IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ADVANCED COMMUNICATIONS AND NETWORKING TECHNIQUES FOR WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS

Received May 25, 2020, accepted June 4, 2020, date of current version June 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001069

Performance Analysis for UAV-Jammer Aided Covert Communication

WEI LIANG[1], JIA SHI[2], (Associate Member, IEEE), ZHUANGZHUANG TIE[2], AND FUCHENG YANG[3]

[1]School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China
[2]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China
[3]Research Institute of Information Fusion, Naval Aviation University, Yantai 264000, China

Corresponding author: Jia Shi (jiashi@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61631015, Grant 61941105, and Grant 61825104, and in part by the Shaanxi Natural Fund Youth Project under Grant 2019JQ-075.

ABSTRACT This paper investigates the performance analysis for a novel covert communication system, where a friendly UAV-jammer is used to protect the covert transmission from Alice to Bob against the eavesdropping from Dave. In particular, by exploiting the spatial diversity, the UAV can emit artificial noise (AN) to complicate the noise uncertainty at Dave. In this letter, two scenarios are studied, where the channels from Alice to Bob and Dave experience 1) AWGN and 2) Nakagami-m fading. The closed-form expression for privacy rate expression under AWGN is derived, where evaluating the condition for achieving a positive gain of using UAV-jammer. Furthermore, under the Nakagami-m fading scenario, an approximate expression of ergodic privacy rate is obtained by using Taylor expansion. In the end, simulation results show that significant performance gain in terms of privacy rate can be achieved by employing UAV-jammer for covert communication.

INDEX TERMS UAV, covert communications, performance analysis.

I. INTRODUCTION

Security issues are vital important for wireless networks, where a lot confidential information need to be transmitted over wireless medium. Due to the inherent broadcast feature of wireless links, traditional security techniques, including physical layer security (PLS) approaches [1], [2] and encryption methods [3], were developed to protect information transmission from various types of eavesdropping. Nevertheless, physical layer security is not able to guarantee the amount of information being eavesdropped due to the unpredictable characteristics of wireless channels, while encryption techniques also would be in failure when facing the adversaries with intelligent anti-encryption and powerful computing capabilities.

In future wireless networks, some circumstances, such as military applications and national events, usually require a higher level of security by shielding the existence of the wireless transmission instead of protecting the content of transmitted information against unauthorized eavesdroppers. In that case, PLS and encryption methods will become invalid. Hence, more and more research efforts are catering for such security concerns referred to as covert communications [5]–[8]. The authors in [5] found the fundamental limit of the covert rate being $\mathcal{O}(\sqrt{n})$ over an additive white Gaussian noise (AWGN) channel, where n is the blocklength used with the assumption of $n \to \infty$. Then, Yan *et al.* [6] extended the work to the case of finite blocklength, i.e. $n \leq N$, and proved that the optimal covert rate could be achieved only when $n = N$. More recently, in [7], [8] the covert rate performance was investigated for a one-way relay network with opportunistic relaying scheme employed. Nevertheless, all the current studies strongly rely on the noise uncertainty of wireless networks, which can not be always guaranteed.

On the other hand, unmanned aerial vehicle (UAV) can exploit the flexibility of deployment, which naturally creates a new degree of noise uncertainty for covert communication. In [9] the UAV based jammer was used to improve the security communication between a legitimate transmitter-receiver pair against the eavesdropper, where the intercept probability security region (IPSR) was maximized. By contrast, Wang *et al.* [10] investigated the PLS of the UAV-enabled relaying wireless system, aiming at maximizing the secrecy rate. In addition, the UAV-enabled relaying scheme was

The associate editor coordinating the review of this manuscript and approving it for publication was Bo Zhang.

extended by the work [11] in the context of the terrestrial point-to-point communications, where the UAV's trajectory is optimized for the secrecy capacity.

In recent, very limited studies [12], [13] have investigated the covert communication in the context of the wireless networks with the existence of UAV. In a little more detail, the authors in [12] have evaluated both the security and covert performance of a multi-hop network under the surveillance of UAV. They maximized the achievable throughput of the network by jointly optimizing the coding rates, transmit power, and required number of hops, and revealed that, there exists a trade-off between the security and efficiency in both secrecy and covert communications. By contrast, the authors in [13] proposed to use UAV link for transmitting covert information, which could exploit the spatial diversity. In particular, this work jointly optimized theUAV's trajectory and transmit power in terms of maximizing the average covert transmission rate, when assuming the locations of both the legitimate receiver Bob and the warden Willie were subject to uncertainties. Unfortunately, so far there is no work considering the UAV as a jamming terminal to protect the covert communication link.

