CISTER

Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Eavesdropping and Jamming Selection Policy for Suspicious UAVs Based on Low Power Consumption over Fading Channels

This article belongs to the Special Issue Low Energy Wireless Sensor Networks: Protocols, Architectures and Solutions.

Xiaoming Wang

Demin Li

Chang Guo

Xiaolu Zhang

Salil S. Kanhere

Kai Li*

Eduardo Tovar*

*CISTER Research Centre

CISTER-TR-190302

2019/03/05

Eavesdropping and Jamming Selection Policy for Suspicious UAVs Based on Low Power Consumption over Fading Channels

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

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: guochang@mail.dhu.edu.cn, kaili@isep.ipp.pt, emt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

Traditional wireless security focuses on preventing unmanned aerial vehicle (UAV) communications from suspicious eavesdropping and/or jamming attacks. However, there is a growing need for governments to keep malicious UAV communications under legitimate surveillance. This paper first investigates a new surveillance paradigm for monitoring suspicious UAV communications via jamming suspicious UAVs. Due to the power consumption limitation, the choice of eavesdropping and jamming will reflect the performance of the UAVs communication. Therefore, the paper analyses the UAV 19s eavesdropping and jamming models in different cases, and then proposes the model to optimize the data package in the constraints of lower power consumption, which can be solved by the proposed selection policy. The simulation results validate our proposed selection policy in terms of power consumption and eavesdropped packets. In different fading models, power consumption increases with time, regardless of distances, and our proposed policy performs better in Weibull fading channels in terms of eavesdropped packets.

sensors

MDPI

Article

Eavesdropping and Jamming Selection Policy for Suspicious UAVs Based on Low Power Consumption over Fading Channels

Xiaoming Wang [1,2,3], Demin Li [1,2,*], Chang Guo [1,2], Xiaolu Zhang [1,2], Salil S. Kanhere [4], Kai Li [5] and Eduardo Tovar [5]

1 College of Information Science and Technology, Donghua University, Shanghai 201620, China; xmwang@shea.gov.cn (X.W.); guochang@mail.dhu.edu.cn (C.G.); xiaoludhu@mail.dhu.edu.cn (X.Z.)
2 Engineering Research Center of Digitized Textile and Apparel Technology, Ministry of Education, Shanghai 201620, China
3 Shanghai Earthquake Administration, Shanghai 200062, China
4 School of Computer Science and Engineering, UNSW Sydney, Sydney, NSW 2052, Australia; salil.kanhere@unsw.edu.au
5 CISTER Research Unit, 4200-135 Porto, Portugal; kaili@isep.ipp.pt (K.L.); emt@isep.ipp.pt (E.T.)
* Correspondence: deminli@dhu.edu.cn

Received: 21 January 2019; Accepted: 28 February 2019; Published: 5 March 2019

Abstract: Traditional wireless security focuses on preventing unmanned aerial vehicle (UAV) communications from suspicious eavesdropping and/or jamming attacks. However, there is a growing need for governments to keep malicious UAV communications under legitimate surveillance. This paper first investigates a new surveillance paradigm for monitoring suspicious UAV communications via jamming suspicious UAVs. Due to the power consumption limitation, the choice of eavesdropping and jamming will reflect the performance of the UAVs communication. Therefore, the paper analyses the UAV's eavesdropping and jamming models in different cases, and then proposes the model to optimize the data package in the constraints of lower power consumption, which can be solved by the proposed selection policy. The simulation results validate our proposed selection policy in terms of power consumption and eavesdropped packets. In different fading models, power consumption increases with time, regardless of distances, and our proposed policy performs better in Weibull fading channels in terms of eavesdropped packets.

Keywords: selection policy; eavesdropping; jamming; fading channel; UAV

1. Introduction

Recently, unmanned aerial vehicle (UAV) techniques have been widely applied to wireless communication systems such emergency rescue, homeland security, etc., owing to the flexible and quick deployment. Researchers from academia, industry, government agencies, etc., have paid lots of attractions to UAV communications. Game theory has been adopted to deal with a smart attacker from UAV [1]. Traditional UAV network security studies generally assume UAV communications are authorized and rightful, so researchers put great efforts to preventing existing UAV communications form malicious attacks such as jamming and eavesdropping [2–5]. However, the paradigm has changed with the development of UAV technologies. Terrorists or criminals may use UAVs to establish wireless communications for committing crimes and terrorism [6,7]. For instance, the eavesdroppers in the UAV communication networks can overhear the secure message, thus improving the capacity of communication network by reporting faked channel state information on the basis of the continuously

changing channel environments [8,9]. More seriously, criminals can use UAV communication networks to commit bombing activities, and business spies may use them to filch trade secrets.

In traditional UAV surveillance works, eavesdropping and jamming UAVs are usually static during their tasks, while in this paper, we consider the UAV's dynamic motion, which can reflect the performance of jamming selection on power consumption. The policy can provide the optimal results of eavesdropping and jamming selection based on power consumption in different locations. As shown in Figure 1, authorized UAVs share information through an existing UAV network, which may change topology occasionally because of UAV's unpredictable trajectory. The new infrastructure-free mobile communication can be easily used by malicious UAVs (marked as red ones), e.g., criminals, terrorists, and business spies, to commit crimes, jeopardize public safety, invade the secret database of other companies, etc., thus imposing new challenges on the public security [1]. Therefore, there is a growing need for government agencies to legitimately monitor and eavesdrop wireless communications of suspicious UAVs [8].

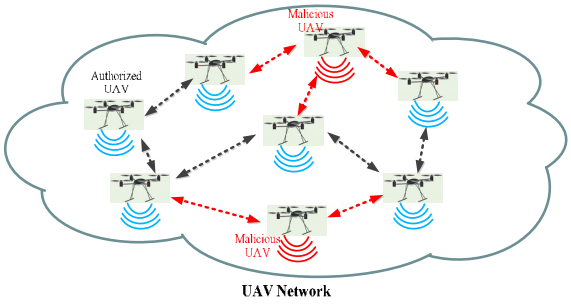
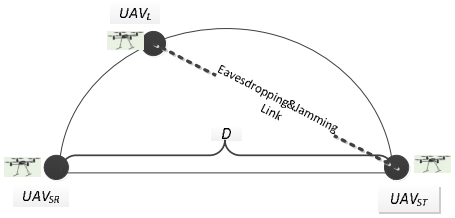
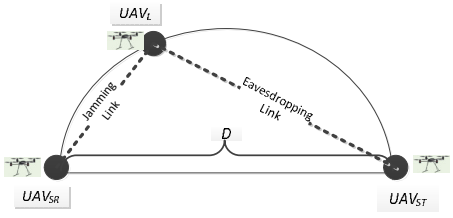


Figure 1. A malicious eavesdropping scenario where malicious unmanned aerial vehicles (UAV) attack authorized UAVs through the UAV network.

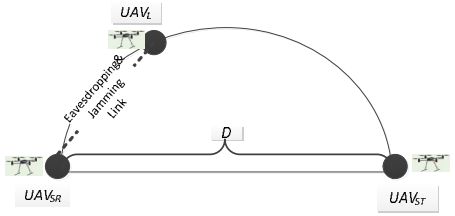
In particular, we consider four surveillance scenarios as shown in Figure 2, where a legitimate UAV, i.e., UAV_L, aims to monitor a suspicious communication link from a suspicious UAV transmitter (UAV_{ST}) to a UAV receiver (UAV_{SR}) over fading channels. It is seldom to have significant multipath links in the sky. However, flying UAVs are strictly restricted according to policies. It is allowed for flying UAVs freely under some low altitudes, which are even lower than tall buildings, and what is more, extreme weather conditions may also influence the state of communication links for UAVs, so there are still scenarios for UAVs communication in multipath links. In reality, UAV transmitter and UAV receiver are relative, since communication links are bi-directional, using a pair of transmitter and receiver for simultaneous transmission in both directions.



