Privacy-Preserving Path-Planning for UAVs

Saeede Enayati
Electrical and Computer Engineering
University of Massachusetts, Amherst
senayati@umass.edu

Dennis L. Goeckel
Electrical and Computer Engineering
University of Massachusetts, Amherst
dgoeckel@ecs.umass.edu

Amir Houmansadr
College of Information and Computer Sciences
University of Massachusetts, Amherst
amir@cs.umass.edu

Hossein Pishro-Nik
Electrical and Computer Engineering
University of Massachusetts, Amherst
pishro@umass.edu

***Abstract*—Because of their potential ubiquity, unmanned aerial vehicles (UAVs) are often viewed as a threat to people's privacy. However, the users of UAVs for applications such as package delivery can also have their own privacy compromised by observations of UAV behavior by an adversary. Hence, this paper looks at privacy-preserving path-planning for a UAV. In particular, we consider a UAV which is delivering a package or operating a service, e.g. a health-emergency service, for users while an adversary tries to infer the UAV's destination by observing its trajectory. We consider two models for the UAV motion for which we provide privacy-preserving path-planning mechanisms (PPPMs) while taking into account the UAV's energy consumption as well. We obtain the tradeoff between privacy and energy consumption guarantees and show that the proposed PPPMs not only satisfy the privacy guarantees but also meet the energy efficiency criteria.**

***Index Terms*—Privacy-preserving path-planning, UAV, trajectory, energy efficiency.**

I. Introduction

The promise of unmanned aerial vehicles (UAVs) has led to a rapid increase in their application areas, ranging from UAV-based wireless access points to search and rescue (SAR) and delivery operations [1]. In particular, using UAVs as a delivery mechanism is an interesting application with broad societal impact that has been under development by Amazon Prime Air delivery since 2013 [2]. Importantly, the UAVs might not only deliver commercial packages but also provide emergency and health-related services at the destinations [3].

Privacy can be defined in a number of ways, but the main idea is to protect users' identities from internal and external adversaries. And privacy in UAV applications can be investigated from several points of view. In fact, UAVs are often viewed as being a threat to users' privacy by providing a ubiquitous observation platform; however, their own privacy can be violated as well [4], which is the focus of this paper. Here, we consider the loss of privacy when UAV destinations may be undesirably identified by an adversary who is observing the UAV's path. In particular, we consider a scenario in which a UAV that is delivering packages or providing health services to residents is observed by an adversary. The adversary tries to identify the UAV's destination based on its trajectory. Hence, the goal is to manipulate the trajectory in a randomized way so that the adversary cannot simply infer the destination.

Thus, in the path privacy scenario considered here, there exists an agent or a set of agents (e.g., UAVs) that follow trajectories to achieve a certain goal G. A potential adversary can observe a portion or all of the trajectories (depending on the strength of the adversary) and is aiming to infer some sensitive information about the goal G.

For example, we might have a drone that delivers a package to a destination, and we may want to hide the delivery location from the adversary. If there were no privacy constraints, the drone might travel with an optimal speed along an approximately straight line from the source location X to the destination Y, drop the package, and return to X again on a straight line. However, due to the privacy concerns, we might have to deviate from the "optimal" path planning algorithm. Of course, we will pay some price for this in terms of energy consumption, delivery time, etc.

A. Related Work

As mentioned above, privacy may be compromised when UAVs monitor and obtain excess information about their operation area other than accomplishing their main task [5], [6]. In this regard, privacy in UAV applications has been extensively studied before [7]–[13]. In [7], [8], the authors provided an algorithm based on the physical stimulus and the corresponding change in the channel traffic in order to determine whether a point of interest (PoI) is being video streamed illegitimately. A central management system was proposed in [9] where given the restrictions and UAV's applications, it is in charge of the permission to the applications as well as monitoring the drone, in order to detect and handle violations at runtime. In [12] a novel detection system for privacy invasion caused by a customer drone was proposed based on the low-cost hardware and using RF signals under a non-line-of-sight (NLOS) condition. Through scrambling windows in images

This work was supported by NSF under grants CNS-1932326 and CNS-1739462.

and videos that UAVs are shooting during their mission, [13] proposed a method to prevent the violation of people's privacy.

