Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5565213, 14 pages
https://doi.org/10.1155/2021/5565213

Research Article

Full-Duplex UAV Legitimate Surveillance System against a Suspicious Source with Artificial Noise

Shen Yi,[1] **Pan Zhiwen**,[2,3] **Liu Nan**,[2] **and You Xiaohu**[2,3]

[1]*School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu 210096, China*
[2]*National Mobile Communications Research Laboratory, Southeast University, Nanjing, Jiangsu 210096, China*
[3]*Purple Mountain Laboratories, Nanjing, Jiangsu 211100, China*

Correspondence should be addressed to Pan Zhiwen; pzw@seu.edu.cn

Received 11 January 2021; Revised 5 April 2021; Accepted 15 April 2021; Published 12 May 2021

Academic Editor: Laurie Cuthbert

We propose a legal full-duplex unmanned aerial vehicle (UAV) surveillance system in the presence of the ground-to-ground suspicious link with antisurveillance technology. UAV performs passive surveillance and active jamming simultaneously, and the suspicious source with multiantenna employs artificial noise to avoid being monitored. In order to ensure effective surveilling, we adopt two beamforming schemes, namely, maximum ratio transmission (MRT)/receiving zero-forcing (RZF) and transmitting zero-forcing (TZF)/maximum ratio combing (MRC), for MIMO UAV. For the two beamforming schemes, we derive the surveilling nonoutage probability in a closed-form expression and analyze the surveilling performance under different system environments. Monte Carlo (MC) simulation validates the correctness of the formula.

1. Introduction

Public safety is becoming more and more important. Illegal nodes transmit suspicious information to conduct actions that endanger public safety, such as illegal crimes and terrorist attacks. Public security agencies can use wireless monitoring equipment to surveil suspicious communication links. Wireless monitoring equipment consists of two categories: ground monitors and unmanned aerial vehicle (UAV) monitors.

The study of ground monitors has been considered in [1–4]. In order to ensure effective surveilling, the authors in [1, 2] propose a legitimate surveilling system in the presence of a suspicious link, where the ground monitor performs proactive surveilling via cognitive jamming. A new proactive surveilling approach, namely, spoofing relay, is proposed in [3] to enhance the surveilling performance. For successful surveilling, the authors in [4] make use of full-duplex technology with self-interference cancellation and multi-antenna technology to increase the surveilling channel quality and reduce the suspicious transmission rate.

Due to on demand deployment and flexible mobility, UAVs can be involved in wireless communication scenes including UAV legitimate terminals [5–7], UAV base station [8–10], UAV friendly jamming [11–13], and UAV friendly relays [14, 15].UAV can pretend a legitimate node that communicates with other nodes, and the existence of UAV does not draw attention from suspicious links.

Due to the relatively high operation altitude, UAVs have a dominant line-of-sight (LoS) commutation channel compared to the ground monitors. As such, compared to ground-to-ground surveillance link with severe fading, the UAV-to-ground surveilling link provides an advantageous communication channel. Furthermore, UAVs can use spatial freedom to obtain the best surveillance performance. UAV monitor has been considered in [16–19]. Authors in [16] investigate a legal UAV monitoring system in the presence of suspicious UAV pairs, where the legal UAV's trajectory is limited by energy. Authors in [17] propose a legitimate UAV surveilling scenario in the presence of a ground-to-ground suspicious relay network, where the suspicious source can only communicate with the suspicious destination

through the suspicious relay. Multiple cooperated UAV surveilling scenario in the presence of a ground-to-ground suspicious relay network with multiple relays where all nodes operate in half-duplex mode is proposed in [18]. Authors in [19] consider two surveilling schemes, namely, proactive surveilling and spoofing relaying, in the UAV surveilling system. However, all above literatures [16–19] assume that the suspicious link is passive, and no antisurveillance technology is adopted to avoid being monitored.

Suspicious nodes have become more and more cunning, and the suspicious source can use artificial noise to avoid being monitored. Artificial noise has been studied in [20–23]. In [20], the authors propose a secure transmission system in which the legitimate source transmits useful information to the legitimate destination in the presence of an eavesdropper. The legal source can use artificial noise to avoid being eavesdropped. Authors in [21] further consider a secure transmission system in the presence of multiple eavesdroppers operating in both noncollusion and collusion modes. In [22], the authors consider a secure transmission system based on [20]. The difference is that [20] knows the statistical characteristics of the eavesdropping channel state information (CSI), while [22] does not know the eavesdropping channel CSI. In [23], the authors further extend the secure transmission system of [22], and the assumption of the system environment changes from knowing the statistical characteristics of the eavesdropping channel CSI to not knowing the eavesdropping CSI channel. However, in the above literatures [20–23], they all stand from the perspective of legitimate nodes, not from the perspective of suspicious nodes, and artificial noise has not been adopted by the suspicious source.

Full-duplex technology has been considered in [24–26]. In [24], the authors propose a beam-domain full-duplex massive MIMO to enable co-time co-frequency uplink and downlink transmission in the cellular system. In [25], the authors consider the benefits, feasibility, and limitations of inband full-duplex massive MIMO in the cellular system. In [26], the authors consider the hybrid time switching and power splitting simultaneous wireless information and power transfer protocol design in a full-duplex massive MIMO system to maximize system achievable sum rate. Therefore, full-duplex technology can be used in the surveillance system to enhance the surveilling performance.

Based on the above investigations, in this paper, we propose a legal full-duplex UAV surveillance system in the presence of a ground-to-ground suspicious communication link with antisurveillance technology. UAV monitor operates in full-duplex mode, where passive surveilling aims to receive the suspicious information from the dubious source, and active jamming aims to reduce the channel capacity of the suspicious link, thus degrading the ability of the dubious source to transmit suspicious messages to the dubious destination. By using antisurveillance technology, the suspicious source with multiantenna employs artificial noise to avoid being monitored. Without loss of generality, LoS link with a certain probability is the most suitable for the UAV-to-ground channel model. We adopt the nonoutage probability to evaluate the surveilling performance of UAV monitor.

The main contributions of this paper are summarized as follows:

We propose a full-duplex UAV monitor scheme based on [27], where the suspicious source adopts a single antenna without artificial noise, while in this paper, the suspicious source with multi-antenna employs artificial noise to avoid being monitored.

In order to improve surveilling performance, two low-complexity linear beamforming schemes, maximum ratio transmission (MRT)/receiving zero-forcing (RZF), and transmitting zero-forcing (TZF)/maximum ratio combing (MRC) are adopted for MIMO UAV. Furthermore, we derive the probability of surveilling non-outage in a closed-form expression.

For various UAV surveilling environments, the optimal angle/radius/height to maximize the surveilling nonoutage probability is determined. The impact of the artificial noise power ratio in the suspicious source, the distance between the suspicious source, and the suspicious destination, as well as the transmitting power of the suspicious source and UAV on the surveilling non-outage probability, is analyzed. For different heights of UAV, configuration of the receiving antennas and transmitting antennas with fixed total number of antennas that maximizes the surveilling nonoutage probability of the UAV monitor is explored for two beamforming schemes.

The optimal power ratio of artificial noise at the suspicious source which minimizes the surveilling non-outage probability is determined. When the power ratio of artificial noise of the suspicious source is unknown, the UAV surveillance system can be designed with reference to the worst case while ensuring surveillance performance.

Notations: $\mathcal{CN}$ denotes the complex Gaussian distribution. $(\cdot)^H$ denotes the conjugate transpose. $|\cdot|$ denotes the absolute value. $\|\cdot\|$ denotes the Frobenius norm of the matrix or vector.

2. System Model and Problem Formulation

The UAV legitimate surveillance system is shown in Figure 1, where a suspicious ground source (S) transmits suspicious messages to a suspicious ground destination (D), and this suspicious communication link is surveilled by a full-duplex UAV legitimate monitor (M). However, the suspicious source with multi-antenna adopts artificial noise to avoid being monitored.

