Lu *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:48
https://doi.org/10.1186/s13638-020-1650-7

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Proactive eavesdropping in UAV-aided mobile relay systems

Haiquan Lu*, Haibo Dai, Ping Sun, Pei Li and Baoyun Wang

Abstract

This paper studies a new wireless surveillance scenario, where a legitimate monitor attempts to eavesdrop on the dubious messages forwarded by an unmanned aerial vehicle (UAV)-aided suspicious relay. Specifically, we consider two relaying protocols commonly used by the UAV-aided relay, namely, amplify-and-forward (AF) and decode-and-forward (DF). For each relaying protocol, we maximize the average effective eavesdropping rate by optimizing the legitimate monitor's jamming power allocation, subject to the average power constraint. The optimal jamming power allocation solutions are derived in closed-form for each of the two protocols, respectively. Numerical results show that the proposed proactive eavesdropping approach can noticeably improve the eavesdropping rate compared to the reference schemes.

Keywords: Legitimate surveillance, Unmanned aerial vehicle, Relay, Proactive eavesdropping

1 Introduction

Unmanned aerial vehicles (UAVs) have been widely used in wireless communications recently (e.g., communication relay, information dissemination, and data collection) due to the controllable mobility and ever-decreasing manufacturing cost [1–6]. On one hand, the integration of UAVs into wireless communications provides new opportunities, such as the on-demand deployment and high flexibility. On the other hand, it also renders the safety problem more emergent. Thus, the secure transmission in UAV-aided communications has received significant research interest [7–10]. However, the UAVs may also be misused by malicious users to jeopardize public safety [11]. To tackle this issue, wireless surveillance, in which authorized agencies eavesdrop on the communications of suspicious users such as criminals and terrorists legitimately, has been introduced [11–19]. In the field of wireless surveillance, passive eavesdropping [12] and proactive eavesdropping [13] are two fundamental strategies. To be specific, the proactive eavesdropping via jamming method has been studied in [20] and [21] to maximize the eavesdropping rate. In [22], the authors propose a proactive eavesdropping with spoofing relay method, which further enhances the eavesdropping capability. Besides the point-to-point suspicious communications, the suspicious relay communication scenarios are investigated in [23–25], where different strategies of the legitimate monitor are proposed. Subsequently, the authors in [26, 27] consider the proactive eavesdropping over multiple suspicious communication links, and the eavesdropping energy efficiency (EEE) is maximized. Meanwhile, Han et al. [28] considers the jamming-assisted eavesdropping over parallel fading channels and proposes the optimal jamming design to maximize the the eavesdropping success probability.

Notably, the suspicious relays in aforementioned literature are all located on the ground, whereas the UAV-aided relay may be dispatched by the suspicious users to assist their communications due to terrain obstacles. Enlightened by this, we attempt to study a new surveillance scenario, where the full-duplex legitimate monitor under perfect self-interference cancelation (SIC) [20, 21] tries to overhear the suspicious information forwarded by a UAV-aided suspicious relay. Moreover, two alternative relaying protocols, i.e., AF and DF [29–32], are available for the suspicious relay. Specifically, the AF scheme has lower implementation complexity and smaller processing delay than DF, while DF scheme attains a higher suspicious rate than AF. Thus, the suspicious relay may select a superior scheme in the practical situation. In this context, the

*Correspondence: 1016010410@njupt.edu.cn
College of Communication and Information, Nanjing University of Posts and Telecommunications, 210003 Nanjing, People's Republic of China

legitimate monitor carefully designs the optimal jamming strategies according to these two protocols. The main contributions of this paper are summarized as follows:

To the best of the authors' knowledge, this paper is the first attempt in the existing literature to study the proactive eavesdropping in the UAV-aided suspicious relay system. According to the UAV-aided relay's trajectory under both the AF and DF relaying protocols, two optimization problems are then respectively formulated to maximize the average effective eavesdropping rate by optimizing the jamming power allocation solutions. The formulated optimization problems are both non-convex and thus are difficult to be solved optimally.

We derive the optimal jamming power allocation solutions in closed-form for both the original non-convex problems, respectively. Specifically, we first verify that the two optimization problems satisfy the time-sharing property, thus guaranteeing a zero duality gap. Then the Lagrange dual method is used to attain the optimal solutions.

2 Method

This paper considers a new wireless surveillance scenario, where a legitimate monitor attempts to eavesdrop on the dubious messages forwarded by an unmanned aerial vehicle (UAV)-aided suspicious relay.

In order to maximize the average effective eavesdropping rate, two optimization problems are formulated according to the UAV-aided relay's relaying protocols (i.e., AF and DF). Due to the fact that these two optimization problems are non-convex, they cannot be directly solved with standard convex optimization techniques. In particular, we first verify that the two optimization problems satisfy the time-sharing property, thus guaranteeing a zero duality gap. Based on this result, the Lagrange dual method is used to attain the optimal solutions. Then, numerical results are provided to verify the performance of the proposed proactive eavesdropping approach.

The rest of this paper is organized as follows. Section 3 introduces the system model and formulates two optimization problems under the AF and DF relaying protocols of the suspicious UAV-aided relay. In Section 4, we derive the optimal solutions to these two optimization problems. Section 5 shows numerical results that justify the performance of the proposed proactive eavesdropping approach. Finally, we conclude this paper in Section 6.

