Energy Efficient Legitimate Wireless Surveillance of UAV Communications

Kai Li*
Razvan Christian Voicu
Salil S. Kanhere
Wei Ni
Eduardo Tovar*

*CISTER Research Centre

CISTER-TR-190103

2019/01/04

Energy Efficient Legitimate Wireless Surveillance of UAV Communications

Kai Li*, Razvan Christian Voicu, Salil S. Kanhere, Wei Ni, 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: kaili@isep.ipp.pt, voicu@gatech.edu, Wei.Ni@data61.csiro.au, emt@isep.ipp.pt

http://www.cister.isep.ipp.pt

Abstract

Unmanned Aerial Vehicles (UAVs) enhance connectivity and accessibility for civilian and military applications. Criminals or terrorists can potentially use UAVs for committing crimes and terrorism, thus endangering public safety. In this article, we consider that a legitimate UAV proactively eavesdrops suspicious UAVs' communication via sending jamming signals, and tracks their flight for preventing intended crimes and terror attacks. An energy-efficient jamming strategy is proposed for the legitimate UAV to maximize the amount of eavesdropped packets. Moreover, a tracking algorithm is developed for the legitimate UAV to track the suspicious flight by comprehensively utilizing eavesdropped packets, angle-of-arrival and received signal strength of the suspicious transmitter's signal. A new simulation framework is implemented to combine the complementary features of optimization toolbox with channel modeling (in Matlab) and discrete event-driven mobility tracking (in NS3). Moreover, numerical results validate the proposed algorithms in terms of packet eavesdropping rate and tracking accuracy of the suspicious UAVs' trajectory.

Energy Efficient Legitimate Wireless Surveillance of UAV Communications

Kai Li, *Member, IEEE,* Razvan Christian Voicu, *Student Member, IEEE,* Salil S. Kanhere, *Senior Member, IEEE,* Wei Ni, *Senior Member, IEEE,* and Eduardo Tovar

***Abstract*—Unmanned Aerial Vehicles (UAVs) enhance connectivity and accessibility for civilian and military applications. Criminals or terrorists can potentially use UAVs for committing crimes and terrorism, thus endangering public safety. In this article, we consider that a legitimate UAV is employed to track flight of suspicious UAVs for preventing safety and security threats. To obtain flight information of the suspicious UAVs, the legitimate UAV intentionally jams the suspicious receiver so as to force the suspicious UAV to reduce its data rate, and hence increase the eavesdropping success. An energy-efficient jamming strategy is proposed for the legitimate UAV to maximize the amount of eavesdropped packets. Moreover, a tracking algorithm is developed for the legitimate UAV to track the suspicious flight by comprehensively utilizing eavesdropped packets, angle-of-arrival and received signal strength of the suspicious transmitter's signal. A new simulation framework is implemented to combine the complementary features of optimization toolbox with channel modeling (in Matlab) and discrete event-driven mobility tracking (in NS3). Moreover, numerical results validate the proposed algorithms in terms of packet eavesdropping rate and tracking accuracy of the suspicious UAVs' trajectory.**

***Index Terms*—Unmanned Aerial Vehicles, Wireless information surveillance, Proactive eavesdropping, Flight tracking**

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. The recent availability of cost-effective UAVs has considerably promoted its use in wireless surveillance for homeland defense [1], [2]. However, with the rapidly growing popularity of UAVs in the consumer market, criminals or terrorists can potentially use them to establish wireless communication for committing crimes and terrorism, e.g., reconnoitring and locating targets together for dropping explosives [3], [4]. Therefore, there is a growing need for government agencies to legitimately eavesdrop critical data exchange of suspicious UAVs and monitor their flight. In particular, different from conventional wireless security that assumes communication links are used for lawful purposes and aims to maximize secrecy against illegitimate eavesdropping [5]–[7], we consider a legitimate information surveillance scenario, where a legitimate surveilling UAV aims to overhear the communication of suspicious UAVs while tracking their flight trajectory, as shown in Fig. 1, which contains a suspicious communication link, a wireless eavesdropping link and a jamming link. Specifically, the suspicious UAVs fly a collision-free formation flight, where they periodically exchange flight information so as to keep a prescribed relative distance and heading direction. Due to fluctuation of wireless channels over time, the suspicious transmitter controls its data rate over the channel to maintain a target outage probability at the suspicious receiver.

The suspicious receiver replies an acknowledgement message (ACK) when the data packet of the suspicious transmitter is successfully received. Otherwise, the data packet has to be retransmitted by the suspicious transmitter. Moreover, the legitimate UAV is able to jam the suspicious receiver in order to force the suspicious UAV to reduce its data rate, and hence increase the eavesdropping success [8]. The legitimate UAV can control its jamming power to improve packet eavesdropping rate, especially when the legitimate UAV is far from the suspicious transmitter and receiver. Note that jamming the ACK packet of the suspicious receiver can only leads to retransmission of the data packet at the suspicious transmitter, where the data rate of the suspicious transmitter is not adapted to the jamming power.

Note that employing UAV as the legitimate eavesdropper is due to the excellent mobility and maneuverability, as well as the limited power of both the legitimate and suspicious UAVs. In this case, the legitimate UAV is capable of following and maintaining a short distance from the suspicious UAVs on the flight in order to monitor and intercept potential safety-threatening messages and commands. We also note that eavesdropping the communication of suspicious UAVs and tracking their flight trajectory significantly affect each other in legitimate surveillance. As shown in Fig. 2, the flight trajectory of suspicious UAVs can be accurately tracked by the legitimate UAV if their flight information is eavesdropped. On the other hand, an accurate flight tracking guarantees that the suspicious UAVs are covered by the radio range of the legitimate UAV, which ensures their communications can be overheard.

The problem of efficiently eavesdropping suspicious

Kai Li, and Eduardo Tovar are with CISTER Research Centre, Portugal (E-mail:{kaili,emt}@isep.ipp.pt).

Razvan Christian Voicu is with Georgia Institute of Technology, Atlanta, USA (E-mail: voicu@gatech.edu).

Salil S. Kanhere is with The University of New South Wales, Australia (E-mail: salil.kanhere@unsw.edu.au).

Wei Ni is with Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia (E-mail: wei.ni@csiro.au).

transmission while tracking the suspicious flight is not trivial. Several critical challenges arise in such a surveillance scenario. First, given the time-varying, lossy airborne, fading channels, the legitimate UAV may not be able to precisely decode the entire message sent to the suspicious receiver as the received signal-to-noise ratio (SNR) (and accordingly the achievable data rate) at the legitimate UAV may not always be above the minimum threshold. Note that the suspicious transmitter can adapt its data rate so as to maintain a target outage probability at the suspicious receiver. It is therefore critical to control the jamming power of the legitimate UAV to ensure the received SNR is enough for decoding the data. Second, jamming the suspicious transmission can decrease the achievable data rate of the suspicious link, which in turn improves the number of eavesdropped packets, i.e., eavesdropping rate, at the legitimate UAV. However, sending jamming signals without an efficient power allocation would result in fast draining the energy of the legitimate UAV. Third, it could be possible that some suspicious packets are not successfully overheard due to poor SNR of the eavesdropping link. Thus, the legitimate UAV needs to be able to persistently track the suspicious flight trajectory given the uncertain channel dynamics.

In this paper, we aim to maximize the eavesdropping rate at the legitimate UAV via optimizing the energy expanded in jamming, given a certain Signal-to-Interference-plus-Noise Ratio (SINR) of the suspicious link. Specifically, an energy-efficient legitimate proactive eavesdropping scheme (PES) is proposed to facilitate the simultaneous eavesdropping and jamming for the legitimate UAV on the flight while deriving the optimal jamming power in polynomial time. In particular, by applying PES, the legitimate UAV eavesdrops all data exchanges between the two suspicious UAVs even when the address of their packets is periodically mutated. Furthermore, a tracking algorithm is studied to figure out waypoints of trajectory for the legitimate UAV by decoding the eavesdropped packet. In case the eavesdropped packet is not successfully decoded by using PES, the proposed tracking algorithm also utilizes angle-of-arrival (AOA) and received signal strength (RSS) of the suspicious UAV's signal to ensure the eavesdropping coverage of the legitimate UAV for the sake of persistent surveillance. In order to evaluate the performance of eavesdropping and tracking, a new simulation framework is implemented to combine the complementary features of optimization toolbox with channel modeling (in Matlab) and discrete event-driven mobility tracking (in NS3).

