

Power Control for UAV-Aided Multiuser Covert IoT Communications Against Colluding Wardens

Yumei Yang, Honghui Cha, Fei Lin, Ruquan Wang, and Wu Wang

School of Mathematics and Computer Science, Yunnan Minzu University, Kunming, Yunnan 650504, China

Unmanned aerial vehicles (UAVs) can rapidly provide wireless access for Internet of Things (IoT) users in emergency, remote, and temporary service scenarios, whereas their line-of-sight air-ground links make signal transmission susceptible to detection. This paper explores a multi-user UAV-aided covert IoT communication system, in which ground wardens improve their detection performance through collusion. The UAV serves legitimate users sequentially along a predefined trajectory. A portion of wardens shares detection observations and forms a super-warden via equal-gain combining. Under noise uncertainty, this paper derives the optimal detection thresholds and the minimum total detection error probability expressions for independent wardens and super wardens. Subsequently, an average covert transmission rate maximization problem is formulated under covertness constraints, peak power constraints, and average power budgets. Through equivalent transformation of covertness constraints, the original problem is converted into a convex optimization problem and solved using the CVX tool. Finally, numerical results verify the theoretical analysis and illustrate the influences of collusion strength, flight altitude, transmit power and other factors on the system's covert performance.

Index Terms—Covert communication, UAV-aided IoT, colluding wardens, energy detection, noise uncertainty, power control.

I. INTRODUCTION

THE Internet of Things (IoT) is pushing wireless networks toward dense, heterogeneous, and delay-sensitive connectivity [1], [2], [3]. In special scenarios such as complex terrain, remote mountainous areas, and disaster rescue, traditional terrestrial base stations are constrained by long deployment cycles, high maintenance costs, and limited coverage, making it difficult to provide timely and comprehensive communication services [4], [5], [6].

As a flexible aerial communication node, the unmanned aerial vehicle (UAV) has gradually become an important technical approach to compensate for insufficient ground network coverage and improve overall system performance, benefiting from its high mobility in three-dimensional space, on-demand dynamic deployment capability, and superior line-of-sight transmission conditions [7], [8]. UAV communication exhibits irreplaceable application value in high-security scenarios such as disaster rescue, military reconnaissance, and border patrol [9], [10].

However, the broadcast nature of wireless channels poses severe security threats to UAV communication [11]. Due to the inherent openness and broadcast characteristics of wireless channels, the signal transmission of UAVs faces a higher risk of exposure, increasing the probability of interception by malicious nodes and leading to potential data leakage and system security threats [12]. Traditional encryption technologies mainly protect data content at the upper network layers, making it difficult to hide the physical characteristic that communication is taking place. In scenarios with high concealment requirements, encryption techniques are likely to attract attention and interference from non-cooperative parties [13]. Therefore, covert communication technology, which aims to hide the existence of communication behavior, has emerged.

Its core idea is to exploit the randomness of the channel environment to hide legitimate signals in background noise, thereby reducing the probability of communication being detected [14], [15], [16].

Covert communication has been widely studied in wireless systems and gradually extended from traditional terrestrial networks to new application scenarios such as UAV-aided communication. In [17], the authors investigate the UAV-aided integrated sensing and communication (ISAC) scenario, and maximize the minimum achievable communication rate of ground users by jointly optimizing UAV power allocation, flight trajectory, and multi-user scheduling under radar sensing performance and covertness constraints. In [18], the authors study the UAV-aided bidirectional air-ground covert communication in low-altitude networks, and maximize the weighted average covert transmission rate by jointly optimizing multi-user association, transmit power, and UAV trajectory under bidirectional covertness constraints. In [19], a multi-user UAV joint covert and secure communication system based on channel inversion power control (CIPC) is studied, and the average effective covert rate is maximized by jointly optimizing rotor/fixed-wing UAV trajectories, transmit power, and user scheduling under security and covertness constraints. In [20], uplink NOMA-based UAV networks are considered, and multi-user cooperative secure and covert communication is investigated, maximizing the total secure and covert rate by jointly optimizing UAV trajectory, kinematic parameters, and ground user transmit power and beamforming under covertness and security constraints.

Moreover, covert communication with multiple detectors has also been investigated. In [21], the authors investigate covert communication schemes to resist detection by multiple colluding wardens in a UAV relay-enabled terahertz system, derive the detection error probabilities corresponding to two collusion detection strategies, and maximize the system covert throughput by jointly optimizing transmission power and

interference power. In [22], a cooperative jamming strategy for joint covert and secure transmission in untrusted relay networks is proposed, and the trade-off that more relays increase secrecy rate but decrease detection error probability is revealed. In [23], multi-antenna covert communication is analyzed via a stochastic geometry framework, showing that maximum covert throughput is independent of jammer density and power, and centralized systems outperform distributed ones.

In summary, existing research has laid a solid foundation for covert UAV communication and collusion detection among multiple detectors. However, there remains room for further advancement in two aspects: first, most studies focus on the joint optimization of trajectory, power, and user scheduling, but generally assume that eavesdroppers are independent or only a single eavesdropper exists, without considering collusive behavior among multiple detectors; the (m, M) collusion model has not yet been introduced into the context of covert UAV communication, thus failing to quantitatively characterize how collusion intensity degrades the performance of covert communication. Second, most work targets static ground-based communication networks, neglecting the line-of-sight-dominated air-to-ground channel and the time-varying channel gain characteristics caused by UAV mobility; furthermore, many studies rely on ideal noise assumptions.

This paper investigates the power optimization problem of UAV-assisted covert communication in a multi-detector collusion scenario. The core differences and main innovations compared to existing works are summarized as follows:

- **Scenario Construction Innovation:** This paper introduces the classic (m, M) collusion framework into the UAV-assisted covert communication scenario and further improves the collusion node selection mechanism. Different from existing studies that adopt random or fixed collusion strategies, this work selects the m wardens with the strongest detection capability according to their average distance to the UAV flight trajectory to form the collusion group, which constructs a super detector via equal gain combining (EGC) for joint detection, while the remaining $(M - m)$ wardens work independently. The proposed refined collusion model characterizes the worst-case intelligent collusion attack and unifies various typical detection scenarios, including single-detector detection, fully independent monitoring, and full collusion, which is more practical for UAV covert adversarial environments.
- **Theoretical Derivation Innovation:** Based on the noise uncertainty model, we derive closed-form expressions for the optimal detection thresholds of both independent detectors and the super detector, as well as their corresponding minimum total detection error probabilities. These derivations quantitatively reveal how collusion strength, UAV position, and transmit power affect the detection performance at the eavesdropper side, laying a theoretical foundation for establishing subsequent covert constraints.
- **Optimization Method Innovation:** We formulate the maximization of the average covert transmission rate as an optimization problem subject to independent-detector

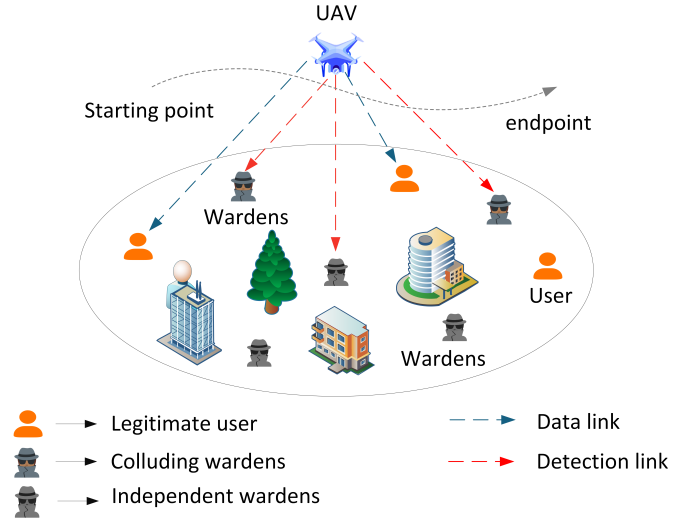


Fig. 1. UAV-aided covert IoT communication network with multiple wardens.

covertiness constraints, super-detector covertness constraints, and UAV power constraints. Addressing the complex initial forms of the covertness constraints, we transform them into standard linear convex constraints through rigorous algebraic identity transformations based on physical premises. This approach realizes an equivalent transformation of the original optimization problem, which is then efficiently solved using the CVX tool.