The main goal of the covert communication is to ensure the non detectability of the transmission information [14]–[19]. In that case, by introducing jammer it certainly creates the uncertainty at the eavesdropper side. As done in [20], an uniformed jammer was employed to protect the covert communication between legitimate transmitter and receiver. The study showed that the covert transmitter could remain covert with a transmit power that does not decrease with the blocklength n even when warden employed an optimal detector. Furthermore, the works of [21], [22] have proposed to design a full-duplex receiver, which can generates artificial noise with a varying power causing uncertainty at the adversary. They provided the guidelines for the optimal choice of artificial noise power range, and the optimal transmission probability of covert information to maximize the detection errors at the adversary. In comparison with the above approaches, the use of UAV has a better performance to improve the noise uncertainty, and can certainly assist the covert communication, but it should be considered that the eavesdropper can detect the existence of the covert communication through the relevant information of UAV (the appearance of UAV, the level of interference power, UAV speed). If the frequency and mode of UAV use are random and confusing, this situation can be avoided.

Against the above background, in this paper we are motivated to study the performance analysis of the UAV-jammer aided covert communication system. The main contributions can be summarized as follows.

- First, we develop a novel covert communication system with the aid of introducing a friendly UAV-jammer for creating a new degree of noise uncertainty.
- Second, the closed-form expressions for the privacy rate achieved by our covert system are derived under both the AWGN and Nakagami-m fading scenarios. Specifically, we obtain the condition for achieving a positive gain of privacy rate, which suggests when to and how to use the UAV-jammer.
- Last, we evaluate and analyze the performance of our covert communication system. It is shown that, the achievable privacy rate can be significantly improved by introducing the UAV-jammer, which can be deemed to a promising option for meeting future high-level security requirements.

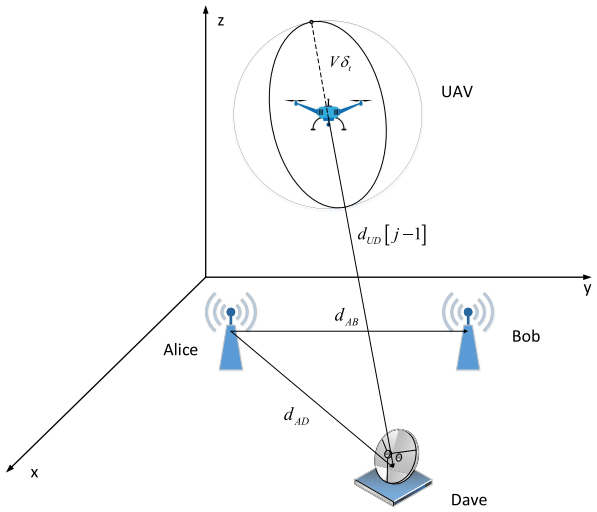

FIGURE 1. System model of the UAV-jamming covert system conceived.

II. SYSTEM MODEL & MAIN ASSUMPTIONS

As shown in Fig. 1, we conceive a covert communication system, which includes, a legitimate transmitter-receiver pair (Alice and Bob), the UAV-enabled jammer, and the eavesdropper Dave. Suppose that, Alice transmits information to Bob with a pre-allocated spectrum, while Dave tries to detect the existence of Alice's transmission. Further, the UAV-enabled jammer is employed to transmit artificial noise (AN) from air to ground, which creates the noise uncertainty at Dave side for protecting the legitimate transmission. Note that, all the nodes in our system are equipped with single antenna.

Let us assume that all the communications happen during the time period t_0, consisting of J consecutive time slots, whose indexes are collected in $\mathcal{J} = \{1, 2, \ldots, J\}$. Suppose that, Alice, Bob and Dave stay still, while the UAV keeps a uniform motion with speed V during t_0. The positions of all the nodes are reflected by the coordinate, such as $c_i = (x_i, y_i, z_i)$. In particular, the coordinates of the ground nodes are denoted by c_A for Alice, c_B for Bob, and c_D for Dave. Hence, the distance for Alice→Bob is $d_{AB} = \|c_A - c_B\|_2$, and that for Alice→Dave is $d_{AD} = \|c_A - c_D\|_2$. Without loss of generality, we assume that, the trajectory of UAV is random, which is not the main focus of this work. At the jth (i.e. $j \in \mathcal{J}$) time instant, $d_{UD}[j]$ for UAV→Dave satisfies

$$d_{UD}[j] \geq d_{UD}^{min}[j] = \|c_U[j-1] - c_D\|_2 - V\delta_t, \quad (1)$$

$$d_{UD}[j] \le d_{UD}^{max}[j] = \|c_U[j-1] - c_D\|_2 + V\delta_t, \quad (2)$$

where $\delta_t = t_0/J$. Note that, similar constraints can be found for $d_{UB}[j]$.