Under a full-duplex mode, UAV performs passive surveillance and active jamming simultaneously. Suppose that the number of UAV receiving antennas used for surveilling is N_r and the number of UAV transmitting antennas used for jamming is N_t, while the suspicious source has N_S transmitting antennas and the suspicious destination has a single receiving antenna. In three-dimensional Cartesian coordinate system, S, D, and M are located at $(g, 0, 0)$, $(-g, 0, 0)$, and $(r\cos\theta_a, r\sin\theta_a, v)$, respectively, where the half separation between suspicious nodes is denoted by g, UAV circle radius r is in the range of 0 to $r^{\max}$, UAV azimuth angle θ_a

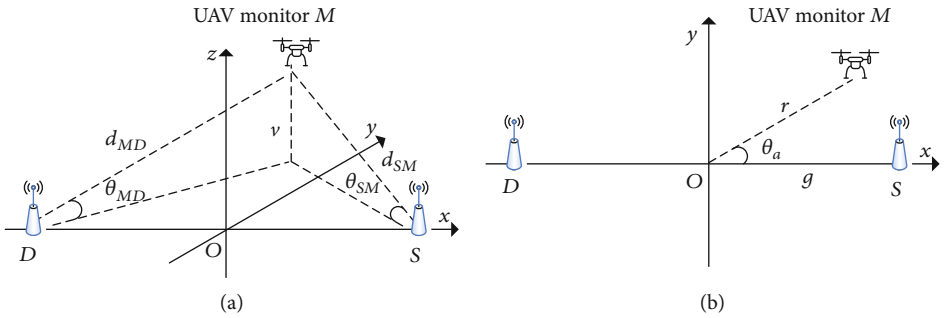

FIGURE 1: (a). System model with 3-D view. (b). System model with top view.

is in the range of 0 to 2π, and UAV altitude v is in the range of 0 to $v^{\max}$. As in [1, 28], UAV knows all channel state information (CSI), while the suspicious nodes only know their own CSI.

We denote $\mathbf{H}_{SM}$, $\mathbf{h}_{MD}$, and $\mathbf{h}_{SD}$ as the $N_r \times N_s$ channel matrix from the suspicious source to UAV, the $1 \times N_t$ channel vector from UAV to the suspicious destination, and the $1 \times N_s$ channel vector from the suspicious source to the suspicious destination, respectively. Model S-D channel as $\sqrt{\beta_1}\mathbf{h}_{SD}/\sqrt{d_{SD}^4}$, where the ground-to-ground channel power gain at a reference distance of 1 m, is denoted by β_1, $\mathbf{h}_{SD}$ represents a Rayleigh fading with entries being independent and identically distributed (i.i.d.) zero-mean circular symmetric complex Gaussian (ZMCSCG) random variable with variance λ_1, and d_{SD} denotes the distances between S and D. Model the self-interference channel as $\sqrt{\rho}\mathbf{H}_{MM}$ [29], where $\mathbf{H}_{MM}$ denotes a Rayleigh channel with entries being i.i.d. ZMCSCG with variance λ_2, and self-interference coefficient ρ is in the range of $0 \le \rho \le 1$.

Due to the high operating altitude of UAV, the UAV-to-ground channels typically have a high probability of LoS link [30] as

$$p_{r\mathrm{LOS}}(\theta_i) = \left(1 + \delta_1 e^{-\delta_2 \theta_i}\right)^{-1}, \tag{1}$$

where δ_1 and δ_2 are constant values determined by the environment, $\theta_i, i \in \{\mathrm{SM}, \mathrm{MD}\}$ is the elevation angle, and

$$\theta_i = \arcsin\left(\frac{v}{d_i}\right), i \in \{\mathrm{SM}, \mathrm{MD}\}, \tag{2}$$

where the distance between S and M is denoted by d_{SM}, and the distance between M and D is denoted by d_{MD}, which can be, respectively, given by

$$\begin{aligned} d_{SM} &= \left(g^2 + r^2 + v^2 - 2gr\cos\theta_a\right)^{1/2}, \\ d_{MD} &= \left(g^2 + r^2 + v^2 + 2gr\cos\theta_a\right)^{1/2}. \end{aligned} \tag{3}$$

Note that the LoS probability in (1) increases as the elevation angle $\theta_i, i \in \{\mathrm{SM}, \mathrm{MD}\}$ increases.

From [31], we model the UAV-to-ground channel as a Rice fading channel, and the Rice factor and path loss exponent are associated with the elevation angle and environment.

We then express the Rician factor between S (or D) and M as $K_i = \alpha_3 e^{\delta_3 \theta_i}, i \in \{SM, MD\}$ and the path loss exponent as $\tau_i = \alpha_1 p_{r\mathrm{LOS}}(\theta_i) + \alpha_2, i \in \{SM, MD\}$, where α_1, α_2, α_3, and δ_3 are constants related to frequency and environment. Therefore, we model the S-M channel as $\sqrt{\beta_2}\mathbf{H}_i/\sqrt{d_i^{\tau_i}}, i \in \{SM\}$ [28], where the UAV-to-ground channel power gain at a reference distance of 1 m is denoted by β_2, and $\mathbf{H}_i$ represents the small-scale fading of the UAV-to-ground channel, which can be expressed as

$$\mathbf{H}_i = \sqrt{\frac{K_i}{K_i + 1}}\bar{\mathbf{H}}_i + \sqrt{\frac{1}{K_i + 1}}\tilde{\mathbf{H}}_i, i \in \{SM\}, \tag{4}$$

where $\bar{\mathbf{H}}_{SM}$ is the deterministic LoS component of the channel between the suspicious source and UAV satisfying $\mathrm{trace}(\bar{\mathbf{H}}_{SM}\bar{\mathbf{H}}_{SM}^{\dagger}) = N_r N_s$. $\tilde{\mathbf{H}}_{SM} \in \mathbb{C}^{N_r \times N_s}$ denotes the scattered component of the channel between the suspicious source and UAV with entries being i.i.d. ZMCSCG random variable with unit variance.

Further, we model the M-D channel as $\sqrt{\beta_2}\mathbf{h}_i/\sqrt{d_i^{\tau_i}}, i \in \{MD\}$ [28], where $\mathbf{h}_i$ represents the small-scale fading in the air, which is given by

$$\mathbf{h}_i = \sqrt{\frac{K_i}{K_i + 1}}\bar{\mathbf{h}}_i + \sqrt{\frac{1}{K_i + 1}}\tilde{\mathbf{h}}_i, i \in \{MD\}, \tag{5}$$

where $\bar{\mathbf{h}}_{MD}$ is the deterministic LoS components of the channel between the suspicious destination and UAV satisfying $\mathrm{trace}(\bar{\mathbf{h}}_{MD}\bar{\mathbf{h}}_{MD}^{\dagger}) = N_t$. $\tilde{\mathbf{h}}_{MD} \in \mathbb{C}^{1 \times N_t}$ denotes the scattered components of the channel between the suspicious destination and UAV with entries being i.i.d. ZMCSCG random variable with unit variance.

The suspicious source is equipped with multiple antennas, where one antenna is used to transmit useful information, while the remaining antennas are used to send artificial noise signals [32]. The transmitting information of the suspicious source can be expressed as

$$\mathbf{x}_s = \mathbf{W}\mathbf{t}, \tag{6}$$

where $\mathbf{W}$ is the $N_s \times N_s$ beamforming matrix and can be expressed as

$$\mathbf{W} = [\mathbf{w}_s\, \mathbf{W}_a], \tag{7}$$

where $\mathbf{w}_s$ denotes the $N_s \times 1$ beamforming vector to maintain the receiving signal quality of the suspicious destination, and $\mathbf{w}_s = \mathbf{h}_{SD}^{\dagger}/\|\mathbf{h}_{SD}\|$. $\mathbf{W}_a$ denotes the $N_s \times (N_s - 1)$ beamforming matrix, which is used for transmitting artificial noise signal to avoid being monitored and will not affect the receiving signal quality of the suspicious destination, hence, $\mathbf{h}_{SD}\mathbf{W}_a = 0$. $\mathbf{t}$ composes of useful information and artificial noise signals and can be expressed by

$$\mathbf{t} = \begin{bmatrix} t_s \\ \mathbf{t}_a \end{bmatrix}, \tag{8}$$

where t_s is a useful information signal, and $\mathbf{t}_a$ is $(N_s - 1) \times 1$ artificial noise vector in the suspicious source. Define α_s with $0 \le \alpha_s \le 1$ as the power ratio allocated to the useful information signal. Therefore,

$$\begin{aligned} E\left[|t_s|^2\right] &= \alpha_s, \\ E\left[\mathbf{t}_a \mathbf{t}_a^{\dagger}\right] &= \frac{1 - \alpha_s}{N_s - 1}\mathbf{I}_{N_s - 1}. \end{aligned} \tag{9}$$

Hence, the signal received by UAV is given by

$$\mathbf{y}_M = \sqrt{\frac{P_s \beta_2}{d_{SM}^{\tau_{SM}}}}\mathbf{H}_{SM}(\mathbf{w}_s \mathrm{t}_s + \mathbf{W}_a \mathbf{t}_a) + \sqrt{\rho P_M}\mathbf{H}_{MM}\mathbf{w}_t x + \mathbf{n}_M, \tag{10}$$

where the transmitting power of the suspicious source is denoted by P_s, and UAV jamming power P_M is in the range of $0 \le P_M \le P_J$. In addition, UAV jamming symbol is x with unit power. Furthermore, $\mathbf{w}_t$ is the transmit beamforming vector at UAV monitor with $\|\mathbf{w}_t\| = 1$. Finally, $\mathbf{n}_M$ is additive white Gaussian noise (AWGN) at UAV, i.e., $\mathbf{n}_M \sim \mathcal{CN}(\mathbf{0}_{N_r \times 1}, \sigma_M^2 \mathbf{I}_{N_r})$.