The rest of this paper is organized as follows. Section II describes the system model. Section III analyzes the detection performance of independent detectors and the super-detector. Section IV formulates and solves the optimization problem. Section V presents numerical results and analysis. Section VI concludes the paper.

II. SYSTEM MODEL

A. System Description

As shown in Fig. 1, this paper considers a multi-user covert communication network based on unmanned aerial vehicles (UAVs). The network consists of one UAV, K legitimate users, and M wardens. Both the legitimate users and wardens are located on the ground. The UAV flies at a fixed altitude H along a predetermined trajectory from the start point to the end point, and covertly transmits messages to the legitimate ground users in sequence during the flight. The M wardens are distributed in the network, aiming to detect whether information transmission occurs between the UAV and the legitimate users.

B. Warden Collusion Model

According to the research in [24], this paper adopts a collusion model to depict the multi-detector scenario. There are a total of M wardens in the model, and given the collusion strength m , the collusion group selects m monitoring nodes with the strongest detection capability for the UAV. Specifically, the average distance of each monitoring node

from the UAV's flight trajectory is calculated, and the m nodes with the closest average distance form the collusion group. Nodes share the received observation information to complete joint detection with equal gain combining. The remaining $(M - m)$ monitoring nodes maintain independent detection. The parameter m is defined as the collusion strength, representing the number of monitoring nodes participating in the collusion. Within this collusion group, a super detector w_z is designated to collect the signal energy received by all collusion detectors. Subsequently, the equal gain combining (EGC) technique is adopted, and these energy values are linearly added to determine whether the UAV is in transmission state. This model has good universality and can describe various special cases, including single detector, independent detectors, and complete collusion among all detectors. Physically, the closer the monitoring node is to the UAV's trajectory, the higher the average channel gain, and the stronger the detection capability. Therefore, the average trajectory distance is used as the physical criterion for selecting collusion nodes.

C. Channel Model

We use $\mathbf{q}_{b_k} = [x_{b_k}, y_{b_k}]^T$ to denote the horizontal location of the k -th legitimate user, and $\mathbf{q}_{w_j} = [x_{w_j}, y_{w_j}]^T$ to denote the horizontal location of the j -th independent warden, where $j \in \{m+1, m+2, \dots, M\}$. In the scenario with m colluding wardens ($w_1, \dots, w_v, \dots, w_m, v \in \{1, 2, \dots, m\}$), $\mathbf{q}_{w_z} = [x_{w_z}, y_{w_z}]^T$ denotes the horizontal location of the super detector, and $\mathbf{q}_a = [x_a, y_a]^T$ denotes the horizontal location of the UAV. We assume that the UAV flies at a fixed altitude above the ground, denoted by H , which can be regarded as the minimum altitude to avoid collisions with ground obstacles. The flight period and the maximum flight speed of the UAV are denoted by T and $V_{\max}$, respectively. The initial location of the UAV is denoted by $\mathbf{q}_{a,0} = [x_{a,0}, y_{a,0}]^T$, and the final location is denoted by $\mathbf{q}_{a,F} = [x_{a,F}, y_{a,F}]^T$.

The UAV is fixed at an altitude that satisfies the line-of-sight (LoS) link condition. We equally divide the flight period T into N time slots, i.e., $T = N\delta_t$. The duration of each time slot is set sufficiently small so that the UAV's position can be approximately considered constant within each time slot. Therefore, the coordinate of the UAV can be expressed as $\mathbf{q}_a(n) = [x_a(n), y_a(n)]^T$, where $n \in \{1, 2, 3, \dots, N\} = \mathbb{N}$. The UAV serves users sequentially in order, and we fix the UAV's trajectory such that it flies from the starting point to the endpoint in a straight line.

We denote the transmit power of the UAV at the n -th time slot by $P_a[n]$, where $P_{a,\max}$ is the peak transmit power and $\bar{P}_{a,\max}$ is the maximum average transmit power.

$$0 \leq P_a[n] \leq P_{a,\max}, \quad \forall n \quad (1a)$$

$$\frac{1}{N} \sum_{n=1}^N P_a[n] \leq \bar{P}_{a,\max} \quad (1b)$$

At the n -th time slot, the channel power gains from the UAV to the k -th legitimate user, the j -th independent warden, and the super detector are respectively given by

$$|h_{a,b_k}[n]|^2 = \frac{\eta_0}{\|\mathbf{q}_a[n] - \mathbf{q}_{b_k}\|^2 + H^2} \quad (2a)$$

$$|h_{a,w_j}[n]|^2 = \frac{\eta_0}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} \quad (2b)$$

$$|h_{a,w_z}[n]|^2 = \frac{\eta_0}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_z}\|^2 + H^2} \quad (2c)$$

where η_0 denotes the channel power gain at the reference distance of 1 meter.

D. Detection Model at Willie

The detection process at Willie results in a binary hypothesis testing problem. In covert communication, Willie must determine whether a transmission between the UAV and the legitimate user has occurred based on his observations. For the i -th channel use in the n -th time slot, the received signals at detectors w_j and w_z are given by

$$y_{w_j}^i[n] = \begin{cases} n_{w_j}(i), & \mathcal{H}_0 \\ \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2}} x(i) + n_{w_j}(i), & \mathcal{H}_1 \end{cases} \quad (3a)$$

$$y_{w_z}^i[n] = \begin{cases} \sum_{v=1}^m n_{w_v}(i), & \mathcal{H}_0 \\ \sum_{v=1}^m \left(\sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} x(i) + n_{w_v}(i) \right), & \mathcal{H}_1 \end{cases} \quad (3b)$$

where $\mathcal{H}_0$ denotes the null hypothesis that the UAV does not transmit any signal, and $\mathcal{H}_1$ denotes the alternative hypothesis that the UAV transmits a signal. Here, $x(i)$, $i = 1, 2, \dots, f$ denotes the signal transmitted by the UAV, satisfying $\mathbb{E}[|x(i)|^2] = 1$, where f is the total number of channel uses in the n -th time slot. $y_{w_j}^i[n]$ denotes the signal received by the independent detector w_j ($j \in \{m+1, m+2, \dots, M\}$) at the i -th channel use, and $y_{w_z}^i[n]$ denotes the signal received by the super detector w_z at the i -th channel use. $n_{w_j}(i)$ is the additive white Gaussian noise at detector w_j with variance $\sigma_{w_j}^2$, and $n_{w_v}(i)$ is the additive white Gaussian noise at colluding detector w_v with variance $\sigma_{w_v}^2$.

