UAV-Assisted Legitimate Wireless Surveillance: Performance Analysis and Optimization

1st Dongxuan He
School of Information and Electronics
Beijing Institute of Technology
Beijing, China
dongxuan_he@bit.edu.cn

2nd Huazhou Hou
Pervasive Communication Research Center
Purple Mountain Laboratories
Nanjing, China
houhuazhou@pmlabs.com.cn

***Abstract*—In this work, we consider a wireless legitimate surveillance system, where a multi-antenna legitimate monitor unmanned aerial vehicle (UAV) aims to eavesdrop a suspicious communication link with the help of a jammer UAV. In particular, the flying height of monitor UAV and jammer UAV can be adjusted to obtain a better monitoring performance. To analyze the monitoring performance, the closed-form expressions of the maximum suspicious communication and eavesdropping non-outage probability are derived, which help us analyze the monitoring performance in terms of average eavesdropping rate. Moreover, based on the derived expressions, the flying height of UAVs is selected to optimize the monitoring performance. The simulation results verify the effectiveness of our derived closed-form expressions and our considered UAV-assisted legitimate wireless surveillance..**

***Index Terms*—Wireless legitimate surveillance, eavesdropping non-outage probability, Rician fading, UAV**

I. Introduction

Due to the broadcasting nature of wireless medium, security has been an important issue in wireless communications. In particular, the user-controllable wireless infrastructures may be embezzled by malicious users such as criminals and terrorists to carry illegal information, which has posed a severe threat to the national and social security [1]. To address this issue, proactive eavesdropping, where the legitimate monitors act as the eavesdroppers, has been proposed to monitor the suspicious communication, thus realizing reliable wireless communication [2], [3].

Aiming at monitoring secretively without exposure, it is reasonable to deploy legitimate monitors far away from the suspicious transmitter [4]. As a result, the received signal of the legitimate eavesdropping channel will be a degraded counterpart compared to the suspicious receiver, thus limiting the monitoring performance of the listening-only surveillance.

To tackle this problem, proactive eavesdropping relying on jamming has been regarded as an efficient methodology to guarantee monitoring performance [4]–[8]. For instance, Xu *et al.* [5] conceived the jamming-assisted proactive eavesdropping paradigm, where a dual antenna monitor operating in a full-duplex manner transmits the jamming signal to enhance the eavesdropping efficiency. As a further development, Zhong *et al.* [4] and Feizi *et al.* [6] proposed jamming-assisted proactive eavesdropping scheme for multi-antenna legitimate monitors, where transmit and receive beamformers are jointly optimized at the legitimate monitor to improve the monitoring performance. Moon *et al.* [7] have shown the superiority of cooperative jamming based monitoring in relay-assisted proactive eavesdropping systems. Moreover, Sun *et al.* [8] developed an alternate-jamming-aided surveillance scheme, where two single-antenna nodes operate at eavesdropping and jamming mode alternately to optimize the monitoring performance. However, in these works, the channel state information (CSI) between the monitor and the suspicious receiver is assumed to be known, which is unavailable in reality.

In contrast, relying on unmanned aerial vehicle (UAV), the legitimate monitor can be deployed flexibly, thus guaranteeing the effectiveness of wireless surveillance [9]. Moreover, since the flying UAV can obtain monitoring link with line-of-sight (LoS) more easily when compared to the terrestrial monitor, the monitoring performance could be improved significantly with the help of UAVs.

Against this background, exploiting the potential of the UAV as a legitimate monitor, UAV-assisted wireless surveillance is investigated in this paper. More specifically, we first consider the system model of UAV-assisted legitimate wireless surveillance, and the closed-form expression of the monitoring performance is derived. Then, based on the derived expressions, the flying height is optimized to have a better monitoring performance. The simulation results verify the accuracy of our derived results and the effectiveness of our considered scheme.

II. System Model

We consider a legitimate surveillance system including a suspicious terrestrial transmission pair (Alice and Bob), a legitimate monitor UAV (Eve) and a jammer UAV (Jam), where Alice transmits to Bob under a delay-limited transmission mode[1] and E aims to monitor the suspicious transmission from Alice to Bob with the help of Jam. In addition, Eve and Jam are equipped with uniform linear arrays (ULAs) with N_e and N_j antenna elements respectively, while Alice and Bob are all equipped with a single antenna. A three-dimensional

[1]Due to the equal importance of information in different transmission blocks, Alice adaptively adjusts its transmission rate to guarantee a predefined outage probability under the delay-limited transmission mode [9], [10].

