Power Allocation for Proactive Eavesdropping with Spoofing Relay in UAV Systems

Mingzhu Zhang*, Yu Chen*, Xiaofeng Tao* and Izzat Darwazeh†
*National Engineering Lab for Mobile Network Technologies
*Beijing University of Posts and Telecommunications, Beijing, 100876, China
Email: {z_mz, y.chen, taoxf}@bupt.edu.cn
†Department of Electronic and Electrical Engineering, University College London (UCL), London, UK
Email: i.darwazeh@ucl.ac.uk

***Abstract*—Unmanned aerial vehicles (UAVs) are used in legitimate surveillance systems. In this paper, we consider a wireless monitor system that consists of three UAVs. One UAV acts as a legitimate eavesdropper that adopts 1) spoofing relaying and 2) proactive eavesdropping via jamming techniques. In particular, two scenarios are considered if the legitimate eavesdropper has enough power for successful eavesdropping throughout flight time. If the legitimate eavesdropper has enough power, the formulated problem is a convex optimization problem, which can be solved by standard convex optimization techniques. If not, we formulate a non-convex optimization problem and solve it by an iterative algorithm. Numerical results show that the proposed power allocation scheme outperforms the passive eavesdropping and equally distributed jamming power allocation schemes.**

I. Introduction

Unmanned aerial vehicles (UAVs) has high mobility and low costs compared to ground nodes [1], [2]. Because wireless channels are accessible by both authorized and unauthorized users, secure transmission in UAV-aided communications has attracted considerable attention [3]–[9]. On the other hand, with an increasing number of activities caused by unauthorized wireless systems, it has become an important issue for legitimate monitors to eavesdrop any suspicious communications [10]–[13].

Recent work shows that there are two common techniques for legitimate surveillance systems: 1) the proactive eavesdropping via jamming [10] and 2) the spoofing relaying [13]. The first technique is achieved by sending jamming signals to suspicious links for eavesdropping successfully. By using the second technique – spoofing relaying, a legitimate eavesdropper forwards constructive signals to a suspicious receiver when eavesdropping links is stronger than suspicious links. However, the above two techniques are mainly used in terrestrial communications, where both suspicious nodes and legitimate eavesdroppers are placed on the ground.

Some research considers using UAVs in legitimate surveillance systems. Consider that a UAV acts as a suspicious transmitter and assume that the UAV can automatically adjust its location to maximize the minimum suspicious rate of all suspicious receivers. Under this assumption, Lu et al. [14] maximized eavesdropping rate by optimizing the jamming power. A UAV working as a receiver was studied when a ground monitor acts as a proactive eavesdropper to eavesdrop the suspicious link and transmit information to the UAV [15]. The eavesdropping performance of the ground monitor is improved by ensuring targeted signal-to-interference plus noise ratio of the UAV. Wang et al. [16] considered a scenario that a legitimate eavesdropper UAV eavesdropped suspicious communications between two UAVs. They maximized the eavesdropping rate at UAV via optimizing its jamming power. However, the above work did not bring the spoofing relay into UAVs legitimate eavesdropping systems, and they did not consider situations when UAVs have limited power.

In this paper, we follow Wang's work [16], i.e., a UAV works as a legitimate eavesdropper to eavesdrop suspicious communications between two suspicious UAVs. Moreover, if the achievable data rate of the eavesdropping link (from a suspicious transmitter to a legitimate eavesdropper) is more than the suspicious link (from a suspicious transmitter to a suspicious receiver), the legitimate eavesdropper will be a spoofing relay to forward signals from suspicious transmitter to suspicious receiver. Otherwise, the legitimate eavesdropper will be a jammer to send jamming signals to suspicious receiver.

The aim of paper is to maximize the effective eavesdropping rate throughout flight time via optimizing power of the legitimate eavesdropper. When the power of the legitimate eavesdropper is enough, an optimal scheme is first proposed to allocate jamming and relay power. Meanwhile, consider that there is not enough power for UAV to successfully eavesdrop at every time slot. Thus, we formulate a non-convex problem and then propose an iterative algorithm to solve it by dividing the problem into two subproblems.

The rest of the paper is organized as follows: we discuss the system model in Section II, we formulate the optimization problem and propose relay and jamming power allocation schemes in Section III. Simulation results are shown in Section IV, followed by a conclusion in Section V.

