Private UAV-Assisted IoT Data Collection: An Energy-Privacy Trade-off

Benjamin Fenelon
College of Information and Computer Sciences
UMass, Amherst
bfenelon@umass.edu

Saeede Enayati
Electrical and Computer Engineering
UMass, Amherst
senayati@umass.edu

Hossein Pishro-Nik
Electrical and Computer Engineering
UMass, Amherst
pishro@ecs.umass.edu

***Abstract*—Unmanned aerial vehicles (UAVs) offer intriguing possibilities for Internet of Things (IoT) data collection. However, it can also jeopardize the privacy of IoT devices. In particular, an adversary can deduce the location of IoTs by monitoring the UAV's mobility patterns, which necessitates the analysis of privacy-preserving mechanisms that protect IoT location privacy. Nonetheless, integrating privacy measures into operations incurs additional expenses. One of these costs is the added distance that UAVs may need to travel to accomplish their task, in turn increasing energy consumption. This paper investigates the trade-off between privacy and energy in the UAV-assisted IoT data collection application. First, we consider a preliminary privacy mechanism and analytically obtain the upper bounds of the extra flight distance and energy consumption for the UAV. Then, we consider a location-based differential privacy mechanism to achieve geo-indistinguishability. As expected, our study shows that imposing privacy constraints on UAV-assisted IoT data collection leads to increased UAV energy consumption. Specifically, as privacy guarantees become more restrictive, the energy consumption of UAVs increases exponentially. Nevertheless, given an energy constraint, one can assure a certain level of privacy guarantee.**

***Index Terms*—Location Privacy, Differential Privacy, UAV, IoT Data Collection, Energy Consumption.**

I. Introduction

A. Background

Unmanned aerial vehicles (UAVs) are becoming increasingly popular for their low cost and agility, making them viable options for various applications. However, UAVs have raised concerns over privacy violations by accessing areas that are otherwise inaccessible. To address these concerns, researchers have proposed privacy-preserving mechanisms (PPMs) that prevent UAVs from compromising citizens' privacy, e.g., [1]–[3].

However, UAV users' privacy can also be compromised through observation of UAV flight patterns. As pointed out in [4], adversaries can infer a UAV's destination from its flight path, leading to privacy breaches. To address this issue, [4] proposed privacy-preserving path design algorithms for UAVs in the presence of adversaries. The authors considered two scenarios: adversaries who can and cannot see the UAV's destinations, and developed path planning algorithms to hide the destinations from the adversary. Their work provides valuable insights into preserving UAV users' privacy. A different approach was developed in [5] where randomized trajectories were introduced to confuse the adversary about the UAV's destination in a package delivery application.

As UAVs are highly appealing for data collection in the realm of the Internet of Things (IoT), preserving IoT devices' locations from an adversary observing the UAV can pose challenges. In particular, leaking an IoT device's location makes it easy for an adversary to locate and potentially steal or destroy the device [6]. In this regard, preserving UAV's privacy is extended to the Internet of Things (IoT) application [7] where the UAV is employed to collect IoT data. The idea is to randomize the UAV's position around the IoT device instead of hovering directly above it.

Privacy comes at a price, however, which can be reflected in a variety of performance metrics. For instance, in an IoT data collection scenario, it may increase the UAV's energy consumption. This subsequently decreases the UAV's mission time and the number of IoT devices it can collect data from.

Therefore, in this paper, we investigate the UAV energy consumption and IoT location privacy trade-off in IoT data collection applications where a UAV is employed to collect data from IoT devices. We consider two types of location privacy mechanisms based on the randomization of the UAV's location: A preliminary privacy mechanism and a differential location privacy mechanism. The latter ensures location privacy for the IoT devices in the sense that by observing the UAV's location, an adversary will have difficulty distinguishing between IoT locations within certain distances. Therefore, each IoT device is satisfied by a degree of privacy within a certain range. We observe that imposing location privacy constraints on the UAV data collection application increases the total path and subsequently the energy consumption of the UAV. To the best of the authors' knowledge, this is the first paper to investigate the trade-off between location privacy and energy consumption in the context of UAV-assisted IoT data collection missions.

