Covert Communication with a Multi-Antenna Warden in Noise Uncertainty UAV-Assisted Wireless Systems

Xiaomeng Xue, Chan Gao, Linying Tian, and Bingbing Xiao
School of Cybersecurity, Xi'an University of Posts and Telecommunications,
Xi'an , Shaanxi, 710121, China

Covert communication ensures the security of information transmission mainly by hiding the existence of the wireless communication process. In this paper, we investigate the covert performance of wireless communication systems in amplify-and-forward unidirectional networks by using unmanned aerial vehicles (UAV) as a relay under the detection from a multi-antenna warden. We propose a cooperative jamming transmission scheme to counteract the detection of a multi-antenna warden that transmits artificial noise of variable power to all participants in a communication system. Based on the transmission scheme, we first develop a theoretical model to derive the expressions for the detection error probability and the optimal detection threshold of the warden. Then, we derive the expressions for the transmission rate to explore the optimal covert performance under a given covertness condition. Finally, the simulation results show the impact of the artificial noise and the noise uncertainty on the covert performance while validating the effectiveness of the scheme.

***Index Terms*—Covert communication, multi-antenna warden, UAV-assisted system, noise uncertainty.**

I. Introduction

With the continuous development of science and technology, wireless communication technology [1] has penetrated all levels of life due to its flexibility, wide range of coverage, and high-speed transmission capability. However, with the rapid popularization of wireless communication technology, information security issues are becoming increasingly prominent, and security risk events such as information leakage [2] and data tampering are occurring frequently. In addressing these challenges, physical layer security (PLS) [3] provides an important protection mechanism, whose core concept is to utilize the physical layer characteristics of communication signals to enhance the security of the communication process. However, the implementation of physical layer security is often affected by channel randomness and environmental conditions [4], and the communication process can still be monitored by illegal third parties. In contrast, covert communications offer a more flexible and effective solution [5].

Covert communication technology aims to hide the existence of the communication process, through which the two communicating parties can securely exchange data in the presence of adversary monitoring, thus reducing the risk of information leakage. Compared to traditional physical layer security, which has stringent requirements on channel characteristics and the signal itself, covert communications can operate effectively in a wide range of environmental conditions and provide superior covertness.

A. Related Works

The participants within the classic covert communication system model mainly include senders, receivers, and detectors [6], and the core goal of the model is to design a communication method that can make the information transfer smoothly under the environment of enemy monitoring. Nowadays, with the rapid development of wireless networks and the diversification of application scenarios in modern covert communication systems, Intelligent Reflecting Surface (IRS) [7] technology and UAV [8] technology show great application potential in the field of covert communication.

Intelligent reflective surface technology, as an emerging technology, enables communication systems to automatically adjust transmission strategies according to environmental changes, reducing signal attenuation and interference [9]. However, its deployment requires consideration of large-scale hardware implementation [10], as well as complex installation and maintenance requirements have greatly increased its cost. UAVs, on the other hand, are capable of rapid deployment, easy and flexible operation, and can be quickly put into use as needed to adapt to changing environments. They can also perform automated flight tasks unattended, relying on advanced navigation and control systems to automatically avoid obstacles and plan flight paths [11]. The advanced sensors and communication equipment carried by UAVs enable them not only to support covert communication but also to realize real-time data collection and detection.

Meanwhile, the integration of UAV technology provides a flexible mobile relay [12] for the wireless communication process. The high mobility of UAVs allows them to travel freely not only among urban skyscrapers but also in remote areas and complex environments to quickly set up temporary communication networks. These unique characteristics allow drones to be used in military, emergency response, and disaster recovery applications [13]. It is also a key tool for the covert transmission of information in these fields.

In covert communication, the information is usually hidden in the noise so that the information is dispersed in the noise to reduce the probability of being detected by Willie, and the

Manuscript received Oct 20, 2024; revised Dec 27, 2024. Corresponding author: Chan Gao (email: gaochan001@163.com).

uncertainty of noise affects the throughput of the concealed system[14], in [15] [16] the addition of artificial noise to enhance the security of information transmission is studied and in [17] a relay based on artificial noise is considered to be used to enhance the confidentiality under the transmission of information from the information source. The authors in [18] consider the covert rate can be achieved under AWGN while the warden is uncertain about the statistics of background noise. [19] suggests that multi-antenna technology can enhance signal quality and coverage, and it is also more effective at mitigating interference from other users or devices. The work in [20] details how to characterize covert rate with a static and known MIMO channel matrix and extends these findings to scenarios where the channel matrix is known but the adversary's matrix is constrained only by its rank and spectral norm. However, all the above works consider a passive warden equipped with an antenna. In practical applications, the warden may use multiple antennas to improve its detection performance. There is still a lot of space for exploration on the impact of multi-antenna warden on covert communication performance.

