UAV-aided Secure Transmission in MISOME Wiretap Channels with Imperfect CSI

YANG CHEN, ZHONGPEI ZHANG
National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China
Corresponding author: Zhongpei Zhang (zhangzp@uestc.edu.cn)
This work was supported in part by the NSFC under Grants 61571003, 61671128, 61831004 and 61871070.

ABSTRACT In this paper, we study secure cooperative transmission for the multiple-input-single-output multiple-eavesdropper (MISOME) systems, where a source (Alice) aims to send confidential messages to a legitimate user (Bob) with the aid of an unmanned aerial vehicle (UAV) enabled friendly jammer (Charlie) in the presence of multiple eavesdroppers (Eves). To further guarantee the secrecy performance, AN (artificial noise) beamforming together with cooperative Jamming (CJ) has been utilized in this considered system with only location and statistical channel state information of the Eves. Specifically, taking imperfect channel state information (CSI) between Charlie and Bob into account, we derive the exact closed form expression of the secrecy outage probability (SOP) and develop an efficient scheme to solve the secrecy rate maximization (SRM) problem which has been verified as a convex one under certain SOP. Moreover, we propose an optimal UAV placement strategy to further enhance the secrecy performance. Numerical results are provided to validate that the system security would be seriously degenerated with channel uncertainty. Besides, the proposed scheme is verified to outperform the terrestrial CJ scheme in improving the secrecy rate and secure energy efficiency (EE) performance under perfect CSI or tolerable channel estimation errors. Finally, the effectiveness of the proposed UAV placement strategy in enhancing transmission security and the applicability of the proposed scheme has also been demonstrated.

INDEX TERMS UAV, physical layer security, secrecy output probability, secrecy rate, imperfect channel state information.

I. INTRODUCTION

Emerging as promising solutions to against eavesdropping and guarantee secure transmission, physical layer security techniques have attracted considerable attention recently [1]. Different from the conventional upper-layer cryptographic techniques such as encryption, the basic principle of physical layer security schemes was investigated from an information-theoretic viewpoint [2], and it has been proved that a positive secrecy capacity can be achieved without using secret keys in wiretap channel models if the channel between the transmitter and the intended receiver outperforms the channel between the transmitter and the eavesdropper [3].

It is shown that when multiple antennas are available at the transmitter, wireless communication systems can improve physical layer security significantly for the noticeable properties of achieving spatial degrees of freedom and diversity gains [4], [5]. Because of some hardware limitations such as terminal size and power constraints, cooperative security techniques have become attractive multi-antennas physical layer security strategies to further enhance the secrecy performance, and the cooperative nodes mainly act two roles including cooperative relaying (CR) [6] and cooperative jamming (CJ) [7], [8]. Particularly, in the CJ scheme, rather than improving the capacity of main channel, the friendly jammers degrade the capacity of the wiretap channel by emitting artificial noise to confuse the eavesdropper [8]. In [9], the secrecy rate maximization (SRM) problem for slow fading multiple-input-single-output (MISO) wiretap channels has been discussed. A solution has been developed to solve the SRM problem under secrecy outage probability (SOP) in [10]. Motivated by [9] and [10], the authors in [7] added a cooperative jammer to strengthen the secrecy performance, and exploited an efficient method to achieve the maximum secrecy rate and a higher secure energy efficiency (EE). Sub-
sequently, the work has been extended to systems with multiple eavesdroppers [11]. In [12]–[14], the authors extended the analyses to MISOME wiretap channels. In the work of [12], the authors optimized the design of AN which was commonly restricted to spatially isotropic, and developed a semidefinite program (SDP)-based optimization approach to handle the AN-aided SRM problem. In [13], the worst-case secrecy rate with respect to both the worst-case channel uncertainties as well as the worst-case eavesdropper among multiple eavesdroppers has been maximized under the transmit power constraint and the worst-case energy harvesting constraint. Furthermore, the authors in [14] maximized the achievable secrecy rate region by jointly optimizing the input covariance matrices of the multicast message, confidential message and AN.

During the past decades, intensive efforts have been devoted to investigating unmanned aerial vehicles (UAVs) which are regarded as promising complements to the existing terrestrial wireless communication systems. Thanks to their outstanding benefits such as low cost, high mobility, and controllable deployment, UAVs have been widely used in not only military but also civilian applications like transport, search and rescue [15]. The recent research has extended UAV techniques to wireless communication systems to realize larger coverage, and achieve higher transmission rate [16]–[18]. Thus, UAV-aided systems offer new possibilities and opportunities for security challenge [19]–[26]. The authors in [19] investigated the optimal power allocation problem for secure mobile relaying systems in the presence of a ground eavesdropper. In the work of [20], the authors maximized the probability of non-zero secrecy capacity by optimizing the instantaneous positions of the aerial BS in the three-dimensional (3D) space under airspace constraints. In [21], the secure communications of both UAV-to-ground (U2G) and ground-to-UAV (G2U) links are considered. Jointly optimizing the trajectory and the transmit power of the UAVs as well as the user scheduling, the minimum secrecy rate among the ground users has been maximized in [22]. Reference [23] studied the maximization of the average secrecy rate in a two-UAV scenario where one UAV transmitter sends information to a GN and the other UAV jammer generates artificial noise (AN) to jam a suspicious eavesdropper on the ground. Similarly, in [24], a UAV-aided jamming method has been developed to enhance the secrecy rate in the ground wiretap channel systems. In the work of [25], UAVs with caching are utilized as mobile base stations to generate jamming signal to disrupt the potential eavesdropping. Furthermore, the maximization problem of the minimum worst-case secrecy rate among the users in dual-UAV-enabled secure systems has been studied in [26].

However, a common assumption in the aforementioned AN-aided works consists in that the CSI of the main channel and statistical CSI of the eavesdropper’s channel are known by the transmitter or the friendly jammer. Obviously, it is impossible in practice since the CSI of the main channel is acquired by training, channel estimation, and feedback, which inevitably result in CSI imperfection [27]–[29]. Definitely, the channel uncertainty causes seriously degeneration of secrecy performance. Comparing with conventional ground transmissions, UAV-aided secure transmission will suffer much more secrecy performance loss via the LoS-dominant air-to-ground links between UAVs and ground nodes under channel errors [30], [31]. Hence, it is meaningful to take account of the imperfect CSI in UAV-aided secure networks.

In this paper, motivated by the aforementioned works, we investigate the physical layer security in a UAV-enabled cooperative transmission system which is fit for military or emergency communication scenarios, where a source intends to secretly communicate with a legitimate ground user in the presence of multiple eavesdroppers with channel uncertainty. Unlike [20] and [32], we consider a more practical emergency communication scenario with coexisting multiple eavesdroppers. And to further strengthen secrecy performance, a UAV is employed as the friendly jammer instead of a terrestrial one considered in [11], [32] or an aerial base station considered in [20] to deteriorate the eavesdropper channel. It is worth mentioning that the locations of the eavesdroppers can be detected and tracked by the UAV via using an optical camera or synthetic aperture radar (SAR) equipped on the UAV [30], [33]. Moreover, the channel gains can be obtained by UAV through the locations of the ground nodes [34], thus making the jamming more effective. Besides, in this more practical communication scenario, we take imperfect CSI of the jammer-to-user channel into account, while perfect CSI is assumed in [11]. More importantly, aiming to improve the applicability and effectiveness of the proposed scheme, an optimal UAV placement strategy is derived via geometric properties to find the best location of the UAV jammer. Different from [20], [22] and [24], we consider a more practical air-to-ground channel model with node-height-dependent probability of having LoS link and only statistical CSI of Eves is available. The jamming signals generated by the cooperative UAV-enabled jammer have been properly designed utilizing AN beamforming to disturb the eavesdropper without causing any interference at the intended receiver. In addition, to guarantee reliable secure transmission, an efficient approach is exploited to maximize the secrecy rate under certain SOP in a more practical scenario with channel uncertainty, while perfect CSI and no SOP constraint are considered in [20], [22] and [24].

