The following publication Huang, H., Savkin, A. V., & Ni, W. (2021). Navigation of a UAV Team for Collaborative Eavesdropping on Multiple Ground Transmitters. IEEE Transactions on Vehicular Technology, 70(10), 10450-10460 is available at https://doi.org/10.1109/TVT.2021.3108182

Navigation of a UAV Team for Collaborative Eavesdropping on Multiple Ground Transmitters

Hailong Huang, Andrey V. Savkin, and Wei Ni

***Abstract*—Thanks to excellent mobility and high probability of a Line-of-Sight (LoS) to ground objects, unmanned aerial vehicles (UAVs) have been widely used in surveillance. This paper considers the use of UAVs to covertly and collaboratively eavesdrop on suspicious wireless transmitters on the ground. We focus on the trajectory planning of the UAVs. To avoid the UAVs being visually noticed by the ground transmitters, we propose a new measure to quantify the disguising performance of the UAVs. The trajectories of the UAVs are planned to maximize the disguising performance, subject to an uninterrupted eavesdropping requirement, UAV collision avoidance and UAV aeronautic maneuverability. A new randomized method based on the Rapidly-exploring Random Tree (RRT) is developed to efficiently construct the trajectories of the UAVs. Computer simulations confirm that the proposed method outperforms the random movement method in eavesdropping performance, while achieving with comparable disguising performance.**

***Index Terms*—Unmanned aerial vehicle (UAV), covert eavesdropping, wireless communications, trajectory planning.**

I. Introduction

UNMANNED Aerial Vehicles (UAVs) have increasingly attracted attention, thanks to their reduced cost, improved mobility and on-demand real-time deployment. UAVs provide a superb means for communications [1], [2], as they have a high probability of a Line-of-Sight (LoS) to other objects. Besides, their mobility enables quick deployment of a network, especially in some emergencies, e.g., after disasters [3]. The UAVs can also be used as aerial relays to provide connectivity between remote users and wireless networks [4]–[6].

The excellent mobility and the availability of the LoS enable UAVs to proactively protect wireless communications. UAVs can function as jammers by transmitting noises to confuse eavesdroppers [7], [8]. When transmitting useful data, they can secure the transmissions by optimizing their trajectories [9], [10], transmit power [11], and transmission schedule [12]. As a result, eavesdroppers cannot decode the collected data, while the intended nodes can. A hybrid system with a UAV jammer and a UAV transmitter has been proposed to improve the security of transmissions [13]–[15]. Beyond securely transmitting data to the intended nodes, UAVs have also been used to carry out eavesdropping on suspicious ground targets [16], [17] and other UAVs [18], [19].

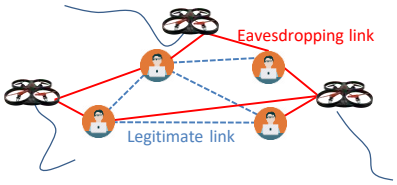


Fig. 1: Illustration of the considered scenario, where there are four ground nodes and three UAV-based aerial eavesdroppers collaboratively eavesdropping on the ground nodes.

In the above studies, UAVs are used for counter-eavesdropping and eavesdropping, where the eavesdroppers are (relatively) stationary UAV [8], [9], move periodically [10], or move randomly [17]. The stationary UAV eavesdroppers and those with periodical movements could be easily noticed, leading to failed surveillance missions. The random movement can help disguise the eavesdropping intention of the UAVs, but the eavesdropping performance can hardly be guaranteed. In this paper, we consider a scenario, where multiple UAVs covertly and collaboratively eavesdrop on several ground targets. This is motivated by applications in which the eavesdropping mission should not be noticed by the targets. One typical example is police surveillance on criminal suspects.

We optimize the trajectories for the UAVs that collaboratively and secretively eavesdrop on a set of ground nodes; see Fig. 1. The eavesdropping performance on any ground link is expected to remain effective at any time, while the UAVs disguise their eavesdropping intention to prevent being visually noticed. This is a new and practically interesting scenario. It is different from the scenarios in the literature where either an integrated jamming or eavesdropping technique is designed [7], [11] or unplanned random trajectories are employed [17]. Neither the integrated jamming and eavesdropping, nor random trajectories can guarantee an instantaneous jamming or eavesdropping performance. To the best of our knowledge, there is no study that jointly considers the covertness of eavesdroppers and the eavesdropping performance.

An important issue of the covert surveillance is how to characterize the disguising performance. We propose a new measure to quantify the disguising, which combines the derivatives of the UAV-node angle and distance. We formulate a new trajectory planning problem to maximize the disguising met-

This work was supported by the Australian Research Council. Also, this work received funding from the Australian Government, via grant AUSMURIB000001 associated with ONR MURI grant N00014-19-1-2571.

H. Huang is with the Department of Aeronautical and Aviation Engineering, the Hong Kong Polytechnic University, Hong Kong. (E-mail: hailong.huang@polyu.edu.hk).

A.V. Savkin is with School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney 2052, Australia. (E-mail: a.savkin@unsw.edu.au).

W. Ni is with Data61, CSIRO, Australia. (E-mail: wei.ni@data61.csiro.au).

ric. Meanwhile, the eavesdropping performance and collision avoidance requirements are met, the distance between a UAV-node pair is sufficiently large at any time, and the movements of the UAVs satisfy the aeronautic maneuverability.

To solve this problem, we present a method based on Rapidly-exploring Random Tree (RRT). For each of the UAVs, a tree of possible trajectories is constructed incrementally from samples drawn randomly in the space. The set of trajectories (one per UAV) maximizing the disguising performance and satisfying all constraint conditions is selected. Different from the complete random walk method, the proposed method can incorporate the eavesdropping requirement as a constraint of trajectory planning. Moreover, the proposed RRT-based method can be decentralized by pre-storing at all UAVs the same set of samples drawn in the space. Only by observing the positions of the others, each UAV can construct consistent RRTs for all the UAVs and select the best trajectories for itself independently and consistently. Extensive simulations confirm that the proposed technique provides effective eavesdropping with a negligible loss of disguising, as compared to UAVs with completely random trajectories.

The contributions of this paper are summarized as follows.

- We propose a new metric to characterize the disguising performance of the surveillance UAVs.
- We formulate a new trajectory optimization problem, which accounts for both the eavesdropping performance and the disguising performance.
- A new RRT-based trajectory planning method is proposed and numerically corroborated via computer simulations.

The remainder of the paper is organized as follows. In Section II, we review the related works. In Section III, we present the system model and formulate the problem of interest. In Section IV, we propose the RRT-based trajectory planning method. Computer simulations are demonstrated in Section V to show the performance of the proposed method. A conclusion is given in Section VI.

II. Related Work

When operating as eavesdroppers, UAVs are likely to collect stronger signals than the ground counterparts due to the high probability of LoS. Existing research has investigated the security rate in the systems with UAV eavesdroppers. The paper [20] investigates the secrecy outage performance of a UAV system with a linear trajectory, where a UAV flies along a straight line and transmits data to a ground node in the presence of a UAV eavesdropper. The reference [19] considers the scenario, where a UAV transmitter sends data to a UAV receiver with UAV eavesdroppers uniformly and randomly deployed. By using stochastic geometry theory, the closed-form expressions for the secrecy outage probability and the average secrecy capacity are derived. In [21], a UAV jammer is added to the system of [19]. The authors derive the secure connection probability of a legitimate ground link as a function of the jamming power, the position of the UAV jammer and the height of UAV eavesdroppers. Besides the relatively stationary deployment, the paper [17] investigates the case in which UAV eavesdroppers move in a 3D space. The authors analyze the ergodic and outage secrecy capacities of a legitimate ground link under selection combining (SC) or maximal ratio combining (MRC) eavesdropping of the UAVs.

The paper [16] considers UAV-assisted proactive eavesdropping in a amplify-and-forward multi-relay system. One UAV is deployed above a suspicious node, and it can either eavesdrop or jam at any time due to its half-duplex constraint. The authors investigate which UAVs should jam and which should eavesdrop to improve the successful eavesdropping rate. The paper [18] uses a legitimate UAV to overhear the communication of suspicious UAVs, while tracking their flight trajectory. Making use of the eavesdropped data, the authors design the movement of a UAV to jam a pair of suspicious UAVs, so as to force the suspicious UAV to reduce its data rate. This helps increase the success of eavesdropping.