2024 IEEE International Conference on Unmanned Systems (ICUS) | 979-8-3503-8418-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICUS61736.2024.10839893

979-8-3503-8418-5/24/$31.00 ©2024 IEEE

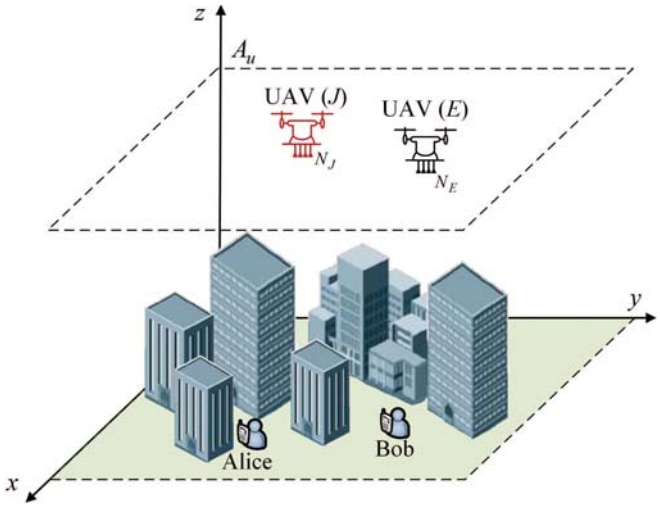

Fig. 1. System model.

Cartesian coordinate is utilized to depict the locations of the nodes, where the locations of of Alice, Bob, Eve and Jam are denoted by $(x_a, y_a, 0)$, $(x_b, y_b, 0)$, (x_e, y_e, A_e) and (x_j, y_j, A_j), respectively. To simplify the design in the sequel, we assume that the monitoring UAV and jammer UAV fly at the same height, i.e., $A_e = A_j = A_u$. Furthermore, the channel coefficients of the Alice-Bob link, Alice-E link, J-Bob link and J-E link between are denoted as h_{ab}, $\mathbf{h}_E$, $\mathbf{h}_J$ and $\mathbf{H}_I$, respectively.

A. Channel Model

Since both Alice and Bob are terrestrial nodes, the suspicious between Alice and Bob is subject to independent and identically distributed (i.i.d.) Rayleigh fading. As a result, $|h_{ab}|^2$ can be modeled as independent exponentially distributed random variables with parameter λ, i.e., $|h_{ab}|^2 \sim \text{Exp}(\lambda_{ab})$.

Due to the random distribution of obstacles between terrestrial nodes and UAVs, the LoS of $\mathbf{h}_E$ and $\mathbf{h}_J$ exists with a given probability, which is determined by the environment, locations of terrestrial devices and the UAV as well as the evaluation angle [11]. As a result, probabilistic LoS channel model is utilized to model the UAV-to-ground channels, i.e., $\mathbf{h}_E$ and $\mathbf{h}_J$. Specifically, the LoS probability of channel can be expressed as [12]

$$P_i^L = \frac{1}{1 + \varphi \exp\left(-\beta\left(\theta_i - \varphi\right)\right)}, \tag{1}$$

where $i \in \{E, J\}$, φ and β are constant values determined by the environment, and θ_i is the elevation angle, given by

$$\theta_i = \frac{180}{\pi} \arcsin\left(\frac{A_u}{d_i}\right), \tag{2}$$

where d_i denotes the distance, given by

$$d_i = \sqrt{\Delta x_i^2 + \Delta y_i^2 + A_u^2}, \tag{3}$$

with $\Delta x_E = x_e - x_a$, $\Delta y_E = y_e - y_a$, $\Delta x_J = x_j - x_b$ and $\Delta y_J = y_j - y_b$. Accordingly, the Non-LoS (NLoS) probability of link i can be calculated as $P_i^{NL} = 1 - P_i^L$.