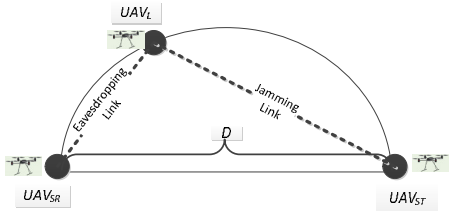
(**a**) UAV_L eavesdrops UAV_{ST} via jamming UAV_{ST}



(**b**) UAV_L eavesdrops UAV_{ST} via jamming UAV_{SR}



(**c**) UAV_L eavesdrops UAV_{SR} via jamming UAV_{SR}



(**d**) UAV_L eavesdrops UAV_{SR} via jamming UAV_{ST}

Figure 2. Eavesdropping via jamming.

In this scenario, we assume that the suspicious pair of UAVs (known as UAV_{ST} and UAV_{SR}) has been detected by authorized agencies at the beginning, and they are eavesdropped by a legitimate UAV monitor (UAV_L). Suspicious users' detection and association can be referred to in Reference [9].

We use the eavesdropping model proposed by Jie Xu, et al. [10] which proactively generate jamming signals to interfere with the suspicious communication link through a full-duplex mode, so as to decrease the achievable data rate at the suspicious transmitter or receiver for overhearing more efficiently.

In order to initialize investigation, we assume that no advanced anti-eavesdropping schemes for security are employed by suspicious UAVs. Based on such assumptions, UAV_L can overhear information successfully from the suspicious UAVs only when the received signal-to-noise ratio (SNR) (and accordingly the achievable data rate) at UAV_L is no smaller than that at UAV_{SR}, since in this case UAV_L can decode the data that can be decoded at UAV_{SR} [10]. Let R_L and R_S denote the achievable data rate of the legitimate eavesdropping link form UAV_{ST} to UAV_L and the communication rate of the suspicious link form UAV_{ST} to UAV_{SR}, respectively. Then, UAV_L can decode transmitted signal correctly (with arbitrarily small error) if, and only if, R_L is no smaller than R_S. We define the eavesdropping rate R_E as the suspicious data rate that UAV_L can successfully decode, which is given as $R_E = R_S$ if $R_L \geq R_S$, and $R_E = 0$ if $R_L < R_S$. UAV_{ST} and UAV_{SR} are assumed to fly following a collision-free formation, where they keep a prescribed relative distance and angle. There are four cases for UAV_L to successfully eavesdrop suspicious communication link. Case 1, as shown in Figure 2a, UAV_L eavesdrops suspicious UAV_{ST} by sending jamming signals to UAV_{SR}. In this case, UAV_{ST} increases transmission power in order to sustain R_S at its original level, thus increasing R_L inevitably in the eavesdropping link. When R_L is no smaller than R_S, UAV_L is able to decode the whole information that can be decoded at UAV_{SR} to fulfill eavesdropping missions. Case 2, as shown in Figure 2b, UAV_L eavesdrops suspicious UAV_{ST} by sending jamming signals to UAV_{SR}. Take the time-division-duplex (TDD) multi-antenna transmission scheme as an example, where UAV_{ST} designs its transmit beamforming vectors based on the reverse-link channel estimation from UAV_{SR}. In that case, UAV_{ST} can spoof the reverse-link transmit signals received by UAV_{ST}, such that UAV_{ST} estimates a fake channel, and changes its beamforming direction towards UAV_L and away from UAV_{SR} [11]. This approach increases R_L and decreases R_S, and accordingly improves R_E. Case 3, as shown in Figure 2c, UAV_L eavesdrops suspicious UAV_{SR} by sending jamming signals to UAV_{SR}. In that case, UAV_{SR} increases transmission power in order to sustain R_S at its original level, thus increasing R_L inevitably in the eavesdropping link. When R_L is no smaller than R_S, UAV_L is able to decode the whole information that can be decoded at UAV_{ST} to fulfill eavesdropping missions. Case 4, as shown in Figure 2d, UAV_L eavesdrops suspicious UAV_{SR} by sending jamming signals to UAV_{ST}. Take the time-division-duplex (TDD) multi-antenna transmission scheme as an example, where UAV_{SR} designs it's transmit beamforming vectors based on the reverse-link channel estimation from UAV_{ST}. In that case, UAV_{SR} can spoof the reverse-link transmit signals received by UAV_{SR}, such that UAV_{SR} estimates a suspicious channel, and changes its beamforming direction towards UAV_L and away from UAV_{ST} [12]. This approach increases R_L and decreases R_S, and accordingly improves R_E.

We have previously discussed the first approach to eavesdrop suspicious communication link by jamming UAV_{SR}, as shown in Figure 2a [13], so this paper mainly focuses on the other three eavesdropping and jamming cases, as shown in Figure 2b–d. In practice, UAV's trajectory period depends on the battery charge. Low power consumption can make sure the UAV fly in a relative long period. In this paper, we aim to (1) minimize the power consumption at UAV_L, and to (2) maximize the eavesdropping rate at UAV_L. Specifically, when the constraint of suspicious data rate is given, we formulate an optimization problem to find the most efficient jamming power allocation at UAV_L to maximize the eavesdropping rate, which is polynomially solvable. Moreover, we propose a selection policy 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, the proposed policy allocates the jamming power over the fading channel according to the limited jamming power

constraint, as well as the position of UAV_L. The impacts of fading states on the performance of our policy are analyzed by applying the proposed policy to four common fading models, i.e., Rayleigh, Ricean, Weibull, and Nakagami.

In our paper, we considered the topology between the legitimate UAV and two suspicious UAVs is a semi-circle with a diameter D. We mainly consider an optimal policy strategy for the legitimate UAV to obtain a good performance on monitoring. From the analysis, it is clear that the distance between UAVs is the key to the problem. Thus, considering UAVs' distance is much more meaningful compared to the trajectory design in our model. In fact, the change of trajectories causes the change of distances between legitimate UAV and suspicious UAV, so we can apply our results in various trajectories. The main contributions of this work can be summarized as follows:

(1) Traditional works focused on achieving secure UAV-ground (U2G) communications in the presence of terrestrial eavesdroppers/jammers, while in our paper, we considered UAV-UAV (U2U) communications in the air, so we formulated suspicious UAVs' distance model, which considered the dynamic mobility of suspicious UAVs in sequence time slots;
(2) Traditional works usually consider one case for eavesdropping and jamming, while in our paper, we proposed four cases of eavesdropping and jamming over fading channels, and then formulated an optimization problem to find the most efficient jamming power allocation at UAV_L to maximize the eavesdropping rate;
(3) Traditional works focus on improving power consumptions or data receive rate respectively, while in our paper, we proposed a selection policy to facilitate the simultaneous eavesdropping and jamming for UAV_L on the flight, which allocated the jamming power over the fading channel according to the limited jamming power constraint as well as the position of UAV_L.

The rest of the paper is organized as follows: Section 2 introduces related works on security techniques in UAV networks. In Section 3, we design the system model on legitimate eavesdropping and jamming. Section 4 proposes the problem formulation and selection policy, as well as the complexity and feasible solution analysis. Simulation results are shown in Section 5, followed by a conclusion in Section 6.

2. Related Works

In the literature, there have been a handful of methods for preventing existing wireless networks (e.g., cellular networks) from malicious attacking since wireless networks are prone to malicious attacks such as eavesdropping attack [12], DoS attack [14], spoofing attack [15], MITM attack [16], message falsification/injection attack [17], etc. For instance, authorized devices in a wireless network can, by interference, be illegal devices in the same network in terms of information stealing or virus attacking. Moreover, malicious device may overhear wireless communications sessions, as long as it is within the transmit coverage area of the transmitting device. Generally speaking, the requirements of confidentiality, availability, integrity, and authenticity should be satisfied by secure wireless communications [18]. Cryptographic techniques for preventing eavesdroppers from intercepting data transmissions between legitimate users are typically employed by existing communication systems, thus maintaining confidential transmission in wireless networks [19,20]. For example, passive eavesdropping is applicable to intercept infrastructure-free wireless communications (e.g., UAV networks) [21].

