Conference Paper

PELE: Power Efficient Legitimate Eavesdropping via Jamming in UAV Communications

Xiaoming Wang
Kai Li*
Salil S. Kanhere
Demin Li
Xiaolu Zhang
Eduardo Tovar*

CISTER-TR-170404
PELE: Power Efficient Legitimate Eavesdropping via Jamming in UAV Communications

Xiaoming Wang, Kai Li*, Salil S. Kanhere, Demin Li, Xiaolu Zhang, Eduardo Tovar*

*CISTER Research Centre
Polytechnic Institute of Porto (ISEP-IPP)
Rua Dr. António Bernardino de Almeida, 431
4200-072 Porto
Portugal
Tel.: +351.22.8340509, Fax: +351.22.8321159
E-mail: http://www.cister.isep.ipp.pt

Abstract

We consider a wireless information surveillance in UAV network, where a legitimate unmanned aerial vehicle (UAV) proactively eavesdrops communication between two suspicious UAVs. However, challenges arise due to lossy airborne channels and limited power of the UAV. In this paper, we study an emerging legitimate eavesdropping paradigm that the legitimate UAV improves the eavesdropping performance via jamming the suspicious communication. Moreover, a power efficient legitimate eavesdropping scheme, PELE, is proposed to maximize the number of eavesdropped packets from the legitimate UAV while maintaining a target signal to interference plus noise ratio at the suspicious link. Numerical results are shown to validate the performance of PELE. Additionally, four typical fading channel models are applied to the network so as to investigate their impact on PELE.
PELE: Power Efficient Legitimate Eavesdropping via Jamming in UAV Communications

Xiaoming Wang∗, †, Kai Li‡, Salil S. Kanhere†, Demin Li∗, Xiaolu Zhang∗, and Eduardo Tovar‡
∗College of Information Science and Technology, Donghua University, China
†Earthquake Administration of Shanghai Municipality, China
‡School of Computer Science and Engineering, The University of New South Wales, Australia

Email: wangyoucao78@163.com, deminli@du.edu.cn (corresponding author), xiaolu@126.com
Email: {kaili,emt}@isep.ipp.pt
Email: salil@cse.unsw.edu.au

Abstract—We consider a wireless information surveillance in UAV network, where a legitimate unmanned aerial vehicle (UAV) proactively eavesdrops communication between two suspicious UAVs. However, challenges arise due to lossy airborne channels and limited power of the UAV. In this paper, we study an emerging legitimate eavesdropping paradigm that the legitimate UAV improves the eavesdropping performance via jamming the suspicious communication. Moreover, a power efficient legitimate eavesdropping scheme, PELE, is proposed to maximize the eavesdropping rate at suspicious link. Additionally, four typical fading channel models are applied to the network so as to investigate their impact on PELE.

Index Terms—UAV, Power Efficiency, Eavesdropping, Jamming

I. INTRODUCTION

Thanks to recent technological advances, many types of Unmanned Aerial Vehicles (UAVs), more popularly known as drones, are being widely used in complex real world environments [1, 2]. The recent availability of cost-effective UAVs has considerably promoted its use in wireless surveillance for homeland defence [3, 4]. These existing works related to security and attack modelling arise from a broader national perspective and mostly, addresses eavesdropping as illegitimate attacks. However, with the rapid popularity of UAVs in the consumer market, criminals or terrorists can potentially use them to establish wireless communication for committing crimes and terrorism [5, 6]. Therefore, there is a growing need for government agencies to legibly monitor and eavesdrop wireless communications of suspicious UAVs [7]. In particular, we consider a surveillance scenario as shown in Fig. 1. A surveilling UAV, i.e., $UAV_L$, aims to eavesdrop a point-to-point wireless communication from a suspicious transmitter UAV ($UAV_{ST}$) to a suspicious receiver ($UAV_{SR}$). $UAV_{ST}$ controls its communication rate over the channel to maintain a target outage probability at $UAV_{SR}$. $UAV_L$ can successfully eavesdrop suspicious link only when its achievable data rate is no smaller than suspicious communication rate. $UAV_L$ is assumed to fly at a predetermined trajectory toward two suspicious UAVs, establishing a wireless eavesdropping link (between $UAV_{ST}$ and $UAV_L$) and a jamming link (between $UAV_L$ and $UAV_{SR}$). Moreover, $UAV_{ST}$ and $UAV_{SR}$ are assumed to fly following a collision-free formation flight, where they keep a prescribed relative distance and angle. The problem of reliably eavesdropping suspicious transmission is not trivial. Several critical challenges arise in such a surveillance scenario. First, the quality of eavesdropping and jamming links fluctuate over time due to the motion of $UAV_L$ relative to the suspicious UAVs. It is therefore critical to control the jamming power of $UAV_L$ according to the varying fading channel to eavesdrop efficiently. Second, jamming the suspicious transmission decreases the achievable data rate at the suspicious link, which in turn improves the eavesdropping rate at $UAV_L$. However, sending jamming signals without an efficient power allocation results in draining energy of $UAV_L$ due to limited battery capacity of the UAV. Third, the achievable data rate at $UAV_L$ is required to be no smaller than that at $UAV_{ST}$ so that the packets generated by $UAV_{ST}$ can be eavesdropped successfully.

