sensors

MDPI

Review

A Survey of Dummy-Based Location Privacy Protection Techniques for Location-Based Services

Shiwen Zhang [1], Mengling Li [1], Wei Liang [1], Voundi Koe Arthur Sandor [2] and Xiong Li [1,3,*]

[1] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[2] School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China
[3] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
* Correspondence: lixiongzhq@163.com

Abstract: As smart devices and mobile positioning technologies improve, location-based services (LBS) have grown in popularity. The LBS environment provides considerable convenience to users, but it also poses a significant threat to their privacy. A large number of research works have emerged to protect users' privacy. Dummy-based location privacy protection solutions have been widely adopted for their simplicity and enhanced privacy protection results, but there are few reviews on dummy-based location privacy protection. Or, for existing works, some focus on aspects of cryptography, anonymity, or other comprehensive reviews that do not provide enough reviews on dummy-based privacy protection. In this paper, the authors provide a review of dummy-based location privacy protection techniques for location-based services. More specifically, the connection between the level of privacy protection, the quality of service, and the system overhead is summarized. The difference and connection between various location privacy protection techniques are also described. The dummy-based attack models are presented. Then, the algorithms for dummy location selection are analyzed and evaluated. Finally, we thoroughly evaluate different dummy location selection methods and arrive at a highly useful evaluation result. This result is valuable both to users and researchers who are studying this field.

Keywords: location privacy; privacy protection; dummy location

Citation: Zhang, S.; Li, M.; Liang, W.; Sandor, V.K.A.; Li, X. A Survey of Dummy-Based Location Privacy Protection Techniques for Location-Based Services. *Sensors* **2022**, *22*, 6141. https://doi.org/10.3390/s22166141

Academic Editor: Ivan Andonovic

Received: 26 July 2022
Accepted: 8 August 2022
Published: 17 August 2022

1. Introduction

In the United States, a large majority (90%) of smartphone owners used location-based services [1]. Locations are being used more frequently than ever before since the global pandemic. For example, the government should keep a record of every location ever visited, and track the whereabouts of people who have tested positive for COVID-19 to determine where the virus is likely to spread next [2]. Furthermore, location-based services will continue to gain attention and become more widely used in the future. According to Federica Laricchia, the annual worldwide blue-tooth location service device shipments reached 183 million units in 2021, with yearly shipments expected to reach 568 million units in 2026 [3].

While location-based services are widely used and provide significant convenience to users and society, they also pose a significant threat to privacy. According to risk-based security [4], the total amount of global data leakage in 2021 has reached 22 billion, which is about 14.5 billion less than in 2020. However, such an amount also quantifies the second highest year for confidential data leakage since 2005. As shown in Figure 1, a survey conducted by the China Consumers Association [5] in 2018 found that more than 80% of respondents had experienced personal information leakage. Moreover, it is common for mobile apps to collect excessive amounts of personal information, while location data have evolved into a type of profitable resource.

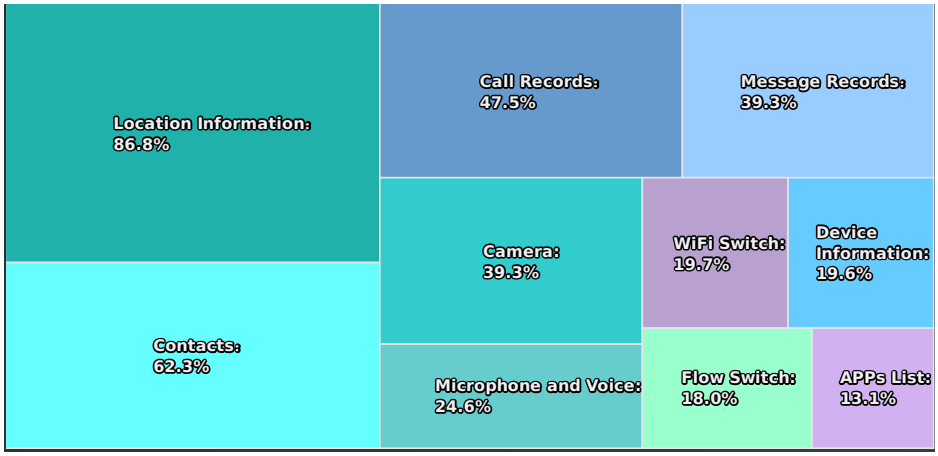


Figure 1. Permissions to install and use mobile apps.

In most cases, location data are linked to other sensitive attributes, such as health status, home address, behavioral habits, and other privacy concerns. As a result, protecting the location information of smartphone users, specially those who use location-based services, is critical and urgent.

Dummy refers to the method of adding multiple dummy locations and sending them to the LBS server along with the real query location to blur the real location. Domestic and foreign researchers have proposed a variety of location privacy protection schemes based on dummy. For example, Kido et al. proposed the first dummy-based location privacy protection techniques in the literature [6]. They generated dummy locations at random using the random walk model. Hara et al. [7] designed a method for selecting dummies that takes real-world constraints into account, such as excluding places where people are unlikely to exist. Niu B. [8] proposed a Cir-dummy- and Grid-dummy-based dummy location selection algorithm. Shu C. [9] proposed two new dummy selection algorithms, MaxMinDistDS and Simp-MaxMinDistDS, that take both the location semantic diversity and the physical dispersion into account.

There are numerous dummy-based schemes being made to deal with location privacy. However, reviews for dummy-based schemes are relatively rare, and some focus on aspects relating to cryptography [10], anonymity [11], or other comprehensive reviews [12], which focus on the whole picture, but there are not enough review on dummy-based privacy protection. In addition, these reviews fail to clarify the relationship between the level of privacy (LoP), the quality of service (QoS), and system overhead. These are struggle to explain the difference and relationship between dummy and other location privacy protection techniques, as well as analyze and summarize the dummy location attack model and how to choose dummies. Therefore, such studies cannot help readers understand the up-to-date challenges of dummy-based privacy protection brought on by attackers' expanding background knowledge and the intersection between LBS and other emerging technologies.

In this paper, we make a review of dummy-based location privacy protection techniques for location-based services. The main contributions are as follows.

