei, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wiress Commun. Lett.*, vol. 6, no. 3, pp. 310-313, Jun. 2017.

[18] N. Zhao, F. Cheng, F. Yu, J. Tang, Y. Chen, G. Gui, and H. Sari, "Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2281-2294, May 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, Jan. 2019.

[20] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2919-2931, Jan. 2019.

[21] 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, Oct. 2018.

[22] 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.

[23] D. Yang, Q. Wu, and Y. Zeng, "Energy tradeoff in ground-to-UAV communication via trajectory design," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6721-6726, Jul. 2018.

[24] C. Zhan, Y. Zeng, and R. Zhang,"Energy-efficient data collection in UAV enabled wireless sensor network," *IEEE Wireless Commun. Lett.*, vol. 7, no. 3, pp. 328-331, Jun. 2018.

[25] C. Wang and Z. Ma, "Design of wireless power transfer device for UAV," in *Proc. IEEE International Conference on Mechatronics and Automation (ICMA)*, pp. 2449-2454, Harbin, China, Aug. 2016.

[26] D. Ke, C. Liu, C. Jiang, and F. Zhao, "Design of an effective wireless air charging system for electric unmanned aerial vehicles," in *Proc. IEEE International Conference on Industrial Electronics (IECON)*, pp. 6949-6954, Beijing, China, Oct. 2017.

[27] Y. Sun, D. Xu, D. W. K. Ng, L. Dai, and R. Schober, "Optimal 3D-trajectory design and resource allocation for solar-powered UAV communication systems," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4281-4298, Jun. 2019.

[28] S. Yin, J. Tan, and L. Li, "UAV-assisted cooperative communications with time-sharing SWIPT," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 20-24, Kansas City, USA, May 2018.

[29] W. Lu, S. Fang, Y. Gong, L. Qian, X. Liu, and J. Hua, "Resource allocation for OFDM relaying wireless power transfer based energy-constrained UAV communication network," in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1-6, Kansas City, USA, May 2018.

[30] M. Hua, C. Li, and Y. Huang, "Throughput maximization for UAV-enabled wireless power transfer in relaying system," in *Proc. International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 11-13, Nanjing, China, Oct. 2017.

[31] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599-4615, Aug. 2014.

[32] X. Chen, D. W. K. Ng, and H. Chen, "Secrecy wireless information and power transfer: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 54-61, Apr. 2016.

[33] X. Hong, P. Liu, F. Zhou, S. Guo, and Z. Chu, "Resource allocation for secure UAV-assisted SWIPT systems," *IEEE Access,* vol. 7, pp. 24248-24257, Feb. 2019.

[34] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong,"Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40-47, Oct. 2019.

[35] M. Jiang, Y. Li, Q. Zhang, and J. Qin, "Joint position and time allocation optimization of UAV enabled time allocation optimization networks," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3806-3816, May 2019.

[36] C. R. Valenta and G. D. Durgin, "Harvesting wireless power: survey of energy-harvester conversion efficiency in far-field, wireless power transfer systems," *IEEE Microw. Mag.*, vol. 15, no. 4, pp. 108-120, Jun. 2014.

[37] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082-2085, Dec. 2015.

[38] Y. Zeng, B. Clerckx, and R. Zhang, "Communications and signals design for wireless power transmission," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2264-2290, May 2017.

[39] X. Sun, W. Yang, Y. Cai, R. Ma, and L. Tao, "Physical layer security in millimeter wave SWIPT UAV-based relay networks," *IEEE Access*, vol. 7, pp. 35851-35861, Apr. 2019.

[40] Y. Li, N. Li, M. Peng, and W. Wang, "Relay power control for two-way full-duplex amplify-and-forward relay networks," *IEEE Signal Process. Lett.*, vol. 23, no. 2, pp. 292-296, Feb. 2016.

[41] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447-3461, Oct. 2014.

[42] Q. Li, W. K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using alamouti-based rank-two beamforming," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1359-1374, Dec. 2016.

[43] W. Wang, R. Wang, W. Duan, R. Feng, and G. Zhang, "Optimal transceiver designs for wireless-powered full-duplex two-way relay networks with SWIPT," *IEEE Access*, vol. 5, pp. 22329-22343, Oct. 2017.