In this paper, we aim to maximise the eavesdropping rate at $UAV_L$ via optimising its jamming power. Specifically, given the constraint of suspicious data rate, we formulate an optimisation problem for finding the optimal jamming power at $UAV_L$ to maximise the eavesdropping rate, which is polynomially solvable. Moreover, a power-efficient legitimate eavesdropping (PELE) scheme is proposed to facilitate the simultaneous eavesdropping and jamming for $UAV_L$ on the flight, which also derives the optimal jamming power by using linear programming.

In particular, PELE cognitively controls the jamming power over the lossy channel under the limited jamming power constraint. Furthermore, we apply four fading models, i.e., Rayleigh, Ricean, Weibull, and Nakagami, to the wireless links in order to validate the impact of fading states on the performance of PELE.

The rest of the paper is organised as follows: Section II presents the related work on security techniques in mobile ad-hoc networks. We discuss the network model in Section III. In Section IV, we formulate the optimal jamming problem,
and present the power efficient jamming scheme. Simulation results are shown in Section V, followed by a conclusion in Section VI.

### II. RELATED WORKS

Some existing works focus on communication security as wireless networks are prone to malicious attacks. Physical layer security is reconized as a promising approach to protect the communications confidentiality against eavesdroppers [8]. The method imposes different challenges in terms of key exchange and distribution, especially in the current trend of dynamic network configurations such as wireless sensor networks and ad-hoc networks. A theoretical communication scheme is presented to use multiple antennas to generate artificial noise to degrade the channel quality of eavesdroppers [9]. In [10], a low-density parity-check protocol is presented to achieve communication rates close to the fundamental security limits in wireless communications. The novel protocol uses a four step procedure to ensure wireless information-theoretic security: (i) common randomness via opportunistic transmission; (ii) message reconciliation; (iii) common key generation via privacy amplification; and (iv) message protection with a secret key. The authors in [11] introduce an idea of using the abstraction of a virtual array of physical arrays to provide security against eavesdropping. They solve the problem that using smart antennas at higher layers for security with an intelligent consideration of MAC and security issues. However, none of these works [9–11] consider the use of proactive eavesdropping to enhance network security.

Jamming the eavesdropper is an emerging approach to enhance the quality of secure wireless transmissions [12–15]. In [12], a cooperative jamming scheme is studied to help a legitimate user improve its data rate via sending jamming signal to eavesdropper. They study the power allocations for the transmitting and jamming users, and show that significant rate gains may be achieved when the eavesdropper has much higher SNR than the receivers. In [13], a self-protection scheme is developed to transmit the jamming signal to degrade the channel of eavesdropper. Using the proposed full-duplex scheme, the system is shown to be no longer interference-limited, in contrast to the half-duplex case. In [14], a hybrid artificial fast fading scheme is proposed to investigate the power allocation problem for passive eavesdropper. With this scheme, the eavesdropper will face a noncoherent Ricean fading single-input-ultiple-output channel, which achieves better secrecy performance. A joint cooperative beamforming, jamming and power allocation scheme is investigated to improve the security of an amplify-and-forward cooperative relay network in this correspondence [15]. This scheme addresses the problem of protecting the data transmissions in half-duplex communications. However, eavesdropping is taken as an illegitimate attack in [12–15]. As a result, they target on decreasing the eavesdropping performance. In general, there is lack of researches on controlling and legitimately eavesdropping suspicious wireless communications. A recent work is studied to fill this gap. In [16], the authors present an approach to improve the eavesdropping rate. However, [16] studies the proactive eavesdropping problem in the view of data rate controlling without considering trajectory variance between the $UAV_L$ and suspicious UAVs.