Recently, physical-layer security has emerged as a promising solution to secure UAV communications against eavesdropping attacks [22–25]. The authors in Reference [22] proposed an algorithm to adaptively control the UAV's location over time to optimize UAV's average secrecy rate basing on a secure single-UAV communication system. In Reference [23], authors regarded UAVs as friendly jammers to protect the ground wireless communication, while authors in References [24,25] employed UAVs as mobile relays to facilitate secure or reliable wireless communications. Authors in [26] introduced a power allocation strategy which was regarded as a zero-sum game between the transmitter and the

eavesdropper. In Reference [27], authors considered a power control strategy based on Q-learning for the transmitter to enhance the secure capacity via preventing from smart attacks in the dynamic game, however, authors in Reference [27] did not consider the practical channel estimation error, which should not be ignored in the practical communication scenarios, since it will give a significant impact on the network performance. The authors in Reference [28] proposed the optimal power allocation strategies by studying the impact of channel estimation error on the capacity of specific channels. Authors in Reference [29] proposed a theoretical communication scheme, which use multiple antennas to generate artificial noise to degrade the channel quality of eavesdroppers. In Reference [30], authors proposed a low-density parity-check protocol, which used a four-step procedure to ensure wireless information-theoretic security, to achieve communication rates close to the fundamental security limits in wireless communications. However, none of these works [22–30] consider the use of proactive eavesdropping to enhance network security.

In order to enhance the quality of secure wireless transmissions, jamming the eavesdropper is an effective approach [31–33]. Authors in Reference [31] presented a cooperative jamming scheme, which help a legitimate user improve its data rate via sending a jamming signal to the eavesdropper. The authors in Reference [32] presented a hybrid artificial fast fading scheme, which achieved better performance for eavesdropper. In Reference [33], authors proposed a full-duplex scheme, which transmitted the jamming signal to degrade the channel of eavesdropper. Under this scheme, the system was no longer interference-limited, compared with the half-duplex case. Reference [34] formulated a stochastic game, and provided insights for secret and reliable communication against both jamming and eavesdropping. However, authors in References [31–34] considered eavesdropping as an illegitimate attack and targeted on decreasing the eavesdropping performance. Authors in References [35–37] focused on achieving secure UAV-ground (U2G) communications in the presence of terrestrial eavesdroppers/jammers, they did not consider UAV-UAV (U2U) communications in the air. Reference [12] discussed how an active eavesdropper can attack the training phase in wireless communication to improve its eavesdropping performance, however, Reference [12] did not consider the mobility of UAVs in their communications, and Reference [12] just considered the case of eavesdropping and jamming. In general, there is a lack of researches on power consumption controlling, legitimately eavesdropping and selection policy towards suspicious UAV communications.

3. System Model

3.1. Assumptions

We consider that the distance between suspicious UAV transmitter (UAV_{ST}) and receiver (UAV_{SR}) is denoted as D meters. The distance can be calculated in the subsequent time slot, considering the dynamic mobility of the two UAVs. Without loss of generality, we consider 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, even though the distance between UAV_L is dynamic with time-depend.

The suspicious communication between UAV_{ST} and UAV_{SR} consists of m number of time slots, and each time 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 generalized and thus agnostic of the MAC protocol in use. In our proposed model, we assume that the suspicious UAVs consider the UAV_L's eavesdropping signal as interference during the wireless communication.

In fact, our policy proposed 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 of trajectories of UAVs. Moreover, Table 1 lists the fundamental variables that have been used in our system model.

Table 1. Notations and variables.

Variables	Descriptions
$P_L(x)$	Legitimate monitor consuming power ($P_E(x) + P_J(x)$) at time slot x
$P_E(x)$	Legitimate monitor eavesdropping power at time slot x
$P_J(x)$	Legitimate monitor jamming power at time slot x
$\gamma_e(x)$	SNR of eavesdropping link at time slot x
$\gamma_s(x)$	SNR of suspicious link at time slot x
K_1, K_2	Two constants relating to the channel
N_0	Power of white Gaussian noise
$d_1(x)$	Distance between UAV_L and UAV_{ST} at time slot x
$d_2(x)$	Distance between UAV_L and UAV_{SR} at time slot x
P_L^{max}	Maximum consuming power of UAV_L
P_L^{total}	Total jamming power of UAV_L
n	Gaussian random number
α_1, α_2	Path-loss exponent of wireless channel
λ	Coefficient considered to adjust the weights of the autocorrelated component and independent component
δ	SINR/SNR threshold
$\rho(x)$	Adaptive modulation and coding (AMC) rate at time slot x
ϵ	The required instantaneous bit error rate

3.2. Suspicious UAVs' Distance Model

The distance between UAV_L and UAV_{ST}, and the distance between UAV_L and UAV_{SR} relate to the performance of eavesdropping and jamming. Therefore, we will discuss the suspicious UAVs' distance model in this part, which is based on the position of UAV_L and the suspicious UAVs' dynamic mobility.

As shown in Figure 3, the distance between UAV_L and UAV_{ST} at time slot x, which was denoted as $d_1(x)$, can be described as:

$$d_1(x) = \sqrt{\left(\frac{D}{2} - \frac{D}{2}\cos\theta(x)\right)^2 + \left(\frac{D}{2}\sin\theta(x)\right)^2} = \frac{\sqrt{2}D}{2}\sqrt{1-\cos\theta(x)} \quad (1)$$

Additionally, 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}.

The angle variation $\theta(x)$ depends on the real-time position of UAV_L. However, as shown in Figure 4, the results of $d_1(x)$ is the same as Equation (1), because the expression of variations a and b can be transformed under the condition of $\theta < \pi/2$, which means that

$$a = \frac{D}{2}\sin(\pi - \theta(x)) = \frac{D}{2}\sin\theta(x), b = \frac{D}{2} + \frac{D}{2}\cos(\pi - \theta(x)) = \frac{D}{2} - \frac{D}{2}cos\theta(x) \quad (2)$$

The model is two-dimensional, and considers the dynamic mobility of suspicious UAVs in sequence time slots, as shown in Figure 5. The distance variation D is improved as a dynamic variation that relates to the time slot,

$$D(x) = D(x-1) + \varphi\Delta v \quad (3)$$

Here, φ is the duration of each time slot, and Δv is a vertex that presents the speeds' difference value of UAV_{ST} and UAV_{SR}. We do not include three-dimensional degrees of freedom for improving the security, but that will be our future works.

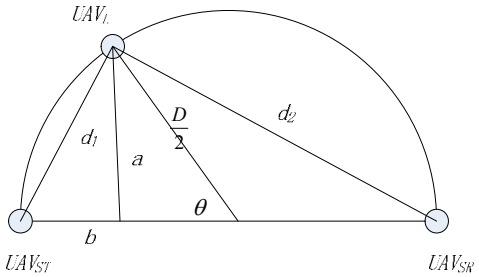


Figure 3. The illustration of distance when $\theta < \pi/2$.

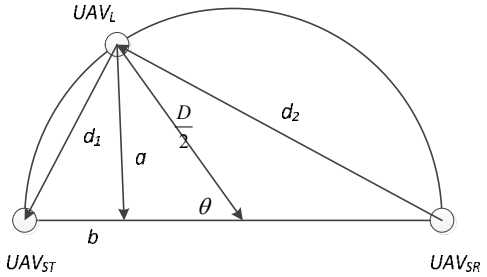


Figure 4. The illustration of distance when $\theta > \pi/2$.

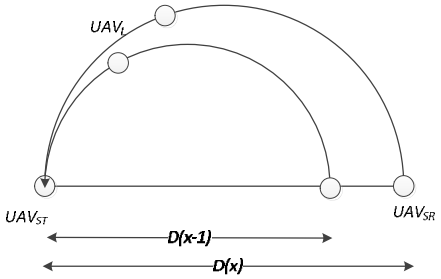


Figure 5. The illustration of dynamic mobility of suspicious UAVs.

3.3. Eavesdropping and Jamming Model

Based on the power constraint of UAVs, the suspicious UAVs' selection for eavesdropping and jamming is an important parameter to be considered in the following algorithm. The optimal selection depends on the UAV_L's position at time slot x. There are four cases as follows:

Case 1: UAV_L eavesdrops and jams UAV_{ST}.