The trajectory control of UAVs has been studied for security protection. The paper [10] considers the use of a UAV to communicate with a moving ground node in the presence of stationary or moving eavesdroppers. By assuming the knowledge on the movements of eavesdroppers, [10] designs the UAV trajectory to keep the UAV far away from the eavesdroppers. The paper [11] considers a UAV-ground communication system with ground eavesdroppers with partially known locations. The goal is to maximize the average worst-case secrecy rate of the system by jointly designing the robust UAV trajectory and transmit power. The references [13]–[15] consider a hybrid system with a source UAV and a jamming UAV in the presence of eavesdroppers. The source UAV sends confidential information and the jamming UAV cooperatively transmits interference signals to jam eavesdroppers. The two UAVs' trajectories and the transmit power are considered as control inputs to maximize the minimum worst-case secrecy rate of the users. The paper [12] investigates a system with multiple source UAVs and jamming UAVs, and maximizes the system secrecy energy efficiency by optimizing the UAVs' trajectories, transmit power, and user scheduling under the UAVs' mobility constraints and the maximum transmit power.

The above studies [10], [11], [13]–[15] design the UAVs' trajectories and other control variables to optimize different security-related metrics. In the context of area surveillance, minimizing the age of information has been used as an objective of the path planning problem [22], [23]. The UAVs periodically visit a given set of positions, and the corresponding path planning problem can be formulated as the conventional travelling salesman problem or its variants. When the target positions are unknown, specific trajectory patterns are adopted to cover the area of interest. The corresponding problem is called coverage path planning, and the widely studied patterns include the zigzag and the spiral-like pattern [24]. Regarding target tracking, UAVs are used for standoff tracking [25] and persistent tracking [26]. While the former [25] requires the UAVs to follow some standoff orbits, the latter [26] aims at maximizing the probability of having targets within the sensing range, especially in cluttered urban environments.

None of the above works [10], [11], [13]–[15], [22], [23], [25], [26] have taken the covertness of the UAVs into account. Covertness can play an important role in applications requiring UAVs to be unnoticed by targets, e.g., pursuit and intercep-

tion, police surveillance and wild animal tracking. Motion camouflage, a stealthy behavior firstly discussed in [27], has been considered for UAV disguising. As presented in [27], a predator often camouflages to the effect that it remains (relatively) stationary in the view of its prey. Various motion camouflage guidance laws have been proposed for UAVs to achieve this [28]–[31]. Specifically, the paper [28] designs a motion camouflage guidance law to monitor a moving target, so that the UAV maintains a constant distance from the target. The paper [29] proposes a bearing-based UAV motion camouflage guidance law, where only the bearing information to the moving target and a fixed reference point is used. With no range information used, the UAV only camouflages its motion with respect to the target by keeping a large distance. The paper [30] presents a virtual-motion-camouflage-based framework. With a pseudospectral discretization approach, it finds analytical solutions for the formation-flying trajectory reconfiguration guidance under boundary conditions. Aiming at capturing a moving target using a net towed by a UAV team, the paper [31] regards the net center as a predator (a virtual UAV). A navigation law is proposed for the virtual UAV first, and then the authors present a formation control law to guide the motion of each real UAV using the virtual UAV. These motion camouflage approaches construct the UAVs' trajectories to the UAVs to maintain relatively stationary with respect to the target and the reference. If these approaches are used in our problem, the UAVs could remain at positions which are not in favor of eavesdropping.

Several researches have focused on UAV detection [32]–[35]. For example, the paper [33] reports the results of using military Doppler radar to detect a DJI UAV. The paper [34] proposes a machine learning framework for detection and classification of UAV sounds out of those of birds, airplanes and thunderstorm. A spatial-temporal fusion detection method for UAVs using electrical-optical cameras is presented in [35]. These approaches can detect and/or locate UAVs in proximity. The aforementioned (relatively) stationary camouflage of the UAVs would fail. It becomes critical for the UAVs to disguise their eavesdropping intention by adjusting the way they move, as opposed to hiding their presence.

III. Problem Statement

We consider that M stationary ground nodes send messages to each other and N heterogeneous UAVs eavesdrop on the ground nodes (see Fig. 1). In this section, we first present the system models and then formally state the problem of interest. The frequently used symbols are listed in TABLE I.

Let $\mathbf{p}_i(t) = [x_i(t), y_i(t), z_i(t)]$ be the position of UAV i at time t. The following flight model is considered to describe the motions of the UAVs [36]:

$$\begin{cases} \dot{x}_i(t) = v_i(t)\cos(\theta_i(t)), \\ \dot{y}_i(t) = v_i(t)\sin(\theta_i(t)), \\ \dot{\theta}_i(t) = u_i(t), \\ \dot{z}_i(t) = w_i(t), \\ Z_{\min} \le z_i(t) \le Z_{\max}, \end{cases} \tag{1}$$

TABLE I: Symbols and definitions.

Parameter	Definition
N	Number of UAVs
M	Number of ground nodes
$\mathbf{q}_j$	Position of node j
C	Eavesdropping performance requirement
d_{safe}	Safety distance between UAVs
C	Eavesdropping performance requirement
D_i	Average distance away from targets for UAV i
T	Time duration for path planning
L	Number of time slots in a duration T
Variable	**Definition**
$\mathbf{p}_i(t)$	Position of UAV i
$\theta_i(t)$	Heading angle of UAV i
$v_i(t)$	Linear speed of UAV i
$w_i(t)$	Angular speed of UAV i
$u_i(t)$	Vertical speed of UAV i
$d_{ij}(t)$	Distance between UAV i and node j
$\delta_{ih}(t)$	Distance between UAVs i and h
$F_j(t)$	Combined SNR of node j
$\alpha_{ij}(t)$	The angle between UAV i and node j

where $\theta_i(t)$ is the heading of UAV i with respect to the x-axis; $v_i(t)$ and $u_i(t)$ are its linear and angular speeds on the horizontal plane, respectively; and $w_i(t)$ is the vertical speed. $\dot{x}_i(t)$, $\dot{y}_i(t)$, $\dot{z}_i(t)$ and $\dot{\theta}_i(t)$ are the derivatives of $x_i(t)$, $y_i(t)$, $z_i(t)$ and $\theta_i(t)$ with respect to t, respectively. Let $V_i^{\max}$, $W_i^{\max}$ and $U_i^{\max}$ be given constants, and $0 \le v_i(t) \le V_i^{\max}$, $-W_i^{\max} \le w_i(t) \le W_i^{\max}$, and $-U_i^{\max} \le u_i(t) \le U_i^{\max}$. Moreover, $Z_{\min}$ and $Z_{\max}$ are the minimum and maximum allowed altitudes, respectively.

Let $\mathbf{q}_j$ $(j = 1, \ldots, M)$ be the location of node j on the ground[1]. Let $d_{ij}(t)$ denote the Euclidean distance between UAV i and node j at time t. Then, $d_{ij}(t)$ is given by:

$$d_{ij}(t) = \|\mathbf{p}_i(t) - \mathbf{q}_j\|, \tag{2}$$

where $\|\cdot\|$ is the standard norm of a vector.

We consider large-scale and small-scale fading in the ground-to-air channel. The large-scale fading depends on the distance between the transmitter and the receiver. Let h_{ij} denote the small-scale channel coefficient between UAV i and ground node j. h_{ij} is assumed to yield independent and identically distributed (i.i.d.) Rician fading with a Rician factor $K > 0$. Let P denote the transmit power of the ground nodes and n_0 denote the zero-mean additive white Gaussian noise with $\mathbb{E}[|n_0|^2] = \sigma_0^2$. Then, the instantaneous signal-to-noise ratio (SNR) at UAV i from node j is $P\mathrm{y}_{ij} d_{ij}^{-a}(t)/\sigma_0^2$, where $\mathrm{y}_{ij} = |h_{ij}|^2$ and a is the path loss exponent. y_{ij} is a random variable following a non-central Chi-square distribution. Since the UAV eavesdroppers collaborate, the collaborative eavesdropping performance on node j by the UAVs at time t, denoted by $F_j(t)$, is given by:

$$F_j(t) = \int_{\mathrm{y}_{1j},\ldots,\mathrm{y}_{Nj}} \cdots \int \sum_{i=1}^{N} \frac{P\mathrm{y}_{ij}}{d_{ij}^a(t)\sigma_0^2} \prod_{i=1}^{N} f(\mathrm{y}_{ij})\, d\mathrm{y}_{1j} \ldots d\mathrm{y}_{Nj}, \tag{3}$$

if the UAVs carry out MRC [17], which is known to maximize the combined SNR of signals captured by the UAVs. Here,

[1]As considered in [37], the UAVs can measure the locations of the ground nodes via an onboard optical camera or a synthetic aperture radar.