### III. NETWORK MODEL

Without loss of generality, we consider that the suspicious transmitter ($UAV_{ST}$) and the receiver ($UAV_{SR}$) work in an autonomous formation flight, where the two UAVs fly at a constant speed, and the distance between them is maintained as $D$ meters. The legitimate eavesdropper ($UAV_L$) patrols in a predetermined circular trajectory between $UAV_{ST}$ and $UAV_{SR}$ with a diameter $D$. Particularly, the wireless link dynamics that are affected by the distance between $UAV_L$ and the suspicious UAVs are identical on a semi-circle of the trajectory. As a result, we consider the trajectory of $UAV_L$ as a semi-circle, as shown in Fig. 1, for illustration in this paper. In fact, our algorithm developed in Section IV is general and can support other shapes of flight trajectory since we have considered different fading channels with path loss that is affected by the distance between hostile UAV pairs, regardless trajectories of UAVs. Moreover, Table I lists the fundamental variables that have been used in our system model.

![Fig. 1: Legitimate eavesdropping via jamming scenario.](image)

**TABLE I: List of fundamental variables that have been used**

<table>
<thead>
<tr>
<th>Variables</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_L(x)$</td>
<td>Legitimate monitor jamming power at time slot $x$</td>
</tr>
<tr>
<td>$\gamma_L(x)$</td>
<td>SNR of eavesdropping link at time slot $x$</td>
</tr>
<tr>
<td>$\gamma_s(x)$</td>
<td>SNR of suspicious link at time slot $x$</td>
</tr>
<tr>
<td>$K_1, K_2$</td>
<td>Two constants relating to the channel</td>
</tr>
<tr>
<td>$N_0$</td>
<td>Power of white Gaussian noise</td>
</tr>
<tr>
<td>$d_L(x)$</td>
<td>Distance between $UAV_L$ and $UAV_{ST}$ at time slot $x$</td>
</tr>
<tr>
<td>$d_{SR}(x)$</td>
<td>Distance between $UAV_L$ and $UAV_{SR}$ at time slot $x$</td>
</tr>
<tr>
<td>$p_{max}^{SR}$</td>
<td>Maximum jamming power of $UAV_L$</td>
</tr>
<tr>
<td>$n$</td>
<td>Gaussian random number</td>
</tr>
<tr>
<td>$\alpha_1, \alpha_2$</td>
<td>Path-loss exponent of wireless channel</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>Coefficient considered to adjust the weights of the autocorrelated component and independent component</td>
</tr>
<tr>
<td>$\delta$</td>
<td>SINR/SNR threshold</td>
</tr>
<tr>
<td>$\rho(x)$</td>
<td>Adaptive modulation and coding (AMC) rate at time slot $x$</td>
</tr>
<tr>
<td>$\epsilon$</td>
<td>The required instantaneous bit error rate</td>
</tr>
</tbody>
</table>
slot is denoted as $x$. We assume that $UAV_{ST}$ communicates with $UAV_{SR}$ in a TDMA fashion, however, it should be noted that our method is generalised and thus agnostic of the MAC protocol in use.

At time slot $x$, the channel gain $H_s(t)$ in the suspicious link, i.e., from $UAV_{ST}$ to $UAV_{SR}$, is given by the following expression \[ H_s(x) = \frac{\lambda H_s(x-1) + n\sqrt{1-\lambda^2}}{D^{\alpha_2}} \] (1)

where $\lambda$ is the coefficient considered to adjust the weights of the autocorrelated component and the independent component, and $\alpha_2$ denotes the path-loss exponent in the suspicious link. $n$ is a Gaussian random number generated by Additive White Gaussian Noise (AWGN). For the suspicious communication link, we define Signal to Interference plus Noise Ratio (SINR) on the jamming link, i.e., between $UAV_{ST}$ and $UAV_{SR}$, at time slot $x$ as $\gamma_s(x)$, which is given by

\[ \gamma_s(x) = \sqrt{H_s(x) \cdot K_2^{-1} \ln K_1 \cdot (2^\epsilon(x) - 1)} / N_0 + P_L(x) \] (2)

where $P_L(x)$ denotes the jamming power of $UAV_L$ at time slot $x$. $\rho(x)$ denotes the adaptive modulation and coding (AMC) rate of the $UAV_{ST}$ at time slot $x$, and the highest mode is denoted by $\rho_{max}$. $K_1$ and $K_2$ are two constants related to the channel. $N_0$ denotes the power of white Gaussian noise. $\epsilon$ is the required instantaneous bit error rate.