Our contributions of this paper can be summarized as follows:

- We first reformulate the expression of the SOP and derive an efficient solution to the SRM problem under certain SOP by transforming the objective function into a strictly concave function through strict mathematical proofs. Then, the optimal power allocation factor for AN-aided beamforming can be acquired to maximize the secrecy rate. Finally, a UAV placement strategy is developed for finding the best location of the UAV jammer to further improve the secrecy performance.
- We examine the impact of specific parameters including
the number of Eves and the channel estimation error on the secrecy performance of the considered system, and the influence on reducing security is shown to be conspicuous.

- Compared with the terrestrial CJ scheme, numerical results indicate that when the channel uncertainty of the communication system is tolerable, the proposed CJ scheme is shown to be more effective on secure transmission and is adapted to green communication scenarios for achieving higher secrecy rate and secure EE. In addition, the optimal UAV placement strategy can be exploited to further enhance the secrecy performance and the applicability of the proposed scheme.

The rest of this paper is organized as follows. The system model and problem formulation is described in Section II. The proposed scheme is presented in Section III. The optimal UAV placement strategy is derived in Section IV. Numerical results are provided in Section V. At last, we conclude the paper in Section VI.

Notation: Boldface upper and lower cases denote matrices and vectors, respectively. Subscripts \((\cdot)^H\) and \([\cdot]^T\) stand for the the conjugate transpose and max-function \(\max(\cdot, 0)\). \(I_N\) represents \(N \times N\) identity matrix. \(\text{null}(X)\) is the null space of \(X\). \(| \cdot |\) denotes the 2D Euclidean distance, and \(|\cdot|^2\) denotes Euclidean norm. \(\Pr(\cdot)\) is the probability measure. \(\mathbb{C}^n\) denotes the n-dimensional complex space and circularly symmetric complex Gaussian random vector submits to \(\mathcal{CN}(\mu, \Lambda)\), with mean \(\mu\) and covariance matrix \(\Lambda\). Exponential distribution with parameter \(\lambda\) and Gamma distribution with shape parameter \(\alpha\) and rate parameter \(\beta\) is denoted as \(\text{Exp}(\lambda)\) and \(\Gamma(\alpha, \beta)\) respectively.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. SYSTEM MODEL

As shown in Fig. 1, we consider a secure transmission network, where the source (Alice) intends to send confidential information to a single-antenna legitimate user (Bob) and is overheard by randomly located non-colluding eavesdroppers (Eves). In order to enhance the secrecy performance, a UAV (Charlie) is deployed as a friendly jammer hovering above Bob at a constant altitude \(h\) (e.g., the minimum required altitude to circumvent ground obstacles) to emit artificial noise to deteriorate the Eves’ channels. We assume Alice and Charlie are equipped with \(N_a\) and \(N_c\) antennas respectively and each Eve has a single antenna. In addition, we assume Alice, Bob and Eves are all ground nodes deploying at fixed locations which are known as a priori information. The set of Eves is defined as \(\mathcal{M} \triangleq \{1, ..., M\}\).

Without loss of generality, in this considered system we express locations in the three-dimensional Cartesian coordinate system, where Alice, Bob and Charlie are located at \((0, 0, 0)\), \((x_b, y_b, 0)\) and \((x_e, y_e, h)\) respectively. For \(m \in \mathcal{M} \triangleq \{1, ..., M\}\), the location of Eve \(m\) is denoted by \((x_m, y_m, 0)\). The channels from Alice to Bob and the \(m\)-th Eve are denoted by \(h_{ab} \in \mathbb{C}^{1 \times N_a}\) and \(h_{ce,m} \in \mathbb{C}^{1 \times N_a}\) respectively, and are modeled as quasi-static independent and identically distributed (i.i.d) Rayleigh fading channels. We also denote the channels from Charlie to Bob and the \(m\)-th Eve by \(h_{cb} \in \mathbb{C}^{N_c \times N_a}\) and \(h_{ce,m} \in \mathbb{C}^{N_c \times N_a}\) respectively. In this paper, we consider \(h_{cb}, h_{ce,m}\) to be air-to-ground channels which are modeled in [34] and the path loss exponent for Line-of-Sight (LoS) and non-Line-of-sight (NLoS) channels between the UAV and the ground nodes can be expressed as

\[
\eta_i = \begin{cases} 
\eta_{\text{LoS}}, & \text{with probability } P_{\text{LoS}}, \\
\eta_{\text{NLoS}}, & \text{with probability } P_{\text{NLoS}},
\end{cases}
\]

where \(\eta_{\text{LoS}} > \eta_{\text{NLoS}}\). The probability of LoS link is determined by the distance between the UAV and the ground nodes, elevation and is effected by environment, which can be given by [34]

\[
P_{\text{LoS}} = \frac{1}{1 + \psi \exp(-\omega(\theta - \psi))},
\]

where \(\psi\) and \(\omega\) are constant values which depend on the environment, \(\theta = \frac{180}{\pi} \arctan \left(\frac{h}{x_b - x_m}\right)\) describes the elevation angle, and \(r = \sqrt{(x_b - x_m)^2 + (y_b - y_m)^2}\). Based on (2) we have \(P_{\text{NLoS}} = 1 - P_{\text{LoS}}\). The probability of being LoS links for \(h_{cb}, h_{ce,m}\) is denoted as \(P_{\text{LoS}}^{cb}\) and \(P_{\text{LoS}}^{ce,m}\) respectively. In addition, for LoS links we consider the channels experience Rician fading, and the Rician factor of the Charlie-to-Bob channel and the Charlie-to-Eve channel is denoted as \(K_{cb}\) and \(K_{ce}\) respectively. Likewise, we consider Rayleigh fading for those NLoS links.

For secure transmission from Alice to Bob, Alice acts as a secure control center and utilizes AN-aided beamforming scheme to emit confidential information along with AN. We denote \(t \in \mathbb{C}^{N_a \times 1}\) and \(t_c \in \mathbb{C}^{N_c \times 1}\) as the signals transmitted by Alice and Charlie respectively. Revisiting [9], \(t\) can be constructed as

\[
t = \sqrt{P_a \phi} w_s x_s + \sqrt{\frac{P_a (1 - \phi)}{N_a - 1}} w_{AN} x_{AN},
\]

FIGURE 1. Secure cooperative transmission network with a UAV-enabled jammer.
where $P_a$ denotes the total transmit power of Alice. The power allocation factor $\phi \in [0, 1]$ denotes the fraction of the total power Alice allocate to transmit information-bearing signals. The information bearing signal is denoted as $x_s \sim CN(0, 1)$, and is independent of AN bearing signal $x_{AN}$ with $E[x_{AN}x_{AN}^H] = I_{N_a - 1}$. Beamforming vector is $w_s = \frac{h_{ab}}{\|h_{ab}\|}$, and the AN beamforming matrix $W_{AN} \in CN_{N_a \times (N_a - 1)}$ is a matrix which is an orthonormal basis for null($h_{ab}$).

In this network, Charlie obtains the estimated $h_{cb}$ through the pilot signals transmitted by Bob, which are usually not perfectly accurate. Referring to the commonly used Gaussian uncertainty channel model in TDD system [35], [36], the exact channel between Charlie and Bob can be modeled as

$$h_{cb} = h_{cb} + e_{cb},$$  \hspace{1cm} (4)

where $e_{cb} \sim CN(0, \sigma^2_{cb} I_{N_c})$ represents the channel estimation error vector, and $h_{cb}$ is known to all nodes.

Since interference caused by Charlie will lead to great secrecy performance degeneration, $t_c$ should be properly designed. In order to eliminate the additional interference at Bob and jam Eve at the same time, i.e., $h_{cb} t_c = 0$, $t_c$ can be designed as

$$t_c = \sqrt{\frac{P_c}{{N_c} - 1}} V_s,$$  \hspace{1cm} (5)

where $P_c$ denotes the transmit power constraint at Charlie, $V_s \in CN_{N_s \times (N_s - 1)}$ is an orthonormal basis for null($h_{cb}$), and Gaussian jamming signal is denoted by $s \sim CN(0, I_{N_s - 1})$.