For a UAV's trajectory, the authors in [10] proposed a privacy-aware path planning where, given the privacy-restricted zones, the optimal path for UAV is designed while collision avoidance and a time budget are considered. In [14], the number of UAV's movements is minimized given the private areas and differential permission of their owners.

On the other hand, UAVs can be under different kinds of privacy and security invasions as well [15]. In this regard, a machine learning (ML)-based attack was trained in [16] to decipher a UAV's location using both the encrypted location data that the UAV transmits and observing its actual location. To preserve privacy, [17] has proposed an authentication scheme based on hyperelliptic curve cryptography in order to design a low computation and communication cost privacy-preserving mechanism. A mutual authentication protocol for UAV-ground terminal and UAV-UAV authentication was proposed in [18] using physically unclonable functions. A path planning algorithm was proposed in [19] to protect UAV-ground station data transmission from an eavesdropper using a modified particle swarm optimization (PSO). [20] proposed a network-coding based pseudonym to provide privacy for the ground users' location data collected by drones and outsourced to an untrusted cloud database.

The most similar work to this paper is [21], where the authors proposed privacy-preserving path design algorithms for a UAV while there is an adversary trying to infer the UAV's destination from its path. The authors consider two scenarios: the adversary can and cannot see the destinations, and they propose path planning algorithms to hide the destinations from the adversary. Our work is different from [21] in several aspects discussed in the next section.

B. Contributions and Organization

Our goal is to develop privacy-preserving path planing mechanisms (PPPMs) that provide a satisfactory tradeoff between privacy and efficiency. Our work is different from [21] in the following ways:

- In contrast to the "Adversary Monitors Source Location" scenario in [21], we consider a scenario where all parts of the zone are observable by the adversary. In other words, there is no safe zone available and the adversary can observe the entire path.
- In contrast to the "Adversary Monitors Destinations" scenario in [21], which is closer to our formulation: (i) we consider a single destination scenario where the privacy is obtained independent of the other possible destinations; (ii) we define a privacy guarantee for the scenarios in hand and prove that it is achievable through the design parameters; and (iii) we consider the UAV's energy efficiency constraint as well as the privacy guarantee and investigate the existing tradeoff.

The problem considered in this paper is analogous to privacy in other areas, for example in social networks where the friendship links of users are anonymized in order to prevent further inference by adversaries [22]–[24]. Preserving location privacy of users when their data is shared for location-based services can be also thought of as another analogy to the presented problem [25]–[28]. Also, privacy of vehicle location data in which, for example, users' home addresses are preserved from being leaked [29], [30] can be thought of as a counterpart in transportation engineering.

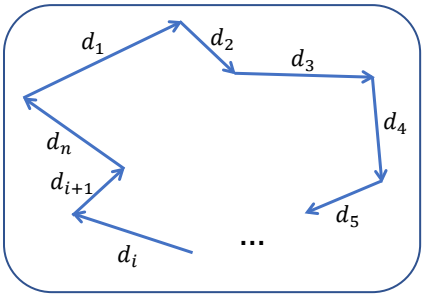

FIGURE 1: The piecewise linear paths

Note that throughout this paper, $||.||$ is the L_2 norm and $\mathbb{E}[.]$ is the expectation operator.

This paper is organized as follows: In Section II, we provide the first scenario descriptions and in Section III, we propose the corresponding PPPM. Subsequently, in Sections IV and V, we propose the second scenario and the corresponding PPPM, respectively. Finally, Section VI concludes the paper.

II. Scenario I: Piecewise Linear Path

In this section, we provide the first system model and assumptions in detail.

A. UAV's Trajectory Model

First we assume that the trajectory is a combination of linear segments. The goal is to design privacy-preserving trajectories that guarantee energy efficiency as well, and analyze the tradeoff between the two performance metrics. In this regard, we consider a drone which flies with constant speed in a piecewise linear paths with different lengths denoted by $d_i, i = 1, 2, \ldots, n$ as shown in Figure 1.