We consider that Jam-Bob link experience Rician fading for LoS propagation conditions and Rayleigh fading for NLoS propagation conditions. In particular, the channel $\mathbf{h}_{jb}$ for LoS propagation condition can be expressed as

$$\mathbf{h}_{jb} = \sqrt{\frac{K_i}{K_i + 1}}\mathbf{h}_i^{\circ} + \sqrt{\frac{1}{K_i + 1}}\mathbf{h}_i^{r}, \tag{4}$$

where K_i denotes the Rician-K factor of $\mathbf{h}_i$, $\mathbf{h}_i^{\circ}$ and $\mathbf{h}_i^{r}$ denote the LoS and scattered components of $\mathbf{h}_i$, respectively. Specifically, the elements of $\mathbf{h}_i^{r}$ are assumed to be i.i.d complex Gaussian random variables with zero mean and unit variance, and $\mathbf{h}_i^{\circ}$ can be expressed as [13]

$$\mathbf{h}_i^{\circ} = [1, \cdots, \exp\left(j2\pi\left(N_i - 1\right)\delta_a \cos\theta_i \sin\varphi_i\right)], \tag{5}$$

where δ_a denotes the constant spacing, in wavelengths, between adjacent antenna elements of UAV i. ϕ_i is the azimuth angle, which can be expressed as

$$\varphi_i = \frac{180}{\pi} \arctan\left(\frac{\Delta y_i}{\Delta x_i}\right), \tag{6}$$

Different from UAV-to-ground channels with probabilistic LoS, we consider Jam-Eve link experiences Rician fading since there does not exist obstacles between J and E. As such, the channel coefficient of J-E link is given by

$$\mathbf{H}_{je} = \sqrt{\frac{K_{je}}{K_{je} + 1}}\mathbf{H}_{je}^{\circ} + \sqrt{\frac{1}{K_{je} + 1}}\mathbf{H}_{je}^{r}, \tag{7}$$

where $\mathbf{H}_{je}^{\circ}$ is the LOS component, and $\mathbf{H}_{je}^{r}$ is the scattered component represented by a matrix with i.i.d circularly-symmetric complex Gaussian random variables with zero mean and unit variance. Specifically, $\mathbf{H}_{je}^{\circ}$ is given by [14]

$$\mathbf{H}_{je}^{\circ} = \mathbf{g}_e^T \mathbf{g}_j, \tag{8}$$

where $\mathbf{g}_E$ denotes the array responses at E, given by

$$\mathbf{g}_e = [1, \cdots, \exp\left(j2\pi\left(N_E - 1\right)\delta_a \cos\phi_J\right)], \tag{9}$$

where ϕ_J represents the angle of arrival from E to J. Besides, $\mathbf{g}_J$ denotes the array response at J, given by

$$\mathbf{g}_j = [1, \cdots, \exp\left(j2\pi\left(N_J - 1\right)\delta_a \cos\phi_E\right)], \tag{10}$$

where ϕ_E represents the angle from J to E.

B. Legitimate Monitoring

Define the message sent by Alice and the jamming signal generated by J as x and $\mathbf{s}$, respectively. Accordingly, the received signals at Bob and E can be respectively formulated as

$$y_b = \sqrt{p_a d_{ab}^{-\eta}} h_{ab} x + \sqrt{p_j d_{jb}^{-\eta}} \mathbf{h}_{jb} \mathbf{w}\mathbf{s} + n_b, \tag{11}$$

$$\mathbf{y}_e = \sqrt{p_a d_{ae}^{-\eta}} \mathbf{h}_{ae}^{\dagger} x + \sqrt{p_j d_{je}^{-\eta}} \mathbf{H}_{je} \mathbf{w}\mathbf{s} + \mathbf{n}_e, \tag{12}$$

where p_a and p_j represent the transmit power of Alice and jamming power of J, respectively, $(\cdot)^\dagger$ denotes the conjugate transposition, $\mathbf{w}$ is the jamming matrix. n_b with zero mean and variance σ_b^2 is the additive white Gaussian noise (AWGN) at Bob, and $\mathbf{n}_e$ with zero mean and variance $\sigma_e^2\mathbf{I}_{N_e}$ is the AWGN at Eve, where $\mathbf{I}_{N_e}$ is a $N_e \times N_e$ identity matrix.