II. System Model

As shown in Fig. 1, we consider a wireless communication system with a moving suspicious transmitter (MST) and a moving suspicious receiver (MSR). They fly at a constant velocity with the same direction, so the distance between them is a fixed value – L meters. The legitimate eavesdropper flies

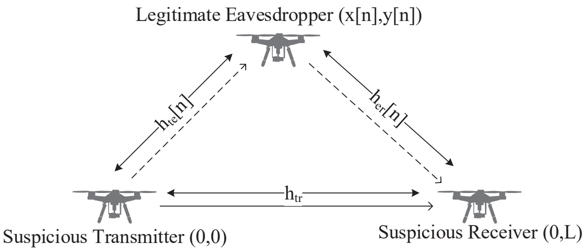
Legitimate Eavesdropper (x[n],y[n])
h_te[n]
h_er[n]
h_tr
Suspicious Transmitter (0,0)
Suspicious Receiver (0,L)

Fig. 1: Proactive eavesdropping in UAV communications.

in a predetermined trajectory between the MST and the MSR and the largest distance between the MSR and the legitimate eavesdropper is larger than L in the system model.

Since the relative locations of the MST and the MSR are static, a Cartesian coordinate system is used with locations of the MST and the MSR denoted as (0,0) and (L,0), respectively. Note that for simplicity, we have ignored the UAV's take-off and landing phases, but instead focus on its operation period of time horizon T. If we divide the flight time T of the legitimate eavesdropper into N equal time slots, the legitimate eavesdropper's trajectory over T can be approximated by a sequence $\{(x[n], y[n]) : n \in 1, 2, \cdots, N\}$, where $(x[n], y[n])$ is the legitimate eavesdropper's x-y coordinate at time slot n.

The legitimate eavesdropper is equipped with a data buffer of limited size, and it operates in a FDD mode with equal bandwidth allocated for information reception from the MSR and jamming to the MST. Moreover, the channel from the MST to the MSR, the MST to the legitimate eavesdropper, the legitimate eavesdropper to the MSR are dominated by line-of-sight (LOS) link, and the Doppler effect due to the UAV's mobility is assumed to be perfectly compensated [17]. Thus, at time slot n, the channel power gain from the MST to the legitimate eavesdropper, from the legitimate eavesdropper to the MSR are respectively expressed as follows:

$$h_{te}[n] = \beta_0 d_{te}^{-2}[n] \tag{1}$$

and

$$h_{er}[n] = \beta_0 d_{er}^{-2}[n], \tag{2}$$

where β_0 denotes the channel power gain at the reference distance $d_0 = 1$ meter, whose value depends on the carrier frequency, antenna gain, etc., and $d_{te}[n] = \sqrt{x^2[n] + y^2[n]}$, $d_{er}[n] = \sqrt{(L - x[n])^2 + y^2[n]}$, are the distance between the MST and the legitimate eavesdropper,the legitimate eavesdropper and the MSR, respectively. We define $h_{tr} = \beta_0 L^{-2}$ as the channel power gain from the MST to the MSR.

We define $R_E[n]$ and $R_R[n]$ as the achievable data rate of the eavesdropping link and the suspicious link respectively. If $R_E[n] \geq R_R[n]$, the legitimate eavesdropper can reliable decode the information sent by the MST with arbitrarily small error probability. Therefore, the effective eavesdropping rate is given by $R_{EV}[n] = R_R[n]$. In this case, the legitimate eavesdropper will act as a spoofing relay to increase achievable data rate of the suspicious link. On the other hand, if $R_E[n] < R_R[n]$, it is impossible for the legitimate eavesdropper to decode the information without any errors. In this case, the effective eavesdropping rate $R_{EV}[n] = 0$. Therefore, the legitimate eavesdropper will be a jammer to reduce achievable data rate of the suspicious link $R_R[n]$ for eavesdropping successfully. We can divide all time slots into two sets, one set $\mathcal{F}$ includes time slots, at which legitimate eavesdropper will be a spoofing relay. For the other set $\mathcal{J}$, legitimate eavesdropper will send jamming signals to suspicious link.