3 System model and problem formulation

As illustrated in Fig. 1, we consider a new legitimate surveillance system, where a full-duplex legitimate monitor E aims to eavesdrop on the malicious communications forwarded by a UAV-enabled suspicious relay with two relaying protocols. Assuming that there is no direct link from the suspicious transmitter S to the suspicious receiver D and the legitimate monitor E due to the severe blockage. The UAV-aided suspicious relay R is thus deployed to assist their communication, which operates in frequency division duplex (FDD) manner with the equal bandwidth for receiving and transmitting. Without loss of generality, S, D, and E are located at $(0,0,0)$, $(L,0,0)$, and $(x_E, y_E, 0)$ in a Cartesian coordinate system, respectively. As an initial study, the relay is supposed to follow the energy-efficient circular trajectory of radius $L/2$ that is centered at $(L/2, 0, H)$, and the speed v and altitude H are constant. Note that with the circular trajectory, the UAV can fly with smooth turning angles. For ease of exposition, the cycling period T, $T = \pi L/v$, is then discretized into N equally spaced time slots, i.e., $T = N\delta_t$. Furthermore, the perfect channel state information (CSI) of all links are assumed to be available at E for characterizing the fundamental performance limit of proactive eavesdropping [13, 18, 22]. Particularly, since wireless channels between ground nodes and the UAV are dominated by LoS links in this paper, the legitimate monitor can perfectly obtain the channel gains of UAV-ground links by detecting the locations of corresponding nodes. In addition, it is practical that the suspicious transmitter is not aware of the existence of the legitimate monitor, and it only has knowledge of the CSI of the suspicious channel[1].

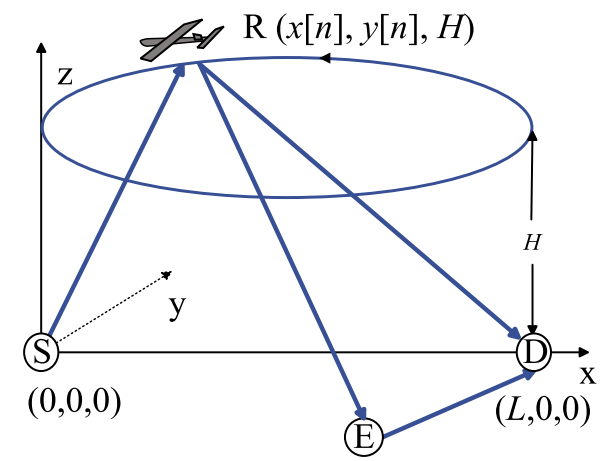

Fig. 1 System model of proactive eavesdropping in a UAV-aided suspicious relay system

In general, the communication links from the UAV to ground users are dominated by LoS links. Thus, the channel power gain $g_{ij}[n]$ in the nth time slot can be given by

$$g_{ij}[n] = \beta_0 d_{ij}^{-2}[n], \; ij \in \{SR, RD, RE\}, \; n \in \mathcal{N}, \tag{1}$$

where β_0 represents the channel power at the reference distance $d_0 = 1$ m, $d_{ij}[n]$ is the distance between ij, and $\mathcal{N} = \{1, \cdots, N\}$. The suspicious transmitter and relay are

[1] Therefore, the suspicious users do not employ the anti-eavesdropping methods (e.g., physical layer security).

considered to adopt the constant transmission power p_S and p_R, which are subjected to the average power constraint. Under this setup, E employs a jamming power $Q[n]$ to interfere with D in time slot n. It is worth mentioning that the jamming signal is in the transmitting band of the relay to effectively perform proactive eavesdropping, and the reception of R will be free from the jamming in FDD mode. Additionally, adaptive rate transmission is considered at the suspicious source according to the effective channel condition at the suspicious receiver. Thus, the suspicious transmitter adaptively adjusts its transmitting rate to a level decodable by the suspicious receiver [18, 22]. Two protocols of the relay are discussed in the following subsections.

3.1 AF relaying

For AF relaying, it has lower implementation complexity and smaller processing delay [22]. The suspicious relay amplifies the received signal in the nth time slot by the factor $\eta[n] = \sqrt{\frac{p_R}{p_S g_{SR}[n]+\sigma^2}}$. Consequently, the received signal-to-interference-plus-noise ratio (SINR) at D and SNR at E are respectively given by

$$\gamma_D(Q[n]) = \frac{\eta^2[n]\, p_S g_{RD}[n]\, g_{SR}[n]}{\eta^2[n]\, g_{RD}[n]\, \sigma^2 + Q[n]\, |h_{ED}|^2 + \sigma^2}, \quad (2)$$

$$\gamma_E[n] = \frac{\eta^2[n]\, p_S g_{RE}[n]\, g_{SR}[n]}{\eta^2[n]\, g_{RE}[n]\, \sigma^2 + \sigma^2}, \quad (3)$$

where the Rayleigh fading channel h_{ED} denotes the link from the legitimate monitor to the suspicious receiver, and σ^2 is the power of the additive white Gaussian noise (AWGN). Furthermore, the indicator function $I_1[n]$, denoting the event of successful eavesdropping at the legitimate monitor, is defined. If $\gamma_E[n] \geq \gamma_D(Q[n])$, $I_1[n] = 1$; otherwise, $I_1[n] = 0$ [13, 21]. Hence, the main objective of the legitimate monitor is to maximize the average eavesdropping rate by optimizing the jamming power allocation $Q[n], n \in \mathcal{N}$, the problem can be formulated as (dropping the constant term $1/N$ in the objective function)

$$\text{(P1)} \max_{\{Q[n]\}_{n=1}^N} \sum_{n=1}^{N} I_1[n] \log_2 (1 + \gamma_D(Q[n])) \quad (4)$$

$$\text{s.t.} \quad Q[n] \geq 0, \ n = 1, \cdots, N, \quad (4a)$$

$$\sum_{n=1}^{N} Q[n] \leq N\bar{Q}, \quad (4b)$$

where $\bar{Q}$ is the maximum average jamming power at E.