B. Related Work

As mentioned earlier, preserving citizens' privacy from potential UAV-related violations has been investigated from various points of view. For example, in [8], a dynamic UAV

This work was supported by NSF under grants CNS-1932326 and CNS-2150832.

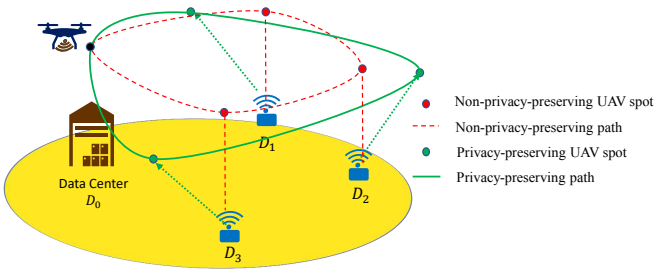

FIGURE 1: UAV-assisted IoT data collection: Instead of the red circle spot, the UAV hovers at a green spot to collect data from an IoT device. Subsequently, the red dashed path shows the non-privacy-preserving path and the solid green path shows a randomized privacy-preserving path.

routing framework was proposed to ensure that UAVs do not fly over the private property of citizens. [9] proposed a UAV detection system to identify unauthorized UAVs flying in a restricted area. [10] proposed a deep learning-based approach to anonymize faces captured by UAV video recordings. As long as the UAV's privacy is concerned, there have been numerous studies to protect UAVs from eavesdropping or adversaries, e.g., [11]–[13]. For instance, in [11], using particle swarm optimization (PSO), a path-planning algorithm has been developed to minimize the probability of being disclosed by an eavesdropper. [12] proposed a general privacy-preserving public cloud audit scheme which supports dynamic data to protect UAVs data.

Privacy challenges within the context of IoT are not a novel issue and have been regarded as a significant concern since its emergence [14]–[16]. Hence, various privacy-preserving techniques for location data have been developed and investigated [17]–[20]. Note that our approach to location privacy differs from that of the literature, which typically considers sets of location data.

C. Contributions and Organization:

The main contributions of this paper are as below:

- We propose two mechanisms for preserving IoT location privacy in UAV-assisted IoT data collection.
- We obtain the UAV energy consumption and IoT location privacy trade-offs of the proposed mechanisms.
- We show that by randomizing the UAV's location, IoT geo-indistinguishability can be obtained at the expense of energy consumption. But, given a certain energy constraint, one can still assure location privacy.

This paper is organized as follows:

In Section II, we describe the system model. In Section III, we provide the privacy-preserving mechanisms and energy consumption and in Section IV we present the results. Finally, in Section V we conclude the paper.

II. System Model

Figure 1 shows a typical UAV-assisted IoT data collection system model. We explain the network model, the adversary model, and the privacy-preserving mechanism in the sequel.

A. UAV-assisted IoT Data Collection Network

We assume that there are N IoT devices randomly located in an arbitrary area $\mathcal{A}$. An UAV is employed to fly from a data center located at the origin towards each device, hover above the devices at a fixed altitude H, and collect IoT data. The 2-dimensional coordinates of the i-th IoT device location are shown by $u_i = (x_i, y_i)$, where $x_i, y_i \in \mathbb{R}^2$ and $i = 1, 2, \ldots, N$. In a non-private scenario, the UAV would hover at (x_i, y_i, H) to maximize the uplink connection performance when collecting data from the i-th device.

However, to maintain location privacy for IoTs during data collection, the UAV hovers over a privacy-preserving spot selected randomly around the real location of the IoT device. The privacy-preserving spot is denoted as $v_i = (x_i', y_i')$, where $x_i', y_i' \in \mathbb{R}^2$.

B. Adversary Model

We assume that an adversary is interested in determining the true location of devices by monitoring the UAV's data collection activities. Consequently, the adversary is capable of tracking the path of the UAV and identifying its stopping points for IoTs data collection. We assume that the adversary cannot estimate the location by measuring the data collection time.