The detector's correct detection is to accept the null hypothesis H_0 when it is true and reject it when it is false. At the n -th time slot, the optimal detection rules for wardens w_j and w_z are expressed as follows [25]:

$$\begin{cases} \bar{P}_{w_j}[n] = \frac{1}{f} \sum_{i=1}^f |y_{w_j}^i[n]|^2 \leq \tau_j[n], & D_0 \\ \bar{P}_{w_j}[n] = \frac{1}{f} \sum_{i=1}^f |y_{w_j}^i[n]|^2 > \tau_j[n], & D_1 \end{cases} \quad (4a)$$

$$\begin{cases} \bar{P}_{w_z}[n] = \frac{1}{f} \sum_{i=1}^f |y_{w_z}^i[n]|^2 \leq \tau_z[n], & D_0 \\ \bar{P}_{w_z}[n] = \frac{1}{f} \sum_{i=1}^f |y_{w_z}^i[n]|^2 > \tau_z[n], & D_1 \end{cases} \quad (4b)$$

where $\bar{P}_{w_j}$ and $\bar{P}_{w_z}$ are the average power per received symbol at w_j and w_z , respectively; f is the number of channel uses in each time slot; $\tau_j[n]$ and $\tau_z[n]$ are the detection

thresholds of w_j and w_z in the n -th time slot, respectively; and D_0 and D_1 are the decisions supporting H_0 and H_1 , respectively. We assume that there are an infinite number of channel uses in each time slot, i.e., $f \rightarrow \infty$.

Since there are an infinite number of channel uses in each time slot, the optimal detection rules for detectors w_j and w_z in the n -th time slot can be reformulated as

$$\bar{P}_{w_j}[n] = \begin{cases} \sigma_{w_j}^2, & \mathcal{H}_0 \\ \frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \sigma_{w_j}^2, & \mathcal{H}_1 \end{cases} \quad (5a)$$

$$\bar{P}_{w_z}[n] = \begin{cases} \sum_{v=1}^m \sigma_{w_v}^2, & \mathcal{H}_0 \\ \left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \sum_{v=1}^m \sigma_{w_v}^2, & \mathcal{H}_1 \end{cases} \quad (5b)$$

Furthermore, we consider a noise uncertainty model, where $\sigma_{w_j}^2$ and $\sigma_{w_v}^2$ are random variables with known distributions. Specifically, the noise at detectors w_j and w_z follows a log-uniform distribution. The probability density function (PDF) of the noise at the j -th independent detector w_j is defined as

$$f_{\sigma_{w_j}^2}(x) = \begin{cases} \frac{1}{2 \ln(\rho_j)x}, & \text{if } \frac{1}{\rho_j} \hat{\sigma}_j^2 \leq x \leq \rho_j \hat{\sigma}_j^2, \\ 0, & \text{otherwise.} \end{cases} \quad (6)$$

where ρ_j denotes the noise uncertainty, and $\hat{\sigma}_j^2$ is the nominal noise power. $\rho_{j1} = \frac{1}{\rho_j} \hat{\sigma}_j^2$, $\rho_{j2} = \rho_j \hat{\sigma}_j^2$.

In this work, we assume that the noise samples of all colluding wardens are fully-correlated. Accordingly, the aggregate noise variance of the super-detector satisfies $\sigma_z^2 = m\sigma_v^2$. Subject to noise uncertainty, the aggregated noise power follows a log-uniform distribution, whose probability density function is given by the following equation. The probability density function (PDF) of the noise at the super detector w_z is defined as

$$f_{\sigma_{w_z}^2}(y) = \begin{cases} \frac{1}{2 \ln(\rho_z)y}, & \text{if } \frac{1}{\rho_z} \hat{\sigma}_z^2 \leq y \leq \rho_z \hat{\sigma}_z^2, \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

where ρ_z denotes the noise uncertainty, and $\hat{\sigma}_z^2$ is the nominal noise power. Here, $\hat{\sigma}_z^2 = m\sigma_v^2$ and $\sigma_{w_z}^2 = \sum_{v=1}^m \sigma_v^2$. We also define $\rho_{z1} = \frac{1}{\rho_z} \hat{\sigma}_z^2$ and $\rho_{z2} = \rho_z \hat{\sigma}_z^2$.

In this work, we denote the false alarm rate and missed detection rate of the independent detector w_j in the n -th time slot as $P_{F_j}[n] = \Pr\{D_1|\mathcal{H}_0\}$ and $P_{M_j}[n] = \Pr\{D_0|\mathcal{H}_1\}$, which can be written as

$$P_{F_j}[n] = \Pr\{\sigma_{w_j}^2 \geq \tau_j[n]\} \quad (8)$$

and

$$P_{M_j}[n] = \Pr\left\{ \frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \sigma_{w_j}^2 \leq \tau_j[n] \right\} \quad (9)$$

We denote the false alarm rate and missed detection rate of the super detector w_z in the n -th time slot as $P_{F_z}[n] =$

$\Pr\{D_1|\mathcal{H}_0\}$ and $P_{M_z}[n] = \Pr\{D_0|\mathcal{H}_1\}$, which can be written as

$$P_{F_z}[n] = \Pr\left\{ \sum_{v=1}^m \sigma_{w_v}^2 \geq \tau_z[n] \right\} \quad (10)$$

and

$$P_{M_z}[n] = \Pr\left\{ \left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \sum_{v=1}^m \sigma_{w_v}^2 \leq \tau_z[n] \right\} \quad (11)$$

Then, the total error rate of the independent detector w_j in the n -th time slot is given by

$$\xi_j[n] = P_{F_j}[n] + P_{M_j}[n], \quad \forall n. \quad (12)$$

The total error rate of the super detector w_z in the n -th time slot is given by

$$\xi_z[n] = P_{F_z}[n] + P_{M_z}[n], \quad \forall n. \quad (13)$$

III. DETECTION PERFORMANCE AT WILLIE'S RECEIVERS

Based on the foregoing analysis, we have derived the total error rates for the independent detector w_j and the super detector w_z . In what follows, we first derive the optimal detection thresholds $\tau_j^*[n]$ and $\tau_z^*[n]$ from Willie's perspective to minimize the total error rates $\xi_j^*[n]$ and $\xi_z^*[n]$. We then design the UAV transmit power such that the minimum total error rates of all independent wardens and the super-detector satisfy $\xi_j^*[n] \geq 1 - \varepsilon_1$, $\forall j, n$ and $\xi_z^*[n] \geq 1 - \varepsilon$.