3.2 DF relaying

In this subsection, the UAV-aided suspicious relay R operates in DF mode, and one slot processing delay at R is considered. Therefore, the maximum data rates at R, D, and E in bits/second/hertz (bps/Hz) are respectively given as

$$R_R[n] = \log_2 \left(1 + \frac{p_S g_{SR}[n]}{\sigma^2}\right), \ n = 1, \cdots, N-1, \quad (5)$$

$$R_D(Q[n]) = \log_2 \left(1 + \frac{p_R g_{RD}[n]}{Q[n]\, |h_{ED}|^2 + \sigma^2}\right), \ n = 2, \cdots, N, \quad (6)$$

$$R_E[n] = \log_2 \left(1 + \frac{p_R g_{RE}[n]}{\sigma^2}\right), \ n = 2, \cdots, N. \quad (7)$$

It is observed that the suspicious transmitter should not transmit in time slot N. Referring to [23], the end-to-end suspicious rate in time slot n is given as $\min(R_R[n-1], R_D(Q[n]))$, $n = 2, \cdots, N$. Provided that $R_E[n] \geq \min(R_R[n-1], R_D(Q[n]))$, the indicator function $I_2[n]$ is set as $I_2[n] = 1$; otherwise, $I_2[n] = 0$. Therefore, the main objective of the legitimate monitor E is also to maximize the average eavesdropping rate by dynamically optimizing the jamming power $Q[n], n = 2, \cdots, N$. This optimization problem can be formulated as (dropping the constant term $1/N$ in the objective function)

$$\text{(P2)} \max_{\{Q[n]\}_{n=2}^N} \sum_{n=2}^{N} I_2[n] \min(R_R[n-1], R_D(Q[n])) \quad (8)$$

$$\text{s.t.} \quad Q[n] \geq 0, \ n = 2, \cdots, N, \quad (8a)$$

$$\sum_{n=2}^{N} Q[n] \leq N\bar{Q}, \quad (8b)$$

4 Optimal solution

In this section, the optimal solutions to problems (P1) and (P2) are derived, respectively.

4.1 Optimal solution to problem (P1)

In this subsection, we will solve problem (P1) and then obtain the optimal jamming power allocation solution to maximize the average effective eavesdropping rate. To this end, we provide the following lemma, which shows that problem (P1) satisfies the time-sharing property.

Lemma 1 *Denote* $\{Q^a[n]\}$ *and* $\{Q^b[n]\}$ *as the optimal solutions to problem (P1) under power constraints* $\bar{Q}^a$ *and* $\bar{Q}^b$*, respectively. Given any* $0 \leq \theta \leq 1$*, there always exists a feasible solution* $\{Q^c[n]\}$ *satisfying that*

$$\sum_{n=1}^{N} S^c[n] \geq \theta \sum_{n=1}^{N} S^a[n] + (1-\theta) \sum_{n=1}^{N} S^b[n], \quad (9)$$

$$\sum_{n=1}^{N} Q^c[n] \leq \theta N\bar{Q}^a + (1-\theta) N\bar{Q}^b, \quad (10)$$

where $S^k[n] = I_1^k[n]\log_2\left(1+\gamma_D(Q^k[n])\right), k \in \{a,b,c\}$, *and* $\{I_1^k[n]\}$, $\{\gamma_D(Q^k[n])\}$ *represent the corresponding indicator function and SINR at D under jamming power* $\{Q^k[n]\}$, *respectively.*

Proof We follow a similar approach as in [33] to prove Lemma 1. For any $n = 1,\cdots,N$, suppose that time slot n happens over a certain amount of time. By configuring jamming power $Q^c[n]$ to be $Q^a[n]$ for a θ percentage of the time in slot n, and $Q^b[n]$ for the remaining $1-\theta$ percentage of the time in slot n, i.e., $Q^c[n] = \theta Q^a[n] + (1-\theta)Q^b[n]$. Then the overall $S^c[n]$ is the linear combination $\theta S^a[n] + (1-\theta)S^b[n]$. Based on this, we combine all N time slots, and it follows that $\sum_{n=1}^N S^c[n] = \theta\sum_{n=1}^N S^a[n] + (1-\theta)\sum_{n=1}^N S^b[n]$, $\sum_{n=1}^N Q^c[n] = \theta\sum_{n=1}^N Q^a[n] + (1-\theta)\sum_{n=1}^N Q^b[n] \le \theta N\bar{Q}^a + (1-\theta)N\bar{Q}^b$. □

Consequently, problem (P1) satisfies the time-sharing conditions proposed in [33], and a zero duality gap holds. Thus, the Lagrange dual method is used to obtain the optimal solution.

Theorem 1 *The optimal solution to (P1) is*

$$Q^*[n] = \begin{cases} \hat{Q}[n], & \text{if } \hat{Q}[n] \in \Psi, \\ 0, & \text{otherwise}, \end{cases} \tag{11}$$

where $\Psi = \left\{ \hat{Q}[n] \middle| 0 < \hat{Q}[n] < \frac{\log_2\left(1+\frac{\eta^2[n]p_S g_{RE}[n] g_{SR}[n]}{\eta^2[n] g_{RE}[n]\sigma^2+\sigma^2}\right)}{\lambda^*} \right\}$, *and* λ^* *is the optimal dual variable. Here,* $\hat{Q}[n] = \frac{1}{|h_{ED}|^2}\left(\frac{g_{RD}[n]}{g_{RE}[n]}\sigma^2 - \sigma^2\right)$ *derives from* $\gamma_E[n] = \gamma_D(Q[n])$.