- First, we distinguish the relationship between the LoP, the QoS, and the system overhead. Additionally, we make an overall comparison of several representative methods of location privacy protection techniques. Then, we describe the merits of dummy-based location privacy protection on LBS. Meanwhile, a summary of the major attacks on dummy-based location privacy protection techniques is also included.
- Second, we systematically and comprehensively analyze and summarize the ways of selecting dummies on three aspects, namely the query probability, the physical dispersion, and the semantic diversity of locations.
- Third, we provide an overview of the methods for achieving query probability, physical dispersion, and semantic diversity while choosing dummies. Furthermore, we

make comparative analysis to indicate the different privacy protection advantages of different selection rules when choosing dummies. Results of this comparative analysis can be of benefit both to users and researchers who are studying this field.

The remainder of this paper is organized as follows. Section 2 gives an overview of location privacy protection, and Section 3 provides a summary of the attack model of dummy-based location privacy protection techniques. Section 4 describes the system architecture and privacy protection methods, and also gives a detailed analysis and summary of how to choose a dummy location. Finally, in Section 5, we conclude our work.

2. Overview of Location Privacy Protection

In this section, we first introduce the key issues in location privacy protection and location privacy protection techniques. Then, we describe the difference and connection of various location privacy protection techniques, and finally make a comparison between them.

2.1. Location Privacy Protection

When users use LBS, their location privacy is compromised to some degree due to dishonest or semi-trusted LBS servers serving private interests. Nonetheless, because location privacy is closely related to explicit sensitive information, other implicit sensitive information about users is also leaked. Take, for example, John. He has been feeling uneasy lately, so he decides to go to the hospital to find out what's wrong with his body. However, because he does not want others to know about his medical condition, the hospital's location is important to him. In reality, "where are you staying" reveals the privacy of "what are you doing". Similarly, the user's historical location data expose the locations he frequently shows up at, and the routes he travels a lot by, which leads to his home address, behavioral habits, work nature, and other sensitive information he cares about potentially being leaked [13]. Therefore, there is no doubt that it is definitely vital to protect a user's location privacy.

2.2. Key Issues of Location Privacy Protection

When it comes to location privacy protection, it is naturally necessary to consider the connection between LoP, QoS, and the system overhead [14].

2.2.1. Issue on the Relationship between LoP and QoS

In location privacy protection, high LoP and QoS cannot be satisfied at the same time. To obtain location services, users must submit their location to the service provider in some way, which risks exposing their private information. Many techniques, such as using cloaking areas instead of the real location, adding noise to the real location, and so on, sacrifice some degree of location accuracy for higher LoP. However, if the location accuracy is too low to meet users' demands, availability will suffer, and privacy protection will be rendered ineffective. Furthermore, the requirements for location service quality vary depending on the user. Users who request to query a specific point of interest will be more concerned with QoS. Users seeking hospital location service, on the other hand, will be more concerned with their location information. As a result, they are willing to sacrifice some service quality in exchange for a higher LoP. Therefore, understanding the relationship between QoS and LoP is one of the most crucial matters in location privacy protection.

2.2.2. Issue on the Relationship between QoS and System Overhead

With the advent of the "fast" era, people are more concerned with speed, even when it comes to location privacy protection. People desire faster response times and lower latency. When a user initiates a query request, the user experience will suffer if the response time is too slow. However, the majority of existing studies improve LoP without taking system overhead into account, or at the expense of a significant increase in system overhead to achieve a minor improvement in LoP. Simultaneously, the costs of communication,

storage, and computation, as well as the loss of precision, all have an impact on the user experience due to the limited resources on the user's device. For example, a large amount of computation cost slows down the processing speed of mobile devices, a large amount of communication cost raises the extra cost for users, and a large amount of electricity overhead affects outdoor use of mobile devices, ultimately hindering the development of location service [15]. Understanding the relationship between LoP and the system overhead is therefore another critical issue in location privacy protection.

2.3. Location Privacy Protection Techniques

Researchers proposed numerous approaches to protect location privacy, such as [16–19]. In general, location privacy protection techniques can be divided into four categories [20]: obfuscation [21], encryption [22–24], cache and collaboration [25], and anonymity mechanisms [26].

2.3.1. Location Privacy Protection Techniques Based on Obfuscation

Location privacy protection techniques based on obfuscation refer to the necessary disruption to the original location information in an LBS query in order to prevent the attacker from obtaining the user's true location while also ensuring that the user can acquire unrestricted services. Dummy [6], spatial cloaking [27,28], differential privacy [29], and other obfuscation techniques can reduce the accuracy of location information. The dummy method adds multiple dummies and sends them to the LBS server along with the real query location to blur the real location. To protect users' location privacy, Li et al. [30] proposed an attribute-aware privacy protection scheme (APS). The Voronoi dividing algorithm (VDA) and the dummy determining algorithm (DDA) are two algorithms included in APS. The VDA algorithm divides the local map into different Voronoi polygons to ensure that the selected dummy locations are scattered, whereas the DDA algorithm chooses dummy locations based on the four-color mapping theorem to ensure that dummy locations differ in attributes. The classical dummy method, which was later extended to trajectory, is frequently used to solve the single location problem. Ni et al. [31] proposed an R-constrained dummy trajectory-based privacy-preserving algorithm (RcDT). The generated dummy locations are in a specific range close to the real location because the generating range R of the dummy location is constrained. Furthermore, by constraining the exposure risk of each dummy location and trajectory, dummy trajectories with a higher similarity to the real trajectory are generated. Differential privacy protects location privacy by adding an appropriate number of noises to the returned value of the query function [29]. Several recent studies [32,33] have investigated the use of differential privacy in location protection. The concept of protecting user locations within a radius R, whose privacy level is dependent on R, is formally defined by the term of geographical indiscernibility [32]. To increase the user's LoP, controlled random noise is added to their location. In general, using the obfuscation strategy will result in a significant loss of precision in query results.