Likewise, the channel gain in the eavesdropping link, i.e., from $UAV_{ST}$ to $UAV_{L}$, at time slot $x$ is given by

\[ H_e(x) = \frac{\lambda H_e(x-1) + n\sqrt{1-\lambda^2}}{D^{\alpha_1}(x)} \] (3)

where $n$ is a Gaussian random number generated by AWGN. $\alpha_1$ denotes the path-loss exponent. $d_1(x)$ is the distance between $UAV_{L}$ and $UAV_{ST}$ at time slot $x$. Moreover, since the exact locations of suspicious UAVs are unknown by $UAV_L$, we present $d_1(x)$ and $d_2(x)$ based on the angle variation along the trajectory of $UAV_L$, which is denoted as $\theta(x)$. Given the diameter $D$, the location of $UAV_{L}$ is known as $(\frac{D}{2} \cos \theta(x), \frac{D}{2} \sin \theta(x))(\theta(x) \in [0, \pi])$, $d_1(x)$. Therefore, $d_1(x)$ is given by

\[ d_1(x) = \sqrt{\left( \frac{D}{2} \cos \theta(x) + \frac{D}{2} \right)^2 + \left( \frac{D}{2} \sin \theta(x) \right)^2} = \frac{\sqrt{2D}}{2} \sqrt{1 + \cos \theta(x)} \] (4)

and the distance between $UAV_{L}$ and $UAV_{SR}$, $d_2(x)$, is given by $d_2(x) = \sqrt{D^2 - d_1^2(x)}$. Note that $d_1(x)$ and $d_2(x)$ can be also estimated by other ways, e.g., measuring receiving signal strength, or signal angle of arrival of $UAV_{ST}$ or $UAV_{SR}$.

Due to the relative motion of $UAV_{L}$ to $UAV_{ST}$, the channel in the eavesdropping link presented here consists of two components, namely, an autocorrelated component that relies on the previous channel condition, and an independent component that is independent of previous channels. A coefficient $\lambda$ is considered to adjust the weights of the two components. Moreover, $\lambda$ decreases with the growth of the speed of $UAV_{L}$. We define Signal to Noise Ratio (SNR) of the eavesdropping link at time slot $x$ as $\gamma_e(x)$, which is

\[ \gamma_e(x) = \sqrt{H_e(x) \cdot K_2^{-1} \ln K_1 \cdot (2^\epsilon(x) - 1)} / N_0 \] (5)

Given $\gamma_e(x)$ and the regression model mapping SNR to Packets Reception Rate (PRR) \[ 19 \], the PRR of suspicious data packets eavesdropped by $UAV_L$ is denoted by $R(x)$, which is given by

\[ R(x) = (1 - \frac{1}{2} \exp^{-\beta_0 \gamma_e(x) + \beta_1 \psi(2f-l)}) \] (6)

where $\beta_0$ and $\beta_1$ are two constants in the regression model. Moreover, $\beta_0$ controls the shape of the regression curve and $\beta_1$ induces horizontal shifts of the curve. $f$ and $l$ denote frame size and preamble size of the data packet, respectively.

IV. LEGITIMATE EAVESDROPPING VIA JAMMING

In this section, we first formulate the optimal jamming problem, which maximises the amount of eavesdropped packets at the $UAV_L$. Next, we propose PELE, a power efficient jamming scheme for the legitimate eavesdropping to improve the eavesdropping rate.

A. Problem Formulation

We consider the wireless communication as shown in Fig. 1, where $UAV_L$ aims to eavesdrop the packet from $UAV_{ST}$ via jamming the suspicious transmission. Based on the notations in the system model, we formulate the optimization problem for finding the optimal jamming power to maximize the eavesdropped packets.