From (3), (4) and (5), the signal received at Bob and the $m$-th Eve can be described as

$$y_b = \sqrt{P_a} \phi d_{ab}^{-\eta_{ab}} h_{ab} w_s x_s + \sqrt{P_c} d_{cb}^{-\eta_{cb}} h_{cb} V_s + n_b$$  \hspace{1cm} (6)

$$y_{c,m} = \sqrt{P_a} \phi d_{ae,m}^{-\eta_{ae,m}} h_{ae,m} w_s x_s$$
$$+ \frac{P_c (1 - \phi) d_{ce,m}^{-\eta_{ce,m}}}{N_a - 1} h_{ce,m} W_{AN} x_{AN}$$  \hspace{1cm} (7)

where $d_{ab} = \sqrt{x_b^2 + y_b^2}$, $d_{cb} = h_c$, $d_{ae,m} = \sqrt{x_{ae,m}^2 + y_{ae,m}^2}$, $d_{ce,m} = \sqrt{(x_b - x_{ae,m})^2 + (y_b - y_{ae,m})^2 + h^2}$ each represents the distances between Alice and Bob, Charlie and Bob, Alice and the $m$-th Eve, Charlie and the $m$-th Eve respectively. $\eta_{ab}$, $\eta_{cb}$, $\eta_{ae,m}$, and $\eta_{ce,m}$ each denotes the path loss exponent for each corresponding links. Given that $n_b, n_{e,m} \in CN(0, 1)$ are mutually independent additive white Gaussian noise at Bob and the $m$-th Eve respectively.

However, the accurate expression of secrecy capacity under imperfect receiver CSI is difficult to be obtained. Notice that $n_b^2$ includes the channel estimation error and thermal noise, an efficient approach was presented in [37] which treats $n_b^2$ as the worst-case Gaussian noise to compute a lower bound of the secrecy capacity. By doing so, and combing (1), (7) and (8), the signal-to-interference-plus-noise ratio (SINR) at Bob and the $m$-th Eve can be written as

$$\zeta = \frac{P_a \phi d_{ab}^{-\eta_{ab}} \| h_{ab} \|^2}{1 + P_c d_{cb}^{-\eta_{cb}} \sigma_b^2} + (1 - P_a \phi) \frac{P_a \phi d_{ab}^{-\eta_{ab}} \| h_{ab} \|^2}{1 + P_c d_{cb}^{-\eta_{cb}} \sigma_b^2},$$  \hspace{1cm} (9)

$$\zeta_{c,m} = \frac{P_a \phi d_{ae,m}^{-\eta_{ae,m}} \| h_{ae,m} \|^2}{1 + P_c d_{ce,m}^{-\eta_{ce,m}} \sigma_{c,m}^2} \left(1 + \frac{P_a (1 - \phi) d_{ae,m}^{-\eta_{ae,m}}}{N_a - 1} \| h_{ae,m} W_{AN} \|^2 \right) \cdot \frac{1}{N_c - 1} \| h_{ce,m} V_s \|^2.$$  \hspace{1cm} (10)

The capacities of the main channel and the $m$-th Eve’s channel are defined as $C_b = \log_2 (1 + \zeta_b)$ and $C_{c,m} = \log_2 (1 + \zeta_{c,m})$ respectively [38]. In this wiretap scenario, we consider the Eves are non-colluding, so the maximal eavesdropped information is determined by the maximal SNR among all the Eves, thus $C_e = \log_2 (1 + \max_{m \in M} \zeta_{c,m})$ [39]. Therefore, the achievable secrecy capacity of the network $C_s$ can be written as [38]

$$C_s = \begin{cases} C_b - C_e, & \text{if } \zeta_b > \max_{m \in M} \zeta_{c,m} \\ 0, & \text{if } \zeta_b \leq \max_{m \in M} \zeta_{c,m} \end{cases}.$$  \hspace{1cm} (11)

In this considered wiretap channel network, utilizing Wyner’s wiretap code [40], the perfect secrecy performance can be obtained if $C_s \geq R_s$, where we denote $R_s$ as a target secrecy transmission rate. Else, the information transmitted by Alice to Bob will be leaked to Eve. The confidential information will be encoded before transmission, so in this scheme we define $R_b = \log_2 (1 + \zeta_b)$ as the rate of the codeword. $R_b = R_c - R_s$ represents the redundant rate that can be utilized for anti-eavesdropping. According to [9], the secrecy outage probability (SOP) can be written as

$$P_{out}(R_s, \phi) = \text{Pr}(R_s > C_s) = \text{Pr}(C_e > R_c).$$  \hspace{1cm} (12)

$$B. \text{PROBLEM FORMULATION}$$

First, the maximum allowable SOP can be defined as $\varepsilon \in (0, 1)$. Thus the SRM problem of this network can be considered as an optimization problem under certain SOP given by
max $\phi$ $[R_s]^+$;

s.t. $P_{out}(R_s, \phi) \leq \varepsilon$; \hspace{1cm} (14)

\[ 0 \leq \phi \leq 1. \]

Then, according to [9], $\varepsilon = \Pr(C_e > R_s) = \Pr(\max_{m \in M} \zeta_{ce,m} > 2C_e - R_s - 1)$. To simplify our analysis, we define $\delta = 2C_e - R_s - 1$. Consequently, the equal expressions of (14) can be described as follows

$$\begin{align*}
\max_{\phi} R_s &= \log_2 \left( 1 + \frac{\zeta \phi}{1 + \delta} \right); \\
\text{s.t.} \quad &\varepsilon = \Pr(\max_{m \in M} \zeta_{ce,m} > \delta); \\
&0 \leq \phi \leq 1,
\end{align*}$$

where $\zeta = P_a d_{ab}^{-\eta_{ab}} \| h_{ab} \|^2$ describes the maximum achievable SINR at Bob.

### III. PROPOSED SOLUTION FOR SRM PROBLEM UNDER CERTAIN SOP CONSTRAINT

It is obviously that the SRM problem of (15) is difficult to solve directly owing to the constraint of SOP. In this section, we first focus on a single eavesdropper scenario and reformulate the expression of SOP by defining some new variables and doing some transformations, then we further extend our analysis to multiple eavesdroppers scenario. Finally, we develop an efficient method to obtain the optimal power allocation factor for maximizing the secrecy rate under certain SOP constraint.

### A. REFORMULATE THE EXPRESSION OF SOP

In order to make the SOP in (15) more explicit, we denote $\varepsilon_m = \Pr(\zeta_{ce,m} > \delta)$, $m \in M$, and the equation (10) can be rewritten as follow

$$\begin{align*}
\zeta_{ce,m} &= \frac{\zeta_{ae,m} \phi}{1 + \frac{(1 - \phi)}{N_a - 1} \zeta_{ae,m}} \| h_{ae,m} \| w_s \|^2 \\
&+ \frac{1}{N_c - 1} \zeta_{ce,m} \| h_{ce,m} \| V \|^2,
\end{align*}$$

where $\zeta_{ae,m} = P_a d_{ae,m}^{-\eta_{ae,m}}$, $\zeta_{ce,m} = P_a d_{ce,m}^{-\eta_{ce,m}}$. To further simplify our analysis, we define new variables as follows

$$\begin{align*}
T_{1,m} &= \zeta_{ae,m} \phi \| h_{ae,m} \| w_s \|^2, \\
T_{2,m} &= \frac{(1 - \phi)}{N_a - 1} \| h_{ae,m} \| W_{AN} \|^2, \\
T_{3,m} &= \frac{1}{N_c - 1} \zeta_{ce,m} \| h_{ce,m} \| V \|^2, \\
U_m &= T_{2,m} + T_{3,m}.
\end{align*}$$

According to [10], [11], with the aid of stochastic theory knowledge, since the entries of $h_{ae,m}$ follow independent $\mathcal{CN}(0, 1)$, the square of each entry’s modulus follows exponential distribution with mean $1$. Therefore, we have $\| h_{ae,m} \| w_s \|^2 \sim \Gamma(1, 1)$ and $\| h_{ae,m} \| W_{AN} \|^2 \sim \Gamma(N_a - 1, 1)$. Finally, $T_{1,m} \sim \exp(\kappa_{1,m})$, $T_{2,m} \sim \Gamma(N_a - 1, \kappa_{2,m})$, where $\kappa_{1,m} = \frac{d_{ae,m}^{-\eta_{ae,m}}}{P_a}$ and $\kappa_{2,m} = \frac{(N_a - 1)d_{ae,m}^{-\eta_{ae,m}}}{P_a}$. can be easily verified. Besides, $\eta_{ae,m} = \eta_{NLoS}$.