2.3.2. Location Privacy Protection Techniques Based on Encryption

To achieve the privacy goals, the cryptographic approach adopts encryption technology to make the user's query content and location information completely transparent to the LBS server. While ensuring QoS, this technique does not reveal any user's location information, ensuring stricter privacy protection. Private information retrieval (PIR) [34,35] is a popular encryption method. PIR prevents the server (the database owner) from determining the user's point of interest and drawing additional conclusions about the client's private information by ensuring that the server (the database owner) cannot determine the correct query object when the user requests the database. Paulet et al. [34] obtained and decrypted location data using a PIR-based protocol. The user's location information was kept private because the server was unable to determine it. The PIR method ensures the confidentiality of the entire communication process (user request, information retrieval, and result return process). However, the issue of over-collected storage and computation overhead in PIR needs to be investigated further. The primary challenge in using PIR

is developing a good retrieval strategy and index structure. However, because the LBS server must store the entire map information of the local map, the server's limited storage space as well as retrieval efficiency make PIR only applicable to a small space range at the present time.

2.3.3. Location Privacy Protection Techniques Based on Collaboration and Cache

Collaboration and caching cut down the time spent communicating with the LBS server as much as possible in order to limit exposure to location-sensitive information. Domingo-ferrer et al. [36] proposed a cooperative method for disturbing users' location information by adding Gaussian noise. This method requests disturbed location information from other users and then forms a cloaking region according to that information. Rather than using the true location, the anonymous group's density center, formed by cooperative users, is used as the anchor point to replace it and launch query requests. Shokri et al. [37] proposed an effective collaborative location privacy protection approach. Zhang et al. [38] proposed a cache and spatial K-anonymity-based privacy enhancement technique.

This strategy employs a multi-level caching method to reduce the possibility of user location information being disclosed. Niu et al. [39] created a privacy protection algorithm using dummy locations and cache awareness. The research on privacy protection techniques based on caching and collaboration focuses on three main areas: reducing cache overhead, improving the cache hit ratio and location privacy, and quantifying the QoS level. Another consideration is how to reduce the expensive communication cost caused by such a collaborative technique architecture.

2.3.4. Location Privacy Protection Techniques Based on Anonymity

Methods based on anonymity to protect location privacy, such as k-anonymity and mix-zone, protect privacy by breaking the link between user identity and location data. The k-anonymity [40] technique ensures that the user's location information cannot be differentiated from that of other $k-1$ users through generalization. As a result, attackers have a $1/k$ chance of discovering users' true location. Stajano et al. [41] proposed the Mix-zone, which differs from the k-anonymity scheme. Attackers are unable to precisely pinpoint the user's real location by frequently changing the user's name or pseudonym in the anonymity area. In a variety of settings, anonymous approaches have been thoroughly researched and tested. However, this strategy raises concerns because maintaining the same level of anonymity in different scenarios is difficult.

The relationship between location privacy, location privacy protection techniques, obfuscation, and dummy generation is depicted in Figure 2. Table 1 compares existing location privacy protection techniques in terms of LoP, outlining their main advantages and disadvantages. The system overhead of the four location-based privacy protection techniques is compared in Table 2. Given that different privacy protection techniques provide different benefits, we must adopt location privacy protection methods that are appropriate for the given application in order to protect the user's location privacy.

Table 1. The comparison among four privacy protection techniques.

LPPT [1]	RM [2]	LoP [3]	TTP
Obfuscation	Dummy Spatial Cloaking Differential Privacy	low	yes
Encryption	PIR	high	no
Collaboration and Cache		medium	no
Anonymity	K-anonymity Mix-zone	medium	yes

[1] LPPT:location privacy protection techniques. [2] RM: representative method. [3] LoP: the level of protection privacy.

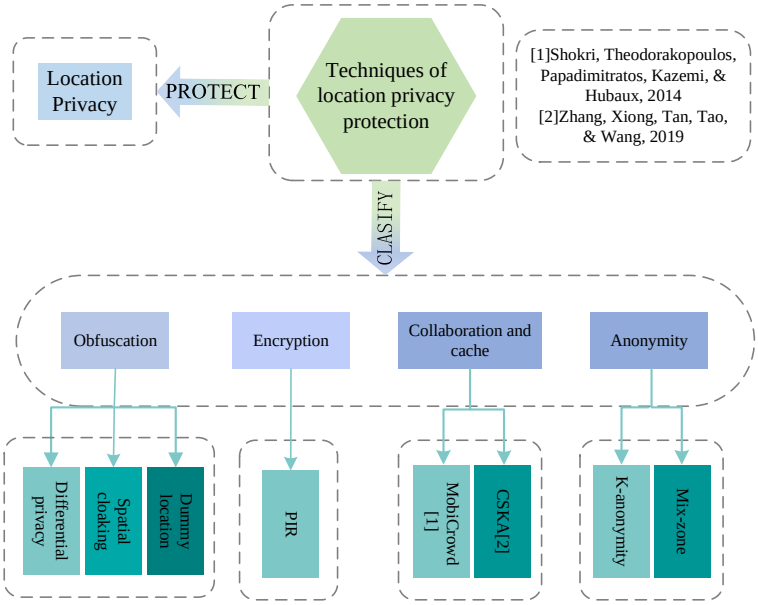


Figure 2. The relationship among location privacy, location privacy protection techniques, the obfuscation, and dummy location.

Table 2. The cost of four privacy protection techniques.

LPPT	Precision Loss	Communication Cost	Computation Cost	Storage Cost
Obfuscation	high	low	low	low
Encryption	low	low	high	medium
Collaboration and Cache	medium	high	low	high
Anonymity	medium	medium	high	medium

Dummy is an important obfuscation method that has stimulated the interest of researchers both at home and abroad. This is becayse it is simple to implement, does not require a trusted third party, and can protect location privacy while maintaining accuracy. Furthermore, we can see that dummy has other advantages over other privacy protections in Tables 1 and 2, such as low communication costs, low computation costs, and low storage costs.

3. Dummy-Based Attack Model

Malicious attackers aim to exploit various types of external information to find sensitive information about users, in addition to processing queries using various privacy protection mechanisms. However, the user's location contains inherent "side information", such as route information, human flow, and population distribution of the geographical region where the user is located [39,42]. Furthermore, attackers can obtain background knowledge in a variety of ways, including collaborative information systems, publicly available data aggregation, data brokers, data mining, and so on, in the age of Big Data and the Internet of Things.