Let us assume, Alice is (or is not) transmitting information during the time slots collected in the set $\hat{\mathcal{J}}$ (or $\tilde{\mathcal{J}}$), where $\mathcal{J} = \hat{\mathcal{J}} \cup \tilde{\mathcal{J}}$. For instance, during time slot j ($j \in \hat{\mathcal{J}}$), Alice transmits N complex valued symbols to Bob, denoted by $\{s[j,n], \forall n\}$, satisfying $s[j,n] \sim \mathcal{CN}(0, P_A[j])$, where $P_A[j]$ is the constant transmit power of each symbol and $n = 1, 2, \ldots, N$. On the other hand, Dave is always passively collecting the symbols, and assume the number of collected channel uses $\tilde{N}$ is relatively large during each time slot. In that case, the received signal power of Bob or Dave is proportion to the distance to Alice, which can be characterized by the free space path loss model, such that $P_{r,B} \propto P_A[j]d_{AB}^{-\alpha}$ or $P_{r,D} \propto P_A[j]d_{AD}^{-\alpha}$ when Alice is transmitting information.

On the other hand, let us denote the AWGN at Bob and Dave as w_B and w_D, where $w_B \sim \mathcal{CN}(0, \Gamma_B)$ is perfectly known by Bob. Whereas, we assume that Dave observes the noise variance uncertainty in the range of $[(1/\rho)\Gamma_D, \rho\Gamma_D]$, where Γ_D is the true noise variance at Dave, and ρ is the uncertainty parameter [16]. In addition, the UAV-jammer can emit AN with power $P_U[j]$, which further complicates the uncertainty of noise variance at Dave. Hence, the uncertainty of Dave's measurements on noise becomes

$$\hat{\Gamma}_D[j] \in \Phi_D[j], \quad j = 1, 2, \ldots, J, \quad (3)$$

$$\Phi_D[j] = \left[1/\rho\Gamma_d + \frac{P_U[j]}{\left(d_{UD}^{min}[j]\right)^{\alpha}}, \rho\Gamma_d + \frac{P_U[j]}{\left(d_{UD}^{max}[j]\right)^{\alpha}}\right] \quad (4)$$

where $P_U[j] > 0$ for UAV emitting, otherwise $P_U[j] = 0$.

A. HYPOTHESIS TESTING AT DAVE

When all the channels are AWGN, to detect Alice's transmission, Dave is always trying to distinguish between the following two signal hypotheses, expressed as

$$H_0 : Y[j,n] = w_D[j,n] + I_U[j,n], \quad (5)$$

$$H_1 : Y[j,n] = s[j,n]\sqrt{\frac{P_A[j]}{d_{AD}^{\alpha}}} + w_D[j,n] + I_U[j,n]. \quad (6)$$

Above, $Y[j,n]$ is the received signal at Dave for the nth sampling during time slot j, and $I_U[j,n] = \frac{P_U[j]}{(d_{UD}[j,n])^{\alpha}}$ is the interference power imposed by the UAV. Further, H_1 (or H_0) denotes the hypothesis that Alice is (or not) transmitting. Let us define that, $P_F = \Pr(D_1 \mid H_0)$ is false alarm probability and $P_M = \Pr(D_0 \mid H_1)$ is misdetection probability, where D_0 and D_1 are the decisions at Dave for noise or signal plus noise. The ultimate goal of Dave is to minimize the error rate of detection, i.e. to minimize the probability of $\xi = P_F + P_M \ge 1 - \epsilon$ for an arbitrary small ϵ.

When radiometer, i.e. energy detector, is employed by Dave, the test statistics for time slot j can be given by

$$T(j) = \frac{1}{N}\boldsymbol{Y}[j]^H\boldsymbol{Y}[j] = \frac{1}{N}\sum_{n=1}^{N} Y[j,n]^* Y[j,n] \ge \Upsilon, \quad (7)$$

where Υ is the detection threshold used by Dave. As a pioneering work, we are motivated to evaluate the covert rate of the system in the presence of friendly UAV-jammer under both AWGN and Nakagami-m fading scenarios.

III. PRIVACY RATE FOR NON-FADING SCENARIO

Let us first consider the non-fading scenario that all the links are AWGN. In [16], the SNR wall was given: Dave cannot detect Alice even if he gathers an infinite number of samples $N \to \infty$ when Alice transmits with an SNR below $\rho - 1/\rho$. Similarly, Dave is assumed to employ the detection metric of the max-min approach on the error rate of ξ over the interval of its noise uncertainty. In this case, the average privacy rate of Alice's transmission can be given by

$$\tilde{R}_{pr} = \frac{1}{J}\sum_{j=1}^{J} \max_{P_A[j] \leftarrow \xi(N, P_U[j])=1} \left\{R_{pr,awgn}[j]\right\}, \quad (8)$$

and defining

$$R_{pr,awgn}[j] = \log_2\left(1 + \frac{P_A[j]}{P_U[j]d_{UB}[j,n]^{-\alpha} + d_{AB}^{-\alpha}\Gamma_B}\right). \quad (9)$$