Assume that UAV adopts a linear receiver $\mathbf{w}_r$ with $\|\mathbf{w}_r\| = 1$ for signal detection, hence, the output of the linear filter $\mathbf{w}_r$ is given by

$$\begin{aligned} \widetilde{\mathbf{y}_M} = \mathbf{w}_r^H \mathbf{y}_M &= \sqrt{\frac{P_s \beta_2}{d_{SM}^{\tau_{SM}}}}\mathbf{w}_r^H \mathbf{H}_{SM}(\mathbf{w}_s \mathrm{t}_s + \mathbf{W}_a \mathrm{t}_a) \\ &+ \sqrt{\rho P_M}\mathbf{w}_r^H \mathbf{H}_{MM}\mathbf{w}_t x + \mathbf{w}_r^H \mathbf{n}_M. \end{aligned} \tag{11}$$

Similarly, the receiving signal of the suspicious receiver D can be expressed as

$$y_D = \sqrt{\frac{P_s \beta_1}{d_{SD}^4}}\mathbf{h}_{SD}\mathbf{w}_s \mathrm{t}_s + \sqrt{\frac{P_M \beta_2}{d_{MD}^{\tau_{MD}}}}\mathbf{h}_{MD}\mathbf{w}_t x + n_D, \tag{12}$$

where n_D is the zero-mean AWGN at the suspicious destination node D with variance σ_D^2.

Therefore, the signal-to-interference-plus-noise ratio (SINR) of the suspicious destination node D can be expressed as

$$\mathrm{SINR}_D = \frac{\left(\alpha_s P_s \beta_1 / d_{SD}^4\right)|\mathbf{h}_{SD}\mathbf{w}_s|^2}{\left(P_M \beta_2 / d_{MD}^{\tau_{MD}}\right)|\mathbf{h}_{MD}\mathbf{w}_t|^2 + \sigma_D^2}, \tag{13}$$

and the SINR of UAV can be expressed as

$$\mathrm{SINR}_M = \frac{\alpha_s P_s \beta_2}{d_{SM}^{\tau_{SM}}}\mathbf{w}_s^H \mathbf{H}_{SM}^H \mathbf{w}_r \mathbf{R}^{-1} \mathbf{w}_r^H \mathbf{H}_{SM}\mathbf{w}_s, \tag{14}$$

where

$$\begin{aligned} \mathbf{R} = &\frac{P_s \beta_2 (1 - \alpha_s)}{d_{SM}^{\tau_{SM}}(N_s - 1)}\mathbf{w}_r^H \mathbf{H}_{SM}\mathbf{w}_a \mathbf{w}_a^H \mathbf{H}_{SM}^H \mathbf{w}_r \\ &+ \rho P_M \mathbf{w}_r^H \mathbf{H}_{MM}\mathbf{w}_t \mathbf{w}_t^H \mathbf{H}_{MM}^H \mathbf{w}_r + \sigma_M^2 \mathbf{I}_{N_r}. \end{aligned} \tag{15}$$

If $SINR_M \ge SINR_D$, the UAV surveillance system is successful, and suspicious messages can be decoded without error. If $SINR_M < SINR_D$, the UAV surveillance system fails, and suspicious messages cannot be decoded without error.

3. Performance Analysis

In order to improve the surveilling performance, two low-complexity linear beamforming schemes, maximum ratio transmission (MRT)/receiving zero-forcing (RZF), and transmitting zero-forcing (TZF)/maximum ratio combing (MRC) are adopted for MIMO UAV.

3.1. MRT/RZF. Aiming to completely eliminate self-interference, the multiantenna receiving end of the UAV monitor M adopts the RZF scheme.

According to [33], the compact form of $\mathbf{w}_r$ can be expressed as

$$\mathbf{w}_r = \frac{\Pi_2 \mathbf{H}_{SM}}{\|\Pi_2 \mathbf{H}_{SM}\|}, \tag{16}$$

where $\Pi_2 = \mathbf{I}_{N_r} - \mathbf{H}_{MM}\mathbf{h}_{MD}^{\dagger}\mathbf{h}_{MD}\mathbf{H}_{MM}^{\dagger}/\|\mathbf{H}_{MM}\mathbf{h}_{MD}^{\dagger}\|^2$ spans the null space of $\mathbf{H}_{MM}\mathbf{h}_{MD}^{\dagger}$.

Furthermore, the MRT scheme is adopted by the transmitting antennas of UAV monitor M for jamming the suspicious destination, i.e.,

$$\mathbf{w}_t = \frac{\mathbf{h}_{MD}^{\dagger}}{\|\mathbf{h}_{MD}\|}. \tag{17}$$

Since UAV completely eliminates its self-interference [4], active jamming has no effect on the UAV signal receiving end. Consequently, UAV can use the full power P_J for jamming the suspicious destination.

The probability of UAV surveilling non-outage with TZF/MRC scheme is given by (39).

Define

$$\gamma_{SD} = \frac{\alpha_s P_s \beta_1}{d_{SD}^4} |\mathbf{h}_{SD}\mathbf{w}_s|^2. \qquad (18)$$
$$\gamma_{MD} = |\mathbf{h}_{MD}\mathbf{w}_t|^2.$$

Then, it is obvious that γ_{SD} follows the central chi-squared distribution with $2N_S(N_S-1)$ degrees of freedom, with CDF (cumulative distribution function) given by [34]

$$F_{SD}(x) = 1 - \exp\left(-\frac{x}{\psi_{SD}}\right) \times \sum_{p=1}^{N_S} \frac{1}{\Gamma(p)} \left(\frac{x}{\psi_{SD}}\right)^{p-1}, \qquad (19)$$

where

$$\psi_{SD} = \frac{\alpha_s P_S \beta_1}{d_{SD}^4}. \qquad (20)$$

In addition, the PDF (probability density function) of γ_{MD} is given by [28]

$$f_{MD}(x) = (K_{MD}+1)e^{-((K_{MD}+1)x+K_{MD}N_t)} \times \left(\frac{(K_{MD}+1)x}{K_{MD}N_t}\right)^{\frac{N_t-1}{2}} \times \mathrm{I}_{N_t-1}\left(2\sqrt{(K_{MD}+1)K_{MD}N_t x}\right). \qquad (21)$$

As such, the probability of surveilling non-outage can be written as

$$\mathrm{P}_{\mathrm{nonout}} = \mathrm{Prob}\left(\mathrm{SINR}_M \geq \frac{\left(\alpha_s P_s \beta_1 / d_{SD}^4\right)|\mathbf{h}_{SD}\mathbf{w}_s|^2}{\left(P_M \beta_2 / d_{MD}^{\tau_{MD}}\right)|\mathbf{h}_{MD}\mathbf{w}_t|^2 + \sigma_D^2}\right). \qquad (22)$$

Conditioning on γ_{SD}, we obtain

$$\mathrm{P}_{\mathrm{nonout}} = 1 - \exp\left(-\frac{\left(\left(P_M \beta_2 / d_{MD}^{\tau_{MD}}\right)|\mathbf{h}_{MD}\mathbf{w}_t|^2 + \sigma_D^2\right)\mathrm{SINR}_M}{\psi_{SD}}\right) \times \sum_{p_1=1}^{N_S} \frac{1}{\Gamma(p_1)} \left(\frac{\left(\left(P_M \beta_2 / d_{MD}^{\tau_{MD}}\right)|\mathbf{h}_{MD}\mathbf{w}_t|^2 + \sigma_D^2\right)\mathrm{SINR}_M}{\psi_{SD}}\right)^{p_1-1}. \qquad (23)$$

Averaging over γ_{MD} and with the help of [35], we have the desired result.