For the set $\mathcal{F}$, the legitimate eavesdropper will be a spoofing relay to eavesdrop signals from the MST during first hop and forward received signals to the MSR during the second hop. The legitimate eavesdropper is adopted amplify-and-forward (AF) manner since this strategy usually has smaller processing delay. At time slot n, the received signal $y_{r1}[n]$ at the MSR and $y_e[n]$ at the legitimate eavesdropper can be respectively expressed as

$$y_{r1}[n] = \sqrt{P_s h_{tr}} x_t[n] + z_1[n] \tag{3}$$

and

$$y_e[n] = \sqrt{P_s h_{te}[n]} x_t[n] + z_2[n], \tag{4}$$

where P_s is the transmission power of the MSR, $x_t[n]$ is the signal of unit energy from the MST, $z_1[n]$ and $z_2[n]$ are the additive white Gaussian noise (AWGN) received at the MSR and the legitimate eavesdropper. Thus $z_1[n]$ and $z_2[n]$ follows $CN(0, N_1)$, $CN(0, N_2)$ respectively.

For the second phase, the legitimate eavesdropper normalizes its received signal by using the normalization factor δ, i.e., $x_r[n] = \delta[n] y_e[n]$. The normalization factor $\delta[n]$ can be expressed as

$$\delta[n] = \sqrt{\frac{1}{P_s h_{te}[n] + N_2}}. \tag{5}$$

The received signal $y_{r2}[n]$ at the MSR in the second phase is given by

$$y_{r2}[n] = \sqrt{P_e[n] h_{er}[n]} x_r[n] + z_3[n], \tag{6}$$

where $P_e[n]$ is the forwarding power of legitimate eavesdropper, $z_3[n]$ is the AWGN received at the MSR. Thus $z_3[n]$ follows $CN(0, N_3)$. We use $\delta[n]$ to redefine the received signal $y_{r2}[n]$

$$\begin{aligned} y_{r2}[n] = \delta[n] & \sqrt{P_s P_e[n] h_{te}[n] h_{er}[n]} x_t[n] \\ & + \delta[n] \sqrt{P_e[n] h_{er}[n]} z_2[n] + z_3[n]. \end{aligned} \tag{7}$$

According to (4)–(8), the signal-to-noise ratio (SNR) at the MSR in the first and second phases can be respectively given by

$$\gamma_{r1} = \sqrt{\frac{P_s h_{tr}}{N_1}} \tag{8}$$

and

$$\gamma_{r2}[n] = \sqrt{\frac{P_s P_e[n] h_{te}[n] h_{er}[n]}{P_e[n] h_{er}[n] + P_s h_{te}[n] N_3 + N_2 N_3}}. \tag{9}$$

The achievable data rate in bits/second/Hz (bps/Hz) of the suspicious link in $\mathcal{F}$ can be given by

$$R_{R1}[n] = \log(1+\gamma_{r1}+\gamma_{r2}[n]), n \in \mathcal{F}. \tag{10}$$

In set $\mathcal{J}$, for the eavesdropping link, we define the Signal to Noise Ratio (SNR) as $\gamma_e[n] = \frac{P_s h_{te}[n]}{N_2}$, and for the suspicious link, we define the Signal to Interference plus Noise Ratio (SINR) as $\gamma_r[n] = \frac{P_s h_{tr}}{N_1+Q[n]h_{er}[n]}$, where $Q[n]$ is the jamming power of the legitimate eavesdropper. The achievable data rate of the eavesdropping link and the suspicious link at time slot n are respectively expressed as

$$R_E[n] = \log(1+\frac{P_s h_{te}[n]}{N_2}), n \in \mathcal{J}, \tag{11}$$

and

$$R_{R2}[n] = \log(1+\frac{P_s h_{tr}}{Q[n]h_{er}[n]+N_1}), n \in \mathcal{J}. \tag{12}$$

Therefore, the effective eavesdropping rate is defined as [13]

$$R_{EV}[n] = \begin{cases} R_{R1}[n], & R_E[n] \geq R_{R1}[n], n \in \mathcal{F}, \\ R_{R2}[n], & R_E[n] \geq R_{R2}[n], n \in \mathcal{J}, \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

III. Problem Formulation and Optimal Power Allocation for Legitimate Eavesdropping

In this section, we maximize the effective eavesdropping rate throughput flight time by optimizing power of legitimate eavesdropper. The problem can be formulated as follows:

$$\begin{aligned} (P1): \max \quad & R_{EV} = \sum_{n=1}^{N} R_{EV}[n] && (14) \\ \text{s.t.} \quad & \sum_{n\in\mathcal{F}} P_e[n] + \sum_{n\in\mathcal{J}} Q[n] \leq Q_{max}, && (15) \\ & P_e[n] \geq 0, Q[n] \geq 0, && (16) \\ & R_E[n] \geq R_{R1}[n], n \in \mathcal{F}, && (17) \end{aligned}$$

where (15) is to guarantee the power constraint of the legitimate eavesdropper, (17) is to guarantee that the legitimate eavesdropper can eavesdrop successfully when the legitimate eavesdropper is worked as a spoofing relay.

