Location Privacy Protection for UAVs in Package Delivery and IoT Data Collection

Saeede Enayati, Graduate Student Member, IEEE, Dennis Goeckel, Fellow, IEEE, Amir Houmansadr, Member, IEEE, and Hossein Pishro-Nik Member, IEEE

Abstract—Unmanned aerial vehicles (UAVs) are well-known for violating citizen's privacy either inadvertently or deliberately. However, UAVs could be victims of privacy violations themselves in the sense that an adversary observing a UAV can infer its destination. This paper proposes several privacy-preserving mechanisms (PPMs) for protecting a UAV's location privacy. In particular, we address the privacy protection problem in two major UAV applications that require significantly different measures: (i) package delivery, and (ii) Internet of Things (IoT) data collection. In the package delivery application, we propose two different PPMs to randomize the UAV's trajectory such that the observing adversary is confused about the UAV's destination; we provide privacy guarantees and analyze the trade-off with energy consumption. In the IoT data collection scenario, the UAV is not necessarily required to hover exactly above the IoT device; hence, we propose a different PPM according to which the UAV chooses a random spot around the IoT device for data collection. Then, considering a minimum mean squared error (MMSE) criterion, we obtain the privacy leakage to the adversary. We also analyze the mean peak age of information (PAoI) of the network and show that the proposed method does not degrade the mean PAoI significantly. Finally, considering the limitations of the MMSE approach for some applications, we also develop a differential privacy (DP)-based counterpart for this PPM. We observe that the mean PAoI degrades significantly in Laplacian DP but is acceptable in Gaussian DP.

Index Terms—Privacy, Internet of Things (IoT), age-of-information (AoI), differential privacy, unmanned aerial vehicles (UAV), data collection.

I. Introduction and Background

Due to their low cost and agile movement ability, unmanned aerial vehicles (UAVs) are promising alternatives for a number of applications. However, they are often envisioned as compromising privacy by allowing access to areas that could not be observed in other manners. Different privacy-preserving mechanisms (PPMs) have been proposed to combat the privacy violations of UAVs in the sense that UAVs violate citizen's privacy [2]–[8]. For example, in [2], [3], an algorithm was developed 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 [4] where, given the restrictions and UAV's applications, it is in charge of permission to the applications as well as monitoring the drone in order to detect and handle violations at runtime.

What is considered less often is that the privacy of UAV users can itself be compromised by observations of UAV flight patterns. In this regard, [9] 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 in [9] consider two scenarios: the adversary can and cannot see the destinations, and they propose path planning algorithms to hide the destinations from the adversary.

In this paper, we consider two compelling scenarios where UAV user privacy can be compromised and consider privacy-utility tradeoffs for metrics and PPMs matched to each case. First, we consider privacy in delivery applications which, for example, have been under development by Amazon Prime Air delivery since 2013 [10]. Importantly, the UAVs might not only deliver commercial packages but also provide emergency and health-related services at the destinations [11], hence making privacy preservation critical.

Next, we consider the privacy of users employing UAVs in an Internet of Things (IoT) data collection application [12] that addresses the limited power capacity and therefore short-range communication of IoT devices [13]. Privacy leakage of the IoT location can help the adversary to easily find the IoT device [14] for the sake of his benefit, i.e., either take it or destroy it. Location privacy in IoT networks has been investigated widely in the literature by developing different anonymization and obfuscation methods [15]. For example, perfect location privacy was introduced in [16] using anonymization. A differential privacy (DP)-based mechanism for IoT data location privacy was proposed in [17]. Also, decentralized mechanisms based on a blockchain for the location privacy-preserving problem were developed in [18], [19] for a mobile crowdsensing framework. Recently, a model-free obfuscation to combat pattern-matching attacks was introduced in [20].

However, it is worth noting that the aforementioned studies, along with similar ones, aim to ensure privacy by protecting "data" against adversarial attempts. For instance, in [21], although a privacy-preserving mechanism was proposed through UAV path-planning, the objective is to protect "data" from potential eavesdropping. In other words, a significant difference of our work is that the primary objective is to ensure privacy of the users' locations rather than users' data.

Therefore, this paper aims at providing PPMs for UAVs

S. Enayati, Dennis Goeckel, and H. Pishro-Nik are with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, 01003 USA, (e-mail: senayati@umass.edu, goeckel@ecs.umass.edu, pishro@engin.umass.edu).

Amir Houmansadr is with the College of Information and Computer Sciences, University of Massachusetts, Amherst, MA, 01003 USA, (e-mail:amir@cs.umass.edu).

This work was supported by NSF under grants CNS-1932326, CNS-2150832, CNS-1739462, and ECCS 2148159.

This work has been partly presented in the 2022 International Symposium on Networks, Computers, and Communications (ISNCC) [1].

in two major applications: package delivery and IoT data collection. In particular, in the first scenario, we consider a UAV that is delivering packages or providing health services to residents, and its trajectory is observed by an adversary. In this scenario, the adversary tries to identify the UAV's destination based on observing the UAV's trajectory. Hence, the goal is to manipulate the trajectory in a randomized way so that the adversary would not be able to easily infer the destination, and we employ the minimum mean squared error (MMSE) of the adversary as the privacy metric. Applying a privacy mechanism always comes with costs in terms of utility. In the context of a delivery application where the UAV changes its trajectory to confuse the adversary, the energy consumption undesirably increases and will be employed as our utility measure.

In the second scenario, first, using the same privacy metric, we consider the privacy problem for a UAV collecting data from an IoT device while being observed by an adversary. In this scenario, the adversary aims at inferring the IoT's location by observing the UAV's location while collecting data. To the best of our knowledge, IoT privacy leakage from a UAV's location has not been considered in the literature despite its potential risks. We propose a different PPM from that of the package delivery scenario. In the package delivery scenario, the UAV needs to fly and hover exactly above the destination to accomplish its mission, but in the IoT data collection, this limiting condition is no longer necessary as the UAV can still collect data via wireless transmission while it is not hovering exactly above the destination.

Although the MMSE approach demonstrates promising results in the second scenario, employing MMSE as the privacy criterion requires knowledge of the a priori distributions of IoT devices. In other words, it cannot be used when the a priori distribution of the IoT's location is not available. To address this problem, we also propose a differential privacy (DP)-based PPM for the IoT locations' privacy.

The costs of applying a PPM are even more critical in the second scenario, i.e., IoT data collection. In particular, for IoT data utility, the age-of-information (AoI) has been widely recognized as a metric to assess the freshness of the updated data. Hence, from its advent in [22], a rich state-of-the-art has been developed towards analyzing the optimal tradeoffs with other performance metrics in different system models, e.g., [23]–[27]. Specifically, AoI analysis in UAV-aided IoT networks has been considered, for example, in [28]–[39], where typically IoT data AoI minimization is considered to obtain an optimal trajectory design for the UAVs as the data collector.

Therefore, considering AoI as the IoT data utility metric, the applicable question is whether applying a PPM to a data collection framework significantly increases the AoI of the collected data or not. If yes, this could be a substantial drawback as fresh update information from IoT devices and sensors to the destinations is vital due to the increasing demand for real-time applications [40], [41]. However, by analyzing the mean PAoI of the network, we will see that the mean PAoI is similar to the case where there is no privacy. In other words, the proposed PPM does not have a significant cost in terms of mean PAoI.

UAV applications rely heavily on wireless technology components to enable seamless communication. Hence, depending on the specific use case, different wireless technologies can be employed, such as Zigbee [42], LoRa [43], and Global Positioning System (GPS) [44] which are mostly used for applications that require low data rates, and communication protocols such as LTE [45] and 5G [46] suitable for applications with high data rates requirements. In this paper, for the package delivery application, we assume the UAV is equipped with a GPS module for delivery positioning. Furthermore, for the IoT data collection application, low data rates technologies such as Zigbee and LoRa can handle the data collection, in addition to utilizing a GPS module for precise positioning.

While UAVs have different hardware components in terms of the airframe, payload, power supply, communication module, computer system, etc. [47], it is important to mention that the UAV examined in the system models described in this paper can encompass a diverse range of models as long as they satisfy two key requirements: (1) they are capable of transporting packages for delivery purposes, and (2) they possess a communication module equipped with positioning capabilities for both applications. Finally, for both applications, employing a rotary-wing UAV (rotorcraft) is essential due to its hovering capabilities, in contrast to fixed-wing UAVs, which are primarily designed for sustained forward flight rather than stationary hovering.

A. Contributions and Organization

In this paper, we develop several PPMs matched to the metrics of two compelling UAV applications and analyze the trade-offs between privacy and utility. In particular, the contributions of this paper are:

- We propose PPMs for a UAV in the package delivery application considering different UAV's maneuverabilities. We then obtain a privacy guarantee as well as an energy consumption guarantee for the proposed PPMs and analyze the existing trade-offs between them. The system model of this part is different from [9] in several ways: (1) we do not consider any safe zone; hence, the adversary is able to observe the UAV's entire trajectory, and (2) we propose PPMs based on a single destination scenario where, independent of the number of other destinations, one can assure a privacy guarantee.
- We propose a PPM for a UAV in the IoT data collection application. In this scenario, assuming that the IoT devices are initially distributed according to a Gaussian distribution and considering the MMSE of the adversary, we obtain a privacy guarantee for the proposed PPM.
- We analyze the mean PAoI of the IoT data collected by the UAV and obtain the trade-off between privacy and mean PAoI.
- To deal with the limitations of the MMSE metric in some scenarios, we also provide a DP-based PPM considering both Laplacian and Gaussian methods.

This paper is organized as follows: In Section II, we describe the system model for the package delivery application and the corresponding PPMs. The IoT data collection application is more complicated and thus covered in multiple sections. In Section III, we provide the system model for the IoT

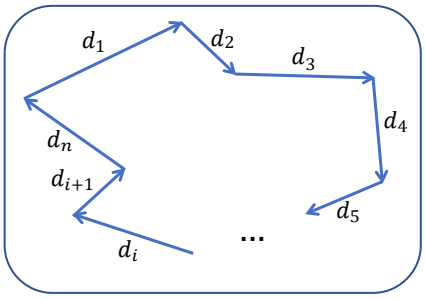


Figure 1: A general representation of a UAV's maneuverability in Scenario I-A where it only flies along linear segments.

data collection application, and in Section IV we provide the proposed PPM. We provide a DP-based PPM for IoT in Section V. Finally, Section VI presents the numerical results, and Section VII concludes the paper.

Notations: Note that throughout this paper, $||.||$ is the L_2 norm, $P(.)$ is the probability, and $E[.]$ is the expectation operator. Random variables are shown in bold letters.

II. Scenario I: PPMs for Package Delivery

In this section, we provide system models for the package delivery UAV application and their corresponding PPMs. We consider two types of maneuverability for each of which we propose a PPM.