B. Adversary Model

We assume that the adversary can observe the entire path. However, he cannot observe the drone's speed. We also assume that the adversary has no prior knowledge about the destinations. In other words, before observing the path, from the adversary points of view, the destination is distributed uniformly in the area that includes the entire path. This assumption will be relaxed in the second scenario of the problem.

C. Energy Consumption Model

In this model, in order to analyze the energy consumption, we first define the energy consumption for a distance unit as $\mathcal{E}_0$. In other words, $\mathcal{E}_0$ is the energy consumed by the drone when traveling a distance unit with a constant speed, i.e., $\mathcal{E}_0 \stackrel{\triangle}{=} \mathcal{E}(d = 1)$. With this definition, the energy consumption of a path with length d_i is $\mathcal{E}_i = d_i \mathcal{E}_0$. Besides the energy on

the linear path, we also define an energy unit for a turning point. In this regard, we assume that the drone consumes ζ amount of energy when it changes its direction. Therefore, the total amount of energy in a path with n different line segments is obtained as

$$\begin{aligned}\mathcal{E}_T &= \sum_{i=1}^{n} d_i \mathcal{E}_0 + \sum_{j=1}^{n-1} \zeta \mathcal{E}_0 \\ &= \mathcal{E}_0 \left(\sum_{i=1}^{n} d_i + (n-1)\zeta \right).\end{aligned}$$

Now assume that the drone is supposed to travel from a source X to the destination Y on a single straight line of length d. In this scenario, the energy consumption of the UAV for a round trip is simply $\mathcal{E} = (2d + \zeta)\,\mathcal{E}_0$. Obviously, the adversary can easily infer the exact location of Y. Hence, $\tilde{Y} = Y$, where $\tilde{Y}$ is the adversary inference of Y. In the next section, we propose the privacy-preserving path planning for this scenario.

III. PPPM I: Fly a Random Triangle

In order to design a PPPM, we intend to randomize the trajectory. To do so, we define the random variable $\Theta \sim \arcsin\left[\frac{U(-l,l)}{d}\right]$ which is a deviation angle from the straight path. Figure 2 shows the schematic model of the privacy-preserving path. As shown in this figure, instead of the path $X - Y - X$, the drone goes along the path $X - Y_1 - Y_2 - X$. Intuitively, as the Θ increases, which is equal to a larger l, the path becomes longer which increases the privacy. On the other hand, the energy consumption increases as well.

Hence, in the next theorem, we obtain the privacy and energy consumption guarantees as a function of l. The privacy guarantee is defined as

$$\mathcal{G}_p \triangleq \text{Inf}\ \mathbb{E}||\tilde{Y} - Y||^2,$$

where Inf is taken over all estimators of Y. We also define the energy consumption guarantee as

$$\mathcal{G}_e \triangleq \mathbb{P}\left[\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} \geq 1 + \delta\right] = 0,$$

where $\mathcal{E}_p$ is the energy consumption of the proposed privacy-preserving path and $\mathcal{E}_{\text{Opt}}$ is the optimal energy consumption obtained when the drone travels through the $X - Y - X$ path. Also, δ is obtained in (4). Now we state the following theorem.

Theorem 1. For the proposed PPPM, the privacy and energy consumption guarantees can be obtained as

$$\text{Inf}\ \mathbb{E}||\tilde{Y} - Y||^2 \geq \frac{l^2}{3}, \tag{1}$$

and

$$\mathbb{P}\left[\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} \geq 1 + \delta\right] = 0, \tag{2}$$

respectively, where δ is obtained in (4).