Lemma 1: The maximum effective eavesdropping rate in $\mathcal{J}$ is obtained if and only if $R_E[n] = R_{R2}[n]$ [12], the effective eavesdropping rate $R_{EV}[n] = R_{R2}[n]$. At time slot n, $n \in \mathcal{J}$, the optimal jamming power $Q^*[n]$ is the jamming power make $R_E[n] = R_{R2}[n]$.

$$Q^*[n] = \frac{h_{tr}N_2 - h_{te}[n]N_1}{h_{te}[n]h_{er}[n]}. \tag{18}$$

Proof: To guarantee $R_E[n] \geq R_{R2}[n]$, the legitimate eavesdropper should send the jamming signal with the power $Q[n]$ and $Q[n] \geq \frac{h_{tr}N_2 - h_{te}[n]N_1}{h_{te}[n]h_{er}[n]}$. We know that $R_{R2}[n] = \log(1+\frac{P_s h_{tr}}{N_1+Q[n]h_{er}[n]})$,we can derive that $R_{R2}[n]$ monotonically decreases with $Q[n]$, when $Q[n] = \frac{h_{tr}N_2 - h_{te}[n]N_1}{h_{te}[n]h_{er}[n]}$, $R_{R2}[n]$ can obtain the maximum value. Therefore, we can derive maximum $R_{R2}[n]$ when $R_E[n] = R_{R2}[n]$.

Based on *Lemma* 1, we can derive the optimal jamming power $Q^*[n]$ in $\mathcal{J}$. In terms of constraint (17), we further have

$$P_e[n] \leq \frac{(h_{te}[n]N_1 - h_{tr}N_2)(P_s h_{te}[n]N_3 + N_1N_3)}{h_{tr}h_{er}[n]N_2^2}, n \in \mathcal{F}. \tag{19}$$

Thus, the problem can be reformulated as

$$\begin{aligned} (P2): \max \quad & R_{EV} = \sum_{n=1}^{N} R_{EV}[n] && (20) \\ \text{s.t.} \quad & \sum_{n\in\mathcal{F}} P_e[n] + \sum_{n\in\mathcal{J}} Q[n] \leq Q_{max}, && (21) \\ & P_e[n] \geq 0, Q[n] \geq 0, && (22) \\ & \text{constraint of (19).} && (23) \end{aligned}$$

We solve (P2) in two scenarios, one is that there is enough power for legitimate eavesdropper to eavesdrop successfully and the other is that there is not enough power for legitimate eavesdropper to ensure successful eavesdropping at all time slots.

A. Scenario 1: Legitimate Eavesdropper with Enough Power to Successfully Eavesdropping

In this scenario, the legitimate eavesdropper can eavesdrop all time slots. Therefore, we define Q_J as sum of jamming power and $Q_J = \sum_{n\in\mathcal{J}} Q^*[n]$, the objective function can be written as

$$R_{EV}[n] = \begin{cases} R_{R1}[n], & R_E[n] \geq R_{R1}[n], n \in \mathcal{F}, \\ R_{R2}[n], & R_E[n] \geq R_{R2}[n], n \in \mathcal{J}, \end{cases} \tag{24}$$

where $R_{R2}[n] = \log(1+\frac{P_s h_{tr}}{N_1+Q^*[n]h_{er}[n]})$, we have $R_{R2} = \sum_{n\in\mathcal{J}} R_{R2}[n]$, the problem can be reformulated as follows.

$$\begin{aligned} (P3): \max \quad & R_{EV} = \sum_{n\in\mathcal{F}} R_{R1}[n] + R_{R2} && (25) \\ \text{s.t.} \quad & \sum_{n\in\mathcal{F}} P_e[n] + Q_J \leq Q_{max}, && (26) \\ & P_e[n] \geq 0, && (27) \\ & \text{constraint of (19).} && (28) \end{aligned}$$

(P3) is a convex optimization problem, which can be solved by standard convex optimization techniques such as the interior-point method.