Note that eavesdropping the communication of suspicious UAVs can be performed even when the suspicious link is encrypted. Once the legitimate UAV successfully eavesdrops the suspicious data, a data hijacking algorithm, e.g., exhaustive-key-search, dictionary or brute force, can be carried out to decipher the eavesdropped packets. However, since we focus on efficient proactive eavesdropping for improving the eavesdropping rate, the data hijacking approach is beyond the scope of this paper.

The rest of the paper is organized as follows: Section II reviews the literature on wireless security and UAV tracking techniques. In Section III, the jamming power optimization problem is formulated while PES is proposed. Moreover, a legitimate tracking algorithm is also proposed for the legitimate UAV to track the suspicious flight trajectory. Simulation results are shown in Section IV, followed by a conclusion in Section V.

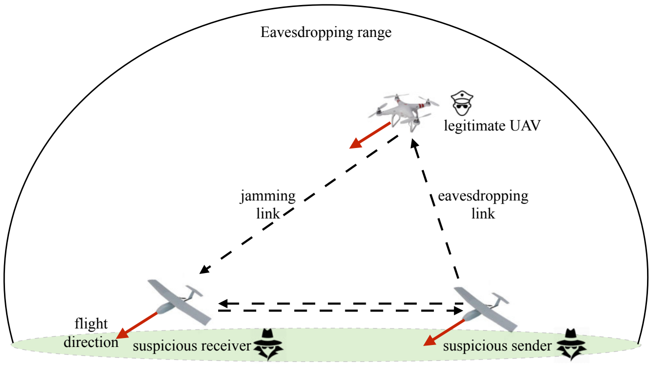


Fig. 1: A wireless surveillance network that contains a legitimate UAV, and two suspicious UAVs following a collision-free formation flight.

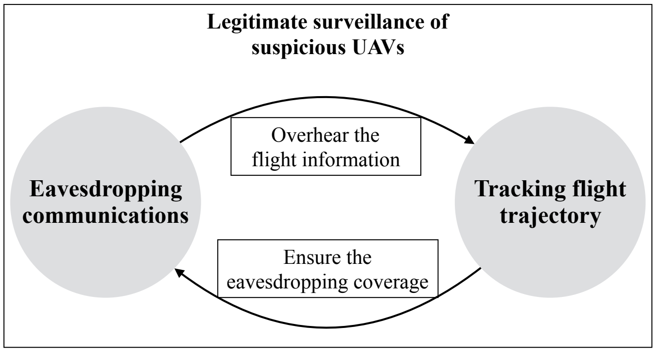

Legitimate surveillance of suspicious UAVs
Eavesdropping communications
Overhear the flight information
Tracking flight trajectory
Ensure the eavesdropping coverage

Fig. 2: Eavesdropping communications while tracking flight in legitimate surveillance of suspicious UAVs.

II. Related work

In this section, we review the literature on wireless communication security and UAV tracking strategies.

A. *Wireless security*

A low-density parity-check protocol is presented in [9] to secure wireless communication links against eavesdropping while achieving an improved data rate. The protocol uses randomness and key generation to ensure wireless communication security. In [10], a framework of key generation schemes is studied to exploit the randomness of wireless channels. In addition, a communication scheme is presented to use multiple antennas to generate artificial noises to degrade the channel quality of eavesdroppers [11]. The authors in [12] introduce an idea of using a virtual array of antennas to provide security against eavesdropping. They solve the problem of using smart antennas at higher layers for security with a consideration of MAC and security issues. As a complement to encryption techniques, physical layer security has been widely recognized as an anti-eavesdropping technique to enhance wireless security by exploiting the characteristics of wireless channels [13], [14]. In [15], physical layer security is studied to enhance data secrecy against eavesdropping in device-to-device communications underlaying cellular networks.

Jamming the eavesdropper is an emerging approach to improving the quality of wireless security. In [16], a jamming scheme is studied to help a legitimate user improve data secrecy via sending jamming signals to the eavesdropper. The transmit power is allocated for the jamming device, and a significant data rate gain can be achieved even when the eavesdropper has much higher SNR than the receiver. In [17], a self-protection scheme is developed to send jamming signals to degrade the channel quality of the eavesdropper. In [18], a hybrid artificial fast fading scheme is presented to allocate transmit powers for a jamming device. Given a non-coherent single-input-multiple-output channel, the jammer using this scheme achieves a high secrecy performance. A beamforming, jamming and power allocation scheme is studied to address data transmission security in an amplify and forward relay network [19]. Zhang *et al.* study jamming power control to improve data secrecy of two legitimate users with an untrusted relay [20]. A Stackelberg game is employed to derive transmit power of the users and the jamming power.

Eavesdropping is taken as an illicit passive attack in the literature, which targets on disrupting or disabling lawful wireless communications. Thus, their algorithms focus on improving the secrecy against eavesdropping, which is not applicable to legitimate wireless surveillance.

In general, there is a lack of research on legitimately eavesdropping suspicious UAVs' communication. Some recent work is trying to fill this gap. In [8], [21], [22], the authors present a number of approaches to improve the eavesdropping rate for the legitimate wireless surveillance. However, they study the proactive eavesdropping problem in the view of data rate controlling without considering the mobility and trajectory variance between the legitimate and suspicious nodes. In our previous work [23], a legitimate surveillance problem in UAV communications is formulated to eavesdrop the suspicious transmission with uncertain channel dynamics. In particular, channel gain information is known to the legitimate UAV at the beginning of each time slot since the legitimate UAV can overhear the channels of suspicious and eavesdropping link via channel probing. The jamming power of the legitimate UAV is cognitively adjusted according to the variation of the relative distance between the legitimate UAV and suspicious UAVs. The surveilling trajectory of the legitimate UAV is fixed as a circle around the suspicious UAVs in [23], and it is assumed that the flight of suspicious UAVs can be accurately tracked, which is not affected by communication link dynamics. Different from [23], in this work, the legitimate UAV has no apriori information of suspicious trajectory. Thus, the flight of the suspicious UAVs needs to be persistently tracked by the legitimate UAV for the wireless surveillance over time-varying channels.

B. UAV tracking strategies

For mobile target tracking with the UAV, the algorithms in the literature can be generally classified to two categories, i.e., *signal-based tracking* and *vision-based tracking*. In the first category, the UAV determines the target's motion based on different aspects of the received wireless signals such as RSS, AOA, or time difference of arrival (TDOA). A navigation law is developed for the UAV to track mobile ground units for communication relay establishment without the apriori knowledge on ground unit positions [24]. The navigation law employs two measurements for each ground unit, the RSS and AOA. Koohifar *et al.* [25] study UAVs that are equipped with wireless transceivers locate a moving radio transmitter. A tracking algorithm is developed to predict mobility of the target, and steers the tracking UAVs only based on the signal strength information obtained from the target. The authors in [26] consider a scenario with two non-collocated UAVs where their sensors measure TDOA over a number of emissions from a targeted moving radio transmitter. To track the target's movement using TDOA, the multiple devices need to be precisely synchronized to achieve meaningful TDOA measurements. Different from the tracking strategies solely relying on the received wireless signals, we propose a new tracking algorithm based on the proactive eavesdropping working with the *signal-based tracking* strategies.

In the second category, the UAV tracks the target by using onboard vision sensors, e.g., camera and optical sensor. The literatures [27]–[29] describe the development and evaluation of the vision-based collision detection and tracking algorithm suitable for UAVs. They also consider optical measurements from cameras onboard the UAV to estimate both the relative pose and relative velocities of another UAV or target object.

III. Energy Efficient Legitimate Wireless Surveillance

In this section, we firstly present channel model in suspicious link, eavesdropping link and jamming link. Secondly, we formulate the optimal jamming problem that maximizes the amount of eavesdropped packets at the legitimate UAV. Thirdly, the energy-efficient PES is proposed to improve the eavesdropping rate. Lastly, the legitimate tracking algorithm is investigated to pursue the suspicious UAVs.

