This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3465871

Enhancing Covert Secrecy Rate in A Zero-Forcing UAV Jammer-Assisted Covert Communication

Xinying Chen, Zheng Chang, *Senior Member, IEEE,* and Timo Hämäläinen, *Senior Member, IEEE*

***Abstract*—Covert communications can hide confidential signals in environmental noise to avoid being detected and provide comprehensive security for wireless transmissions. However, there still exist significant risks in wireless transmission once being detected. In this paper, we propose a more secure covert scheme, where a multiple antennas transmitter, assisted by a multi-antenna UAV jammer, maximizes the covert secrecy rate under the scenarios of both correct and incorrect detection by a warden with both error detection probability and eavesdropping rate limitations satisfied. The transmitter and jammer adopt maximum ratio transmission (MRT) and zero-forcing, respectively, to maximize the transmission rate and minimize the interference at the legitimate receiver. First, we analyze the monotonicity of error detection probability to determine the optimal power detection threshold and the corresponding smallest error detection probability. Then, under this worst case, we jointly optimize the transmit and jamming power to maximize the covert secrecy rate while guaranteeing the covert and eavesdropping limits meet their requirements, respectively. Finally, simulation results are presented to prove the correctness of the theoretical conclusion and evaluate the effectiveness of our proposed scheme.**

***Index Terms*—Covert communication, Gaussian signaling, secure transmission, UAV, zero-forcing.**

I. Introduction

Wireless communication has brought tremendous convenience and enabled fast connections to everyone. However, the characteristic of broadcasting in wireless networks also posts confidential messages under the risk of leakage. Therefore, transmission security becomes more and more important, especially when the messages contain personal data or sensitive information [1]. There are two typical methods to achieve secure wireless communications, i.e., physical layer security (PLS) and covert communications [2]. PLS attains secure transmission by utilizing the randomness of wireless channels combined with precoding and signal processing, which aims to reduce the eavesdropping rate [3]. However, PLS can still be exposed to a higher risk of being eavesdropped as the wireless techniques develop. Different from PLS, covert communications provide concealment via hiding confidential signals in environmental noise, where the warden does not decode the signals without detection, and thus provide transmission security [4]. Nevertheless, the covert communication cannot provide secure transmission once the transmission behavior is correctly detected.

The unmanned aerial vehicle (UAV), widely exploited in wireless communications, has plenty of advantages, e.g., fast deployment, light volume, and high mobility, among which it can also leverage the air-to-ground line-of-sight (LoS) channels [5]. Channel randomness has been exploited to offer secure transmission in PLS and covert networks, which also brings the difficulties of obtaining channel state information (CSI). In one respect, the difficulty of acquiring CSI makes it hard for malicious users to eavesdrop; in another respect, it is also difficult to obtain CSI for legitimate users while utilizing channel uncertainty [6]. The introduction of UAVs changes this predicament. Although the characteristic of the LoS channel increases the risk of information leakage, on the other hand, benefiting from the UAV employment, it also enables legitimate users to obtain CSI easily within the network [7]. The easy obtainment of CSI in LoS channels proliferates the study and application of the multi-antenna technique. The multi-antenna technique, which leverages channel multiplexing, has been broadly exploited in PLS and covert communications to achieve better transmission performance [8]. The multiple antennas can be used to realize maximum ratio transmission (MRT), where the precoding vector is designed according to the CSI to achieve a maximum signal-to-interference ratio (SINR) [9]. It can also be employed in jamming-assisted networks to realize zero-forcing, which can minimize the undesired interference at specific users [10].

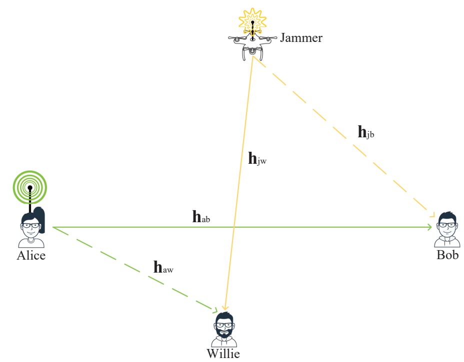


Fig. 1. System model of a zero-forcing UAV jammer-assisted covert communication network.