$f(\mathrm{y}) = \frac{(K+1)}{\Omega}\exp(-K - \frac{(K+1)\mathrm{y}}{\Omega})I_0(2\sqrt{\frac{K(K+1)\mathrm{y}}{\Omega}})$ is the probability density function (PDF) of the gain of the Rician fading channel, where $I_0(\cdot)$ is the 0th order modified Bessel function of the first kind, and K and Ω are the given model parameters.

Let C be a given threshold for the collaborative eavesdropping measure. Suppose that if this measure is smaller than C, it is not possible to extract useful information from the collected data. In this sense, C is the channel capacity between node j and its intended receiver on the ground. To guarantee that the collected data at any time by the UAVs is meaningful, the following constraint should hold:

$$F_j(t) \geq C, \ \forall j, \ \forall t. \tag{4}$$

It is worth pointing out that constraint (4) uses the MRC method to characterize the eavesdropping performance. Compared to SC which only picks the UAV with the highest SNR at an instant, MRC combines the signals of all the UAVs to maximize the SNR at every instant for eavesdropping. This corresponds to the best eavesdropping capability and performance that the UAVs could have.

Apart from the eavesdropping task, the UAVs should also avoid collisions and disguise their intention of eavesdropping. For collision avoidance, a safety distance d_{safe} between any two UAVs is considered. Let $\delta_{ih}(t) = \|\mathbf{p}_i(t) - \mathbf{p}_h(t)\|$ is the distance between UAVs i and h at time t. Then, any pair of UAVs should be at least d_{safe} apart at any time:

$$\delta_{ih}(t) \geq d_{\text{safe}}, \forall i \neq h, \forall t. \tag{5}$$

In practice, the safety distance d_{safe} is a constant. It is selected based on the type of the UAVs and should be sufficient to avoid possible collisions between the UAVs; see e.g. [38], [39].

For disguising, the UAVs should not be too close to the nodes, since the smaller the distance, the higher the probability of being noticed. We consider the following constraints:

$$\frac{1}{T}\int_{kT}^{(k+1)T} d_{ij}(t)dt \geq D_i, \ \forall j, \ \forall i, \tag{6}$$

where $[kT, (k+1)T]$ ($k = 0, 1, \ldots, K$, and T is the duration of a time interval) is a time interval during which the accumulative distance between node j and UAV i is sufficiently large. D_i is the given threshold which depends on the size of UAV i. For a large UAV i, D_i should also be large, since it is more noticeable than a small UAV.

It is worth pointing out that constraint (4) is a hard constraint, and can lead to the infeasibility of the considered problem, especially when there are fewer UAVs than nodes and the nodes are well apart from each other. In the presence of a sufficient number of UAV eavesdroppers (e.g., no fewer than the nodes), constraint (4) could enforce the UAVs to reduce their altitudes and get the UAVs closer to the nodes if needed, until constraint (6), becomes active. One could potentially set D_i in constraint (6) as a hyperparameter, and adjust D_i to make (4) satisfied.

We propose a new metric to quantify the disguising performance which evaluates the derivative of the UAV-node angle and the derivative of the UAV-node distance. By frequently changing the relative positions of the UAVs against the targets, the movements of the UAVs appear to be random to the targets (i.e., the ground nodes). The targets are unlikely to connect the UAVs with an eavesdropping or monitoring mission (as compared to structured movements with recognizable patterns). When the targets use cameras to monitor their surrounding, it is generally difficult for the cameras to focus their lens on a UAV that frequently changes distance and angle with respect to the camera. A ground node can hardly obtain a clear view of the UAV. In light of this, our disguising metric evaluates the derivative of the UAV-node angle and the derivative of the UAV-node distance.

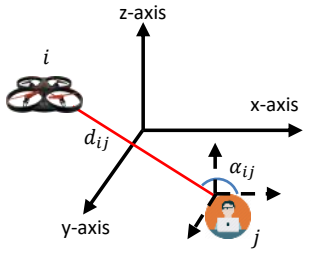


Fig. 2: Illustration of the UAV-node distance and angle.

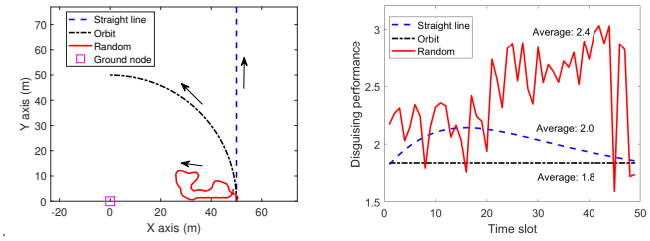
Let α_{ij} denote the angle between two vectors: the x-axis (which is agreed and pre-stored by all the UAVs for global reference) and the vector connecting UAV i and node j; see Fig. 2. The disguising performance is modelled as a weighted sum of the amplitudes of the derivatives of the UAV-node angle and distance, i.e.,

$$g_{ij}(t) = \eta|\dot{\alpha}_{ij}(t)| + |\dot{d}_{ij}(t)|, \tag{7}$$

where $\eta > 0$ weights the importance of the angular and distance aspects. As shown in (7), when node j looks at UAV i, the UAV appears to move in different directions with significant changes in their relative angle and distance. Then, the UAV does not look suspicious. The disguising performance is unitless. A larger value of (7) indicates a better disguising performance. We compare several typical movement patterns in terms of disguising performance, including straight line, orbit, and random movement, as shown in Fig. 3a. For the random pattern, the UAV randomly selects a turning direction. As shown in Fig. 3b, the average disguising performance of the random movement is much higher than that of the other two movement patterns. This is consistent with the common sense that the random movement can better hide the intention than the straight line and the arc trajectories. To this end, the proposed metric (7) is reasonable. As mentioned in Section I, to the best of our knowledge, no existing model is available to model the disguising performance. The proposed model (7) is the first of the kind.

The following objective function is specified to maximize the overall disguising performance of the UAVs over the time interval $[kT, (k+1)T]$ ($k = 0, 1, \ldots$):

$$\max_{\mathbf{p}_1(t),\cdots,\mathbf{p}_N(t)} \sum_{i=1}^{N}\sum_{j=1}^{M} \frac{1}{D_i}\int_{kT}^{(k+1)T} \eta\left(|\dot{\alpha}_{ij}(t)| + |\dot{d}_{ij}(t)|\right)dt, \tag{8}$$



(a) (b)

Fig. 3: (a) Typical movement patterns: straight line, orbit, random. (b) The disguising performance by the metric (7). The average values of the three movements are 2.0 (straight line), 1.8 (arc) and 2.4 (random), respectively, where $\eta = 1$.

Here, we use $\frac{1}{D_i}$ as the weight of UAV i. This is because that a large UAV should make more effort to disguise itself than a small UAV, since the former is more noticeable than the latter.

Problem Statement: We focus on an eavesdropping trajectory planning problem. Given the locations of nodes $\mathbf{q}_j$ $(j = 1, \ldots, M)$ and K, T, C, d_{safe}, D_i, $V_i^{\max}$, $W_i^{\max}$ and $U_i^{\max}$ $(i = 1, \ldots, N)$, we plan the trajectory for each UAV at each time interval $[kT, (k+1)T]$ $(k = 0, 1, \ldots, K)$ to maximize the objective function (8), subject to the instantaneous eavesdropping requirement (4), collision avoidance (5), the requirement of keeping an average distance away from the ground nodes (6), and the mobility constraint (1). In other words, given the locations of the ground nodes, we optimize the trajectories for a UAV team so that the UAVs can decode the collected data, disguise their eavesdropping intention, and fly safely.