B. Motivation and Contributions

In this work, we consider the interference of noise on the signal during the communication process as well as the improved ability of a multi-antenna warden to detect the delivery of covert communication with uncertain noise for the first time. We propose a communication jamming scheme to utilize a UAV as a relay in order to amplify and retransmit the signals to improve the quality and coverage of the signals and mitigate the noise effects. At the same time, we introduce a friendly jammer node for broadcasting artificial noise to ensure the covert of the secret message. By designing a transmission scheme to ensure covertness condition under a given threshold, then develop the theoretical models to characterize the impact of system parameters and optimize transmission rates. The main contributions of this paper can be summarized as follows.

- We consider a wireless communication system that consists of several key players, including the source Alice, a UAV the receiver Bob, a friendly jammer, and a multi-antenna warden Willie. We assume the UAV acts as a relay and is responsible for indirectly forwarding the covert messages transmitted by Alice to the destination Bob.
- For this communication process, we consider a warden that can detect the communication behaviors of Alice and Bob from multiple antennas, which makes its coverage and efficiency stronger than a single channel. For a such warden, based on cooperative jamming technology, we design a transmission scheme where the friendly jammer sends noise to all participants in the system to confuse Willie's detection of Alice to improve the covert rate. Meanwhile, we also explore the impact of the noise uncertainty feature on the detection result of the warden. This makes our analysis results more in line with the wireless channels in practical applications.
- Based on the transmission scheme, we first develop a theoretical model to derive the expressions for the detection error probability and the optimal detection threshold of the warden. Then, we derive the expressions for the transmission rate to explore the optimal covert performance under a given covertness condition.
- The transmission scheme is validated by simulation tools and provides a large amount of data that demonstrates a significant improvement in its covert performance. The simulation results show the impact of the artificial noise and the noise uncertainty on covert performance while validating the effectiveness of the scheme.

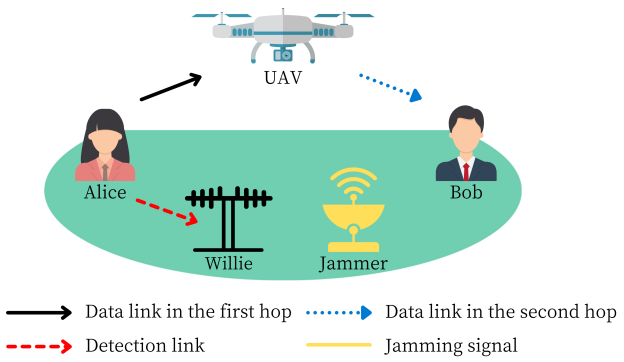

Fig. 1. Covert communication scenario.

For the remainder of the paper, the following structure will be adopted: Section II presents the system model. Section III provides an analysis of the performance under covertness constraints. Section IV discusses the achievable covert rate of the system. Section V employs extensive simulations and data to validate our design, while Section VI offers a summary of the paper.

II. System Model

In this section, we will describe in detail this wireless communication system model that utilizes UAVs as relays with amplification and forwarding, and detail the communication scheme, including transmission and forwarding strategies and jamming methods.

In the first part, we provide a detailed description of each actor in the model and its function and introduce the channel, noise, etc. In the second part, the detector performs a binary hypothesis test based on the received signals and analyzes the two hypotheses in depth to provide the prerequisites for the subsequent covertness requirements.

A. Network Model

The communication scenario is shown in Fig.1, we consider a wireless relay system composed of one source (Alice), one destination (Bob), one friendly jammer, one warden (Willie), and one relay (UAV) in the air. We assume Willie is equipped with L antennas and the other nodes are single-antenna devices. The transmission process is divided into two periods. In the first phase, Alice transmits covert messages to the UAV while Willie detects it. In the second phase, the UAV forwards covert messages to Bob by amplification and forwarding method. It is worth noting that the friendly jammer

transmits jamming signals throughout the process to confuse Willie's detection. We use a quasi-static Rayleigh fading to model the wireless channels in a time-slotted system. With the fading, all channel coefficients keep unchanged within one time slot and change independently from one time slot to another, and follow a complex Gaussian distribution with zero mean and unit variance. For the ground devices, the channel fading coefficients between Alice and Willie and Jammer and Willie are denoted as h_{aw}, h_{jw}, respectively. For air-to-ground channels, we presume that the hovering height of the UAV is H. The channel between the UAV and the ground devices features a Line-of-Sight (LOS) link, and thus we can indicate their channel fading coefficients as

$$h_{un} = \sqrt{\frac{\beta}{\| \mathbf{L_u} - \mathbf{L_n} \|^2 + H^2}}, \ n = a, b, j \tag{1}$$

where $L_a = [x_a, y_a]$, $L_b = [x_b, y_b]$, $L_j = [x_j, y_j]$ and $L_u = [x_u, y_u]$ mean their horizontal positions respectively, β means the wireless channel gain at a reference distance of 1 metre, For the small scale fading, The $|h_{ij}|^2$ is the corresponding channel gain, where $ij \in \{aw, jw, ua, ub, uj\}$. We assume that the channel gain includes the antenna gain of the transmit/receive antennas as well as the distance between any two nodes [21].