Unlike most of the existing research works on covert communications, which primarily focuses on improving the performance during miss detection phase, i.e., maximizing the transmission rate, this paper investigates a covert network that aims to provide comprehensive security protection for both correct and incorrect detection cases [4], [7], [9]. We jointly optimize the transmit and jamming power to maximize the covert secrecy rate while avoiding being detected and eavesdropped, thereby ensuring secure transmission even when the transmission behavior of the transmitter is correctly detected. First, the optimal power detection threshold and the corresponding minimized error detection probability at the warden are derived. Then, the transmit and jamming power are optimized to achieve a higher covert secrecy rate while

This work is partly supported by the National Natural Science Foundation of China (NSFC) under Grant 62071105 and supported in part by Horizon EU Grant No. 101086159.

X. Chen and Timo Hämäläinen are with the Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland (email: xinying.x.chen@jyu.fi; timo.t.hamalainen@jyu.fi).

Z. Chang is with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, and also with Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland. (email: zheng.chang@jyu.fi).

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3465871

guaranteeing both the optimal error detection probability and the eavesdropping rate are within the limits.

II. System Model

Consider a covert communication system where Alice transmits confidentially to Bob while avoiding detection by Willie, aided by a UAV jammer emitting jamming signals constantly, as shown in Fig.1. The locations of Alice, the jammer, Bob, and Willie are $L_a(x_a, y_a, 0)$, $L_j(x_j, y_j, H)$[1], $L_b(x_b, y_b, 0)$, $L_w(x_w, y_w, 0)$, respectively, where H is the fixed hovering altitude of the drone jammer. Assume that Alice is equipped with M antennas, the jammer is equipped with N antennas, while both Bob and Willie are equipped with single receiving antennas. The channel coefficients for ground users from Alice to Bob $\mathbf{h}_{ab} \in \mathbb{C}^{1\times M}$ and to Willie $\mathbf{h}_{aw} \in \mathbb{C}^{1\times M}$ are assumed to follow a large-scale path loss and a small-scale Rayleigh fading, which can be described as

$$\mathbf{h}_{ab} = \sqrt{\rho_0/d_{ab}^{-\alpha}}\mathbf{g}_{ab}, \tag{1}$$

$$\mathbf{h}_{aw} = \sqrt{\rho_0/d_{aw}^{-\alpha}}\mathbf{g}_{aw}, \tag{2}$$

where $d_{ab} = ||L_a - L_b||$ and $d_{aw} = ||L_a - L_w||$ are the distances from Alice to Bob and to Willie, respectively. ρ_0 is the reference power gain at 1 m and α denotes the large-scale path loss exponent. In addition, each Rayleigh fading component $g_{a_i b}$ and $g_{a_i w}$, $\forall i \in \{1, \cdots, M\}$, in both $\mathbf{g}_{ab}$ and $\mathbf{g}_{aw}$ is independent and identically distributed (i.i.d), which follows complex Gaussian distribution with zero mean and unit variance, i.e., $g_{a_i b} \sim \mathcal{CN}(0,1)$ and $g_{a_i w} \sim \mathcal{CN}(0,1)$.

The air-to-ground channels from the jammer to Bob $\mathbf{h}_{jb} \in \mathbb{C}^{1\times N}$ and to Willie $\mathbf{h}_{jw} \in \mathbb{C}^{1\times N}$ are assumed to be LoS channels. They can be denoted as

$$\mathbf{h}_{jb} = \sqrt{\rho_0/d_{jb}^{-\alpha}}\mathbf{g}_{jb}, \tag{3}$$

$$\mathbf{h}_{jw} = \sqrt{\rho_0/d_{jw}^{-\alpha}}\mathbf{g}_{jw}, \tag{4}$$

where $d_{jb} = ||L_j - L_b||$ and $d_{jw} = ||L_j - L_w||$ are the distances from the jammer to Bob and to Willie, respectively. $\forall i \in \{1, \cdots, N\}$, we have $|g_{j_i b}| = |g_{j_i w}| = 1$, where $g_{j_i b} \in \mathbf{g}_{jb}$ and $g_{j_i w} \in \mathbf{g}_{jw}$.

In order to achieve higher uncertainty and avoid being detected by Willie, Alice selects time slots with a probability of $\pi = 0.5$ to transmit baseband signal $x[k]$ with transmit power P_a to Bob. Suppose the CSI among legitimate users is known to each other, which can be obtained through channel sounding, CSI feedback, and fast CSI reporting techniques. Alice adopts MRT towards Bob to achieve better performance, where her precoding vector $\mathbf{u} \in \mathbb{C}^{M\times 1}$ can be defined as

$$\mathbf{u} = \mathbf{g}_{ab}^H/||\mathbf{g}_{ab}||. \tag{5}$$

Additionally, the jammer constantly emits jamming signals to assist Alice in avoiding being detected by Willie. In order to introduce uncertainty at Willie, the jammer applies Gaussian signaling $\mathbb{J}x_j[k] \sim \mathcal{CN}(0, P_j)$. With CSI $\mathbf{g}_{jb}$ obtainable at the jammer, it can employ zero-forcing precoding towards Bob, where the precoding vector $\mathbf{v} \in \mathbb{C}^{N\times 1}$can be described as

$$\begin{cases} \mathbf{g}_{jb}\mathbf{v} = 0, \\ \|\mathbf{v}\|^2 = 1. \end{cases} \tag{6}$$