As shown in Figure 2a, UAV_L only chooses UAV_{ST} for eavesdropping and jamming. According to References [19,38], at time slot xth, the channel gain from UAV_{ST} to UAV_{SR}, which was denoted as $H_s(x)$, is expressed as:

$$H_s(x) = \frac{\lambda H_s(x-1) + n\sqrt{1-\lambda^2}}{D^{\alpha_2}} \tag{4}$$

where α_2 denotes the path-loss exponent in the suspicious link and λ presents the coefficient which adjusts two components: the weights of the auto-correlated and the independent. 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) at UAV_{ST} at time slot x as $\gamma_s(x)$, which is given by

$$\gamma_s(x) = \sqrt{\frac{H_s(x) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon} \cdot \left(2^{\rho(x)} - 1\right)}{N_0 + P_L(x)}} \tag{5}$$

where $\rho(x)$ denotes the adaptive modulation and coding (AMC) rate of the UAV_{ST} at time slot x, and the highest mode is denoted by ρ_M. K_1 and K_2 are two constants related to the channel. N_0 denotes the power of white Gaussian noise. ϵ is the required instantaneous bit error rate. As elaborated in the assumption part, the suspicious UAVs consider the UAV_L's eavesdropping signal as interference during the wireless communication. Hence, the eavesdropping power at time slot x is a part of interference in suspicious communication. Another part of interference is the jamming power from UAV_L. Therefore, the interference power at time slot x is denoted as $P_E(x) + P_J(x)$. Likewise, at time slot x, the channel gain in the eavesdropping and jamming links, i.e., from UAV_{ST} to UAV_L, is given by

$$H_e(x) = H_j(x) = \frac{\lambda H_e(x-1) + n\sqrt{1-\lambda^2}}{d_1^{\alpha_1}(x)} \tag{6}$$

where n is a Gaussian random number generated by AWGN. α_1 denotes the path-loss exponent. $d_1(x)$ is the distance between UAV_L and UAV_{ST} at time slot x, which can be acquired by Equation (1).

As the relative position of UAV_L to UAV_{ST}/UAV_{SR} changes from time to time, there are two components in the eavesdropping link, which named as auto-correlated component and independent component. The former relies on the previous channel condition and the latter is independent of previous channels. The two components are adjusted by a coefficient λ. Moreover, λ decreases with the growth of the speed of UAV_L. We define Signal to Noise Ratio (SNR) of the eavesdropping and jamming links at time slot x as $\gamma_e(x)$, which is

$$\gamma_e(x) = \gamma_j(x) = \sqrt{\frac{H_e(x) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon} \cdot \left(2^{\rho(x)} - 1\right)}{N_0}} \tag{7}$$

According to the regression model proposed in Reference [20], the PRR of suspicious data packets eavesdropped by UAV_L, which was denoted as $R(x)$, is given by

$$R(x) = \left(1 - \frac{1}{2} exp^{-\beta_0 \gamma_e(x) + \beta_1}\right)^{8(2f-l)} \tag{8}$$

where β_0 and β_1 are two constants in the regression model. Moreover, β_0 controls the shape of the regression curve and β_1 induces horizontal shifts of the curve. f and l denote frame size and preamble size of the data packet, respectively.

Case 2: UAV_L eavesdrops UAV_{ST} by jamming UAV_{SR}.

As shown in Figure 2b, UAV_L chooses UAV_{ST} for eavesdropping and UAV_{SR} for jamming. In this case, the channel gain in the eavesdropping link is the same as in Equation (6), and because of the jamming object selection of UAV_{SR}, the channel gain in the jamming link is changed as:

$$H_j(x) = \frac{\lambda H_j(x-1) + n\sqrt{1-\lambda^2}}{d_2^{\alpha_1}(x)} \tag{9}$$

where $d_2(x) = \sqrt{D(x)^2 - d_1^2(x)}$. Accordingly, the Signal to Noise Ratio (SNR) in the jamming link denotes as:

$$\gamma_j(x) = \sqrt{\frac{H_j(x) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon} \cdot \left(2^{\rho(x)} - 1\right)}{N_0}} \tag{10}$$

Case 3: UAV_L eavesdrops and jams UAV_{SR}.

As shown in Figure 2c, UAV_L only chooses UAV_{ST} for eavesdropping and jamming. The channel gains for eavesdropping and jamming links are denoted as:

$$H_e(x) = H_j(x) = \frac{\lambda H_e(x-1) + n\sqrt{1-\lambda^2}}{d_2^{\alpha_1}(x)} \tag{11}$$

where $d_2(x) = \sqrt{D(x)^2 - d_1^2(x)}$. Accordingly, the Signal to Noise Ratio (SNR) in the jamming link is the same as in Equation (7).

Case 4: UAV_L eavesdrops UAV_{SR} by jamming UAV_{ST}.

As shown in Figure 2d, UAV_L chooses UAV_{ST} for jamming and UAV_{SR} for eavesdropping. In this case, the channel gain in the eavesdropping link is the same as in Equation (11), and the channel gain in the jamming link is the same as in Equation (6).

4. Formulation and Policy

4.1. Problem Formulation

Without loss of generality, we consider the wireless communication, as shown in Figure 2b for the problem formulation, where UAV_L aims to eavesdrop data packets from UAV_{ST} via jamming UAV_{SR}. Note that our algorithm is common in the other three cases because channel gains for eavesdropping links are associated with $D(x)$ according to Equation (11). $D(x)$ is the only parameter that influences eavesdropped data packets. Based on the notations in the system model, we formulate the optimization problem to maximize the eavesdropped data packets via optimizing jamming power. Assume that each suspicious data packet has b bytes and then successfully eavesdropped data (in bytes) can be calculated as $\sum_{x=1}^{m} b \cdot R(x)$ in m time slots. To prevent legitimate jamming and eavesdropping being detected by suspicious UAVs, SINR of the suspicious link has to be maintained at a certain threshold δ, which presents $\gamma_s(x) = \delta$. Specifically, the modulation of UAV_{ST} that is used to transmit data to UAV_{SR} is $2^{\rho(x)}$ Quadrature Amplitude Modulation (QAM), where $\rho(x) = \{1, \ldots, \rho_{max}\}$. ρ_{max} indicates the number of modulation levels available for rate adaptation. Constraint $0 \leq \sum_{x=1}^{m} P_L(x) \leq P_L^{total}$ specifies that the total consuming power (eavesdropping plus jamming) of UAV_L during the eavesdropping period is required to be less than the total obtained power of the UAV_L, P_L^{total}. Constraint $P_L(x) \leq P_L^{max}$ $(\forall x,\ x = 1, 2, \ldots, m)$ specifies that, in each eavesdropping period, UAV_L consumes no more than P_L^{max} power. Then, the formulation of the problem is presented as follows.

$$\max_{P_L(x), \rho(x)} \sum_{x=1}^{m} b \cdot R(x) \tag{12}$$

Subject to:

$$\gamma_s(x) = \delta \tag{13}$$

$$0 \leq \sum_{x=1}^{m} P_L(x) \leq P_L^{total} \tag{14}$$

$$P_L(x) \leq P_L^{max} \ (\forall x,\ x = 1, 2, \ldots, m) \tag{15}$$

$$1 \leq \rho(x) \leq \rho_{max} \tag{16}$$

Furthermore, in terms of Equation (13), we have

$$\rho(x) = \log_2 \left(\frac{\delta^2 (N_0 + P_L(x))}{H_s(x) \cdot K_2^{-1} \ln \frac{K_1}{\epsilon}} + 1 \right) \tag{17}$$

which indicates that the modulation level is adapted by UAV_{ST} in terms of the consuming power $P_L(x)$ of UAV_L. Specifically, UAV_{ST} increases $\rho(x)$ to transmit data with an increasing $P_L(x)$ so that

SINR of the suspicious link at time slot x is maintained at δ. Moreover, considering Equation (5) and Equation (13), the upper bound and the lower bound of the consuming power $P_L(x)$ can be obtained by

$$P_L(x) = \begin{cases} \frac{H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0 \; if \; \rho(x) = 1 \\ \frac{(2^{\rho max}-1)H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0 \; if \; \rho(x) = \rho_{max} \end{cases} \tag{18}$$

Consequently, by substituting Equations (6), (7), (8), (9), (10), and (11) into (13), (14), (15), and (16) the optimization problem is reformulated as follows:

Optimal Eavesdropping and Jamming Problem:

$$\max_{P_L(x)} b\cdot \sum_{x=1}^{m} \left(1 - \frac{1}{2} exp^{\beta_1 - \beta_0 \delta \sqrt{\frac{H_e(x)+H_j(x)}{H_s(x)}\cdot(1+\frac{P_L(x)}{N_0})}}\right)^{8(2f-l)}$$

Subject to:

$$0 \le \sum_{x=1}^{m} P_L(x) \le P_L^{total}$$
$$P_L(x) \le P_L^{max} \; (\forall x, \; x = 1, 2, \ldots, m)$$
$$P_L(x) \ge \frac{H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0$$
$$P_L(x) \le \frac{(2^{\rho max}-1)H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0$$

4.2. Selection Policy For Eavesdropping and Jamming

First, the optimal consuming power, $P_L^*(x)$ in the optimization problem is able to be derived by linear optimization techniques, e.g., linear programming. Next, we propose the selection policy to allocate jamming power for UAV_L in real time, as shown in Policy 1. According to Reference [10], UAV_L overhears the channels of suspicious and eavesdropping link via channel probing, so the channel gains $H_s(x)$, $H_e(x)$, $H_j(x)$ and N_0 are known by UAV_L at the beginning of time slot x. Since $\gamma_s(x) = \delta$ is required by UAV_L to successfully eavesdrop the suspicious transmission, we have

$$P_L(x) \ge \frac{N_0\cdot\left(H_s(x) - H_e(x) - H_j(x)\right)}{H_e(x) + H_j(x)}$$

where $\rho(x)$ is given by Equation (11). Therefore, the jamming power at $x = k$ is initialized as

$$P_L^0(k) = \frac{N_0\cdot\left(H_s(x) - H_e(x) - H_j(x)\right)}{H_e(x) + H_j(x)}$$

Next, initialized jamming and eavesdropping power $P_L^0(k)$ is examined by UAV_L if the four constraints in the optimization problem 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 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 suspicious UAVs for the purpose of power efficiency. Moreover, if $\sum_{x=1}^{k-1} P_L(x) + P_L^0(k) \le P_L^{max}$ and constraints (14), (15), and (16) hold, the optimization problem is derived by UAV_L, and the optimal consuming power $P_L^*(x)$ is obtained.

Policy 1 Selection Policy

1: **BEGIN:**
2: k: denotes the current time slot, x: denotes the duration of time slot.
3: INPUT: $D(0)$, n, λ, α, $\alpha_2, \Delta v$
4: **If** $\Delta v = 0$ **then**
5: $$D = D(0)$$
6: **Else**
7: $$D(k) = D(k-1) = kx\Delta v$$
8: **End if**
9: Acquire: $H_s(k)$, $\gamma_s(k)$ via $D(k)$
10: Acquire: UAV_L's position: $d_1(k)$, $d_2(k)$
While
11: $E(k) = [0,1]^T \Big| |E(k) = [1,0]^T | \Big| J(k) = [0,1]^T || J(k) = [1,0]^T$
do
12: Acquire: $P_L(k) = P_L^e(k) + P_L^j(k)$
13: power set in all cases: $\left\{ P_L^i(k) \right\}$, i $= 1, 2, 3, 4$.
14: **End while**
15: **For** $i = 1 : 4$, $i++$ do
16: **If** the Equations (13) (14) (15) **then**
17: derive Power-efficient package rate maximum problem
18: Acquire $P_L^{i*}(k)$
19: **else**
20: $$P_L^{i*}(k) = 0,\ E(k) = [0,0]^T,\ J(k) = [0,0]^T$$
21: **Endif**
22: **endfor**
23: $$P_L^*(k) = \min\left\{ P_L^{i*}(k) \right\},\ i^* = \operatorname{argmin}\left\{ P_L^{i*}(k) \right\}$$
24: Output: $E(k) = E^{i*}(k)$, $J(k) = J^{i*}(k)$
25: **If** $E(k) = E(k-1) \&\& J(k) = J(k-1)$ then
26: UAV_L doesn't shift the eavesdropping-jamming model.
27: **else**
28: UAV_L shifts the eavesdropping-jamming model from $E(k-1)$, $J(k-1)$ *to* $E(k)$, $J(k)$
29: **endif**
30: $$k = k + 1$$
31: Go back to line 6 until $k = m + 1$
32: **END**

4.3. Policy Analysis

4.3.1. Computing Complexity

Note that the power consumption of executing selection policy is much smaller than the jamming power of UAV_L, which is negligible. The time complexity of selection policy is denoted as $O(n^2m + nm)$. Based on [13], the time complexity of Power Efficient Legitimate Eavesdropping (PELE) that calculate the optimal power result is $O(m)$ which depends on the number of time slots. Considering the number of cases used in eavesdropping and jamming models, which are denoted as n, the selection policy's time consumption in finding optimal power solutions is $O(nm)$. After calculating optimal power consumptions in all cases in each time slot, the algorithm uses the Bubble method [39] to acquire the minimum power in all cases, which are denoted as $O(n^2)$ in each time slot and $O(mn^2)$ in the whole eavesdropping and jamming process.

Therefore, the selection policy's time complexity can be denoted as $O(n^2m + nm)$, where n denotes the number of cases and m denotes the number of time slots.

In our research, we find that it is a challenging problem to solve the optimal number of time slots for accurate resolution of the optimization problem. As the complexity increases, it is really difficult to obtain the optimal number of slots for accurate resolution of our problem. Due to the limitations on laboratory equipment, we only discuss the algorithm performance with six time slots in our simulations. Our further research is to design an algorithm to research the optimal number of slots for accurate resolution of the optimization problem.

4.3.2. Feasible Solution

Regarding the proposed Optimal Eavesdropping and Jamming Problem, we will discuss whether it has the feasible solution or not. Based on Reference [40], the optimization model that has the feasible solution should satisfy three constraints: (a) The variable is effective collection based on the constraints in the optimization model, (b) the objective of the optimization model is the continuous function, and (c) the objective of the optimization model is a convex function. We will prove these three properties in this part.

First, we will discuss the variable's effective collection under the constraints in our proposed optimization model. The constraints $0 \leq \sum_{x=1}^{m} P_L(x) \leq P_L^{total}$ and $P_L(x) \leq P_L^{max}$ $(\forall x,\ x = 1, 2, \ldots, m)$ relates to the practice in the reality, which defines $P_L(x)$'s maximums of upper and lower bound. The last two constraints should be proved, satisfying the effective collection. They make further definition of $P_L(x)$'s upper and lower bound, furthermore, the relationship between $\frac{H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0$ and $\frac{(2^{\rho_{max}}-1)H_s(x)\cdot K_2^{-1}\ln\frac{K_1}{\epsilon}}{\delta^2} - N_0$ should be considered. In fact, the parameters $H_s(x)$, K_2^{-1}, and δ^2 are larger than zero. K_1 is larger than ϵ, which means that $\ln\frac{K_1}{\epsilon} > 0$, then the last two constraints can be transformed into:

$$1 \leq \frac{\delta^2 P_L(x)}{H_s(x)\ K_2^{-1}\ln\frac{K_1}{\epsilon}} \leq 2^{\rho_{max}} - 1$$

ρ_{max} is a parameter that is larger than 1. Therefore, the variable $P_L(x)$ has the effective collection under the four constraints in the optimization model.

Second, we will discuss the objective's consecutiveness in the optimization model. Obviously, the objective is a composite function, which uses the constant function, power function, exponential function and the logarithmic function based on $P_L(x)$, $H_s(x)$, $H_e(x)$, and $H_j(x)$. It is easy to prove that the functions of $P_L(x)$, $H_s(x)$, $H_e(x)$, and $H_j(x)$ are all continuous functions. Moreover, the sum function does not affect the function's consecutiveness. Therefore, the objective in our proposed Optimal Eavesdropping and Jamming Problem is a continuous function.