Proof. For the proof of Equation (1), we first note that given the adversary's observation denoted by ψ, Y has a uniform distribution over the line $Y_1 - Y_2$, i.e., $Y|\psi \sim U[Y_1, Y_2]$. This is essentially resulted from the proposed privacy-preserving mechanism where we have assumed that $\Theta \sim \arcsin\left[\frac{U(-l,l)}{d}\right]$. Using the proposed definition of Θ and Figure 2, we have

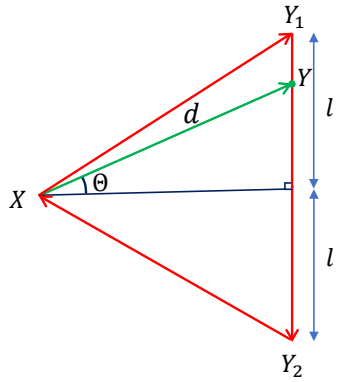

Figure 2: The privacy-preserving path and the corresponding parameters. The optimal path is shown by green arrow and the privacy-preserving path is shown by the red arrows.

$$\begin{aligned}\sin\Theta &= \frac{U(-l,l)}{d} \\ &= \frac{Y}{d},\end{aligned}$$

which gives us $Y \sim U(-l, l)$. In other words, the adversary is estimating a uniform random variable in the interval $(-l, l)$. Now, we note that considering a minimum mean squared error (MMSE) criterion, the best estimator is the mean value and the least estimation error is the variance, i.e.,

$$\mathbb{E}||\tilde{Y} - Y||^2 = \frac{(2l)^2}{12} = \frac{l^2}{3},$$

which completes the proof for Eq. (1).

To prove Eq. (2), we need to obtain the upper bound for $\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}}$ and the corresponding δ. To do so, we note that in the worst case scenario, the energy consumption is

$$\mathcal{E}_p = 2\sqrt{d^2 + l^2} + 2l + 2\zeta.$$

This is obtained since in the worst case scenario, Y is exactly in the middle of $Y_1 - Y_2$. Therefore, we can write the following equation

$$\begin{aligned}\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} &= \frac{2\sqrt{d^2 + l^2} + 2l + 2\zeta}{2d + \zeta} \\ &< \frac{2\sqrt{d^2 + l^2 + 2dl} + 2l + 2\zeta}{2d + \zeta} \\ &= \frac{2d + \zeta + 4l + \zeta}{2d + \zeta} \\ &= 1 + \frac{4l + \zeta}{2d + \zeta} \\ &= 1 + \delta.\end{aligned} \tag{3}$$

Therefore, we obtain

$$\delta = \frac{4l + \zeta}{2d + \zeta}, \tag{4}$$

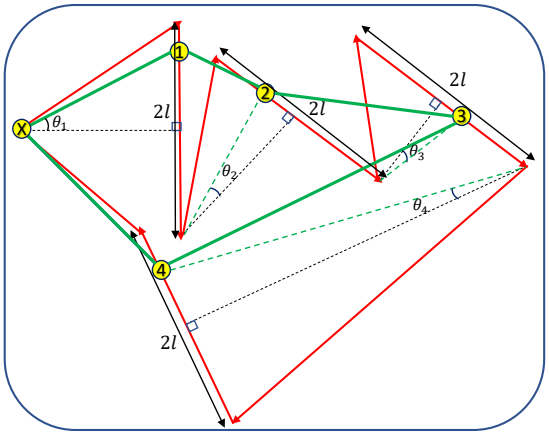

FIGURE 3: The extended PPPM I for a 4-destinations scenario. The green simple line path is the optimal path, the red arrowed path is the privacy-preserving path, the green dashed lines show the shortest path from each point to the next destination, and the black dotted lines are the vertical perpendicular to show the random parameter of the design algorithm, θ.

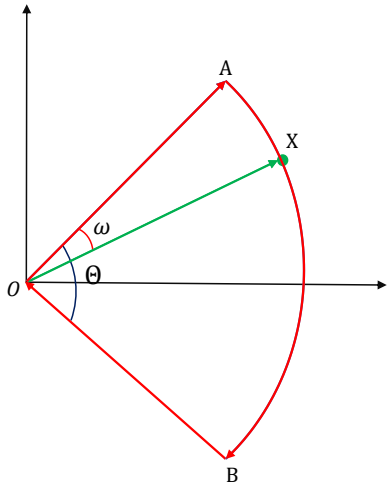

FIGURE 4: The privacy-preserving path mechanism: The green arrow is the optimal path, and the red arrows represent the privacy-preserving path.

and Eq. (2) is concluded. □

Discussion 1. Equations (1) and (2) represent a tradeoff between the privacy guarantee and energy consumption based on l, such that the larger the l is, the tighter the privacy guarantee becomes. However, this increases the upperbound of the energy efficiency, i.e., $1+\delta$, which is undesired. Hence, one needs to determine l such that a given privacy and energy guarantee are met.