Therefore, the received signals at Bob in each time slot can be denoted as

$$y_b[k] = \sqrt{P_a}\mathbf{h}_{ab}\mathbf{u}x[k] + n_b[k], \tag{7}$$

where $n_b[k]$ is the additive white Gaussian noise (AWGN) received at Bob, and it follows complex Gaussian distribution, i.e., $n_b[k] \sim \mathcal{CN}(0, \sigma_b^2)$. Correspondingly, the transmission rate R_b at Bob can be expressed as

$$R_b = \log_2\left(1 + P_a\rho_0|\mathbf{g}_{ab}\mathbf{u}|^2/(d_{ab}^{\alpha}\sigma_b^2)\right). \tag{8}$$

Since the zero-forcing is designed towards only Bob, Willie receives signals from both Alice and the jammer, which can be denoted as

$$y_w[k] = \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k] + \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], \tag{9}$$

where $n_w[k]$ is the i.i.d AWGN received at Willie in each time slot and follows $n_w[k] \sim \mathcal{CN}(0, \sigma_w^2)$. The corresponding eavesdropping rate R_e at Willie can be calculated as

$$R_e = \log_2\left(1 + \frac{P_a\rho_0|\mathbf{g}_{aw}\mathbf{u}|^2/d_{aw}^{\alpha}}{\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2P_j/d_{jw}^{\alpha} + \sigma_w^2}\right). \tag{10}$$

III. The Optimal Detection of Willie

Willie needs to decide whether Alice is transmitting $\mathcal{H}_1$ or silent $\mathcal{H}_0$ according to his received signal power, and then decide whether to decode the received signals or not. The received signals of the two above-mentioned cases can be denoted as

$$y_w[k] = \begin{cases} \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], & \mathcal{H}_0, \\ \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k] + \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], & \mathcal{H}_1. \end{cases} \tag{11}$$

Willie measures his received samples N times and derives the averaged received signal power P_w to compare with his preset power detection threshold ξ, and then makes his decision. The decision rule can be described as

$$P_w = \frac{1}{N}\sum_{k=1}^{N}|y_w[k]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \xi, \tag{12}$$

where N is the number of samples. Willie decides that Alice is transmitting $\mathcal{D}_1$ when P_w is larger than ξ, and Alice keeps silent $\mathcal{D}_0$ when P_w is smaller than ξ.

We consider the interference limit network, i.e., σ_b^2 and σ_w^2 can be ignored in Willie's detection. As the signal samples get larger, i.e., $N \to \infty$, the averaged received power P_w can be rewritten as

$$P_w = \begin{cases} J, & \mathcal{H}_0, \\ S + J, & \mathcal{H}_1, \end{cases} \tag{13}$$

where J and S represent the jamming and signal power, respectively. They can be summarized as

$$J = |\mathbb{J}x_j[k]|^2|\mathbf{h}_{jw}\mathbf{v}|^2, \tag{14}$$

$$S = P_a|\mathbf{h}_{aw}\mathbf{u}|^2. \tag{15}$$

According to the decision rule in (12), there are two types of mistakes that Willie may make, which are the false alarm (FA) and the miss detection (MD). The FA mistake indicates that Willie believes that Alice is transmitting while she is silent. MD indicates that Willie believes that Alice is silent while she is transmitting. The error detection probability p_e is defined as the probability that Willie makes FA and MD mistakes, which can be described as

$$p_e = \mathbb{P}_{FA} + \mathbb{P}_{MD} = \mathbb{P}(\mathcal{D}_1|\mathcal{H}_0) + \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1) = \mathbb{P}(J \geq \xi) + \mathbb{P}(J+S \leq \xi). \tag{16}$$

On the other hand, the correct detection probability of Willie can be expressed as

[1]The jammer can adjust its location and track Willie for optimal jamming once Willie's location is obtainable.