B. Scenario 2: Legitimate Eavesdropper with Limited Power to Eavesdrop

In this scenario, there is not enough power for the legitimate eavesdropper to send jamming signals in $\mathcal{J}$, so the problem towards to reasonably allocate jamming and relay power. The problem (P2) is a non-convex optimization problem that is difficult to solve. In what follows, we divide the problem (P2) into two subproblems, we develop an iterative algorithm to solve (P2) by optimizing the relay power with fixed jamming power and optimizing the jamming power with fixed relay power.

For any given jamming power, the problem can be written like the problem (P3), we can solve it by standard convex optimization techniques.

For any given relay power, since the relay power and effective eavesdropping rate in set $\mathcal{F}$ are constant value, we can only optimize jamming power in set $\mathcal{J}$. According to *Lemma* 1, the optimal power is $Q^*[n]$, we can define R_{R2} as

$$R_{R2}[n] = \log(1 + \frac{P_s h_{tr}}{Q^*[n]h_{er}[n] + N_1}), n \in \mathcal{J}. \tag{29}$$

The objective function can be given by

$$R_{EV2}[n] = \begin{cases} R_{R2}[n], & R_E[n] \geq R_{R2}[n], \\ 0, & \text{otherwise.} \end{cases} \tag{30}$$

And the problem can be formulated as follows

$$(P4): \max \quad R_{EV2} = \sum_{n \in \mathcal{J}} R_{EV2}[n] \tag{31}$$

$$\text{s.t.} \quad P_e + \sum_{n \in \mathcal{J}} Q[n] \leq Q_{max}, \tag{32}$$

$$Q[n] \geq 0. \tag{33}$$

We introduce the following indicator function in set $\mathcal{J}$ to denote whether the legitimate eavesdropper has eavesdropped successfully or not:

$$R[n] = \begin{cases} 1, & R_E[n] \geq R_{R2}[n], \\ 0, & \text{otherwise.} \end{cases} \tag{34}$$

Therefore, we can define the effective eavesdropping rate as

$$R_{EV2}[n] = R[n]R_{R2}[n], n \in \mathcal{J}. \tag{35}$$

However, considering the actual situation, there is not enough power for legitimate eavesdropper to send the jamming signal at every time slot n, $n \in \mathcal{J}$. In this case, the jamming power $Q[n]$ at some time slots can not achieve $Q^*[n]$, the optimal scheme is to set $Q[n] = 0$, thus we can derive $R_{EV2}[n] = 0, R_E[n] < R_{R2}[n]$, $R[n] = 0$. At the other slots, the jamming power $Q[n]$ can achieve $Q^*[n]$, according to *Lemma* 1 the optimal scheme is to set $Q[n] = Q^*[n]$, and we derive $R_E[n] \geq R_{R2}[n]$, $R[n] = 1$. Therefore, $Q[n]$ in $\mathcal{J}$ can be given by

$$Q[n] = \begin{cases} Q^*[n], & R_E[n] \geq R_{R2}[n], \\ 0, & \text{otherwise.} \end{cases} \tag{36}$$

Thus, the jamming power at time slot n can be expressed as

$$Q[n] = R[n]Q^*[n], n \in \mathcal{J}. \tag{37}$$

By introducing the indicator function, the problem can be reformulated as follows:

$$(P5): \max \quad R_{EV2} = \sum_{n \in \mathcal{J}} R[n]R_{R2}[n] \tag{38}$$

$$\text{s.t.} \quad P_e + \sum_{n \in \mathcal{J}} R[n]Q^*[n] \leq Q_{max}, \tag{39}$$

$$Q[n] \geq 0, R[n] \in \{0, 1\}. \tag{40}$$

The problem (P4) is a non-convex optimization problem, which can not be solved by standard convex optimization techniques. We consider indicator function into the problem (P4) transforming it to an integer linear programming problem (P5). According to above analysis, we can derive the following conclusion.