C. Privacy-preserving Mechanism

As mentioned earlier, in order to keep the IoTs location preserved from an adversary, we randomize the UAV's data collection spot so that the adversary would have difficulty identifying the exact location. To this end, we first consider a preliminary privacy mechanism and then a differential privacy alternative where locations within a certain range are indistinguishable. The details of the privacy mechanisms are provided in the next section.

III. IoT Location Privacy And UAV Energy Consumption

In this section, we provide the privacy-preserving mechanism and the UAV energy consumption analysis. Before that, we provide some preliminary results on the cost of location privacy-preserving mechanisms in the proposed context.

A. Preliminary result on the distance cost of location privacy

It is quite well-known that any privacy-preserving mechanism, regardless of its nature, has an associated cost to the utility. Regarding UAV-assisted IoT data collection, this cost could be perceived as the additional distance that the UAV has to fly. In other words, to ensure privacy and maintain a safe distance from the real location of the IoT device, the UAV may need to travel further to reach the privacy-preserving spot. This additional distance can impact the efficiency of data collection and may result in increased energy consumption or longer flight times for the UAV. In the following lemma, we show that there is an upper bound on the extra distance that any privacy mechanism with a privacy-preserving radius R might impose. This means that the total distance that the UAV

must travel in a privacy-preserving scenario, can be adjusted by the radius of the privacy mechanism.

Lemma 1. For N IoT devices, if we randomly choose a privacy-preserving spot within a distance R from each device, then the privacy-preserving path is longer than the non-privacy-preserving path by no more than $2NR$. Formally, we have

$$\sum_{i=1}^{N+1} d'_i \leq 2NR + \sum_{i=1}^{N+1} d_i, \tag{1}$$

where $d_i = ||u_i - u_{i-1}||_2$ and $d'_i = ||v_i - v_{i-1}||_2$ for $i = 1, \ldots, N$. Also, $d_{N+1} = ||u_N||_2$ and $d'_{N+1}||v_N||_2$. In (1), the left sum shows the overall privacy-preserving path and the right sum shows the overall non-privacy-preserving path.

Proof. Proof can be obtained using the triangle inequality for the devices subsequently. □

Discussion: It is not difficult to see that R is the privacy parameter. In other words, as R increases the perimeter of the circle around the IoT device increases which makes it more difficult for the adversary to estimate true device locations u_i.

B. Privacy-preserving Mechanism

We consider a differential location privacy (DLP) approach. It is important to note that DLP differs from Differential Privacy (DP) in that DP is typically used for aggregating data from multiple users. Whereas DLP is applied to the location data of a single user. The underlying principle behind DLP is that a small change in the location data of a user should not significantly impact the results of queries made using that data [21]. DLP has been developed using the notion of geo-indistinguishability [21] and has since garnered significant attention [22]–[24]. The advantage of utilizing a DP-based approach, as opposed to error-based approaches is particularly evident in scenarios where the prior distribution of IoTs is either unknown or known but results in intricate analysis.

The DLP considered in this paper is based on the Laplacian mechanism where the noise added to u_i is derived from the following PDF

$$f_{\epsilon,u_i}(w_i) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(u_i,w_i)}, i = 1, 2, \ldots, N, \tag{2}$$

where $d(u_i, w_i)$ denotes the Euclidean distance between u_i and w_i. Intuitively, (2) implies that the probability of selecting a random spot w_i decreases exponentially with increasing the distance from u_i. If we substitute ϵ with ϵ/d_0, where d_0 is the desired indistinguishability distance, the mechanism provides a (d_0, ϵ)-location privacy [25].

C. Energy Consumption Model

To compute the energy consumption of the drone, we use the propulsion power consumption of a rotary-wing UAV derived in [26] as

$$\begin{aligned} P(V) =& P_0 \left(1 + \frac{3V^2}{U_{\text{tip}}^2}\right) + P_i \left(\sqrt{1 + \frac{V^4}{4v_0^4}} - \frac{V^2}{2v_0^2}\right)^{1/2} \\ &+ \frac{1}{2} d_0 \rho s A V^3, \end{aligned} \tag{3}$$

where V denotes the drone's velocity and other parameters are constant metrics corresponding to the drone's physical features [26]. We assume that the UAV's communication power is negligible in comparison to the propulsion power consumption. Though future work can jointly consider communication [27] to prove tighter energy bounds.