Finally, we will discuss whether the objective in our proposed Optimal Eavesdropping and Jamming Problem is a convex function or not. In order to simplify, we define the objective function as G(x), where

$$\mathrm{G(x)} = \left(1 - \frac{1}{2} exp^{\beta_1 - \beta_0\delta\sqrt{\frac{H_e(x)+H_j(x)}{H_s(x)}\cdot(1+\frac{P_L(x)}{N_0})}}\right)^{8(2f-l)}$$

We have proved that the objective is a continuous function in the above paragraph, and then the convex property can be proved by the second derivation, which is denoted as:

$$G''(x) = -bln[8(2f-l)]\cdot\tfrac{1}{2}\exp\left(\beta_1 - \beta_0\delta\sqrt{\frac{H_e(x)+H_j(x)}{H_s(x)}\cdot\left(1+\frac{P_L(x)}{N_0}\right)}\right)$$
$$\cdot ln\tfrac{1}{2}\left[\left(\frac{H_e(x)+H_j(x)}{H_s(x)}\right)'' + \left(\frac{P_L(x)}{N_0}\frac{H_e(x)+H_j(x)}{H_s(x)}\right)''\right]$$

According to the non-negativity of exponential function, the second term of $G''(x)$ will be larger than zero. Regarding the first term of $G''(x)$, the preamble size l is always smaller than the frame size

f in the practice, then the result of $8(2f - l)$ will be larger than 1, thus the first term is smaller than 0. Regarding the third term of $G''(x)$, which is denoted as:

$$\left(\frac{H_e(x)+H_j(x)}{H_s(x)}\right)'' \frac{1}{N_0}\left[2P_L'(x)\left(\frac{H_e(x)+H_j(x)}{H_s(x)}\right)' + P_L(x)\left(\frac{H_e(x)+H_j(x)}{H_s(x)}\right)'' + P_L''(x)\left(\frac{H_e(x)+H_j(x)}{H_s(x)}\right)\right] \geq 0$$

Therefore, the first term $G''(x)$ is smaller than zero, and the second and the third terms are larger than zero. The second derivate result is smaller than zero. The objective of our proposed Optimal Eavesdropping and Jamming Problem is a convex function.

Finally, from the discussions above, we have the conclusions that: (1) The time complexity of selection policy is $O(n^2m + nm)$, and (2) our proposed Optimal Eavesdropping and Jamming Problem has the feasible solution.

5. Numerical Results

In this section, we provide simulation results to verify the performance of our proposed selection policy. Furthermore, we choose four normal fading channels, e.g., Rayleigh, Ricean, Weibull, and Nakagami, to investigate the impacts on our proposed selection policy.

5.1. Simulation Configurations

The distance between the two suspicious UAVs is D, which various from 500 m to 2000 m, and the path length of UAV_L is $\pi D/2$. The patrolling speed of UAV_L is set to 10 m/s. In fact, we do realize the policies for using UAVs in our country. It is allowed for flying UAVs freely under altitudes of 120 m. In our research, the distance variation (from 500 m to 2000 m) is mainly in the same altitude, which can be within the permission of policies. We use MATLAB to conduct the experiments instead of an actual simulator, however, the experiments can be legally carried if there are enough equipped UAVs. The detailed system-level simulation parameters are shown in Table 2.

Table 2. Simulation Parameters.

Parameters	Values
K_1	0.2
K_2	3
β_0	2.6
β_1	1
φ	60
φv	$[-10, 10]$
θ	$[0, \pi]$
f	20
l	10
ϵ	0.05
N_0	3.98×10^{-12} W
b	100 bytes
δ	3
λ	0.3
n	0.005377
α_1	3
α_2	2.5
D	500 m, 1000 m, 1500 m, 2000 m
P_L^{max}	8×10^{-6} W
ρ	1, 2, 4, 8
Constant Jamming Power	10^{-8} W

UAV_{ST} communicates with UAV_{SR} in a TDMA fashion for suspicious collision-free transmission. Especially, we consider that a TDMA frame contains 6 time slots, and each of which is 10 s long. In one time slot, UAV_{ST} transmits its data to UAV_{SR}, where UAV_L eavesdrops and decides to jam the suspicious communication according to the selection policy. 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.

5.2. Eavesdropping Rate and Power Consumption

For comparison, we consider other two legitimate eavesdropping strategies: proactive eavesdropping with constant jamming power and zero jamming power. For the former scheme, we set the constant jamming power to 10^{-8} W (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). For the latter scheme, we set the constant jamming power to 0, which means UAV_L passively overhears the packets transmitted by suspicious UAVs without sending jamming signal to the suspicious link [17,18,21].

Figure 6 shows that selection policy saves 65.79%, 52.66%, 78.12%, and 13.92% more power than the constant-Jamming scheme, when D = 500 m, 1000 m, 1500 m, and 2000 m, respectively. Selection policy saves 74.73%, 39.02%, 74.35%, and 8.40% more power than the No-Jamming scheme, when D = 500 m, 1000 m, 1500 m, and 2000 m, respectively. The power consumption of selection policy increases as time goes on in each simulation. The reason is that UAV_L consumes power to eavesdrop suspicious UAVs either by jamming or not, thus the power consumption increases as time goes on. Power consumptions are not compared with each other under different distances, because in each simulation, UAVs fly at random speeds (e.g., random Δv), thus causing different power consumptions that cannot simply be compared with each other.

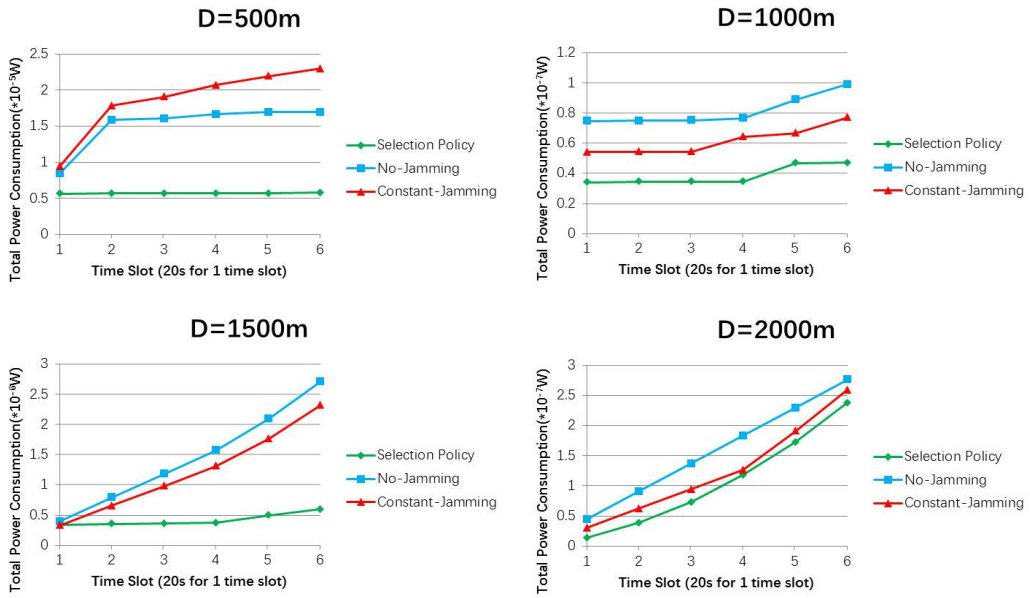


Figure 6. Total power consumptions by UAV_L in different Ds with different jamming methods.

Figure 7 presents the other two methods with optimal solutions in terms of the eavesdropped packets. Selection policy outperforms No-Jamming and Constant-Jamming schemes under different distances in the simulations. The reason is that selection policy purposely adapts the jamming power of UAV_L to change the suspicious communication (e.g., to a smaller data rate) for overhearing more packets. In each eavesdropping time slot, UAV_L selects proper eavesdropping case according to the selection policy, thus eavesdropping more information. When D = 500 m, selection policy outperforms the other two schemes by nearly 1.2 times. However, the divisions between the selection policy and the other two methods are narrowed when distances increase. That is because in such long-distance cases,

channel conditions dominate the data rate rather than eavesdropping methods, so UAV_L can receive almost the same number of eavesdropped packets regardless which algorithm UAV_L has chosen.