A. UAV with Only Linear Trajectory

We assume a system model in which there is a UAV aiming to deliver a package to a destination. There is also an adversary who is observing the UAV trajectory to infer the location of the destination. Below, we describe the assumptions on the UAV's mobility, the adversary, and the UAV's energy consumption in detail.

1) UAV's Trajectory Model: We assume that the UAV's trajectory is a combination of linear segments. In this regard, the drone can fly with a constant speed in a piecewise linear path with segments of different lengths denoted by $d_i, i = 1, 2, \ldots, N$, as shown in Figure 1.

2) Adversary Model: We assume that the adversary can observe the entire path. However, he cannot observe the UAV'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's point of view, the destination is distributed uniformly in the area that includes the entire path. This assumption will be relaxed in the next part. Finally, the adversary knows the randomization mechanism along with its parameters, l, m which are explained in detail in the next section.

3) Energy Consumption Model: The goal is to design privacy-preserving trajectories that guarantee energy efficiency as well and analyze the tradeoff between the two performance metrics. Therefore, in this model, in order to analyze the energy consumption, we first define the energy consumption for a distance unit as E_0. In other words, E_0 is the energy consumed by the drone when traveling a distance unit with a constant speed, i.e., $E_0 \triangleq E(d = 1)$. With this definition, the energy consumption of a path with length d_i is $E_i = d_i E_0$. 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

$$E_T = \sum_{i=1}^{N} d_i E_0 + \sum_{j=1}^{N-1} \zeta E_0 = E_0 \left(\sum_{i=1}^{N} d_i + (N-1)\zeta \right).$$

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 $E = (2d + \zeta) E_0$. In this case, the adversary can easily infer the exact location of Y. Hence, $\tilde{Y} = Y$, where $\tilde{Y}$ is the adversary's inference of Y. In the next section, we propose privacy-preserving path planning for this scenario.

B. Package Delivery PPM I: Fly a Random Triangle

Figure 2 shows the schematic model for this scenario. The UAV intends to deliver a package from source X to destination Y. Normally, the UAV would choose the shortest path, which is the green arrow with length d in Fig. 2. However, for the sake of Y's privacy, we randomize the trajectory. To do so, we define the random variable $\theta \triangleq \arcsin U$ as a deviation angle from the path $X - Y$, where U is a discrete uniform random variable with the following range:

$$\text{Range}(U) = \left\{ \frac{lj}{md}, \; j = -m, -(m-1), \ldots, m-1, m \right\},$$

where $0 < l \leq d_{\min}$, and $d_{\min} = \min_i d_i, i = 1, \ldots, N$ in a multi-destination scenario. Also, $m \triangleq N$ is another randomization parameter that shows the number of potential destinations on the line $A - B$ in Fig 2. As shown in this figure, instead of the path $X - Y - X$, the drone goes along the path $X - A - B - X$. Intuitively, as the θ increases, the path becomes longer which increases the privacy. On the other hand, the energy consumption increases as well.

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

$$G_p \triangleq \text{Inf } E||\tilde{Y} - Y||^2,$$

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

$$G_e \triangleq P\left(\frac{E_p}{E_{Opt}} \geq 1 + \delta \right) = 0,$$

where E_p is the energy consumption of the proposed privacy-preserving path, E_{Opt} is the optimal energy consumption obtained when the drone travels through the $X - Y - X$ path, and δ is a parameter to be determined below. Now we state the following theorem.

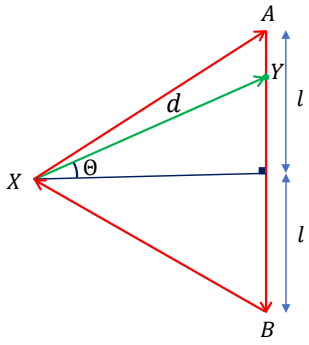


Figure 2: The optimal path and the privacy-preserving path: in the optimal path the UAV flies from X to the destination located at Y directly as shown by the green arrow, whereas in the privacy-preserving path it flies from X to A and B, respectively, as shown by the red arrows. In this figure, l is the randomization parameter and θ is the deviation angle obtained as $\theta = \arcsin(U)$.

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

$$\inf \mathrm{E}\left[\|\tilde{Y} - Y\|^2\right] \geq \frac{l^2}{3}, \tag{1}$$

and

$$P\left(\frac{E_p}{E_{Opt}} \geq 1 + \delta\right) = 0, \tag{2}$$

respectively, where $\delta = \frac{4l+z}{2d+z}$.

Proof. For the proof of (1), we first note that given the adversary's observation denoted by $\psi = X - A - B - X$, Y has a discrete uniform distribution over the line $A - B$, i.e., $Y|\psi = X - A - B - X \sim U[A, B]$. This essentially resulted from the proposed distributions for θ and U. In fact, given $\psi = X - A - B - X$, the adversary has $2m+1$ potential destinations according to the set $\mathrm{Range}(U) = \left\{\frac{lj}{md}, j = -m, -(m-1), \ldots, m-1, m\right\}$, where each of the elements times d are the distance of Y to the middle of the line. Figure 3 shows these potential points that the adversary considers for his estimation. To show this mathematically, we can write

$$\frac{P(Y = Y_j|\psi = X - A - B - X)}{P(Y = Y_k|\psi = X - A - B - X)} = \frac{P(\psi = X - A - B - X|Y = Y_j)f_Y(Y_j)}{P(\psi = X - A - B - X|Y = Y_k)f_Y(Y_k)} \overset{(a)}{=} 1, \quad \forall j = k,$$

where (a) comes from: (1) $f_Y(Y_j) = f_Y(Y_k)$, since the prior information of the adversary is that the destination is uniformly distributed in the area, and (2) $\forall j = -m, \ldots, m$, given $Y = Y_j$ the probability that the line $A - B$ is selected is actually the probability that the corresponding θ is selected uniformly amongst the $2m + 1$ values for θ. In other words, given $Y = Y_j$, the probability that $X - A - B - X$ is selected is $\frac{1}{2m+1}$

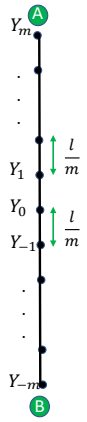


Figure 3: Given an observation of the UAV's path, ψ, there are $2m + 1$ points uniformly distributed across the line that the adversary considers for his estimation of the destination.

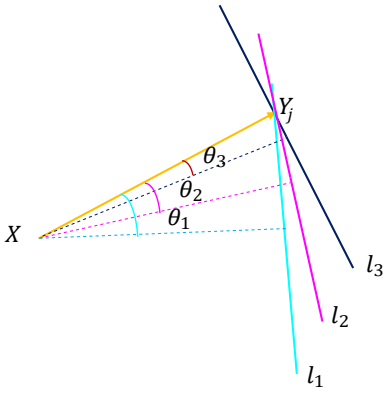


Figure 4: Given $Y = Y_j$, there can be different lines passing from Y_j. In fact, there is a line corresponding to each value that θ can take which is $2m + 1$. The orange line shows the real path, the dashed lines show the selected θs, and the solid lines l_1, l_2, l_3, show the possible lines corresponding to the θs.

which gives us the posterior probability as $P(Y = Y_j|\psi = X - A - B - X) = \frac{1}{2m+1}$ (See Fig. 4).

Now considering the MMSE criterion, the best estimator is the mean value and the least estimation error is the variance, i.e., $\forall m \in \mathbb{N}$

$$\begin{aligned}\mathrm{E}\left[\|Y - Y\|^2\right] &= \frac{2}{2m+1}\left[0 + \frac{l^2}{m^2} + \frac{(2l)^2}{m^2} + \cdots + \frac{(ml)^2}{m^2}\right] \\ &= \frac{2l^2}{m^2} \times \frac{m(m+1)(2m+1)}{6} \\ &= \frac{(m+1)l^2}{3m} \\ &\geq \frac{l^2}{3}.\end{aligned}$$

To prove (2), we obtain the upper bound for $\frac{E_p}{E_{Opt}}$ and the corresponding δ. To do so, we note that in the worst-case scenario, Y is exactly in the middle of $A - B$ and the energy

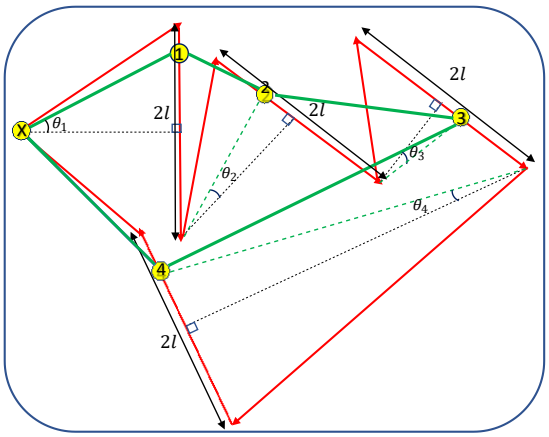


Figure 5: The extended PPM I for a 4-destination scenario. The green solid line shows the shortest path, the red arrowed path shows the privacy-preserving path, the green dashed lines show the shortest path segment from each point to the next destination, and the black dotted lines are the vertical perpendicular to show the deviation angle, θ.

consumption is

$$E_p = E_p = 2\sqrt{d^2 + l^2} + 2l + 2\zeta.$$

Therefore,

$$\begin{aligned}\frac{E_p}{E_{Opt}} &= \frac{2\sqrt{d^2 + l^2} + 2l + 2\zeta}{2d + \zeta} \\ &< \frac{2\sqrt{d^2 + l^2 + 2dl} + 2l + 2\zeta}{2d + \zeta} \\ &= \frac{2d + \zeta + 4l + \zeta}{2d + \zeta} \\ &= 1 + \frac{4l + \zeta}{2d + \zeta} \\ &= 1 + \delta.\end{aligned}$$

with

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

and (2) is concluded. □

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

We can extend the proposed PPM 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 B in Figure 2 instead of returning to the origin X. Figure 5 shows the optimal and the extended PPM applied to a 4-destination scenario.

C. UAV with Linear and Arc Trajectory

In this section, we provide the second PPM for the package delivery application. In the following, we provide the assumptions for this scenario in detail.

1) 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 which 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.

2) 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 the 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 adversary's perspective, θ_X is distributed uniformly in $[0, 2\pi)$.

3) Energy Consumption Model: To model the energy consumption of the proposed system, as before we define 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., $E_0 \triangleq E(d = 1)$. With this definition, the energy consumption of a path with length d_i is $E_i = d_i E_0$. 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

$$E_p(R, \theta) = \theta R k E_0,$$

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 $E_{Opt} = 2RE_0$.

D. Package delivery PPM II: Fly a Random Arc

Similar to PPM I, the idea here is to deviate the UAV's trajectory randomly from its original shortest path. This is shown in Figure 6 where the privacy-preserving path of the proposed scheme is illustrated by red arrows. According to this mechanism and as shown in Figure 6, 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 increases the energy consumption undesirably.