If $R_E[n] < R_{R2}[n]$, in some time slots, we send optimal Jamming power $Q^*[n] = \frac{h_{tr}N_2 - h_{te}[n]N_1}{h_{te}[n]h_{er}[n]}$ and derive $R_{EV2}[n] = \log(1 + \frac{P_s h_{tr}}{N_1 + Q^*[n]h_{er}[n]})$, $R[n] = 1$. At the other time slots, we will not send jamming power for saving power, we can derive $R_{EV2}[n] = 0$, $R[n] = 0$. Is that, if $R[n] = 1$, the legitimate eavesdropper must allocate jamming power to jam the MST at time slot n and the optimal jamming power is $Q^*[n]$. Therefore, the problem (P5) can be solved by 0-1 integer linear programming.

Based the analysis of two subproblems, we can solve the problem (P2) by algorithm 1. The following is the algorithm 1, which optimize relay power by iterating jamming power obtained by 0-1 integer linear programming.

Algorithm 1 Iterative Jamming Power Optimization (IJPO) Algorithm

```
Initialize the UAV's trajectory.
Obtain jamming power allocation $\mathcal{M}$ by 0-1 integer linear programming.
Sort selected jamming power set $\mathcal{M}$ in ascend and derive a ordered jamming power set $\mathcal{Q}$ with size of $m$, that is the number of time slots in set $\mathcal{J}$.
Input $Q_J = 0$, $Q_{max}$
for all $j = 1$ to $m$ do
    allocate $Q[1:j]$ for jamming
    $Q_J \leftarrow Q_J + Q[j]$
    Solve problem (P3) by the standard convex optimization to obtain the new relay power allocation $\{P_e[n]\}$,$n \in \mathcal{F}$, and $P$ is the sum of $\{P_e[n]\}$.
    $Q_{used} \leftarrow Q_J + P$
    for all $k = j + 1$ to $m$ do
        if $Q_{max} - Q_{used} \geq Q[k]$ then
            allocate $Q[k]$ for jamming
            $Q_{used} \leftarrow Q_{used} + Q[k]$
        else
            break
        end if
    end for
    Record the total effective eavesdropping rate and corresponding power allocation scheme
end for
```

Note that the algorithm 1 contains standard convex optimization and integer linear programming algorithm, thus, the algorithm complexity of it is relatively high. The overall complexity of algorithm 1 is $\mathcal{O}(mN^{5.5})$.

IV. Numerical Results

We provide numerical results to validate performance of the proposed power allocation scheme. We assume that the

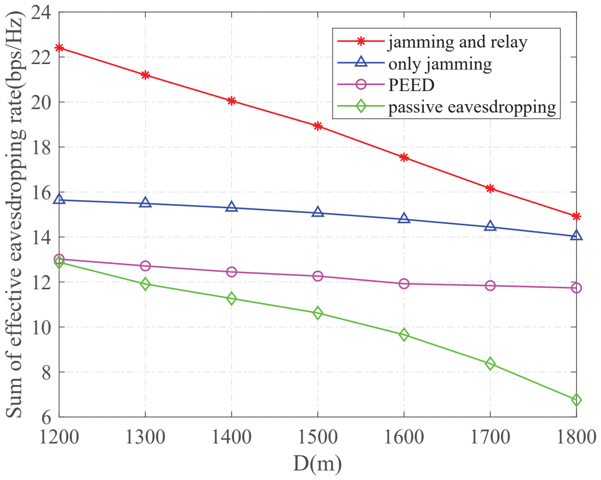

Fig. 2: The sum of effective eavesdropping rate of four schemes by beginning distance D meters between the legitimate eavesdropper and the MST(N=50).

distance between the MST and the MSR is 2000 meters. The maximum flying speed of legitimate eavesdropper is $V_1 = 50$ m/s and the maximum flying speed of MST and MSR is $V_2 = V_3 = 20$ m/s. The communication bandwidth B_0 per link is 1 MHz with the carrier frequency at 5 GHz, we assume the noise power spectrum density $N0$ at the legitimate eavesdropper and the MSR are equal and the value is -170 dBm/Hz. Thus the noise power $N_1 = N_2 = N_3 = N0B_0 = -110$ dBm. The channel power gain at the reference distance $d_0 = 1$ meter is assumed to be $\beta_0 = -60$ dB [15]. The transmit power of MST is $P_s = 10$ dBm.