A. Channel model

Without loss of generality, we assume that the suspicious transmitter (denoted by UAV$_{ST}$) communicates with receiver (denoted by UAV$_{SR}$) in a Time Division Duplex (TDD) fashion. The suspicious communication between UAV$_{ST}$ and UAV$_{SR}$ consists of m number of time slots, and each time slot is indicated by t. The distance between

TABLE I: List of fundamental variables that have been used

Variables	Descriptions
$P_L(t)$	Legitimate monitor jamming power at time slot t
P_L^{max}	Maximum jamming power of UAV$_L$
$P_{ST}(t)$	Transmit power of UAV$_{ST}$ at time slot t
$\gamma_e(t)$	SNR of eavesdropping link at time slot t
$\gamma_s(t)$	SNR of suspicious link at time slot t
$H_s(t)$	Channel gain in the suspicious link
$H_e(t)$	Channel gain in the eavesdropping link
K_1,K_2	Two constants relating to the channel
N_0	Power of white Gaussian noise
$d(t)$	Distance between UAV$_L$ and UAV$_{ST}$ at time t
$D(t)$	Distance between the two suspicious UAVs
n_1, n_2	Gaussian random variable
α_1, α_2	Path-loss exponent of wireless channel
λ_1, λ_2	Coefficient considered to adjust the weights of the autocorrelated component and independent component
δ	SINR/SNR threshold
$\rho(t)$	AMC rate at time slot t
ϵ	The required instantaneous bit error rate
$R(t)$	PRR of suspicious data packets eavesdropped by UAV$_L$

UAV$_{ST}$ and UAV$_L$ is $d(t)$ at time t. We consider that UAV$_{ST}$ and UAV$_{SR}$ move in an autonomous formation flight, where the two UAVs synchronize their flight speed at time slot t, and the distance between them is $D(t)$ meters. Moreover, the suspicious and legitimate UAVs fly in free space, where the signals reflected from the ground and surface of buildings are neglectable.

At time slot t, the channel gain $H_s(t)$ in the suspicious link, i.e., from UAV$_{ST}$ to UAV$_{SR}$, is given by the following expression [30], [31]

$$H_s(t) = \frac{\lambda_1 H_s(t-1) + n_1\sqrt{1-\lambda_1^2}}{D(t)^{\alpha_2}}, \tag{1}$$

where α_2 denotes the path-loss exponent in the suspicious link. n_1 is a complex Gaussian random variable. Due to relative motion of the UAVs, the channel presented here consists of two components, namely, an autocorrelated component that relies on the previous channel condition, and a component that is independent of previous channels. The coefficient λ_1 is considered to adjust the weights of the two components. Typically, λ_1 decreases with a growth of the flying speed of the UAV. We define the SINR of the suspicious link at time slot t as $\gamma_s(t)$ [23], which is given by

$$\gamma_s(t) = \sqrt{\frac{H_s(t)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}\cdot(2^{\rho(t)}-1)}{N_0 + P_L(t)}}, \tag{2}$$

where $P_L(t)$ denotes the jamming power of UAV$_L$ at t. $\rho(t)$ denotes the adaptive modulation and coding (AMC) rate of UAV$_{ST}$ at t, and the highest AMC mode is denoted by ρ_M. K_1 and K_2 are two constants related to the channel. N_0 denotes the power of the AWGN. ϵ is the required instantaneous bit error rate.

Likewise, the channel gain of the eavesdropping link, i.e., from UAV$_{ST}$ to UAV$_L$, at time slot t is given by

$$H_e(t) = \frac{\lambda_2 H_e(t-1) + n_2\sqrt{1-\lambda_2^2}}{d^{\alpha_1}(t)}, \tag{3}$$

where n_2 is a Gaussian random variable, and λ_2 is the coefficient adjusting the weights of the two components. α_1 denotes the path-loss exponent. $d(t)$ defines the distance between UAV$_{ST}$ and UAV$_L$, which varies with their time-variant movement. In addition, the channel gains $H_s(t)$, $H_e(t)$ and N_0 are known to UAV$_L$ at the beginning of time slot t, since UAV$_L$ can overhear the suspicious and eavesdropping links via channel probing [32].

We define SNR of the eavesdropping link at t as $\gamma_e(t)$, which is

$$\gamma_e(t) = \sqrt{\frac{H_e(t)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}\cdot(2^{\rho(t)}-1)}{N_0}}. \tag{4}$$

The eavesdropping and jamming are conducted in parallel at the same frequency, which may introduce self-interference from the jamming to the eavesdropping antenna. In our model, the self-interference at UAV$_L$ is assumed to be cancelled by separating its eavesdropping and jamming antennas for an extended distance, and employing advanced analog and digital self-interference cancellation methods [33], [34].

Given $\gamma_e(t)$ and the regression model mapping SNR to Packets Reception Rate (PRR) [35], the PRR of suspicious data packets eavesdropped by UAV$_L$, denoted by $R(t)$, is given by

$$R(t) = (1 - \frac{1}{2}e^{\beta_1 - \beta_0\gamma_e(t)})^{8(2f-l)}, \tag{5}$$

where β_0 and β_1 are two constants in the regression model. β_0 controls the shape of the regression curve and β_1 induces horizontal shifts of the curve. f and l denote the frame size and preamble size of a data packet, respectively. Moreover, we have $f > l$ as the frame must be longer than the preamble.

In addition, Table I lists the notations and parameters that are used in our channel model.

B. Problem formulation

UAV$_L$ aims to eavesdrop the packet from UAV$_{ST}$ via energy-efficiently jamming the suspicious transmission. Based on the notations in the channel model, we formulate the optimization problem for finding the optimal jamming power to maximize the number of eavesdropped packets.

The amount of data successfully eavesdropped is $\sum_{t=1}^{m} R(t)$ given m time slots. To guarantee that the legitimate jamming and eavesdropping is undetectable by the suspicious UAVs, the SINR of the suspicious link has to be maintained at a certain value δ, which presents $\gamma_s(t) = \delta$. Specifically, the modulation of UAV$_{ST}$ that is used to transmit data to UAV$_{SR}$ is $2^{\rho(t)}$ Quadrature Amplitude Modulation (QAM), where $\rho(t) \in \{1, \cdots, \rho_{max}\}$. When $\rho = 1$, the modulation is the Binary Phase Shift Keying (BPSK). When $\rho = 2$, the modulation is the Quadrature

Phase Shift Keying (QPSK). ρ_{max} indicates the number of modulation levels available for rate adaptation. Constraint $0 \leq P_L(t) \leq P_L^{max}, \forall t \in [1, m]$ specifies that the average jamming power of UAV$_L$ during the eavesdropping period must be no greater than the maximum transmit power of the UAV, P_L^{max}.

Then, the formulation of the problem is presented as follows.

$$
\begin{aligned}
\textbf{P1:} \quad & \max_{P_L(t)} \quad \sum_{t=1}^{m} R(t) \\
& subject\ to: \quad \gamma_s(t) = \delta && (6) \\
& \qquad\qquad 0 \leq P_L(t) \leq P_L^{max}, \forall t \in [1, m] && (7) \\
& \qquad\qquad 1 \leq \rho(t) \leq \rho_{max} && (8)
\end{aligned}
$$

However, the optimal jamming power cannot be explicitly determined in **P1**, since $\rho(t)$ in (6) is unknown to UAV$_L$. Thus, to solve **P1**, the expression of $\rho(t)$ is presented in terms of (6), which is

$$\rho(t) = \log_2\left(\frac{\delta^2 (N_0 + P_L(t))}{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}} + 1\right). \tag{9}$$

In particular, (9) indicates that the modulation level at UAV$_{ST}$ is adapted to the jamming power $P_L(t)$ at UAV$_L$. Specifically, UAV$_{ST}$ increases $\rho(t)$ to transmit data with an increasing $P_L(t)$ so that the SINR of the suspicious link at time slot t is maintained at δ. Moreover, considering Constraint (8), the lower bound and the upper bound of the jamming power $P_L(t)$ can be obtained by

$$P_L(t) = \begin{cases} \frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0, & \text{if } \rho(t) = 1; \\ \frac{(2^{\rho_{max}} - 1) H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0, & \text{if } \rho(t) = \rho_{max}. \end{cases} \tag{10}$$

Consequently, by substituting (4), (5) and (9) into **P1**, the optimization problem is reformulated as follows.

$$
\begin{aligned}
\textbf{P2:} \quad & \max_{P_L(t)} \sum_{t=1}^{m} \left(1 - \frac{1}{2} e^{\beta_1 - \beta_0 \delta \sqrt{\frac{H_e(t)}{H_s(t)} \cdot (1 + \frac{P_L(t)}{N_0})}}\right)^{8(2f-l)} \\
& subject\ to: \quad 0 \leq P_L(t) \leq P_L^{max}, \forall t \in [1, m] && (11) \\
& \qquad P_L(t) \geq \frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0 && (12) \\
& \qquad P_L(t) \leq \frac{1}{\delta^2}\left((2^{\rho_{max}} - 1) H_s(t) K_2^{-1} \ln \frac{K_1}{\epsilon}\right) - N_0 && (13)
\end{aligned}
$$

Furthermore, we have the following lemma.