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3465871

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \mathbb{P}(J+S \geq \xi). \tag{17}$$

Owing to $\mathbb{J}x_j[k] \sim \mathcal{CN}(0, P_j)$, $|\mathbb{J}x_j[k]|^2$ follows a chi-square distribution with 2 degrees of freedom, which equivalents to exponential distribution. Thus, we can conclude $J \sim \exp(\lambda_j)$, $\lambda_j = \frac{d_{jw}^{\alpha}}{P_j \rho_0 |\mathbf{g}_{jw}\mathbf{v}|^2}$.

As for $\mathbf{g}_{aw} \sim \mathcal{CN}(0, \mathbf{I})$ and $\mathbf{g}_{ab} \sim \mathcal{CN}(0, \mathbf{I})$ are i.i.d and follow the same distribution, we can conclude that $|\mathbf{h}_{aw}\mathbf{u}|^2 \sim \exp(1)$. This further leads to $S \sim \exp(\lambda_s)$, where denote $\lambda_s = \frac{d_{aw}^{\alpha}}{P_a \rho_0}$.

Correspondingly, p_e in (16) can be changed into

$$\begin{aligned} p_e &= 1-\mathbb{F}_J(\xi)+\mathbb{F}_{J+S}(\xi) = e^{-\lambda_j \xi} + \int_0^{\xi} \mathbb{F}_J(\xi - x) f_S(x) dx \\ &= \begin{cases} 1-\lambda_j \left(e^{-\lambda_j \xi} - e^{-\lambda_s \xi}\right)/(\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ 1 - \lambda_s \xi e^{-\lambda_s \xi}, & \lambda_s = \lambda_j. \end{cases} \end{aligned} \tag{18}$$

Similarly, the correct detection probability $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)$ in (17) can be altered to

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \begin{cases} \left(\lambda_s e^{-\lambda_j \xi} - \lambda_j e^{-\lambda_s \xi}\right)/(\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ (1+\lambda_s \xi) e^{-\lambda_s \xi}, & \lambda_s = \lambda_j. \end{cases} \tag{19}$$

From the definition of λ_j, λ_s, and the expression of p_e in (18), we can see that p_e is related to ξ. Willie can achieve a smaller p_e by properly choosing his power detection threshold. The optimal ξ to minimize Willie's error detection probability p_e is derived in Proposition 1.

Proposition 1: The optimal power detection threshold at Willie can be expressed as

$$\xi^* = \begin{cases} (\ln \lambda_s - \ln \lambda_j)/(\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ 1/\lambda_s, & \lambda_s = \lambda_j. \end{cases} \tag{20}$$

and the corresponding minimized error detection probability p_e^* can be derived as

$$p_e^* = \begin{cases} 1 - (\lambda_s/\lambda_j)^{-\frac{\lambda_s}{\lambda_s - \lambda_j}}, & \lambda_s \neq \lambda_j, \\ 1 - 1/e, & \lambda_s = \lambda_j. \end{cases} \tag{21}$$

Proof. We first analyze the general case when $\lambda_s \neq \lambda_j$. The impact of ξ on p_e can be obtained by analyzing the monotonicity of p_e. The first-order derivative of p_e with respect to ξ can be derived as

$$p_e'(\xi) = -\lambda_j \left(-\lambda_j e^{-\lambda_j \xi} + \lambda_s e^{-\lambda_s \xi}\right)/(\lambda_s - \lambda_j). \tag{22}$$

The zeros of $p_e'(\xi)$ in (22) can be derived as $\xi_0 = \frac{\ln \lambda_s - \ln \lambda_j}{\lambda_s - \lambda_j}$.

Based on the definition of λ_s and λ_j, we can have $\lambda_s > 0$ and $\lambda_j > 0$. We discuss the monotonicity of p_e with respect to ξ under two cases, i.e., $\lambda_s > \lambda_j$ and $\lambda_s < \lambda_j$, to derive the optimal ξ.

- $\lambda_s > \lambda_j$: In this case, we can conclude that $p_e'(\xi) > 0$, when $\xi > \xi_0$; and $p_e'(\xi) < 0$, when $\xi < \xi_0$. This indicates that p_e monotonically decreases with ξ, when $\xi < \xi_0$; and monotonically increases, when $\xi > \xi_0$. p_e obtains its minimum at ξ_0.
- $\lambda_s < \lambda_j$: We can also have $p_e'(\xi) > 0$, when $\xi > \xi_0$; and $p_e'(\xi) < 0$, when $\xi < \xi_0$. This also indicates that p_e monotonically decreases when $\xi < \xi_0$, and increases when $\xi > \xi_0$. p_e reaches its minimum at ξ_0 as well.