Based on the attacker's prior knowledge in two dimensions, namely temporal information and context information, attacks can be classified into context dimension attacks and temporal dimension attacks [43]. In the former case, the attacker only has a single snapshot of a user's location, whereas in the latter case, the attacker has several locations collected over time or even a trajectory. We only consider the attack model on the context dimension in this paper because time is not taken into account. The most common threat to

dummy-based location privacy protection techniques is background knowledge attacks in the context dimension. Such attacks can be classified into three types based on the attackers' prior knowledge: location-distributed attack, probability-distributed attack, and semantic similarity attack. This section will summarize the attack model of dummy-based location privacy protection techniques.

3.1. Location-Distributed Attack

The location distribution attack is a type of attack method in which the attacker explores the location distribution characteristics in the user-specified cloaking area. It is classified into three types. One is that the location distribution of the cloaking area is overly concentrated, resulting in a small hidden area. For example, all of the locations are in the same neighborhood. However, although it successfully blurs users' real locations, users' location privacy cannot be adequately protected. Regarding the second type, the user's true location is in the middle of the entire cloaking region, and the attacker can significantly reduce the user's range [44]. For instance, all of the dummy positions are centered on the real location. In the third type, the real cloaking area shrinks as a result of the uneven location distribution caused by the attacker's exclusion of some locations, which fails to meet the theoretical cloaking requirements. For example, if the majority of locations are distributed in a concentrated manner while one or two or a small portion of them are distributed in a relatively scattered manner, attackers can easily filter out those locations, reducing the original privacy protection intensity [45].

3.2. Probability-Distributed Attack

The probability distributed attack is defined as the attacker calculating historical query probability information by collecting historical service request records for all locations within a specific geographical region and over a specific time period [46]. When the probability distribution in the anonymous set generated by the user's query request is uneven, the attacker filters out the dummy locations with a large gap, resulting in a failure to achieve the true location privacy protection effect. If the chosen dummy locations set includes several dummy locations in the middle of the lake with zero query probability, the attacker can simply deduce that they are dummy locations and filter them out.

3.3. Semantic Similarity Attack

The semantic similarity attack refers to the attacker's speculation on the privacy information of users by parsing semantic information of locations in cloaking regions, such as behavior habits, health status, and professional attributes [47]. As long as all dummies' query probabilities and the real location of the user's query probability are equal or close, attackers can easily infer user behavior if all dummies in cloaking areas belong to the same kind of semantics.

4. Dummy-Based Location Privacy Protection Techniques

In this section, we outline the two system architectures of dummy-based location privacy protection techniques, then review the dummy-based location privacy protection techniques, and finally analyze and summarize how the dummy-based location privacy protection techniques choose dummies to handle background knowledge attacks.

4.1. System Architectures of Dummy-Based Location Privacy Protection

Dummy generation system architectures can be divided into two types: architecture with a third party and architecture without a third party, depending on whether a third party is deployed or not [48].

4.1.1. Architecture with a Third Party

This architecture consists of users, a third party, and an LBS server. One or more servers represent a third party [49,50], and these are the servers that generate the dummy location set for the query user in order to mask the true location. Figure 3 depicts a third-party

architecture. The primary responsibility of the third party is to collect and process user query requests, protect sensitive location information using privacy protection techniques, and then forward the processed query requests to the LBS server. After receiving these requests from the third party, the LBS server retrieves the database and transmits the matching result sets to the third-party servers. Finally, the requesting users receive the result sets from the third-party servers. Third-party servers, for example, create a cloaking zone with multiple users, and all users in the zone submit the same query to LBS. In this case, the LBS server is unable to determine who initiated the query and, as a result, is unable to find out which location is the original requesting location.

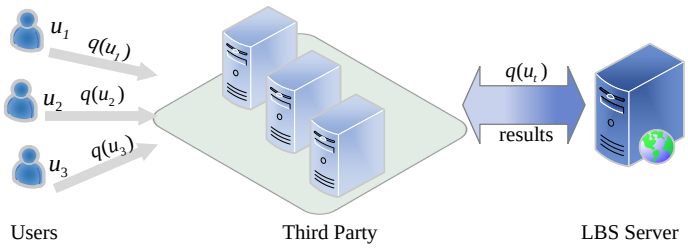


Figure 3. The architecture with a third party.

Obtaining a completely trustworthy third party, on the other hand, is difficult, and the "honest but curious" third party is vulnerable to a single point of attack and other vulnerabilities. As a result, the researchers have proposed an architecture that does not rely on a third party.

4.1.2. Architecture without a Third Party

Figure 4 depicts the architecture in the absence of a third party, which consists of users and an LBS server.

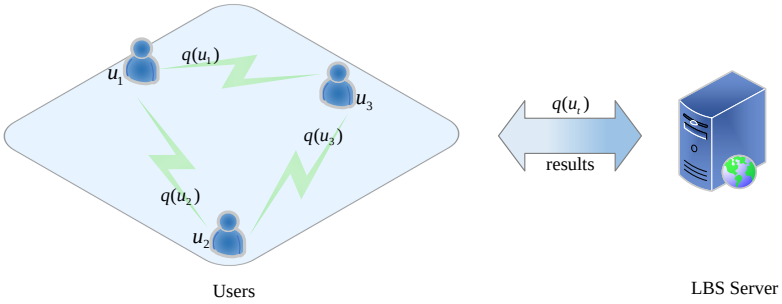


Figure 4. The architecture without a third party.

The architecture requires that mobile devices carried by users have certain computational and storage capabilities that can be used to select dummy locations, create cloaking areas, and save map data within a certain range. The non-third-party architecture can be divided into two types based on whether or not users collaborate. In the first type, users' location information is concealed in accordance with their privacy requirements [51]. For example, the Apple differential privacy team uses local differential privacy [52]. Users' personal data can be randomized on their devices before being uploaded to the server, which can improve the user experience without infringing on privacy. In the second type, users collaborate for the sake of secrecy [53]. Tor, for example, is a volunteer-run distributed relay network that enables users to conceal their location while providing a variety of services. When using this method of obscuring through user collaboration, it is important to consider the additional communication cost between users as well as the risk of collusion attack [54].