Following (3), we obtain the propulsion energy consumption of the drone as below

$$E = \sum_{i=0}^{N} P(V) t_{f,(i,i+1)} + \sum_{i=1}^{N} P_h t_{h,i}, \tag{4}$$

where $t_{f,(i,i+1)}$ denotes the flight time from the spot i to the spot $i+1$, and $t_{h,i}$ is the hovering time above the i-th spot obtained as below

$$t_{h,i} = \frac{\omega_i}{B \log_2(1 + \gamma_i)}, i = 1, 2, \ldots, N, \tag{5}$$

where ω_i is the i-th device's data size, B is the bandwidth, and γ_i is the received signal to noise ratio (SNR) obtained as $\gamma_i = \frac{p_0 (H^2 + l^2)^{-\alpha/2}}{\sigma_0^2 B}$. Also, p_0 is the IoT's transmit power, l is the horizontal distance between an IoT and the UAV, α is the path-loss coefficient, and σ_0^2 is the thermal noise density.

Furthermore, in (4), P_h is the UAV's power consumption during the hovering which can be obtained as $P_h = \frac{\delta}{8} \rho s A \Omega^3 R^3 + (1 + k) \frac{W^{3/2}}{\sqrt{2\rho A}}$, where the parameters refer to fixed values that correspond to the physical attributes of the drone [26].

Lemma 2. For the preliminary privacy-preserving mechanism in Lemma 1, the additional energy consumption for a (d_0, ϵ)-private path (d'_t) is bounded as below

$$E(d'_t) - E(d_t) \leq P(V) \frac{2NR}{V} + \mathcal{E}, \tag{6}$$

where $\mathcal{E} = N P_h \frac{\omega}{B} \left(\frac{1}{\log_2\left(1 + \frac{p_0 (H^2 + R^2)^{-2}}{\sigma_0^2 B}\right)} - \frac{1}{\log_2\left(1 + \frac{p_0 H^{-2}}{\sigma_0^2 B}\right)} \right)$.

Proof. Assuming the same data size for all the devices, the second sum in (4) is a constant term. Therefore, energy is a function of the total path as defined below

$$E(d_t) = P(V) \frac{d_t}{V} + N P_h t^h \tag{7}$$

Hence, the energy difference in the private path (d'_t) and the non-private path (d_t) is obtained as below

$$\begin{aligned} E(d'_t) - E(d_t) &= P(V) \frac{d'_t - d_t}{V} + \mathcal{E} \\ &\leq P(V) \frac{2NR}{V} + \mathcal{E}, \end{aligned} \tag{8}$$

where $\mathcal{E}$ is given above. □

TABLE I: Simulation Parameters

Parameter	Value
Number of IoT devices	$N = 5$
UAV velocity	$V = 15$ m/s
UAV's altitude	$H = 20$ m
IoT Transmit power	$p_0 = 1$ mW
Bandwidth	$B = 1$ MHz
Data size	$\omega = 2$ Mb
Pathloss attenuation coefficient	$\alpha = 2, 4$

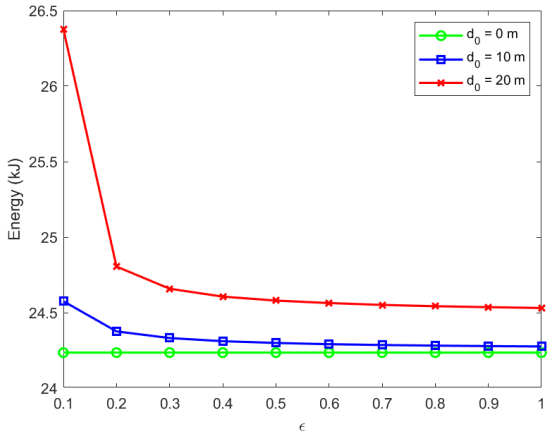

FIGURE 2: UAV energy consumption for (d_0, ϵ)-privacy

IV. Numerical Results

We now provide the numerical results for the trade-off between the proposed location privacy mechanism and the UAV energy consumption. The setting of simulation parameters follows from UAV energy minimization literature [7] [26] and are partially written in Table I. The goal is to model the effect of privacy parameters ϵ and d_0 on the total travel length (m) and energy consumption (kJ). For all graphs, the non-private path ($d_0 = 0$m) is ≈ 2600m.