Note that the system parameters D_i $(i = 1, \ldots, N)$ impact the disguising performance and C impacts the eavesdropping performance. When these parameters are not well selected, the considered problem may be infeasible. In such a case, instead of adjusting the parameter C, we can use smaller UAVs and then reduce the parameters of $D_1, \ldots, D_N$. Since smaller UAVs have better disguising ability, we can set smaller values for $D_1, \ldots, D_N$, which enlarge the solution space.

In the considered trajectory optimization problem, the UAVs are not required to reach some desired positions at the end of the operation, which is different from the common goal of the conventional UAV path planning problem [40]. It is also different from the path planning problem in typical search-and-rescue or search-and-track scenarios, which needs to produce trajectories for UAVs to traverse a certain space [41]. Moreover, our eavesdropping mission can be conducted collaboratively by the UAV team even when all the UAVs are relatively far from a target. This is different from video surveillance that requires a target to be within the view of a UAV [42], [43], i.e., at least one UAV should be close enough to the target, in the collaborative radio surveillance problem. These features make this paper distinct to the existing literature.

IV. Trajectory Planning Method

Problem of (8), subject to constraints (1), (4), (5) and (6), is intractable and cannot provide analytical solutions for the following reasons. The absolute value operator in (8) makes the problem non-differentiable. Both $|\dot{\alpha}_{ij}(t)|$ and $|\dot{d}_{ij}(t)|$ are non-convex with respect to $(x_i(t), y_i(t), z_i(t))$. Moreover, since each UAV has three control variables $v_i(t)$, $w_i(t)$ and $u_i(t)$, the solution space of the problem is $O(3^N)$ during an interval if the solution space remains unchanged. This can degrade the disguising performance, and the ground nodes may detect the UAVs' intention with a high probability. Thus, $v_i(t)$, $w_i(t)$ and $u_i(t)$ are expected to vary, to improve the disguising performance. This leads to a much larger solution space than $O(3^N)$ and, in turn, makes problem (8) more complex. To address this challenging problem, we present a new randomized method based on RRT [44] to construct the UAVs' trajectories efficiently.

We first discretize the interval $[kT, (k+1)T]$ into L small slots with equal lengths τ, i.e., $T = L\tau$. Without loss of generality, we focus on the trajectory planning for the interval $[0, T]$. The objective function and the constraints of the considered problem can be rewritten, as follows:

$$\max_{\mathbf{p}_1(l\tau), \cdots, \mathbf{p}_N(l\tau)} \sum_{i=1}^{N} \sum_{j=1}^{M} \sum_{l=1}^{L} \frac{1}{D_i} (\eta |\alpha_{ij}(l\tau) - \alpha_{ij}((l-1)\tau)| + |d_{ij}(l\tau) - d_{ij}((l-1)\tau)|), \tag{9}$$

$$F_j(l\tau) \geq C, \ \forall l, \ \forall j, \tag{10}$$

$$\delta_{ih}(l\tau) \geq d_{\text{safe}}, \ \forall l, \ \forall i \neq h, \tag{11}$$

$$\frac{1}{L} \sum_{l=1}^{L} d_{ij}(l\tau) \geq D_i, \ \forall i, \ \forall j. \tag{12}$$

The UAV dynamic model can be discretized and simplified as:

$$\begin{cases} x_i(l\tau) = x_i((l-1)\tau) + V_i^{max} \cos(\theta_i((l-1)\tau)), \\ y_i(l\tau) = y_i((l-1)\tau) + V_i^{max} \sin(\theta_i((l-1)\tau)), \\ z_i(l\tau) = z_i((l-1)\tau) + w_i((l-1)\tau), \\ \theta_i(l\tau) = \theta_i((l-1)\tau) + u_i((l-1)\tau), \\ Z_{min} \leq z_i(l\tau) \leq Z_{max}, \\ w_i((l-1)\tau) \in \{-W_i^{max}, 0, W_i^{max}\}, \\ u_i((l-1)\tau) \in \{-U_i^{max}, 0, U_i^{max}\}, \end{cases} \tag{13}$$

for $l = 1, \ldots, L$. Compared to (1), V_i^{max} in (13) is given. $u_i((l-1)\tau)$ and $w_i((l-1)\tau)$ in (13) have three options at interval $(l-1)\tau$, respectively. This simplifies the control of UAVs and also reduces the solution space significantly.

The trajectories of the UAVs are planned by repeatedly solving problem (9), subject to constraints (10) – (13), for K intervals. Having the initial positions and headings of the UAVs, a set of trajectories per interval (with L slots) are constructed. With the positions and headings of the UAVs at the end of the L-th slot, which are the initial status of the next interval, the trajectories for the next L slots are constructed. Planning the trajectories for L slots is a core of constructing the whole trajectories.

The developed method is summarized in Algorithm 1. A random tree for each UAV with its initial status as the root is constructed by randomly placed R samples. Specifically,

Algorithm 1 Trajectory Planning Algorithm.

1: **for** $i = 1, \cdots, N$ **do**
2: Construct RRT for UAV i.
3: Select β trajectories with L consecutive vertices from the RRT satisfying (12), i.e., $\mathcal{T}_i$.
4: **end for**
5: **for** $\kappa = 1, \ldots, \gamma$ **do**
6: Randomly select a trajectory from each of $\mathcal{T}_i$, $i = 1, \cdots, N$.
7: **if** (10) and (11) are satisfied by these trajectories **then**
8: Record them with the corresponding objective function value (9).
9: **end if**
10: **end for**
11: Find the recorded combination that has the largest objective function value.

for UAV i, the samples are placed in a cylinder centred at the current location of the UAV with the horizontal radius of $V_i^{max}T$ and height of $2U_i^{max}T$. Starting from the root, β number of trajectories with L consecutive vertices from the random tree are selected. Some of them may be so close to the root that constraint (12) is not satisfied by these trajectories. These invalid trajectories are precluded. Let $\mathcal{T}_i$ denote the set of valid trajectories satisfying (12) for UAV i. For N UAVs, there are N sets of valid trajectories. Then, one trajectory is randomly selected from each set, which makes a combination of trajectories. For each combination, constraints (10) and (11) are assessed for each slot l. If they are satisfied, we say this combination of trajectories is valid. Then, the objective function (9) is evaluated. Among γ number of combinations, the one maximizing (9) can be identified.

Note that constraint (10) requires the UAVs to be close to the nodes, while constraint (12) requires the UAVs to be far away. Given C, the parameters $D_1, \ldots, D_N$ can make the problem infeasible. Nevertheless, $D_1, \ldots, D_N$ can be adjusted periodically for the feasibility of the problem. For example, when the ground nodes become too close to each other and reduce their transmit power, we can reduce the values of $D_1, \ldots, D_N$ and allow the UAVs to be closer to the nodes.

Also note that, apart from the mathematical intractability of the constrained problem (9), another reason for designing the RRT-based method is its potential decentralized implementation. Specifically, the RRT is an algorithm designed to efficiently search a space by constructing a space-filling tree incrementally from samples drawn randomly from the space. In other words, each UAV can produce the tree of possible trajectories for any UAV (including itself), given the samples from the space and the current position of the latter UAV. To this end, we can pre-sample the space and pre-store the samples at all UAVs. By only observing the positions of itself and the others, each UAV can independently produce consistent trees of possible trajectories for all UAVs. The best set of trajectories, one from each of the trees, can be consistently identified in a decentralized fashion.

It is worth pointing out that the proposed RRT-based navigation method inherits the randomness in the trajectory generation. It takes into account the UAVs' dynamic model (1) when constructing the trajectories. Compared to completely random trajectories which are effective for disguising, the proposed method further considers constraints (4), (5) and (6), which guarantee that during the movement, the eavesdropping on the ground nodes is effective and the UAVs keep away from each other for safety. It is also worth pointing out that the proposed method can be straightforwardly extended to avoid stationary or moving obstacles. This can be achieved by simply removing samples that encounter any obstacles from the generated random trees in Line 2 of Algorithm 1.