Both cases lead to the same optimal detection threshold ξ^* as shown in (20). Based on (18), the corresponding p_e^* is presented in (21). The conclusion for case $\lambda_s = \lambda_j$ can be derived similarly. □

With the optimal power detection threshold ξ^* in (20), the correct detection probability in (19) becomes

$$\mathbb{P}^*(\mathcal{D}_1|\mathcal{H}_1) = \begin{cases} (\lambda_s/\lambda_j)^{-\frac{\lambda_s}{\lambda_s - \lambda_j}} + (\lambda_s/\lambda_j)^{-\frac{\lambda_j}{\lambda_s - \lambda_j}}, & \lambda_s \neq \lambda_j, \\ 2/e, & \lambda_s = \lambda_j. \end{cases} \tag{23}$$

IV. Transmit and Jamming Power Optimization for a More Secure Covert Communication

A. Problem Formulation

We aim to provide a more secure transmission for covert communication between Alice and Bob against Willie. In this section, we jointly optimize transmit and jamming power to maximize the covert secrecy rate while guaranteeing Willie's optimal error detection probability is larger than the limit and the eavesdropping rate is lower than the limit. The optimization problem can be summarized as

$$\begin{aligned} \textbf{P1:} \quad & \max_{P_a, P_j} \quad R_{cs} && (24a) \\ & s.t. \quad p_e^* \geq \epsilon, && (24b) \\ & \quad R_e \leq r_e, && (24c) \\ & \quad R_b \geq r, && (24d) \\ & \quad P_a \leq P_{amax}, && (24e) \\ & \quad P_j \leq P_{jmax}, && (24f) \end{aligned}$$

where ϵ is the lower limit of Willie's error detection probability, r_e represents the upper limit of Willie's eavesdropping rate, r is the lower threshold of transmission rate, P_{amax} and P_{jmax} are the maximum allowed transmit and jamming power, respectively. In addition, the covert secrecy rate R_{cs} is defined as the secrecy rate in covert communication when Alice is transmitting. It includes two cases: 1) Willie decides $\mathcal{D}_0$ when $\mathcal{H}_1$. Willie does not attempt to decode Alice's signals when he believes she is silent. 2) Willie decides $\mathcal{D}_1$ when $\mathcal{H}_1$. Alice is still possible to transmit securely without the risk of being eavesdropped on. Therefore, R_{cs} can be denoted as

$$R_{cs} = R_b \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1) + (R_b - R_e)\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = R_b - \mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) R_e. \tag{25}$$

B. Impact of Constraint ϵ on P_a and P_j

According to Proposition 1, Willie can obtain his minimum error detection probability p_e^* by setting the power detection threshold as (20). To guarantee that p_e^* satisfies the constraint, the requirement of P_a and P_j is shown in Proposition 2.

Proposition 2: To guarantee (24b), the transmit and jamming power should satisfy

$$\frac{P_a}{P_j} \leq \frac{d_{aw}^{\alpha} |\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}} \frac{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}{\ln(1-\epsilon)}. \tag{26}$$

Proof. With the expression of p_e^* in (21) and in order to satisfy the constraint in (24b), we have

$$\left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\frac{\lambda_s}{\lambda_j}}{\frac{\lambda_s}{\lambda_j} - 1}} \leq 1 - \epsilon. \tag{27}$$

Let $t = \frac{\lambda_s}{\lambda_j}$, and we have $t > 0$. Then, (27) can be altered to

$$\frac{t}{t-1} \ln \frac{1}{t} \leq \ln(1-\epsilon). \tag{28}$$

To further obtain the limitation of P_a and P_j, we need to discuss t by classifying $t > 1$ and $0 < t < 1$.

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3465871

- Case $t > 1$:
  With $t \in (1, \infty)$, (28) can be changed into

$$\begin{aligned} \ln \frac{1}{t} &\leq \frac{t-1}{t} \ln(1-\epsilon) \\ \frac{1}{t} &\leq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)}. \end{aligned} \tag{29}$$