Proof Using the Lagrange dual method, Theorem 1 can be verified. The partial Lagrangian of problem (P1) is first given by

$$\begin{aligned} &L_1(\{Q[n]\},\lambda) \\ &= \sum_{n=1}^N I_1[n]\log_2(1+\gamma_D(Q[n])) - \lambda\left(\sum_{n=1}^N Q[n] - N\bar{Q}\right) \\ &= \sum_{n=1}^N \left(I_1[n]\log_2(1+\gamma_D(Q[n])) - \lambda Q[n]\right) + \lambda N\bar{Q}, \end{aligned} \tag{12}$$

where $\lambda \ge 0$ is the dual variable associated with (4b). The dual function of problem (P1) is expressed as

$$g_1(\lambda) = \max_{\{Q[n]\ge 0\}} L_1(\{Q[n]\},\lambda). \tag{13}$$

The dual problem of (P1), denoted as (D1), is thus defined as $\min_{\lambda\ge 0} g_1(\lambda)$. To garner the optimal solution to (P1), its dual problem (D1) can be solved equivalently. Without loss of optimality, problem (13) can be converted into multiple subproblems. For any $n = 1,\cdots,N$,

$$\max_{Q[n]\ge 0} I_1[n]\log_2(1+\gamma_D(Q[n])) - \lambda Q[n]. \tag{14}$$

□

Consequently, the subproblem (14) is considered. To ensure the successful eavesdropping, we have $\gamma_E[n] \ge \gamma_D(Q[n])$, namely, $Q[n] \ge \hat{Q}[n]$, where $\hat{Q}[n] = \frac{1}{|h_{ED}|^2}\left(\frac{g_{RD}[n]}{g_{RE}[n]}\sigma^2 - \sigma^2\right)$. Problem (14) can be solved by discussing two cases.

Case 1 *When* $\hat{Q}[n] \le 0$, *it means that* $I_1[n] = 1$. *In this case, problem* (14) *becomes* $\max_{Q[n]\ge 0}\log_2(1+\gamma_D(Q[n])) - \lambda Q[n]$. *Due to the fact that this objective function decreases with* $Q[n]$, *the optimal jamming power is* $Q^\lambda[n] = 0$.

Case 2 *When* $\hat{Q}[n] > 0$, *two subcases are considered to solve problem* (14).

Subcase 1 $Q[n] \ge \hat{Q}[n]$, *which leads to* $I_1[n] = 1$. *Problem* (14) *is thus rewritten as* $\max_{Q[n]\ge\hat{Q}[n]}\log_2(1+\gamma_D(Q[n])) - \lambda Q[n]$. *The optimal jamming power is* $Q[n] = \hat{Q}[n]$, *and the corresponding optimal value is* $V_1[n] = \log_2\left(1+\frac{\eta^2[n]p_S g_{RE}[n] g_{SR}[n]}{\eta^2[n] g_{RE}[n]\sigma^2+\sigma^2}\right) - \frac{\lambda}{|h_{ED}|^2}\left(\frac{g_{RD}[n]}{g_{RE}[n]}\sigma^2 - \sigma^2\right)$.

Subcase 2 $Q[n] < \hat{Q}[n]$, *namely,* $I_1[n] = 0$. *Problem* (14) *can be re-expressed as* $\max_{0\le Q[n]<\hat{Q}[n]} -\lambda Q[n]$. *The optimal jamming power is* $Q[n] = 0$, *and the optimal value is 0.*

Comparing the two subcases, if $V_1[n] > 0$, then $Q^\lambda[n] = \hat{Q}[n]$; otherwise, $Q^\lambda[n] = 0$.

In summary, the optimal jamming power to problem (14) is given by

$$Q^\lambda[n] = \begin{cases} \hat{Q}[n], & \text{if } \hat{Q}[n] \in \Psi, \\ 0, & \text{otherwise}, \end{cases} \tag{15}$$

where $\Psi = \left\{ \hat{Q}[n] \middle| 0 < \hat{Q}[n] < \frac{\log_2\left(1+\frac{\eta^2[n]p_S g_{RE}[n] g_{SR}[n]}{\eta^2[n] g_{RE}[n]\sigma^2+\sigma^2}\right)}{\lambda} \right\}$.

Subsequently, the optimal dual variable λ^* is obtained by solving problem (D1). It can be seen that the subgradient of $g_1(\lambda)$ is $s_1(\lambda) = N\bar{Q} - \sum_{n=1}^N Q^\lambda[n]$, the binary search is then employed to attain λ^*. The proof of Theorem 1 is thus completed.

It can be observed that if the channel quality of E is superior to that of D in time slot n, which corresponds to $\hat{Q}[n] \le 0$, passive eavesdropping at E is optimal. In

addition, due to the average power constraint, the legitimate monitor E interferes with the suspicious receiver D only when the jamming power meets the condition, i.e., $\hat{Q}[n] \in \Psi$.

4.2 Optimal solution to dual problem of (P2)

In this subsection, we turn our attention to problem (P2). Analogously, we can also prove that problem (P2) has the time-sharing property, and the detail is omitted for brevity.

Lemma 2 *The time-sharing condition holds for problem (P2).*

Next, we attain the optimal solution to problem (P2) via solving its dual problem.