Figure 2 shows the energy consumption vs. privacy guarantee for different distinguishability settings. A $d_0 = 0$ represents the case where there is no differential location privacy. In other words, there are no other locations near an IoT device's location that are indistinguishable from it. As the d_0 increases, the locations that are indistinguishable from the real IoT's location increase which means more differential location privacy is imposed. This, in turn, increases the UAV's energy consumption. Observe the exponential decrease in energy required when relaxing the privacy with ϵ.

Figure 3 shows the UAV's energy consumption on a log scale versus the location indistinguishability for different values of ϵ. It can be seen that the small value of $\epsilon_0 = 0.1$ results in a significant increase in energy consumption. Meanwhile, with an imposed energy consumption constraint, one may adjust the desired values of both d_0 and ϵ. This (d_0, ϵ)-privacy mechanism increases UAV's energy consumption exponentially while in Lemma 2, we see a linear relationship between energy consumption and the privacy parameter, R.

Figure 4 shows the total distance added to the UAV's

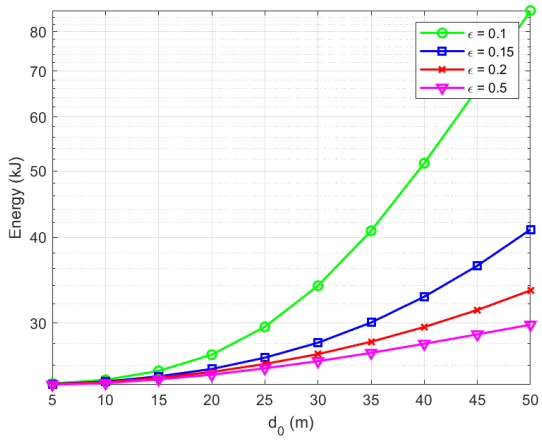

FIGURE 3: UAV energy consumption and geo-indistinguishability trade-off for (d_0, ϵ)-privacy

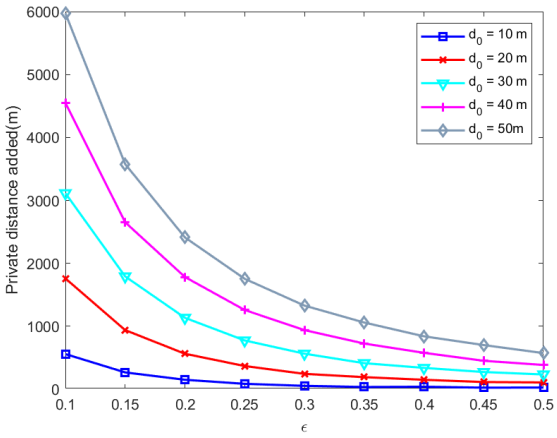

FIGURE 4: Total path increase for (d_0, ϵ)-privacy

path after imposing (d_0, ϵ) privacy. The additional distance covered assumes critical importance in scenarios where energy consumption is not the primary concern, but flight time duration and subsequently the freshness of updates from IoT devices, as measured by their age of information (AoI), are of significance. In such cases, adjusting the UAV's velocity to comply with the AoI constraint may be a viable option. As velocity, among other parameters in 3, scales the energy consumption linearly. Finally, Figure 5 presents the proportion of the total distance covered by a privacy-preserving path relative to a non-privacy-preserving path, providing an intuitive comparison between the two. It is worth noting that the privacy-preserving path can be up to three times longer than the non-privacy-preserving path.

V. Conclusion

In this paper, we investigated the trade-off between UAV energy consumption and IoT location privacy in the context of an IoT data collection application. We obtained the upper bound of the total distance increase and UAV's energy consumption increase for a preliminary privacy mechanism.