A. Legitimate Eavesdropper with Enough Power

We simulate a linear predetermined trajectory in this part, and we set the maximum power of the legitimate eavesdropper $Q_{max} = 1$ W. Without loss of generality, we compare jamming and relay scheme with three legitimate eavesdropping schemes: (i) passive eavesdropping scheme: the legitimate eavesdropper will not send jamming signals or forward signals to the MSR. (ii) PEED scheme: the legitimate eavesdropper adopts proactive eavesdropping with equally distributed (PEED) jamming power. (iii) only jamming scheme: the legitimate eavesdropper adopt optimal jamming power allocation.

Fig. 2 presents the sum of effective eavesdropping rate obtained by four schemes. The legitimate eavesdropper starts flying at D-meters above the MST. Obviously, these two schemes, which adopt optimal jamming power allocation outperform the PEED scheme and the passive eavesdropping scheme. PEED scheme outperforms passive eavesdropping scheme by adopting proactive eavesdropping. Meanwhile, with the increase of D, the number of time slots for the legitimate eavesdropper is worked as relay decrease and the eavesdropping link becomes more weaker. Therefore, the sum of effective eavesdropping rate of jamming and relay scheme will decrease as D increases. Comparing with only jamming scheme, the sum of effective eavesdropping rate obtained by relay and jamming scheme increases.

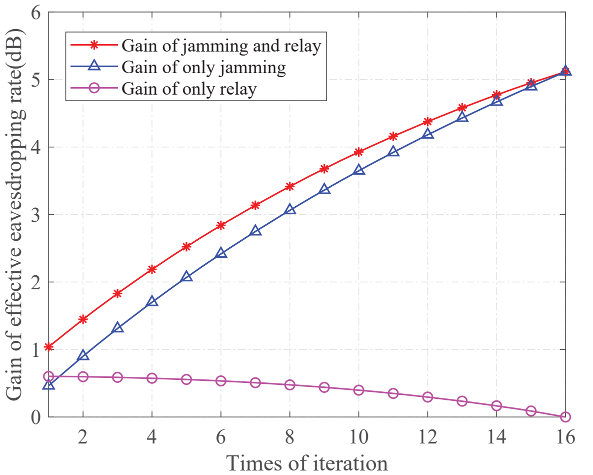

Fig. 3: The gain of effective eavesdropping rate of three schemes for each iteration when N = 50, D = 1800m.

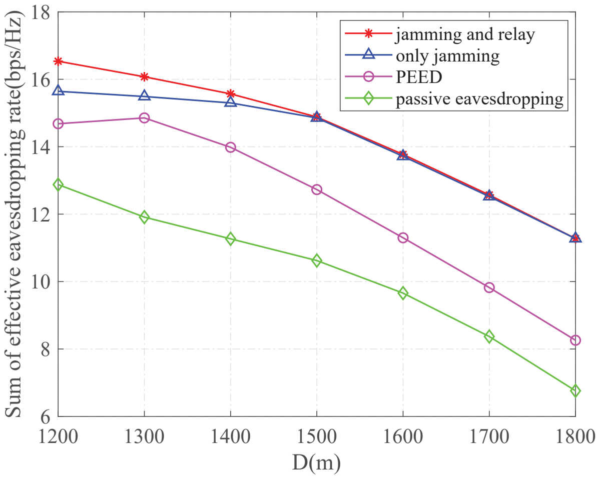

Fig. 4: The sum of effective eavesdropping rate of four schemes by beginning distance D meters between the legitimate eavesdropper and the MST(N=50).

B. Legitimate Eavesdropper without Enough Power

We simulate a linear predetermined trajectory in this part, and we set $Q_{max} = 0.1$ W. We compare IJPO algorithm with the following three legitimate eavesdropping schemes: (i) passive eavesdropping scheme. (ii) PEED scheme. (iii) only jamming scheme: the legitimate eavesdropper adopts jamming power allocation scheme obtained by 0-1 integer linear programming.

Fig. 3 presents the gain of effective eavesdropping rate for each iteration in algorithm 1. We derive the gain of only jamming, only relay and jamming and relay from each iteration. At the first iteration, the gain of relay is more than the gain of jamming, however, the total gain is lowest in entire iteration process. The maximum gain of the effective eavesdropping rate is obtained at last iteration, it means that we can obtain the maximum sum of effective eavesdropping rate when all power is used for jamming.

As shown in Fig. 4, we can see that IJPO algorithm outperforms only jamming algorithm when $D < 1500m$, the reason is that there is enough power for legitimate eavesdropper to jam the MSR at $\mathcal{J}$. However, when $D \geq 1500m$, the IJPO algorithm and only jamming algorithm get almost same effective eavesdropping rate, because there is very little power for relay since all power is first used for jamming. When power of the legitimate eavesdropper is not enough, the optimal power allocation scheme is to prioritize jamming.