In this case, upon applying the Central Limit Theorem (CLT) on the chi square distribution of the test statistics for H_0 in (5) and H_1 in (6), the false alarm probability and the detection probability at Dave can be given by

$$P_F[j] = P_r(T(j) > \Upsilon; H_0) = Q_{\chi^2_{2N}}\left(\frac{2N\Upsilon}{\hat{\Gamma}_D[j]}\right), \quad (10)$$

$$P_D[j] = P_r(T(j) > \Upsilon; H_1) = Q_{\chi^2_{2N}}\left(\frac{2N\Upsilon}{\hat{\Gamma}_D[j] + P_A[j]d_{AD}^{-\alpha}}\right), \quad (11)$$

where $\hat{\Gamma}_D[j] \in \Phi_D[j]$. In order to maximize the privacy rate in (9), it needs to find the highest transmit power allowed for Alice while guaranteeing the error rate of detection at Dave is approaching 1, i.e. $\xi \to 1$, which corresponds to the condition that satisfying $P_F[j] \to 1$ or $P_D[j] \to 0$. When considering $N \to \infty$, we can derive the following results:

$$\lim_{N\to\infty} P_F[j] = 1 \ \text{ for } \Upsilon < \hat{\Gamma}_D[j], \quad (12)$$

$$\lim_{N\to\infty} P_D[j] = 0 \ \text{ for } \Upsilon > \hat{\Gamma}_D[j] + P_A d_{AD}^{-\alpha}. \quad (13)$$

For the AWGN scenario, when Alice is not transmitting signals, the following theorem can be derived.

Theorem 1: If Alice is not transmitting signals during time slot j, in order to realize covert communication, one should adjust the uncertainty of the noise variance at Dave to force $P_F[j] \to 1$, thereby setting

$$\hat{\Gamma}_D = \begin{cases} \rho\Gamma_d & \text{w.o. UAV's emission} \\ \rho\Gamma_d - \dfrac{P_U[j]}{\left(d_{UB}^{max}[j]\right)^{\alpha}} & \text{w. UAV's emission} \end{cases} \quad (14)$$

for the case of Dave having the threshold $\Upsilon < \rho\Gamma_d$.

Proof 3.1: When the UAV-jammer is not emitting AN, the noise uncertainty at Dave falls in the range of (4)

for $P_U[j] = 0$. To achieve the result in (10), it simply needs to choose the upper bound of Φ_D for $\hat{\Gamma}_D$. On the other hand, when the UAV-jammer is emitting AN, the noise uncertainty at Dave becomes that in (4) for $P_U[j] > 0$. In that case, by subtracting the received power from the UAV it readily derives the result in the second case of (14) so that $P_F[j] \to 1$ is guaranteed. □

By contrast, the following theorem can be given for deriving the achievable privacy rate when Alice is transmitting signals.

Theorem 2: The privacy rate for Alice's transmission over time period t_0 is given by

$$\tilde{R}_{pr} = \frac{1}{|\hat{\mathcal{J}}|} \sum_{j \in \hat{\mathcal{J}}} \log_2 \left(1 + \frac{P_A^{max}[j] d_{AB}^{-\alpha}}{P_U[j](d_{UB}[j])^{-\alpha} + \Gamma_B} \right) \quad (15)$$

for the case of Dave having $\Upsilon > \rho\Gamma_D$, where $P_A^{max}[j]$ is the maximal transmit power allowed for Alice, defined as

$$P_A^{max}[j] = d_{AD}^{\alpha} \left[(\rho - 1/\rho)\, \Gamma_D + P_U[j]\theta[j] \right]. \quad (16)$$

Proof 3.2: The proof is given in Appendix A. □

Known from Theorem 2, by introducing UAV's emission it can complicate the noise uncertainty at Dave, which in turn enhances the covert rate achieved by the legitimate pair. Nevertheless, there is always a cost that the legitimate receiver, i.e. Bob, also suffers from the UAV's interference. Hence, the following lemma is derived to investigate what is the best condition for employing UAV.

Lemma 1: In order to achieve a positive gain on privacy rate of the legitimate transmitter-receiver pair, the UAV-jammer should emit AN if the following condition is satisfied:

$$(d_{UD}^{max}[j])^{\alpha} > (\rho - 1/\rho)\, \Gamma_D d_{UB}[j] / \Gamma_B + (d_{UD}^{min}[j])^{\alpha} \quad (17)$$

during time slot j, where $j \in \mathcal{J}$.

Proof 3.3: The proof is given in Appendix B. □

IV. PRIVACY RATE FOR NAKAGAMI-*m* FADING SCENARIO

Under Nakagami-m fading scenario, all the system setups are identical to those for AWGN scenario, except that Alice→Bob and Alice→Dave links experience Nakagami-m fading, which are respectively denoted by $h_{AB}[j]$ and $h_{AD}[j]$. Without loss of generality, let us assume that, the channel gains are static during each time slot, and the channel state information (CSI) of the fading channels is known by Alice only. In that case, Alice and Dave maintain the same objectives as the AWGN scenario.