Discussion 2. We can extend PPPM I to a multi-destination scenario where the UAV follows a trajectory similar to Figure 1. The difference is that, after completing its mission, the UAV moves toward the next destination through another privacy-preserving path from Y_2 in Figure 2 instead of returning to the origin X. Figure 3 shows the optimal and the extended PPPM I applied to a 4-destinations scenario. The detailed analysis for the multi-destination case is left for the longer version of this paper.

In the next section, we propose the second scenario and the corresponding PPPM.

IV. Scenario II: Curved Path

In this section, we provide the second system model. Again, the goal is to design privacy-preserving trajectories that guarantee energy efficiency as well, and analyze the tradeoff between the two performance metrics. In the following, we provide the assumptions for this scenario.

A. UAV's Trajectory Model

We assume that the drone can use any of the following two possible movements at each segment of its trajectory: (1) flying at a constant speed v_l on a linear line segment, or (2) flying at a constant speed v_c on a circular path. By a circular path, we mean an arc of a circle. It is assumed that v_c and v_l are given and are potentially determined to ensure an optimal operation.

B. Adversary Model

We assume that the adversary can observe the entire path. However, he cannot observe changes in the drone's speed. Hence, he cannot infer if the drone stops at a location. The adversary also has no prior/side information about the direction of the destination. Specifically, assuming a polar coordinate for destination point denoted by X, i.e., $X=(R,\theta_X)$, he has no information about θ_X. This means that before observing the path, from the adversaries perspective, θ_X is distributed uniformly in $[0,2\pi)$.

C. Energy Consumption Model

To model the energy consumption of the proposed system model, as before, we define $\mathcal{E}_0$ as the energy consumed by the drone when traveling a unit of distance on a straight line with the assumed constant speed, i.e., $\mathcal{E}_0 \triangleq \mathcal{E}(d=1)$. With this definition, the energy consumption of a path with length d_i is $\mathcal{E}_i = d_i\mathcal{E}_0$. Besides the energy on the linear path, we also define the energy consumption for the arc path. In particular, for an arc with angle θ and radius R, we model the energy consumption as below

$$\mathcal{E}_p(R,\theta) = \theta R k \mathcal{E}_0,$$

where $k \geq 1$ is due to the excess energy consumption resulting from the nonzero centripetal acceleration and a potential difference between v_l and v_c.

Without loss of generality, we assume that the drone is initially located at location $O(0,0)$ and is supposed to deliver a package to the destination at X. From the energy consumption perspective, the optimal way would be to travel from the source O to the destination X on a single straight line (length R). Hence, in this scenario, the energy consumption is simply $\mathcal{E}_{\text{Opt}} = 2R\mathcal{E}_0$.

Now, in the next section, we propose our PPPM for this scenario.

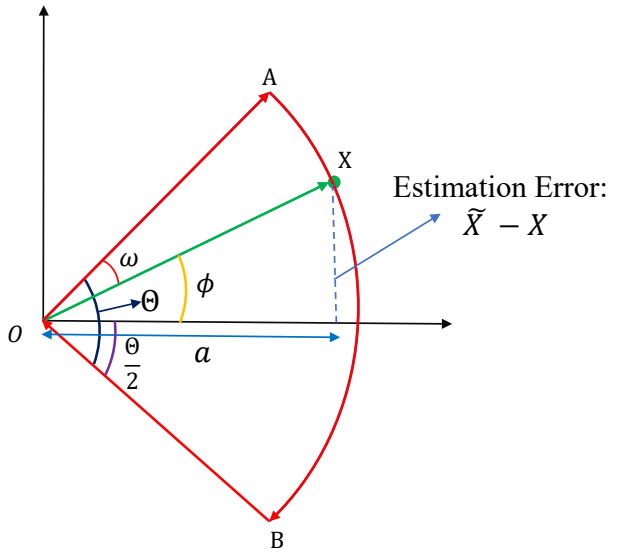

FIGURE 5: The privacy-preserving path for Scenario II and the corresponding parameters.