Assume that each suspicious data packet has $b$ bytes. The amount of data (in bytes) successfully eavesdropped is $\sum_{x=1}^{m} b \cdot R(x)$ given $m$ time slots. To guarantee that the legitimate jamming and eavesdropping is undetectable by the two suspicious UAVs, SINR of the suspicious link has to be maintained at a certain threshold $\delta$, which presents $\gamma_s(x) = \delta$. Specifically, the modulation of $UAV_{ST}$ that is used to transmit data to $UAV_{SR}$ is $\rho_{max}$ Quadrature Amplitude Modulation (QAM), where $\rho(x) \in \{1, \cdots, \rho_{max}\}$. When $\rho = 1$, the modulation is essentially the Binary Phase Shift Keying (BPSK). When $\rho = 2$, the modulation is the Quadrature Phase Shift Keying (QPSK). $\rho_{max}$ indicates the number of modulation levels available for rate adaptation.

Constraint $0 \leq \sum_{x=1}^{m} P_L(x) \leq P_{L_{max}}$ specifies that the average jamming power of $UAV_L$ during the eavesdropping period is required to be less than the maximum transmit power of the UAV, $P_{L_{max}}$. 
Then, the formulation of the problem is presented as follows.

\[ \max_{P_L(x),\rho(x)} \sum_{x=1}^{m} b \cdot R(x) \] (7)

subject to: \[ \gamma_s(x) = \delta \] (8)
\[ 0 \leq \sum_{x=1}^{m} P_L(x) \] (9)
\[ 1 \leq \rho(x) \leq \rho_{\text{max}} \] (10)

Furthermore, in terms of Constraint (8), we have

\[ \rho(x) = \log_2 \left( \frac{\delta^2 (N_0 + P_L(t))}{H_s(x) \cdot K_2^{-1} \ln \frac{K_s}{\epsilon}} + 1 \right) \] (11)

which indicates that the modulation level is adapted by \( UAV_{ST} \) in terms of the jamming power \( P_L(x) \) of \( UAV_L \).

Specifically, \( UAV_{ST} \) increases \( P_L(x) \) to transmit data with an increasing \( P_L(x) \) so that SINR of the suspicious link at time slot \( x \) is maintained at \( \delta \). Moreover, considering Constraint (10), the upper bound and the lower bound of the jamming power \( P_L(x) \) can be obtained by

\[ P_L(x) = \begin{cases} \frac{H_s(x) \cdot K_2^{-1} \ln \frac{K_s}{\epsilon}}{\delta^2} - N_0, & \text{if } \rho(x) = 1; \\ \frac{H_s(x) \cdot K_2^{-1} \ln \frac{K_s}{\epsilon}}{\delta^2} - N_0, & \text{if } \rho(x) = \rho_{\text{max}}; \\ \end{cases} \] (12)

Consequently, by substituting Equations (5), (6) and (11) into (7), (8) and (10), the optimisation problem is reformulated as follows.

**Optimal Jamming Problem:**

\[ \max_{P_L(x)} \sum_{x=1}^{m} (1 - \frac{1}{2}) \exp \left( \frac{\rho(x)}{H_s(x) \cdot K_2^{-1} \ln \frac{K_s}{\epsilon}} \right) \] (13)

subject to: \[ 0 \leq \sum_{x=1}^{m} P_L(x) \leq P_{L_{\text{max}}} \] (14)
\[ P_L(x) \geq \frac{H_s(x) \cdot K_2^{-1} \ln \frac{K_s}{\epsilon}}{\delta^2} - N_0 \] (14)
\[ P_L(x) \leq \frac{1}{\delta^2} \left( (2P_{L_{\text{max}}} - 1)H_s(x)K_2^{-1} \ln \frac{K_1}{\epsilon} \right) - N_0 \] (15)

B. PELE Algorithm

The optimal jamming power, \( P_L^*(x) \) in the optimisation problem is able to be derived by linear optimisation techniques, e.g., linear programming. Next, we propose the PELE algorithm to allocate jamming power for \( UAV_L \) in real time. The algorithm is shown in Algorithm 1. Specifically, the channel gains \( H_s(x), H_e(x) \) and \( N_0 \) are known by \( UAV_L \) at the beginning of time slot \( x \), since \( UAV_L \) overhears the channels of suspicious and eavesdropping link via channel probing [9]. Since \( \gamma_e(x) \geq \delta \) is required by \( UAV_L \) to successfully eavesdrop the suspicious transmission, we have

\[ P_L(x) \geq \frac{N_0 \cdot (H_s(x) - H_e(x))}{H_s(x)} \] (16)

where \( \rho(x) \) is given by Equation (11). Therefore, the jamming power at \( x = k \) is initialised as \( P_L^0(k) = \frac{N_0 \cdot (H_s(x) - H_e(x))}{H_s(x)} \).