When Alice is not transmitting information, the conclusions derived in Theorem 1 keep the same for Nakagami-m fading scenario. Hence, we are now focus on the case that Alice is transmitting information. In that case, the privacy rate during each time slot, such that in (9), becomes

$$R_{pr,naka}[j] = \log_2 \left(1 + \frac{P_A^{max}[j]|h_{AB}[j]|^2}{P_U[j] d_{UB}[j,n]^{-\alpha} + d_{AB}^{-\alpha}\Gamma_B} \right) \quad (18)$$

where $j \in \hat{\mathcal{J}}$. In particular, we have

$$P_D[j] = Q_{\chi^2_{2N}} \left(\frac{2N\Upsilon}{\hat{\Gamma}_D[j] + P_A[j]|h_{AD}|^2 d_{AD}^{-\alpha}} \right). \quad (19)$$

In order to achieve $P_D[j] \to 0$, it needs to find the maximum allowable transmit power. By applying the same approach used in Theorem 2, the expression for $P_A^{max}[j]$ is derived as follows

$$P_A^{max}[j] = \frac{d_{AD}^{\alpha}}{|h_{AD}[j]|^2} \left[(\rho - 1/\rho)\, \Gamma_D + P_U[j]\theta[j] \right]. \quad (20)$$

When the CSI is available, it can evaluate the average performance of the privacy rate during each time slot, thereby introducing the ergodic rate, defined as

$$R_{pr,naka}^{erg}[j] = E[R_{pr,naka}[j](|h_{AB}[j]|^2/|h_{AD}[j]|^2)]. \quad (21)$$

Due to the property of Nakagami-m fading channels, both $|h_{AB}[j]|^2$ and $|h_{AD}[j]|^2$ follow Gamma distribution, denoted by $|h_{AB}[j]|^2 \sim \Gamma(m_0, \theta_0)$, $|h_{AD}[j]|^2 \sim \Gamma(m_1, \theta_1)$. Specifically, the ergodic privacy rate can be found as follows.

Theorem 3: The ergodic privacy rate for Alice's transmission over time period t_0 is given by

$$\begin{aligned} \tilde{R}_{pr} \approx\ & \frac{1}{\ln(2)} \ln(m_1\theta_1 + bm_0\theta_0) \\ & + \frac{1}{\ln(2)} \left\{ \frac{1}{2(m_1\theta_1 + bm_0\theta_0)^2} m_1\theta_1^2 \right. \\ & \left. + \frac{b^2}{2(m_1\theta_1 + bm_0\theta_0)^2} m_0\theta_0^2 - \psi(m_1) - \ln(\theta_1) \right\} \end{aligned} \quad (22)$$

for the case of Dave having the detection threshold $\Upsilon > \rho\Gamma_D$.

Proof 4.1: The proof is given in Appendix C. □

In Table 1, it evaluates the accuracy of the approximated expression for the ergodic privacy rate, where the degree of difference with the simulation ones are compared. Let us assume that $m_0 = m_1 = m$ and $\theta_0 = \theta_1 = 1$. From the results, we readily obtain the remark below.

Remark 1: When Taylor expansion of order 2 is used, the difference is very small and is acceptable in practice. Furthermore, the higher degree of Taylor polynomials it uses, the worse approximations it derives. This is due to the logarithmic function in (22), which is similar to Runge's phenomenon.

V. SIMULATION RESULTS

In this section, we provide the numerical results to evaluate the performance of the UAV-jammer aided covert communication system. Unless otherwise stated, we have the following system setups: 1) $d_{AB} = d_{AD} = 50$m, $d_{UB}[j-1] = 50$m, $d_{UD}[j-1] = 25$m; 2) α=2; 3) $\Gamma_B = \Gamma_D = 0.1$w, $P_U[j] = P_U = 1$w; 4) $\delta_t = 1$s.

Fig. 2 evaluates the privacy rate of our covert system under AWGN channel, when considering different noise uncertainties and different UAV speeds. First, it observes that, regardless of UAV speed, the privacy rate achieved can be enhanced as the noise uncertainty gets higher. Second, it finds

TABLE 1. Accuracy evaluation of the approximation in Theorem 3.

the value of m \ Degree	2	3	4	5	6
1	0.8480	16.8779	22.5290	77.9253	261.2268
2	0.2179	4.7442	3.1767	7.6862	13.8972
3	0.0964	2.1876	0.9783	2.0269	2.5426
4	0.0539	1.2526	0.4205	0.7981	0.7696
5	0.0344	0.8100	0.2177	0.3904	0.3063