Finally, we analyze the computational complexity of evaluating one of the combinations. The results returned by Algorithm 1 are a set of N trajectories for the N UAVs. Each trajectory is designed for the future L slots. For each set of the trajectories, the first operation is to verify the flight safety of the UAVs for collision avoidance. At any slot l, the distance between any two UAVs is no shorter than d_{safe}. Since we have N UAVs and L slots, it takes $O(LN^2)$ time to verify whether the positions of the UAVs satisfy constraint (11) at any slot. Regarding the verification of the eavesdropping performance, i.e., constraint (10), for any ground node j at any slot l, it takes $O(N)$ time to compute $F_j(t)$, as all the N UAVs contribute to the eavesdropping. Given the M nodes and L slots, the complexity is $O(LMN)$. Therefore, it takes $O(LMN+LN^2)$ to check whether constraints (10) and (11) are satisfied by this combination. Furthermore, to evaluate the objective function (9), it takes $O(LMN)$ time. Then, the complexity to evaluate a combination is $O(LMN + LN^2)$. For the random tree construction part, the complexity of constructing one RRT (line 2) by randomly placing a number of R samples is $O(R^2)$. The complexity of selecting β trajectories from each RRT satisfying constraint (12), i.e., line 3, is at least $O(\beta L)$, since some randomly selected trajectories may not meet constraint (12). As a result, the total complexity of Algorithm 1 is $O(NR^2 + \beta NL + \gamma LMN + \gamma LN^2)$.

V. Simulation Results

We present the simulation results of the proposed technique. The maximum angular speed is 1 rad/s and the maximum vertical speed is 10 m/s for all the UAVs. $d_{\text{safe}} = 20$ m, $C = 3$ dB, $\eta = 10$, $P = 20$ dBm, $\sigma_0^2 = -80$ dBm, $K = 10$, $L = 15$, and each slot is 1 second. $Z_{\text{min}} = 200$ m and $Z_{\text{max}} = 600$ m. We place $R = 5000$ random samples to construct an RRT, $\beta = 20$ trajectories are selected from each RRT, and $\gamma = 100$ combinations tested for each interval.

Simulations are conducted on the simulator platform CoppeliaSim. The UAVs on the platform can be controlled by MATLAB via a built-in API. The simulation fowchart is shown in Fig. 4. The simulation starts from the MATLAB side by calling the functions of remApi() and simxStart(). We set a certain simulation time. During the simulation time, Algorithm 1 constructs the UAVs' trajectories. The trajectories are exported to CoppeliaSim via the command of simxSetObjectPosition(). Then, in CoppeliaSim, we simulate the UAVs' ights with the embedded controller. The UAVs' positions are then sent back to MATLAB script by the command simxGetObjectPosition().

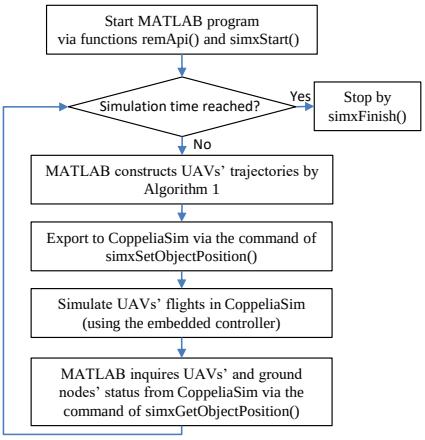
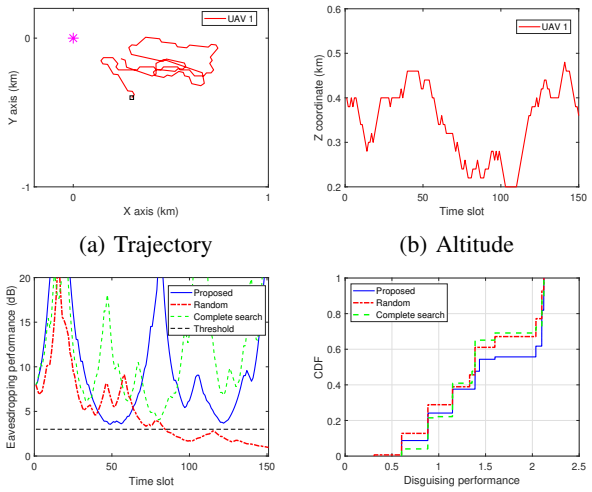


Fig. 4: The flowchart of the MATLAB-CoppeliaSim simulation of the proposed method, where MATLAB scripts are imported to CoppeliaSim to simulate the movement of the UAVs and eavesdropping results are returned to MATLAB for performance analysis.



(a) Trajectory (b) Altitude

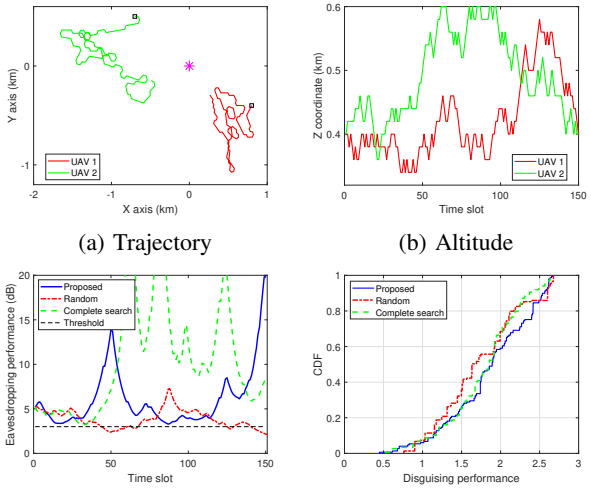
(c) Eavesdropping performance (d) Disguising performance

Fig. 5: One UAV and one node (Case 1).

When the simulation time is reached, we stop the simulation by simxFinish().

To evaluate the proposed method, we compare it with the following two benchmark methods:

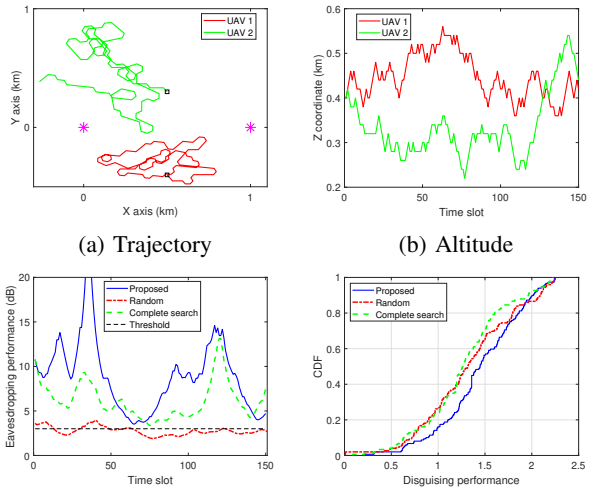
- The first benchmark method, referred to as "random", follows [17] to allow the UAVs to fly completely randomly, where each UAV can randomly select its moving direction. Generally speaking, such a movement comes with covertness, and the targets are least likely to connect the UAVs with an eavesdropping or monitoring mission (as compared to structured movements with recognizable patterns).
- The second benchmark, referred to as "complete search", searches all the feasible paths generated by all the possible control inputs defined in (13). There are a total of 9 control input combinations for each UAV i, accounting for three possible options for each of the horizontal angular speed and the vertical speed, and one possible option for the linear speed. This benchmark is deterministic, and is expected to provide the optimal solution to the considered problem under the discretization (13) at the cost of a high computational complexity. This method can find the paths which offer good disguising performance and guarantee the eavesdropping performance.



(a) Trajectory (b) Altitude

(c) Eavesdropping performance (d) Disguising performance

Fig. 6: Two UAVs and one node (Case 2).