Next, \( P_L^0(k) \) is examined by \( UAV_L \) if the three constraints in the optimisation problem are satisfied. Specifically, if one of the constraint does not hold, it indicates that the required jamming power is much higher than the optimal solution, i.e., the link quality of the eavesdropping link is too low to decode the suspicious packet. In this case, \( UAV_L \) does not send the jamming signal to \( UAV_{SR} \) for purpose of power efficiency.

Moreover, if \( \sum_{k=1}^{L} P_L^0(k) \leq P_{L_{\text{max}}} \) and Constraints (14) and (15) hold, the optimisation problem is derived by \( UAV_L \), and the optimal jamming power \( P_L^*(x) \) is obtained.

**Algorithm 1 PELE**

1: \( k \) denotes the current time slot when \( UAV_L \) sends jamming signal.
2: **Initialise**: \( P_L^0(k) = \frac{N_0 \cdot (H_s(x) - H_e(x))}{H_s(x)} \).
3: **Input**: \( D, n, \lambda, \alpha_1, \alpha_2 \).
4: **Algorithm**: \( UAV_L \) overcomes the channels on suspicious and eavesdropping links.
5: if \( \sum_{k=1}^{L} P_L^0(k) \leq P_{L_{\text{max}}} \) or \( H_s(x)K_2^{-1} \ln \frac{K_1}{\epsilon} - N_0 \leq P_L^0(k) \leq \frac{1}{\delta^2} \left( (2P_{L_{\text{max}}} - 1)H_s(x)K_2^{-1} \ln \frac{K_1}{\epsilon} \right) - N_0 \) then
6: derive the Optimal Jamming Problem \( P_L^*(x) \)
7: else
8: \( P_L^*(x) = 0 \)
9: end if

Note that the power consumption of executing PELE is much smaller than the jamming power of \( UAV_L \), which is negligible. Moreover, the time complexity of PELE is \( O(m) \), which depends on the number of slots. Therefore, PELE algorithm can be conducted in real time due to the linearity of the proposed Optimal Jamming Problem.

V. SIMULATION EVALUATION

In this section, we provide numerical results to validate the performance of our proposed PELE algorithm. Furthermore, we apply Rayleigh, Ricean, Weibull, and Nakagami channel to the wireless links, respectively, so as to investigate the impact of different fading models on PELE algorithm.

A. Simulation Configurations

The distance between the two suspicious UAVs is \( D \), and the path length of \( UAV_L \) is \( \pi \times D/2 \). The patrolling speed of \( UAV_L \) is set to \( 10m/s \). The detailed system-level simulation parameters are shown in Table II.

\( UAV_{ST} \) communicates with \( UAV_{SR} \) in a TDMA fashion for suspicious collision-free transmission. Especially, we consider that a TDMA frame contains 7 time slots, and each of which is 10 seconds long. In one time slot, \( UAV_{ST} \) transmits its data to \( UAV_{SR} \), where \( UAV_L \) eavesdrops and decides to jam the suspicious communication. In addition, the suspicious link, eavesdropping link, and jamming link are assumed to be block-fading, i.e., the channels remain unchanged during each transmission block, and may change from block to block.
### B. Eavesdropping rate and Power consumption

Without loss of generality, we compare PELE with two legitimate eavesdropping strategies: (i) Proactive eavesdropping with constant jamming power, where the jamming power is set to $2 \times 10^{-9} W$, which is half of the maximum transmit power of our simulated UAV (In fact, the constant jamming power can be set to any value below $P_{L}^{max}$, which has little effects on simulation results as observed in the performance); and (ii) Passive eavesdropping without jamming, where $UAV_L$ passively overhears the packets broadcasted by $UAV_{ST}$, however, it does not send jamming signal to the suspicious link [16, 17, 20].