$$\mathrm{P}_{\mathrm{nonout}} = 1 - (K_{MD}+1)^{N_t} \exp\left(-K_{MD}N_t - b_1 c_1\right) \cdot \sum_{p_1=1}^{N_S} \frac{1}{\Gamma(p_1)} (a_1 c_1)^{p_1-1} \sum_{\nu_1=0}^{p_1-1} \binom{\nu_1}{p_1-1} \left(\frac{b_1}{a_1}\right)^{p_1-1-\nu_1} \times \sum_{i_1=0}^{\infty} \frac{(K_{MD}N_t(K_{MD}+1))^i \Gamma(N_t+\nu_1+i_1)}{(a_1 c_1 + K_{MD}+1)^{N_t+\nu+i} \Gamma(i_1+1)\Gamma(N_t+i_1)}, \qquad (24)$$

where

$$a_1 = \frac{P_M \beta_2}{d_{MD}^{\tau_{MD}}}$$
$$\mathrm{b}_1 = \sigma_D^2 \qquad (25)$$
$$c_1 = \frac{SINR_M}{\psi_{SD}}.$$

As such, $SINR_M$ can be written as

$$SINR_M = \frac{z_1}{w z_2 + \sigma_M^2}, \qquad (26)$$

where

$$w = \frac{P_s \beta_2 (1-\alpha_s)}{d_{SM}^{\tau_{SM}}(N_s-1)}. \qquad (27)$$

Define

$$z_1 = \frac{\alpha_s P_s \beta_2}{d_{SM}^{\tau_{SM}}} \mathbf{w}_r^H \mathbf{H}_{SM} \mathbf{w}_s \mathbf{w}_s^H \mathbf{H}_{SM}^H \mathbf{w}_r. \qquad (28)$$
$$z_2 = \mathbf{w}_r^H \mathbf{H}_{SM} \mathbf{w}_a \mathbf{w}_a^H \mathbf{H}_{SM}^H \mathbf{w}_r,$$

Then, it is obvious that z_1 follows the central chi-squared distribution with $2(N_r-1)$ degrees of freedom, with CDF given by [34]

$$F(z_1) = 1 - \exp\left(-\frac{z_1}{\phi_{z_1}}\right) \times \sum_{p_2=1}^{N_r-1} \frac{1}{\Gamma(p_2)} \left(\frac{z_1}{\phi_{z_1}}\right)^{p_2-1}, \qquad (29)$$

where

$$\phi_{z_1} = \frac{2\alpha_s P_s \beta_2 N_s}{d_{SM}^{\tau_{SM}}(K_{SM}+1)}. \qquad (30)$$

Then, it is obvious that γ_{SD} follows the central chi-squared distribution with $2N_S$ degrees of freedom [28], and the pdf of z_2 is given by

$$f_{z_2}(x) = (K_{SM}+1)e^{-((K_{SM}+1)x+K_{SM}(N_s-1)N_s)} \times \left(\frac{(K_{SM}+1)x}{K_{SM}(N_s-1)N_s}\right)^{\frac{(N_s-1)N_s-1}{2}} \times \mathrm{I}_{(N_s-1)N_s-1}\left(2\sqrt{(K_{SM}+1)K_{SM}(N_s-1)N_s x}\right). \tag{31}$$

Conditioning on z_1, we obtain the CDF of $SINR_M$ as

$$F_T = 1-\exp\left(-\frac{SINR_M\left(wz_2+\sigma_M^2\right)}{\phi_{z_1}}\right) \times \sum_{p_2=1}^{N_r-1}\frac{1}{\Gamma(p_2)}\left(\frac{SINR_M\left(wz_2+\sigma_M^2\right)}{\phi_{z_1}}\right)^{p_2-1}. \tag{32}$$

Averaging over z_2 and with the help of [35], we have the desired result.

$$F_T = 1-(K_{SM}+1)^{(N_s-1)N_s}\exp\left(-K_{SM}(N_s-1)N_s-b_2c_2\right) \times \sum_{p_2=1}^{N_r-1}\frac{1}{\Gamma(p_2)}(a_2c_2)^{p_2-1}\sum_{\nu_2=0}^{p_2-1}\binom{\nu_2}{p_2-1}\left(\frac{b_2}{a_2}\right)^{p_2-1-\nu_2} \times \sum_{i_2=0}^{\infty}\frac{(K_{SM}(K_{SM}+1)(N_s-1)N_s)^{i_2}\Gamma((N_s-1)N_s+\nu_2+i_2)}{(a_2c_2+K_{SM}+1)^{(N_s-1)N_s+\nu_2+i_2}\Gamma(i_2+1)\Gamma((N_s-1)N_s+i_2)}, \tag{33}$$

where

$$a_2 = \frac{P_s\beta_2(1-\alpha_s)}{d_{SM}^{\tau_{SM}}(N_s-1)}, \quad \mathrm{b}_2 = \sigma_M^2, \quad c_2 = \frac{\mathrm{SINR}_M}{\phi_{z_1}} = \frac{\mathrm{SINR}_M d_{SM}^{\tau_{SM}}(K_{SM}+1)}{2\alpha_s P_s\beta_2 N_S}. \tag{34}$$

The probability of UAV surveilling non-outage with TZF/MRC scheme is given by

$$\mathrm{P}_{\mathrm{nonout}} = 1-(K_{MD}+1)^{N_t}\exp\left(-K_{MD}N_t\right) \cdot \sum_{p_1=1}^{N_S}\frac{1}{\Gamma(p_1)}(a_1)^{p_1-1}\sum_{\nu_1=0}^{p_1-1}\binom{\nu_1}{p_1-1}\left(\frac{b_1}{a_1}\right)^{p_1-1-\nu_1} \times \sum_{i_1=0}^{\infty}\frac{(K_{MD}N_t(K_{MD}+1))^{i_1}\Gamma(N_t+\nu_1+i_1)}{\Gamma(i_1+1)\Gamma(N_t+i_1)} \times (K_{SM}+1)^{(N_s-1)N_s}\exp\left(-K_{SM}(N_s-1)N_s\right) \times \sum_{p_2=1}^{N_r-1}\frac{1}{\Gamma(p_2)}(a_2)^{p_2-1}\sum_{\nu_2=0}^{p_2-1}\binom{\nu_2}{p_2-1}\left(\frac{b_2}{a_2}\right)^{p_2-1-\nu_2} \times \sum_{i_2=0}^{\infty}\frac{(K_{SM}(K_{SM}+1)(N_s-1)N_s)^{i_2}\Gamma((N_s-1)N_s+\nu_2+i_2)}{\Gamma(i_2+1)\Gamma((N_s-1)N_s+i_2)} \times Q_1 \tag{35}$$

where

$$\begin{aligned} Q_1 = {} & \sum_{k_1=0}^{\infty}\binom{k_1}{N_t+\nu_1+i_1+k_1-1}(-a_1)^{k_1}\psi_{SD}{}^{-(k_1+p_1-1)}(K_{MD}+1)^{-(N_t+\nu_1+i_1)-k_1} \\ & \times \sum_{k_2=0}^{\infty}\binom{k_2}{N_S(N_S-1)+\nu_2+i_2+k_2-1}(-a_2)^{k_2}\phi_{z_1}{}^{-(k_2+p_2-1)}(K_{SM}+1)^{-(N_S(N_S-1)+\nu_2+i_2)-k_2} \\ & \times \Gamma(p_1+p_2+k_1+k_2-1)\left(b_1/\psi_{SD}+b_2/\phi_{z_1}\right)^{-(p_1+p_2+k_1+k_2-1)} \\ & \times \left(\frac{-b_2}{\phi_{z_1}}+(p_2-1)\frac{b_1/\psi_{SD}+b_2/\phi_{z_1}}{p_1+p_2+k_1+k_2-2}\right)-\frac{a_2(N_S(N_S-1)+\nu_2+i_2)}{\phi_{z_1}} \\ & \times \sum_{k_1=0}^{\infty}\binom{k_1}{N_t+\nu_1+i_1+k_1-1}(-a_1)^{k_1}\psi_{SD}{}^{-(k_1+p_1-1)}(K_{MD}+1)^{-(N_t+\nu_1+i_1)-k_1} \\ & \times \sum_{k_2=0}^{\infty}\binom{k_2}{N_S(N_S-1)+\nu_2+i_2+k_2}(-a_2)^{k_2}\phi_{z_1}{}^{-(k_2+p_2-1)}(K_{SM}+1)^{-(N_S(N_S-1)+\nu_2+i_2+1)-k_2} \\ & \times \Gamma(p_1+p_2+k_1+k_2-1)\left(b_1/\psi_{SD}+b_2/\phi_{z_1}\right)^{-(p_1+p_2+k_1+k_2-1)} \end{aligned} \tag{36}$$

3.2. TZF/MRC. Different from the RZF scheme, the transmitter of UAV with multiple antennas adopts the TZF scheme to completely eliminate the self-interference.