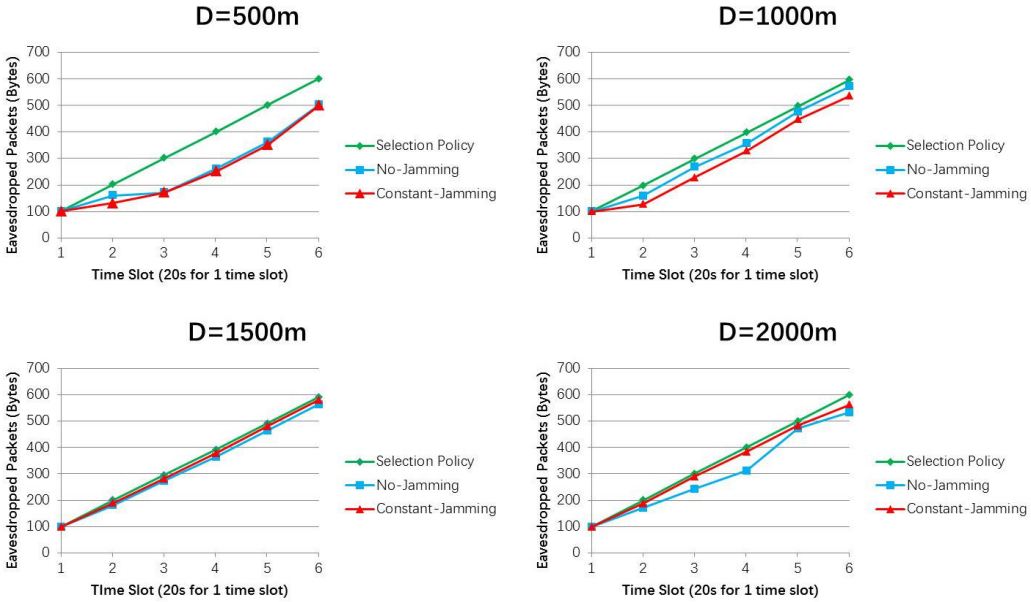


Figure 7. Eavesdropped packets by UAV_L in different Ds with different jamming methods.

5.3. Impact of Typical Fading Models

We apply selection policy into four typical fading channel models, i.e., Rayleigh, Ricean, Weibull and Nakagami, to study the impacts. Each fading channel is characterized with a specific coefficient component. In particular, the coefficient component of Rayleigh, Rician, Weibull, and Nakagami is set to 2, 1, 2, and 0.5, respectively [30].

In Figure 8, total power consumption increases with time going on regardless of distances. However, power consumption increases more sharply in short-distance cases (D = 500 m). That is because in short-distance cases, eavesdropping algorithms dominate eavesdropping performances, while in long-distance cases, fading channels dominate power consumptions rather than eavesdropping algorithms. This can also be interpreted by the eavesdropped packets in regards to the time slots, which is shown in Figure 9.

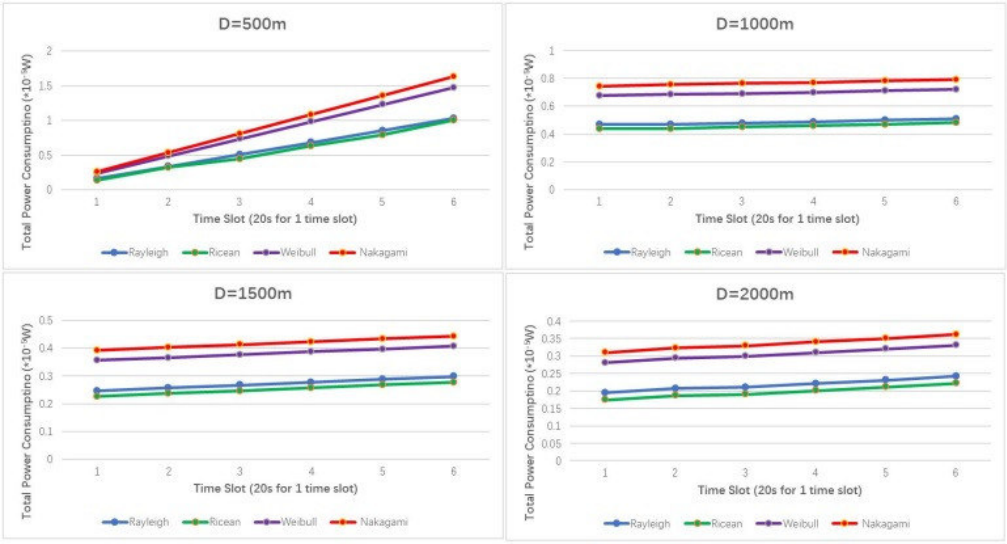


Figure 8. Total power consumptions by UAV_L in different Ds under different fading channels.

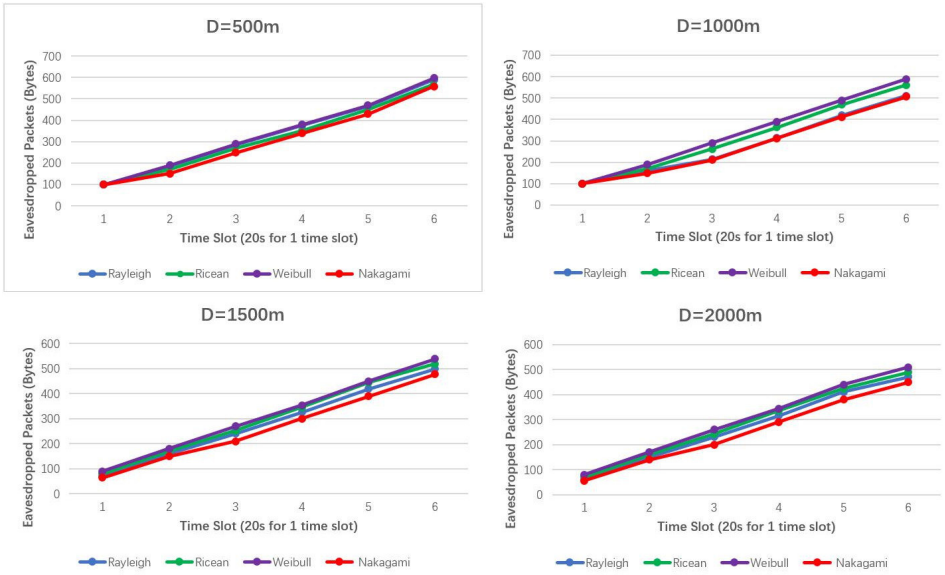


Figure 9. Eavesdropped packets by UAV_L in different Ds under different fading channels.

Figure 9 shows that eavesdropped packets under selection policy linearly grows with time in the four typical fading channels. Selection policy performs best in Weibull fading channel, but not obviously. Total eavesdropped packets are less in Nakagami fading channel 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 [41,42], 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.

6. Conclusions

In this paper, we investigated a proactive eavesdropping and jamming scenario which include four cases for UAV_L to fulfil surveillance tasks. In such a surveillance paradigm, we formulated a power-efficient eavesdropping and jamming problem which has acceptable computing complexity and can be solved. Then, we proposed a selection policy for UAV_L to allocate eavesdropping and jamming power efficiently. Particularly, UAV_L selects the most efficient case for eavesdropping and jamming suspicious UAVs according to the selection policy in each time slot. With such policy, UAV_L can eavesdrop more data by consuming less power. Simulation results showed that selection policy outperformed No-Jamming and Constant-Jamming schemes in both power consumption and data reception. Moreover, we applied selection policy into four typical fading channels to validate the performance, results showed that selection policy performs better in Weibull fading channels in terms of the package received rate (PRR). For future works, we plan to study the problems about jamming and eavesdropping towards suspicious UAV groups, which is a challenge for eavesdropping and jamming policy selection.

Author Contributions: Methodology, X.W.; software, X.Z.; validation, S.S.K., K.L. and E.T.; formal analysis, C.G.; writing—review and editing, X.W.; supervision, D.L.