Theorem 2 *The optimal solution to (P2) is*

$$Q^*[n] = \begin{cases} \tilde{Q}[n], & \text{if } R_E[n] < \min\left(R_R[n-1], R_D[n]\right) \text{ and } \tilde{Q}[n] \in \Omega, \\ 0, & \text{otherwise,} \end{cases} \tag{16}$$

where $\Omega = \left\{ \tilde{Q}[n] \middle| 0 < \tilde{Q}[n] < \frac{1}{\lambda^*} \log_2\left(1 + \frac{p_R g_{RE}[n]}{\sigma^2}\right) \right\}$, λ^* *is the optimal dual variable, and* $\tilde{Q}[n] = \frac{\sigma^2}{|h_{ED}|^2}\left(\frac{g_{RD}[n]}{g_{RE}[n]} - 1\right)$. *Here,* $R_D[n] = \log_2\left(1 + p_R g_{RD}[n]/\sigma^2\right)$.

Proof Analogous to the proof of Theorem 1, the Lagrange dual method is utilized, and a set of subproblems are considered. For any $n = 2, \cdots, N$,

$$\max_{Q[n] \geq 0} I_2[n] \min\left(R_R[n-1], R_D(Q[n])\right) - \lambda Q[n]. \tag{17}$$

□

Problem (17) can be solved by discussing two cases.

Case 1 *When* $R_E[n] \geq \min\left(R_R[n-1], R_D[n]\right)$, *the legitimate monitor can overhear the suspicious message with passive eavesdropping, and* $I_2[n] = 1$. *Thus, the optimal jamming power is* $Q^{\lambda}[n] = 0$.

Case 2 *On the other hand, when* $R_E[n] < \min\left(R_R[n-1], R_D[n]\right)$, *it indicates that the jamming power* $\tilde{Q}[n] = \frac{1}{|h_{ED}|^2}\left(\frac{g_{RD}[n]}{g_{RE}[n]}\sigma^2 - \sigma^2\right) > 0$ *for the successful eavesdropping, where* $\tilde{Q}[n]$ *derives from* $R_D(Q[n]) = R_E[n]$. *Here,* $Q[n] < \tilde{Q}[n]$ *and* $Q[n] \geq \tilde{Q}[n]$ *are respectively considered. Similar to the proof of Theorem 1, the process is omitted for brevity.*

Combining the two cases, the optimal solution to the dual problem of (P2) is given as (16) after obtaining the optimal dual variable. Theorem 2 thus follows.

Theorem 2 shows that the jamming strategy depends on the channel qualities from S to R as well as that from R to D and E. Provided that $R_E[n] \geq \min\left(R_R[n-1], R_D[n]\right)$, no jamming performed at E in time slot n is optimal, and the effective eavesdropping rate is $\min\left(R_R[n-1], R_D[n]\right)$. On the other hand, subject to the average power constraint, E only implements the jamming according to the above condition. In this case, the jamming degrades the suspicious rate $R_D[n]$ to $R_E[n]$, and the effective eavesdropping rate is thus $R_E[n]$.

Furthermore, subject to both the average and peak power constraints at E, i.e., $0 \leq Q[n] \leq Q_{\text{peak}}$, $n = 1, \cdots, N$ and $\sum_{n=1}^{N} Q[n] \leq N\bar{Q}$ for AF relaying; $0 \leq Q[n] \leq Q_{\text{peak}}$, $n = 2, \cdots, N$ and $\sum_{n=2}^{N} Q[n] \leq N\bar{Q}$ for DF relaying, the new optimization problems are formulated. Analogously, by using the Lagrange dual method, the optimal solutions to dual problems can be obtained, which serve as the upper bounds of the new optimization problems.

However, when the peak power is sufficiently large, it can be proved that the upper bounds are tight. Specifically, denote $\{Q^a[n]\}$ and $\left\{Q^b[n]\right\}$ as the optimal solutions to problem (P1) under power constraints Q^a_{peak}, $\bar{Q}^a$, and Q^b_{peak}, $\bar{Q}^b$, respectively. When the peak power is sufficiently large, it follows that $0 \leq Q^c[n] \leq \theta Q^a_{\text{peak}} + (1-\theta) Q^b_{\text{peak}}$. Similar to Lemma 1, the time-sharing conditions also hold in this case, thus guaranteeing the strong duality.

5 Numerical results and discussions

In this section, numerical simulations are presented to evaluate the performance of our proposed jamming strategy. Similar to [34], in our simulations, the parameters are set as in Table 1.

Figures 2 and 3 investigate the impact of the average jamming power on the average achievable eavesdropping rate for the suspicious relay's two protocols, respectively. Two reference schemes are used for comparison, i.e., (1) passive eavesdropping and (2) proactive eavesdropping with constant jamming power $\bar{Q}$. Here, the transmission power at suspicious nodes is set as $p_S = p_R = 15$ dBm, and the position of E is $(x_E, y_E, 0) = (1500, 1000, 0)$ m. As

Table 1 Simulation parameters

Parameter	Value
Distance between S and $D(L)$	2000 m
UAV altitude (H)	100 m
UAV speed (v)	π m/s
Noise power (σ^2)	− 110 dBm
Channel gain at reference distance (β_0)	− 60 dB
Time slot length (δ_t)	0.5 s