According to [33], the compact form of $\mathbf{w}_t$ can be expressed as

$$\mathbf{w}_t = \frac{\Pi_1 \mathbf{h}_{MD}^{\dagger}}{\left\| \Pi_1 \mathbf{h}_{MD}^{\dagger} \right\|}, \tag{37}$$

where $\Pi_1 = \mathbf{I}_{N_t} - \mathbf{H}_{MM}^{\dagger}\mathbf{h}_{SM}\mathbf{h}_{SM}^{\dagger}\mathbf{H}_{MM}/\left\|\mathbf{h}_{SM}^{\dagger}\mathbf{H}_{MM}\right\|^2$ spans the null space of $\mathbf{h}_{SM}^{\dagger}\mathbf{H}_{MM}$.

Furthermore, the MRC scheme is adopted by the receive antennas of UAV monitor M to maximize the receiving of the suspicious information, i.e.,

$$\mathbf{w}_r = \frac{\mathbf{H}_{SM}}{\left\|\mathbf{H}_{SM}\right\|}. \tag{38}$$

Since UAV completely eliminates its self-interference [4], active jamming has no effect on the UAV signal receiving end. Consequently, UAV can use the full power P_J for jamming the suspicious destination.

By deriving similar to MRT/RZF, the probability of UAV surveilling non-outage with TZF/MRC scheme is given by

$$\begin{aligned} \mathrm{P}_{\mathrm{nonout}} = {} & 1 - (K_{MD}+1)^{N_t-1} \exp\left(-K_{MD}(N_t-1)\right) \\ & \cdot \sum_{p_1=1}^{N_S} \frac{1}{\Gamma(p_1)} (a_1)^{p_1-1} \sum_{\nu_1=0}^{p_1-1} \binom{\nu_1}{p_1-1} \left(\frac{b_1}{a_1}\right)^{p_1-1-\nu_1} \\ & \times \sum_{i=0}^{\infty} \frac{(K_{MD}(N_t-1)(K_{MD}+1))^{i_1} \Gamma(N_t+\nu_1+i_1-1)}{\Gamma(i_1+1)\Gamma(N_t+i_1-1)} \\ & \times (K_{SM}+1)^{(N_s-1)N_s} \exp\left(-K_{SM}(N_s-1)N_s\right) \\ & \times \sum_{p_2=1}^{N_r} \frac{1}{\Gamma(p_2)} (a_2)^{p_2-1} \sum_{\nu_2=0}^{p_2-1} \binom{\nu_2}{p_2-1} \left(\frac{b_2}{a_2}\right)^{p_2-1-\nu_2} \\ & \times \sum_{i_2=0}^{\infty} \frac{(K_{SM}(K_{SM}+1)(N_s-1)N_s)^{i_2} \Gamma((N_s-1)N_s+\nu_2+i_2)}{\Gamma(i_2+1)\Gamma((N_s-1)N_s+i_2)} \\ & \times Q_2 \end{aligned} \tag{39}$$

where

$$\begin{aligned} Q_2 = {} & \sum_{k_1=0}^{\infty} \binom{k_1}{N_t+\nu_1+i_1+k_1-2} (-a_1)^{k_1} {\psi_{SD}}^{-(k_1+p_1-1)} (K_{MD}+1)^{-(N_t+\nu_1+i_1-1)-k_1} \\ & \times \sum_{k_2=0}^{\infty} \binom{k_2}{N_S(N_S-1)+\nu_2+i_2+k_2-1} (-a_2)^{k_2} {\phi_{z_1}}^{-(k_2+p_2-1)} (K_{SM}+1)^{-(N_S(N_S-1)+\nu_2+i_2)-k_2} \\ & \times \Gamma(p_1+p_2+k_1+k_2-1) \left(b_1/\psi_{SD} + b_2/\phi_{z_1}\right)^{-(p_1+p_2+k_1+k_2-1)} \\ & \times \left(\frac{-b_2}{\phi_{z_1}} + (p_2-1)\frac{b_1/\psi_{SD}+b_2/\phi_{z_1}}{p_1+p_2+k_1+k_2-2}\right) - \frac{a_2(N_S(N_S-1)+\nu_2+i_2)}{\phi_{z_1}} \\ & \times \sum_{k_1=0}^{\infty} \binom{k_1}{N_t+\nu_1+i_1+k_1-2} (-a_1)^{k_1} {\psi_{SD}}^{-(k_1+p_1-1)} (K_{MD}+1)^{-(N_t+\nu_1+i_1-1)-k_1} \\ & \times \sum_{k_2=0}^{\infty} \binom{k_2}{N_S(N_S-1)+\nu_2+i_2+k_2} (-a_2)^{k_2} {\phi_{z_1}}^{-(k_2+p_2-1)} \\ & \cdot (K_{SM}+1)^{-(N_S(N_S-1)+\nu_2+i_2+1)-k_2} \times \Gamma(p_1+p_2+k_1+k_2-1) \left(b_1/\psi_{SD} + b_2/\phi_{z_1}\right)^{-(p_1+p_2+k_1+k_2-1)} \end{aligned} \tag{40}$$

4. Numerical and Simulation Results

In this part, we analyze the surveilling performance of the UAV monitor through numerical and simulation results. $\rho = 0.1$ represents the self-interference coefficient, and the Rayleigh channel variances are $\lambda_1 = \lambda_2 = 1$. The ground-to-ground channel power gain at a reference distance of 1 m is $\beta_1 = -5$ dB, and the UAV-to-ground channel power gain at a reference distance of 1 m is $\beta_2 = -65$ dB. The maximize height of UAV is 4000 m, the maximized circle radius of UAV is 1200 m, and the maximized distance between suspicious nodes is 6000 m. In [31], we obtain the system environment and frequency parameters as follows: $\alpha_1 = 1$, $\alpha_2 = 3$, $\alpha_3 = 5$, $\delta_1 = 44$, $\delta_2 = 9$, and $\delta_3 = 2 \ln 3/\pi$. We obtain the simulation results through Monte Carlo (MC) simulation. In order to ensure the accuracy of the simulation, the number of simulations is 100,000. The detailed parameters in the simulations will be introduced in the description of the figures.

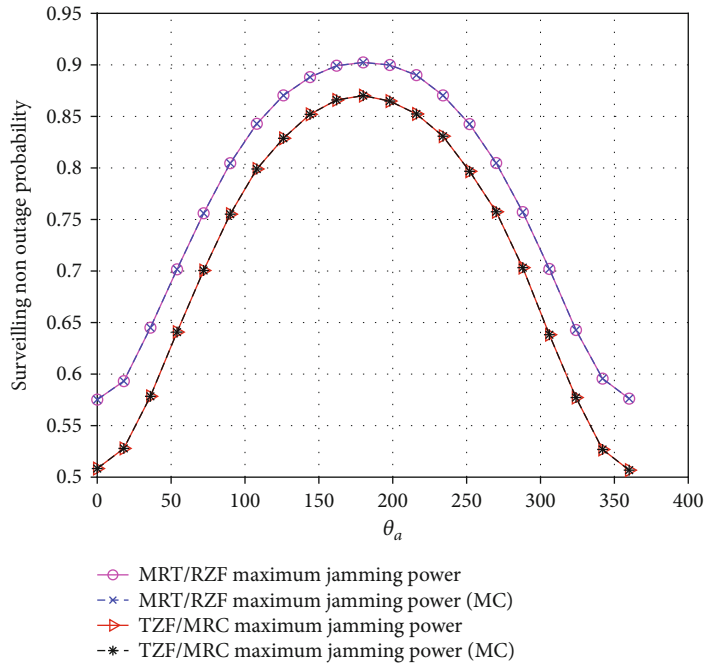

FIGURE 2: The probability of UAV surveilling nonoutage with MRT/RZF and TZF/MRC schemes versus θ_a, $P_S = 10$W, $P_J = 10$W, $v = 1000$m, $d = 600$m, $r = 400$m, $\alpha_s = 0.1$, $N_s = 10$, $N_r = N_t = 5$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

Curves without (MC) represent numerical results, and curves with (MC) represent simulated results.