A. Detection Performance of Independent Wardens

Based on (8) and (9), the false alarm rate and missed detection rate of independent detector w_j at time slot n are expressed as

$$P_{F_j}[n] = \begin{cases} 1, & \tau_j[n] < \frac{\hat{\sigma}_j^2}{\rho_j}, \\ \varphi_1[n], & \frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] \leq \rho_j \hat{\sigma}_j^2, \\ 0, & \tau_j[n] > \rho_j \hat{\sigma}_j^2. \end{cases} \quad (14a)$$

$$P_{M_j}[n] = \begin{cases} 0, & \tau_j[n] < Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}, \\ \varphi_2[n], & Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] \leq Q_j[n] + \rho_j \hat{\sigma}_j^2, \\ 1, & \tau_j[n] > Q_j[n] + \rho_j \hat{\sigma}_j^2. \end{cases} \quad (14b)$$

where $Q_j[n] = \frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2}$, and

$$\varphi_1[n] = \int_{\tau_j[n]}^{\rho_j \hat{\sigma}_j^2} \frac{1}{2 \ln(\rho_j)x} dx = \frac{1}{2 \ln(\rho_j)} \ln \left(\frac{\rho_j \hat{\sigma}_j^2}{\tau_j[n]} \right), \quad (15a)$$

$$\varphi_2[n] = \int_{\frac{\hat{\sigma}_j^2}{\rho_j}}^{\tau_j[n] - Q_j[n]} \frac{1}{2 \ln(\rho_j)x} dx = \frac{\ln \left(\frac{\rho_j(\tau_j[n] - Q_j[n])}{\hat{\sigma}_j^2} \right)}{2 \ln(\rho_j)}. \quad (15b)$$

The following lemma characterizes the optimal threshold $\tau_j^*[n]$ ($\forall n$) that minimizes the total error rate $\xi_j[n]$ of detector w_j .

Lemma 1: The optimal detection threshold $\tau_j^*[n]$ minimizing the total error rate $\xi_j[n]$ at independent detector w_j is $\tau_j^*[n] = Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}$. The corresponding minimum total error rate satisfies

$$\xi_j^*[n] = \frac{1}{2 \ln(\rho_j)} \ln \left(\frac{\rho_j \hat{\sigma}_j^2}{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \frac{\hat{\sigma}_j^2}{\rho_j}} \right). \quad (16)$$

B. Detection Performance of the Super-Detector

According to (10) and (11), the false alarm probability and missed detection probability of the super-detector w_z at time slot n are given by

$$P_{F_z}[n] = \begin{cases} 1, & \tau_z[n] < \frac{\hat{\sigma}_z^2}{\rho_z}, \\ \varphi_3[n], & \frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] \leq \rho_z \hat{\sigma}_z^2, \\ 0, & \tau_z[n] > \rho_z \hat{\sigma}_z^2. \end{cases} \quad (17a)$$

$$P_{M_z}[n] = \begin{cases} 0, & \tau_z[n] < Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}, \\ \varphi_4[n], & Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] \leq Q_z[n] + \rho_z \hat{\sigma}_z^2, \\ 1, & \tau_z[n] > Q_z[n] + \rho_z \hat{\sigma}_z^2. \end{cases} \quad (17b)$$

where

$$Q_z[n] = \left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2, \quad (18a)$$

$$\varphi_3[n] = \int_{\tau_z[n]}^{\rho_z \hat{\sigma}_z^2} \frac{1}{2 \ln(\rho_z) y} dy = \frac{1}{2 \ln(\rho_z)} \ln \left(\frac{\rho_z \hat{\sigma}_z^2}{\tau_z[n]} \right), \quad (18b)$$

$$\varphi_4[n] = \int_{\frac{\hat{\sigma}_z^2}{\rho_z}}^{\tau_z[n] - Q_z[n]} \frac{1}{2 \ln(\rho_z) y} dy = \frac{\ln \left(\frac{\rho_z (\tau_z[n] - Q_z[n])}{\hat{\sigma}_z^2} \right)}{2 \ln(\rho_z)}. \quad (18c)$$

In the following lemma, we derive the optimal detection threshold $\tau_z^*[n]$, $\forall n$, that minimizes the total error rate $\xi_z[n]$ at the super-detector w_z .

Lemma 2: The optimal detection threshold $\tau_z^*[n]$ minimizing the total error rate $\xi_z[n]$ at the super-detector w_z is $Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}$. The corresponding minimum total error rate is

$$\xi_z^*[n] = \frac{1}{2 \ln(\rho_z)} \ln \left(\frac{\rho_z \hat{\sigma}_z^2}{\left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \frac{\hat{\sigma}_z^2}{\rho_z}} \right). \quad (19)$$

IV. PROBLEM FORMULATION AND SOLUTION METHOD

A. Problem Formulation

We aim to maximize the average covert transmission rate of the system by optimizing the UAV's transmit power. The problem is subject to the covertness constraints of ordinary detectors, the covertness constraint of the super detector, and the power constraints. Therefore, the optimization problem is formulated as:

$$(P1): \max_{P_a[n]} \bar{R} \quad (20a)$$

$$\xi_j^*[n] \geq 1 - \varepsilon_1, \quad \forall j, n \quad (20b)$$

$$\xi_z^*[n] \geq 1 - \varepsilon_2 \quad (20c)$$

$$0 \leq P_a[n] \leq P_{a,\max} \quad (20d)$$

$$\frac{1}{N} \sum_{n=1}^N P_a[n] \leq \bar{P}_{a,\max} \quad (20e)$$

where (20b) and (20c) denote the covertness requirements, while (20d) and (20e) correspond to the peak and average transmit power constraints of the UAV, respectively.

The instantaneous covert transmission rate from the UAV to the scheduled legitimate user at time slot n is

$$R[n] = \log_2 \left(1 + \frac{P_a[n] |h_{a,b_{kn}}[n]|^2}{\sigma_u^2} \right). \quad (21)$$

Accordingly, the average covert rate over all N time slots is written as

$$\bar{R} = \frac{1}{N} \sum_{n=1}^N \log_2 \left(1 + \frac{P_a[n] |h_{a,b_{kn}}[n]|^2}{\sigma_u^2} \right). \quad (22)$$

B. Solution Approach

In the original optimization problem, the covertness constraints for independent wardens and the super-warden contain logarithmic and composite fractional functions. These two constraints are complicated in their initial mathematical forms, which renders the problem intractable to be solved directly using convex optimization tools. In what follows, we handle the covertness constraints (20b) and (20c) separately to facilitate the solution of problem (P1).

(a) Covertness constraint for independent wardens (20b): Substituting the minimal error rate expression (16) into (20b), we obtain

$$\frac{1}{2 \ln(\rho_j)} \ln \left(\frac{\rho_j \hat{\sigma}_j^2}{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \frac{\hat{\sigma}_j^2}{\rho_j}} \right) \geq 1 - \varepsilon_1. \quad (23)$$

Since $\rho_j > 1$, we have $2 \ln(\rho_j) > 0$. Multiplying both sides of (23) by $2 \ln(\rho_j)$ preserves the inequality direction, yielding

$$\ln \left(\frac{\rho_j \hat{\sigma}_j^2}{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \frac{\hat{\sigma}_j^2}{\rho_j}} \right) \geq 2(1 - \varepsilon_1) \ln(\rho_j). \quad (24)$$

$$\frac{\rho_j \sigma_j^2}{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + \frac{\sigma_j^2}{\rho_j}} \geq e^{(1-\varepsilon_1)2 \ln(\rho_j)}. \quad (25)$$

$$\rho_j \sigma_j^2 \geq e^{(1-\varepsilon_1)2 \ln(\rho_j)} \frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} + e^{(1-\varepsilon_1)2 \ln(\rho_j)} \frac{\sigma_j^2}{\rho_j}. \quad (26)$$

$$P_a[n] \left[\frac{e^{(1-\varepsilon_1)2 \ln(\rho_j)} \eta_0}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_j}\|^2 + H^2} \right] \leq \sigma_j^2 \left(\rho_j - \frac{e^{(1-\varepsilon_1)2 \ln(\rho_j)}}{\rho_j} \right). \quad (27)$$

Since the flight trajectory of the UAV is known, the coefficient term inside the square bracket in (27) is a strict constant. At this point, we have transformed the constraint (20b) into a linear-inequality constraint (27) with respect to the optimization variable.