4.2. The Dummy-Based Location Privacy Protection Techniques

The dummy-based location privacy protection techniques select many dummy locations (assuming $k-1$ dummies) and send the same query request to the LBS server with

the real location, making it difficult for the LBS server to distinguish the real ones from those k locations. However, if those dummies are chosen at random or without taking into account the attacker's background knowledge, some of the dummy locations will be too large for the attacker to filter out, and the theoretical LoP will be impossible to achieve. Figure 5 shows a cloaking zone with $k = 8$ users. The colorful one represents the user's true location, whereas the black ones represent the user's chosen dummy locations. The k locations cover the cloaking area.

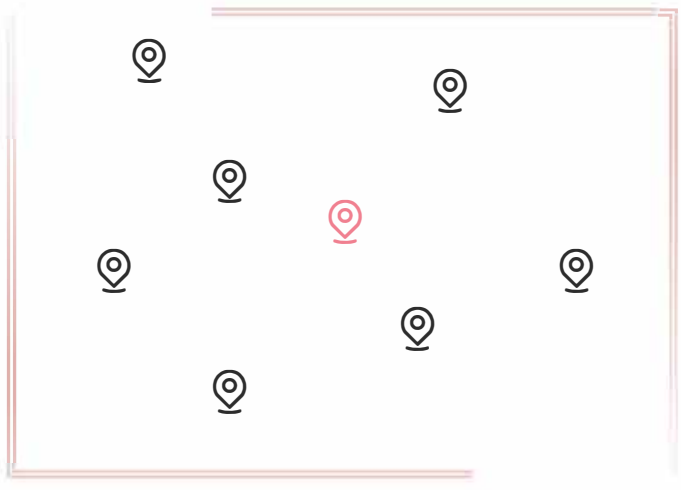


Figure 5. A cloaking area with $k = 8$ users.

In general, the higher the k value, the greater the privacy protection; otherwise, the lower the privacy security. When the value of k increases, the corresponding QoS decreases and the system overhead increases.

4.3. Algorithms of Dummy Location Selection

Researchers proposed a variety of approaches in the dummy-based locations' selection to withstand the background knowledge attack, such as [55]. The main work of these studies is to choose appropriate dummy locations to construct a candidate set that protects users' privacy effectively. The aim of dummy-based location privacy protection is to camouflage the user's real location in the dummy locations concentration; thus, the quality of these selected candidate dummies is crucial to attaining the desired level of location privacy in the overall system. As a result, it is critical to reduce the distinguishability of real and dummy locations in all aspects; that is, we must choose dummy locations that can satisfy user desires while also protecting user privacy. In this subsection, we summarize and discuss the rules on dummy selection for dummy-based location privacy protection techniques.

4.3.1. Take the Historical Query Probability of Locations into Consideration

The popularity of a location within a geographic location area over time is reflected by its historical query probability. The ratio of the number of times a location is queried to the total number of times all locations are requested in the global geographical area is used to calculate the historical query probability of a location in a certain period of time. For example, the following is the calculation formula for the historical query probability of location i inside a specific geographical area over time:

$$q_i = \frac{times \quad of \quad queries \quad in \quad location \quad i}{times \quad of \quad queries \quad in \quad all \quad locations}, \tag{1}$$

Because the LBS server has background information such as historical query probability of map locations, the server filters out dummy locations with obvious differences based

on the probability distribution information of the candidate set, and thus the expected level of privacy protection cannot be achieved.

If the server filters out m dummy locations, the likelihood of identifying the user's dummy location increases from $\frac{1}{k}$ to $\frac{1}{k-m}$. In the entire map space, Figure 6 depicts the distribution of all locations and their historical query probability. Each little grid cell in the diagram represents a location. Varied shadow shapes portray different historical query probabilities, and the sum of the probabilities of all locations initiating query requests in the entire grid space is 1. Location A represents the user's real location, whereas B, C , and D are the dummy locations that have been chosen. Because their historical query probability is smaller than the real location's or even zero, the server can easily filter these dummy locations out.

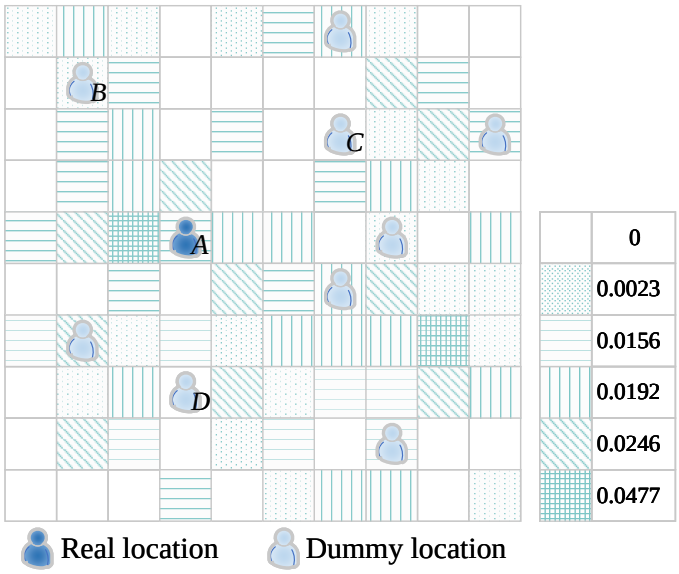


Figure 6. The historical query probability distribution of all locations.