Figure 2 shows the probability of UAV surveilling nonoutage with MRT/RZF and TZF/MRC schemes versus θ_a. The numerical results and the simulation results completely agree, which verifies our derivation. It is obvious that the surveilling performance of MRT/RZF scheme outperforms that of TZF/MRC scheme, since for facing artificial noise from the suspicious source, it is more effective to use more transmitting antennas to degrade the channel capacity of the suspicious link than improving the surveilling channel capacity by employing the more receiving antennas. When the azimuth angle θ_a is in the range of 0 to π, since UAV moves in a half circle and is getting closer to the suspicious destination, thus the jamming power on the suspicious destination becomes larger, the artificial noise power on the receiving of UAV becomes smaller, and the monitoring performance of the UAV becomes better. However, as the azimuth angle θ_a is in the range of π to 2π, the monitoring performance of the UAV becomes worse.

Figure 3 shows the probability of UAV surveilling nonoutage with MRT/RZF and TZF/MRC schemes versus radius r. The numerical results and the simulation results completely agree, which validates our derivation. The surveilling non-outage probability increases with the radius until 400 m, since UAV starts linear motion from the origin and is getting closer to the suspicious destination; thus, the jamming power on the suspicious destination becomes larger, and the artificial noise power on the receiving of UAV becomes smaller. Then, as the monitoring distance becomes larger and the channel quality of the legal monitoring link becomes worse, the surveilling non-outage probability decreases as the radius increases.

Figure 4 shows the probability of UAV surveilling nonoutage with MRT/RZF and TZF/MRC schemes versus the distance between suspicious nodes d_{SD}. The numerical results and the simulation results completely agree, which validates our derivation. Since the distance between suspicious nodes increases and the monitoring link has better channel quality than the suspicious link, the probability of surveilling nonoutage increases with d_{SD} increasing until 2000 m, where the probability of surveilling nonoutage is the largest. Then, as the monitoring distance becomes larger and the channel quality of the legal monitoring link becomes worse, the possibility of UAV surveilling nonoutage decreases as d_{SD} increases.

Figure 5 shows the comparison of the surveilling performance versus height when UAV adopts three schemes, that is, active monitoring with the MRT/RZF beamforming scheme, active monitoring with the TZF/MRC beamforming scheme, and the passive monitoring scheme. It is obvious that the surveilling nonoutage probability of passive monitoring scheme is 0, while MRT/RZF and TZF/MRC beamforming schemes with maximum jamming power have better monitoring performance. This shows that UAV passive monitoring scheme is not suitable for the case where the suspicious source uses artificial noise. Only by using the MRT/RZF and TZF/MRC beamforming schemes can UAV improve the surveilling performance. Since the monitoring link has better channel quality than the suspicious link and the active jamming signal received at the suspicious destination becomes larger, the probability of surveilling nonoutage

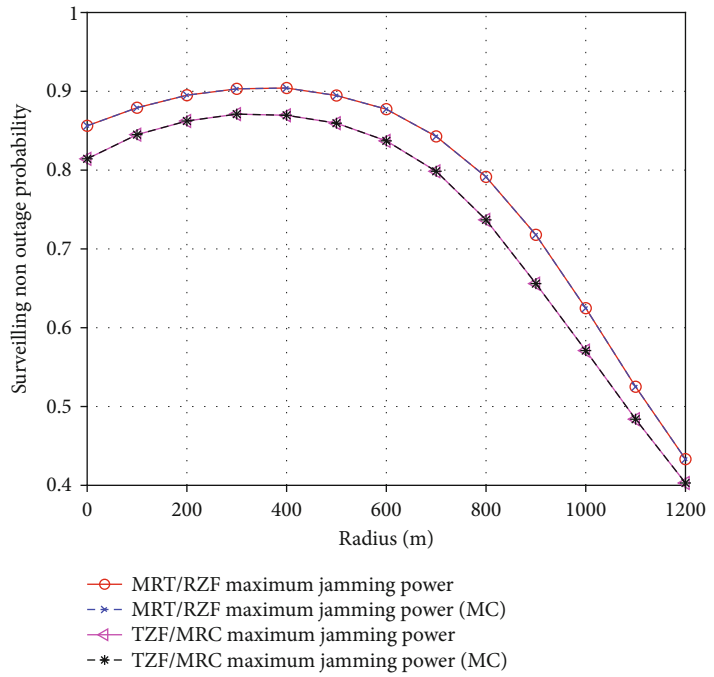

FIGURE 3: The probability of UAV surveilling nonoutage with MRT/RZF and TZF/MRC schemes versus radius r, $P_S = 10$W, $P_J = 10$W, $v = 1000$m, $d = 600$m, $\theta_a = \pi$, $\alpha_s = 0.1$, $N_s = 10$, $N_r = N_t = 5$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

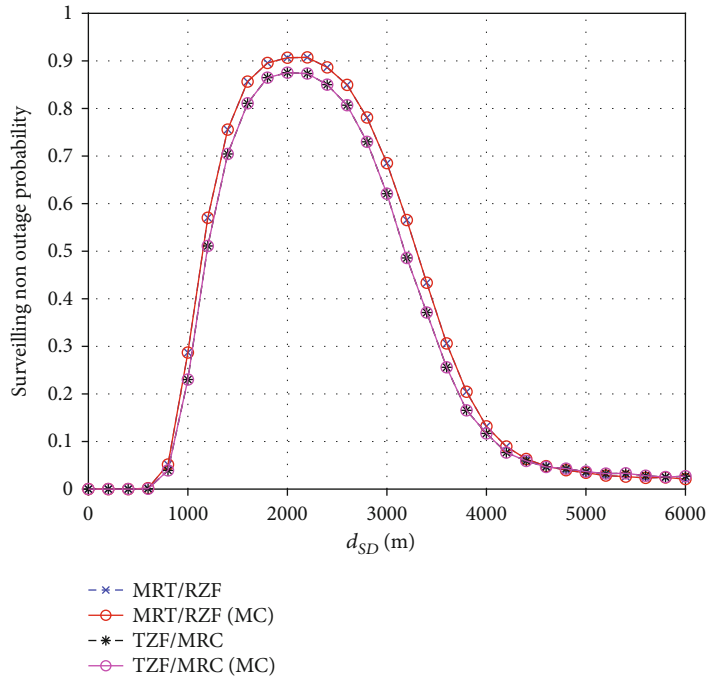

FIGURE 4: The probability of UAV surveilling non-outage with MRT/RZF and TZF/MRC schemes versusd_{SD}, $P_S = 10$W, $P_J = 10$W, $v = 1000$m, $r = 400$m, $\theta_a = 0$, $\alpha_s = 0.1$, $N_s = 10$, $N_r = N_t = 5$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

increases with height until 900 m, where the surveilling performance is the best, and then the surveilling performance decreases as the UAV height increases, since the monitoring distance becomes larger, while channel quality keeps unchanged, and active jamming signal received at the suspicious destination becomes smaller. It indicates that reasonable height control can improve UAV surveillance performance.

Figure 6 shows the probability of UAV surveilling nonoutage versus the number of receiving antennas for the MRT/RZF beamforming scheme with different jamming powers. It is obvious that the probability of surveilling

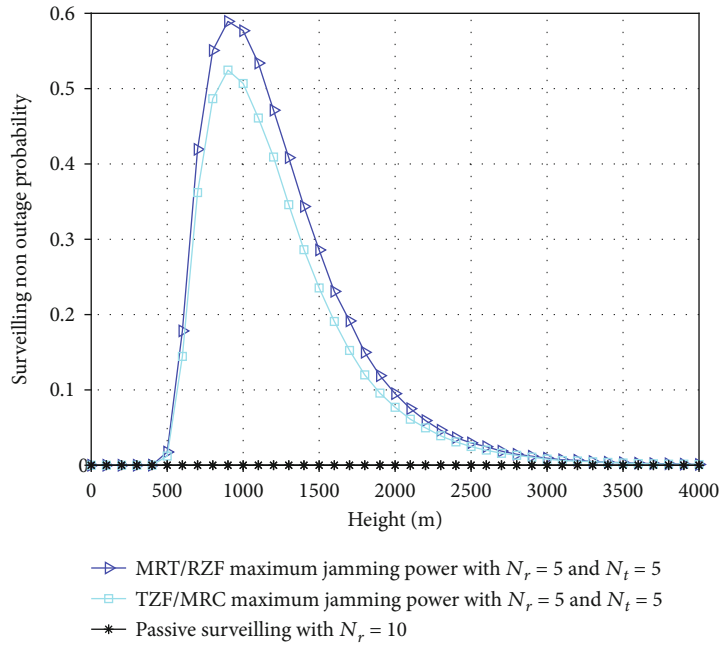

FIGURE 5: The probability of surveilling nonoutage with different jamming schemes versus the height of UAV, $P_S = 10$W, $P_J = 10$W, $d = 600$m , $r = 400$m, $\alpha_s = 0.1$, $\theta_a = 0$, $N_s = 10$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