As we have discussed in the previous section that the air-to-ground channels between the UAV and the ground nodes can be modeled as LoS links with probability $P_{LoS}$ and NLoS links with probability $1 - P_{LoS}$ respectively, thus we have

$$\begin{align*}
T_{3,m} &= \begin{cases} 
\frac{T_{1,m}^{(1)}}{T_{3,m}}, & \text{with probability } P_{c}^{\text{LoS}}; \\
\frac{T_{2,m}^{(2)}}{T_{3,m}}, & \text{with probability } 1 - P_{c}^{\text{LoS}}.
\end{cases}
\end{align*}$$

and the equation (20) can be re-expressed as

$$U_m = \begin{cases} 
U_{m}^{(1)} = T_{2,m} + T_{3,m}^{(1)}, & \text{with probability } P_{c}^{\text{LoS}}; \\
U_{m}^{(2)} = T_{2,m} + T_{3,m}^{(2)}, & \text{with probability } 1 - P_{c}^{\text{LoS}}.
\end{cases}$$

The SOP constraint in (15) can be rewritten as

$$\varepsilon_m = \Pr(\zeta_{ce,m} > \delta) = \Pr(\{T_{1,m} > \delta + U_m\}) = P_{c}^{\text{LoS}} \varepsilon_m + (1 - P_{c}^{\text{LoS}}) \varepsilon_{NLoS},$$

where $\varepsilon_{NLoS} = \Pr(\{T_{1,m} > \delta + U_m^{(2)}\})$ and $\varepsilon_{NLoS} = \Pr(\{T_{1,m} > \delta + U_m^{(2)}\})$ describe the expressions of the SOP for the cases of LoS and NLoS links respectively, then the statistics of $\varepsilon_m$ can be characterized with following results.

1) $\varepsilon_{NLoS}$ For LoS Links

Given the assumption that LOS links are considered experiencing Rician fading, we go one step further to regard Rician fading as a special case of Nakagami fading [41]. So in this case, the cumulative distribution function (CDF) of $T_{3,m}^{(1)}$ can be obtained as

$$F_{T^{(1)}_{3,m}}(z) = \frac{\gamma((N_c - 1)\eta_{ce}, \frac{(\eta_{ce} - 1)\eta_{ae,m}}{P_a})}{\Gamma(m_{ce})},$$

where, $m_{ce} = \frac{(\eta_{ce} + 1)^2}{2\eta_{ce} + 1}$, $\eta_{ce,m} = \eta_{LoS}$. $\gamma(\cdot)$ is the lower incomplete gamma function, defined as [42, Eq. 8.350]

$$\gamma(\mu, \nu) = \int_{0}^{\nu} \exp(-t)t^{\nu-1}dt,$$

and $\Gamma(\cdot)$ is the Gamma function, defined as [42, Eq. 8.310]

$$\Gamma(z) = \int_{0}^{\infty} \exp(-t)t^{z-1}dt,$$

From (25), we have

$$T_{3,m}^{(1)} \sim \Gamma\left(m_{ce}(N_c - 1), \kappa_{3,m}^{(1)}\right),$$

VOLUME 4, 2016
where \( \kappa_{3,m}^{(1)} = \frac{m_{ce}(N_c-1)}{P_c} \). Thus a closed form expression for \( \varepsilon_m^{\text{LoS}} \) can be given by [7]

\[
\varepsilon_m^{\text{LoS}} = \Pr \left\{ T_{1,m} > \delta + \delta U_m^{(1)} \right\} = \frac{1}{e^{\kappa_{1,m}\delta}} \left( \frac{\kappa_{2,m}}{\kappa_{2,m} + \kappa_{1,m}\delta} \right)^{\alpha_1} \left( \frac{\kappa_{3,m}^{(1)}}{\kappa_{3,m}^{(1)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(1)}}, \tag{29}\]

where \( \alpha_1 = N_a - 1, \alpha_2^{(1)} = m_{ce}(N_c - 1) \).

2) \( \varepsilon_m^{\text{NLoS}} \) For NLoS Links

The CDF of \( T_{3,m}^{(2)} \) can be obtained similarly with \( T_{1,m} \) and \( T_{2,m} \), as

\[
T_{3,m}^{(2)} \sim G(N_c - 1, \kappa_{3,m}^{(2)}), \tag{30}\]

where \( \kappa_{3,m}^{(2)} = \frac{(N_c-1)d_{ae,m}^2}{P_c \eta_{ce,m}}, \eta_{ce,m} = \eta_{NLoS}. \) Hence, \( \varepsilon_m^{\text{NLoS}} \) can be re-expressed as [7]

\[
\varepsilon_m^{\text{NLoS}} = \Pr \left\{ T_{1,m} > \delta + \delta U_m^{(2)} \right\} = \frac{1}{e^{\kappa_{1,m}\delta}} \left( \frac{\kappa_{2,m}}{\kappa_{2,m} + \kappa_{1,m}\delta} \right)^{\alpha_1} \left( \frac{\kappa_{3,m}^{(2)}}{\kappa_{3,m}^{(2)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(2)}}, \tag{31}\]

where \( \alpha_2^{(2)} = N_c - 1 \).

Substituting (29) and (31) into (24), finally, a closed form expression for \( \varepsilon_m \) can be described as

\[
\varepsilon_m = \frac{P_{ce,m}}{e^{\kappa_{1,m}\delta}} \left( \frac{\kappa_{2,m}}{\kappa_{2,m} + \kappa_{1,m}\delta} \right)^{\alpha_1} \left( \frac{\kappa_{3,m}^{(1)}}{\kappa_{3,m}^{(1)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(1)}} + \left( 1 - \frac{P_{ce,m}}{e^{\kappa_{1,m}\delta}} \right) \left( \frac{\kappa_{2,m}}{\kappa_{2,m} + \kappa_{1,m}\delta} \right)^{\alpha_1} \left( \frac{\kappa_{3,m}^{(2)}}{\kappa_{3,m}^{(2)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(2)}} \tag{32}\]

For the non-colluding \( M \) Eves, based on [43], the SINR at each Eve is independent of each other due to the fact that the functions of independent random variables are independent. Thus, the SOP in (15) can be given by

\[
\varepsilon = 1 - \Pr \left( \max_{m \in \mathcal{M}} \zeta_{m, \leq \delta} \right) = 1 - \left( \Pr \left( \zeta_{m, \leq \delta} \right) \right)^M = 1 - (1 - \varepsilon_m)^M \tag{33}\]

From (32) and (33), a closed form expression of SOP in (15) can be calculated as

\[
\varepsilon = 1 - \left\{ 1 - \left[ \frac{P_{ce,m}^{\text{LoS}}}{e^{\kappa_{1,m}\delta}} \left( \frac{\kappa_{2,m}}{\kappa_{2,m} + \kappa_{1,m}\delta} \right)^{\alpha_1} \left( \frac{\kappa_{3,m}^{(1)}}{\kappa_{3,m}^{(1)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(1)}} \right]^M \right\} \tag{34}\]