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

$$G_p' \triangleq \text{Inf } E||\tilde{X} - X||^2.$$

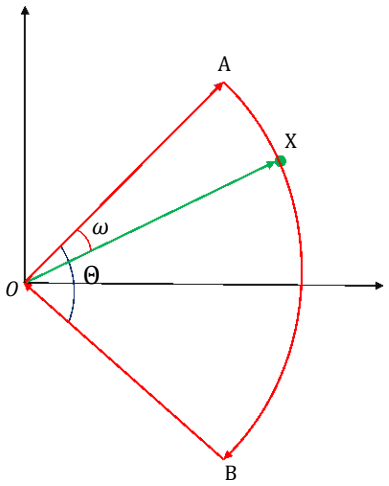


Figure 6: The shortest path and the privacy-preserving path for the UAV with linear and arc maneuverability: in the shortest path the UAV flies from O to the destination located at X directly as shown by the green arrow, whereas in the privacy-preserving path, it flies from O to A and B, respectively, as shown by the red arrows. In this figure, Θ is the randomization parameter and ω is the deviation angle obtained as $\omega \sim U(0, \Theta)$.

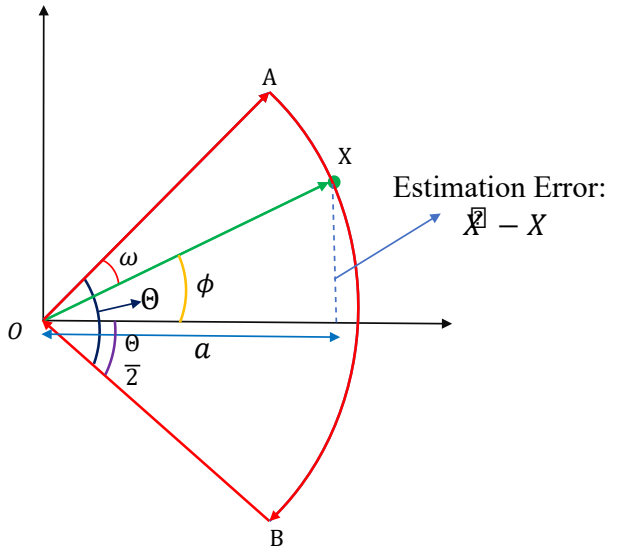


Figure 7: The privacy-preserving path for the UAV with linear and arc trajectory and the corresponding parameters: Θ is the randomization parameter, ω is the deviation angle, and a is the adversary's estimation of the destination.

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

$$G'_e \triangleq P\left(\frac{E_p}{E_{Opt}} \geq 1 + \delta\right) = 0,$$

where E_p is the energy consumption of the proposed privacy-preserving path, E_{Opt} is the optimal energy consumption obtained when the drone travels through the $O - X - O$ path, and δ is determined below.

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

$$\text{Inf } E||\tilde{X} - X||^2 = R^2\left(1 - \text{sinc}^2\frac{\Theta}{2}\right), \quad (3)$$

and

$$P\left(\frac{E_p}{E_{Opt}} > 1 + \delta\right) = 0, \quad (4)$$

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

Proof. Let ψ be the observation of the adversary, that is, the path $O - A - B - O$. For the proof of (3), 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, $X|\psi = (R, \varphi \sim U(-\frac{\Theta}{2}, \frac{\Theta}{2}))$. This 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 coordinates is

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

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

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

From Figure 7 we can obtain $E||\tilde{X} - X||^2$ using the right triangle rule as

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

which completes the proof.

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

$$E_p = 2RE_0 + \Theta RkE_0.$$

Therefore, we can write the following equations:

$$\begin{aligned}\frac{E_p}{E_{Opt}} &= \frac{2RE_0 + \Theta RkE_0}{2RE_0}\\ &= 1 + \frac{\Theta k}{2}\\ &= 1 + \delta,\end{aligned}$$

where

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

□

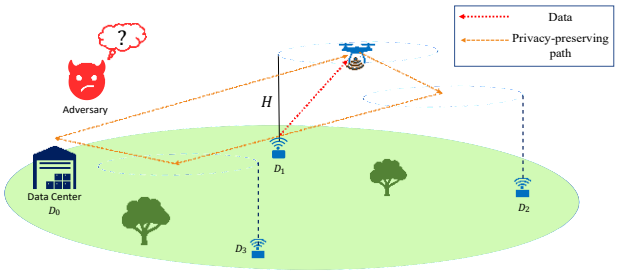


Figure 8: IoT data collection system model. The UAV flies at altitude H from D_0 to the IoT devices with respect to their index. Instead of hovering exactly above the devices, the UAV chooses a random spot around each device. The adversary can observe the entire path but cannot see the locations of IoT devices.

It can be seen from Theorem 2 that increasing Θ improves G_p', while at the same time, it degrades energy efficiency by increasing δ. Hence, one should consider this trade-off to balance the performance of both guarantees as desired.

It is important to highlight that the values ϵ_0, ζ, and k can be determined based on the specific hardware configuration of a given UAV. Finally, we note that employing the proposed privacy-preserving mechanism does not substantively increase the computation cost as it is based on adding a random number selection to the non-private operation. This applies to the IoT data collection application as well.

III. Scenario II: IoT Data Collection Application

A. Network Model and Metrics

Figure 8 shows a typical IoT data collection system model where there are N IoT devices[1] in the network. We denote the set of IoT devices by $D = \{D_1, D_2, \ldots, D_N\}$ where D_i is the indicator of the $i-th$ device. There is a UAV in the network as the IoT data collector that starts flying from the data center, denoted by D_0, to the set of sensors through a predetermined trajectory. The set of 2-D locations corresponding to set D are represented by $U = \{U_1, U_2, \ldots, U_N\}$, where $U_i = (x_i, y_i)$ is the 2-D location of device D_i. Also, x_i and y_i are assumed to be independent and distributed according to a Gaussian distribution. In other words, $U_i \sim \mathcal{N}(\mu_U, \Sigma_U)$, where $\mu_U \in \mathbb{R}^2$ and $\Sigma_U \in \mathbb{R}^{2\times 2}$ are the mean vector and the covariance matrix, respectively.

The UAV flies at a fixed height H over the region. Without considering IoT location privacy, the UAV hovers exactly above its intended sensor which favorably minimizes data collection time due to the minimum transmission range and the likely existence of a LoS link. However, for the sake of privacy, here a randomization mechanism is exploited where the UAV randomly chooses a point (spot) associated with each device. The set of these random points or privacy-preserving spots associated with devices is represented by $W = \{W_1, W_2, \ldots, W_N\}$ where $W_i = (x_i', y_i', H)$ and we assume that the UAV chooses the same random spot whenever it returns to D_i. The randomization process according to which a random spot is chosen is explained in detail in the next section. After locating the privacy-preserving spots, the UAV collects the data from the sensor and continues this process until all of the devices are visited, after which it flies back to the data center. Finally, the distance between the UAV at W_i and device D_i is obtained as

$$d_i = \sqrt{(x_i - x_i')^2 + (y_i - y_i')^2 + H^2}.$$

1) Privacy Guarantee: For this scenario, we define the privacy guarantee as:

$$G_P = \text{Inf}\, E||\tilde{U} - U||^2,$$

where the Inf is taken over all possible estimators. In the following section, we obtain the lower bound of the privacy guarantee.

2) AoI Analysis: At each time instant t, the AoI of D_i, $i = 1, \ldots, N$, is defined as [22]

$$\Delta_i(t) = t - \delta_i,$$

where δ_i is the time stamp at which data has been generated and is ready to be transmitted to the UAV. In this paper, we analyze the mean PAoI for the proposed PPM in the IoT network which is defined as the average of the mean peak AoI of the IoT devices. Mathematically speaking, if we denote the peak AoI of D_i by Δ_i^{max}, the mean PAoI of N IoT devices, denoted by Δ_N^{max} is defined as

$$\bar{\Delta}_N^{max} = \frac{1}{N}\sum_{i=1}^{N} E[\Delta_i^{max}].$$

We first consider a single-device scenario and then extend the analysis to an IoT network with multiple devices.

B. Adversary Model And Privacy Mechanism

1) Adversary Model: We assume that the adversary can observe the entire path, and we do not consider edge effects in the network. He is also assumed to know the number of IoT devices, N. Furthermore, we assume that the adversary knows the privacy-preserving mechanism and its parameters. However, he does not know the realizations of the randomizations.

2) Privacy-Preserving Mechanism: In order to provide location privacy for the IoT devices in the network, we apply a different randomization mechanism from that of the package delivery application. This is due to the fact that in the package delivery application, the UAV is required to fly over the destination. However, in the IoT data collection application, we take advantage of the fact that the UAV is not necessarily required to fly exactly over the destination. Hence, the proposed randomization is as follows: for each device, D_i and given $\Sigma_Q \in \mathbb{R}^{2\times 2}$, let $Q_i = (x_{q_i}, y_{q_i})$, where $Q_i \sim \mathcal{N}(0, \Sigma_Q)$ is independent of U_i, be the noise vector random variable in

[1]Throughout this paper, the terms IoT devices and sensors are used interchangeably.

which x_{q_i} and y_{q_i} are assumed to be independent. Now, the UAV's privacy-preserving destination, $W_i = (x_i', y_i', H)$ is obtained as:

$$W_i = U_i + Q_i. \tag{5}$$

Hence, for each D_i, W_i is a Normal random variable with the mean $\mu_{W_i} = \mu_{U_i}$ and covariance $\Sigma_{W_i} = \Sigma_{U_i} + \Sigma_{Q_i}$ as W_i is the sum of two independent Normal random variables. Thus, we have

$$f_{W_i}(w_i) = N(\mu_{U_i}, \Sigma_{U_i} + \Sigma_{Q_i}),$$

We can write (5) in terms of x and y in the Cartesian basis as:

$$x_i' = x_i + x_{q_i},$$
$$y_i' = y_i + y_{q_i}.$$

Now let the adversary's observation be denoted by ψ. Given ψ, the adversary's estimation of D_i's location denoted by $\tilde{U}_i = (\tilde{x}_i, \tilde{y}_i)$ can exploit knowledge of the a priori distribution of (x_i, y_i) to employ Bayesian estimation.