V. PPPM II: FLY A RANDOM ARC

In this part, we explain the randomization method used in the path-planning in order to provide a privacy-preserving path. The idea is to deviate the UAV's trajectory randomly from its original and optimal path. This is shown in Figure 4 where a scheme of the privacy-preserving path is illustrated by red arrows. According to this mechanism and as shown in Figure 4, instead of the path $O - X - O$, the drone goes along the path $O - A - B - O$. In this mechanism, ω is a uniform random variable, i.e., $\omega \sim U(0, \Theta)$, where Θ is the design parameter. Intuitively, as Θ increases, the path becomes longer which improves the privacy but degrades the energy consumption undesirably.

Now in the next theorem, we obtain the privacy and energy consumption guarantees as a function of Θ. The privacy guarantee is defined as

$$\mathcal{G}'_p \triangleq \text{Inf } \mathbb{E}||\tilde{X} - X||^2.$$

To obtain an energy consumption guarantee, similar to the first scenario, we require that

$$\mathcal{G}'_e \triangleq \mathbb{P}\left[\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} \geq 1 + \delta\right] = 0,$$

where $\mathcal{E}_p$ is the energy consumption of the proposed privacy-preserving path, $\mathcal{E}_{\text{Opt}}$ is the optimal energy consumption obtained when the drone travels through the $O - X - O$ path, and δ shows the energy efficiency (obtained in (7)).

Theorem 2. For the second proposed PPPM, the privacy and the energy consumption guarantees can be obtained as

$$\text{Inf } \mathbb{E}||\tilde{X} - X||^2 = R^2\left(1 - \text{sinc}^2\frac{\Theta}{2}\right), \tag{5}$$

and

$$\mathbb{P}\left[\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} > 1 + \delta\right] = 0, \tag{6}$$

respectively, where $\delta = k\frac{\Theta}{2}$, and $\text{sinc}(x) \triangleq \frac{\sin(x)}{x}$.

Proof. Let ψ show the observation of the adversary, that is, the path $O - A - B - O$. For the proof of (5), we note that the adversary knows R based on his observation, ψ. Hence, given ψ, the phase of X has a uniform distribution over $(-\frac{\Theta}{2}, \frac{\Theta}{2})$. In other words, $X|\psi = (R, \phi \sim U(-\frac{\Theta}{2}, \frac{\Theta}{2}))$. This is essentially resulted from the proposed privacy preserving mechanism where we have assumed that $\omega \sim U(0, \Theta)$. Therefore, with the MMSE criterion, the best estimator for X in polar coordinate is

$$\begin{aligned}\tilde{X} = \mathbb{E}[X|\psi] &= (0, \mathbb{E}(R|\psi)) \\ &= (0, \mathbb{E}[R\cos\phi]).\end{aligned}$$

Therefore, $\tilde{X}$ is estimated in polar coordinates as $\tilde{X} = (0, a)$, where $a \triangleq \mathbb{E}[R\cos\phi]$ and is obtained as

$$\begin{aligned}a &= R\int_{-\frac{\Theta}{2}}^{\frac{\Theta}{2}} \frac{1}{\Theta}\cos\phi d\phi \\ &= 2R\frac{\sin\frac{\Theta}{2}}{\Theta} \\ &= R\,\text{sinc}\,\frac{\Theta}{2},\end{aligned}$$

where we assume that $\text{sinc}\,\alpha = \frac{\sin\alpha}{\alpha}$.