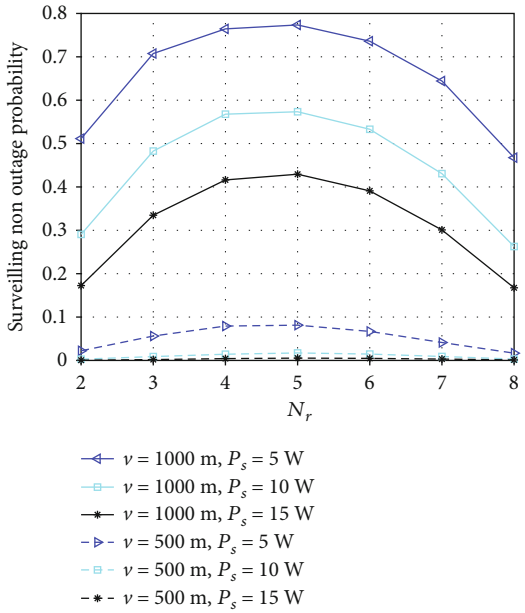

FIGURE 6: The probability of UAV surveilling nonoutage versus the number of receiving antennas for the MRT/RZF beamforming scheme with different jamming powers, $P_J = 10$W, $d = 600$m, $r = 400$m, $\theta_a = 0$, $\alpha_s = 0.1$, $\sigma_D^2 = \sigma_M^2 = -115$dBm, $N_s = 10$, and $N_r + N_t = 10$.

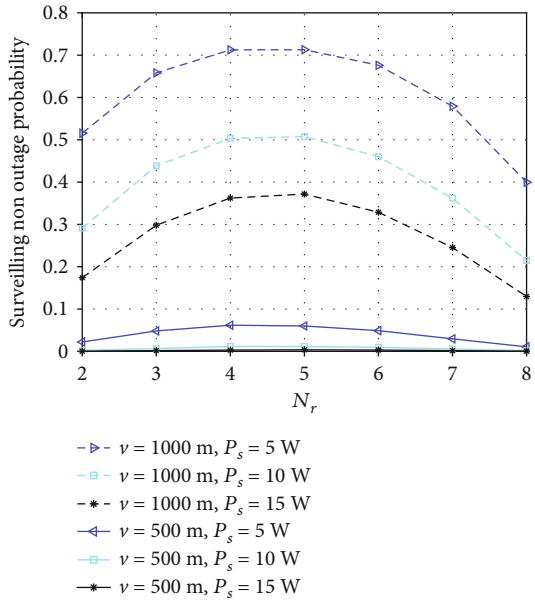

FIGURE 7: The probability of UAV surveilling nonoutage versus the number of receiving antennas for the TZF/MRC beamforming scheme with different jamming powers, $P_J = 10$W, $d = 600$m, $r = 400$m, $\theta_a = 0$, $\alpha_s = 0.1$, $\sigma_D^2 = \sigma_M^2 = -115$dBm, $N_s = 10$, and $N_r + N_t = 10$.

nonoutage increases with the number of receiving antennas until $N_r = 5$, since it is more effective to improve the surveilling channel capacity than degrading the channel capacity of the suspicious link. Then, the probability of surveilling nonoutage decreases as the number of receiving antennas increases, since it is more effective to degrade the channel capacity of the suspicious link than improving the surveilling channel capacity. For UAV monitor with the MRT/RZF beamforming scheme, it should adopt reasonable N_r to improve the surveilling performance.

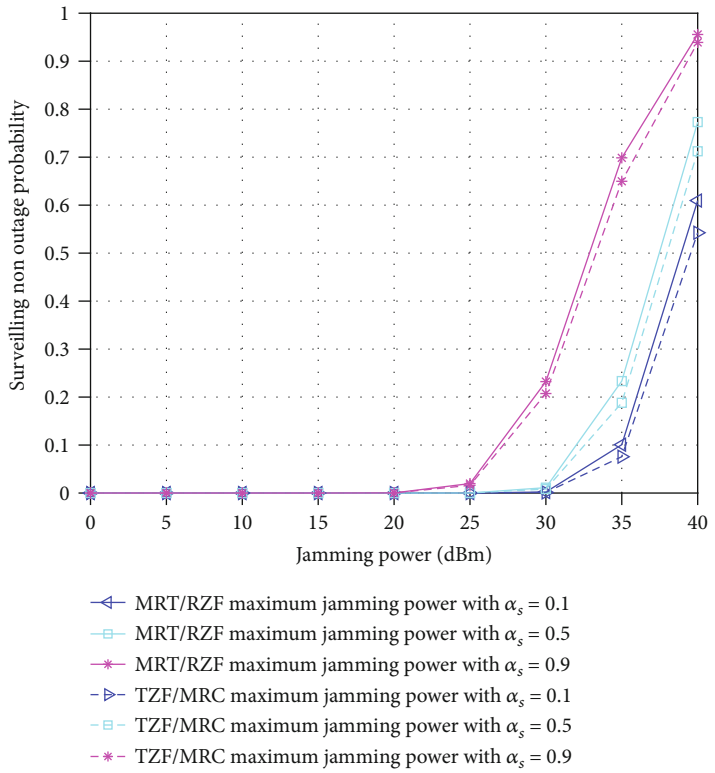

FIGURE 8: The probability of UAV surveilling nonoutage with different α_S versus UAV maximized jamming power P_J for the MRT/RZF and TZF/MRC beamforming scheme, $v = 1000$m, $d = 600$m, $r = 400$m, $\theta_a = 0$, $N_r = N_t = 5$, $N_s = 10$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

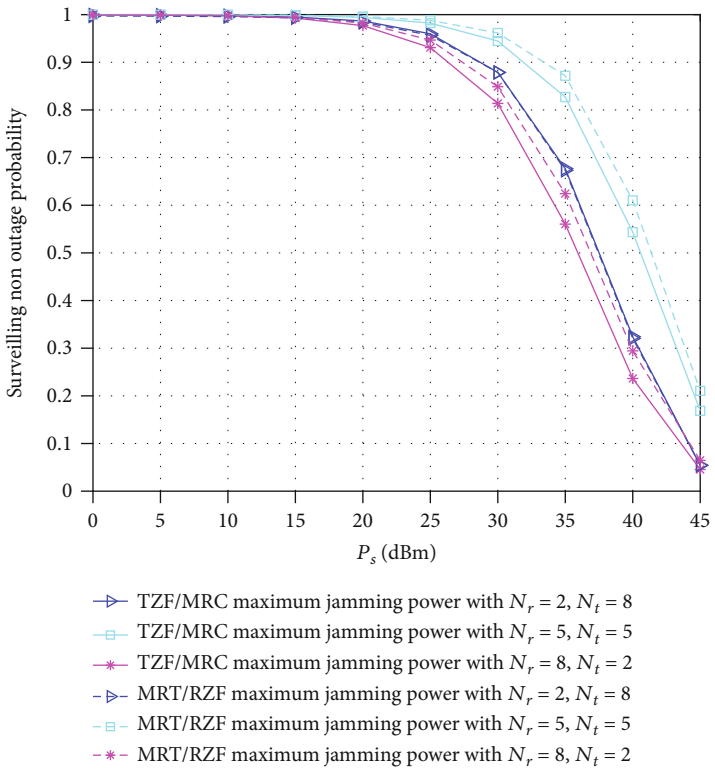

FIGURE 9: The probability of UAV surveilling nonoutage with different N_r and N_t versus P_S, $P_J = 10$W, $v = 1000$m, $d = 600$m, $r = 400$m, $\alpha_s = 0.1$, $\theta_a = 0$, $N_s = 10$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