In the communication process, Alice wants to transmit the covert message to Bob through the UAV under the Willie's detection. We use a jammer send the jamming signal to confuse Willie in order to achieve covert communication. The signal received by the UAV can be represented as

$$y_u(i) = \sqrt{P_a}|h_{ua}|x_a(i) + \sqrt{P_j}|h_{uj}|x_j(i) + n_u(i), \tag{2}$$

where $x_a(i)$ and $x_j(i)$ are the transmission signal and P_a and P_j are the transmission power by Alice and jammer, respectively. The $n_u(i)$ is the additive noise in the AWGN, and satisfying $n_u(i) \sim \mathcal{CN}(0, \sigma_u^2)$. The UAV amplifies and then forwards the signal to the Bob with power P_u and transmits the signal as

$$x_u(i) = G y_u(i), \tag{3}$$

this is a version of the received signal with G as a linear scale. G is a scalar quantity, and in order to satisfy $E[x_u(i)x_u(i)^\dagger] = 1$, the expression for G is

$$G = \frac{1}{\sqrt{P_a|h_{ua}|^2 + P_j|h_{uj}|^2 + \sigma_u^2}}, \tag{4}$$

Then, the received signal $y_b(i)$ at Bob from UAV is given by

$$y_b(i) = \sqrt{P_u}|h_{ub}|x_u(i) + \sqrt{P_j}|h_{jb}|x_j(i) + n_b(i), \tag{5}$$

where $x_u(i)$ and $x_j(i)$ are the transmission signal and P_u and P_j are the transmission power by UAV and jammer, respectively. The $n_b(i)$ is the AWGN at Bob with variance σ_b^2, i.e.,$n_b(i) \sim \mathcal{CN}(0, \sigma_b^2)$.

B. Hypothesis Test at Willie

In order to determine that Alice committed the act of sending the ciphertext, Willie will perform a binary hypothesis test on the received signal, where he has two alternative hypotheses, H_0 and H_1, where H_0 means that Alice did not send the signal, and H_1 means that Alice sent the signal with the help of the UAV relay.

Based on those two hypotheses, we can express the signal received by the l-th antenna at Willie in the i-th channel use as

$$y_{w_l}(i) = \begin{cases} \sqrt{P_j}|h_{jw_l}|x_j(i) + n_w(i), & H_0 \\ \sqrt{P_a}|h_{aw_l}|x_a(i) + \sqrt{P_j}|h_{jw_l}|x_j(i) + n_w(i), & H_1 \end{cases} \tag{6}$$

where $n_w(i)$ is the AWGN at Willie with variance σ_w^2. The average received power at Willie's l-antenna as

$$P_{w_l} = \frac{1}{N}\sum_{i=1}^{N} |y_{w_l}(i)|^2 \tag{7}$$

where the N is total numbers of channel uses. So the total average received power at Willie as

$$P_w = \mathbb{E}[\sum_{l=1}^{L} P_{w_l}], \tag{8}$$

where $\mathbb{E}[*]$ stands for expectation.

The Neyman-Pearson optimal decision rule aims to minimize Willie¡¯s total detection error probability. Therefore, Willie¡¯s decision rule can be expressed as

$$\overline{P_w} \underset{D_0}{\overset{D_1}{\gtrless}} \tau, \tag{9}$$

in this above equations, τ is the detection threshold selected by Willie, and under the assumptions that H_0 and H_1 hold, D_0 and D_1 denote Willie's choices, respectively.

The average power received by the multi-antenna monitor Willlie can be expressed as

$$P_w = \begin{cases} \sum_{l=1}^{L} P_j|h_{jw_l}|^2 + \sigma_w^2, & H_0 \\ \sum_{l=1}^{L} P_a|h_{aw_l}|^2 + \sum_{l=1}^{L} P_j|h_{jw_l}|^2 + \sigma_w^2, & H_1 \end{cases} \tag{10}$$

Based on the analyses mentioned above, we can calculate Willie's two detection error probabilities as follows

$$\mathbb{P}_F = P(D_1|H_0) \tag{11}$$

$$\mathbb{P}_M = P(D_0|H_1) \tag{12}$$

where $\mathbb{P}_F$ is the probability that Willie incorrectly decides that the alternative hypothesis H_1 is true when, in fact, the null hypothesis H_0 is true, $\mathbb{P}_M$ refers to the probability that when the alternative hypothesis H_1 is actually true, and Willie fails to detect the information, i.e., incorrectly judges H_0 to be true.

Thus, the overall detection error probability for Willie can

be expressed as follows

$$\mathbb{P}_E = \mathbb{P}_F + \mathbb{P}_M. \tag{13}$$

III. Analysis of Detection Performance

The main objective of this subsection is to assess the performance of the system with respect to its covert constraints. In particular, we thoroughly derive the precise values for the two detection error probabilities at Willie. Additionally, we summarize the formula for the total detection error probability at Willie, which incorporates these two detection error probabilities.