Lemma 3.1: **P2** is monotonically increasing with respect to $P_L(t) \geq \frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0$.

Proof: Let $f_{\mathbf{P2}}(P_L(t))$ define the objective function of **P2**. The first-order derivative of $f_{\mathbf{P2}}(P_L(t))$ is given as (14). Due to $P_L(t) \geq \frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0$, the relationship in (15) can be known. Moreover, we have $(1 - \frac{1}{2} e^{\beta_1 - \beta_0 \sqrt{\frac{H_e(t) K_2^{-1} \ln \frac{K_1}{\epsilon}}{N_0}}})^{8(2f-l)-1} \geq 0$ since it is known that $R(t) \geq 0$. Thus, $(1 - \frac{e^{\beta_1 - \beta_0 \delta \sqrt{\frac{H_e(t)}{H_s(t)} (1 + \frac{P_L(t)}{N_0})}}}{2})^{8(2f-l)-1} \geq 0$, which leads to $f'_{\mathbf{P2}}(P_L(t)) \geq 0$. Therefore, we know that $f_{\mathbf{P2}}(P_L(t))$ is monotonically increasing, and the monotonicity of **P2** with respect to $P_L(t) \geq \frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0$ is verified. ■

C. Legitimate Eavesdropping Scheme

The optimal jamming power, $P_L^{\star}(t)$ in the problem **P2**, is able to be derived by convex optimization techniques, e.g., interior-point method. Next, we propose the PES to allocate jamming power for UAV$_L$ in real time, which is shown in Algorithm 1. Specifically, $\gamma_e(t) \geq \delta$ is required by UAV$_L$ to successfully eavesdrop the suspicious transmission, which gives (see Appendix for details)

$$P_L(t) \geq \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}, \tag{16}$$

where $\rho(t)$ is given by (9). Therefore, the jamming power can be initialized by $P_L^0(t) = \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}$.

Next, $P_L^0(t)$ is examined by UAV$_L$ if the three constraints in problem **P2** are satisfied. Specifically, if one of the constraints does not hold, it indicates that the required jamming power is much higher than the optimal solution, i.e., the quality of the eavesdropping link is too poor to decode the suspicious packet. In this case, UAV$_L$ eavesdrops without sending jamming signals to interfere suspicious transmission for the purpose of power efficiency. Moreover, if Constraints (11), (12) and (13) hold, the optimal jamming power $P_L^{\star}(t)$ is obtained by UAV$_L$ according to **P2**.

Algorithm 1 Proactive Eavesdropping Scheme

```
$k$ denotes the time slot when UAV$_L$ sends jamming signals.
Initialize: $P_L^0(t) = \frac{N_0 \cdot (H_s(t) - H_e(t))}{H_e(t)}$.
Input: $D, n, \lambda, \alpha_1, \alpha_2, \delta$.
UAV$_{ST}$ transmits the packet using $\rho(t)$ over the suspicious link, where the SINR is $\gamma_s(t)$.
UAV$_L$ overhears the packet in the eavesdropping link, where the SNR is $\gamma_e(t)$.
UAV$_L$ obtains $\rho(t)$ with regards to (9) and $P_L^0(t)$.
if $0 \leq P_L^0(t) \leq P_L^{max}$ then
    derive the problem P2 $\rightarrow P_L^{\star}(t)$.
    if $\frac{H_s(t) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}}{\delta^2} - N_0 \leq P_L^{\star}(t) \leq \frac{1}{\delta^2}\left((2^{\rho_{max}} - 1) H_s(t) K_2^{-1} \ln \frac{K_1}{\epsilon}\right) - N_0$ then
        PES is completed.
        t = t + 1.
    else
        $P_L^{\star}(t) \leftarrow P_L^0(t)$.
    end if
else
    $P_L^{\star}(t) \leftarrow 0$.
end if
Output: $P_L^{\star}(t)$.
```

Note that the power consumption of executing PES is much smaller than the jamming power of UAV$_L$, and is comparatively negligible. Moreover, since $(1 -$

$$f'_{\mathbf{P2}}(P_L(t)) = \frac{H_e(t)\cdot 2\beta_0\delta(2f-l)\cdot e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)}{H_s(t)}(1+\frac{P_L(t)}{N_0})}}}{H_s(t)N_0}\cdot(1-\frac{e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)}{H_s(t)}(1+\frac{P_L(t)}{N_0})}}}{2})^{8(2f-l)-1}\cdot(\frac{H_e(t)}{H_s(t)}(1+\frac{P_L(t)}{N_0}))^{-\frac{1}{2}} \tag{14}$$

$$\begin{aligned}(1-\frac{e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)}{H_s(t)}(1+\frac{P_L(t)}{N_0})}}}{2})^{8(2f-l)-1} &\geq (1-\frac{e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)}{H_s(t)}(1+\frac{\frac{H_s(t)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2}-N_0}{N_0})}}}{2})^{8(2f-l)-1}\\ &\geq (1-\frac{e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2 N_0}}}}{2})^{8(2f-l)-1}\\ &\geq (1-\frac{1}{2}e^{\beta_1-\beta_0\sqrt{\frac{H_e(t)K_2^{-1}\ln\frac{K_1}{\epsilon}}{N_0}}})^{8(2f-l)-1}\end{aligned} \tag{15}$$

$\frac{1}{2}e^{\beta_1-\beta_0\delta\sqrt{\frac{H_e(t)}{H_s(t)}\cdot(1+\frac{P_L(t)}{N_0})}})^{8(2f-l)}$ in **P2** monistically increases with an increase of $P_L(t)$, the optimal jamming power, $P_L^{\star}(t)$, can be obtained by comparing the upper bound required by (11) and (13), and the lower bound required by (12). Therefore, **P2** can be solved by using linear programming, and the time complexity of PES is $O(m)$, which depends on the number of slots.

D. Legitimate Tracking Algorithm

Next, we present the legitimate tracking algorithm to properly pursue the suspicious UAVs by using PES. In case the eavesdropped packet is not successfully decoded by using PES, the proposed tracking algorithm also utilizes the AOA and RSS of the suspicious UAV's signal to ensure the eavesdropping coverage of the legitimate UAV for the sake of persistent surveillance.

Due to terrestrial propagation environment and antenna gain, the RSS at UAV$_L$, denoted by $\phi_L(t)$, can be given by [36]

$$\phi_L(t) = \frac{G_{ST}G_L P_{ST}(t)H_{ST}^2(t)h_L^2(t)}{d^4(t)}, \tag{17}$$

where $P_{ST}(t)$ denotes the transmit power of UAV$_{ST}$. G_{ST} is the transmit antenna gain (i.e., UAV$_{ST}$), and G_L is the receive antenna gain (i.e., UAV$_L$). $H_{ST}(t)$ and $h_L(t)$ define the heights of UAV$_{ST}$ and UAV$_L$ at time t, respectively.