(b) Covertiness constraint for the super-detector (20c): Substituting (19) into (20c), we have

$$\frac{1}{2 \ln(\rho_z)} \ln \left(\frac{\rho_z \hat{\sigma}_z^2}{\left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \frac{\hat{\sigma}_z^2}{\rho_z}} \right) \geq 1 - \varepsilon_2. \quad (28)$$

Multiplying both sides of the above equation by $2 \ln(\rho_z)$, we obtain

$$\ln \left(\frac{\rho_z \hat{\sigma}_z^2}{\left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \frac{\hat{\sigma}_z^2}{\rho_z}} \right) \geq 2(1-\varepsilon_2) \ln(\rho_z). \quad (29)$$

$$\frac{\rho_z \hat{\sigma}_z^2}{\left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \frac{\hat{\sigma}_z^2}{\rho_z}} \geq e^{2(1-\varepsilon_2) \ln(\rho_z)}. \quad (30)$$

$$\rho_z \sigma_z^2 \geq e^{2(1-\varepsilon_2) \ln(\rho_z)} \left[\left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 + \frac{\sigma_z^2}{\rho_z} \right]. \quad (31)$$

$$\rho_z \sigma_z^2 - e^{2(1-\varepsilon_2) \ln(\rho_z)} \frac{\sigma_z^2}{\rho_z} \geq e^{2(1-\varepsilon_2) \ln(\rho_z)} \times \left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2. \quad (32)$$

$$\sigma_z^2 \left(\rho_z - e^{2(1-\varepsilon_2) \ln(\rho_z)} \frac{1}{\rho_z} \right) \geq e^{2(1-\varepsilon_2) \ln(\rho_z)} \times \left(\sum_{v=1}^m \sqrt{\frac{\eta_0 P_a[n]}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2. \quad (33)$$

Since the transmit power $P_a[n]$ is independent of the summation index v for any time slot n , the common factor $\sqrt{P_a[n]}$ can be taken out from the summation symbol. Consequently, the above secrecy constraint is given by:

$$P_a[n] \left[e^{2(1-\varepsilon_2) \ln(\rho_z)} \left(\sum_{v=1}^m \sqrt{\frac{\eta_0}{\|\mathbf{q}_a[n] - \mathbf{q}_{w_v}\|^2 + H^2}} \right)^2 \right] \leq \sigma_z^2 \left(\rho_z - \frac{e^{2(1-\varepsilon_2) \ln(\rho_z)}}{\rho_z} \right). \quad (34)$$

Up to now, through algebraic identity transformations, we have equivalently converted the conventional-warden secrecy constraint (20b) and the super-warden secrecy constraint (20c) in the original problem into the linear convex constraints (27) and (34) with respect to the optimization variables, respectively. Following the above-mentioned equivalent transformations, the original optimization problem (P1) is reformulated as the following convex problem:

$$(P2): \max_{P_a[n]} \bar{R} \quad (35a)$$

$$\text{s.t. (27), (34), (20d), (20e)} \quad (35b)$$

The convex problem (P2) can be readily solved via standard convex optimization solvers such as CVX.

V. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed power optimization scheme via numerical simulations.

In the simulation scenario, the colluding monitoring nodes are selected based on the average distance to the flight trajectory of the unmanned aerial vehicle. The m monitoring nodes with the shortest average distance are selected to form a colluding group, while the remaining monitoring nodes operate independently. The UAV flies at a fixed altitude H along a straight trajectory from the starting point $(0, 500)^T$ to the terminal point $(1000, 500)^T$. The entire flight duration is evenly divided into $N = 50$ time slots. The network contains $K = 4$ legitimate ground users with horizontal coordinates $(200, 400)^T$, $(400, 400)^T$, $(600, 400)^T$, and $(800, 400)^T$, respectively. There are $M = 7$ wardens distributed at $(100, 600)^T$, $(250, 400)^T$, $(400, 600)^T$,

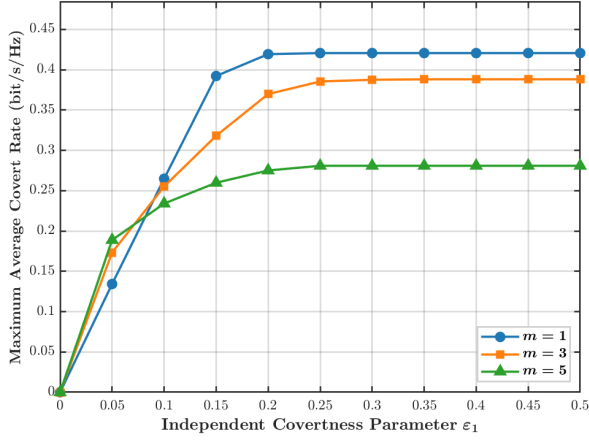


Fig. 2. Impact of covertness requirement ε_1 for independent wardens on the maximum average covert transmission rate.

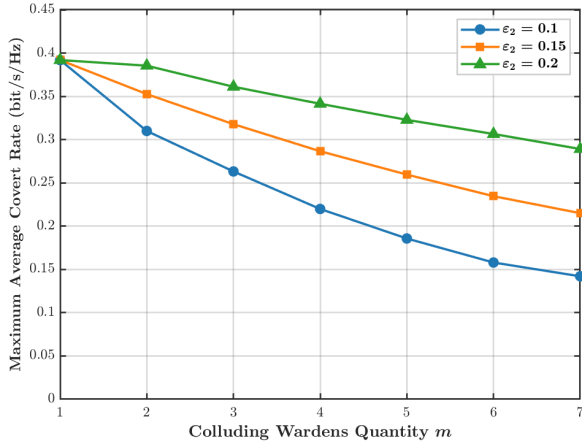


Fig. 3. Impact of collision strength m on the maximum average covert transmission rate.

$(550, 400)^T$, $(700, 600)^T$, $(850, 400)^T$, and $(950, 600)^T$. The key simulation parameters are summarized as follows: $\eta_0 = -60$ dB, $H = 100$ m, $\bar{P}_{a,\max} = 0.8$ W, $P_{a,\max} = 2$ W, $T = 50$ s, $\Delta t = 1$ s, $\rho_j = 3$ dB, $\rho_z = 3$ dB.

Fig. 2 plots the maximum average covert rate against the covertness parameter ε_1 under different collusion sizes m . All curves first rise and then saturate. When $\varepsilon_1 \leq 0.20$, relaxed covertness constraints enlarge the feasible transmit power region of the UAV, yielding an approximately linear rate growth. When $\varepsilon_1 \geq 0.20$, the curves enter the saturation regime, where the system performance is limited by the average power constraint and the collusion covertness constraint $\varepsilon_2 = 0.15$. The saturated rate decreases monotonically with m , which reveals that larger collusion groups bring stronger combined detection gain, forcing the UAV to lower transmit power. Notably, for $\varepsilon_1 \in [0, 0.1]$, the curves for $m = 3$ and $m = 5$ lie above the curve for $m = 1$. This phenomenon arises because the constraint ε_1 is tighter than ε_2 in this region; only a small subset of independent wardens dominate the power limit, which leaves more power margin for the UAV.