Since the probability density function (PDF) of the random variable $|h_{aw_l}|^2$ and $|h_{jw_l}|^2$ is given by

$$f_{|h_{aw_l}|^2,|h_{jw_l}|^2}(x) = e^{-x}, x > 0 \tag{14}$$

using the convolution theorem, the PDF of $\sum_{l=1}^{L}|h_{aw_l}|^2$ and $\sum_{l=1}^{L}|h_{jw_l}|^2$ can be determined as

$$f_{\sum_{l=1}^{L}|h_{aw_l}|^2,\sum_{l=1}^{L}|h_{jw_l}|^2}(x) = \frac{1}{L!}x^L e^{-x}.x > 0 \tag{15}$$

Based on (10), (11) and (12), we can derive the expressions for both the false alarm probability and the missed detection probability as detailed below

$$\begin{aligned}\mathbb{P}_F &= P(\sum_{l=1}^{L}P_j|h_{jw_l}|^2 + \sigma_w^2 > \tau) \qquad (16)\\ &= P\left(\sum_{l=1}^{L}|h_{jw_l}|^2 > \frac{\tau-\sigma_w^2}{P_j}\right)\\ &= \begin{cases}\frac{1}{L!}\Gamma(L+1), & \tau \le \frac{1}{\rho}\widehat{\sigma}_w^2\\ \frac{1}{2L!\ln\rho}[\Upsilon(-\frac{x}{P_j}+\frac{\tau}{P_j},\frac{\widehat{\sigma}_w^2}{\rho},\tau,L)\\ +\ln\frac{\rho\widehat{\sigma}_w^2}{\tau}\Gamma(L+1)], & \frac{1}{\rho}\widehat{\sigma}_w^2 < \tau \le \rho\widehat{\sigma}_w^2\\ \frac{1}{2L!\ln\rho}\Upsilon(-\frac{x}{P_j}+\frac{\tau}{P_j},\frac{\widehat{\sigma}_w^2}{\rho},\rho\widehat{\sigma}_w^2,L), & \tau \ge \rho\widehat{\sigma}_w^2\end{cases}\end{aligned}$$

in which $\Gamma(L) = \int_0^\infty e^{-t}t^{L-1}dt$, $\Upsilon(y_1,x_1,x_2,L) = \int_{y_1}^{\infty}\int_{x_1}^{x_2}y^L e^{-L}\frac{1}{x}dxdy$ and where σ_w^2 is indeterministic and the function is represented as follows

$$f_{\sigma_w^2}(x) = \begin{cases}\frac{1}{2(\ln\rho)x}, & \frac{1}{\rho}\widehat{\sigma}_w^2 \le x \le \rho\widehat{\sigma}_w^2\\ 0, & \text{otherwise.}\end{cases} \tag{17}$$

thus, $\mathbb{P}_F$ can be straightforwardly calculated from the above expression by analyzing it across three different cases.

To simplify our analysis, define $Z = \sum_{l=1}^{L}P_a|h_{aw_l}|^2 + \sum_{l=1}^{L}P_j|h_{jw_l}|^2$. Based on (15), we can calculate the probability density function for Z as follows

$$f_Z(z) = \frac{1}{(L!)^2(P_aP_j)^{L+1}}e^{-\frac{z}{P_j}}Q(y,z,L,c), z > 0 \tag{18}$$

in which $Q(y,z,L,c) = \int_0^\infty[y(z-y)]^L e^{cy}dy$ and $c = \frac{1}{P_j} - \frac{1}{P_a}$. Therefore, $\mathbb{P}_M$ is as follows

$$\begin{aligned}\mathbb{P}_M &= P(\sum_{l=1}^{L}P_a|h_{aw_l}|^2 + \sum_{l=1}^{L}P_j|h_{jw_l}|^2 + \sigma_w^2 < \tau) \qquad (19)\\ &= P\left(Z < \tau - \sigma_w^2\right)\\ &= \begin{cases}0, & \tau \le \frac{1}{\rho}\widehat{\sigma}_w^2\\ \frac{1}{2(L!)^2(P_aP_j)^{L+1}\ln\rho}\Phi(\frac{1}{\rho}\widehat{\sigma}_w^2,\tau,\frac{e^{-\frac{z}{P_j}}}{x},Q), & \frac{1}{\rho}\widehat{\sigma}_w^2 < \tau \le \rho\widehat{\sigma}_w^2\\ \frac{1}{2(L!)^2(P_aP_j)^{L+1}\ln\rho}\Phi(\frac{1}{\rho}\widehat{\sigma}_w^2,\rho\widehat{\sigma}_w^2,\frac{e^{-\frac{z}{P_j}}}{x},Q), & \tau \ge \rho\widehat{\sigma}_w^2\end{cases}\end{aligned}$$

where $\Phi(x_1,x_2,d,Q) = \int_0^{-x+\tau}\int_{x_1}^{x_2}dQ(y,z,L,c)dxdz$

Based on equations (13), (16) and (19), we can determine Willie's overall detection error probability. By analyzing this expression, we can find the optimal detection threshold that minimizes the total error probability.