Suppose that $\theta(t)$ is the AOA of the eavesdropping signal at UAV$_L$ at time t. The distance between UAV$_{ST}$ and UAV$_L$ at t_1 and t_2 is given by $d(t_1)$ and $d(t_2)$, respectively, which can be obtained by in-flight RSS measurement [37], [38]. Hence, the distance of UAV$_{ST}$'s flight from t_1 to t_2, denoted by Δd_{ST}, can be given by

$$\Delta d_{ST} = \sqrt{d^2(t_1)+d^2(t_2)-2d(t_1)d(t_2)\cos(\theta(t_2)-\theta(t_1))}. \tag{18}$$

Assume that the coordinates of UAV$_L$ at t_1 and t_2 in the three-dimensional space are $(x_L(t_1), y_L(t_1), z_L(t_1))$ and $(x_L(t_2), y_L(t_2), z_L(t_2))$, respectively. Then, we have

$$(x_L(t_2), y_L(t_2), z_L(t_2)) \rightarrow \begin{cases} x_L(t_2) = x_L(t_1) + \Delta d_{ST} \\ y_L(t_2) = y_L(t_1) + \Delta d_{ST} \\ z_L(t_2) = d(t_2)\sin(1-\theta(t_2)) \end{cases} \tag{19}$$

In particular, when the packet is successfully eavesdropped, the coordinates of UAV$_{ST}$, denoted by $(x_{ST}(t), y_{ST}(t), z_{ST}(t))$, can be known to UAV$_L$. In this case, UAV$_L$ is able to derive the next waypoint of its flight, which is $x_L(t_2) = x_L(t_1) + [x_{ST}(t_2) - x_{ST}(t_1)]$; $y_L(t_2) = y_L(t_1) + [y_{ST}(t_2) - y_{ST}(t_1)]$; $z_L(t_2) = z_L(t_1) + [z_{ST}(t_2) - z_{ST}(t_1)]$.

Furthermore, Algorithm 2 presents the legitimate tracking scheme that comprehensively considers the eavesdropping outcome of PES, and the in-flight measurement of AOA and RSS. Specifically, if the suspicious packet is successfully eavesdropped by PES, i.e., $\gamma_e(t) \geq \delta$, UAV$_L$ is able to derive its next waypoint based on (19). Otherwise, UAV$_L$ measures the AOA and RSS of the suspicious transmission in order to obtain $\theta(t)$ and $\phi_L(t)$ at t_1 and t_2. According to (17), the distance between UAV$_{ST}$ and UAV$_L$ at t_1 and t_2 can be given by applying $d(t) = \sqrt[4]{G_{ST}G_L P_{ST}(t)H_{ST}^2(t)h_L^2(t)/\phi_L(t)}$. Therefore, Δd_{ST} can be obtained by (18). Given (19), the next waypoint of UAV$_L$ is updated by substituting Δd_{ST} and $\theta(t_2)$. In terms of computational complexity, the legitimate tracking scheme requires $O(m)$ time in the worst case as the PES could be conducted in Algorithm 2.

In addition, trajectory planning can be applied for UAV$_L$ to track the suspicious UAVs in an energy efficient manner [39]. However, since we focus on optimizing the jamming power for wireless surveillance, the trajectory design for UAV$_L$ is beyond the scope of this paper.

IV. Performance Evaluation

In this section, we firstly develop a new simulation framework, Jamming and Aerial Mobility SIMulator (JAMSIM), which combines the complementary features of a constrained optimization solver, i.e., Matlab, and a network

Algorithm 2 Legitimate Tracking Algorithm

```
Initialize: $\phi_L(t) = 0$, $\theta(t) = 0$, $\Delta d_{ST} = 0$, $f_0, P_{ST}(t), G_{ST}, G_L$.
if $\gamma_e(t) \geq \delta$ then
    UAV$_L$ carries out PES in Algorithm 1 $\rightarrow$ $(x_{ST}(t_1), y_{ST}(t_1), z_{ST}(t_1))$; $(x_{ST}(t_2), y_{ST}(t_2), z_{ST}(t_2))$.
    The next waypoint of UAV$_L$'s flight is updated by $x_L(t_2) \rightarrow x_L(t_1) + [x_{ST}(t_2) - x_{ST}(t_1)]$; $y_L(t_2) \rightarrow y_L(t_1) + [y_{ST}(t_2) - y_{ST}(t_1)]$; $z_L(t_2) \rightarrow z_L(t_1) + [z_{ST}(t_2) - z_{ST}(t_1)]$.
else
    Measure AOA of the eavesdropping signal at $t_1$ and $t_2 \rightarrow \theta(t_1)$ and $\theta(t_2)$.
    Measure RSS of the eavesdropping signal at $t_1$ and $t_2 \rightarrow \phi_L(t_1)$ and $\phi_L(t_2)$.
    $d(t_1)$ and $d(t_2) \leftarrow$ Equation (17).
    The $\Delta d_{ST} \leftarrow$ Equation (18).
    The next waypoint of UAV$_L$'s flight is updated $\leftarrow$ Equation (19).
end if
```

simulator, i.e., NS3. Next, we evaluate the eavesdropping and tracking performance of PES working with the legitimate tracking algorithm based on JAMSIM.

A. Legitimate Surveillance Simulation Framework

Our use of MATLAB is also because the proposed optimization problem **P2** in PES can be readily implemented by using the MATLAB CVX toolbox. In addition, it is convenient to generate fast changing airborne wireless channels in MATLAB to simulate the proposed PES. However, tracking UAV's trajectory based on AOA and RSS has to be evaluated using a discrete event-driven simulator [40], e.g., NS3. To achieve a meaningful simulation, JAMSIM is developed to evaluate proactive eavesdropping and legitimate tracking performance in parallel.

Fig. 3 shows the block diagram of JAMSIM, which contains the simulation carried out by Maltab and NS3. Specifically, Algorithm 1 is implemented in MATLAB. The patrolling speed of UAV$_L$ is set to 10 m/s. The total number of data packets transmitted by UAV$_{ST}$ is 100. UAV$_{ST}$ sends the flight information to UAV$_{SR}$ every time slot. Meanwhile, UAV$_L$ eavesdrops the suspicious packet and decides to jam its transmission. 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. The detailed system-level simulation parameters are shown in Table II.

In terms of NS3 simulator, the flight trajectory of UAV$_{ST}$ is predetermined, which is unknown to UAV$_L$. Consequently, UAV$_L$ tracks suspicious flight based on either the overheard packets using PES or the AOA and RSS using Algorithm 2.

TABLE II: Simulation Parameters

Parameters	Values
K_1	0.2
K_2	3
β_0	2.6
β_1	1
m	100
f	20 bytes
l	10 bytes
ϵ	0.005
N_0	3.98×10^{-12} W
λ	0.3
α_1	3
α_2	2.5
n	0.005377
D	50 m
P_L^{max}	40 dB
ρ_{max}	8

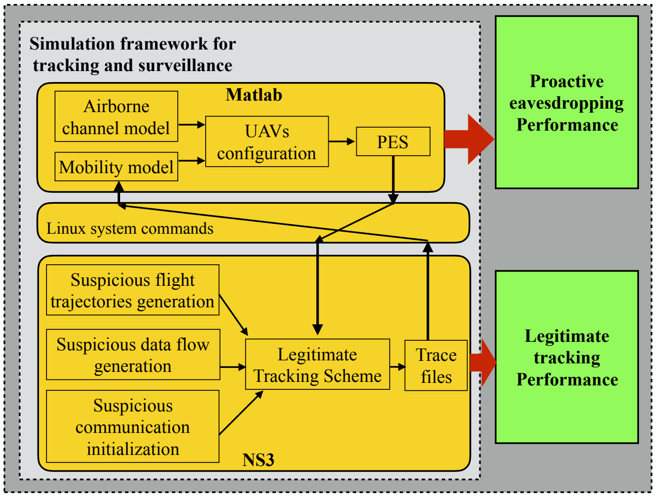

Simulation framework for tracking and surveillance
Matlab
Airborne channel model
Mobility model
UAVs configuration
PES
Linux system commands
Suspicious flight trajectories generation
Suspicious data flow generation
Suspicious communication initialization
Legitimate Tracking Scheme
Trace files
NS3
Proactive eavesdropping Performance
Legitimate tracking Performance

Fig. 3: A legitimate wireless surveillance simulation framework for UAVs.

B. Eavesdropping communications between the suspicious UAVs

Without loss of generality, we compare PES with two legitimate eavesdropping strategies: (i) *Proactive eavesdropping with constant jamming power* (ConstJam), where UAV$_L$ jams the suspicious link when it fails to decode the packet. Moreover, the jamming power is set to 20 dB, which is half the maximum transmit power of our simulated UAV (In fact, the constant jamming power can be set to any value below P_L^{max}); and (ii) *Passive eavesdropping without jamming* (NoJam), where UAV$_L$ passively overhears the packet broadcasted by UAV$_{ST}$, however, it does not send jamming signals to the suspicious link [23], [33].