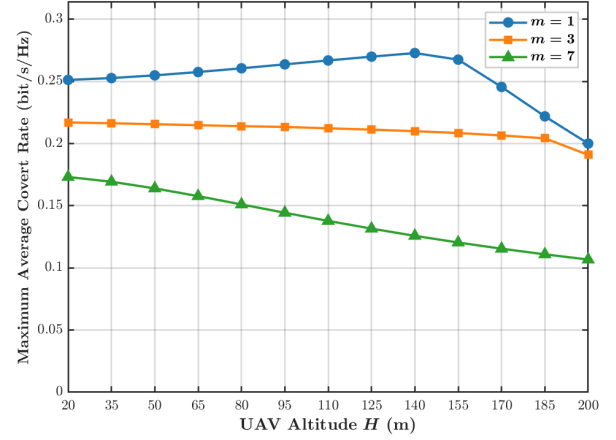


Fig. 4. Impact of UAV flight altitude H on the maximum average covert transmission rate.

Fig. 3 depicts the maximum average covert rate versus the number of colluding wardens m . All curves decrease monotonically as m increases, demonstrating that larger collusion groups severely degrade covert communication performance. At $m = 1$, the rate under all three ε_2 configurations is around 0.39 bit/s/Hz. When m rises to 7, the rates corresponding to $\varepsilon_2 = 0.1$, 0.15, and 0.2 drop to approximately 0.14, 0.21, and 0.29 bit/s/Hz, respectively. Moreover, the vertical gaps between curves widen with m , meaning the influence of ε_2 becomes more prominent for larger collusion scales. A larger ε_2 relaxes the detection constraint of colluding wardens, allowing higher transmit power and thus a higher covert rate.

Fig. 4 illustrates how the maximum average covert rate varies with UAV altitude H under fixed covertness parameters. The curve for $m = 1$ first increases and then decreases, peaking at $H = 95$ m. At low altitudes, the UAV stays close to wardens, so strict covertness constraints limit transmit power. As altitude grows, the channel gains of wardens decay, the covertness constraints loosen, and the rate rises accordingly. Further increasing altitude weakens the legitimate user channels, leading to rate degradation. In contrast, curves for $m = 3$ and $m = 7$ show a global monotonic decline. The collusion constraints suppress the UAV power close to the average power limit even at low altitudes. For sufficiently high altitudes ($H > 150$ m), the curves of $m = 1$ and $m = 3$ converge. At such altitudes, covertness constraints are nearly inactive, the system is bounded solely by the average power budget, and the impact of collusion strength vanishes.

Fig. 5 shows the optimal UAV transmit power $P_a[n]$ across time slots under different collusion intensities m . All curves present a U-shaped profile. In the middle time slots, the UAV reaches the horizontal position closest to wardens, leading to the strictest covertness constraints and the minimum transmit power. At the initial and final time slots, the UAV is far from wardens, constraints are relaxed, and power approaches the average power ceiling. Larger m shifts the entire curve downward, since more colluding wardens enhance the combined detection capability of the super-detector and shrink the

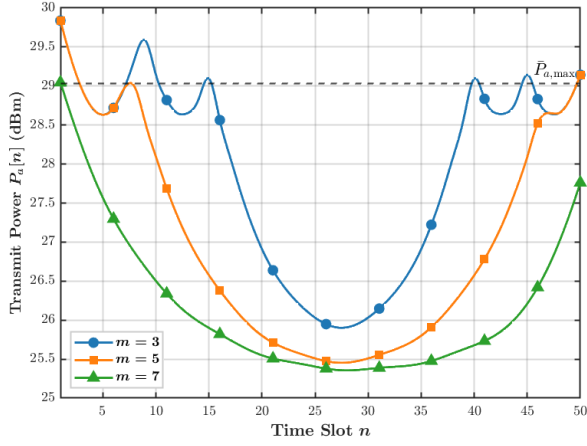


Fig. 5. Optimal UAV transmit power $P_a[n]$ versus time slot index n .

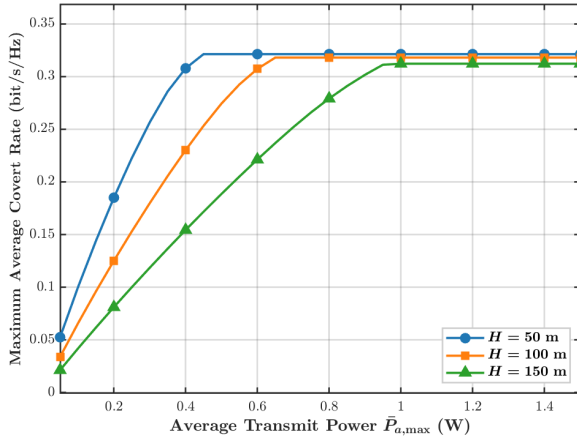


Fig. 6. Impact of maximum average transmit power $\bar{P}_{a,\max}$ on the maximum average covert transmission rate.

feasible power range for the UAV.

Fig. 6 plots the maximum average covert rate against the average power limit $\bar{P}_{a,\max}$ with fixed collusion strength $m = 3$ and identical covertness thresholds $\varepsilon_1 = \varepsilon_2$. The three curves correspond to flight altitudes $H = 50$ m, $H = 100$ m, and $H = 150$ m. Each curve first rises and then saturates. When $\bar{P}_{a,\max}$ is small, the rate grows linearly with the power budget. Once $\bar{P}_{a,\max}$ exceeds a threshold, the curve plateaus, where the covertness constraints instead of the average power become the dominant bottleneck. Saturation occurs earlier at lower altitudes, as the UAV is closer to wardens and faces tighter covertness limits. Nevertheless, low-altitude flight improves the channel gain of legitimate users. Consequently, the saturated rate at $H = 50$ m is slightly higher than that at $H = 150$ m, which verifies that properly reducing flight altitude can boost the covert transmission performance of the network.

Fig. 7 depicts the curves of the maximum average covert transmission rate versus the noise-uncertainty factor ρ ($\rho_j = \rho_z = \rho$) under different collusion intensity m . It can be observed that as ρ increases, the covert rate rises monoton-

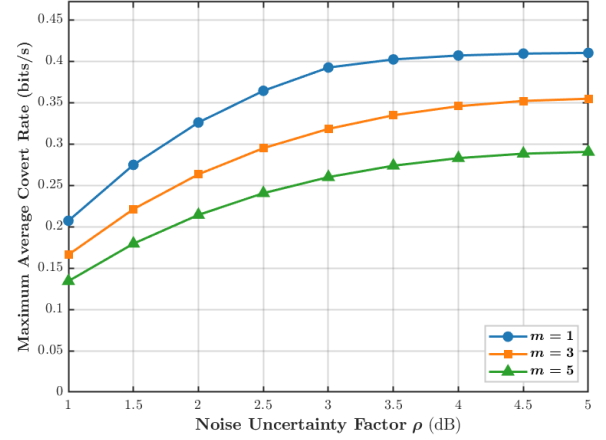


Fig. 7. Impact of noise-uncertainty factor ρ on the maximum average covert transmission rate of the system.