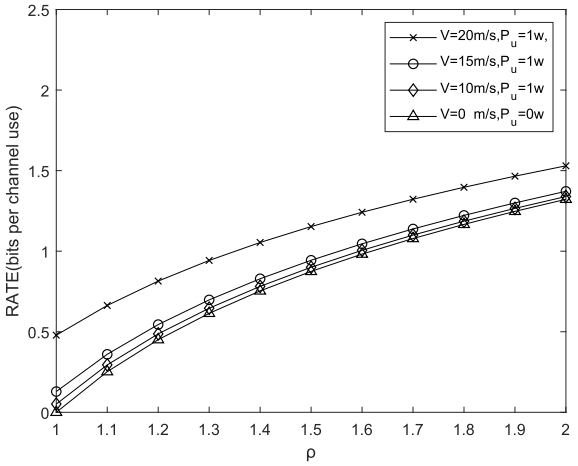

FIGURE 2. Privacy rate v.s. ρ under AWGN channel.

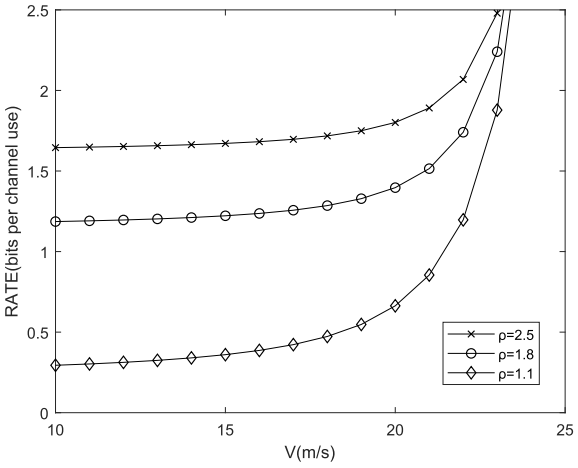

FIGURE 3. Privacy rate v.s. V under AWGN channel.

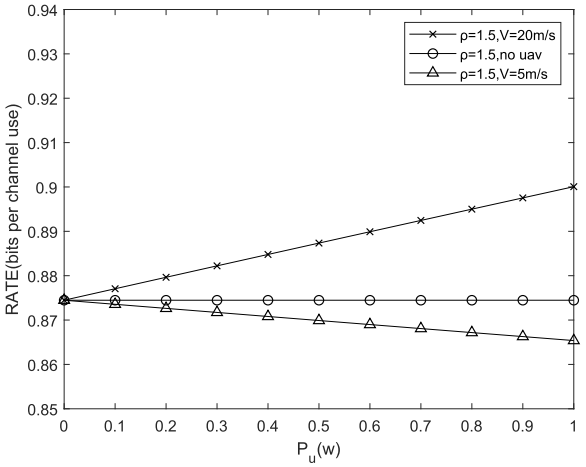

FIGURE 4. Privacy rate v.s. V under AWGN channel.

that, by introducing the UAV-jammer, the privacy rate can be significantly improved, compared to the case without UAV (i.e. the curve of $V = 0$m/s). Furthermore, the faster the UAV speed uses, the higher privacy rate it achieves. At last, when Dave obtains the noise information exactly, that is, when $\rho = 1$, Alice will not be able to transmit covert information without the help of UAV-jammer.

Fig. 3 shows the influence of UAV speed on covert communication rate under different noise uncertainty in AWGN channel. First, it observes that, regardless of noise uncertainty, the privacy rate achieved can be enhanced as the UAV speed gets higher. Secondly, it can be found that the influence of low-speed jamming UAV on the covert communication rate is very small. At this time, the covert communication rate P_U is mainly affected by the noise uncertainty ρ. In addition, when the speed of UAV increases, the rate of covert communication is significantly increased, and the noise uncertainty can no longer effectively affect the rate of covert communication.

In Fig. 4, it shows the privacy rate versus interference power P_U when varying $d_{UB}[j-1]$ and $d_{UD}[j-1]$. It is apparent that, a positive gain in terms of privacy rate can be obtained under the case of $V = 20$m/s as P_U increases, and is much higher than that without UAV. By contrast, for the case of $V = 5$m/s, we set the distances $d_{UB}[j-1] = 25$m, $d_{UD}[j-1] = 50$m, thereby resulting in a negative gain of privacy rate compared to the case without UAV. Therefore, the above two observations can verify the conditions deduced in *lemma*1, which provides the guidelines when and how to employ UAV-jammer for covert communication.

Fig. 5 provides the performance of ergodic privacy rate under the Nakagami-m fading channel. In the simulation, we set $m_0 = m_1 = m$ and θ_1=θ_1=1, and the argument b defined in Appendix C is the effective SINR of legitimate receiver. As shown, the analytical results almost perfectly match the simulation under different values of m, which validates the accuracy of the approximation approach introduced by *Theorem*3. Furthermore, as the fading effect becomes less severe, the achievable privacy rate decreases. This reveals that the condition of eavesdropping channel determines how much covert information can be transmitted.