Furthermore, the signal-to-interference-plus-noise ratio (SINR) at Bob can be calculated as

$$\gamma_b = \widetilde{\gamma}_{ab}|h_{ab}|^2 / \left(\widetilde{\gamma}_{jb}|\mathbf{h}_{jb}\mathbf{w}|^2 + 1\right), \tag{13}$$

where $\widetilde{\gamma}_{ab} = p_a d_{ab}^{-\eta_{ab}}/\sigma_b^2$ and $\widetilde{\gamma}_{jb} = p_j d_{jb}^{-\eta_{jb}}/\sigma_b^2$, and the SINR at monitor UAV can be expressed as [15]

$$\gamma_e = \frac{\widetilde{\gamma}_{ae}\|\mathbf{h}_{ae}\|^2}{\widetilde{\gamma}_{je}\|\mathbf{H}_{je}\mathbf{w}\|^2 + 1}, \tag{14}$$

where $\widetilde{\gamma}_{me}$ for $m \in \{a, j\}$ is given by

$$\widetilde{\gamma}_{me} = \begin{cases} \widetilde{\gamma}_{me}^{L}, & \text{with probability } P_{me}^{L} \\ \widetilde{\gamma}_{me}^{NL}, & \text{with probability } 1 - P_{me}^{NL} \end{cases}, \tag{15}$$

with $\widetilde{\gamma}_{me}^{L} = p_m d_{me}^{-\eta_{me}^{L}}/\sigma_e^2$ and $\widetilde{\gamma}_{me}^{NL} = p_m d_{me}^{-\eta_{me}^{NL}}/\sigma_e^2$ with $\eta_{me}^{NL} > \eta_{me}^{L} > 2$.

Given the transmission environment under jamming, Alice would adjust its transmission rate R_s to guarantee the transmission outage probability p_{to} satisfy a target value δ_0, $0 < \delta_0 < 1$, which can be mathematically expressed as

$$p_{to} = \Pr\left(\gamma_b \le \gamma_0\right) = \delta_0, \tag{16}$$

with $\gamma_0 = 2^{R_s} - 1$.

Obviously, the monitor UAV can reliably decode the information if $\gamma_e \ge \gamma_b$ and fails to decode the information without any error when $\gamma_e < \gamma_b$. To evaluate the eavesdropping performance of our considered monitor UAV in detail, average eavesdropping rate is selected as performance metric, which depicts the average rate successfully decoded by monitor UAV, given by

$$R_{\text{ave}} = R_s\left(1 - p_{eo}\right), \tag{17}$$

where $p_{eo} = \Pr\left(\gamma_e \le \gamma_0\right)$ represents the eavesdropping outage probability (EOP), indicating the probability that monitor UAV fails to decode the information without any error.

In this work, the main objective is to maximize the average eavesdropping rate by adjusting the height of UAV and jamming power, which can be formulated as

$$\max_{P_J, A_u} \quad R_{\text{ave}}, \tag{18a}$$

$$s.t. \quad 0 \le p_j \le P_{\max}, \tag{18b}$$

$$0 < A_u < A_{\max}, \tag{18c}$$

where $P_{\max}$ is the maximum transmit power of Jam, and $A_{\max}$ is the highest operating height of UAV.

III. CSI-Aware Monitoring

In this section, we investigate the CSI-aware monitoring scheme, where $\mathbf{H}_{je}$ is accurately estimated with the help of communication between Eve and Jam.

Due to the lack of channel information about Jam-Bob link, the optimal jamming signal should lie in the null space of $\mathbf{H}_{je}$ to minimize the adverse effect of jamming signal on monitoring performance. Therefore, $\mathbf{w}_1 \in \mathbb{C}^{N_j \times (N_j - N_e)}$ satisfying $\mathbf{H}_{je}\mathbf{w}_1 = \mathbf{0}$ is designed, and the SINR at Eve can be simplified as

$$\gamma_e = \widetilde{\gamma}_{ae}\|\mathbf{h}_{ae}\|^2. \tag{19}$$

A. Performance Analysis

We now present the performance analysis of the CSI-aware monitoring scheme. Firstly, we give out the closed-form expression for the transmission outage probability of the suspicious transmission pair when jammer UAV transmits with the beamformer $\mathbf{w}_1$.