By calculating the same interval, we can get the total detection error probability of Willie as follows

$$\mathbb{P}_E = \tag{20}$$
$$\begin{cases}\frac{1}{L!}\Gamma(L+1), & \tau \le \frac{1}{\rho}\widehat{\sigma}_w^2\\ \frac{1}{2L!\ln\rho}[\Upsilon(-\frac{x}{P_j}+\frac{\tau}{P_j},\frac{\widehat{\sigma}_w^2}{\rho},\tau,L)+\ln\frac{\rho\widehat{\sigma}_w^2}{\tau}\Gamma(L+1)]\\ +\frac{\Phi(\frac{1}{\rho}\widehat{\sigma}_w^2,\tau,\frac{e^{-\frac{z}{P_j}}}{x},Q)}{2(L!)^2(P_aP_j)^{L+1}\ln\rho}, & \frac{1}{\rho}\widehat{\sigma}_w^2 < \tau \le \rho\widehat{\sigma}_w^2\\ \frac{1}{2L!\ln\rho}\Upsilon(-\frac{x}{P_j}+\frac{\tau}{P_j},\frac{\widehat{\sigma}_w^2}{\rho},\rho\widehat{\sigma}_w^2,L)\\ +\frac{\Phi(\frac{1}{\rho}\widehat{\sigma}_w^2,\rho\widehat{\sigma}_w^2,\frac{e^{-\frac{z}{P_j}}}{x},Q)}{2(L!)^2(P_aP_j)^{L+1}\ln\rho}. & \tau > \rho\widehat{\sigma}_w^2\end{cases}$$

In order to satisfy the covert requirements of the system, we need to find a suitable detection threshold τ^* to minimize the total detection error probability at Willie, and the corresponding minimum total detection error probability is P_E^*.

IV. Performance Analysis and Optimisation

The focus of this section is on the covert rate of covert communication. We analyze covert communication as a unified system, considering the received signal and signal-to-noise ratio at the receiver to determine the final covert rate. To accurately assess this covert rate, we assume that the UAV is used for covertness and reliable.

Regardless of the amount of data transmitted by the source node, the UAV can effectively amplify and forward the concealed information to the receiver. Based on (3), (4), and (5), we can represent the signal received by Bob as

$$\begin{aligned}\mathbf{y}_b(i) &= \sqrt{P_u}|h_{ub}|x_u(i) + \sqrt{P_j}|h_{jb}|x_j(i) + n_b(i),\\ &= \sqrt{P_u}|h_{ub}|G[\sqrt{P_a}|h_{ua}|x_a(i)\\ &+ \sqrt{P_j}|h_{uj}|x_j(i) + n_u(i)]\\ &+ \sqrt{P_j}|h_{jb}|x_j(i) + n_b(i),\end{aligned} \tag{21}$$

using the above equation, we can determine the received signal-to-noise ratio as

$$\gamma_b = \frac{P_u|h_{ub}|^2 G^2 P_a|h_{ua}|^2}{P_u|h_{ub}|^2 G^2 P_j|h_{uj}|^2 + P_u|h_{ub}|^2 G^2 \sigma_u^2 + P_j|h_{jb}|^2 + \sigma_b^2} \tag{22}$$

we can derive the final covert rate of the system as

$$C_b = \log(1+\gamma_b) \tag{23}$$

Since the goal of this communication is to maximize the covert rate achievable by the system, our optimization problem can be summarized as follows

$$\begin{aligned} \text{Maximize} \quad & C_b \\ \textit{s.t.} \quad & \overline{P_E}^* \geq 1-\varepsilon, && \text{(24a)} \\ & P_a, P_j, P_u \leq P_{max}, && \text{(24b)} \\ & \varepsilon \in (0,1), && \text{(24c)} \end{aligned}$$

where ε represents the covert requirement, (23(a)) represents the covert constraint, and (23(b)) represents the range of the transmission and jamming power of Alice, UAV and jammer. The objective function of the optimization problem is an increasing function with respect to the covert transmit power, so the covert rate can be maximized by finding the optimal covert transmit power that satisfies the constraints. It is difficult to solve for the extreme value of τ by substituting τ^* back into (20) because of the expression (20) includes Lambert-W and gamma functions. Therefore, the closed-form expression for the optimal covert transmit power is unavailable with the optimization conditions such that we cannot find an analytical solution of the optimization problem. To this end, we employ an iterative algorithm based on the stochastic gradient descent (SGD) method to solve this optimization problem.