  Owing to $\ln(1-\epsilon) < 0$, (29) can be altered to

$$\ln(1-\epsilon)e^{\ln(1-\epsilon)} \leq \frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} < 0, \tag{30}$$

  which satisfies the form of the Lambert W function. Therefore, we can have

$$\frac{\ln(1-\epsilon)}{t} \leq \mathscr{W}_{-1}(\ln(1-\epsilon)e^{\ln(1-\epsilon)}), \tag{31}$$

  or

$$\mathscr{W}_0(\ln(1-\epsilon)e^{\ln(1-\epsilon)}) \leq \frac{\ln(1-\epsilon)}{t} < 0, \tag{32}$$

  where $\mathscr{W}_0(*)$ is the principle branch of Lambert W function, and $\mathscr{W}_{-1}(*)$ represents the negative branch. Practically, the error detection probability limit ϵ is close to 1. Therefore, from (31) we can have

$$0 < \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}\left((1-\epsilon)\ln(1-\epsilon)\right)} = 1, \tag{33}$$

  which is against the initial assumption of $t > 1$. From (32), we can have

$$\frac{\lambda_s}{\lambda_j} \geq \frac{\ln(1-\epsilon)}{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}. \tag{34}$$

  Then, we can further derive the upper limit of P_a/P_j as shown in (26).
- Case $0 < t < 1$:
  Similarly, when $t \in (0, 1)$, (28) can be changed into

$$\begin{aligned} \ln \frac{1}{t} &\geq \left(1 - \frac{1}{t}\right) \ln(1-\epsilon) \\ \frac{1}{t} &\geq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)} \\ \frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} &\leq \ln(1-\epsilon)e^{\ln(1-\epsilon)}. \end{aligned} \tag{35}$$

  According to Lambert W function, the solution to (35) can be derived as

$$\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} \leq \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_0((1-\epsilon)\ln(1-\epsilon))}. \tag{36}$$

  Owing to $\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} = 1$, (36) is against the assumption of $t \in (0, 1)$.

The overall constraint of P_a/P_j is demonstrated in (26). □

C. Optimize P_a and P_j to Maximize R_{cs}

To maximize the covert secrecy rate R_{cs}, the transmit power P_a and jamming power P_j need to be adjusted properly while satisfying constraints in (24). The objective function (24a) is non-convex and mathematically difficult to solve. Based on the expression of $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)^*$ in (23) and R_{cs} in (25), we can further conclude

$$R_{cs} \geq R_b - R_e = \tilde{R}_{cs}, \tag{37}$$

where $\tilde{R}_{cs}$ can be defined as

$$\tilde{R}_{cs} = \log_2\left(1 + \frac{P_a \rho_0 |\mathbf{g}_{ab}\mathbf{u}|^2}{d_{ab}^{\alpha} \sigma_b^2}\right) - \log_2\left(1 + \frac{P_a \rho_0 |\mathbf{g}_{aw}\mathbf{u}|^2 / d_{aw}^{\alpha}}{\rho_0 |\mathbf{g}_{jw}\mathbf{v}|^2 P_j / d_{aw}^{\alpha} + \sigma_w^2}\right). \tag{38}$$

Thus, maximize R_{cs} is equivalent to maximize $\tilde{R}_{cs}$. Then, We analyze the monotonicity of $\tilde{R}_{cs}$ with respect to P_a and P_j to derive the optimal transmit and jamming power.

The first-order derivative of $\tilde{R}_{cs}$ with respect to P_a and P_j can be demonstrated respectively as

$$\tilde{R}'_{cs}(P_a) = \frac{||\mathbf{h}_{ab}||^2 (|\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2) - |\mathbf{h}_{aw}\mathbf{u}|^2 \sigma_b^2}{\ln 2 \left(P_a ||\mathbf{h}_{ab}||^2 + \sigma_b^2\right)(|\mathbf{h}_{aw}\mathbf{u}|^2 P_a + |\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2)}, \tag{39}$$

$$\tilde{R}'_{cs}(P_j) = \frac{\left(|\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2\right) |\mathbf{h}_{aw}\mathbf{u}|^2 |\mathbf{h}_{jw}\mathbf{v}|^2 P_a}{\ln 2 (P_a ||\mathbf{h}_{ab}||^2 + \sigma_b^2)(|\mathbf{h}_{aw}\mathbf{u}|^2 P_a + |\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2)^2}. \tag{40}$$

From (39), we can see that $\tilde{R}_{cs}$ monotonically increases with P_a. To achieve larger $\tilde{R}_{cs}$, P_a needs to be set to its maximum. However, P_a is still constrained by (24b), (24c), (24d), and (24e). From (40), we can see that $\tilde{R}_{cs}$ monotonically increases with P_j. A larger $\tilde{R}_{cs}$ can be achieved by setting P_j to its maximum, where P_j is constrained by (24b), (24c), and (24f).