\section*{B. OPTIMIZE THE POWER ALLOCATION FACTOR \( \phi \)}

Notice from (15) that, (34) holds with equality at \( \max_{m \in \mathcal{M}} \zeta_{m, \leq \delta} \), and it can be observed that \( \delta \) is an implicit function of \( \phi \), here we define \( \rho(\phi) = \frac{\delta}{\phi} \). For a given \( \varepsilon \), after some transformation, (34) can be simplified and rewritten as

\[
\ln \left( \frac{1}{1 - \varepsilon} \right) = \frac{d_{\text{LoS}}^{\text{NLoS}}}{P_c} \rho(\phi) + \alpha_1 \ln \left( \frac{1 + \frac{1 - \phi}{N_a} \rho(\phi)}{1 + \frac{\rho(\phi)}{N_c - 1}} \right) + \alpha_2^{(2)} \ln \left( 1 + \frac{P_c}{P_a} \left( \frac{d_{ae}}{d_{ce}} \right)^{\eta_{NLoS}} \frac{1}{N_c - 1} \rho(\phi) \right) + \ln G, \tag{35}\]

where \( G = \frac{P_{ce}^{\text{LoS}}}{e^{\kappa_{1,m}\delta}} \left( \frac{\kappa_{3,m}^{(1)}}{\kappa_{3,m}^{(1)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(1)}} / \left( \frac{\kappa_{3,m}^{(2)}}{\kappa_{3,m}^{(2)} + \kappa_{1,m}\delta} \right)^{\alpha_2^{(2)}} + 1 - P_{ce}^{\text{LoS}} \).

and \( h_{ae}, h_{ce}, d_{ae}, d_{ce}, \kappa_1, \kappa_3, \kappa_3^{(1)}, \kappa_3^{(2)} \) and \( P_{ce}^{\text{LoS}} \) each represents the corresponding parameters that belong to the strongest Eve that gains \( \max_{m \in \mathcal{M}} \zeta_{m, \leq \delta} \) respectively. Since \( G > 1 \), we have \( \ln G > 0 \), so for \( \phi \in [0, 1] \), \( \rho(\phi) > 0 \) can be easily verified. For convenience, we assume the network configuration with \( N_a = 4 \) and \( N_c = 2 \), then we have \( \alpha_1 = 3, \alpha_2^{(1)} = m_{ce}, \alpha_2^{(2)} = 1 \), and it is definite that our analysis here can be extended to more general cases. In order to develop a useful method to solve the SRM problem in (15), following results are utilized to facilitate our analysis.

\begin{lemma} \( \rho(\phi) \) is a monotonically increasing function with respect to \( \phi \) when \( \phi \in [0, 1] \).
\end{lemma}

\begin{proof} please refer to Appendix A. \end{proof}

\begin{lemma} \( \rho'(\phi) \) is a monotonically increasing function with respect to \( \phi \) when \( \phi \in [0, 1] \).
\end{lemma}

\begin{proof} please refer to Appendix B. \end{proof}

The above results about \( \rho(\phi) \) can be utilized to facilitate our analysis for the objective function in (15), and we have following propositions.

\begin{proposition} \( R_s \) is a strictly concave function of \( \phi \).
\end{proposition}

\begin{proof} From (15), it can be deduced that \( R_s(\phi) \) is given by

\[
R_s(\phi) = \frac{1}{\ln 2} \left[ \frac{\zeta}{1 + \zeta \phi} - \frac{\rho(\phi) + \phi \rho'(\phi)}{1 + \phi \rho(\phi)} \right] = \frac{\zeta - \rho(\phi)}{(1 + \zeta \phi)(1 + \phi \rho(\phi)) \ln 2 - \left( 1 + \phi \rho(\phi) \right) \ln 2}. \tag{36}\]

According to Lemma 1 and Lemma 2, the first term on the right-hand side of (38) is shown to be a strictly decreasing function of \( \phi \), and increasing function of \( \phi \) for the second one, respectively. Consequently, \( R'_s(\phi) < 0 \) can be obtained. Based on convex optimization theory [44] we derive Proposition 1.

VOLUME 4, 2016
**Proposition 2.** The optimal power allocation factor $\phi^*$ can be characterized as

$$
\phi^* = \begin{cases} 
1, & \text{if } R_s'(1) \geq 0; \\
\phi_{\text{opt}}, & \text{if } R_s'(1) < 0 \& R_s'(0) > 0; \\
0, & \text{if } R_s'(0) \leq 0.
\end{cases}
$$

(38)

where $\phi_{\text{opt}} \in [0, 1]$ is the unique optimal solution that satisfying $R_s'(\phi_{\text{opt}}) = 0$, and we describe the corresponding maximum secrecy rate as $R_s^*(\phi)$.

**Proof.** Utilizing above results, an efficient numerical method to solve (15) can be exploited, and we discuss the details in following three different cases.

1) Case 1: $R_s'(1) \geq 0$.

From Proposition 1, we can conclude that $R_s'(\phi) > R_s'(1) \geq 0$ for $\phi \in [0, 1]$, and the secrecy rate $R_s(\phi)$ is shown to be a monotonically increasing function of $\phi$. Then by (37), $\zeta - \rho(1) \geq (1 + \zeta)\rho'(1)$ can be obtained from the condition $R_s'(1) \geq 0$, and since $(1 + \zeta)\rho'(1) > 0$, we derive that $\zeta > \rho(1)$. As a result, $\phi^* = 1$ is the optimal solution to problem (15), a positive secrecy rate can be guaranteed and the corresponding maximum secrecy rate can be expressed as $R_s'(1)$. Based on (3), in this case it is wise for Alice to allocate full power to generate information-bearing signals.

2) Case 2: $R_s'(1) < 0 \& R_s'(0) > 0$.

By Proposition 1, $R_s(\phi)$ is shown to be a function that first increase and then decrease with $\phi$. Consequently, based on the characteristics of the concave function, there must be a unique $\phi_{\text{opt}} \in (0, 1)$ that satisfying $R_s'(\phi_{\text{opt}}) = 0$, and therefore, $R_s^*(\phi) = R_s(\phi_{\text{opt}})$. Moreover, a positive secrecy rate can be guaranteed since $R_s(\phi_{\text{opt}}) > R_s(0) = 0$.

3) Case 3: $R_s'(0) \leq 0$.

$\zeta < \rho(0)$ can be deducted according to (36). Similarly to Case 1, we have $R_s'(\phi) < R_s'(0) \leq 0$ for $\phi \in [0, 1]$ according to Proposition 1, so $R_s(\phi)$ is a monotonically decreasing function of $\phi$. Since $R_s(0) < 0$, we cannot achieve a positive secrecy rate. In this case, it is optimal for Alice to stop secure transmission, which leads to $\phi^* = 0$ and $R_s^* = 0$.

This completes the proof of Proposition 2.

From above conclusion, we summarize the details of the overall algorithm in Algorithm 1.