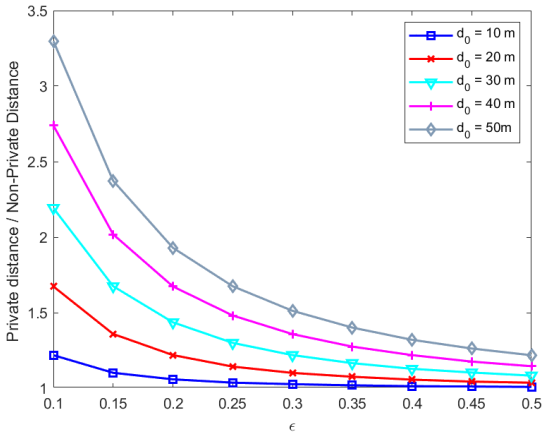

FIGURE 5: Private vs. Non-Private Path Ratio

Then, considering the differential location privacy, we obtained the UAV's energy consumption and privacy parameters using simulations. We have established that, by adjusting the privacy parameters, it is possible to attain a desired degree of privacy while adhering to a given UAV energy constraint. Also, the total distance added to the UAV's path has been obtained which can be crucial for analyzing AoI.

This paper has several avenues for future work: One can investigate the trade-off between the energy consumption of IoT devices and privacy policies. This is important since the performance of IoT devices is typically constrained by their limited power supply. Another direction is to optimize the privacy-preserving spots among a network of IoTs such that different IoTs could be under coverage from a shared privacy-preserving spot. In this problem instead of subsequently flying between different spots, a UAV may hover at the same spot for a longer duration to collect data from more than one device.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] S. Enayati, D. Goeckel, and H. Houmansadr, Amir Pishro-Nik, "Location privacy protection for UAVs in package delivery and IoT data collection," *Under Review in IEEE Internet of Things Journal*, Jan. 2023.

[8] 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.

[9] A. Aouto, J.-M. Lee, and D.-S. Kim, "UAV detection using split-parallel CNN for surveillance systems," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Republic of, October 2021, pp. 1178–1181.

[10] H. Lee, M. U. Kim, Y. Kim, H. Lyu, and H. J. Yang, "Development of a privacy-preserving UAV system with deep learning-based face anonymization," *IEEE Access*, vol. 9, pp. 132 652–132 662, September 2021.

[11] 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)*, Zhanjiang, China, 2020, pp. 837–842.

[12] J. Liu, X. A. Wang, Z. Liu, H. Wang, and X. Yang, "Privacy-preserving public cloud audit scheme supporting dynamic data for unmanned aerial vehicles," *IEEE Access*, vol. 8, pp. 79 428–79 439, April 2020.

[13] Z. Lv, L. Qiao, M. S. Hossain, and B. J. Choi, "Analysis of using blockchain to protect the privacy of drone big data," *IEEE Network*, vol. 35, no. 1, pp. 44–49, January/February 2021.

[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, October 2017.

[15] S. Wilson, N. Moustafa, and E. Sitnikova, "A digital identity stack to improve privacy in the IoT," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, February 2018, pp. 25–29.

[16] A. Assiri and H. Almagwashi, "IoT security and privacy issues," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, April 2018, pp. 1–5.

[17] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IOT," in *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology*, Shenzhen, China, 2011, pp. 192–195.

[18] I. Ullah and M. Ali Shah, "A novel model for preserving location privacy in internet of things," in *22nd International Conference on Automation and Computing (ICAC)*, Colchester, UK, Sept. 2016, pp. 542–547.

[19] 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, August 2018.

[20] M. Bi, Y. Wang, Z. Cai, and X. Tong, "A privacy-preserving mechanism based on local differential privacy in edge computing," *China Communications*, vol. 17, no. 9, pp. 50–65, September 2020.

[21] 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.

[22] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, pp. 1–38, 2018.

[23] 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.

[24] 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.

[25] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Transactions on Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.

[26] Y. Zeng, J. Xu, and R. Zhang, "Energy minimization for wireless communication with rotary-wing uav," *IEEE Transactions on Wireless Communications*, vol. 18, no. 4, pp. 2329–2345, Apr. 2019.

[27] Z. Wang, R. Liu, Q. Liu, J. S. Thompson, and M. Kadoch, "Energy-efficient data collection and device positioning in uav-assisted iot," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1122–1139, 2020.