To meet the constraints (24d) and (24e), the transmit power P_a needs to satisfy

$$\frac{(2^r - 1)\sigma_b^2}{||\mathbf{h}_{ab}||^2} \leq P_a \leq P_{amax}. \tag{41}$$

To comply the constraints (24c) and (24f), the jamming power P_j needs to satisfy

$$\frac{|\mathbf{h}_{aw}\mathbf{u}|^2 P_a - (2^{r_e} - 1)\sigma_w^2}{(2^{r_e} - 1)|\mathbf{h}_{jw}\mathbf{v}|^2} \leq P_j \leq P_{jmax}. \tag{42}$$

From (42), we can further conclude the constraints for P_a as

$$P_a \leq \frac{P_j (2^{r_e} - 1)|\mathbf{h}_{jw}\mathbf{v}|^2 + (2^{r_e} - 1)\sigma_w^2}{|\mathbf{h}_{aw}\mathbf{u}|^2} = P_a^{URe}. \tag{43}$$

In addition, according to the constraint (24b) and the corresponding conclusion in Proposition 1, we can further conclude

$$P_a \leq \frac{d_{aw}^{\alpha} |\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}} \frac{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}{\ln(1-\epsilon)} P_j = P_a^{Upe}. \tag{44}$$

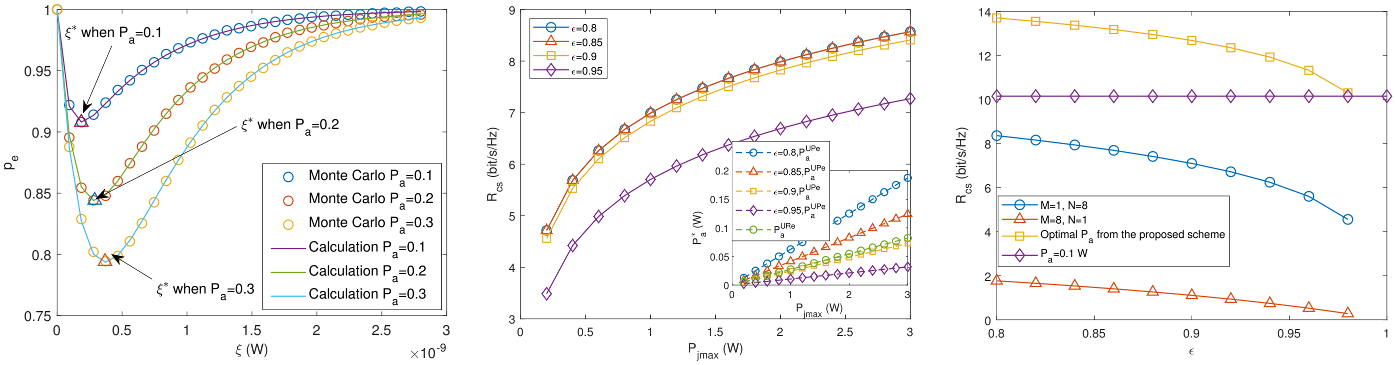
Overall, we can set P_j as its maximum and P_a satisfy constraints of (43) and (44) to obtain the optimal transmit power P_a^* and jamming power P_j^* as

$$\begin{cases} P_j^* = P_{jmax}, \\ P_a^* = \min\{P_a^{URe}, P_a^{Upe}\}. \end{cases} \tag{45}$$

Therefore, the maximum R_{cs} can be achieved by setting P_a and P_j according to (45).

V. Simulation

In this section, simulation results are presented and discussed to evaluate the effectiveness of our proposed covert communication scheme. We assume that Alice, Bob, Willie, and the jammer are located at $L_a = (0, 0, 0)$, $L_b = (200, 0, 0)$, $L_w = (200, 100, 0)$, and $L_j = (200, 100, 130)$ in meters, respectively. The large-scale path loss exponent is set to $\alpha = 2.6$, and the reference power gain at the distance of 1 m is set to $\rho_0 = -30$ dB [1], [11]. Without loss of generality, we set the AWGN variance received at Bob and Willie as $\sigma_b^2 = \sigma_w^2 = -120$ dBm, since both Bob and Willie are on the ground.



(a) (b) (c)

Fig. 2. (a) Error detection probability versus power detection threshold at Willie; (b) Achievable covert secrecy rate versus maximum allowed jamming power; (c) Achievable covert secrecy rate versus error detection probability limit in different schemes.

In Fig. 2(a), the impact of power detection threshold ξ on the error detection probability p_e is investigated under different transmit power P_a. The transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. $P_{jmax} = 1$ W. From the results, we can see that the Monte Carlo simulation results match our theoretical calculation results as shown in (18). In addition, we can also see that p_e first decreases then increases with ξ, which indicates there exists the optimal power detection threshold to minimize p_e. The results also show that the ξ^* derived from (20) corresponds to the simulation results and leads to the minimum p_e, which agrees with Proposition 1. We can further see from the results that the error detection probability p_e decreases as P_a increases. This is because larger transmit power leads to a higher risk of being detected. Therefore, Alice can reduce her transmit power for better covertness.