Based on (13), transmission outage probability can be reexpressed as

$$\begin{aligned} p_{to} &= \Pr\left(\frac{\widetilde{\gamma}_{ab}|h_{ab}|^2}{\widetilde{\gamma}_{jb}|\mathbf{h}_{jb}\mathbf{w}_1|^2 + 1} < \gamma_0\right) \\ &= \int_0^{\infty}\int_0^{\gamma_0 y + \gamma_0} f_{\gamma_{ab}}(x)\, f_{\gamma_{jb}}(y)\, dxdy, \end{aligned} \tag{20}$$

where $f_{\gamma_{ab}}(\cdot)$ and $f_{\gamma_{jb}}(\cdot)$ represent the probability density function (PDF) of $\widetilde{\gamma}_{ab}|h_{ab}|^2$ and $\widetilde{\gamma}_{jb}|\mathbf{h}_{jb}\mathbf{w}_1|^2$, respectively.

Due to the fact that the generation of $\mathbf{w}_1$ is independent of $\mathbf{h}_{jb}$, $\mathbf{h}_{jb}\mathbf{w}_1$ has the same distribution as $\mathbf{h}_{jb}$. Therefore, the entries of $\mathbf{h}_{jb}\mathbf{w}_1$ are i.i.d complex Gaussian random variables and $\widetilde{\gamma}_{jb}|\mathbf{h}_{jb}\mathbf{w}_1|^2$ follows a Gamma distribution $\mathcal{G}\left(N_j - N_e, \widetilde{\gamma}_{jb}\lambda_{jb}\right)$, where $N_j - N_e$ and $\widetilde{\gamma}_{jb}\lambda_{jb}$ represent the shape parameter and scale parameter, respectively. With the help of [16], the exact expression of p_{to} is derived as

$$p_{to} = 1 - e^{-\frac{\gamma_0}{\widetilde{\gamma}_{ab}\lambda_{ab}}}\left(\frac{\widetilde{\gamma}_{ab}\lambda_{ab}}{\widetilde{\gamma}_{jb}\lambda_{jb}\gamma_0 + \widetilde{\gamma}_{ab}\lambda_{ab}}\right)^{N_j - N_e}. \tag{21}$$

Accordingly, the maximum suspicious communication rate that guarantees the transmission outage probability requirement (16) can be obtained, which has been shown in (22). Here, $\mathcal{W}$ denotes the Lambert W function of x with $\mathcal{W}(x)\, e^{\mathcal{W}(x)} = x$ [17].

Moreover, the eavesdropping outage probability can be expressed as

$$p_{eo} = \frac{P_E^L \cdot \gamma\left(N_e\widetilde{m}_{ae}, \frac{\widetilde{m}_{ae}\gamma_0}{\widetilde{\gamma}_{ae}^{L}}\right)}{\Gamma\left(N_e\widetilde{m}_{ae}\right)} + \frac{\left(1 - P_E^L\right) \cdot \gamma\left(N_e, \frac{\gamma_0}{\widetilde{\gamma}_{ae}^{NL}\lambda_{ae}}\right)}{\Gamma\left(N_e\right)}, \tag{23}$$

where $\widetilde{m}_{ae} = \frac{(K_{ae}+1)^2}{2K_{ae}+1}$, $\Gamma(\cdot)$ is the Gamma function [18, eq. (8.310)], given by $\Gamma(z) = \int_0^{\infty}\exp(-t)t^{z-1}dt$, and $\gamma(\cdot,\cdot)$ is the lower incomplete gamma function, given by [18, eq. (8.350)] $\gamma(\mu,\nu) = \int_0^{\nu}\exp(-t)t^{\mu-1}dt$.

$$R_s = \frac{\widetilde{\gamma}_{ab}\lambda_{ab}}{\widetilde{\gamma}_{jb}\lambda_{jb}}\left(-1+\widetilde{\gamma}_{jb}\lambda_{jb}\left(N_j-N_e\right)\mathcal{W}\left(e^{\frac{1}{\widetilde{\gamma}_{jb}\lambda_{jb}\left(N_j-N_e\right)}+\frac{i\pi}{\left(N_j-N_e\right)}}\left(-1+\delta_0\right)^{-\frac{1}{\left(N_j-N_e\right)}}\right)\right). \tag{22}$$