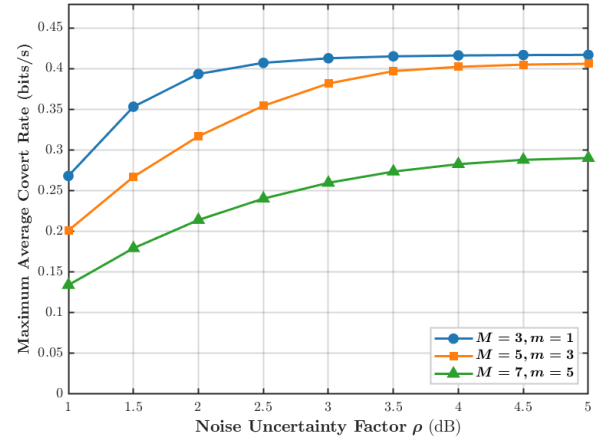


Fig. 8. Impact of different collusion models (m, M) on the maximum average covert transmission rate of the system.

ically and gradually levels off. This is because a larger ρ makes it harder for wardens to distinguish background noise from the UAV-transmitted signal, which relaxes the covertness constraint and enables the UAV to increase its transmit power. Nevertheless, when ρ becomes sufficiently large, the system is constrained by the upper limit on the average transmit power of the UAV, and the covert rate stops increasing.

Fig. 8 illustrates the variation of the maximum average covert transmission rate with the noise-uncertainty factor ρ under different collusion model combinations. It can be observed that for the same noise-uncertainty level, expanding the network scale M leads to a remarkable overall downward shift of the achievable covert rate curves. This indicates that a larger warden network not only increases the local detection probability, but also suppresses the dynamic power adjustment space of the UAV through denser spatial coverage, which significantly reduces the upper bound of the system's overall covert capacity.

VI. CONCLUSION

This paper investigates the power-control problem for UAV-aided multi-user covert IoT communications in the presence of colluding wardens. An (m, M) collusion model is adopted to characterize the scenario where a subset of wardens share their observations and form a virtual super-warden via equal-gain combining. Under the condition of noise uncertainty, the optimal energy-detection thresholds and the minimum total detection error probabilities for independent wardens and colluding wardens are derived, respectively. With a fixed UAV trajectory, the covertness constraints are further equivalently transformed, and a convex optimization problem for maximizing the average covert transmission rate is formulated. Numerical results reveal that warden collusion greatly shrinks the feasible transmit-power region and degrades the achievable covert rate. Meanwhile, the UAV flight altitude and average-power budget affect the covert communication performance through different limiting regimes. Future work can extend this model to the joint optimization of UAV trajectory and transmit power, or consider imperfect conditions with uncertain information on wardens' locations and collusion behaviors.

Furthermore, it should be specially pointed out that the system model in this paper is built upon the assumption of an ideal line-of-sight (LoS) air-ground channel, so as to focus on the core mathematical mechanism of power allocation under the multi-warden collusion scheme. Nevertheless, in practical IoT deployment scenarios in urban and suburban areas, the high mobility of UAVs makes the communication links between UAVs and ground nodes inevitably suffer from severe impacts of building occlusion, vegetation scattering and multipath effects. Such complex channel fading and shadowing effects impose remarkable influences on the covert-communication performance of the system. On the one hand, multipath fading causes random fluctuations in signal amplitude, which degrades the received signal-to-noise ratio at legitimate users and thus reduces the instantaneous effective transmission rate. On the other hand, from the perspective of physical-layer security, the channel-state uncertainty introduced by fading is deeply coupled with the noise uncertainty in the background environment. For the super-warden, this multiplicative fading disturbance greatly increases the difficulty of binary hypothesis testing. It becomes extremely difficult for the detector to distinguish whether the sharp fluctuation of received energy stems from natural fluctuations of background noise, weak signals transmitted by the UAV, or energy nulling caused by deep channel fading. This objectively raises the false-alarm and missed-detection probabilities of the super-warden, which provides natural physical-layer concealment for the UAV to a certain extent and relaxes the absolute covertness boundary of the system.

Therefore, investigating UAV covert power control in complex fading-channel environments is a promising research direction with considerable theoretical and engineering significance. Specifically, the optimization framework proposed in this paper can be extended to more general channel models such as Rician fading or probabilistic LoS/NLoS hybrid chan-

nels. In terms of mathematical modeling, since instantaneous channel state information is unavailable in practice, the existing deterministic covertness constraints should be replaced by statistical covertness outage-probability constraints, and the optimization objective can be updated to maximize the ergodic covert transmission rate of the system. From the algorithm-solving perspective, because expectation operators involving complex random variables are introduced, future research can adopt advanced mathematical tools including stochastic optimization and chance-constrained programming to further develop the existing equivalent convexification framework, so as to improve the practical engineering value of the theoretical model in non-ideal heterogeneous network environments.

APPENDIX A PROOF OF LEMMA 1

According to (14a) and (14b), the total error probability $\xi_j[n]$ of independent warden w_j at time slot n is expressed as

$$\xi_j[n] = \begin{cases} 1, & \tau_j[n] < \frac{\hat{\sigma}_j^2}{\rho_j}, \\ \varphi_1[n], & \frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] < Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}, \\ \varphi_1[n] + \varphi_2[n], & Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] \leq \rho_j \hat{\sigma}_j^2, \\ \varphi_2[n], & \rho_j \hat{\sigma}_j^2 < \tau_j[n] \leq Q_j[n] + \rho_j \hat{\sigma}_j^2, \\ 1, & \tau_j[n] > Q_j[n] + \rho_j \hat{\sigma}_j^2. \end{cases} \quad (36)$$

where

$$\varphi_1[n] + \varphi_2[n] = \frac{1}{2 \ln(\rho_j)} \ln \left(\rho_j^2 - \frac{\rho_j^2 Q_j[n]}{\tau_j[n]} \right). \quad (37)$$

Clearly, $\xi_j[n] = 1$ attains its maximum value when $\tau_j[n] < \frac{\hat{\sigma}_j^2}{\rho_j}$ or $\tau_j[n] > Q_j[n] + \rho_j \hat{\sigma}_j^2$. For $\frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] < Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}$, $\xi_j[n]$ decreases monotonically with $\tau_j[n]$. For $Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j} \leq \tau_j[n] \leq \rho_j \hat{\sigma}_j^2$ and $\rho_j \hat{\sigma}_j^2 < \tau_j[n] \leq Q_j[n] + \rho_j \hat{\sigma}_j^2$, $\xi_j[n]$ increases monotonically with $\tau_j[n]$. It can be readily verified that $\xi_j[n]$ is continuous with respect to $\tau_j[n]$ over the entire domain. Hence, the optimal detection threshold minimizing $\xi_j[n]$ is $\tau_j^*[n] = Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}$. Substituting this threshold yields the minimal total error probability

$$\xi_j^*[n] = \frac{1}{2 \ln(\rho_j)} \ln \left(\frac{\rho_j \hat{\sigma}_j^2}{Q_j[n] + \frac{\hat{\sigma}_j^2}{\rho_j}} \right). \quad (38)$$

This completes the proof of Lemma 1.