Fig. 4 shows the number of eavesdropped packets with an increasing SNR of the eavesdropping link, i.e., $\gamma_e(t)$, where the SINR threshold of the suspicious link, i.e., δ in Constraint (6), is configured to be 10 dB or 20 dB. We can see that PES achieves more eavesdropped packets than ConstJam and NoJam. Generally, the performance of PES and ConstJam increases linearly with $\gamma_e(t)$, while the one in NoJam does not vary much. Particularly, when $\gamma_e(t) = 25$ dB, PES eavesdrops about 50% more packets than ConstJam, and 92% more than NoJam. This is because PES adaptively allocates the jamming power of UAV$_L$ based on the quality of the eavesdropping link to purposely change the data rate of UAV$_{ST}$, i.e., $\rho(t)$, for overhearing more packets.

Furthermore, it is also observed that PES with $\delta = 10$ dB eavesdrops more packets than the one with $\delta = 20$ dB when $\gamma_e(t)$ increases from 0 to 10 dB, while converging to 100 packets when $\gamma_e(t)$ increases from 10 to 25 dB. The reason is that an increased SINR threshold of the suspicious link leads to a high $\rho(t)$ as shown in (6), which requires a high jamming power of UAV$_L$ given a low SNR of the eavesdropping link. However, UAV$_L$ is unable to jam the suspicious link if the required power is higher than the maximum transmit power according to (7). Therefore, a smaller number of packets can be eavesdropped in this case. Moreover, with an increasing SNR of the eavesdropping link, UAV$_L$ can successfully decode the suspicious packets even the jamming power is low.

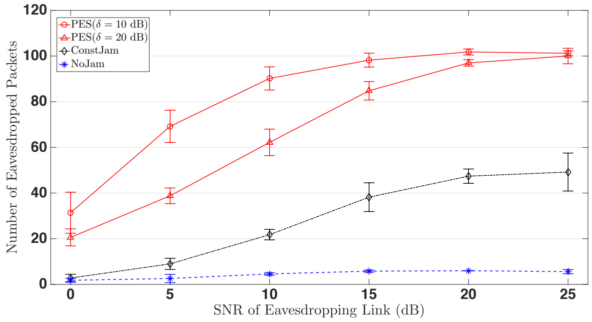


Fig. 4: Number of eavesdropped packets by UAV$_L$, where the error bars show the standard deviation over 50 runs.

Fig. 5 depicts the energy consumption of UAV$_L$ on jamming. It can be observed that the jamming energy consumptions using PES and ConstJam decrease when SNR of the eavesdropping link increases. This confirms that UAV$_L$ jams the suspicious communications with a low power given a high SNR of the eavesdropping link. NoJam does not consume energy on jamming since UAV$_L$ does not send jamming signals in this case. Moreover, PES incurs 82.9% less energy consumption than ConstJam on average when $\delta = 10$ dB and the SNR of the eavesdropping link is 0 dB. This is due to the fact that PES adaptively adjusts the jamming power of UAV$_L$ based on channel conditions of the eavesdropping link. In particular, PES with $\delta = 10$ dB saves more energy than the one with $\delta = 20$ dB given a low SNR of the eavesdropping link. This is because a high SINR threshold of the suspicious link requires a high jamming power, which causes high energy consumption of UAV$_L$.

In Fig. 6, we compare PES and the two existing algorithms in terms of the number of eavesdropped/received packets at UAV$_L$ and UAV$_{SR}$. Specifically, the number of eavesdropped packets at UAV$_L$ increases while the amount of received packets at UAV$_{SR}$ drops when the average jamming power increases from 0 to 16 dB. It confirms the fact that UAV$_L$ using PES can eavesdrop more packets with an increasing jamming power, which causes a large interference to UAV$_{SR}$. Moreover, we can also see that UAV$_L$ and UAV$_{SR}$ receive similar amounts of packets from 16 to 40 dB. The reason is because the number of received packets is bounded by a certain SNR of the eavesdropping link. In this case, UAV$_L$ is unable to eavesdrop more packets even the jamming power increases. Similarly, the number of received packets at UAV$_{SR}$ does not further drop since Constraint (7) does not hold. In addition, PES also outperforms ConstJam and NoJam in terms of the number of eavesdropped packets. Note that the average jamming power with PES is $P_L^\star(t)$ given by Algorithm 1 while the one in ConstJam is the fixed jamming power.

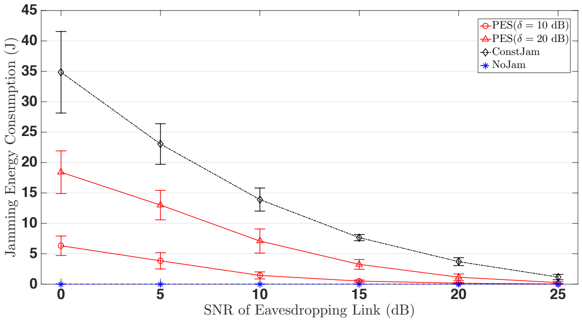


Fig. 5: Energy consumption on jamming, where the error bars show the standard deviation over 50 runs.

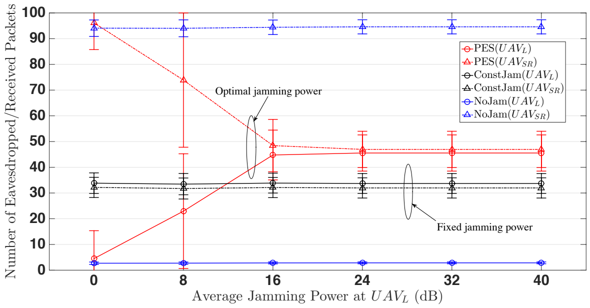


Fig. 6: Number of eavesdropped/received packets for an increasing average jamming power, where the error bars show the standard deviation over 50 runs.

Note that the jamming energy consumption at UAV$_L$ can slightly increase as a function of transmit duration of a packet, due to the reduced transmit rate, given a certain SNR of the eavesdropping link. This is because transmitting a larger data packet takes longer time at the suspicious UAV, which extends the eavesdropping and jamming duration at UAV$_L$ for fully decoding the data. On the other hand, the data packet size can also effect the eavesdropping rate. The reason is that a large packet size leads to a high packet error probability at the suspicious receiver (also at UAV$_L$). As a result, the suspicious transmitter has to lower the data rate for maintaining the target outage probability at the suspicious receiver, which improves the eavesdropping rate at UAV$_L$. Moreover, jamming the suspicious receiver also downgrades the data rate of the suspicious transmitter for more efficiently eavesdropping.

C. Tracking flight trajectory of the suspicious UAVs

We evaluate trajectory tracking error of the proposed legitimate tracking algorithm. In particular, we define the tracking error as a distance between the actual next waypoint of UAV$_L$, which is obtained by the proposed legitimate tracking algorithm, and its expected next waypoint (i.e., ground truth), which is calculated by the coordinates of UAV$_L$ plus the moving distance of UAV$_{ST}$ along its heading.

Fig. 7 shows the flight tracking performance of the proposed legitimate tracking algorithm when δ in PES is set to 10 dB and 20 dB, respectively. Based on Figs. 7(a) and 7(b), it can be observed that the trajectory of UAV$_L$ generally matches the one of the suspicious UAVs, which confirms that UAV$_L$ using the tracking algorithm is able to pursue the suspicious UAVs in the case that the packet eavesdropped by PES is not successfully decoded. In particular, when δ = 10 dB in PES, the suspicious flight can be tracked more accurately than the one with δ = 20 dB. The reason is that a lower δ in PES leads to a larger number of successfully eavesdropped packets on UAV$_{ST}$. To observe the performance difference more clearly, a numerical comparison of tracking error is provided in Fig. 7(c). Specifically, the average tracking error on "(δ in PES = 20 dB)" and "(δ in PES = 10 dB)" is around 1.23 and 0.45 meters, respectively. In particular, the suspicious UAVs fly horizontally at the first 240 seconds, and from 380 to 620 seconds, while UAV$_L$ tracks their flight along the x-axis. During the other time, the suspicious UAVs fly vertically, and UAV$_L$ tracks the flight along the y-axis. The maximum tracking error is 27.5 meters, which appears at the starting point when UAV$_{ST}$ changes their heading from horizontal to vertical. Additionally, NoJam and ConstJam are not plotted due to the low eavesdropping rate or high energy consumption according to Figs. 4 and 5.