**Algorithm 1 Solution to the SRM problem in (15).**

**Input:** $\varepsilon, P_a, P_c, P_{\text{LoS}}, P_{\text{NLoS}}, \eta_{\text{LoS}}, \eta_{\text{NLoS}}, d_{ab}, d_{ae}, d_{eb}, d_{ce}, N_a, N_c, K_{ce}, h_{ab}, h_{ae}, h_{eb}, h_{ce}$;

**Output:** $R_s^*(\phi) = R_s(\phi^*)$;

1. calculate $R_s'(0)$ and $R_s'(1)$ according to (38);
2. if $R_s'(1) \geq 0$, according to (38) in Proposition 2 $\phi^* = 1$;
3. else if $R_s'(0) \leq 0$, according to (38) in Proposition 2 $\phi^* = 0$;
4. else obtain $\phi^*$ by numerical root-finding of $R_s'(\phi) = 0$;
5. end if
6. return $\phi^*$

Partially different from the system model depicted in Fig. 1, Charlie is still deployed at a constant altitude $h$ as a friendly jammer to strengthen physical layer security but subjects to some movement airspace restriction [20]. Specifically, the reduced UAV-to-ground nodes distance not only decreases the signal attenuation but also increases the probability of the LoS link between them [23]. And referring to [18], we would better reduce the movement of the UAV jammer from the previously fixed point that over Bob as much as possible to prolong the lifetime of the UAV. Hence, aiming to guarantee a long period of secure transmission and achieve higher secure EE, we consider a circular horizontal airspace restriction for the UAV jammer. Since the locations of the ground nodes can be obtained by the UAV via using an optical camera or synthetic aperture radar (SAR) equipped on the UAV [30], [33]. Charlie can degrade the channels of the eavesdroppers by flying closer to them from the previously fixed point that over Bob, and the coordinate of Charlie is denoted as $(x_c, y_c, h)$. Thus, recall (14), the SRM problem under certain SOP can be reformulated by

$$
\max_{\phi, x_c, y_c} \frac{|R_s|_+}{s.t. P_{\text{out}}(R_s, \phi) \leq \varepsilon; \quad 0 \leq \phi \leq 1; \quad (x_c - x_b)^2 + (y_c - y_b)^2 \leq L^2},
$$

(39)

where the constraint $(x_c - x_b)^2 + (y_c - y_b)^2 \leq L^2$ is a circular horizontal airspace, and $L$ is the radius. The coordinate of the origin of the plane is $(x_b, y_b, h)$ [20].

**Lemma 3.** The UAV jammer should be deployed as closely as possible to the Eve that gains $\max_{\gamma, m \in M} \gamma_{e,m}$ (determined based on the case when the UAV jammer hovers over Bob).

**Proof.** As discussed in Section II, the maximal eavesdropped information is determined by the maximal SNR among all the Eves, hence $C_e = \log_2(1 + \max_{\gamma, m \in M} \gamma_{e,m})$ [39]. From (11), $C_s = |\log_2(1 + \rho_0) - \log_2(1 + \max_{\gamma, m \in M} \gamma_{e,m})|$. Recall (10), for fixed $P_a, P_c$ and $d_{ae}$, it can be easily verified that $\gamma_{e,m}$ is a strictly decreasing function of $d_{ce}$. Thus, in a multiple eavesdroppers scenario, in order to address the

---

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2929844, IEEE Access
SRM problem in (39), the UAV jammer should be deployed as closely as possible to the Eve that gains $\max_{m \in M} \zeta_{C,m}$ (determined based on the case when the UAV jammer hovers over Bob) [45]. Consequently, Lemma 3 is established.

**Lemma 4.** The UAV jammer should be deployed as far away from the legitimate user as possible.

**Proof.** From (9) and (11), the UAV jammer has an effect on deteriorating $\zeta_b$ due to the channel estimation error when compared with perfect CSI scenario, and it is easy to verify that for fixed $P_a$, $P_e$, $d_{ab}$ and $\sigma_b^2$, $\zeta_b$ is a strictly increasing function with respect to $d_{db}$. In addition, it is worth noting that the location of the UAV jammer does not affect $\sigma_b^2$ and $R_e$ under perfect CSI. As a result, after recalling that $C_s = [\log_2(1 + \zeta_b) - \log_2(1 + \max_{m \in M} \zeta_{C,m})]^+$, it can be easily deduced that the UAV jammer should be placed as far away from the legitimate user as possible. Thus, we have Lemma 4.

According to Lemma 3 and 4, for a constant altitude $h$, the placement optimization problem can be solved by utilizing the geometric properties of the considered systems to derive the optimal horizontal coordinate of the UAV jammer. As illustrated in Fig. 2, for simplicity, we focus on the strongest Eve that gains $\max_{m \in M} \zeta_{C,m}$ and the location of it is denoted as $(x_{m,max}, y_{m,max}, 0)$. In Fig. 2, the position of Bob, Charlie and the strongest Eve are denoted as point $B$, $C$ and $E$ respectively, and the projection point of Charlie on the horizontal plane is denoted as $C'$. Besides, the optimal position of Charlie is described as point $C^*$ with coordinate $(x^*, y^*, h)$ and the corresponding projection point on the horizontal plane is denoted as $C^{*'} (x^*, y^*, 0)$, $d_{AB} = |AB| = \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}$ denotes the horizontal distance between points $A$ and $B$. Generally, in UAV-enabled communication, UAVs are of limited onboard battery, and the total energy consumption mainly comes from propulsion energy required to maintain UAVs airborne and support their mobility [46]. Hence, in order to prolong the lifetime of the UAV jammer for guaranteeing secure transmission, we assume $L \leq d_{BE}$ in this considered systems [47]. And it is worth to note that this assumption has not been considered in the work of [20].

To get the optimal horizontal position of Charlie, we have the following proposition.

**Proposition 3.** The optimal horizontal position of the UAV jammer $(x^*, y^*)$ lies on the intersection point (the one between point $B$ and $E$) of the circle $(x_c - x_b)^2 + (y_c - y_b)^2 = L^2$ and the straight line $\frac{y - y_{m,max}}{y_{m,max} - y_b} = \frac{x - x_{m,max}}{x_{m,max} - x_b}$ when $L < d_{BE}$; otherwise, $(x^*, y^*) = (x_{m,max}, y_{m,max})$ when $L = d_{BE}$.

**Proof.** From Fig. 2, utilizing Lemma 3 and 4, our analysis can be facilitated in the following two different cases.

1) **Case 1:** $L < d_{BE}$.

Firstly, we set $C^{*'} (x^*, y^*)$ as the interaction point (the one between point $B$ and $E$) of the circle $(x_c - x_b)^2 + (y_c - y_b)^2 = L^2$ and the straight line $\frac{y - y_{m,max}}{y_{m,max} - y_b} = \frac{x - x_{m,max}}{x_{m,max} - x_b}$. Then we assume $C'$ $(x'_c, y'_c)$ is an arbitrary feasible point satisfying the condition $(x_c - x_b)^2 + (y_c - y_b)^2 \leq L^2$, except for $C^{*'}$. It is obviously from Lemma 3 that $C'$ should be placed on the circle. Thus we have

$$ (x'_c - x_b)^2 + (y'_c - y_b)^2 = L^2, \quad (40) $$

and it can be easily deduced from Fig. 2 that

$$ |BC'| + |C'E| > |BE|. \quad (41) $$

Based on the geometric properties of the considered settings, we have

$$ |BC'| = |BC^{*'}|, \quad |BC'| + |C'E| > |BC^{*'}| + C^{*'}E, \quad (42) $$

$$ C^{*'}E < |C'E|, $$

hence point $C^{*'}$ is better than other points for satisfying Lemma 3 and 4 simultaneously.

2) **Case 2:** $L = d_{BE}$.

In this case, we assume the coordinate of $C^{*'} (x^*, y^*)$ is $(x_{m,max}, y_{m,max})$, hence we have

$$ (x_c - x_b)^2 + (y_c - y_b)^2 = L^2, \quad |C^{*'}E| = 0. \quad (43) $$

Consequently, Lemma 3 and Lemma 4 can be satisfied at the same time.

This completes the proof of Proposition 3.

**V. NUMERICAL RESULTS**

In this section, numerical results are presented to validate the secrecy performance of the proposed scheme, as compared to the terrestrial CJ scheme presented in [11] and more insights on the effectiveness of proposed optimal placement strategy are provided. To conduct simulations, Alice, Bob
are assumed as ground nodes with coordinates (0,0,0) m, (10,10,0) m respectively. The $M$ Eves are considered randomly and uniformly distributed within a Two-Dimensional (2D) area of $[-100, 100]^2 m \times [-100, 100]^2 m$ [48]. Other system parameters are set as $N_a = 4$, $N_c = 2$, $\varepsilon = 0.01$ and $\|h_{ab}\|^2 = 10$ dB. In addition, we consider an urban environment with $\psi = 11.95$, $\omega = 0.14$, $K_{cb} = K_{cc} = 10$, $\eta_{LoS} = 2$ and $\eta_{N,LoS} = 3$ [34]. Here, all the simulation results are averaged over 200 channel realizations. Defining as the ratio of the secrecy rate at Bob to the total power consumption of the system, the secure EE performance is measured by bits per joule [49].