V. Numerical Results

In this section, we will mainly evaluate the performance of the program through simulation. We set specific experimental conditions, including signal strength, noise level, and transmission distance. These parameters are chosen to simulate different scenarios in real applications and help us evaluate the conditions that the system may encounter in actual operation.

A. Detection capability of warden

First, when calculating Willie¡¯s overall detection error rate, we base our numerical calculations on the following assumptions: the jammer's transmission power $P_j = 15$W, noise uncertainty $\rho = 0.2$, the wireless channel gain at a reference distance of 1 meter is 10dB, and Willie¡¯s noise variance is $\sigma_w^2 = 5$dB. We set the square of the UAV's height $H^2 = 900$m, $d_{jw} = 30$m, while allowing the source node Alice to transmit the secret information at powers of $P_a = \{2,3,5\}$W. Without loss of generality, we assume that the total system bandwidth is 1 MHz.

It can be clearly seen from Fig.2 that there is a minimum value of $\overline{P}_E^*$, which verifies our discussion in Section III, and as Alice's transmit power increases, the minimum total detection error rate decreases, because, under the condition that the interference signal remains constant, the larger P_a means that the relative decrease of the interference so the strength of Alice's transmitted signal is greater, which makes it easier for Willie to distinguish between the effective signal and the noise, so that $\overline{P}_E^*$ decreases, Willie has a greater probability of detecting a secret communication.

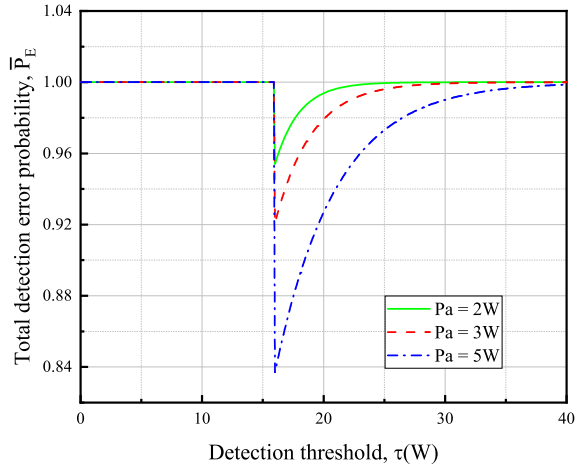

Fig. 2. The impact of the detection threshold on the total detection error probability with three transmission power of Alice.

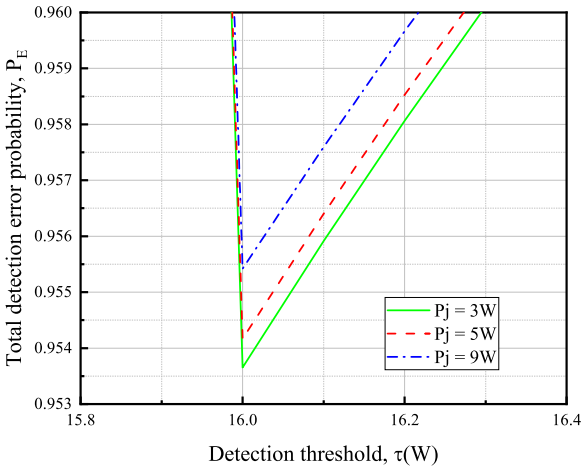

Fig. 3. The impact of the detection threshold on the total detection error probability with three power of Jammer.

We set the source node Alice to transmit signals with $P_a = 2$W, and the interference power is $P_j = \{3,5,9\}$W, so from Fig. 3, we can clearly see that as the interference power increases, the minimum total detection error rate increases, because under the condition that Alice transmits the same amount of power, the larger P_j means the larger interference, and the strength of the signal transmitted by Alice is relatively small. Alice transmits a relatively weak signal, which makes it more difficult for Willie to distinguish a valid signal from the noise.

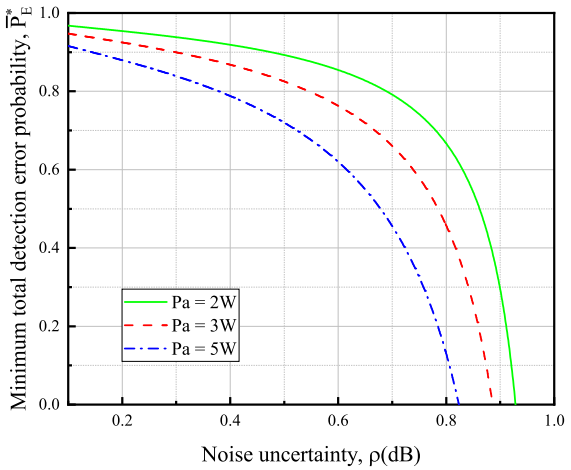

Fig. 4. The impact of the noise uncertainty on the covert transmission rate with three Covertness requirement.