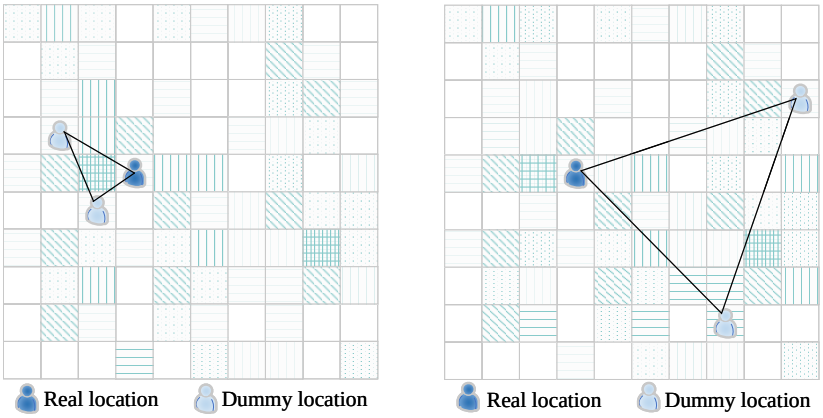
Hara et al. [7] developed a dummy location selection algorithm that considers real-world environmental constraints and avoids dummy locations in inaccessible locations, such as the middle of a lake. However, this method only eliminates a small number of impossible locations, those where $q_i = 0$. As a result, the dummy quality is poor, as is the LoP. In order to improve the quality of dummies and the LoP, the DLS algorithm chooses dummy locations that have the same probability as the real ones. It not only keeps these $q = 0$ locations at bay, but it also reduces the difference in query probability between the real ones and dummies. In the literature [56], the greedy algorithm idea is used to select dummy locations so that the new location set composed of each new dummy location and the previously selected dummy locations have the best hiding effect. Other authors [57,58] have employed an information entropy-based method, with the historical query probability as a variable, to choose dummy locations. In [57,58], the set of dummy locations with the highest entropy value acts as the final set of candidate dummy locations. Because the historical query probability of each location over time is insufficient to convey the prevalence of each location, [59] introduced the concept of "current query probability", which was used to replace historical query probability as the criterion for selecting dummy locations. Users choose different geographical regions for different time periods, with each location's current query probability being different. As a result, the "historical query probability" is more diverse, posing a greater challenge to attackers.

4.3.2. Taking the Physical Dispersion of Locations into Consideration

The physical dispersion between locations describes the spatial distribution of locations. The obscuring of users' true locations will also perform poorly if an attacker learns this background knowledge in order to carry out location distribution attacks on them. As

a result, selecting dummy locations solely on historical query probability is insufficient. In practical applications, physical dispersion between locations should be highlighted.

If the physical dispersion between locations is too small, the cloaking area will be too small. The cloaking area, as shown in Figure 7a, is small, allowing the attacker to quickly deduce that the real user is in a very small area. As a result, something like Figure 7b would be preferable because it provides a larger cloaking area for the real user. Simultaneously, the query probability of those chosen dummy locations is not too far off from the user's actual location. As a result, when selecting dummy locations, the spatial distribution of the $k-1$ dummy locations and the real ones should be guaranteed, while the historical query probability should be the same or similar.



(**a**) small area (**b**) large area

Figure 7. The physical dispersion situation between dummies and the real location.

To meet the requirements of physical dispersion of locations, Niu B. et al. [8] proposed a method for selecting candidate locations based on virtual circles and virtual grids. Because the user's true location is likely to be close to the center of the local map, the virtual circle algorithm may have performed poorly in terms of privacy. To provide a more obscured area, a virtual grid-based algorithm was introduced, which ensures that candidate locations are distributed fairly evenly around the true location and that the size of the cloaking area meets user needs.

In order to achieve physical dispersion between locations, Niu B et al. proposed the enhanced DLS algorithm in reference [42]. They argued that the product of locational distances was more accurate in depicting locational dispersion than the sum of locational distances. As Figure 8 shows, $CA + CB = DA + DB$ while $CA \cdot CB > DA \cdot DB$; as a result, we would prefer to choose C over D from the perspective of privacy. They used a multi-objective optimization model as well, where the probability and physical dispersion of locations are considered simultaneously to pick the best candidate set of dummy locations.

In addition to the previous research on location dispersion in physical space, there are numerous studies on how to portray the physical distance, such as the effective distance [60] or the road network distance [61,62], between two locations. The idea of effective distance was developed by Xu et al. [60] to characterize the distribution features of locations, and the effective distance between these two locations was defined as the shortest distance between the current location and any other location. Consider real user u_r and any other user u_i; their coordinates are (x_r, y_r) and (x_i, y_i), resulting in an effective distance of

$$d(u_r, u_i) = \min \mid u_r, u_i \mid = \min \sqrt{(x_r - x_i)^2 + (y_r - y_i)^2} \quad (2)$$

It is apparent from the effective distance calculation formula that the essence of the effective distance specified by them is the Euclidean distance. Despite the fact that the article is based on a real-world road network, Euclidean distance is nevertheless employed to measure location distribution features. Chen et al. [62] proposed a privacy protection

method for the road network in response to the fact that the distance between any two points in real life is not a simple linear distance (Euclidean distance), and that users' activities are more restricted to the planned road. This approach requires that the number of road sections in the selected dummy sites satisfy the value given by the user in order to attain the purpose of physical dispersion between the selected dummy locations when picking dummy locations. This road network, however, is an undigraph road network model, which is insufficiently realistic for real-world road network simulation, as illustrated in Figure 9a. Zhou Changli et al. proposed a location privacy protection approach based on the digraph road network architecture (as shown in Figure 9b), in which an anchor point (dummy location) was used to replace users' real locations when initiating query requests. However, when choosing the anchor point, the historical query probability of the anchor and its geographical spatial distribution link with a real user were not taken into account.