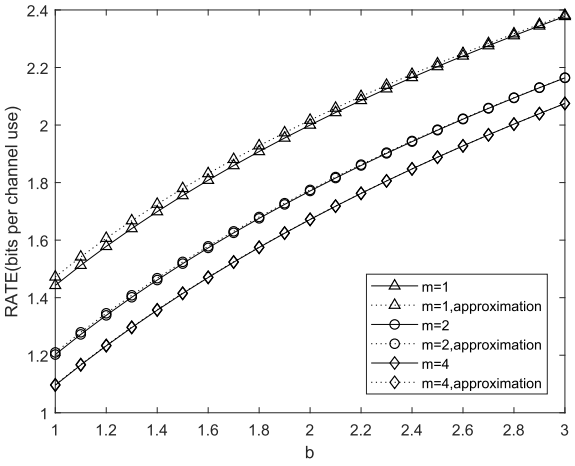

FIGURE 5. Privacy rate under Nakagami-*m* fading channel.

VI. CONCLUSION

This letter has studied the performance analysis for the UAV-jammer aided covert communication system. In order to create a new degree of noise uncertainty at Dave, the UAV can emit artificial noise to protect the covert transmission from Alice to Bob against Dave. Two scenarios have been investigated: the channels from Alice to Bob and Dave experience AWGN and Nakagami-*m* fading, respectively. We have derived the privacy rate expressions for both scenarios. Simulation results have shown that, the privacy rate can be significantly improved by introducing the UAV-jammer, where the positive gain condition under the AWGN scenario is analyzed. Furthermore, for the Nakagami-*m* fading scenario, the approximation of ergodic privacy rate has also been validated with very high accuracy. Therefore, the proposed UAV-jammer aided covert communication can be deemed to a promising option for meeting future high-level security requirements.

APPENDIX A PROOF OF THEOREM 1

When Dave has the threshold $\Upsilon > \rho\Gamma_D$, it is impossible to achieve the target of $P_F[j] \to 1$, since the condition in (12) can never be met regardless of UAV emits AN or not. Instead, it should aim to find achieve the target of $P_D[j] \to 0$. On the other hand, due to the independency of every time slot, one should motivate to maximize the privacy rate during each time slot, formulated as

$$\max_{P_A[j]} \{P_{pr,awag}[j](P_A[j]), \forall j \in \mathcal{J}\}, \tag{23}$$

which is subject to (13). The expression of $P_{pr,awag}[j](P_A[j])$ can be found in (9), which is a monotonic function of $P_A[j]$. In that case, solving problem (23) is equivalent to finding the maximal transmit power for Alice. Hence, the optimal solution can be derived by setting up $\hat{\Gamma}_D = \frac{1}{\rho}\Gamma_D - P_U[j]\theta[j]$ and finding the upper bound of the condition in (13). As a result, we can obtain the following equation:

$$\rho\Gamma_D = \frac{1}{\rho}\Gamma_D - P_U[j]\theta[j] + P_A^{max}[j]d_{AD}^{-\alpha}. \tag{24}$$

From (24), the expression for $P_A^{max}[j]$ is derived. Then, by substituting it into (9) the proof of Theorem 1 is completed.

APPENDIX B PROOF OF LEMMA 1

To ensure a positive gain on the privacy rate, the following condition should be met:

$$R_{pr,awgn}[j] - R_{pr,0} > 0 \tag{25}$$

where $R_{pr,0}$ is the privacy rate without UAV's emission. From Theorem 1, we readily know that

$$R_{pr,0} = \log_2\left(1 + \frac{(\rho - 1/\rho)\,\Gamma_D}{(d_{AD}/d_{AB})^{-\alpha}\Gamma_B}\right). \tag{26}$$

When substituting (26) into (25), the following inequality holds

$$\frac{(\rho - 1/\rho)\,\Gamma_D + P_U[j]\theta[j]}{P_U[j](d_{UB}[j])^{-\alpha} + \Gamma_B} > \frac{(\rho - 1/\rho)\,\Gamma_D}{\Gamma_B}. \tag{27}$$

Applying some manipulations on (27), the condition in Lemma 1 can be obtained, and the proof is completed.