V. Conclusion

In this paper, we study the power allocation in a wireless surveillance system with three UAVs. One UAV is a legitimate eavesdropper that proactively eavesdrops suspicious communications between two other UAVs, and moreover, the legitimate eavesdropper enhances the effective eavesdropping rate via jamming and spoofing. An optimal power allocation scheme is designed when the legitimate eavesdropper UAV has enough power. Furthermore, a more realistic situation that the UAV has limited power is considered. We develop an iterative jamming power optimization (IJPO) algorithm to allocate jamming and relay power. The simulation results show that 1) with enough power, the legitimate eavesdropper improves eavesdropping performance by introducing spoofing and jamming techniques, and 2) with a limited power constraint, the legitimate eavesdropper obtains maximum effective eavesdropping rate throughout flight time when all power is used for jamming.

References

[1] Y. Zeng, R. Zhang, and T. J. Lim. Wireless communications with unmanned aerial vehicles: opportunities and challenges. *IEEE Communications Magazine*, 54(5):36–42, May 2016.

[2] L. Gupta, R. Jain, and G. Vaszkun. Survey of important issues in uav communication networks. *IEEE Communications Surveys Tutorials*, 18(2):1123–1152, Secondquarter 2016.

[3] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng. Robust trajectory and transmit power design for secure uav communications. *IEEE Transactions on Vehicular Technology*, 67(9):9042–9046, Sep. 2018.

[4] Q. Wang, Z. Chen, and H. Li. Energy-efficient trajectory planning for uav-aided secure communication. *China Communications*, 15(5):51–60, May 2018.

[5] Y. Zeng, R. Zhang, and T. J. Lim. Throughput maximization for uav-enabled mobile relaying systems. *IEEE Transactions on Communications*, 64(12):4983–4996, Dec 2016.

[6] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha. Energy-efficient cooperative relaying for unmanned aerial vehicles. *IEEE Transactions on Mobile Computing*, 15(6):1377–1386, June 2016.

[7] X. Jiang, Z. Wu, Z. Yin, and Z. Yang. Power and trajectory optimization for uav-enabled amplify-and-forward relay networks. *IEEE Access*, 6:48688–48696, 2018.

[8] H. Lee, S. Eom, J. Park, and I. Lee. Uav-aided secure communications with cooperative jamming. *IEEE Transactions on Vehicular Technology*, 67(10):9385–9392, Oct 2018.

[9] A. Li and W. Zhang. Mobile jammer-aided secure uav communications via trajectory design and power control. *China Communications*, 15(8):141–151, Aug 2018.

[10] J. Xu, L. Duan, and R. Zhang. Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels. *IEEE Wireless Communications Letters*, 5(1):80–83, Feb 2016.

[11] Y. Zhang, X. Jiang, C. Zhong, and Z. Zhang. Performance of proactive eavesdropping in dual-hop relaying systems. In *2017 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6, Dec 2017.

[12] B. Li, Y. Yao, H. Zhang, Y. Lv, and W. Zhao. Energy efficiency of proactive eavesdropping for multiple links wireless system. *IEEE Access*, 6:26081–26090, 2018.

[13] Y. Zeng and R. Zhang. Wireless information surveillance via proactive eavesdropping with spoofing relay. *IEEE Journal of Selected Topics in Signal Processing*, 10(8):1449–1461, Dec 2016.

[14] H. Lu, H. Zhang, H. Dai, W. Wu, and B. Wang. Proactive eavesdropping in uav-aided suspicious communication systems. *IEEE Transactions on Vehicular Technology*, pages 1–1, 2018.

[15] Z. Mobini, B. K. Chalise, M. Mohammadi, H. A. Suraweera, and Z. Ding. Proactive eavesdropping using uav systems with full-duplex ground terminals. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, May 2018.

[16] X. Wang, K. Li, S. S. Kanhere, D. Li, X. Zhang, and E. Tovar. Pele: Power efficient legitimate eavesdropping via jamming in uav communications. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 402–408, June 2017.

[17] Umberto Mengali and Aldo N. DAndrea. *Synchronization Techniques for Digital Receivers*. 1997.