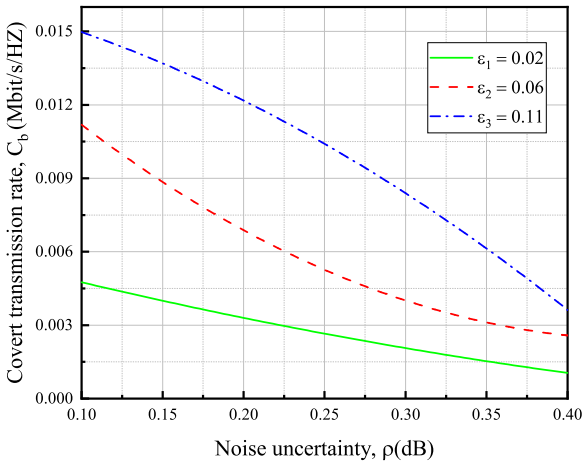

Fig. 5. The impact of the noise uncertainty on the covert transmission rate under three covertness requirements.

Fig.4 is the variation curve of the minimum error detection probability $\overline{P}_E^*$ and the noise uncertainty ρ with the setting of $P_j = 13$W and $|h_{jw}|^2 = 10/30^2$. From Fig.4, it can be clearly observed that the relationship between the minimum error probability of Willie and $\overline{P}_E^*$ decreases as ρ increases. This is because as noise uncertainty increases, the covertness requirement increases accordingly to cope with more complex transmission environments. By changing the value of covert transmission powerP_a, it can be found that the smaller the value of P_a, the larger the $\overline{P}_E^*$, which corroborates with Fig.2.

B. Covert Performance Optimization

By solving optimization problem (24), we analyse the effect of quantifies the size of noise uncertainty ρ dB and covertness requirement ε on the maximum covert rate with the different parameter in Fig.5 and Fig.6, respectively.

Firstly, Fig.5 illustrates that the impact of noise uncertainty ρ dB on the maximum covert rate with the setting of $\varepsilon = \{0.02, 0.06, 0.11\}$, $P_u = 3$W, $|h_{ua}|^2 = |h_{uj}|^2 = |h_{ub}|^2 = 10/(30^2 + 900)$, $|h_{ua}|^2 = 10/25^2$, $d_{jb} = 25$m, and the noise variance of UAV $\sigma_u^2 = -10$dB. We can observe from Fig.5 that with the same covertness requirement ε, as noise uncertainty ρ increases, the covert transmission rate C_b will decrease. This phenomenon is due to that the noise uncertainty is increased, which means that the imperfect knowledge of the channel gain has more impact on the minimum detection error probability of Willie. In light of our preceding theoretical analyses, it can be posited that the detection error probability of Willie is inversely proportional to that of the covert rate. Consequently, Alice can be transmitted at a reduced covert rate, despite the growing detection capabilities of Willie.

Fig.5 also shows that covert rates decreases with increasing covertness requirement ε because of the covert requirement is increased, which means that the covert condition for transmission is reduced and then Alice can use a higher optimal covert transmission power P_a to reduce the negative consequence of transmission outage, resulting in an increase in the maximum covert rate.

Then we vary the background noise at Bob σ_b^2 to investigate the effect of the increasing ε on the covert rate under cooperative jamming scheme with the setting of $P_u = 3$W, $|h_{ua}|^2 = |h_{uj}|^2 = |h_{ub}|^2 = 10/(30^2 + 900)$, $|h_{jb}|^2 = 10/30^2$, $d_{jb} = 30$m, $|h_{jw}|^2 = 10/40^2$, $d_{jw} = 40$m, and the noise variance of the UAV is $\sigma_u^2 = -5$dB. We can observe from Fig.6 that as ε_c increases, the C_b increases. The reason is similar to Fig.4, as the increasing of ε leads to the increasing of the optimal transmission power, which corresponds to an increase in the probability of transmission being detected. A careful observation of Fig.6 indicates that for each fixed ε, as the σ_b^2 increases, the covert rate decreases. The reason of this phenomenon as follows. When σ_b^2 increases, it leads to a decrease in the signal-to-noise ratio at Bob, resulting in a decrease in the decoding rate. Therefore, adjusting the covert transmission power based on background noise, jamming power, and noise uncertainty is critical to covert transmission performance.

VI. Conclusion

In this paper, we investigate the stealth performance of a one-way amplify-and-forward network relay-assisted wireless communication system using UAVs as repeaters. In this scheme, we use a multi-antenna detector and propose an artificial noise-based jamming scheme whereby an artificial noise of variable power is sent to all participants in the communication system by a jammer to counteract the detecting of the multi-antenna detector. In conclusion, simulation results show that the uncertainty of artificial noise transmission has a significant impact on the effectiveness of covert communication as well as the overall performance of the system while validating the effectiveness of the proposed scheme.