### A. SECRECY PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME

- **Figure 3**: Secrecy rate $R_s$ vs. transmit power of Alice $P_a$ with $h(d_{cb}) = 10$ m and $\sigma_{cb}^2 = 0$.
- **Figure 4**: Secrecy rate $R_s$ vs. transmit power of Alice $P_a$ with different values of $h(d_{cb})$, $P_c = 20$ dB, $M = 4$ and $\sigma_{cb}^2 = 0$.

Without loss of generality the strongest Eve that gains $\max_{m \in M} S_{e,m}$ is assumed to be located at $(10,12,0)$ m. Specially, for the proposed scheme, the UAV-aided Charlie is considered deploying at the coordinate with $(10, 10, h)$ m. It is worth noting that when referring the terrestrial CJ scheme in [11], the coordinate of the terrestrial Jammer is set to satisfy that the distances from Charlie to Bob and Charlie to the strongest Eve on the horizontal plane consistent with the corresponding ones in the case of deploying a UAV jammer. For fairness, and we describe this assumption as $d_{cb} = h$ in each comparison for simplicity.

Figs. 3 and 4 present the secrecy rates achieved by both schemes with different numbers of Eves and values of $h(d_{cb})$ in the case of perfect CSI respectively. It can be shown that the proposed CJ scheme outperforms the terrestrial CJ scheme [11] with the help of the UAV-enabled jammer. From Fig. 3, it is obvious that when $P_c$ increases the UAV-enabled Jammer becomes much more effective in confusing Eves for given $M$ and $h(d_{cb})$. This is mainly due to the fact that comparing with a terrestrial one, the UAV-enabled Jammer owns a higher channel quality for generating artificial noise to interfere Eves without causing performance degradation at Bob. Besides, we can see from Fig. 4 that the impact of $h(d_{cb})$ on the secrecy rate in our scheme is greater than that in another one for a high probability of LoS air-to-ground links.

**Figure 5**: Secure EE vs. the total transmit power $P_a + P_c$ with $\sigma_{cb}^2 = 0$ and $h(d_{cb}) = 10$ m.

**Figure 6**: Secrecy rate $R_s$ vs. transmit power of Alice $P_a$ for the proposed scheme with different values of $\sigma_{cb}^2$, $M = 4$, $h = 10$ m.
CSI. It can be observed that a higher secure EE performance can be achieved in a wide range of total transmit power for the UAV-aided CJ scheme, thus the UAV-enabled jammers suit green communication scenarios for the ability of achieving a relatively sufficient secure EE with less power consumption. Besides, we can see from Fig. 3 and 5 that both secrecy rate and secure EE performance decrease as $M$ increases.

The secrecy rates with respect to the channel estimation error $\sigma_b^2$ and $M$ for the proposed scheme with given $h$ are illustrated in Figs. 6 and 7 respectively. As shown in Fig. 6, the secrecy performance significantly deteriorates as $\sigma_b^2$ increases. In particular, when $\sigma_b^2$ is relatively small, the secure curve nearly matches that in perfect CSI systems. Conversely, when $\sigma_b^2$ grows relatively large, once Charlie is sufficiently powerful, the generated interference may be leaked to the legitimate user and a positive secrecy rate may not be guaranteed, consequently the secure transmission suspends. The impact of the number of Eves in the imperfect CSI systems has been described in Fig. 7. It is shown that the secrecy rate decreases as $M$ increases.

Figs. 8 and 9 demonstrate the impacts of $\sigma_b^2$ and $h(d_{cb})$ on the secrecy rates for both schemes with given $M$ in the case of imperfect CSI systems respectively. It is notable that, partially different from the conclusions that drew from Figs. 3 and 4, we should choose a cooperative jammer which is located at ground to enhance the secrecy performance of the communication systems rather than a UAV-enabled one when the channel estimation error is large e.g., $\sigma_b^2 = 1$. These observations are consistent with our previous analyses that since the air-to-ground channels are dominated by LoS links, the gain of the channel from the UAV-aided jammer to Bob is much greater than that from the terrestrial jammer to Bob. As a result, the UAV-aided jammer causes much stronger interference leakage at Bob when compared with a terrestrial one under given $P_c$ and $\sigma_b^2$. Accordingly, the proposed scheme performs worse than the terrestrial CJ under high CSI uncertainty.

Figs. 10 and 11 show the secure EE performance of both schemes with different $\sigma_b^2$ and $h(d_{cb})$ respectively. As shown in Fig. 10, the proposed scheme can achieve a higher secure EE performance under tolerable channel estimation errors,
however, the increasing of the total power may lead to secure EE performance degradation. Hence, this observation gives us an insight that a trade-off should be concerned between the secrecy rate and the secure EE. In addition, we can deduce from Fig. 11 that, if the channel errors cannot be ignored, a terrestrial cooperative jammer should be deployed in secure transmission networks instead of a UAV.

B. SECRECY PERFORMANCE ANALYSIS OF THE PROPOSED SCHEME WITH UAV PLACEMENT OPTIMIZATION

In this subsection, we examine the performance of the proposed scheme with optimal UAV placement strategy. Considering there are 4 eavesdroppers existing in the wireless transmission system, we assume Eve1, Eve2, Eve3 and Eve4 are located at $(20,20,0)$ m, $(40,0,0)$ m, $(-55,-5,0)$ m and $(-10,-80,0)$ m respectively. When Charlie is regarded as a terrestrial jammer referring to [11], the coordinate of Charlie is set similarly with that in the previous subsection, but only considering the case of UAV jammer with $L = d_{BE}$ for simplicity. And we describe this assumption as $d_{ce} = h$ here in each comparison. Furthermore, we set $L = 5\sqrt{2}$ m in the case of $L \leq d_{BE}$.

Fig. 12 presents the secrecy rates achieved for each Eve in the system with perfect CSI. In this comparison, Charlie is set to be hovering over Bob for fairness, it is obviously that Eve1 is the strongest Eve that gains $\max_{m \in M_{E}} \zeta_{e,m}$. Numerical results are consistent with our analyses in Section II and IV, and according to Lemma 3, we should deploy the UAV jammer as closely as possible to Eve1 in the considered multiple eavesdroppers scenario for UAV placement optimization. In addition, when Charlie is set to be hovering over the geometric center of the Eves, the secrecy rates for Eve1 is shown in Fig. 12 and the effectiveness of this placement strategy is proved to be insufficient.

Secrecy rates with respect to $h$ for UAV optimal location under perfect CSI are illustrated in Fig. 13. As we can see, the impact of $h$ on the secrecy performance is apparent for a high probability of LoS air-to-ground Links and the results also confirm our analysis in Lemma 3.

Fig. 14 compares the secrecy rates achieved by the proposed scheme utilizing two different UAV placement strategies and the terrestrial CJ scheme with different values of $h(d_{ce})$. $P_{c} = 20$ dB and $\sigma_{b}^{2} = 0$. 

VOLUME 4, 2016
gories with the terrestrial CJ scheme presented in [11] under perfect CSI. It is observed when the location of the UAV jammer is optimized, the secrecy performance of the considered system obviously outperforms that of the other two schemes, and increases with $P_c$. With LoS-dominant air-to-ground links, the UAV jammer becomes much more effective in deteriorating the channel of Eve1 via getting closer to Eve1.

Fig. 15 demonstrates the impact of $\sigma_b^2$ on the secrecy rates for the proposed scheme with UAV optimal placement strategy. Similarly to the conclusion we have drawn from Fig. 6, channel estimation errors significantly deteriorate the secrecy performance, and the secrecy rates obviously decrease with the increasing of $\sigma_b^2$. As we can see from Fig. 15, the secure rates curve almost matches that in perfect CSI systems with negligible $\sigma_b^2$. However, for a high probability of LoS air-to-ground links, Charlie will cause terrible secrecy performance degradation when $\sigma_b^2$ is relatively big, and the secure transmission cannot be guaranteed.