Funding: This work is supported by Shanghai Science and Technology Committee under Grant No. 18DZ1200500; the NSF of China under Grant No. 71171045, No. 61772130 and No. 61301118; the Innovation Program of Shanghai Municipal Education Commission under Grant No. 14YZ130; and the International S&T Cooperation Program of Shanghai Science and Technology Commission under Grant No. 15220710600.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, C.; Xu, Y.; Xia, J.; Zhao, J. Protecting secure communication under UAV smart attack with imperfect channel estimation. *IEEE Access* **2018**, *6*, 76395–76401. [CrossRef]
2. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
3. Ju, H.; Zhang, R. Throughput maximization in wireless powered communication networks. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 418–428. [CrossRef]
4. Xu, J.; Zhang, R. Energy beamforming with one-bit feedback. *IEEE Trans. Signal Process.* **2014**, *62*, 5370–5381. [CrossRef]
5. Xu, J.; Liu, L.; Zhang, R. Multiuser MISO beamforming for simultaneous wireless information and power transfer. *IEEE Trans. Signal Process.* **2014**, *62*, 4798–4810. [CrossRef]
6. Xu, J.; Zhang, R. A general design framework for MIMO wireless energy transfer with limited feedback. *IEEE Trans. Signal Process.* **2016**, *64*, 2475–2488. [CrossRef]
7. Tran, H.; Zepernick, H.J. Proactive attack: A strategy for legitimate eavesdropping. In Proceedings of the IEEE International Conference on Communications and Electronics (ICCE), Ha Long, Vietnam, 27–29 July 2016; pp. 457–461.
8. Zeng, Y.; Zhang, R. Wireless information surveillance via proactive eavesdropping with spoofing relay. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1449–1461. [CrossRef]
9. Ayub, M.F.; Ghawash, F.; Shabbir, M.A.; Kamran, M.; Butt, F.A. Next Generation Security and Surveillance System Using Autonomous Vehicles. In Proceedings of the 2018 Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS), Wuhan, China, 22–23 March 2018.
10. Xu, J.; Duan, L.; Zhang, R. Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm. *IEEE Wirel. Commun.* **2017**, *24*, 152–159. [CrossRef]
11. Xu, J.; Duan, L.; Zhang, R. Proactive eavesdropping via cognitive jamming in fading channels. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2790–2806. [CrossRef]
12. Zhou, X.; Maham, B.; Hjorungnes, A. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 903–907. [CrossRef]
13. Wang, X.; Li, K.; Kanhere, S.S.; Li, D.; Zhang, X.; Tovar, E. PELE: Power efficient legitimate eavesdropping via jamming in UAV communications. In Proceedings of the Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 402–408.
14. Lakshmanan, S.; Tsao, C.; Sivakumar, R.; Sundaresan, K. Securing wireless data networks against eavesdropping using smart antennas. In Proceedings of the 28th International Conference on Distributed Computing Systems, Beijing, China, 17–20 June 2008; pp. 19–27.
15. Raymond, R.; Midkiff, S. Denial-ofservice in wireless sensor networks: Attacks and defenses. *IEEE Perv. Comput.* **2008**, *7*, 74–81. [CrossRef]
16. Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A. A survey of routing attacks in mobile ad hoc networks. *IEEE Wirel. Commun.* **2007**, *14*, 85–91. [CrossRef]
17. Meyer, U.; Wetzel, S. A man-in-themiddle attack on UMTS. In Proceedings of the 3rd ACM Workshop Wireless Security, Philadelphia, PA, USA, 1 October 2004; pp. 90–97.
18. Ohigashi, T.; Morii, M. A practical message falsification attack on WPA. In Proceedings of the Joint Workshop Inf. Security, Kaohsiung, Taiwan, 6–7 August 2009; pp. 1–12.
19. Shiu, Y.-S.; Chang, S.Y.; Wu, H.-C.; Huang, S.C.-H.; Chen, H.-H. Physical layer security in wireless networks: A tutorial. *IEEE Wirel. Commun.* **2011**, *18*, 66–74. [CrossRef]
20. Christof, P.; Pelzl, J.; Preneel, B. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2009.
21. Elliott, C. Quantum cryptography. *IEEE Secur. Priv.* **2004**, *2*, 57–61. [CrossRef]
22. Cui, M.; Zhang, G.; Wu, Q.; Ng, D.W.K. Robust trajectory and transmit power design for secure UAV communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 9042–9046. [CrossRef]
23. Zhou, Y.; Yeoh, P.L.; Chen, H.; Li, Y.; Hardjawana, W.; Vucetic, B. Secrecy outage probability and jamming coverage of UAV-enabled friendly jammer. In Proceedings of the 11th IEEE Australia International Conference on Signal Processing and Communication Systems (ICSPCS), Surfers Paradise, QLD, Australia, 13–15 December 2017; pp. 1–6.

24. Wang, Q.; Chen, Z.; Mei, W.; Fang, J. Improving physical layer security using UAV-enabled mobile relaying. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 310–313. [CrossRef]
25. Zhang, S.; Zhang, H.; He, Q.; Bian, K.; Song, L. Joint trajectory and power optimization for UAV relay networks. *IEEE Commun. Lett.* **2018**, *22*, 161–164. [CrossRef]
26. Mukherjee, A.; Swindlehurst, A.L. Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in mimo channels. In Proceedings of the Military Communications Conference, San Jose, CA, USA, 31 October–3 November 2010; pp. 1695–1700.
27. Li, Y.; Xiao, L.; Dai, H.; Poor, H.V. Game theoretic study of protecting MIMO transmissions against smart attacks. In Proceedings of the IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
28. Mukherjee, A.; Swindlehurst, A.L. Jamming games in the MIMO wiretap channel with an active eavesdropper. *IEEE Trans. Signal Process.* **2013**, *61*, 82–91. [CrossRef]
29. Yoo, T.; Goldsmith, A. Capacity and power allocation for fading MIMO channels with channel estimation error. *IEEE Trans. Inf. Theory* **2006**, *52*, 2203–2214.
30. Edman, M.; Kiayias, A.; Yener, B. On passive inference attacks against physical-layer key extraction? In Proceedings of the Fourth European Workshop on System Security, ACM, Salzburg, Austria, 10 April 2011; Volume 8.
31. Mitrpant, C.; Vinck, A.; Luo, Y. An achievable region for the Gaussian wiretap channel with side information. *IEEE Trans. Inf. Theory* **2006**, *52*, 2181–2190. [CrossRef]
32. Negi, R.; Goel, S. Secret communication using artificial noise. In Proceedings of the IEEE International Conference on Vehicular Technology (VTC), Dallas, TX, USA, 28 September 2005; Volume 3, pp. 1906–1910.
33. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
34. Zheng, G.; Krikidis, I.; Li, J.; Petropulu, A.P.; Ottersten, B. Improving physical layer secrecy using fullduplex jamming receivers. *IEEE Trans. Signal Process.* **2013**, *61*, 4962–4974. [CrossRef]
35. Wu, Q.; Mei, W.; Zhang, R. Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective. *arXiv* **2019**, arXiv:1902.02472.preprint.
36. Li, A.; Wu, Q.; Zhang, R. UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel. *IEEE Wirel. Commun. Lett.* **2018**, *8*, 181–184. [CrossRef]
37. Zhang, G.; Wu, Q.; Cui, M.; Zhang, R. Securing UAV communications via joint trajectory and power control. *IEEE Trans. Wirel. Commun.* **2019**. [CrossRef]
38. Li, K.; Ni, W.; Wang, X.; Liu, R.P.; Kanhere, S.S.; Jha, S. Energy-efficient cooperative relaying for unmanned aerial vehicles. *IEEE Trans. Mobile Comput.* **2016**, *15*, 1377–1386. [CrossRef]
39. Schoel, W.M.; Schürch, S.; Goerke, J. The captive bubble method for the evaluation of pulmonary surfactant: Surface tension, area, and volume calculations. *Biochim. Biophys. Acta (BBA)-Gen. Subj.* **1994**, *1200*, 281–290. [CrossRef]
40. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.
41. Wu, Q.; Zhang, R. Common throughput maximization in UAV-enabled OFDMA systems with delay consideration. *IEEE Trans. Commun.* **2018**, *66*, 6614–6627. [CrossRef]
42. Wu, Q.; Zeng, Y.; Zhang, R. Joint trajectory and communication design for multi-UAV enabled wireless networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2109–2121. [CrossRef]