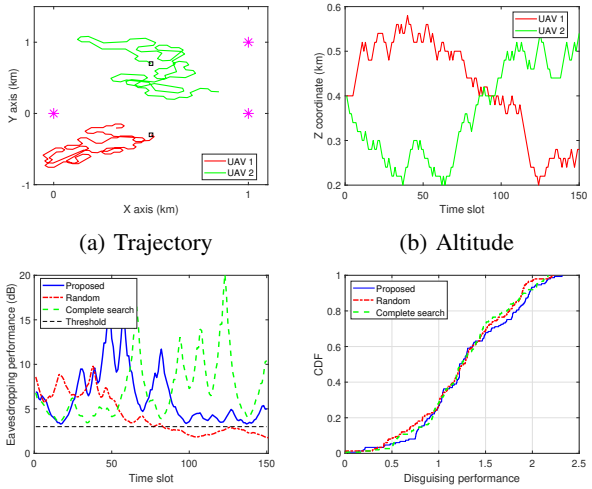
(a) Trajectory (b) Altitude

(c) Eavesdropping performance (d) Disguising performance

Fig. 7: Two UAVs and two nodes (Case 3).

By comparing with the two benchmarks, our algorithm is compared against the best possible covertness performance (i.e., random), and the best possible covertness under guaranteed eavesdropping performance (i.e., complete search).

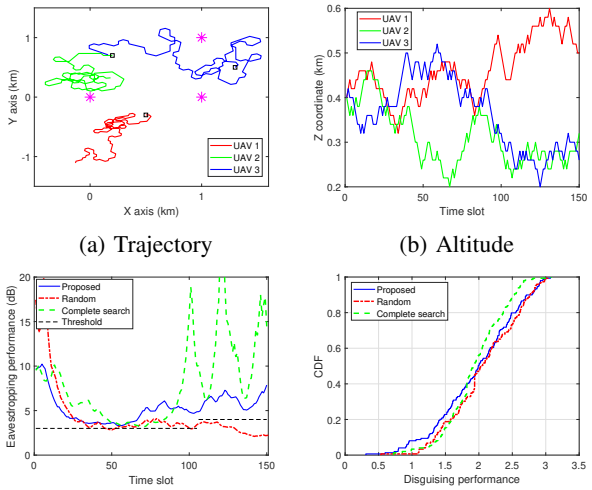
We start with a simple case of a single UAV and a single node. The maximum linear speed $V_1^{\max} = 30$ m/s and $D_1 = 400$ m. The horizontal movement of the UAV is shown in Fig. 5a, where the black square is the initial position. The altitude is shown in Fig. 5b. Fig. 5c shows that the eavesdropping rate at any time is over C. The cumulative density function (CDF)



(a) Trajectory (b) Altitude

(c) Eavesdropping performance (d) Disguising performance

Fig. 8: Two UAVs and three nodes (Case 4).

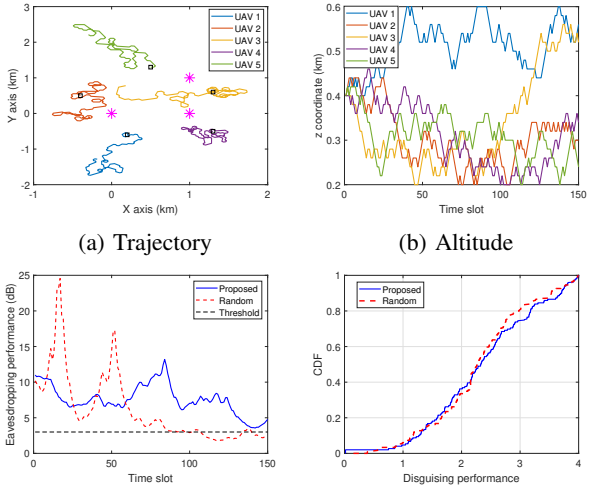


(a) Trajectory (b) Altitude

(c) Eavesdropping performance (d) Disguising performance

Fig. 9: Three UAVs and three nodes (Case 5).

of the corresponding disguising performance is shown in Fig. 5d. For the same node, we also consider two UAVs, where $V_1^{\max} = 30$ m/s, $V_2^{\max} = 25$ m/s, $D_1 = 400$ m, and $D_2 = 350$ m. The eavesdropping performance is much better than the single-UAV case (see Fig. 6c), and the disguising performance is improved as shown in Fig. 6d. We further consider a case with two UAVs and two nodes, and a case with two UAVs and three nodes. Compared to Figs. 6c and 6d, with an increasing number of nodes, both the eavesdropping performance and the disguising performance decrease (see Figs. 7c and 8c, and Figs. 7d and 8d). In the case of three nodes, we add one more UAV and the simulation results are shown in Fig. 9, where $V_3^{\max} = 20$ m/s and $D_3 = 300$ m. Clearly, adding a UAV improves both the eavesdropping performance and the disguising performance. Another set of the simulation results under five UAVs and three nodes is presented in Fig. 10. Compared to the case shown in Fig. 9, having two more UAVs can significantly improve the eavesdropping performance; see



(a) Trajectory (b) Altitude

(c) Eavesdropping performance (d) Disguising performance

Fig. 10: Five UAVs and three nodes (Case 6).

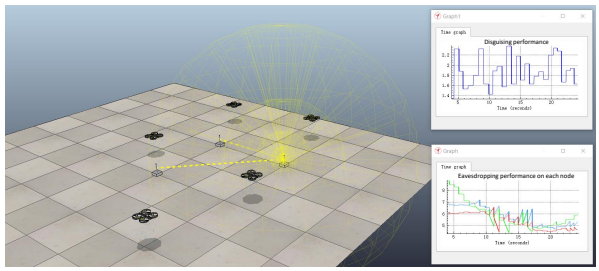


Fig. 11: A screenshot of the simulation for five UAVs and three ground nodes (Case 6). The graphs on the right show the disguising performance and the eavesdropping performance of each node. A video recording the movements of the UAVs is available: https://youtu.be/80l9vq7GPws. Other recordings are available at https://youtu.be/f3adKTWqDIA and https://youtu.be/mEYe-o5l5BA.

Figs. 9c and 10c. When $N > 1$, we only show the lowest eavesdropping performance on the nodes in Figs. 7c, 8c and 9c. As long as a curve in these figures is above the threshold C, the collaborative eavesdropping is effective. From these simulations, we see that the proposed method guarantees that the worst-case eavesdropping is still above the given threshold. To better illustrate the movements of the UAVs under the navigation of the proposed method, we record the simulation in CoppeliaSim for the case with five UAVs. A video link is available at the caption of Fig. 11.

In Fig. 5c, we see that the random movements of UAVs fail to satisfy the eavesdropping requirement at some times, since the corresponding curves fall below the given threshold C. The collaborative eavesdropping is effective if the curves remain above C. This can also be observed later in Figs. 6c, 7c, 8c, 9c and 10c. Like the proposed method, the UAV trajectories generated by the complete search method also ensure the effective eavesdropping. In the case with five UAVs, only the random method is used for comparison, as the complete search method is computationally prohibitive and

TABLE II: Result summary. E stands for eavesdropping performance, i.e., the ratio of successful eavesdropping in the whole duration, and D stands for the average disguising performance in the whole duration.

Case	Metric	Proposed	Random method	Complete search
1	E	1	0.55	1
	D	1.52	1.64	1.65
2	E	1	0.20	1
	D	2.02	2.11	2.14
3	E	1	0.81	1
	D	1.63	1.68	1.72
4	E	1	0.52	1
	D	1.45	1.48	1.51
5	E	1	0.67	1
	D	2.11	2.18	2.22
6	E	1	0.87	-
	D	2.52	2.60	-

cannot produce the result within a reasonable timeframe. In Fig. 5d, we see that the complete search method achieves better disguising performances than the proposed method (as can also be observed later in Figs. 6d, 7d, 8d and 9d). The reason is that the proposed method randomly tests a subset of trajectories, instead of all the possible trajectories (as tested in the complete search method). The simulation results of the eavesdropping performance and the disguising performance of the above cases are summarized in TABLE II. In particular, for the eavesdropping performance, we count the ratio of successful eavesdropping in the simulations. For the disguising performance, we present the average value of (7). Clearly, the proposed method achieves the ratio of 1 in terms of eavesdropping performance, and the disguising performance is very close to the benchmark methods. In other words, the proposed method enables UAVs to successfully eavesdrop on the ground nodes with comparable disguising performance. We note that the parameters in the proposed method can be adjusted during the trajectory construction process. For example, in Fig. 9, we can adjust the parameter of the eavesdropping requirement during the simulation. Specifically, in the first 105 slots, the parameter $C = 3$ and in the next 45 slots, it is set as 4; see Fig. 9c. Clearly, the proposed method can construct the UAVs' trajectories to satisfy the increased eavesdropping requirement.