[44] Q. Li and L. Yang. "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Trans. Inf. Forensics and Security*, vol. 15, no. 1, pp. 130-143, May 2019.

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

[46] W. Wang, R. Wang, H. Mehrpouyan, N. Zhao, and G. Zhang, "Beamforming for simultaneous wireless information and power transfer in two-way relay channels," *IEEE Access*, vol. 5, pp. 9235-9250, May 2017.

[47] J. Bibby, "Axiomatisations of the average and a further generalisation of monotonic sequences," *Glasgow Math. J.*, vol. 15, pp. 63-65, 1974.

[48] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154-162, Jan. 2016.

[49] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secrecy performance of the UAV enabled cognitive relay network," in *Proc. International Conference on Communication and Information Systems (ICCIS)*, pp. 1-6, Singapore, Singapore, Dec. 2018.

Wei Wang (M'19) received the B.S. degree in electronic and information engineering from China West Normal University, China, in 2005, and the M.S. degree in signal and information processing from Chengdu University of Technology, China, in 2008, and the Ph.D. degree in communication and information system from Shanghai University, China, in 2011. From Aug. 2011 to Jul. 2014, he was with the School of Information Science and Technology, Nantong University as a Lecturer, where he is currently an Associate Professor. He is also with the Peng Cheng Laboratory and the Nantong Research Institute for Advanced Communication Technologies. From Feb. 2016 to Aug. 2016, he was a Visiting Scholar in the Department of Electrical and Computer Engineering at the Boise State University, ID, USA. From Feb. 2019 to Aug. 2019, he was an Academic Visitor in the Department of Electronic Engineering at the University of York, York, UK. His current research interests include wireless information and power transfer, physical layer security, unmanned aerial vehicle communications, fog/edge computing and machine learning for wireless communications.

Xinrui Li received the B.S. degree in electronic and information engineering from Nantong University, China, in 2018, where he is currently pursuing the M.S. degree in information and communication engineering. His major research interests include wireless information and power transfer, physical layer security and unmanned aerial vehicle communications.

Miao Zhang (S'18) received his B.Sc. degree in Optical Information Science and Technology from Guizhou University, Guiyang, China, M.Sc. in Communications and Signal Processing from the University of Newcastle upon Tyne, Newcastle upon Tyne, UK and PhD degree in Electronic Engineering from the University of York, in 2011, 2015 and 2019, respectively. He is currently working toward the Ph.D. degree in the Department of Electronic Engineering, University of York, York, UK. His research interests are convex optimization techniques, wireless energy harvesting networks, physical layer security and machine learning for wireless communications.

Kanapathippillai Cumanan (M'10-SM'19) received the BSc degree with first class honors in electrical and electronic engineering from the University of Peradeniya, Sri Lanka in 2006 and the PhD degree in signal processing for wireless communications from Loughborough University, Loughborough, UK, in 2009.

He is currently a lecturer at the Department of Electronic Engineering, The University of York, UK. From March 2012 to November 2014, he was working as a research associate at School of Electrical and Electronic Engineering, Newcastle University, UK. Prior to this, he was with the School of Electronic, Electrical and System Engineering, Loughborough University, UK. In 2011, he was an academic visitor at Department of Electrical and Computer Engineering, National University of Singapore, Singapore. From January 2006 to August 2006, he was a teaching assistant with Department of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka. His research interests include non-orthogonal multiple access (NOMA), cell-free massive MIMO, physical layer security, cognitive radio networks, convex optimization techniques and resource allocation techniques. He has published more than 80 journal articles and conference papers which attracted more than 1200 Google scholar citations. He has been also recently appointed as an associate editor for IEEE Access journal.

Dr. Cumanan was the recipient of an overseas research student award scheme (ORSAS) from Cardiff University, Wales, UK, where he was a research student between September 2006 and July 2007.

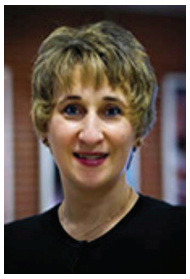
Derrick Wing Kwan Ng (S'06-M'12-SM'17) received the bachelor degree with first-class honors and the Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He received his Ph.D. degree from the University of British Columbia (UBC) in 2012. He was a senior postdoctoral fellow at the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), Germany. He is now working as a Senior Lecturer and a Scientia Fellow at the University of New South Wales, Sydney, Australia. His research interests include convex and non-convex optimization, physical layer security, IRS-assisted communication, UAV-assisted communication, wireless information and power transfer, and green (energy-efficient) wireless communications.