In fact, considering the a priori Normal distribution for the IoT devices, the PDF of $U_i|\psi$ can be obtained as below:

$$\begin{aligned} f_{U_i|\psi}(u_i|\psi) &= f_{U_i|W_i}(u_i|w_i) \\ &= \frac{f_{W_i|U_i}(w_i|u_i) f_{U_i}(u_i)}{f_{W_i}(w_i)} \\ &= \frac{f_{Q_i}(w_i - u_i) f_{U_i}(u_i)}{f_{W_i}(w_i)}. \end{aligned}$$

The posterior distribution in terms of x_i and y_i are obtained in the following lemma:

Proposition 1. The posterior distributions of x_i and y_i, $i = 1, 2, \ldots, N$, given $(\acute{x}_i, \acute{y}_i)$, can be obtained as:

$$f_{x_i|\acute{x}_i}(x_i|\acute{x}_i) = \frac{1}{\sqrt{2\pi}\sigma_{x_i|\acute{x}_i}} e^{-\frac{\left(x_i - \left(\frac{\sigma_x^2}{\sigma_x^2 + \sigma_{x_q}^2}\acute{x}_i + \frac{\sigma_{x_q}^2}{\sigma_x^2 + \sigma_{x_q}^2}\mu_x\right)\right)^2}{2\sigma_{x_i|\acute{x}_i}^2}}, \tag{6}$$

and

$$f_{y_i|\acute{y}_i}(y_i|\acute{y}_i) = \frac{1}{\sqrt{2\pi}\sigma_{y_i|\acute{y}_i}} e^{-\frac{\left(y_i - \left(\frac{\sigma_y^2}{\sigma_y^2 + \sigma_{y_q}^2}\acute{y}_i + \frac{\sigma_{y_q}^2}{\sigma_y^2 + \sigma_{y_q}^2}\mu_y\right)\right)^2}{2\sigma_{y_i|\acute{y}_i}^2}}, \tag{7}$$

respectively, where $\sigma^2_{x_i|\acute{x}_i} = \frac{\sigma_{x_q}^2 \sigma_x^2}{\sigma_x^2 + \sigma_{x_q}^2}$ and $\sigma^2_{y_i|\acute{y}_i} = \frac{\sigma_{y_q}^2 \sigma_y^2}{\sigma_y^2 + \sigma_{y_q}^2}$ are the corresponding variances.

Now considering a minimum mean-squared error (MMSE) estimator for (x_i, y_i), $i = 1, 2, \ldots, N$, the adversary's estimate denoted by $\tilde{U}_i = (\tilde{x}_i, \tilde{y}_i)$ is the conditional expected value:

$$\begin{aligned} \tilde{U}_i &= (\tilde{x}_i, \tilde{y}_i) \\ &= \left(E(x_i | x_i' = x_i'), E(y_i | y_i' = y_i')\right) \\ &= \left(\frac{\sigma_x^2}{\sigma_x^2 + \sigma_{x_q}^2} x_i' + \frac{\sigma_{x_q}^2}{\sigma_x^2 + \sigma_{x_q}^2} \mu_x, \right. \\ &\quad \left. \frac{\sigma_y^2}{\sigma_y^2 + \sigma_{y_q}^2} y_i' + \frac{\sigma_{y_q}^2}{\sigma_y^2 + \sigma_{y_q}^2} \mu_y \right), \end{aligned} \tag{8}$$

where (8) is concluded from (6) and (7).

IV. Privacy Guarantee and AoI Analysis

A. Privacy Guarantee:

Lemma 1. For the MMSE estimator discussed above, the privacy guarantee of D_i, denoted by G_{P_i} is lower bounded as:

$$G_{P_i} \geq \frac{\sigma_{x_{q_i}}^2 \sigma_{x_i}^2}{\sigma_{x_i}^2 + \sigma_{x_{q_i}}^2} + \frac{\sigma_{y_{q_i}}^2 \sigma_{y_i}^2}{\sigma_{y_i}^2 + \sigma_{y_{q_i}}^2} \tag{9}$$

Proof. Since the MMSE is the optimal estimator in terms of the mean-squared error (MSE), it is sufficient to obtain the MSE value of this estimator, as every other estimator will result in a greater MSE. Finally, since we have an independent error in a two dimension plane, we add the MSE of the two dimensions to obtain the overall MSE. □

Intuitively, for the sake of protecting privacy, one may increase the lower bound in (9) to make sure that the adversary makes larger errors in his estimation. Therefore, to better protect privacy, one needs to increase the added noise variance. However, it is crucial to analyze the effect of this added noise on other performance metrics. In this paper, we consider the AoI of the IoT data.

B. AoI Analysis

1) Single Sensor scenario: We obtain the mean PAoI for a network with a single IoT device in the following lemma.

Lemma 2. Let the time the UAV needs to hover over D_i to collect its data be τ_i. Then, the mean PAoI for the proposed PPM in a single-sensor IoT network is obtained as

$$\bar{\Delta}_1^{max} = 2E[\tau_i] + \frac{3}{v}\left(\frac{\pi}{2}\right)^q \sqrt{\sigma_u^2 + \sigma_q^2}\, L_{\frac{1}{2}}\left(\frac{-(\mu_x^2 + \mu_y^2)}{2(\sigma_u^2 + \sigma_q^2)}\right),$$

where we assume that $\sigma_u^2 = \sigma_{x_i}^2 = \sigma_{y_i}^2$ and $\sigma_q^2 = \sigma_{x_{q_i}}^2 = \sigma_{y_{q_i}}^2$. Also, $L_n(x)$ is the Laguerre polynomial and can be calculated as

$$L_n(x) = {}_1F_1(-n; 1; x),$$

where ${}_1F_1(-n; 1; x)$ is the confluent Hypergeometric function of the first kind.

Proof. If we denote the flight time from the data center to D_i by t_i and assume that after delivering the data to the data center the UAV will turn back to the device to recollect updated

data, then the maximum AoI of for a single device is obtained as

$$\Delta_1^{max} = 2\tau_i + 3t_i.$$

Figure 9 shows the AoI trend for a single device scenario ($i = 1$).

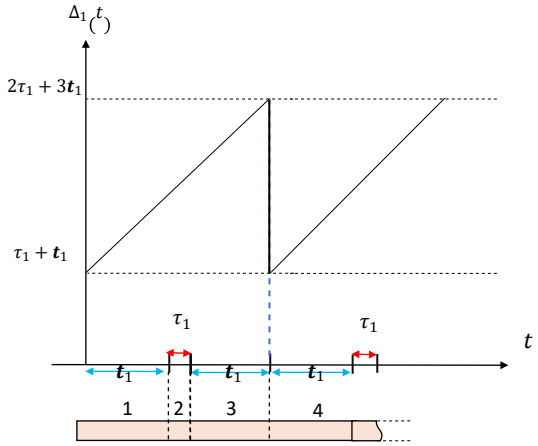


Figure 9: AoI trend for D_1 in a single device scenario. Assuming that the UAV has already delivered data, the minimum AoI is $\tau_1 + t_1$, and the explanation for the time intervals are as follows: (1): The UAV goes to D_1, (2): The UAV collects new data, (3): The UAV returns to the data center, (4): The UAV goes back to D_1 for a new data collection.

Now we note that for a privacy-preserving spot associated with D_i located at $(\acute{x}_i, \acute{y}_i)$, we have

$$t_i = \frac{\sqrt{\acute{x}_i^2 + \acute{y}_i^2}}{v},$$

where we remember that $\acute{x}_i \sim N(\mu_{x_i}, \sigma^2_{\acute{x}_i} = \sigma^2_{x_i} + \sigma^2_{x_{q_i}})$ and $\acute{y}_i \sim N(\mu_{y_i}, \sigma^2_{\acute{y}_i} = \sigma^2_{y_i} + \sigma^2_{y_{q_i}})$. Therefore, assuming $\sigma^2_{\acute{x}_i} = \sigma^2_{\acute{y}_i} = \sigma^2_u + \sigma^2_q$, we can conclude that $r_i = \sqrt{\acute{x}_i^2 + \acute{y}_i^2}$ has a Rician distribution as:

$$f_{r_i}(r_i) = \frac{r_i}{\sigma^2_{u_i} + \sigma^2_{q_i}} \exp\left(-\frac{r_i^2 + v^2}{2(\sigma^2_u + \sigma^2_q)}\right) I_0\left(\frac{v r_i}{\sigma^2_u + \sigma^2_q}\right),$$

where $v = \sqrt{\mu^2_{x_i} + \mu^2_{y_i}}$. Then, we have

$$E[r_i] = \sqrt{\frac{\pi}{2}}\sqrt{\sigma^2_u + \sigma^2_q}\, L_{\frac{1}{2}}\left(\frac{-(\mu^2_{x_i} + \mu^2_{y_i})}{2(\sigma^2_u + \sigma^2_q)}\right).$$

This completes the proof. □

2) Multi Sensor Scenario: For a scenario where the UAV collects data from multiple IoT devices, we assume that the UAV flies to the devices in the order of their indices, i. In other words, starting from the data center it flies to D_1 then flies to D_2, D_3, and so on. In this setup, the mean PAoI is obtained in the following lemma.

Lemma 3. The mean PAoI of the multi IoT device network, $\bar{\Delta}_N^{max}$, is obtained as

$$\bar{\Delta}_N^{max} = \frac{1}{v}\sum_{i=1}^{N-1}\left(1 + \frac{i}{N}\right)E[l_i] + \frac{2}{v}E[r_N] + \frac{1}{v}E[r_1] + \sum_{i=1}^{N}\left(1 + \frac{i}{N}\right)E[\tau_i], \quad (10)$$

where

$$E[l_i] = \sqrt{\frac{\pi}{2}}\sqrt{\sigma^2_u + \sigma^2_q}\, L_{\frac{1}{2}}\left(\frac{-v_i^2}{4(\sigma^2_u + \sigma^2_q)}\right), \quad (11)$$

$$E[r_1] = \sqrt{\frac{\pi}{2}}\sqrt{\sigma^2_u + \sigma^2_q}\, L_{\frac{1}{2}}\left(\frac{-(\mu^2_{x_1} + \mu^2_{y_1})}{2(\sigma^2_u + \sigma^2_q)}\right), \quad (12)$$

$$E[r_N] = \sqrt{\frac{\pi}{2}}\sqrt{\sigma^2_u + \sigma^2_q}\, L_{\frac{1}{2}}\left(\frac{-(\mu^2_{x_N} + \mu^2_{y_N})}{2(\sigma^2_u + \sigma^2_q)}\right), \quad (13)$$

and v_i is given in (14).

Proof. Let the distance between the privacy-preserving spots be denoted by $l_i = l_{i\to i+1} = ||W_{i+1} - W_i|| = \sqrt{(\acute{x}_{i+1} - \acute{x}_i)^2 + (\acute{y}_{i+1} - \acute{y}_i)^2}$, $i = 1, \ldots, N-1$. Hence, the PDF of l_i is obtained as

$$f_{l_i}(l_i) = \frac{l_i}{\sigma^2_l}\exp\left(-\frac{l_i^2 + v_i^2}{2\sigma^2_l}\right) I_0\left(\frac{v_i l_i}{\sigma^2_l}\right),$$

where

$$v_i = \sqrt{(\mu_{x_{i+1}} - \mu_{x_i})^2 + (\mu_{y_{i+1}} - \mu_{y_i})^2}, \quad (14)$$

and $\sigma^2_l = \sigma^2_{x_i} + \sigma^2_{x_{q_i}} + \sigma^2_{x_{i+1}} + \sigma^2_{x_{q_{i+1}}} = \sigma^2_{y_i} + \sigma^2_{y_{q_i}} + \sigma^2_{y_{i+1}} + \sigma^2_{y_{q_{i+1}}}$ assuming that $\sigma^2_{x_i} = \sigma^2_{y_i} = \sigma^2_u$, and $\sigma^2_{x_{q_i}} = \sigma^2_{y_{q_i}} = \sigma^2_q$, $i = 1, 2, \ldots, N$. Hence, $\sigma^2_l = 2(\sigma^2_u + \sigma^2_q)$.