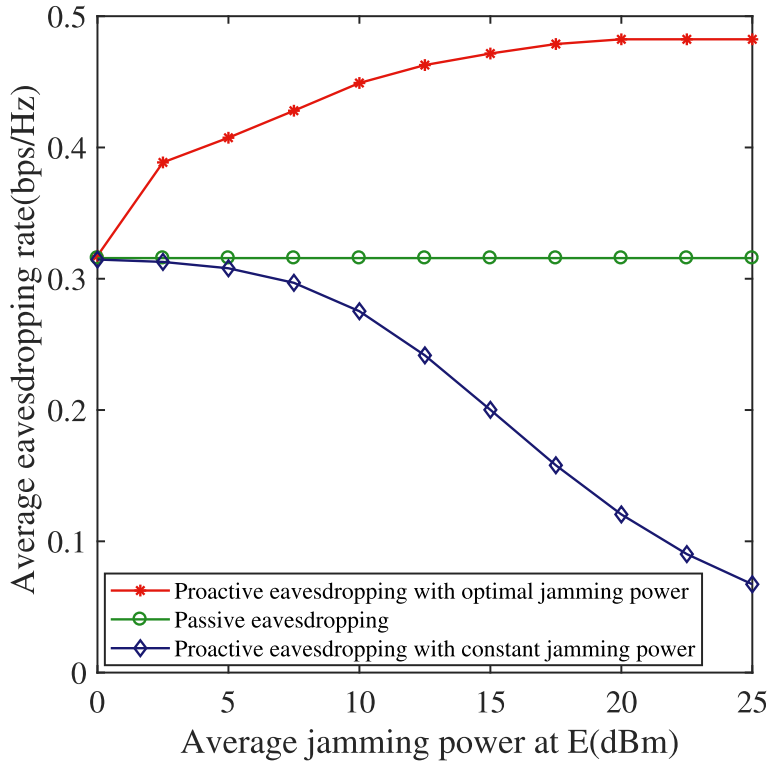

Fig. 2 Eavesdropping rate versus average jamming power $\bar{Q}$ for AF relaying

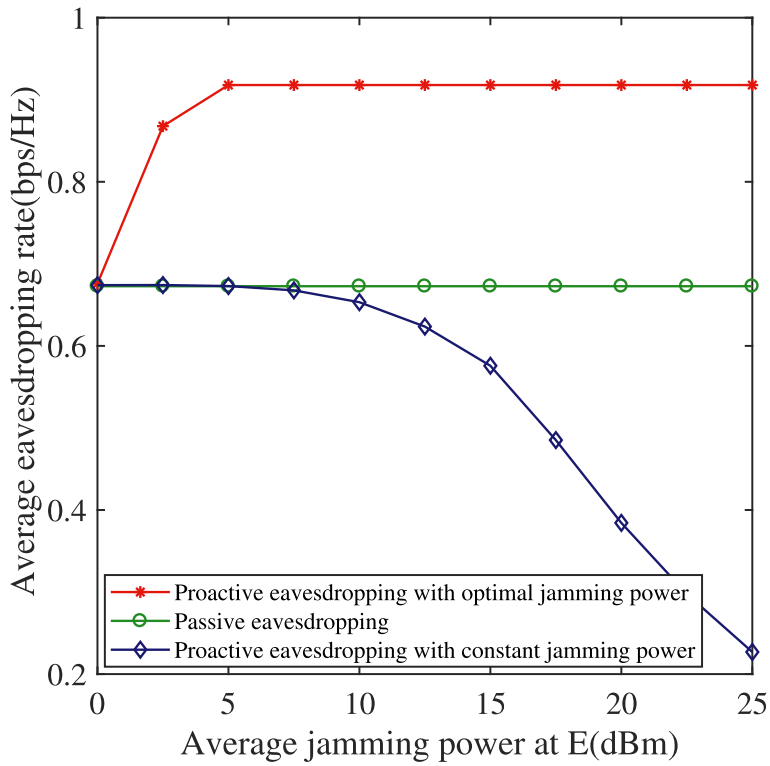

Fig. 3 Eavesdropping rate versus average jamming power $\bar{Q}$ for DF relaying

expected, the proposed proactive eavesdropping approach outperforms the other two reference schemes under two protocols, and the average eavesdropping rate begins to plateau with the sufficiently large jamming power. It is observed that the performance of scheme 2 deteriorates. The reason is that the constant jamming power $\bar{Q}$ exceeds the optimal jamming power, which meanwhile degrades the effective eavesdropping rate despite the successful eavesdropping.

Figures 4 and 5 show the maximum achievable eavesdropping rate versus the position of E in the form of a contour map. Intuitively, the higher eavesdropping rate is obtained around D owing to the similar channel condition between D and E, thus needing a smaller jamming power for the successful eavesdropping for AF relaying. For DF relaying, it is observed that in the middle region of the contour map, E obtains the maximum average eavesdropping rate. This is attributed to the fact E enjoys a relatively good channel conditions under a sufficiently small time slot δ_t. Furthermore, the achievable average eavesdropping rate declines with the increasing distance between E and the center. This is because the ever-increasing jamming power to guarantee the successful eavesdropping meanwhile degrades the effective eavesdropping rate.