Dr. Ng received the Australian Research Council (ARC) Discovery Early Career Researcher Award 2017, the Best Paper Awards at the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications (ICC) 2018, IEEE International Conference on Computing, Networking and Communications (ICNC) 2016, IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He has been serving as an editorial assistant to the Editor-in-Chief of the IEEE Transactions on Communications from Jan. 2012 to Dec. 2019. He is now serving as an editor for the IEEE Transactions on Communications, the IEEE Transactions on Wireless Communications, and an area editor for the IEEE Open Journal of the Communications Society. Also, he is listed as a Highly Cited Researcher by Clarivate Analytics in 2018 and 2019.

Guoan Zhang received the B.S. degree in precision instrument in 1986, the M.S. degree in automatic instrument and equipment in 1989, and the Ph.D. degree in communication and information system in 2001, from Southeast University, Nanjing, China. He is currently a full professor and doctoral supervisor in the School of Information Science and Technology of Nantong University, Nantong, China. His current research interests include wireless communication networks and internet of vehicles.

Jie Tang (S'10-M'13-SM'18) received the B.Eng. degree in Information Engineering from the South China University of Technology, Guangzhou, China, in 2008, the M.Sc. degree (with Distinction) in Communication Systems and Signal Processing from the University of Bristol, UK, in 2009, and the Ph.D. degree from Loughborough University, Leicestershire, UK, in 2012. From 2003 to 2015, he was a research associate at the School of Electrical and Electronic Engineering, University of Manchester, UK. He is currently a full professor at the School of Electronic and Information Engineering, South China University of Technology, China.

His current research centers around 5G and beyond mobile communications, including topics such as massive MIMO, full-duplex communications, edge caching and fog networking, physical layer security, wireless power transfer and mobile computing. He is a senior member of IEEE, CIE and CIC, and currently serving as an Editor for IEEE Wireless Communications Letters, IEEE Access, and EURASIP Journal on Wireless Communications and Networking. He also served as a track co-chair for IEEE VTC-Spring 2018, EAI GreeNets 2019, ICCC Workshop 2019 and ICCC 2020. He is a co-recipient of the 2018 IEEE ICNC, 2018 CSPS and 2019 IEEE WCSP Best Paper Award.



Octavia A. Dobre (M'05-SM'07-F'20) received the Dipl. Ing. and Ph.D. degrees from Politehnica University of Bucharest (formerly Polytechnic Institute of Bucharest), Romania, in 1991 and 2000, respectively. Between 2002 and 2005, she was with New Jersey Institute of Technology, USA. In 2005, she joined Memorial University, Canada, where she is currently Professor and Research Chair. She was a Visiting Professor with Massachusetts Institute of Technology, USA and Universit de Bretagne Occidentale, France. Her research interests include enabling technologies for beyond 5G, blind signal identification and parameter estimation techniques, as well as optical and underwater communications. She authored and co-authored over 300 refereed papers in these areas.

Dr. Dobre serves as the Editor-in-Chief (EiC) of the IEEE Open Journal of the Communications Society and Editor of the IEEE Communications Surveys and Tutorials and IEEE Vehicular Technology Magazine. She was the EiC of the IEEE Communications Letters, as well as Senior Editor, Editor, and Guest Editor for various prestigious journals and magazines. Dr. Dobre was the General Chair, Technical Program Co-Chair, Tutorial Co-Chair, and Technical Co-Chair of symposia at numerous conferences.

Dr. Dobre was a Royal Society Scholar and a Fulbright Scholar. She obtained Best Paper Awards at various conferences, including IEEE ICC, IEEE Globecom and IEEE WCNC. Dr. Dobre is a Distinguished Lecturer of the IEEE Communications Society and a Fellow of the Engineering Institute of Canada. She is a member-at-large of the Board of Governors of the IEEE Communications Society, has served with the Administrative Committee of the IEEE Instrumentation and Measurement Society, as well as with many other committees in these professional societies.