Thus, the squared error $||\tilde{X} - X||^2$ is the distance between X and $\tilde{X}$ as shown in Figure 5, and the mean squared error is obtained using the Cosine rule as below

$$\begin{aligned}\mathbb{E}||\tilde{X} - X||^2 &= a^2 + R^2 - 2aR\mathbb{E}[\cos\phi] \\ &= R^2\,\text{sinc}\,\frac{\Theta}{2} + R^2 - 2R^2\,\text{sinc}^2\frac{\Theta}{2} \\ &= R^2\left(1 - \text{sinc}^2\frac{\Theta}{2}\right),\end{aligned}$$

which completes the proof.

To obtain the energy efficiency's upperbound, we first note that the energy consumption for the proposed PPPM is

$$\mathcal{E}_p = 2R\mathcal{E}_0 + \Theta Rk\mathcal{E}_0.$$

Therefore, we can write the following equations:

$$\begin{aligned}\frac{\mathcal{E}_p}{\mathcal{E}_{\text{Opt}}} &= \frac{2R\mathcal{E}_0 + \Theta Rk\mathcal{E}_0}{2R\mathcal{E}_0} \\ &= 1 + \frac{\Theta k}{2} \\ &= 1 + \delta,\end{aligned}$$

where

$$\delta = k\frac{\Theta}{2}. \tag{7}$$

□

Discussion 3. It can be seen from Theorem 2 that Θ has a crucial rule in the tradeoff between the privacy and energy guarantees, such that increasing Θ will improve $\mathcal{G}'_p$ while at the

same time it degrades energy efficiency by increasing δ. Hence, one should consider this tradeoff to balance the performance of both guarantees as desired.

VI. Conclusion

In this paper, we proposed two PPPMs for UAVs. Particularly, we considered two scenarios in which the trajectory of a UAV is being observed by an adversary to infer the destination. In the first scenario, we assume that the UAV has only linear movements, while in the second scenario, it can have semi-circular movements too. Considering both privacy and energy consumption guarantees of the UAV, we proposed randomization mechanisms for each scenario. We showed that the proposed PPPMs can provide a privacy guarantee as well as energy efficiency as long as the design parameters are being adjusted carefully. Privacy-energy tradeoff analysis for more sophisticated scenarios such as multi-destination scenario along with stronger adversary are left for our future work.

References

[1] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634, April 2019.

[2] D. Gross. (2013) Amazon's drone delivery: How would it work? [Online]. Available: http://www.cnn.com/2013/12/02/tech/innovation/amazon-drones-questions/

[3] D. Cawthorne and A. R.-V. Wynsberghe, "From healthdrone to frugaldrone: Value-sensitive design of a blood sample transportation drone," in *IEEE International Symposium on Technology and Society (ISTAS)*, Medford, MA, USA, Nov. 2019, pp. 1–7.

[4] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and privacy in the age of commercial drones," in *2021 IEEE Symposium on Security and Privacy (SP)*, San Fransisco, CA, USA, May 2021, pp. 1434–1451.

[5] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[6] P. Blank, S. Kirrane, and S. Spiekermann, "Privacy-aware restricted areas for unmanned aerial systems," *IEEE Security Privacy*, vol. 16, no. 2, pp. 70–79, Mar. 2018.

[7] B. Nassi, R. Ben-Netanel, A. Shamir, and Y. Elovici, "Drones' cryptanalysis - smashing cryptography with a flicker," in *IEEE Symposium on Security and Privacy (SP)*, San Fransisco, CA, USA, May 2019, pp. 1397–1414.

[8] A. Raja and J. Yuan, "Detecting spying activities from the sky via deep learning," in *IEEE International Conference on Communications (ICC)*, Montreal, Qc, Canada, June 2021.

[9] N. Grigoropoulos and S. Lalis, "Flexible deployment and enforcement of flight and privacy restrictions for drone applications," in *50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Valencia, Spain, July 2020, pp. 110–117.

[10] Y. Luo, Y. Yu, Z. Jin, Y. Li, Z. Ding, Y. Zhou, and Y. Liu, "Privacy-aware UAV flights through self-configuring motion planning," in *IEEE International Conference on Robotics and Automation (ICRA)*, Paris, France, Aug. 2020, pp. 1169–1175.