Proof. Since the Alice-Eve link experiences Rician fading and Rayleigh fading with different probabilities, eavesdropping outage probability can be mathematically expressed as

$$p_{eo} = P_E^L F_{\gamma_{ae}^L}\left(\gamma_0\right) + \left(1-P_E^L\right) F_{\gamma_{ae}^{NL}}\left(\gamma_0\right), \tag{24}$$

where $F_{\gamma_{ae}^L}(\cdot)$ denotes the cumulative distribution function (CDF) of $\widetilde{\gamma}_{ae}^L\|\mathbf{h}_{ae}\|^2$ when Alice-Eve link experiences Rician fading, and $F_{\widetilde{\gamma}_{ae}^{NL}\|\mathbf{h}_{ae}\|^2}(\cdot)$ denotes the CDF of $\widetilde{\gamma}_{ae}^{NL}\|\mathbf{h}_{ae}\|^2$ when Alice-Eve link experiences Rayleigh fading. As such, the exact expression of p_{eo} is investigated from the following two cases.

When the Alice-Eve link experiences Rician fading, with the help of [19], the PDF of $\widetilde{\gamma}_{ae}^L\|\mathbf{h}_{ae}\|^2$ is given by

$$f_{\gamma_{ae}^L}\left(x\right) = \left(\frac{\widetilde{m}_{ae}}{\widetilde{\gamma}_{ae}^L}\right)^{N_e\widetilde{m}_{ae}} \frac{x^{N_e\widetilde{m}_{ae}-1}}{\Gamma\left(N_e\widetilde{m}_{ae}\right)} \exp\left(-\frac{\widetilde{m}_{ae}x}{\widetilde{\gamma}_{ae}^L}\right), \tag{25}$$

and the CDF of $\widetilde{\gamma}_{ae}^L\|\mathbf{h}_{ae}\|^2$ is then obtained, given by

$$F_{\gamma_{ae}^L}\left(x\right) = \frac{\gamma\left(N_e\widetilde{m}_{ae}, \frac{\widetilde{m}_{ae}x}{\widetilde{\gamma}_{ae}^L}\right)}{\Gamma\left(N_e\widetilde{m}_{ae}\right)}. \tag{26}$$

When the Alice-Eve link experiences Rayleigh fading, $\widetilde{\gamma}_{ae}^{NL}\|\mathbf{h}_{ae}\|^2$ follows a Gamma distribution $\mathcal{G}\left(N_e, \widetilde{\gamma}_{ae}^{NL}\lambda_{ae}\right)$. As a result, the PDF and CDF of $\widetilde{\gamma}_e^{NL}\|\mathbf{h}_{ae}\|^2$ can be respectively expressed as

$$f_{\gamma_{ae}^{NL}}\left(x\right) = \frac{x^{N_e-1}\exp\left(-\frac{x}{\widetilde{\gamma}_{ae}^{NL}\lambda_{ae}}\right)}{\Gamma\left(N_e\right)\left(\widetilde{\gamma}_{ae}^{NL}\lambda_{ae}\right)^{N_e}}, \tag{27}$$

and

$$F_{\gamma_{ae}^{NL}}\left(x\right) = \frac{\gamma\left(N_e, \frac{x}{\widetilde{\gamma}_{ae}^{NL}\lambda_{ae}}\right)}{\Gamma\left(N_e\right)}. \tag{28}$$

Substituting (26) and (28) into (24), (23) can be obtained. The proof is completed. □

B. Optimization

Based on the above analysis, the eavesdropping performance can be optimized by properly selecting flying height A_u and jamming power p_j. In particular, the effect of A_u and p_j on the average eavesdropping rate can be summarized as follows.