Figure 10 shows the AoI trend for a multi-device scenario. In this figure, $t_1 = \frac{r_1}{v}$, $t_i = \frac{l_i}{v}$, $i = 2, \ldots, N-1$, and $t_N = \frac{r_N}{v}$.

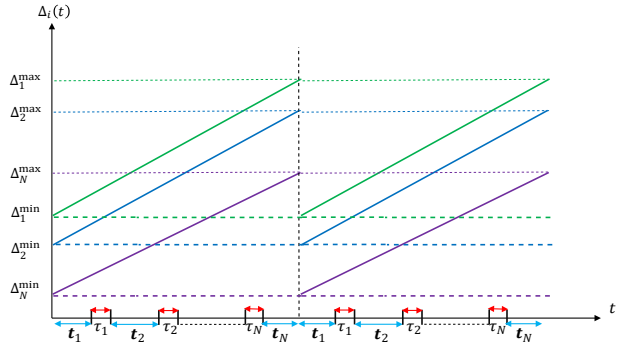


Figure 10: AoI trend in a multi-device scenario. The green line shows the AoI trend for D_1, the blue line shows the AoI trend for D_2, ..., and the purple line shows the AoI for trend for D_N. Note that we do not need the values of Δ_i^{min}, $i = 1:, \ldots, N$ in our analysis.

Now the PAoI for each device $i = 1, 2, \ldots, N$ can be obtained as as

$$\Delta_1^{\max} = \frac{1}{v}\left(2\sum_{i=1}^{N-1} l_i + 2r_N + r_1 + 2\sum_{i=1}^{N}\tau_i\right)$$

$$\Delta_2^{\max} = \frac{1}{v}\left(2\sum_{i=2}^{N-1} l_i + l_1 + 2r_N + r_1 + 2\sum_{i=1}^{N}\tau_i - \tau_1\right)$$

$$\Delta_N^{\max} = \frac{1}{v}\left(\sum_{i=1}^{N-1} l_i + 2r^N + r_1 + 2\sum_{i=1}^{N}\tau_i - \sum_{i=1}^{N-1}\tau_i.\right)$$

Therefore, the mean PAoI is obtained as

$$\begin{aligned}
\bar{\Delta}_N^{\max} &= E\left[\frac{1}{N}\sum_{i=1}^{N}\Delta_i^{max}\right] \\
&= \frac{1}{N}E\left[\frac{1}{v}\left(\sum_{i=1}^{N-1}(N+i)l_i + 2Nr_N + Nr_1 + \sum_{i=1}^{N}(N+i)\tau_i\right)\right] \\
&= \frac{1}{Nv}\sum_{i=1}^{N-1}(N+i)E[l_i] + 2NE[r_N] + NE[r_1] + \\
&\quad + \frac{1}{N}E\left[\sum_{i=1}^{N}(N+i)\tau_i\right] \\
&= \frac{1}{v}\sum_{i=1}^{N-1}\left(1+\frac{i}{N}\right)E[l_i] + \frac{2}{v}E[r_N] + \frac{1}{v}E[r_1] \\
&\quad + \sum_{i=1}^{N}\left(1+\frac{i}{N}\right)E[\tau_i]. \qquad (15)
\end{aligned}$$

□

C. Privacy Guarantee and AoI Trade-off

1) Case 1: Negligible data collection time ($\tau_i = 0$): In this scenario, we assume that the collection time is negligible in comparison to the flight time. Hence, for a single-sensor scenario, $\bar{\Delta}_1^{\max}$ can be obtained as below

$$\bar{\Delta}_1^{\max} = \frac{3}{2}\sqrt{\frac{\pi}{2}}\sqrt{\sigma_u^2 + \sigma_q^2}L_1 - \frac{(\mu_x^2 + \mu_y^2)}{2(\sigma_x^2 + \sigma_y^2)}.$$

Similarly, for the multi-device scenario, we obtain

$$\bar{\Delta}_N^{\max} = \frac{1}{v}\sum_{i=1}^{N-1}\left(1+\frac{i}{N}\right)E[l_i] + \frac{2}{v}E[r_N] + \frac{1}{v}E[r_1].$$

2) Case 2: Constant collection time ($\tau_i = c$): In this scenario, we consider the case where $\tau_i = c$, and c is chosen such that one can make sure the data is received at the UAV completely. In fact, we assume that the data collection time is small enough that we can choose c arbitrarily large to make sure the IoT data is received. Hence, $\bar{\Delta}_N^{\max}$ is obtained as

$$\bar{\Delta}_N^{\max} = \frac{1}{v}\sum_{i=1}^{N-1}\left(1+\frac{i}{N}\right)E[l_i] + \frac{2}{v}E[r_N] + \frac{1}{v}E[r_1] + \frac{3N+1}{2}c,$$

where the last term is obtained from the last sum in (15).

3) Case 3: τ_i as a function of σ_q^2: In this case, we consider the case where the data collection time from the IoT device to the UAV is a function of noise added for privacy protection. In other words, given σ_q^2, we can obtain τ. We have the following proposition:

Proposition 2. Suppose that $\sigma_{x_q}^2 = \sigma_{y_q}^2 = \sigma_q^2$. Then, there exists a time τ for which the IoT data is collected completely by the UAV with a high probability. Mathematically, we have:

$$\forall\, \epsilon_0 > 0, \sigma_{x_q}^2, \sigma_{y_q}^2 \text{ where } \sigma_{x_q}^2 = \sigma_{y_q}^2 = \sigma_q^2,\ \exists\tau^{\star}: \forall t > \tau^{\star},\ P\left[tB\log_2(1+\gamma) \geq \Omega\right] \geq 1 - \epsilon_0, \qquad (16)$$

where B is the bandwidth, γ is the signal-to-noise ratio (SNR), and Ω is the IoT data size in bits.

To obtain τ, first we compute the probability in (16) as:

$$\begin{aligned}
&P\left[\tau^{\star}B\log_2(1+\gamma) \geq \Omega\right] \\
&= P\left[\tau^{\star} \geq \frac{\Omega}{B\log_2\left(1+\frac{p_0}{\sigma_0^2 B}d^{-\alpha}\right)}\right] \\
&= P\left[1+\frac{p_0}{\sigma_0^2 B}d^{-\alpha} \geq 2^{\frac{\Omega}{\tau^{\star}B}}\right] \\
&= P\left[d \leq \left(\frac{\sigma_0^2 B}{p_0}\left(2^{\frac{\Omega}{\tau^{\star}B}} - 1\right)\right)^{-\frac{1}{\alpha}}\right] \\
&= P\left[\zeta \leq \left(\frac{\sigma_0^2 B}{p_0}\left(2^{\frac{\Omega}{\tau^{\star}B}} - 1\right)\right)^{-\frac{2}{\alpha}} - H^2\right] \\
&= 1 - \exp\left(-\frac{Z}{2\sigma_q^2}\right), \qquad (17)
\end{aligned}$$

where α is the path-loss exponent, $\zeta \triangleq x_q^2 + y_q^2 \sim \exp(\frac{1}{2\sigma_q^2})$, and $Z \triangleq \left(\frac{\sigma_0^2 B}{p_0}\left(2^{\frac{\Omega}{\tau^{\star}B}} - 1\right)\right)^{-\frac{2}{\alpha}} - H^2$. From (17) and (16), we obtain

$$\tau^{\star} \geq \frac{\Omega}{B\log_2\left(1+\frac{P_0}{\sigma_0^2 B}\right)^{-2\sigma_q^2\ln\epsilon_0 + H^2}}. \qquad (18)$$

Therefore, given σ_q^2, the mean PAoI can be obtained as

$$\bar{\Delta}_N^{\max} \geq \frac{1}{v}\sum_{i=1}^{N-1}\left(1+\frac{i}{N}\right)E[l_i] + \frac{2}{v}E[r_N] + \frac{1}{v}E[r_1] + \frac{3N+1}{2}\tau^{\star},$$

where the last term is obtained from the last sum in (15).

4) Case 4: τ_i as a function of σ_q^2 and fading: In this case, we consider the case where the collection time is a function of noise and fading. In other words, we take into account the effect of both σ_q^2 and the fading on τ. We assume a Rayleigh channel model for the link between the IoT device and the UAV. Hence, to obtain $\tau^{\star}$, the minimum value of τ, similar to Case 3, we first calculate the probability term in (16) as below.

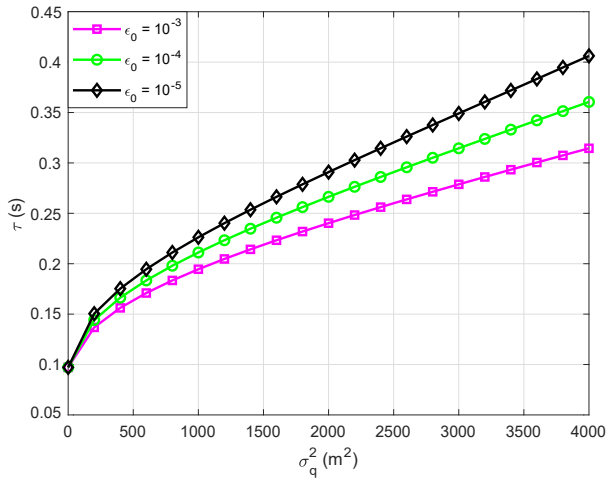


Figure 11: The value of τ with respect to σ_q^2 in (18) for different values of ϵ_0.

$$
\begin{aligned}
&P[\tau B \log_2(1+\gamma) \geq \Omega] \\
&= P\left[\tau B \log_2\left(1+\frac{p_0 h}{\sigma^2 B} d^{-\alpha}\right) \geq \Omega\right] \\
&= E_h P\left[\log_2\left(1+\frac{p_0 h}{\sigma_0^2 B} d^{-\alpha}\right) \geq \frac{\Omega}{\tau B} \,\middle|\, h=h\right] \\
&= E_h P\left[d \leq \left(\frac{\sigma_0^2 B}{p_0 h}\left(2^{\frac{\Omega}{\tau B}}-1\right)\right)^{-\frac{1}{\alpha}} \,\middle|\, h=h\right] \\
&= E_h P\left[\zeta \leq \left(\frac{\sigma_0^2 B}{p_0 h}\left(2^{\frac{\Omega}{\tau B}}-1\right)\right)^{-\frac{2}{\alpha}} - H^2 \,\middle|\, h=h\right] \\
&= E_h\left[1-\exp\left(-\frac{Z(h)}{2\sigma_q^2}\right)\right] \qquad (19) \\
&= 1-\eta_1 \int_0^{\infty} e^{-(h+\eta_2 h^{\frac{2}{\alpha}})} dh \qquad (20)
\end{aligned}
$$

where $\zeta \triangleq x_q^2 + y_q^2$, $\zeta \sim \exp(\frac{1}{2\sigma_q^2})$, $Z(h) \triangleq \left(\frac{\sigma_0^2 B}{p_0 h}\left(2^{\frac{\Omega}{\tau B}}-1\right)\right)^{-\frac{2}{\alpha}} - H^2$ in (19), and in (20), $\eta_1 \triangleq e^{\frac{H^2}{2\sigma_q^2}}$ and $\eta_2 \triangleq \frac{1}{2\sigma_q^2}\left(\frac{p_0}{\sigma_0^2 B}\left(2^{\frac{\Omega}{\tau B}}-1\right)\right)^{-\frac{2}{\alpha}}$. Note that the integral in (20), is obtained by assuming $h \sim \exp(1)$. Unfortunately, the integral in (20) is not analytically solvable, and therefore we present the results through simulations.