[11] S. Park and K. Lee, "Developing criteria for invasion of privacy by personal drone," in *International Conference on Platform Technology and Service (PlatCon)*, Busan, Korea (South), 2017, pp. 1–7.

[12] Y. Tian, L. Njilla, A. Raja, J. Yuan, S. Yu, A. Steinbacher, T. Tong, and J. Tinsley, "Cost-effective NLOS detection for privacy invasion attacks by consumer drones," in *IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, San Diego, CA, USA, Sept. 2019, pp. 1–7.

[13] A. Fitwi, Y. Chen, and S. Zhu, "No peeking through my windows: Conserving privacy in personal drones," in *IEEE International Smart Cities Conference (ISC2)*, Casablanca, Morocco, Oct. 2019, pp. 199–204.

[14] H. Kim, J. Ben-Othman, and L. Mokdad, "UDiPP: A framework for differential privacy preserving movements of unmanned aerial vehicles in smart cities," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3933–3943, Apr. 2019.

[15] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, Sept. 2016.

[16] X. C. Chen and Y. J. Chen, "A machine learning based attack in UAV communication networks," in *IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Honolulu, HI, USA, Sept. 2019.

[17] M. Asghar Khan, I. Ullah, A. Alkhalifah, S. Ur Rehman, J. Ali Shah, I. I. Uddin, M. H. Alsharif, and F. Algarni, "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3416–3425, May 2022.

[18] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15 068–15 077, Dec. 2020.

[19] Y. Gu, X. Cao, and C. Sun, "A route planning algorithm for privacy protection of UAV states against eavesdropping," in *2020 35th Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, Beijing, China, Aug. 2020, pp. 837–842.

[20] Y.-J. Chen and L.-C. Wang, "Privacy protection for internet of drones: A network coding approach," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019.

[21] I. Vakilinia, M. Jafari, D. Tosh, and S. Vakilinia, "Privacy preserving path planning in an adversarial zone," in *International Symposium on Networks, Computers and Communications (ISNCC)*, Montreal, QC, Canada, Oct. 2020, pp. 1–6.

[22] M. U. Ilyas, M. Zubair Shafiq, A. X. Liu, and H. Radha, "Who are you talking to? Breaching privacy in encrypted IM networks," in *21st IEEE International Conference on Network Protocols (ICNP)*, Goettingen, Germany, Oct. 2013.

[23] S. Ji, P. Mittal, and R. Beyah, "Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1305–1326, Secondquarter 2017.

[24] A. Majeed and S. Lee, "Anonymization techniques for privacy preserving data publishing: A comprehensive survey," *IEEE Access*, vol. 9, pp. 8512–8545, 2021.

[25] J. Meyerowitz and R. Roy Choudhury, "Hiding stars with fireworks: Location privacy through camouflage," in *Proceedings of the 15th annual international conference on Mobile computing and networking*, Beijing, China, Sept. 2009, pp. 345–356.

[26] F. M. Naini, J. Unnikrishnan, P. Thiran, and M. Vetterli, "Where you are is who you are: User identification by matching statistics," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 358–372, Feb. 2016.

[27] S. Oya, C. Troncoso, and F. Pérez-González, "Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1959–1972.

[28] H. Wang, Y. Li, C. Gao, G. Wang, X. Tao, and D. Jin, "Anonymization and de-anonymization of mobility trajectories: Dissecting the gaps between theory and practice," *IEEE Transactions on Mobile Computing*, Mar. 2021.

[29] Y. Zhou, Z. Mo, Q. Xiao, S. Chen, and Y. Yin, "Privacy-preserving transportation traffic measurement in intelligent cyber-physical road systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3749–3759, May 2016.

[30] P. Sui, X. Li, and Y. Bai, "A study of enhancing privacy for intelligent transportation systems: k-correlation privacy model against moving preference attacks for location trajectory data," *IEEE Access*, vol. 5, pp. 24 555–24 567, Oct. 2017.