In fact, although the flight trajectory of the suspicious UAVs in our simulation is fixed, it should be noted that UAV$_L$ persistently eavesdrops data exchange of the suspicious UAVs to track their flight in real time. As the eavesdropped suspicious packets are maximized on UAV$_L$, the proposed PES and Legitimate Tracking Algorithm are general and can track any flight trajectory.

V. Conclusion and Future Work

This paper presents the legitimate wireless surveillance of UAV communications. The energy-efficient proactive eavesdropping problem is formulated to facilitate the simultaneous eavesdropping and jamming for the legitimate UAV on the flight. PES is proposed to optimize the jamming power of the legitimate UAV to maximize the eavesdropping rate. The legitimate tracking algorithm is also studied to utilize the AOA and RSS of the suspicious transmitter's signal to track their flight in case the eavesdropped packet is not successfully decoded. Moreover, we developed a new simulation framework, JAMSIM, to evaluate the wireless surveillance performance of the PES working with the legitimate tracking algorithm in UAV communications.

In our future work, incomplete self-interference cancellation will be considered for the legitimate UAV. Furthermore, multiple legitimate UAVs will be employed to cooperatively eavesdrop the communication of the suspicious UAVs and track their flight. We will also build a multi-UAV testbed to test the proposed legitimate wireless surveillance of UAV communications in outdoor scenario. In terms of system implementation and deployment, first, a new autopilot software will be developed for the resource-constrained embedded hardware on the UAV. Since many motion control operations on the UAV need to be executed in real time, new software online testing techniques will be implemented to verify the correctness of crucial safety-related autopilot functionality. Second, a flexible software architecture will be developed to aid scalability when controlling multiple UAVs simultaneously without loss in control stability. In this sense, the limits of tracking the suspicious flight trajectory in a real world environment will be determined under the effect of uncertainty and disturbances.

Appendix

According to (4), $\gamma_e(t) \geq \delta$ can be further written as

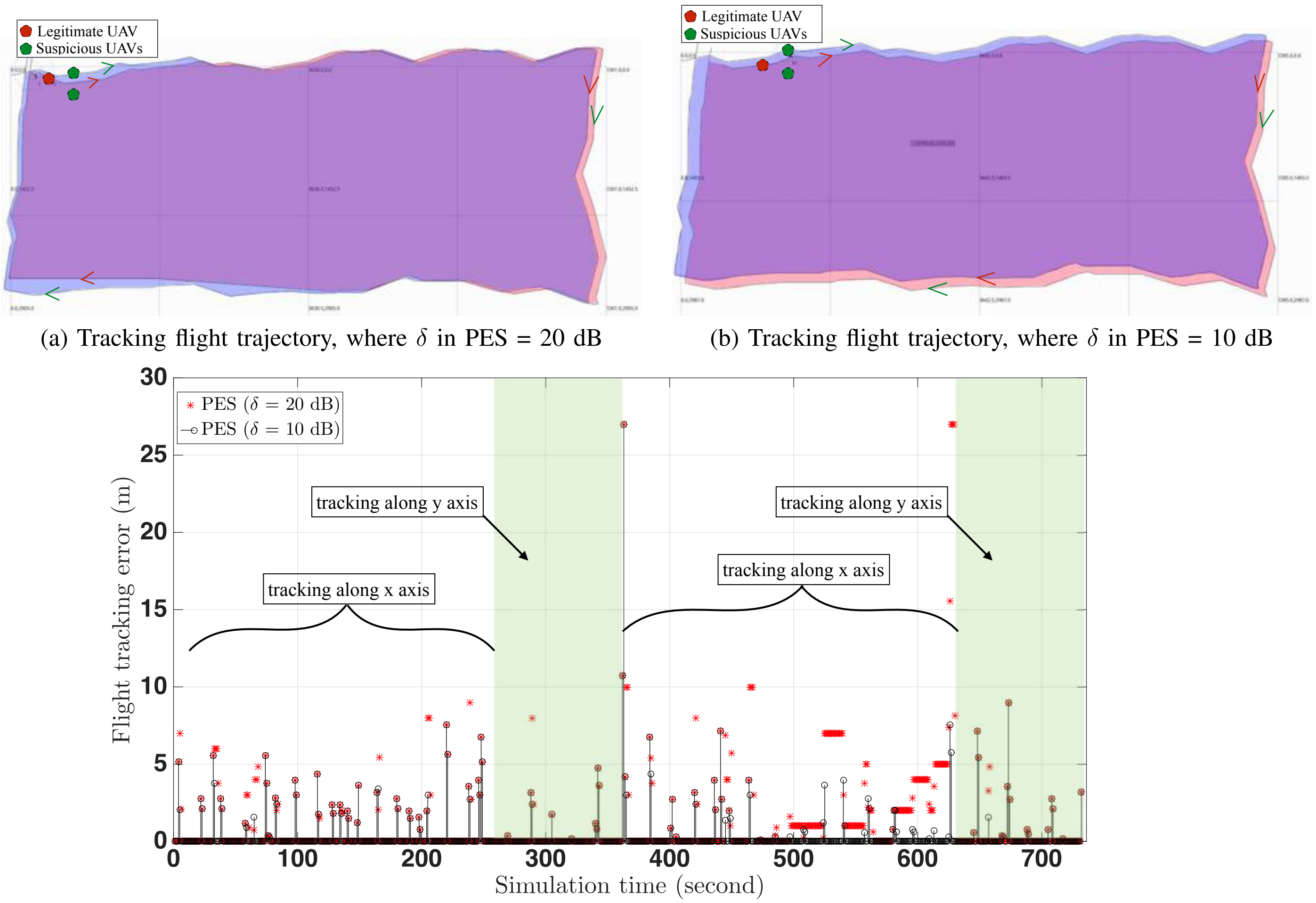
$$\begin{aligned} \sqrt{\frac{H_e(t)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{N_0}} &\geq \delta, \\ \frac{H_e(t)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{N_0} &\geq \delta^2, \\ \frac{K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} &\geq \frac{N_0}{H_e(t)} \end{aligned} \tag{20}$$

where $\rho(t)$ is initialized to 1 to obtain the lower bound of the jamming power. Eq. (12), by substituting (20) to its right-hand side (RHS), can be rewritten as

$$\begin{aligned} P_L(t) &\geq \frac{H_s(t)\cdot N_0}{H_e(t)} - N_0, \\ P_L(t) &\geq \frac{N_0\cdot(H_s(t)-H_e(t))}{H_e(t)}. \end{aligned} \tag{21}$$

Acknowledgement

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (CEC/04234); also by the Operational Competitiveness Programme and Internationalization (COMPETE 2020) through the European Regional Development Fund (ERDF) and by national funds through the FCT, within project POCI-01-0145-FEDER-029074 (ARNET).



(a) Tracking flight trajectory, where δ in PES = 20 dB

(b) Tracking flight trajectory, where δ in PES = 10 dB

(c) Comparison of tracking error

Fig. 7: Flight tracking performance of the proposed legitimate tracking algorithm.

References

[1] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IOT platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[2] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

[3] (2017, April) Homeland security in united states. [Online]. Available: https://en.wikipedia.org/wiki/Homeland_security

[4] C. C. Haddal and J. Gertler, "Homeland security: Unmanned aerial vehicles and border surveillance." DTIC Document, 2010.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[6] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] J. Xu, K. Li, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming over HARQ-based communications," in *IEEE Global Communications Conference (GLOBECOM)*, 2017.

[9] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, 2011.

[11] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference (VTC)*, vol. 62, no. 3. IEEE; 1999, 2005, p. 1906.

[12] S. Lakshmanan, C.-L. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2008, pp. 19–27.

[13] X. Chen, D. W. K. Ng, W. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, 2016.

[14] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[15] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5651–5663, 2016.

[16] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[17] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[18] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs.

artificial fast fading," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 94–106, 2015.

[19] H. M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4893–4898, 2015.

[20] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[21] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 152–159, 2017.

[22] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 80–83, 2016.

[23] 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 *International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 402–408.

[24] A. Chamseddine, O. Akhrif, G. Charland-Arcand, F. Gagnon, and D. Couillard, "Communication relay for multiground units with unmanned aerial vehicle using only signal strength and angle of arrival," *IEEE Transactions on Control Systems Technology*, vol. 25, no. 1, pp. 286–293, 2017.