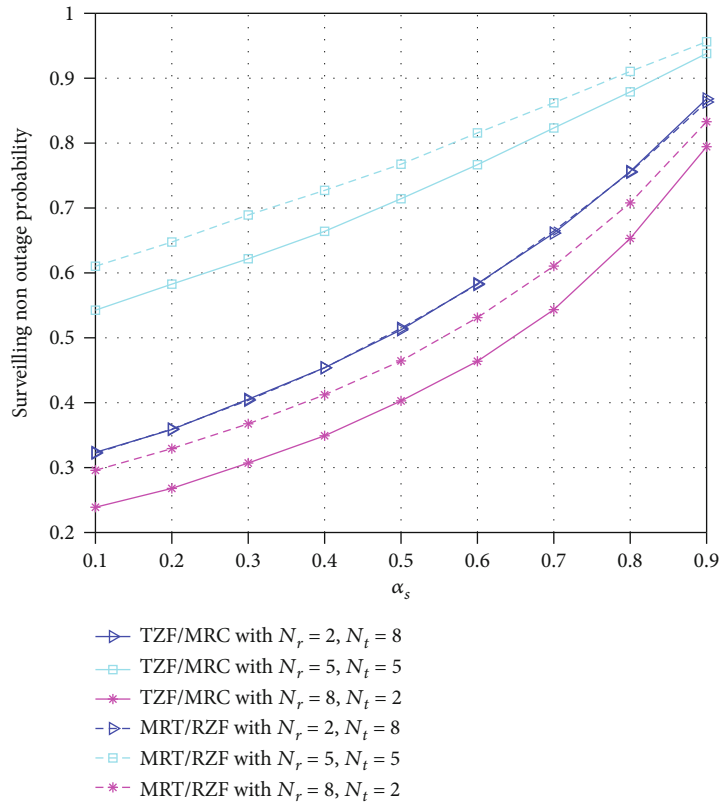

FIGURE 10: The probability of UAV surveilling nonoutage with different N_r and N_t versus α_S, $P_S = 10$W, $P_J = 10$W, $v = 1000$m, $d = 600$m, $r = 400$m, $\theta_a = 0$, $N_s = 10$, and $\sigma_D^2 = \sigma_M^2 = -115$dBm.

Figure 7 shows the probability of UAV surveilling non-outage versus the number of receiving antennas for the TZF/MRC beamforming scheme with different jamming powers. The reason why the surveilling performance of the TZF/MRC scheme increases with N_r and then decreases with N_r is the same as that of the MRT/RZF scheme. For UAV monitor with the TZF/MRC beamforming scheme, it should adopt reasonable N_r to improve the surveilling performance.

Figure 8 shows the probability of UAV surveilling non-outage with different α_S versus UAV maximized jamming power P_J for MRT/RZF and TZF/MRC beamforming schemes. It is obvious that the probability of UAV surveilling non-outage increases with P_J increasing. Furthermore, the probability of UAV surveilling non-outage increases with α_S increasing. The MRT/RZF beamforming scheme has a little better surveilling performance than the TZF/MRC beamforming scheme. For UAV monitor, it should adopt larger P_J to improve the surveilling performance.

Figure 9 shows the probability of UAV surveilling non-outage with different N_r and N_t versus P_S for MRT/RZF and TZF/MRC beamforming schemes. It is obvious that the probability of UAV surveilling non-outage decreases with P_S increasing. Furthermore, when $N_r = N_t = 5$, the probability of UAV surveilling non-outage is the largest. The MRT/RZF beamforming scheme has a little better surveilling performance than the TZF/MRC beamforming scheme.

For the suspicious source, it should adopt larger P_S to avoid being monitored.

Figure 10 shows the probability of UAV surveilling non-outage with different N_r and N_t versus α_S for MRT/RZF and TZF/MRC beamforming schemes. It is obvious that the probability of UAV surveilling non-outage increases with α_S increasing. Furthermore, when $N_r = N_t = 5$, the probability of UAV surveilling non-outage is the largest. The MRT/RZF beamforming scheme has a little better surveilling performance than the TZF/MRC beamforming scheme.

For the suspicious source, it should adopt lower α_S to avoid being monitored.

5. Conclusion

We propose a legal full-duplex UAV surveillance system in the presence of the ground-to-ground suspicious link with antisurveillance technology. UAV performs passive surveillance and active jamming simultaneously. However, the suspicious source with multiantenna adopts artificial noise to avoid being monitored. The probability of surveilling non-outage is derived for MRT/RZF and TZF/MRC beamforming schemes. For different heights of UAV, the optimal number of receiving antennas with a fixed total number of antennas that maximizes the probability of UAV surveilling non-outage is determined. Impact of angle/radius/height on the surveilling non-outage probability is analyzed. For the suspicious source, impact of the distance between suspicious nodes on the surveilling non-outage probability is analyzed.

Data Availability

All data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is partially supported by the National Key Research and Development Project of China under Grant 2020YFB1806805.

References

[1] 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.

[2] 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, article 8083, 2016.

[3] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal on Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1449–1461, 2016.

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

[5] C. Liu, T. Q. S. Quek, and J. Lee, "Secure UAV communication in the presence of active eavesdropper," in *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Nanjing, China, October 2017.

[6] 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.

[7] H. Wang, J. Chen, G. Ding, and J. Sun, "Trajectory planning in UAV communication with jamming," in *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Hangzhou, China, October 2018.

[8] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, 2019.

[9] M. Cui, G. Zhang, Q. Wu, and D. W. K. Ng, "Robust trajectory and transmit power design for secure UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 9042–9046, 2018.

[10] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy rate analysis of UAV-enabled mmWave networks using Matérn hardcore point processes," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1397–1409, 2018.

[11] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 181–184, 2019.

[12] Y. Zhou, P. L. Yeoh, H. Chen et al., "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11280–11284, 2018.

[13] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 310–313, 2017.

[14] Q. Wang, Z. Chen, H. Li, and S. Li, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," *IEEE Access*, vol. 6, pp. 62849–62855, 2018.

[15] H. Liu, S. Yoo, and K. S. Kwak, "Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers," *Journal of the Communications Network*, vol. 20, no. 5, pp. 496–508, 2018.

[16] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovar, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2283–2293, 2019.

[17] D. Hu, Q. Zhang, Q. Li, and J. Qin, "Proactive unmanned aerial vehicle Surveilling via jamming in decode-and-forward relay networks," *IEEE Access*, vol. 7, pp. 90465–90475, 2019.

[18] G. Hu and Y. Cai, "UAVs-assisted proactive eavesdropping in AF multi-relay system," *IEEE Communications Letters*, vol. 1, no. 1, pp. 1089–7798, 2019.

[19] M. Zhang, Y. Chen, X. Tao, and I. Darwazeh, "Power allocation for proactive eavesdropping with spoofing relay in UAV systems," in *2019 26th International Conference on Telecommunications (ICT)*, pp. 8–10, Hanoi, Vietnam, April 2019.

[20] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, 2013.

[21] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[22] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: transmission optimization in multi-input single-output wiretap channels," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1771–1783, 2015.

[23] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2170–2181, 2016.

[24] X. Xia, K. Xu, D. Zhang, Y. Xu, and Y. Wang, "Beam-domain full-duplex massive MIMO: realizing co-time co-frequency uplink and downlink transmission in the cellular system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 8845–8862, 2017.

[25] X. Xia, K. Xu, Y. Wang, and Y. Xu, "A 5G-enabling technology: benefits, feasibility, and limitations of in-band full-duplex mMIMO," *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 81–90, 2018.

[26] K. Xu, Z. Shen, X. Xia, and D. Zhang, "Hybrid time-switching and power splitting SWIPT for full-duplex massive MIMO systems: a beam-domain approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7257–7274, 2018.

[27] Y. Shen, Z. Pan, N. Liu, and X. You, "Joint design and performance analysis of a full-duplex UAV legitimate surveillance system," *Electronics*, vol. 9, no. 3, p. 407, 2020.

[28] Q. Song, F.-C. Zheng, Y. Zeng, and J. Zhang, "Joint beamforming and power allocation for UAV-enabled full-duplex relay,"

IEEE Transactions on Vehicular Technology, vol. 68, no. 2, pp. 1657–1671, 2019.

[29] 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.

[30] D. W. Matolak and R. Sun, "Unmanned aircraft systems: air-ground channel characterization for future applications," *IEEE Vehicular Technology Magazine*, vol. 10, no. 2, pp. 79–85, 2015.

[31] M. M. Azari, F. Rosas, K. C. Chen, and S. Pollin, "Ultra reliable UAV communication using altitude and cooperation diversity," *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 330–344, 2018.

[32] C. Liu, J. Lee, and T. Q. S. Quek, "Safeguarding UAV communications against full-duplex active eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 18, pp. 2919–2931, 2019.

[33] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Transactions on Communications*, vol. 64, no. 4, pp. 1769–1785, 2016.

[34] G. John, *Proakis, Masoud Salehi, Digital Communications*, McGraw-Hill, New York, NY, USA, 5th edition, 2008.

[35] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic, San Diego, CA, USA, 6th edition, 2000.