V. Differential Privacy

As mentioned earlier, the PPM based on the MMSE estimator developed in the previous part requires knowledge about the prior distribution of IoT devices. Therefore, for the cases where the prior distribution is not Gaussian or it is not known at all, we propose a DP-based PPM. In particular, in this section, we introduce a similar PPM based on a DP framework and investigate the trade-off between privacy and AoI. The notation of DP in location privacy has been introduced in [48] in the form of geo-indistinguishability which has received great attention ever since [49]–[51]. We consider two cases for the DP-based PPM: The Laplacian mechanism and the Gaussian mechanism.

A. Laplace Mechanism

Definition 1. Given ϵ and for all locations u and $\acute{u}$, a randomized mechanism A satisfies geo-indistinguishability iff [48]

$$d_P(A(u), A(\acute{u})) \leq \epsilon d(u, \acute{u}), \qquad (21)$$

where $d_P(A(u), A(\acute{u}))$ is the multiplicative distance between two distributions $A(u)$ and $A(\acute{u})$ on some set S defined as $d_P(A(u), A(\acute{u})) = \sup_{S} \left|\ln \frac{A(u)(S)}{A(\acute{u})(S)}\right|$, and $d(u, \acute{u})$ is the Euclidean distance between u and $\acute{u}$.

Equation (21) can be equivalently written as

$$A(u)(w) \leq e^{\epsilon d(u,\acute{u})} A(\acute{u})(w),$$

for $w \in W$, and W is the set of possible outcomes.

To apply the Laplace mechanism, the noise added to u is derived from the following PDF:

$$f_{\epsilon,u}(w) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(u,w)}. \qquad (22)$$

The PDF in (22) implies that the probability of selecting w decreases exponentially with increasing the distance from u, i.e., $d(u, w)$. Substituting ϵ with ϵ/d_0, where d_0 is the desired indistinguishability distance, the mechanism provides a (d_0, ϵ)-location privacy [52]. Adopting the same procedure for generating Laplacian noise from [48], we can apply the Laplacian mechanism to the IoT data collection scenario. The mean PAoI of the network then can be obtained through simulation presented in the next section.

B. Gaussian Mechanism

For two neighboring datasets Z and $\acute{Z}$ and any output result T of a randomized mechanism M, the Gaussian mechanism of DP, also known as (ϵ, δ)-DP or approximate DP, where $\delta = 0$, is defined as [53]

$$P(M(Z) \in T) \leq e^{\epsilon} P(M(\acute{Z}) \in T) + \delta. \qquad (23)$$

To achieve (23), the sufficient condition is that an ϵ-DP is guaranteed with probability $1-\delta$. In other words, with probability δ, ϵ−privacy is no longer guaranteed [53].

The Gaussian mechanism applied to location privacy is similar. In particular, applying the same procedure in [53], we can see that for any location u and $\acute{u}$ and given $||u-\acute{u}||_2 \leq d_0$, a Gaussian noise $Q \sim N_q(0, \sigma_q)$ provides an (ϵ, δ) differential privacy if $\sigma_q \geq \frac{d_0}{\epsilon}\sqrt{2\ln\frac{2}{\delta}}$. The proof is presented in an Appendix at the end of the paper. We will provide the AoI and the Gaussian mechanism trade-off in the next section.

VI. Numerical Results

In this section, we provide the numerical results for the privacy of the proposed PPMs and mean PAoI trade-offs. The parameters values are listed in Table I.

TABLE I: Simulation Parameters

Parameter	Value
Number of IoT devices	N = 5
IoT Transmit power	p_0 = 1 mW
Bandwidth	B = 1 MHz
Thermal noise density	σ_0^2 = −174 dBm/Hz
UAV's altitude	H = 20 m
Data size	Ω = 2 Mb
Pathloss attenuation coefficient	α = 2, 4
UAV's velocity	v = 15 m/s
IoT devices location variance	σ_u^2 = 1000m^2

A. MMSE-based PPM

In this section, we provide the results for the MMSE-based PPMs. Figure 12a shows the AoI and privacy guarantee trade-off for N = 5 IoT devices in Case 1 where τ = 0. In this case, AoI is only due to the time it takes the UAV to complete the data collection. The trade-off is also shown in Figure 12b. From the two figures, it can be seen that, for example, for a noise variance of σ_q^2 = 4000 m^2, a privacy of 1600 m^2 is obtained for the adversary's mean squared estimation error. This is true for Cases 2 and 3 as well. Furthermore, we see that providing privacy comes with little cost. In particular, for σ_q^2 = 4000, which gives us a root mean squared (Rms) privacy of 40 m, we have only a 2.5% increase in AoI.

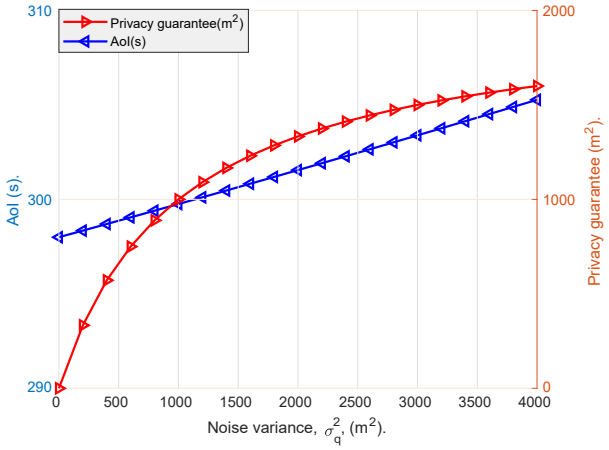
Figure 13a shows the trade-off in Case 2, where we assume a fixed data collection time. For simulation, we consider the least value of τ that would be needed for all values of σ_q^2. That is, assuming ϵ_0 = 0.001, we can consider τ ≥ 0.35 seconds. However, the AoI is increased by almost the very same 2.5%. Again, obtaining privacy has little cost on AoI. The achievable range is shown in the green shaded area in Figure 13b.

Figures 14a and 14b show the same trade-off for Case 3, where we consider τ as a function of σ_q^2, i.e., (18). In this case, and assuming ϵ_0 = 0.001, it can be seen that the AoI is increased by almost 3% for σ_q^2= 4000.

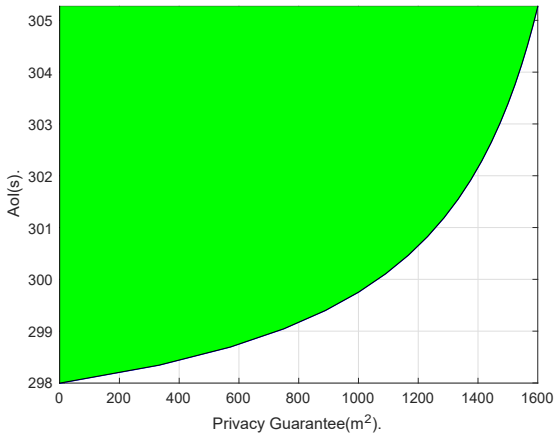
However, Case 4 is a little different as we recall that first, in this case, τ changes according to the fading as well as σ_q^2. And second, the adversary not only observes the UAV's location but also the time duration the UAV spends at each privacy-preserving point, τ. This leads to additional privacy leakage. Figure 15 shows the privacy leakage due to the observation of τ by the adversary. The point is that since the adversary only observes τ and has no idea about the channel power gains, h, (note that he knows σ_q^2), there is some error in his observations. For example, the adversary may infer that the IoT device is located at a distance d_1 from the UAV's location by simply observing τ. However, the IoT device is in fact at a distance of d_2 = d_1 due to the presence of channel power gain. In this case, Figures 16a and 16b show the AoI and privacy trade-off. It can be seen that the best Rms privacy guarantee of 40 m is decreased by 3.2% and the AoI is increased by 2.3%.

B. DP-based PPM

Now, we provide the results for the DP-based PPMs. Figure 17a shows the AoI-privacy trade-off for a Laplacian mechanism DP. Note in DP that smaller ϵ corresponds to larger privacy. Hence for the smaller values of ϵ and for a



(a) AoI and privacy guarantee trends.



(b) AoI and privacy guarantee trade-off in Case 1. The green-shaded area shows the achievable region.

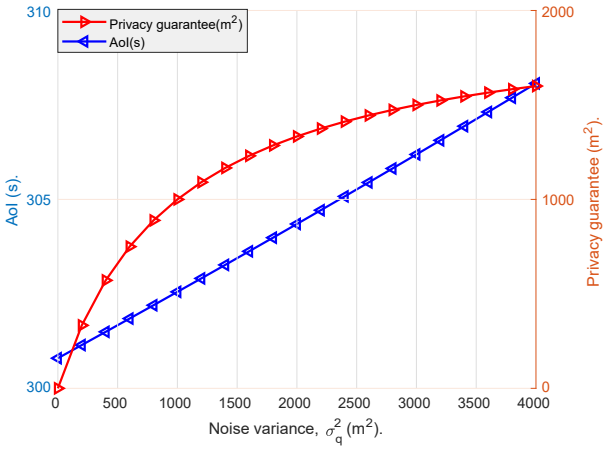
Figure 12: Privacy and AoI trade-offs in Case 1 (τ = 0).

geo-indistinguishability of d_0 = 10 m, we observe an almost 20% increase and for d_0 = 20 m a 60% increase in AoI, respectively.

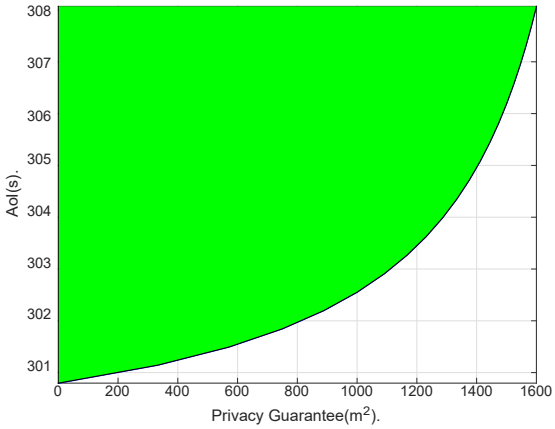
Finally, Figure 17b shows the AoI-privacy trade-off for the Gaussian-based DP which results in approximate DP. Assuming δ = 0.001, it can be seen that the AoI increase is negligible even for d_0 = 20 m.