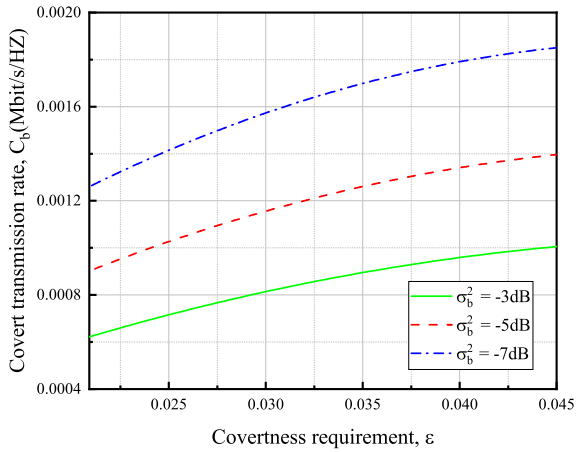

Fig. 6. The impact of the covertness requirement on the covert transmission rate with three background noise at Bob.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China under Grant No. 62072371, the Youth Innovation Team of Shaanxi Universities.

REFERENCES

[1] W. Yang, X. Lu, S. Yan, F. Shu, and Z. Li, "Age of information for short-packet covert communication," *IEEE Wireless Communications Letters*, vol. 10, no. 9, pp. 1890–1894, 2021.

[2] S. K. Sakib, G. T. Amariucai, and Y. Guan, "Variations and extensions of information leakage metrics with applications to privacy problems with imperfect statistical information," *2023 IEEE 36th Computer Security Foundations Symposium (CSF)*, pp. 407–422, 2023.

[3] T. Nazzal and H. Mukhtar, "Evaluation of key-based physical layer security systems," *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)*, pp. 84–87, 2021.

[4] H. Wei, B. Zheng, and X. Hou, "Compressive channel sensing based on random pilot for physical layer communication security," *2013 22nd Wireless and Optical Communication Conference*, pp. 693–698, 2013.

[5] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019.

[6] L. Huang, J. Lei, and Y. Huang, "Spatial modulation covert communication assisted by artificial noise," *2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 1–6, 2023.

[7] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[8] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint optimization of a uav's trajectory and transmit power for covert communications," *IEEE Transactions on Signal Processing*, vol. 67, no. 16, pp. 4276–4290, 2019.

[9] Y. Yang, S. Shen, Y. She, W. Wang, B. Yang, and Y. Gao, "Joint covert and secure communications for intelligent reflecting surface (irs)-aided wireless networks," *2023 International Conference on Networking and Network Applications (NaNA)*, pp. 138–142, 2023.

[10] C. Chen, M. Wang, B. Xia, Y. Guo, and J. Wang, "Performance analysis and optimization of irs-aided covert communication with hardware impairments," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5463–5467, 2023.

[11] Y. Zeng, Q. Wu, and R. Zhang, "Accessing from the sky: A tutorial on uav communications for 5g and beyond," *Proceedings of the IEEE*, vol. 107, no. 12, pp. 2327–2375, 2019.

[12] Z. Wei, M. Zhu, N. Zhang, L. Wang, Y. Zou, Z. Meng, H. Wu, and Z. Feng, "Uav-assisted data collection for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15 460–15 483, 2022.

[13] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K.-K. Wong, "Uav-assisted emergency networks in disasters," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 45–51, 2019.

[14] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2019.

[15] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.

[16] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," *2016 IEEE International Conference on Communications (ICC)*, pp. 1–5, 2016.

[17] P. M. Shemi, M. G. Jibukumar, and M. A. Ali, "Artificial noise aided secrecy enhancement in amplify-and-forward relay networks," *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 192–196, 2018.

[18] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1195–1205, 2015.

[19] Q. Guo, "Application research of multi-antenna technology in 5ghz modulation system," *2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI)*, pp. 158–161, 2022.

[20] S.-Y. Wang and M. R. Bloch, "Covert mimo communications under variational distance constraint," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4605–4620, 2021.

[21] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu and J. Li, "Achieving covert wireless communications using a full-duplex receiver," in *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517-8530, 2018.

Xiaomeng Xue is currently a college student and continues to pursue her B.S. degree in information security from Xi'an University of Posts and Telecommunications. Her research interest focuses on the covert communication in physical layer.

Chan Gao received her B.S. and M.S. degrees in Xi'an University of Posts and Telecommunications, Xi'an, China, in 2014 and 2018, and Ph.D. degree in systems information science from Future University Hakodate, Japan in 2021, respectively. She is currently a assistant professor at Xi'an University of Posts and Telecommunications and is also connected with the National Engineering Laboratory for Wireless Security, Xi'an, China. Her research interest focuses on the covert communication in physical layer.

Linying Tian Linying Tian received her B.S. degree from Xi'an University of Posts and Telecommunications in 2023. From 2023, She continues to pursue her M.S. degree in network and information security from Xi'an University of Posts and Telecommunications. Her research interest focuses on the covert communication in physical layer.

Bingbing Xiao BingbingXiao is a Ph.D. student at the School of Communication and Information Engineering, Xi'an University of Posts and Telecommunications. She research interest focuses on blockchain, public key cryptography and distributed randomness generation.