APPENDIX B

PROOF OF LEMMA 2

According to (17a) and (17b), the total error probability $\xi_z[n]$ of the super-detector w_z at time slot n is given by

$$\xi_z[n] = \begin{cases} 1, & \tau_z[n] < \frac{\hat{\sigma}_z^2}{\rho_z}, \\ \varphi_3[n], & \frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] < Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}, \\ \varphi_3[n] + \varphi_4[n], & Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] \leq \rho_z \hat{\sigma}_z^2, \\ \varphi_4[n], & \rho_z \hat{\sigma}_z^2 < \tau_z[n] \leq Q_z[n] + \rho_z \hat{\sigma}_z^2, \\ 1, & \tau_z[n] > Q_z[n] + \rho_z \hat{\sigma}_z^2. \end{cases} \quad (39)$$

where

$$\varphi_3[n] + \varphi_4[n] = \frac{1}{2 \ln(\rho_z)} \ln \left(\rho_z^2 - \frac{\rho_z^2 Q_z[n]}{\tau_z[n]} \right). \quad (40)$$

Obviously, $\xi_z[n] = 1$ is the maximum value when $\tau_z[n] < \frac{\hat{\sigma}_z^2}{\rho_z}$ or $\tau_z[n] > Q_z[n] + \rho_z \hat{\sigma}_z^2$. When $\frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] < Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}$, $\xi_z[n]$ decreases monotonically with $\tau_z[n]$. When $Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z} \leq \tau_z[n] \leq \rho_z \hat{\sigma}_z^2$ and $\rho_z \hat{\sigma}_z^2 < \tau_z[n] \leq Q_z[n] + \rho_z \hat{\sigma}_z^2$, $\xi_z[n]$ increases monotonically with $\tau_z[n]$. We can easily confirm that $\xi_z[n]$ is a continuous function of $\tau_z[n]$ across all intervals. Accordingly, the optimal detection threshold is $\tau_z^*[n] = Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}$, and the corresponding minimal total error probability is

$$\xi_z^*[n] = \frac{1}{2 \ln(\rho_z)} \ln \left(\frac{\rho_z \hat{\sigma}_z^2}{Q_z[n] + \frac{\hat{\sigma}_z^2}{\rho_z}} \right). \quad (41)$$

This completes the proof of Lemma 2.

REFERENCES

- [1] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. M. Leung, "Enabling massive IoT toward 6G: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11891–11915, Aug. 2021.
- [2] D. C. Nguyen, M. Ding, P. N. Pathirana, et al., "6G Internet of Things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, Jan. 2022.
- [3] H. Lee, B. Lee, H. Yang, J. Kim, S. Kim, W. Shin, B. Shim, and H. V. Poor, "Towards 6G hyper-connectivity: Vision, challenges, and key enabling technologies," *Journal of Communications and Networks*, vol. 25, no. 3, pp. 344–354, Jun. 2023.
- [4] N. Zhao et al., "UAV-assisted emergency networks in disasters," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 45–51, Feb. 2019.
- [5] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart. 2019.
- [6] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 36–42, May 2016.
- [7] J. Wei, Y. Guo, H. Wang, J. Gu, J. Liu, and G. Ding, "Cognitive Jamming-Aided UAV Multi-User Covert Communication," *IEEE Journal on Selected Areas in Communications*, vol. 44, pp. 1873–1887, 2026.
- [8] 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, Dec. 2019.
- [9] J. Wang et al., "Physical layer security for UAV communications: A comprehensive survey," *China Communications*, vol. 19, no. 9, pp. 77–115, Sep. 2022.

- [10] K. Meng et al., "UAV-enabled integrated sensing and communication: Opportunities and challenges," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 97–104, Apr. 2024.
- [11] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, Oct. 2019.
- [12] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, Feb. 2019.
- [13] X. Jiang et al., "Covert communication in UAV-assisted air-ground networks," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 190–197, Aug. 2021.
- [14] X. Chen et al., "Covert communications: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart. 2023.
- [15] T.-X. Zheng, Z. Yang, C. Wang, Z. Li, J. Yuan, and X. Guan, "Wireless covert communications aided by distributed cooperative jamming over slow fading channels," *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7026–7039, Nov. 2021.
- [16] B. Kang, N. Ye, and J. An, "Achieving Positive Rate of Covert Communications Covered by Randomly Activated Overt Users," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 2480–2495, 2025.
- [17] Y. Zhou, P. Fan, and Z. Ma, "A UAV-enabled integrated sensing and covert communication system," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 7, pp. 11540–11545, Jul. 2025.
- [18] X. Ji, H. Yang, X. Jiang, B. Li, and N. Zhao, "Bidirectional air-ground covert communications for low-altitude networks: A joint optimization approach," *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 4043–4061, 2026.
- [19] Y. He, J. Xu, L. Zhou, J. Wang, and C. Jiang, "Channel inversion power control-aided multi-user secret and covert UAV communications," *IEEE Transactions on Wireless Communications*, vol. 25, pp. 11002–11018, 2026.
- [20] J. Xu, L. Bai, X. Xie, and L. Zhou, "Collaborative secret and covert communications for multi-user multi-antenna uplink UAV systems: Design and optimization," *IEEE Transactions on Wireless Communications*, vol. 24, no. 7, pp. 6020–6035, Jul. 2025.
- [21] X. Pi, B. Yang, Y. Shen, and X. Jiang, "UAV Relay-Enabled THz Covert Communications Against Colluding Detection," *Transactions on Emerging Telecommunications Technologies*, vol. 36, no. 6, p. e70165, Jun. 2025.
- [22] M. Forouzes, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, Jun. 2020.
- [23] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1974–1987, Mar. 2019.
- [24] S. Zhao, J. Liu, Y. Shen, X. Jiang, T. Taleb, and N. Shiratori, "On the impact of warden collusion on covert communication in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 2297–2312, 2025.
- [25] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 129–140, Jan. 2019.

Yumei Yang graduated with a Bachelor of Science degree in Mathematics and Applied Mathematics from Yunnan Minzu University in 2024. She is currently pursuing a Master of Science degree in Probability Theory and Mathematical Statistics at Yunnan Minzu University. Her research interests focus on covert communication.





Honghui Cha graduated from the School of Big Data, Chongqing College of Mobile Communication in 2025, majoring in Data Science and Big Data Technology, and was awarded a Bachelor of Engineering degree. He is currently pursuing a Master of Engineering degree in Electronic Information at Yunnan Minzu University. His research interests mainly focus on UAV covert communication.



Fei Lin graduated with a Bachelor of Engineering degree in Computer Science and Technology from Yunnan Minzu University, College of Applied Technology in 2024. He is currently pursuing a Master of Engineering degree in Electronic Information at Yunnan Minzu University. His research interests focus on covert communication and secure communication.



Ruquan Wang graduated with a Bachelor of Science degree in Mathematics and Applied Mathematics from the School of Mathematics and Computer Science, Yunnan Minzu University in 2025. He is currently pursuing a Master of Science degree in Probability Theory and Mathematical Statistics at Yunnan Minzu University. He research interests focus on communication networks.



Wu Wang received his B.S. and M.S. degrees from Yunnan University, China, in 2003 and 2007, respectively. He received his Ph.D. degree from Future University Hakodate, Japan, in 2018. He is currently an associate professor at the School of Mathematics and Computer Science at Yunnan Minzu University. His research interests include ad hoc networks, neural networks, and network security.