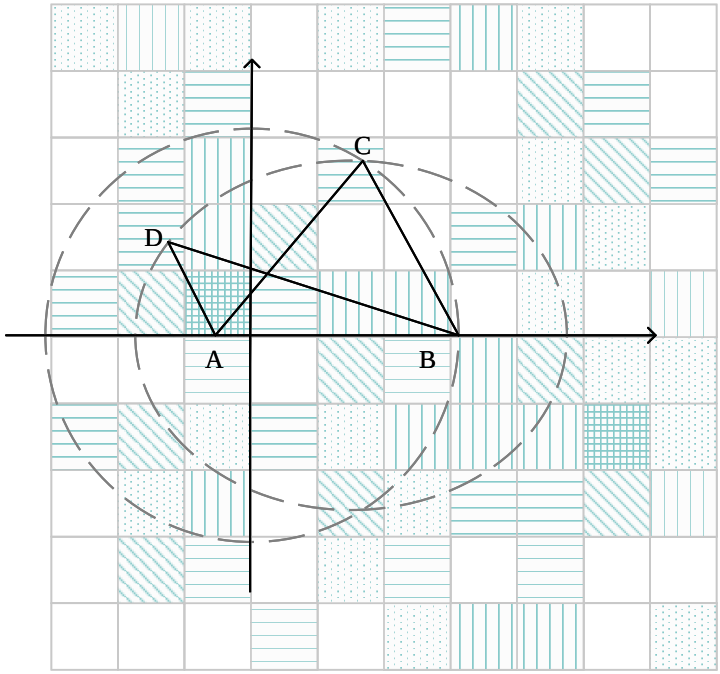
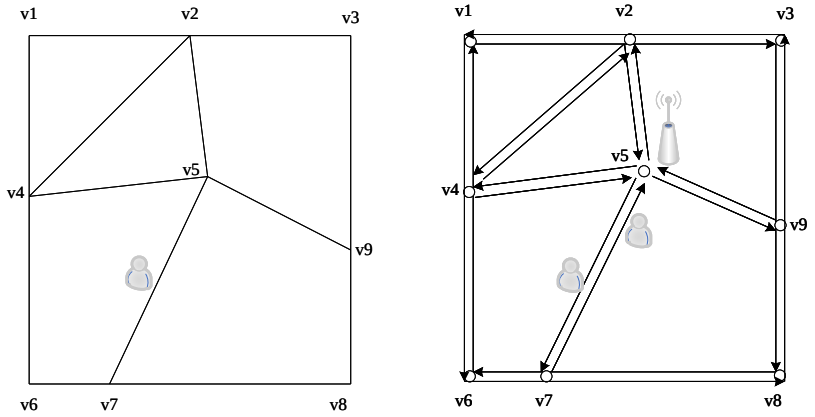


Figure 8. The enhanced DLS.



(**a**) undigraph road network (**b**) digraph road network

Figure 9. Undigraph/digraph road network.

4.3.3. Taking the Semantic Diversity of Locations into Consideration

A location's semantic information refers to its semantic properties, such as hospitals, restaurants, banks, schools, parks, and so on. Semantic features can be extracted using

context information. The greater the number of location semantic features collected, the more accurate the semantic categorization, and the greater the ability to protect users' location privacy. Consider the semantics of a user's location for "hospital" which implies semantic information on the user's health, professional property, and so on. Because the user's state of health or professional attributes belong to the users of the important content of privacy, semantic information must be considered when selecting dummy locations.

Bostanipour [63] presented a method for combining obfuscation location information with semantic information to ensure that many semantically identical locations are cloaked, therefore preventing attackers from performing semantic inference attacks. The locations derived using this method, on the other hand, are semantically related to those of real users. For example, the real user's semantic tag is "Pizza Place", but the cloaking region includes venues such as "Noodle House" and "Hamburger Palace", all of which belong to the parent semantic tag "Restaurant". As a result, such a method is still vulnerable to semantic inference attacks.

In order to achieve semantic diversity, each location in the candidate dummy set should have a diverse set of semantic properties as much as possible. While representing semantic differences between locations is a challenge, Zeng et al. proposed the similarity of two semantic location types using Euclidian distance to calculate [64]. Tian et al. measure semantic distance based on the intersection and union of a location's semantic attributes:

$$sem_{dist}(A, B) = \frac{[sem_A \cup sem_B] - [sem_A \cap sem_B]}{sem_A \cup sem_B} \quad (3)$$

This then transforms the results to show semantic similarity [65]. Using Euclidean distance and the relationship between sets to quantify semantic difference not only consumes a lot of effort but also weakens the algorithm's efficiency. Another author [9] created a location semantic tree (LST) to arrange all locations, as shown in Figure 10, in order to achieve semantic similarity control that can serve the tailored needs of users and increase the efficiency of algorithm execution. The most fundamental semantic information is stored in the leaf nodes of the location semantic tree, and the hop number between the leaf nodes is used to calculate the semantic distance, which is then used to calculate the semantic difference degree. This approach can rapidly find and categorize the semantic associations of all locations in a specified geographical area.

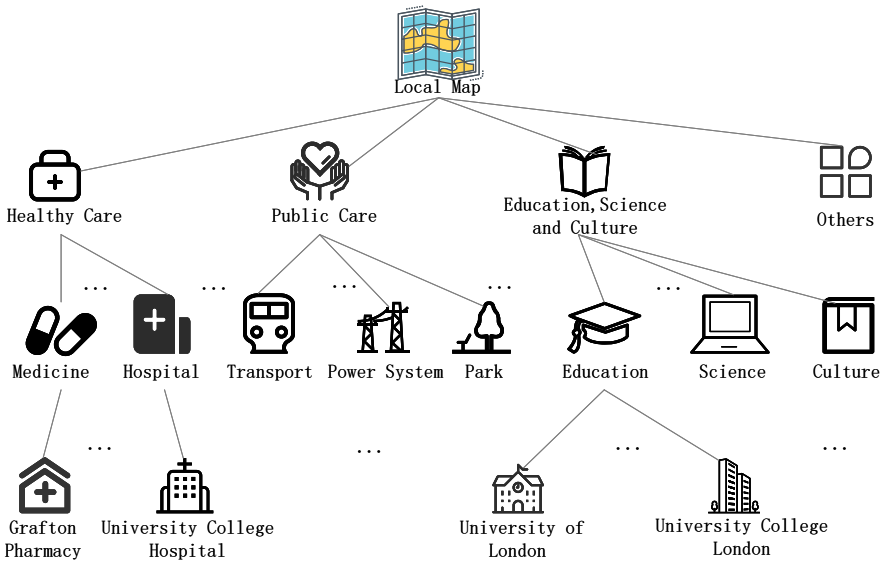


Figure 10. The location semantic tree.

When there are many different semantic varieties in a given geographical area and there are crossover circumstances, the depth and breadth of the semantic tree grow quite

large, decreasing search efficiency. As a result, the location semantic tree is not ideal for such scenarios.