A better disguising performance is achieved at the cost of runtime, as shown in TABLE III. The runtime is measured at a PC with Intel Core i7-7500U CPU using MATLAB. The proposed method has an affordable runtime (less than 1 second for the considered cases), while the complete search method takes dramatically longer. For example, when $M = 4$, $N = 3$ and $L = 20$, the complete search method takes about 20 minutes to find the optimal solution. Moreover, the complete search method cannot solve large-scale problems, e.g., $M = 3$, $N = 4$ and $L = 15$, within a reasonable time.

We test the complexity of Algorithm 1 in terms of floating point operations using a MATLAB FLOPs tool[2] by evaluating both the path combination and the RRT generation of the algorithm. The results are summarized in TABLE IV. When M is fixed, the number of floating point operations to assess a path combination increases with N. When N is fixed, the number of of floating point operations increases linearly. For the RRT generation of Algorithm 1, the complexity depends on the number of random samples placed in the field, rather than M, N and L. As shown in TABLE IV, the number of floating point operations increases significantly with the number of samples (R), and is much larger than that of the path evaluation. To this end, the complexity of the algorithm is dominated by the RRT generation and depends on the number of UAVs. As listed in [45, Tab. IV], a Qualcomm Snapdragon Flight is equipped with a Qualcomm Adreno 330 GPU with 167GFLOPs. Constructing an RRT with 5000 samples (2.6 giga floating point operations) at such a UAV only takes 0.015 seconds. The proposed method meets the needs of an actual large scene with an acceptable delay.

Now, we discuss the impact of C, N and M on the average disguising performance of the proposed method. We consider the disguising performance of a UAV on a node over 100 independent simulations. We first consider C, and the rest of the parameters remain the same as the above case of three UAVs and three nodes. With the increase of C, the average disguising performance decreases (see Fig. 12a). Since the eavesdropping performance decreases with an increasing distance between the UAV and the node, the increase of C leads to a smaller feasible movement space of the UAV. This phenomenon is more likely to worsen the disguising performance. For the impact of N, we keep $C = 3$ and $M = 3$. As shown in Fig. 12b, increasing UAVs in the system can significantly improve the average disguising performance when the number of UAVs is relatively small. In the presence of a large number of UAVs, the disguising performance improves slightly with a further increase of the UAV number. The reason is that with more UAVs in the system, the eavesdropping workload is reduced, so that the UAVs can make more effort to disguise their intention. When

TABLE III: Computation time (in seconds).

$N = 3$	L	5	10	15	20
$M = 3$	Proposed	0.47	0.52	0.56	0.63
	Complete search	2.58	30.62	189.56	1134.63
$L = 15$	N	1	2	3	4
$M = 3$	Proposed	0.46	0.52	0.63	0.85
	Complete search	52.67	118.43	189.56	-
$L = 15$	M	1	2	3	4
$N = 3$	Proposed	0.41	0.53	0.63	0.92
	Complete search	48.52	103.56	189.56	-

TABLE IV: Number of floating point operations (FPOs) for evaluating a path combination under different numbers of UAVs (N) and nodes (M), and for constructing a random tree with different numbers of samples (R).

Evaluating a path combination in line 8 of Algorithm 1

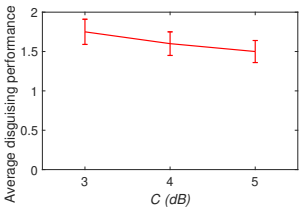
$M = 4$	N	3	4	5	6	7	8
	FPOs	2630	3835	5220	6900	8700	11000
$N = 3$	M	3	4	5	6	7	8
	FPOs	2194	2630	3100	3560	4120	4710

Constructing a random tree for one UAV in line 2 of Algorithm 1

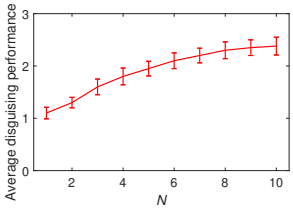
R	1000	2000	3000	4000	5000	6000
Giga FPOs	0.34	0.71	1.2	1.8	2.6	3.5

[2]https://www.mathworks.com/matlabcentral/fileexchange/50608-counting-the-floating-point-operations-flops

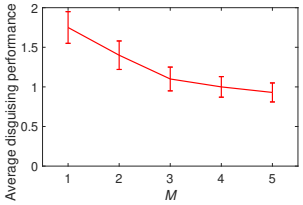
the number of UAVs is sufficient, adding extra UAVs does not help much in terms of disguising, but the eavesdropping performance improves. As shown in Fig. 12c, the disguising performance degrades with an increasing number of ground nodes. The reason is that with more ground nodes in the system, the eavesdropping burden of UAVs increases. Thus, the eavesdropping performance degrades. Therefore, for a given number of ground nodes, we can select the number of UAVs according to the expected disguising performance. Such selection should also consider the gain in disguising performance and system cost.



(a) The impact of C



(b) The impact of N



(c) The impact of M

Fig. 12: Impacts of several parameters on disguising.

VI. Conclusion

In this paper, we used UAVs to collaboratively and secretively eavesdrop on a set of stationary ground nodes. We proposed a new measure to quantify the disguising performance, and formulated a new optimization problem that maximizes the disguising performance subject to the eavesdropping performance, the collision avoidance, and the aeronautic maneuverability. A randomized method based on RRT was developed to construct the trajectories. It can achieve better eavesdropping performance than the random movement method without compromising the disguising performance. The proposed method achieves close disguising performance with the complete search algorithm at much shorter computation time. As an extension of the current results, collaboratively and covertly eavesdropping on moving ground nodes will be considered. Another future activity is to carry out outdoor experiments to verify the proposed method.

References

[1] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[2] D. Ma, Y. Li, X. Hu, H. Zhang, and X. Xie, "An optimal three-dimensional drone layout method for maximum signal coverage and minimum interference in complex pipeline networks," *IEEE Transactions on Cybernetics*, pp. 1–9, 2020.

[3] S. Shakoor, Z. Kaleem, M. I. Baig, O. Chughtai, T. Q. Duong, and L. D. Nguyen, "Role of UAVs in public safety communications: Energy efficiency perspective," *IEEE Access*, vol. 7, pp. 140 665–140 679, 2019.

[4] S. Zeng, H. Zhang, K. Bian, and L. Song, "UAV relaying: Power allocation and trajectory optimization using decode-and-forward protocol," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018, pp. 1–6.

[5] Y. Chen, W. Feng, and G. Zheng, "Optimum placement of UAV as relays," *IEEE Communications Letters*, vol. 22, no. 2, pp. 248–251, Feb 2018.

[6] S. Zhang, H. Zhang, Q. He, K. Bian, and L. Song, "Joint trajectory and power optimization for UAV relay networks," *IEEE Communications Letters*, vol. 22, no. 1, pp. 161–164, 2018.

[7] 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.

[8] H. Lei, D. Wang, K. Park, I. S. Ansari, J. Jiang, G. Pan, and M. Alouini, "Safeguarding UAV IoT communication systems against randomly located eavesdroppers," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1230–1244, 2020.

[9] H. Huang, A. V. Savkin, and W. Ni, "Energy-efficient 3D navigation of a solar-powered UAV for secure communication in the presence of eavesdroppers and no-fly zones," *Energies*, vol. 13, no. 6, p. 1445, 2020.

[10] A. V. Savkin, H. Huang, and W. Ni, "Securing UAV communication in the presence of stationary or mobile eavesdroppers via online 3D trajectory planning," *IEEE Wireless Communications Letters*, pp. 1–5, 2020.

[11] 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, Sep. 2018.

[12] M. Hua, Y. Wang, Q. Wu, H. Dai, Y. Huang, and L. Yang, "Energy-efficient cooperative secure transmission in multi-UAV-enabled wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7761–7775, 2019.

[13] Y. Cai, F. Cui, Q. Shi, M. Zhao, and G. Y. Li, "Dual-UAV-enabled secure communications: Joint trajectory design and user scheduling," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1972–1985, Sep. 2018.

[14] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9385–9392, 2018.