APPENDIX C PROOF OF THEOREM 3

In order to obtain an approximate solution of (21), a Taylor expansion is performed thereon. In order to minimize the approximation error of Taylor expansion, (21) is first transformed as follows

$$\begin{aligned}
&R_{pr,naka}^{erg}[j] \\
&= E\left[\log_2\left(1 + b\frac{|h_{AB}[j]|^2}{|h_{AD}[j]|^2}\right)\right] \\
&= \frac{1}{\ln 2}E\left[\ln\left(|h_{AD}[j]|^2 + b|h_{AB}[j]|^2\right) - \ln\left(|h_{AD}[j]|^2\right)\right] \\
&= \frac{1}{\ln 2}\left\{\underbrace{E\left[\ln\left(|h_{AD}[j]|^2 + b|h_{AB}[j]|^2\right)\right]}_{Q_1}\right. \\
&\quad \left. - \underbrace{E\left[\ln\left(|h_{AD}[j]|^2\right)\right]}_{Q_2}\right\},
\end{aligned} \tag{28}$$

where $b = \frac{d_{AD}^{\alpha}[(\rho-1/\rho)\Gamma_D + P_U[j]\theta[j]]}{d_{AB}^{-\alpha}[P_U[j]d_{UB}[j,n]^{-\alpha} + \Gamma_B]}$. Then, a second-order Taylor expansion is performed at $(m_0\theta_0, m_1\theta_1)$ on the first term in (28).Therefore, Q_1 can be rewritten as follows

$$\begin{aligned}
Q_1 &= E\left[\ln\left(|h_{AD}[j]|^2 + b|h_{AB}[j]|^2\right)\right] \\
&= E\left[\ln\left(m_1\theta_1 + bm_0\theta_0\right)\right. \\
&\quad + \frac{1}{2(m_1\theta_1 + bm_0\theta_0)^2}\left(|h_{AD}[j]|^2 - m_1\theta_1\right)^2 \\
&\quad \left. + \frac{b^2}{2(m_1\theta_1 + bm_0\theta_0)^2}\left(|h_{AB}[j]|^2 - m_0\theta_0\right)^2\right] \\
&= \ln\left(m_1\theta_1 + bm_0\theta_0\right) + \frac{1}{2(m_1\theta_1 + bm_0\theta_0)^2}m_1\theta_1^2 \\
&\quad + \frac{b^2}{2(m_1 + bm_0)^2}m_0\theta_0^2.
\end{aligned} \tag{29}$$

Note that, $m_0\theta_0$ and $m_0\theta_0^2$ are the mean and variance of $|h_{AB}[j]|^2$, and the same conclusion applies to $||h_{AD}[j]|^2$.The second term in (28) can be calculated as

$$Q_2 = \psi(m_1) + \ln(\theta_1), \tag{30}$$

where ψ is the digamma function. From (29) and (30), the expression for (22) is derived, then the proof of Theorem 3 is completed.

REFERENCES

[1] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.

[2] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for MISO wiretap channels with channel uncertainty," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2096–2099, Nov. 2013.

[3] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[4] J. S. Hu, F. Shu, and J. Li, "Robust synthesis method for secure directional modulation with imperfect direction angle," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1084–1087, Jun. 2016.

[5] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[6] S. Yan, B. He, Y. Cong, and X. Zhou, "Covert communication with finite blocklength in AWGN channels," *Proc. IEEE ICC*, Paris, France, May 2017, pp. 1–6.

[7] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert communication in wireless relay networks," in *Proc. IEEE GlobeCom*. Singapore: Singapore, Dec. 2017, pp. 1–6.

[8] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 7, pp. 4766–4779, Jul. 2018.

[9] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280–11284, Nov. 2018.

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

[11] L. Shen, N. Wang, and X. Mu, "Iterative UAV trajectory optimization for physical layer secure mobile relaying," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Zhengzhou, China, Oct. 2018, pp. 19–194.

[12] H.-M. Wang, Y. Zhang, X. Zhang, and Z. Li, "Secrecy and covert communications against UAV surveillance via multi-hop networks," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 389–401, Jan. 2020.

[13] 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 Trans. Signal Process.*, vol. 67, no. 16, pp. 4276–4290, Aug. 2019.

[14] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 2945–2949.

[15] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[16] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp. 4–17, Feb. 2008.

[17] J. Zhang, T. Chen, S. Zhong, J. Wang, W. Zhang, X. Zuo, R. G. Maunder, and L. Hanzo, "Aeronautical ad hoc networking for the Internet-above-the-clouds," *Proc. IEEE*, vol. 107, no. 5, pp. 868–911, May 2019.

[18] J.-K. Zhang, S. Chen, R. G. Maunder, R. Zhang, and L. Hanzo, "Adaptive coding and modulation for large-scale antenna array-based aeronautical communications in the presence of co-channel interference," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1343–1357, Feb. 2018.

[19] J. Zhang, S. Chen, R. G. Maunder, R. Zhang, and L. Hanzo, "Regularized zero-forcing precoding-aided adaptive coding and modulation for large-scale antenna array-based air-to-air communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2087–2103, Sep. 2018.

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

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

[22] F. Shu, T. Xu, J. Hu, and S. Yan, "Delay-constrained covert communications with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. 8, no. 3, pp. 813–816, Jun. 2019.