Fig. 2(b) demonstrate the influence of the maximum allowed jamming power P_{jmax} on the achievable secrecy rate R_{cs} under different error detection probability limits ϵ. The transmit power at Alice and jamming power are set according to (45). The transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. From the results, we can see that R_{cs} increases as P_{jmax} gets larger. This is because the transmit power P_a^* increases as P_{jmax} rises, and thus results in a larger R_{cs}. Additionally, it also indicates that R_{cs} decreases with ϵ, however, $\epsilon = 0.8$ and $\epsilon = 0.85$ result to the same R_{cs}. This is because when $\epsilon = 0.8$ and $\epsilon = 0.85$ we have $P_a^{URe} < P_a^{Upe}$, therefore, P_a^* in both cases are set to P_a^{URe}.

The effectiveness of our proposed covert scheme is compared in Fig. 2(c) with No MRT, no zero-forcing, and fixed transmit power of $P_a = 0.1$ W scheme. In our proposed scheme, the transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. $P_{jmax} = 1$ W. From the results, we can see that the covert secrecy rate R_{cs} decreases with the error detection probability limit ϵ. This is because a larger ϵ requirement leads to stricter covert constraint, and thus the allowed transmit power P_a gets smaller. We can further observe from the results that our proposed scheme is much more effective in covertness compared with other schemes, which is more obvious when there is no zero-forcing applied. This is because the jamming signal inevitably reduces the transmission rate when there is no zero-forcing adopted.

VI. Conclusion

In this paper, we proposed a more secure UAV-assisted covert communication scheme, where a multi-antenna MRT transmitter transmits covertly against a warden assisted by a multi-antenna zero-forcing UAV jammer, to achieve a higher covert secrecy rate while guaranteeing the covertness. The security and performance can be improved with more antennas applied. In addition, this scheme also guarantees the security when the transmission is correctly detected by the warden. Under the worst case of the warden's optimal detection, we jointly optimized the transmit and jamming power to maximize the covert secrecy rate in both detected and undetected situations while guaranteeing the error detection probability and eavesdropping rate both under their limits. Simulation results prove the correctness and effectiveness of our proposed covert scheme. In our future work, we will focus on adapting our scheme to a more complex multi-receiver scenario with the location uncertainty of the warden considered.

References

[1] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "IRS-assisted secure UAV transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, Feb. 2022.

[2] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart. 2023.

[3] X. Chen, N. Zhao, Z. Chang, T. Hämäläinen, and X. Wang, "UAV-aided secure short-packet data collection and transmission," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2475–2486, Apr. 2023.

[4] X. Chen, F. Gao, M. Qiu, J. Zhang, F. Shu, and S. Yan, "Achieving covert communication with a probabilistic jamming strategy," *IEEE Trans. Info. Forensics. Security*, vol. 19, pp. 5561–5574, May 2024.

[5] Y. Bai, H. Zhao, X. Zhang, Z. Chang, R. Jäntti, and K. Yang, "Toward autonomous multi-UAV wireless network: A survey of reinforcement learning-based approaches," *IEEE Commun Surveys Tuts.*, vol. 25, no. 4, pp. 3038–3067, 4th quart. 2023.

[6] X. Yu, D. Li, Z. Wang, and S. Sun, "An integrated new deep learning framework for reliable CSI acquisition in connected and autonomous vehicles," *IEEE Network*, vol. 37, no. 4, pp. 216–222, Jul./Aug. 2023.

[7] Z. Chen, S. Yan, X. Zhou, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface-assisted passive covert wireless detection," *IEEE Trans. Vehi. Tech.*, vol. 73, no. 2, pp. 2954–2959, Feb. 2024.

[8] X. Chen, Z. Chang, N. Zhao, and T. Hämäläinen, "IRS-based secure UAV-assisted transmission with location and phase shifting optimization," in *Proc. IEEE ICC Workshops'23*, pp. 1672–1677, Rome, Italy, 2023.

[9] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Info. Forensics Security*, vol. 17, pp. 760–773, Feb. 2022.

[10] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M.-S. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[11] Y. Zeng, X. Xu, and R. Zhang, "Trajectory design for completion time minimization in UAV-enabled multicasting," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2233–2246, Apr. 2018.