Remark 1. *Due to the path loss of Alice-Eve link, the received signal strength at UAV will decrease as the increase of flying height. In addition, small flying height will result in NLoS propagation with high probability, which deteriorates the monitoring performance. As a result, the proper selection of flying height A_u will be helpful to improve the eavesdropping non-outage probability $(1-p_{eo})$.*

Remark 2. *R_s increases monotonically as the decrease of p_j. However, given a flying height A_u, larger R_s would make information eavesdropping more difficult, which deteriorates the eavesdropping non-outage probability $(1-p_{eo})$. To maximize the average eavesdropping rate, jamming power p_j should be designed properly.*

To be noticed, due to the lack of information about Bob, $\widetilde{\gamma}_B$, λ_{ab}, $\widetilde{\gamma}_J$, λ_{jb} and δ_0 are hard to obtain in practical. However, with the help of spectrum sensing techniques, the transmission rate of the suspicious link can be accurately estimated [20]. Accordingly, to maximize the eavesdropping performance, **Algorithm** 1 can be performed to find the optimal A_u^*, which has been detailed as follows.

Algorithm 1 Algorithm to determine the optimal flying height A_u^*

1: **for** every $A_u \in [A_{\min}, A_{\max}]$ with step size ΔA_u **do**
2: Sense the transmission rate R_s and calculate p_{eo} using (23).
3: Calculate the average eavesdropping rate using (17).
4: Find the maximal average eavesdropping rate of current flying height.
5: **end for**
6: Set the flying height corresponding to the maximum R_{ave}^* as A_u^*.

IV. Numerical Results

In this section, we present numerical results to validate the effectiveness of our considered UAV-assisted legitimate wireless surveillance scheme. Specifically, we first demonstrate the accuracy of our derived closed-form expression for the eavesdropping non-outage probability. Then, we examine the impact of A_u on the monitoring performance. Throughout this section, we consider that $K = 10$ dB, $\varphi = 11.95$, $\beta = 0.14$ [12].

To show the accuracy of the derived performance, Fig.2 is presented. Obviously, the analytical results obtained from (28) and (26) match closely with the simulations results, which verifies the accuracy of our derived closed-form expression of eavesdropping outage probability. In addition, it can be observed that the eavesdropping outage probability in the situation of Rayleigh fading is much higher than that in the situation of Rician fading, which is due to the fact that the line-of-sight (LoS) in Rician channel is helpful to monitor the suspicious link. However, to obtain the LoS, the UAV is required to fly higher, which will reduce the received signal power, thus decreasing the average eavesdropping rate. As a result, the flying height should be well designed to obtain a better surveillance performance.

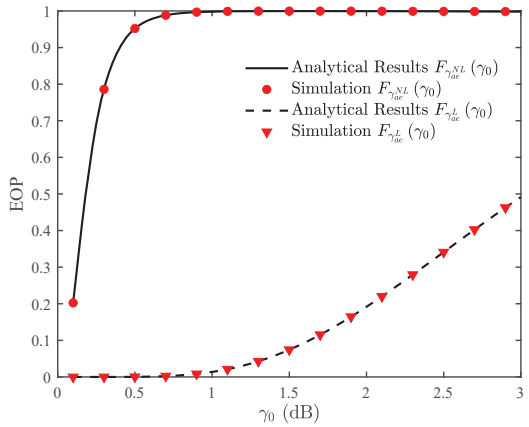

Fig. 2. Eavesdropping outage probability.

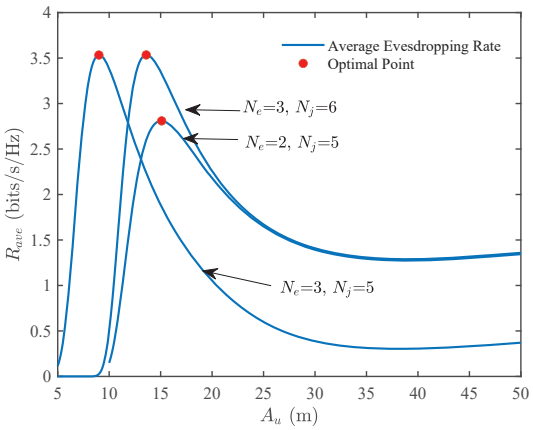

Fig. 3. Average eavesdropping rate versus flying height with different antenna configurations.