[25] F. Koohifar, A. Kumbhar, and I. Guvenc, "Receding horizon multi-UAV cooperative tracking of moving RF source," *IEEE Communications Letters*, 2016.

[26] N. Okello, F. Fletcher, D. Musicki, and B. Ristic, "Comparison of recursive algorithms for emitter localisation using TDOA measurements from a pair of UAVs," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 47, no. 3, pp. 1723–1732, 2011.

[27] M. Izadi, A. K. Sanyal, R. Beard, and H. Bai, "GPS-denied relative motion estimation for fixed-wing UAV using the variational pose estimator," in *Annual Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 2152–2157.

[28] L. Mejias, S. McNamara, J. Lai, and J. Ford, "Vision-based detection and tracking of aerial targets for UAV collision avoidance," in *International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2010, pp. 87–92.

[29] Z. Li, N. Hovakimyan, V. Dobrokhodov, and I. Kaminer, "Vision-based target tracking and motion estimation using a small UAV," in *International Conference on Decision and Control (CDC)*. IEEE, 2010, pp. 2505–2510.

[30] 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*, vol. 15, no. 6, pp. 1377–1386, 2016.

[31] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "EPLA: Energy-balancing packets scheduling for airborne relaying networks," in *IEEE International Conference on Communications (ICC)*, 2015, pp. 6246–6251.

[32] B. Li and A. Eryilmaz, "Distributed channel probing for efficient transmission scheduling in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 6, pp. 1176–1188, 2015.

[33] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2790–2806, 2017.

[34] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, 2014.

[35] D. Son, B. Krishnamachari, and J. Heidemann, "Experimental study of concurrent transmission in wireless sensor networks," in *International Conference on Embedded Networked Sensor Systems (SenSys)*. ACM, 2006, pp. 237–250.

[36] N. Ahmed, S. S. Kanhere, and S. Jha, "Utilizing link characterization for improving the performance of aerial wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 8, pp. 1639–1649, 2013.

[37] A. Masiero, F. Fissore, A. Guarnieri, F. Pirotti, and A. Vettore, "UAV positioning and collision avoidance based on RSS measurements," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 40, no. 1, p. 219, 2015.

[38] C. Luo, S. I. McClean, G. Parr, L. Teacy, and R. De Nardi, "UAV position estimation and collision avoidance using the extended kalman filter," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 6, pp. 2749–2762, 2013.

[39] Y. Zeng and R. Zhang, "Energy-efficient uav communication with trajectory optimization," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3747–3760, 2017.

[40] Z. Pan, Q. Xu, C. Chen, and X. Guan, "NS3-MATLAB co-simulator for cyber-physical systems in smart grid," in *Chinese Control Conference (CCC)*. IEEE, 2016, pp. 9831–9836.

Kai Li (S'09–M'14) received the B.E. degree from Shandong University, China, in 2009, the M.S. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2010, and the Ph.D. degree in Computer Science from The University of New South Wales, Sydney, Australia, in 2014. Currently he is a research scientist and project leader at Real-Time and Embedded Computing Systems Research Centre (CISTER), Portugal. Prior to this, Dr. Li was a postdoctoral research fellow at The SUTD-MIT International Design Centre, The Singapore University of Technology and Design, Singapore (2014-2016). He was a visiting research assistant at ICT Centre, CSIRO, Australia (2012-2013). From 2010 to 2011, he was a research assistant at Mobile Technologies Centre with The Chinese University of Hong Kong. His research interests include vehicular communications and security, resource allocation optimization, Cyber-Physical Systems, Internet of Things (IoT), human sensing systems, sensor networks and UAV networks.

Dr. Li serves as the Associate Editor for IEEE Access Journal, the Demo Co-chair for ACM/IEEE IPSN 2018, the TPC member of IEEE Globecom'18, MASS'18, VTC-Spring'18, Globecom'17, VTC'17, and VTC'16.

Razvan Christian Voicu received two B.S. degrees in electrical engineering and computer engineering respectively from Kennesaw State University, Atlanta, GA, USA, in 2013. Currently, he is a graduate student at the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. In 2004, he founded a successful IT company by the name of World Technology, LLC. at Lawrenceville, Georgia. His current research interests include the heterogeneous networks, new infrastructure-less network paradigms, machine learning, Internet of Things (IoT), and biomedical devices. Razvan's works have been published in reputable international conferences.

Salil S. Kanhere (M'01–SM'11) received the MS and PhD degrees, both in electrical engineering from the Drexel University, Philadelphia, in 2001 and 2003, respectively.

He is Professor with the School of Computer Science and Engineering, University of New South Wales, Sydney, NSW, Australia. He is currently a contributing research staff with the National ICT Australia, Sydney, NSW, Australia, and a Faculty Associate with the Institute for Infocomm Research, Singapore. His current research interests include pervasive computing, crowdsourcing, embedded sensor networks, mobile networking, privacy, and security. He has authored/coauthored more than 140 peer-reviewed articles and delivered more than 15 tutorials and keynote talks on these research topics.

Prof. Kanhere regularly serves on the organizing committee of a number of IEEE and ACM international conferences (e.g., IEEE PerCom, ACM MobiSys, ACM SenSys, ACM CoNext, IEEE WoWMoM, IEEE LCN, ACM MSWiM, IEEE DCOSS, IEEE SenseApp, ICDCN, and ISSNIP). He currently serves as the area editor for Pervasive and Mobile Computing, Computer Communications, International Journal of Ad Hoc, and Ubiquitous Computing and Mobile Information Systems. He received the Humboldt Research Fellowship in 2014.

Wei Ni (M'09-SM'15) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. Currently he is a Team Leader at CSIRO, Sydney, Australia, and an adjunct professor at the University of Technology Sydney (UTS). He also holds adjunct positions at the University of New South Wales (UNSW) and Macquarie University (MQ). Prior to this, he was a postdoctoral research fellow at Shanghai Jiaotong University from 2005-2008; Deputy Project Manager at the Bell Labs R&I Center, Alcatel/Alcatel-Lucent from 2005-2008; and Senior Researcher at Devices R&D, Nokia from 2008-2009. His research interests include stochastic optimization, game theory, graph theory, as well as their applications to network and security.

Dr Ni has been serving as Vice Chair of IEEE NSW VTS Chapter and Editor of IEEE Transactions on Wireless Communications since 2018, secretary of IEEE NSW VTS Chapter from 2015 - 2018, Track Chair for VTC-Spring 2017, Track Co-chair for IEEE VTC-Spring 2016, and Publication Chair for BodyNet 2015. He also served as Student Travel Grant Chair for WPMC 2014, a Program Committee Member of CHINACOM 2014, a TPC member of IEEE ICC'14, ICCC'15, EICE'14, and WCNC'10.

Eduardo Tovar was born in 1967 and has received the Licentiate, MSc and PhD degrees in electrical and computer engineering from the University of Porto, Porto, Portugal, in 1990, 1995 and 1999, respectively. Currently he is Professor in the Computer Engineering Department at the School of Engineering (ISEP) of Polytechnic Institute of Porto (IPP), where he is also engaged in research on real-time distributed systems, wireless sensor networks, multiprocessor systems, cyber-physical systems and industrial communication systems. He heads the CISTER Research Unit, an internationally renowned research centre focusing on RTD in real-time and embedded computing systems. He is deeply engaged in research on real-time distributed systems, multiprocessor systems, cyber-physical systems and industrial communication systems. He is currently the Vice-chair of ACM SIGBED (ACM Special Interest Group on Embedded Computing Systems) and was for 5 years, until December 2015, member of the Executive Committee of the IEEE Technical Committee on Real-Time Systems (TC-RTS). Since 1991 he authored or co-authored more than 150 scientific and technical papers in the area of real-time and embedded computing systems, with emphasis on multiprocessor systems and distributed embedded systems. Eduardo Tovar has been consistently participating in top-rated scientific events as member of the Program Committee, as Program Chair or as General Chair. Notably he has been program chair/co-chair for ECRTS 2005, IEEE RTCSA 2010, IEEE RTAS 2013 or IEEE RTCSA 2016, all in the area of real-time computing systems. He has also been program chair/co-chair of other key scientific events in the area of architectures for computing systems and cyber-physical systems as is the case of ARCS 2014 or the ACM/IEEE ICCPS 2016 or in the area of industrial communications (IEEE WFCS 2014).