VII. Conclusion

This paper proposed privacy-preserving mechanisms (PPMs) for UAVs in package delivery and IoT data collection applications. In the former, we proposed two PPMs for a UAV in which the goal is to confuse an adversary who is observing the UAV about the UAV's destination. This is accomplished through two randomization mechanisms. We obtained privacy guarantees along with energy efficiency guarantees for the proposed PPMs and analyzed the trade-offs. Then, we proposed a PPM for a UAV in the IoT data collection setting. The PPM is based on adding noise to the UAV's optimum location for data collection. We analyzed the privacy guarantee of the proposed PPM along with the AoI of the network. We showed that the proposed PPM has a negligible drawback on the AoI performance. Considering

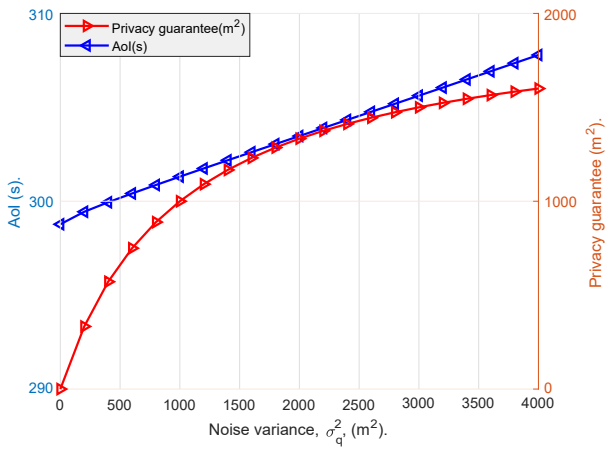


(a) AoI and privacy guarantee trends.

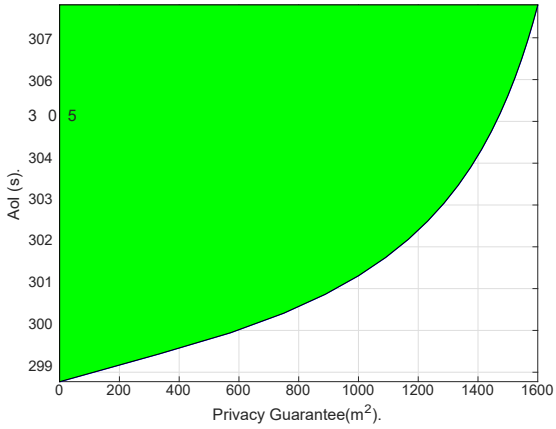


(b) AoI and privacy guarantee trade-off in Case 2. The green-shaded area shows the achievable region.

Figure 13: Privacy and AoI trade-offs in Case 2 ($\tau = c$).



(a) AoI and privacy guarantee trends.



(b) AoI and privacy guarantee trade-off in Case 3. The green-shaded area shows the achievable region.

Figure 14: Privacy and AoI trade-offs in Case 3 ($\tau(\sigma_q^2)$), $\epsilon_0 = 0.001$.

the limitations of the proposed PPM in some applications, we also provided DP-based counterparts for the proposed PPM and analyzed privacy trade-offs with the AoI.

There can be several avenues for future work: One can consider optimization problems for the proposed PPMs and other performance metrics such as UAV energy consumption, IoT energy harvesting, maximum coverage of devices, etc. Another direction can be considering stronger adversaries. In particular, in the IoT data collection scenario, by observing τ and having side information on the channel gains (Cases 3 and 4), an adversary is able to estimate the IoT device's distance from the UAV to the IoT device accurately. Therefore, it is essential to design stronger PPMs for this problem. Finally, in the package delivery scenario, one can design PPMs for a strong adversary where he can observe the UAV's speed as well as the UAV's trajectory.

Appendix

Here we show the proof of how the noise variance is obtained in the (ϵ, δ)-DP. Assume that $x \in \mathbb{R}^2$, $y \in \mathbb{R}^2$ are two arbitrary points with independent elements for which we define $v = x - y$ and $||v||_2 = d_0$. Let $x' = x + n$, where $n \in \mathbb{R}^2$ is a Gaussian noise $n \sim \mathcal{N}(0, \sigma^2)$, be the noisy version of x and y' be the noisy version of y. The privacy loss random variable is defined as $\kappa = \ln \frac{f_{x'}(x)}{f_{y'}(x)}$. We have

$$\kappa = \ln \frac{f_{x'}(x+n)}{f_{y'}(x+n)} \overset{(a)}{=} \ln \frac{\frac{1}{2\pi\sigma} e^{-\frac{||n||_2^2}{2\sigma^2}}}{\frac{1}{2\pi\sigma} e^{-\frac{||n+v||_2^2}{2\sigma^2}}}$$

$$= \ln e^{\frac{1}{2\sigma^2}(||n||_2^2 - ||n+v||_2^2)}$$

$$= \frac{1}{2\sigma^2} \sum_{k=1}^{2} 2v_k n_k + v^2,$$

where (a) comes from the fact that $\acute{x} \sim \mathcal{N}(x, \sigma^2)$ and $\acute{y} \sim \mathcal{N}(y, \sigma^2)$. It can be shown that $\kappa \sim \mathcal{N}(-\frac{d_0^2}{2\sigma^2}, \frac{d_0^2}{\sigma^2})$. Now, according to the definition of the approximate DP, we require that the probability of the privacy loss being larger than ϵ maintains below δ, i.e., $P[|\kappa| \geq \epsilon] \leq \delta$. After a few manipulations, we have

$$P[|\kappa| \geq \epsilon] \leq \delta = P[z > z] \leq \frac{\delta}{2}$$

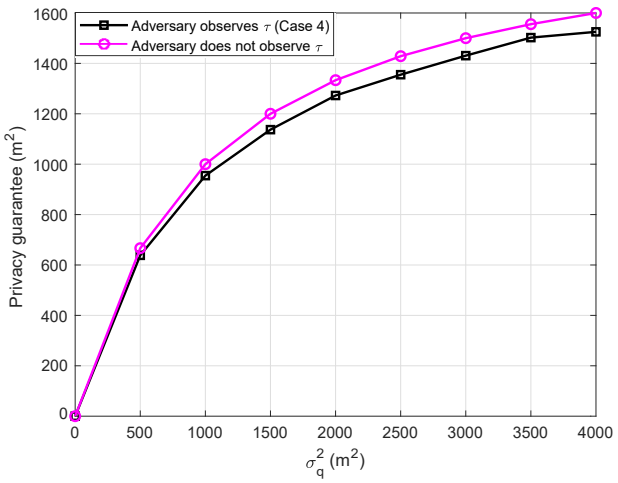
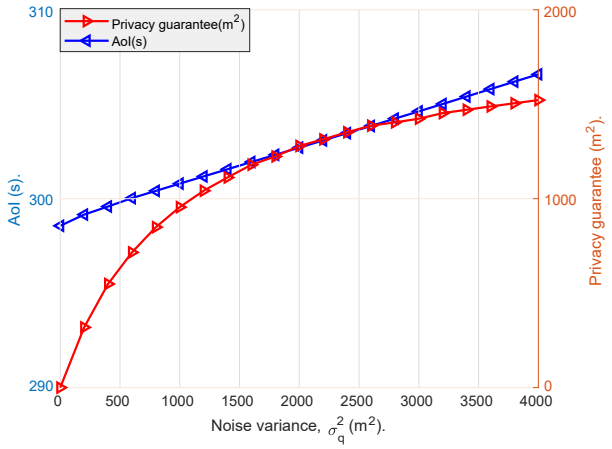
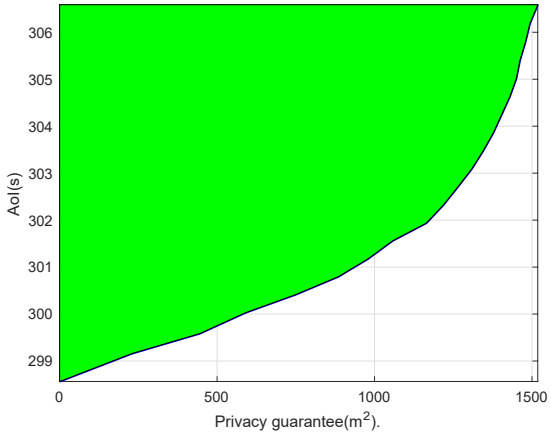


Figure 15: Privacy leakage when the adversary observes τ.

where $z \sim N(0,1)$, and $z = \frac{\sigma\epsilon}{d_0}$. Using the tail bound $P[z > z] \leq e^{-\frac{z^2}{2}}$ and a few more manipulations, we conclude that $\sigma \geq \frac{d_0}{\epsilon}\sqrt{2\ln\frac{2}{\delta}}$ is sufficient.



(a) AoI and privacy guarantee trends.



(b) AoI and privacy guarantee trade-off in Case 4. The green-shaded area shows the achievable region.

Figure 16: Privacy and AoI trade-offs in Case 4 where the adversary observes τ but does not know the channel fading, h.

REFERENCES

[1] S. Enayati, D. Goeckel, A. Houmansadr, and H. Pishro-Nik, "Privacy-preserving path-planning for UAVs," in International Symposium on Networks, Computers, and Communications, (ISNCC'22), Shenzhen, China, July. 2022.

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

[3] 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, pp. 1–6.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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/

[11] D. Cawthorne and A. R.-V. Wynsberghe, "From healthdrone to frugal-drone: 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.

[12] S. Say, H. Inata, J. Liu, and S. Shimamoto, "Priority-based data gathering framework in UAV-assisted wireless sensor networks," IEEE Sensors Journal, vol. 16, no. 14, pp. 5785–5794, May 2016.

[13] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications," IEEE Transactions on Wireless Communications, vol. 16, no. 11, pp. 7574–7589, Nov. 2017.

[14] M. Bradbury and A. Jhumka, "Quantifying source location privacy routing performance via divergence and information loss," IEEE Transactions on Information Forensics and Security, pp. 1–1, Early Access, 2022.

[15] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the internet of things: Perspectives and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2159–2187, April 2019.