Fig. 2 presents the other two methods with optimal solutions in terms of the eavesdropping rate. The error bar shows the standard deviation over 100 runs. PELE outperforms non-

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K_1$</td>
<td>0.2</td>
</tr>
<tr>
<td>$K_2$</td>
<td>3</td>
</tr>
<tr>
<td>$\beta_0$</td>
<td>2.6</td>
</tr>
<tr>
<td>$\beta_1$</td>
<td>1</td>
</tr>
<tr>
<td>$f$</td>
<td>20</td>
</tr>
<tr>
<td>$l$</td>
<td>10</td>
</tr>
<tr>
<td>$\epsilon$</td>
<td>0.005</td>
</tr>
<tr>
<td>$N_0$</td>
<td>$3.98 \times 10^{-12} W$</td>
</tr>
<tr>
<td>$b$</td>
<td>100 byte/s</td>
</tr>
<tr>
<td>$\delta$</td>
<td>3</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>0.3</td>
</tr>
<tr>
<td>$\alpha_1$</td>
<td>3</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>2.5</td>
</tr>
<tr>
<td>$n$</td>
<td>0.005377</td>
</tr>
<tr>
<td>$D$</td>
<td>1700 m</td>
</tr>
<tr>
<td>$P_{L}^{max}$</td>
<td>$4 \times 10^{-9} W$</td>
</tr>
<tr>
<td>$\rho_{max}$</td>
<td>8</td>
</tr>
</tbody>
</table>

### C. Impact of typical fading models

We study the impact of four typical fading channel models, i.e., Rayleigh, Ricean, Weibull and Nakagami, with a specific coefficient component that is used to characterise the channel. In particular, the coefficient component of Rayleigh, Ricean, Weibull, and Nakagami is set to 2, 1, 2, and 0.5, respectively [21]. Fig. 4 shows that the eavesdropping rate achieved by PELE linearly grows with time in Rayleigh, Ricean and Weibull fading channels. PELE performs best in Weibull fading channel, but worst in Nakagami fading channel. Total received packets in Nakagami fading channel are much less than in other three channels with different time slots. This is because Weibull distribution is typically descriptive of channel fading with a dominant line-of-sight (LOS) propagation, which leads to a small amount of time the channel remains in a fade. For Nakagami channel with the coefficient component of 0.5, the received signal consists of a large number of noise waves with randomly distributed amplitudes, phase, and angles of arrival, which causes distortion and fading of the received signal. In Fig. 5, the eavesdropping rate drops with an increase of $D$ over the four fading models, which
results from channel gain of the suspicious link decreases. Weibull fading model achieves the highest eavesdropping rate while Nakagami model performs the worst. This can also be interpreted by the eavesdropping rate regarding to time, which is shown in Fig. 4.

![Fig. 4: Eavesdropping rate in 1000 time slots when $D = 1700m$](image)

![Fig. 5: Eavesdropping rate with different fading channels](image)

Fig. 4: Eavesdropping rate in 1000 time slots when $D = 1700m$

Fig. 5: Eavesdropping rate with different fading channels

Fig. 6 presents the power consumption of $UAV_L$ with the four fading models. Specifically, $UAV_L$ consumes the least jamming power in Nakagami model. This is because Nakagami model leads to a high channel fading, namely, small eavesdropping rate as observed in Fig. 4. Consequently, the optimal solution to the proposed Optimal Jamming Problem is not able to be achieved by PELE in some of the time slots; therefore, $UAV_L$ does not jam the suspicious link in order to save energy.

VI. CONCLUSION

In this paper, we considered a wireless information surveillance paradigm by investigating a scenario where a legitimate UAV aims to intercept a wireless communication between two suspicious UAVs over fading channels. We have formulated a power-efficient jamming problem for $UAV_L$ to eavesdrop the suspicious transmission with uncertain channel dynamics. PELE algorithm was proposed to maximise the eavesdropping rate, which jointly considers jamming power and maintaining outage rate of the suspicious link. Numerical results have shown that PELE outperforms non-Jamming and constant-Jamming schemes on eavesdropping rate. In addition, the impact of different fading models are also analysed on PELE.

ACKNOWLEDGMENT

This work was partially supported by Shanghai Science and Technology Committee program (15dz1207600), China Scholarship Council (No. 201504190015), National Funds through FCT/MEC (Portuguese Foundation for Science and Technology) and co-financed by ERDF (European Regional Development Fund) under the PT2020 Partnership, within the CISTER Research Unit (CEC/04234); also by FCT/MEC and the EU ECSEL JU under the H2020 Framework Programme, within project ECSEL/0002/2015, JU grant nr. 692529-2 (SAFECOP).

REFERENCES