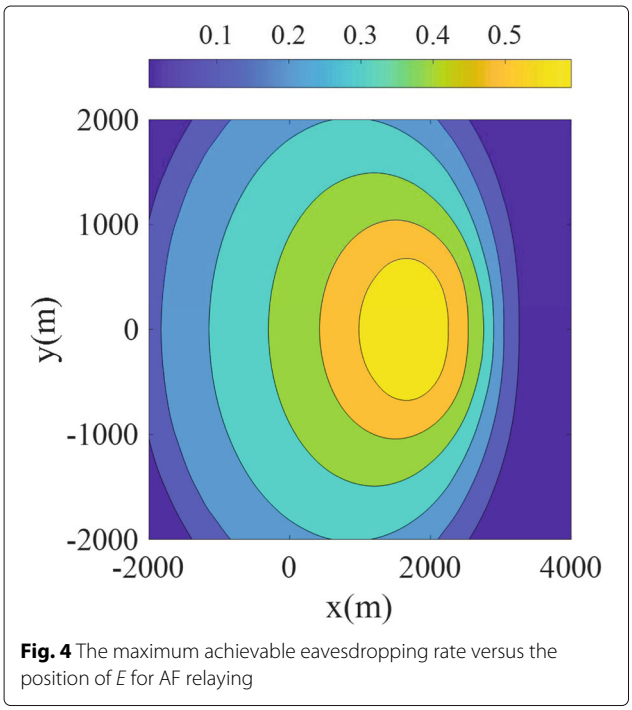

Fig. 4 The maximum achievable eavesdropping rate versus the position of E for AF relaying

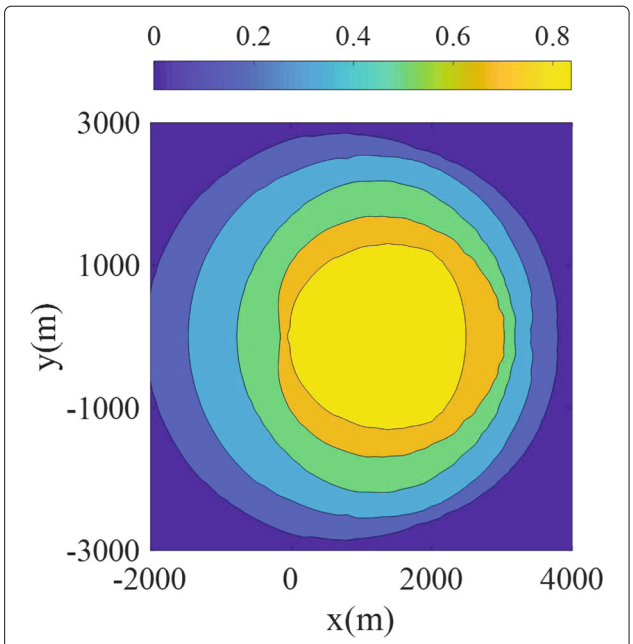

Fig. 5 The maximum achievable eavesdropping rate versus the position of E for DF relaying

6 Conclusion

This paper studied the wireless surveillance in a malicious UAV-enabled relay system, where both AF and DF relaying protocols were considered for the suspicious relay. In this context, we maximized the average effective eavesdropping rate by optimizing the legitimate monitor's jamming power allocation. The optimal jamming power allocation solutions were then presented in closed-form for each of the two protocols, respectively. Numerical results showed the significant benefits were achieved by applying the approach of proactive eavesdropping compared to the reference schemes.

Abbreviations

AF: Amplify-and-forward; AWGN: Additive white Gaussian noise; CSI: Channel state information; DF: Decode-and-forward; EEE: Eavesdropping energy efficiency; FDD: Frequency division duplex; LoS: Line-of-sight; SIC: Self-interference cancelation; SINR: Signal-to-interference-plus-noise ratio; SNR: Signal-to-noise ratio; UAV: Unmanned aerial vehicle

Acknowledgements

Not applicable

Authors' contributions

HL is the main author of the current paper. HL contributed to the development of the ideas, design of the study, theory, result analysis, and article writing. HD contributed to the development of the ideas, design of the study, the theory and article writing. HL and PS conceived and designed the experiments. HL and PL performed the experiments. BW undertook revision works of the paper. All authors read and approved the final manuscript.

Funding

This paper was supported in part by the National Natural Science Foundation of China under Grants 61971238 and 61372126, the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under 18KJB510026, and the Foundation of Nanjing University of Posts and Telecommunications under NY218124.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Received: 26 October 2019 Accepted: 16 January 2020
Published online: 24 February 2020