In Fig.3, we show the average eavesdropping rate versus flying height with different antenna configurations. As the flying height A_u increases, the achievable average eavesdropping rate first increase and then decreases, which indicates that there exists a flying height with respect to the optimal surveillance performance. In addition, since the monitoring ability can be enhance when more antennas are deployed at the legitimate monitor UAV, a better surveillance performance can be obtained with lager N_e. Besides, due to the jamming ability is determined by the number of antenna at jammer UAV, the optimal flying height, as well as the surveillance performance, changes as N_j varies.

V. Conclusion

In this paper, we investigates the UAV-assisted legitimate wireless surveillance, where a legitimate monitor UAV and a jammer UAV are deployed to monitor the suspicious terrestrial transmission. Considering the channel state information aware case, the monitoring performance in terms of average eavesdropping rate is derived, where both the closed-form expressions of maximum suspicious communication and eavesdropping non-outage probability are obtained. Then, based on the derived expressions, the flying height corresponding to the maximum average eavesdropping rate can be obtained. The simulation results verifies the accuracy of our derived expressions and the effectiveness of our considered UAV-assisted legitimate wireless surveillance scheme.

References

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

[2] H. Zhang, L. Duan and R. Zhang, "Jamming-assisted proactive eavesdropping over two suspicious communication links", *IEEE Trans. Wireless Commun.*, vol. 19, no. 7, pp. 4817– 4830, Jul. 2020.

[3] D. Xu and H. Zhu, "Spectrum sharing incentive for legitimate wireless information surveillance", *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2529–2543, Mar. 2021.

[4] C. Zhong, X. Jiang, F. Qu and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, Jul. 2017.

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

[6] F. Feizi, M. Mohammadi, Z. Mobini and C. Tellambura, "Proactive eavesdropping via jamming in full-duplex multi-antenna systems: Beamforming design and antenna selection", *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7563–7577, Dec. 2020.

[7] J. Moon, H. Lee, C. Song, S. Kang and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing", *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6958–6971, Oct. 2018.

[8] L. Sun, et al., "Alternate-jamming-aided wireless physical-layer surveillance: Protocol design and performance analysis", *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1989-2003, 2021.

[9] G. Hu, Y. Cai and Y. Cai, "Joint optimization of position and jamming power for UAV-aided proactive eavesdropping over multiple suspicious communication links", *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2093–2097, Dec. 2020.

[10] J. Xu, L. Duan and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading Channels", *IEEE Wireless Commun. Lett.*, vol. 5,no. 1, pp. 80–83, Feb. 2016.

[11] Y. Zeng, Q. Wu and R. Zhang, "Accessing from the sky: A tutorial on UAV communications for 5G and beyond", *Proc. IEEE*, vol. 107, no.'12, pp. 2327–2375, Dec. 2019.

[12] C. Liu, J. Lee and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper", *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 2919–2931, Jun. 2019.

[13] J.-A. Tsai, R. M. Buehrer, and B. D. Woerner, "BER performance of a uniform circular array versus a uniform linear array in a mobile radio environment", *IEEE Trans. Wireless Commun.*, vol. 3, no. 3, pp. 695–700, May 2004.

[14] S. Yan and R. Malaney, "Location-based beamforming for enhancing secrecy in rician wiretap channels", *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 2780–2791, Apr. 2016.

[15] M. Yang, B. Zhang, Y. Huang, N. Yang, D. B. da Costa and D. Guo, "Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise", *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11394–11398, Dec. 2017.

[16] Y. Bi and H. Chen, "Accumulate and jam: Towards secure communication via a wireless-powered full-duplex jammer,", *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1538–1550, Dec. 2016.

[17] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the Lambert W Functionr,", *Adv. Comput. Math.*, vol. 5, no. 4, pp. 329–359, 1996.

[18] I. S. Gradshteyn and I. M. Ryzhik, *Tabel of Integrals, Series, and Products,* 7th ed. New York, NY, USA: Academic, 2007.

[19] A. Goldsmith, *Wireless Communication.* Cambridge, U.K.: Cambridge Univ. Press, 2005.

[20] J. Schreck, P. Jung and S. Stańczak, "Compressive rate estimation with applications to device-to-device communications", *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 7001–7012, Oct. 2018.