[15] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, "UAV-enabled secure communications: Joint trajectory and transmit power optimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 4069–4073, 2019.

[16] G. Hu and Y. Cai, "UAVs-assisted proactive eavesdropping in AF multi-relay system," *IEEE Communications Letters*, vol. 24, no. 3, pp. 501–505, 2020.

[17] X. Yuan, Z. Feng, W. Ni, R. P. Liu, J. A. Zhang, and W. Xu, "Secrecy performance of terrestrial radio links under collaborative aerial eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 604–619, 2019.

[18] 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.

[19] J. Ye, C. Zhang, H. Lei, G. Pan, and Z. Ding, "Secure UAV-to-UAV systems with spatially random UAVs," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 564–567, 2018.

[20] G. Pan, H. Lei, J. An, S. Zhang, and M. S. Alouini, "On the secrecy of UAV systems with linear trajectory," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6277–6288, 2020.

[21] J. Tang, G. Chen, and J. P. Coon, "Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 3026–3041, 2019.

[22] J. Hu, H. Zhang, K. Bian, L. Song, and Z. Han, "Distributed trajectory design for cooperative internet of UAVs using deep reinforcement learning," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–6.

[23] W. Li, L. Wang, and A. Fei, "Minimizing packet expiration loss with path planning in UAV-assisted data sensing," *IEEE Wireless Communications Letters*, vol. 8, no. 6, pp. 1520–1523, 2019.

[24] E. Galceran and M. Carreras, "A survey on coverage path planning for robotics," *Robotics and Autonomous systems*, vol. 61, no. 12, pp. 1258–1276, 2013.

[25] H. Oh, S. Kim, H.-s. Shin, and A. Tsourdos, "Coordinated standoff tracking of moving target groups using multiple UAVs," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 51, no. 2, pp. 1501–1514, 2015.

[26] J. Keller, D. Thakur, M. Likhachev, J. Gallier, and V. Kumar, "Coordinated path planning for fixed-wing UAS conducting persistent surveillance missions," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 1, pp. 17–24, 2016.

[27] M. V. Srinivasan and M. Davey, "Strategies for active camouflage of motion," *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 259, no. 1354, pp. 19–25, 1995.

[28] R. Strydom and M. V. Srinivasan, "UAS stealth: target pursuit at constant distance using a bio-inspired motion camouflage guidance law," *Bioinspiration & Biomimetics*, vol. 12, no. 5, p. 055002, 2017.

[29] A. V. Savkin and H. Huang, "Bioinspired bearing only motion camouflage UAV guidance for covert video surveillance of a moving target," *IEEE Systems Journal*, pp. 1–4, 2020.

[30] Y. Xu, "Analytical solutions to spacecraft formation-flying guidance using virtual motion camouflage," *Journal of Guidance, Control, and Dynamics*, vol. 33, no. 5, pp. 1376–1386, 2010.

[31] J. Kim, "Three-dimensional discrete-time controller to intercept a targeted UAV using a capture net towed by multiple aerial robots," *IET Radar, Sonar & Navigation*, vol. 13, no. 5, pp. 682–688, 2018.

[32] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, 2018.

[33] J. Farlik, M. Kratky, J. Casar, and V. Stary, "Radar cross section and detection of small unmanned aerial vehicles," in *2016 17th International Conference on Mechatronics-Mechatronika (ME)*. IEEE, 2016, pp. 1–7.

[34] M. Z. Anwar, Z. Kaleem, and A. Jamalipour, "Machine learning inspired sound-based amateur drone detection for public safety applications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2526–2534, 2019.

[35] J. Xie, J. Yu, J. Wu, Z. Shi, and J. Chen, "Adaptive switching spatial-temporal fusion detection for remote flying drones," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 6964–6976, 2020.

[36] Y. Kang and J. K. Hedrick, "Linear tracking for a fixed-wing UAV using nonlinear model predictive control," *IEEE Transactions on Control Systems Technology*, vol. 17, no. 5, pp. 1202–1210, 2009.

[37] 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, Feb 2019.

[38] A. S. Matveev, A. V. Savkin, M. Hoy, and C. Wang, *Safe robot navigation among moving and steady obstacles*. Elsevier, 2015.

[39] Y. Wu and K. H. Low, "An adaptive path replanning method for coordinated operations of drone in dynamic urban environments," *IEEE Systems Journal*, pp. 1–12, 2020.

[40] A. V. Savkin and H. Huang, "Optimal aircraft planar navigation in static threat environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 5, pp. 2413–2426, Oct 2017.

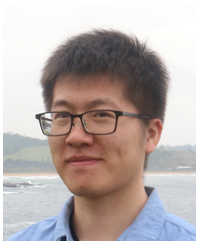
[41] Y. Wu, K. H. Low, and C. Lv, "Cooperative path planning for heterogeneous unmanned vehicles in a search-and-track mission aiming at an underwater target," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6782–6787, 2020.

[42] J. Wu, H. Wang, N. Li, P. Yao, Y. Huang, Z. Su, and Y. Yu, "Distributed trajectory optimization for multiple solar-powered UAVs target tracking in urban environment by adaptive grasshopper optimization algorithm," *Aerospace Science and Technology*, vol. 70, pp. 497–510, 2017.

[43] H. Huang and A. V. Savkin, "An algorithm of reactive collision free 3-D deployment of networked unmanned aerial vehicles for surveillance and monitoring," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 132–140, 2020.

[44] S. M. LaValle, "Rapidly-exploring random trees: A new tool for path planning," *Technique Report*, 1998.

[45] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1027–1070, 2020.



Hailong Huang received the B.Sc. degree in automation, from China University of Petroleum, Beijing, China, in 2012, and received Ph.D degree in Systems and Control from the University of New South Wales, Sydney, Australia, in 2018. He was a post-doctoral research fellow at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He is now an Assistant Professor at the Department of Aeronautical and Aviation Engineering, the Hong Kong Polytechnic University, Hong Kong. His current research interests include guidance, navigation, and control of mobile robots, multi-agent systems, and distributed control.

Andrey V. Savkin was born in 1965 in Norilsk, Russia. He received the M.S. and Ph.D. degrees in mathematics from the Leningrad State University, Saint Petersburg, Russia, in 1987 and 1991, respectively. From 1987 to 1992, he was with the Television Research Institute, Leningrad, Russia. From 1992 to 1994, he held a Postdoctoral position in the Department of Electrical Engineering, Australian Defence Force Academy, Canberra. From 1994 to 1996, he was a Research Fellow in the Department of Electrical and Electronic Engineering and the Cooperative Research Centre for Sensor Signal and Information Processing, University of Melbourne, Australia. From 1996 to 2000, he was a Senior Lecturer, and then an Associate Professor in the Department of Electrical and Electronic Engineering, University of Western Australia, Perth. Since 2000, he has been a Professor in the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW, Australia. His current research interests include robust control and state estimation, hybrid dynamical systems, guidance, navigation and control of mobile robots, applications of control and signal processing in biomedical engineering and medicine. He has authored/coauthored seven research monographs and numerous journal and conference papers on these topics. Prof. Savkin has served as an Associate Editor for several international journals.

Wei Ni M'09-SM'15) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. Currently, he is a Group Leader and Principal Research Scientist at CSIRO, Sydney, Australia, and an Adjunct Professor at the University of Technology Sydney and Honorary Professor at Macquarie University, Sydney. He was a Postdoctoral Research Fellow at Shanghai Jiaotong University from 2005 – 2008; Deputy Project Manager at the Bell Labs, Alcatel/Alcatel-Lucent from 2005 to 2008; and Senior Researcher at Devices R&D, Nokia from 2008 to 2009. His research interests include signal processing, stochastic optimization, learning, as well as their applications to network efficiency and integrity.

Dr Ni is the Chair of IEEE Vehicular Technology Society (VTS) New South Wales (NSW) Chapter since 2020 and an Editor of IEEE Transactions on Wireless Communications since 2018. He served first the Secretary and then Vice-Chair of IEEE NSW VTS Chapter from 2015 to 2019, Track Chair for VTC-Spring 2017, Track Co-chair for IEEE VTC-Spring 2016, Publication Chair for BodyNet 2015, and Student Travel Grant Chair for WPMC 2014.