References

1. Y. Zeng, R. Zhang, T. J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges. IEEE Commun. Mag. **54**(5), 36–42 (2016)
2. Y. Zeng, J. Xu, R. Zhang, Energy minimization for wireless communication with rotary-wing UAV. IEEE Trans. Wirel. Commun. **18**(4), 2329–2345 (2019)
3. J. Xu, Y. Zeng, R. Zhang, UAV-enabled wireless power transfer: trajectory design and energy optimization. IEEE Trans. Wirel. Commun. **17**(8), 5092–5106 (2018)
4. Y. Zeng, X. Xu, R. Zhang, Trajectory design for completion time minimization in UAV-enabled multicasting. IEEE Trans. Wirel. Commun. **17**(4), 2233–2246 (2018)
5. H. Dai, H. Zhang, M. Hua, C. Li, Y. Huang, B. Wang, How to deploy multiple UAVs for providing communication service in an unknown region?. IEEE Wirel. Commun. Lett. **8**(4), 1276–1279 (2019)
6. H. Dai, H. Zhang, B. Wang, L. Yang, The multi-objective deployment optimization of UAV-mounted cache-enabled base stations. Physical Commun. **34**, 114–120 (2019)
7. N. Zhao, F. Cheng, F. R. Yu, J. Tang, Y. Chen, G. Gui, H. Sari, Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment. IEEE Trans. Commun. **66**(5), 2281–2294 (2018)
8. G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing UAV communications via joint trajectory and power control. IEEE Trans. Wirel. Commun. **18**(2), 1376–1389 (2019)
9. M. Hua, Y. Wang, Q. Wu, H. Dai, Y. Huang, L. Yang, Robust trajectory and transmit power design for secure UAV communications. IEEE Trans. Veh. Technol. **68**(8), 7761–7775 (2019)
10. M. Cui, G. Zhang, Q. Wu, D. W. K. Ng, Energy-efficient cooperative secure transmission in multi-UAV-enabled wireless networks. IEEE Trans. Veh. Technol. **67**(9), 9042–9046 (2018)
11. H. Lu, H. Zhang, H. Dai, W. Wu, B. Wang, Proactive eavesdropping in UAV-Aided suspicious communication systems. IEEE Trans. Veh. Technol. **68**(2), 1993–1997 (2019)
12. J. Xu, L. Duan, R. Zhang, Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm. IEEE Wirel. Commun. **24**(4), 152–159 (2017)
13. C. Zhong, X. Jiang, F. Qu, Z. Zhang, Multi-antenna wireless legitimate surveillance systems: design and performance analysis. IEEE Trans. Wirel. Commun. **16**(7), 4585–4599 (2017)
14. P. Li, H. Zhang, W. Wu, H. Dai, B. Wang, in *2018 IEEE Global Communications Conference (GLOBECOM)*. Proactive eavesdropping via jamming in cognitive radio networks (IEEE, 2018). https://doi.org/10.1109/glocom.2018.8647517
15. H. Zhang, L. Duan, R. Zhang, in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. Proactive eavesdropping of two suspicious communication links via jamming (IEEE, 2019). https://doi.org/10.1109/icc.2019.8761976
16. J. Moon, S. Lee, H. Lee, I. Lee, Proactive eavesdropping with jamming and eavesdropping mode selection. IEEE Trans. Wirel. Commun. **18**(7), 3726–3738 (2019)
17. J. Moon, H. Lee, C. Song, S. Kang, I. Lee, Relay-assisted proactive eavesdropping with cooperative jamming and spoofing. IEEE Trans. Wirel. Commun. **17**(10), 6958–6971 (2018)
18. J. Moon, H. Lee, C. Song, S. Lee, I. Lee, Proactive eavesdropping with full-duplex relay and cooperative jamming. IEEE Trans. Wirel. Commun. **17**(10), 6707–6719 (2018)
19. S. Huang, Q. Zhang, Q. Li, J. Qin, Robust proactive monitoring via jamming with deterministically bounded channel errors. IEEE Sig. Process. Lett. **25**(5), 690–694 (2018)
20. J. Xu, L. Duan, R. Zhang, Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels. IEEE Wirel. Commun. Lett. **5**(1), 80–83 (2016)
21. J. Xu, L. Duan, R. Zhang, Proactive eavesdropping via cognitive jamming in fading channels. IEEE Trans. Wirel. Commun. **16**(5), 2790–2806 (2017)
22. Zeng Y., R. Zhang, Wireless information surveillance via proactive eavesdropping with spoofing relay. IEEE J. Sel. Topics Sig. Process. **10**(8), 1449–1461 (2016)
23. G. Ma, J. Xu, L. Duan, R. Zhang, in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. Wireless surveillance of two-hop communications (IEEE, 2017). https://doi.org/10.1109/spawc.2017.8227700
24. X. Jiang, H. Lin, C. Zhong, X. Chen, Z. Zhang, Proactive eavesdropping in relaying systems. IEEE Sig. Process. Lett. **24**(6), 917–921 (2017)
25. D. Hu, Q. Zhang, P. Yang, J. Qin, Proactive monitoring via jamming in amplify-and-forward relay networks. IEEE Sig. Process. Lett. **24**(11), 1714–1718 (2017)
26. B. Li, Y. Yao, H. Zhang, Y. Lv, Energy efficiency of proactive cooperative eavesdropping over multiple suspicious communication links. IEEE Trans. Veh. Technol. **68**(1), 420–430 (2019)
27. B. Li, Y. Yao, H. Zhang, Y. Lv, W. Zhao, Energy efficiency of proactive eavesdropping for multiple links wireless system. IEEE Access. **6**, 26081–26090 (2018)
28. Y. Han, L. Duan, R. Zhang, Jamming-assisted eavesdropping over parallel fading channels. IEEE Trans. Inf. Forensic. Secur. **14**(9), 2486–2499 (2019)
29. C. Li, H. J. Yang, F. Sun, J. M. Cioffi, L. Yang, Multiuser overhearing for cooperative two-way multiantenna relays. IEEE Trans. Veh. Technol. **65**(5), 3796–3802 (2016)
30. C. Li, S. Zhang, P. Liu, F. Sun, J. M. Cioffi, L. Yang, Overhearing protocol design exploiting inter-cell interference in cooperative green networks. IEEE Trans. Veh. Technol. **65**(1), 441–446 (2016)
31. C. Li, P. Liu, C. Zou, F. Sun, J. M. Cioffi, L. Yang, Spectral-efficient cellular communications with coexistent one- and two-hop transmissions. IEEE Trans. Veh. Technol. **65**(8), 6765–6772 (2016)
32. C. Li, F. Sun, J. M. Cioffi, L. Yang, Energy efficient MIMO relay transmissions via joint power allocations. IEEE Trans. Circuits Syst. II, Exp. Briefs. **61**(7), 531–535 (2014)
33. W. Yu, R. Lui, Dual methods for nonconvex spectrum optimization of multicarrier systems. IEEE Trans. Commun. **54**(7), 1310–1322 (2006)
34. Y. Zeng, R. Zhang, T. J. Lim, Throughput maximization for UAV-enabled mobile relaying systems. IEEE Trans. Commun. **64**(12), 4983–4996 (2016)

Publisher's Note