Figs. 16 and 17 show the secure EE performance of the proposed scheme with the two different UAV placement strategies under imperfect CSI. It can be shown that when the UAV jammer is placed at the optimal location, a higher secure EE can be certainly achieved regardless of the value of $\sigma_b^2$. This observation can be explained as follows. From (9) and (11), we can see that the channel estimation errors have harmful effect on the secrecy performance, and when the location of the UAV jammer is optimized, the distance between Charlie and Bob is much greater than that in non-optimal UAV placement strategy, so the impact of the interference generated by Charlie on the secrecy rates under imperfect CSI is weakened. Meanwhile, the distance between Charlie and Eve1 is shortened when optimal UAV placement strategy is exploited, thus Charlie obtains a stronger channel gain to confuse Eve1.

The secrecy rates achieved by the proposed scheme utilizing two different UAV placement strategies and the terrestrial CJ scheme under imperfect CSI are demonstrated in Figs. 18 and 19. It is noteworthy that even though compared with the terrestrial CJ scheme, the UAV jammer play a worse role in reducing the secrecy rates for a high probability
of LoS air-to-ground links under relatively large channel estimation error, the performance of the proposed scheme can be significantly improved by optimizing the location of the UAV jammer. Specifically, it can be seen that when both $P_c$ and $\sigma_b^2$ are relatively large e.g., $P_c = 20 \text{ dB}$ and $\sigma_b^2 = 1$, the proposed scheme with optimal UAV placement strategy is still effective. As a result, exploiting optimal UAV placement strategy, a wider range of tolerable channel errors can be achieved by our proposed CJ scheme.

Figs. 20 and 21 depict the secure EE performance of the proposed scheme with two different UAV placement strategies and the terrestrial CJ scheme under imperfect CSI. Simulation results reveal that when the location of the UAV jammer is optimized by the strategy proposed in Section IV, the communication system owns a much higher secure EE, compared with those utilizing non-optimal UAV placement strategy. Furthermore, it can be shown that systems with proposed scheme exploiting optimal UAV placement strategy can tolerate a relatively larger channel estimation error, hence the applicability and adaptability of the proposed scheme has been significantly enhanced.

VI. CONCLUSION

In this paper, we investigate the physical layer security in MISOME wiretap channel networks, where a UAV is deployed as a cooperative jammer to enhance the secrecy performance against multiple eavesdroppers with imperfect CSI. Specifically, an efficient scheme has been developed to obtain the optimal power allocation factor between information signals and AN signals for solving the SRM problem under certain SOP. Furthermore, we derived an optimal UAV placement strategy to obtain the best location of the UAV jammer. Numerical results have been provided to reveal the effects of eavesdropper numbers and the values of channel estimation error on the secrecy performance. In addition, the effectiveness of the proposed scheme with optimal UAV placement strategy in enhancing the secrecy rate and the secure EE under tolerable channel uncertainty have been verified.

APPENDIX A PROOF OF LEMMA 1

Firstly, we define $j_1 = \frac{P_c}{P_a} \frac{d_{\text{LoS}}^{m_{\text{LoS}}}}{m_{\text{ce}}} \frac{1}{m_{\text{ce}}}$ and $j_2 = P_c \left( \frac{d_{\text{LoS}}}{d_{\text{ce}}} \right)^{\eta_{\text{LoS}}}$. Hence, by taking the derivate on both sides of (35), we have

$$0 = \frac{d_{\text{LoS}}^{m_{\text{LoS}}}}{P_a} \rho'(\phi) + \frac{3[(1-\phi)\rho'(\phi) - \rho(\phi)]}{3 + (1-\phi)\rho(\phi)} \quad (44)$$

and $G$ can be simplified as

$$G = \frac{[1 + j_1 \rho(\phi)]^{m_{\text{ce}}}}{A^{m_{\text{ce}}}}$$

$$= \frac{P_{\text{LoS}}^{m_{\text{ce}}} B + (1 - P_{\text{LoS}}^{m_{\text{ce}}}) A^{m_{\text{ce}}}}{}$$

VOLUME 4, 2016

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/.

10.1109/ACCESS.2019.2929844, IEEE Access
where \( A = 1 + j_1 \rho \) and \( B = 1 + j_2 \rho \). Then \( (\ln(\gamma))' \) is given by

\[
\frac{(\ln(\gamma))'}{\rho'} = \frac{P_{\text{LoS}} \left( \frac{B}{A} m_{\text{ce}j1} - j_2 \right)}{P_{\text{LoS}} B + (1 - P_{\text{LoS}}) A^{m_{\text{ce}}}}.
\]

From (41), we know that the denominator of \( \frac{(\ln(\gamma))'}{\rho'} > 0 \), and the numerator on the right-hand side of (41) can be simplified as

\[
m_{\text{ce}j1} - j_2 + m_{\text{ce}j1} j_2 \rho - j_1 j_2 \rho = \frac{1 + j_1 \rho}{1 + j_1 \rho(\phi)}.
\]

Since \( \rho(\phi) > 0 \), and \( m_{\text{ce}} > 1 \), so we can deduce that

\[
m_{\text{ce}j1} - j_2 > 0.
\]

Thus \( m_{\text{ce}}j1 - j_2 \) can be simplified as

\[
m_{\text{ce}j1} - j_2 = \frac{P_c}{P_a} \left( \frac{d_{\text{LoS}}^{m_{\text{ce}}}}{d_{\text{LoS}}^{m_{\text{ce}}} - d_{\text{LoS}}^{m_{\text{ce}}}} \right),
\]

and we have \( m_{\text{ce}}j1 - j_2 > 0 \) for \( \eta_{\text{LoS}} > \eta_{\text{LoS}} \). As a result, \( (\ln(\gamma))' > 0 \) can be verified.

Substituting (41) into (35). And after some transformation, we have

\[
\rho'(\phi) = \left( \frac{3(\rho(\phi))}{3 + (1 - \phi)\rho(\phi)} \right) \left[ \frac{d_{\text{LoS}}^{m_{\text{ce}}}}{P_a} + \frac{3(1 - \phi)\rho(\phi)}{P_a} + \frac{j_2}{1 + j_2 \rho(\phi)} + \frac{P_c}{P_{\text{LoS}} B + (1 - P_{\text{LoS}}) A^{m_{\text{ce}}}} \right],
\]

and it is obvious from (45) that the first three terms of the denominator of the right-hand side strictly decrease with respect to \( \phi \), hence we pay our attention to the last term.

Since \( (\ln(\gamma))' > 0 \) and \( \rho'(\phi) > 0 \) have been proved in Appendix A, we have \( P_{\text{LoS}} \left( \frac{B}{A} m_{\text{ce}j1} - j_2 \right) > 0 \). Then we rewrite the last term of the denominator of (45) as

\[
\frac{P_c}{P_{\text{LoS}} B + (1 - P_{\text{LoS}}) A^{m_{\text{ce}}}} \left[ 3 + (1 - \phi)\rho(\phi) \right] = \frac{C_2}{C_1},
\]

where \( C_1 = P_{\text{LoS}} B + (1 - P_{\text{LoS}}) A^{m_{\text{ce}}} \), \( C_2 = P_{\text{LoS}} \left( \frac{B}{A} m_{\text{ce}j1} - j_2 \right) \), and \( C_3 = \left[ 3 + (1 - \phi)\rho(\phi) \right] \). Since \( C_1, C_2, C_3 > 0 \), and \( C_3' > 0 \) can be easily verified, we have

\[
\{ \frac{C_2}{C_1} \} < 0. \text{ Hence the denominator on the right-hand side of (45) strictly decreases with } \phi, \text{ this completes the proof of Lemma 2.}
\]

**ACKNOWLEDGEMENT**

The authors would like to thank the editor and the anonymous reviewers for their constructive comments and excellent suggestions.

**REFERENCES**