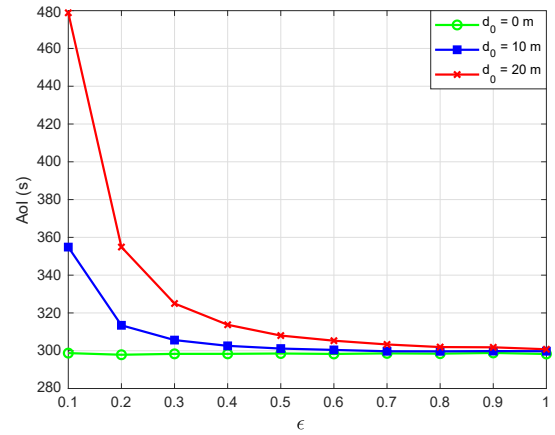
[16] Z. Montazeri, A. Houmansadr, and H. Pishro-Nik, "Achieving perfect location privacy in wireless devices using anonymization," IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2683–2698, Nov. 2017.

[17] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

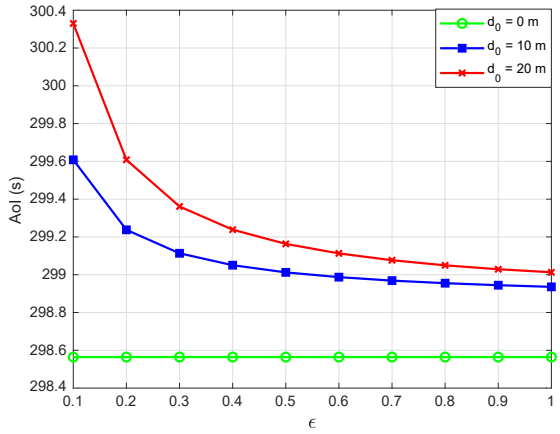
[18] S. Zou, J. Xi, H. Wang, and G. Xu, "CrowdBLPS: A blockchain-based location-privacy-preserving mobile crowdsensing system," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4206–4218, June 2020.

[19] S. Zou, J. Xi, G. Xu, M. Zhang, and Y. Lu, "CrowdHB: A decentralized location privacy-preserving crowdsensing system based on a hybrid blockchain network," IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14 803–14 817, Aug. 2022.

[20] B. Guan, N. Takbiri, D. Goeckel, A. Houmansadr, and H. Pishro-Nik,



(a) AoI and privacy guarantee trade-off for a Laplacian DP.



(b) AoI and privacy guarantee trade-off for a Gaussian DP mechanism with $\delta = 0.001$.

Figure 17: Privacy and AoI trade-offs in DP-based PPMs.

"Superstring-based sequence obfuscation to thwart pattern matching attacks," IEEE Internet of Things Journal, pp. 1–1, Early Access 2022.

[21] 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.

[22] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Orlando, FL, USA, Mar. 2012, pp. 2731–2735.

[23] X. Wang, C. Chen, J. He, S. Zhu, and X. Guan, "AoI-aware control and communication co-design for industrial IoT systems," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8464–8473, 2021.

[24] H. Zhang, Z. Jiang, S. Xu, and S. Zhou, "Error analysis for status update from sensors with temporally and spatially correlated observations," IEEE Transactions on Wireless Communications, vol. 20, no. 3, pp. 2136–2149, 2021.

[25] J. P. Champati, R. R. Avula, T. J. Oechtering, and J. Gross, "Minimum achievable peak age of information under service preemptions and request delay," IEEE Journal on Selected Areas in Communications, vol. 39, no. 5, pp. 1365–1379, 2021.

[26] L. Hu, Z. Chen, Y. Dong, Y. Jia, L. Liang, and M. Wang, "Status update in IoT networks: Age-of-information violation probability and optimal update rate," IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11 329–11 344, 2021.

[27] W. Yang, X. Lu, S. Yan, F. Shu, and Z. Li, "Age of information for short-packet covert communication," IEEE Wireless Communications Letters, pp. 1–1, 2021.

[28] Z. Jia, X. Qin, Z. Wang, and B. Liu, "Age-based path planning and data acquisition in UAV-assisted IoT networks," in IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, May 2019, pp. 1–6.

[29] H. Hu, K. Xiong, G. Qu, Q. Ni, P. Fan, and K. B. Letaief, "AoI-minimal trajectory planning and data collection in UAV-assisted wireless powered IoT networks," IEEE Internet of Things Journal, vol. 8, no. 2, pp. 1211–1223, Jan. 2021.

[30] J. Liu, P. Tong, X. Wang, B. Bai, and H. Dai, "UAV-aided data collection for information freshness in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 20, no. 4, pp. 2368–2382, 2021.

[31] W. Jiang, C. Shen, B. Ai, and H. Li, "Peak age of information minimization for UAV-aided wireless sensing and communications," in 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, July 2021, pp. 1–6.

[32] R. Han, J. Wang, L. Bai, J. Liu, and J. Choi, "Age of information and performance analysis for UAV-aided IoT systems," IEEE Internet of Things Journal, pp. 1–1, 2021.

[33] X. Lu, W. Yang, S. Yan, Z. Li, and D. W. K. Ng, "Covertness and timeliness of data collection in UAV-aided wireless-powered iot," IEEE Internet of Things Journal, vol. 9, no. 14, pp. 12 573–12 587, July 2022.

[34] C. Liu, Y. Guo, N. Li, and X. Song, "AoI-minimal task assignment and trajectory optimization in multi-UAV-assisted IoT networks," IEEE Internet of Things Journal, vol. 9, no. 21, pp. 21 777–21 791, Nov. 2022.

[35] X. Diao, X. Guan, and Y. Cai, "Joint offloading and trajectory optimization for complex status updates in UAV-assisted internet of things," IEEE Internet of Things Journal, pp. 1–1, Early Access 2022.

[36] C. Zhou, H. He, P. Yang, F. Lyu, W. Wu, N. Cheng, and X. Shen, "Deep RL-based trajectory planning for AoI minimization in UAV-assisted IoT," in 11th International Conference on Wireless Communications and Signal Processing (WCSP), Cian, China, Oct. 2019, pp. 1–6.

[37] M. Sun, X. Xu, X. Qin, and P. Zhang, "AoI-energy-aware UAV-assisted data collection for IoT networks: A deep reinforcement learning method," IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17 275–17 289, Dec. 2021.

[38] B. Zhu, E. Bedeer, H. H. Nguyen, R. Barton, and Z. Gao, "UAV trajectory planning for AoI-minimal data collection in UAV-aided IoT networks by transformer," IEEE Transactions on Wireless Communications, pp. 1–1, Early Access 2022.

[39] Z. Li, P. Tong, J. Liu, X. Wang, L. Xie, and H. Dai, "Learning-based data gathering for information freshness in UAV-assisted IoT networks," IEEE Internet of Things Journal, pp. 1–1, Early Access 2022.

[40] M. Rana and V. Mittal, "Wearable sensors for real-time kinematics analysis in sports: A review," IEEE Sensors Journal, vol. 21, no. 2, pp. 1187–1207, 2021.

[41] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1275–1313, 2019.

[42] A. F. Khalifeh, M. AlQudah, R. Tanash, and K. A. Darabkh, "A simulation study for UAV- aided wireless sensor network utilizing zigbee protocol," in 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, 2018, pp. 181–184.

[43] J.-M. Martinez-Caro and M.-D. Cano, "IoT system integrating unmanned aerial vehicles and lora technology: A performance evaluation study," Wireless Communications and Mobile Computing, vol. 2019, pp. 1–12, Nov. 2019.

[44] P. Marcon, J. Janousek, and R. Kadlec, "Vision-based and differential global positioning system to ensure precise autonomous landing of UAVs," in 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), Toyama, Japan, 2018, pp. 542–546.

[45] S. Qazi, A. S. Siddiqui, and A. I. Wagan, "UAV based real time video surveillance over 4G LTE," in 2015 International Conference on Open Source Systems & Technologies (ICOSST), Lahore, Pakistan, Dec. 2015, pp. 141–145.

[46] S. K. Khan, U. Naseem, A. Sattar, N. Waheed, A. Mir, A. Qazi, and M. Ismail, "UAV-aided 5G network in suburban, urban, dense urban, and high-rise urban environments," in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2020, pp. 1–4.

[47] E. Pastor, J. Lopez, and P. Royo, "A hardware/software architecture for UAV payload and mission control," in 2006 ieee/aiaa 25TH Digital Avionics Systems Conference, Portland, OR, USA, 2006, pp. 1–8.

[48] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 901–914.

[49] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," ACM Computing Surveys (CSUR), vol. 51, no. 3, pp. 1–38, 2018.
[50] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," ACM Computing Surveys (CSUR), vol. 54, no. 1, pp. 1–36, 2021.
[51] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," ACM Computing Surveys (CSUR), vol. 54, no. 10s, pp. 1–28, 2022.
[52] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," Transactions on Data Privacy, vol. 9, no. 1, pp. 15–48, 2016.
[53] C. Dwork, A. Roth et al., "The algorithmic foundations of differential privacy," Foundations and Trends® in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.

Saeede Enayati received the B.Sc. from Shahid Beheshti University in 2012 and the M.Sc. from Tarbiat Modares University in 2015 in Tehran, Iran, where she was a research assistant from 2016 to 2019 too. She received her Ph.D. degree from the Department of Electrical and Computer Engineering of the University of Massachusetts (UMass), Amherst, MA, USA in 2023 where she is currently a postdoctoral researcher. Her research interests include unmanned aerial vehicle networks, wireless network analysis, and covert communications.

Dennis Goeckel (Fellow, IEEE) received his BS from Purdue University in 1992, and his MS and PhD from the University of Michigan in 1993 and 1996, respectively. Since 1996, he has been with the ECE Department at the University of Massachusetts at Amherst, where he is currently a Professor. Prof. Goeckel has been a Lilly Teaching Fellow (2000-2001) and received the University of Massachusetts Distinguished Teaching Award in 2007. He received the NSF CAREER Award in 1999 and is an IEEE Fellow for "contributions to wireless communication systems and networks."

Amir Houmansadr (Member, IEEE) received the Ph.D. degree from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 2012. He is currently an Associate Professor with the Manning College of Information and Computer Sciences, University of Massachusetts at Amherst, Amherst, MA, USA. He works on specific problems, such as privacy-enhancing technologies, adversarial machine learning, statistical traffic analysis, and covert communications. His broad area of research is network security and privacy. Dr. Houmansadr has received several awards, including the Best Practical Paper Award at the IEEE Symposium on Security and Privacy in 2013, a Google Faculty Research Award in 2015, an NSF CAREER Award in 2016, and a DARPA Young Faculty Award in 2022.

Hossein Pishro-Nik (S'01-M'06) received the B.Sc. from the Sharif University of Technology, Tehran, Iran, and the M.Sc. and Ph.D. from the Georgia Institute of Technology, all in electrical and computer engineering. He is currently a Professor in the Department of Electrical and Computer Engineering at the University of Massachusetts, Amherst, MA, USA. His research interests include information theory, wireless networks, vehicular/UAV networks, privacy, statistical learning, and decision-making. His awards include an NSF Faculty Early Career Development (CAREER) Award, an Outstanding Junior Faculty Award from UMass, and an Outstanding Graduate Research Award from the Georgia Institute of Technology. He has served as an Associate Editor for IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, and IEEE Transactions on Information Forensics and Security.