4.4. Summary

In general, we classify the existing dummy location selection methods into three categories according to the types of attacks they can defend against, as shown in Table 3. The first category of selection method can successfully defend against the probability similarity attack. The second category of the selection method can effectively prevent physical distribution attacks launched by attackers on the distribution pattern of locations. The third category of selection method can make it difficult for attackers trying to obtain cracking clues from the semantic information of locations. Different methods have different characteristics, and we can select relatively appropriate methods according to our own needs and purposes when using these methods to select dummies to construct dummy location's set.

Table 3. Selection methods of dummy on query probability similarity, physical dispersion and semantic diversity.

Category	Reference	Methods of Selection
Query probability similarity	[7]	avoids dummies with $q_i = 0$
	[42]	dummies have the same probability as the real ones
	[58]	information entropy-based
	[59]	current query probability
Physical dispersion	[8]	virtual circles and virtual grids
	[42]	the product of locational distances
	[60]	the effective distance
	[62]	the road network distance
Semantic diversity	[9]	location semantic tree
	[64]	Euclidian distance
	[65]	the intersection and union of a location's semantic attributes

An overall comparison of random selection and other selection schemes that consider different factors when selecting dummies is shown in Table 4. In Table 4, we observe that different schemes can choose different system structures and take different factors into account to design different schemes according to their own purposes and needs. As a consequence, the types of attacks they can defend against are not the same, and, of course, the corresponding computational overheads are somewhat different. Dummy location selection methods that take into account query probability, physical dispersion, and semantic diversity yield better security than random selection with a relatively small computational overhead. Furthermore, depending on different selection factors, the attacks that can be defended against are varied when selecting a dummy location. When a dummy location is chosen, the more factors are taken into account, the better the privacy protection effects of the scheme are strengthened, while the difference in computing overhead is not readily apparent. As a result, schemes increasingly seek to take more factors into account when selecting dummies. They are no longer always based on a single factor, such as [21,66], which incorporates two factors, and three factors are considered simultaneously in the literature [46]. As the research goes further, new factors are discovered and considered, and new rules are established in [67,68].

Table 4. Summary of dummy selection.

Selection Method	Reference	CO [a]	Architecture		Attack		
			TTP	Non-TTP	AoQ [b]	AoD [c]	AoS [d]
Random Selection	[6]	$O(k \log k)$		√			
Considering Q	[42]	$O(k)$		√	√		
Considering D	[7]	$Null$		√		√	
Considering S	[62]	$Null$	√				√
	[64]	$Null$	√				√
Considering Q+D	[8]	$O(k)$		√	√	√	
	[9]	$O(\log k)$		√	√	√	
	[58]	$O(\alpha \log_2 \alpha)$		√	√	√	
	[60]	$O(k^2 + IJU)$		√	√	√	
Considering D+S	[59]	$O(k)$		√		√	√
Considering Q+S	[65]	$O(It \cdot k)$		√	√		√
All of them	[18]	$O(\log N)$	√		√	√	√

[a] CO: the computation overhead. [b] AoQ: the attack of query probability; Q: Query probability. [c] AoD: the attack of location distribution; D: Location distribution. [d] AoS: the attack of semantic similarity; S: Semantic similarity. Notes: k: the number of dummies; α: $(\omega + m)\log(\omega + m)$, $\omega = (maxtier - 1)(1 - e)m$, m: the number of dummies candidate set, $maxtier$: the max times of iteration; IJ: an area is divided into IJ cells; U: the number of services; It: the times of iteration; N: the total number of users in the region to be clocked.

5. Conclusions

In this article, we provide a review of dummy-based location privacy protection techniques for LBS. First, we distinguished the relationship between the LoP, QoS, and system overhead. At the same time, we made an overall comparison of several representative methods of location privacy protection techniques. We described the merits of dummy-based location privacy protection on LBS. Meanwhile, a summary of the major attacks on dummy-based location privacy protection techniques was also included.

Second, we systematically and comprehensively analyzed and summarizde the ways of selecting dummies on three aspects, namely the query probability, the physical dispersion, and the semantic diversity of locations.

Third, we provided an overview of the methods for achieving query probability, physical dispersion, and semantic diversity while choosing dummies. Furthermore, the different privacy protection advantages of different selection rules when choosing dummies can be seen from a comparative analysis. The results of this comparative analysis can benefit both users and researchers who are studying this field. When the requesting service needs to construct a hiding area that hides their true location, the user can refer to this comparative evaluation to choose a dummy-based location privacy protection method that better meets their needs. Moreover, researchers studying this area can gain a better understanding of dummy-based privacy protection schemes from the results of this comparative analysis. They can also get to know the challenges posed by the expanding background knowledge of attackers and the intersection between LBS and other emerging technologies.

Dummy location selection approaches that took into account new circumstances in the selection of dummies emerged as research progressed. There are still some significant issues to be resolved and perfected in the area of dummy location selection.

First, as new technologies such as social networks, edge computing, and federal learning have been advanced, new privacy concerns have also emerged.

- Because location acquisition technology is becoming more widely available, it is now possible to add geo-information to already-existing social networks, which has

facilitated in the emergence and expansion of LBSN. LBSN, a combination of LBS and social networks, involves a range of personal private information, such as shared common locations, personal interests, daily behaviors and activities, etc. [69].

- LBS@E [70] delocalizes LBSs and retrieves local information from nearby edge servers around them instead of the cloud. Consequently, it tackles the location privacy problem innovatively. However, LBS@E brings new challenges to location privacy. Mobile users can still be localized to specific privacy areas jointly covered by edge servers accessed by mobile users. The small privacy area puts the mobile user's location at risk of similarity.
- Ref. [71] uses federated learning to select the best location privacy protection mechanism (LPPM) for each user according to the real location and the user's configuration, which avoids the direct use of the real location information. Nevertheless, it is vulnerable to poisoning attacks and untrusted users who intend to add a backdoor to the model [72] or defend against attacks on model information leakage [73].

Second, existing dummy-based solutions do not account for all aspects of real-world privacy protection [74], and there is a significant gap between theoretical and real-world privacy protection effects. According to Sun et al. [75], attackers can also rule out impossible dummy locations by determining whether users can reach the query location in a reasonable amount of time from their current location.

Third, dummy-based approaches that focus on the spatio-temporal correlation of location are commonly used in trajectory privacy protection, which poses new challenges in trajectory privacy. Zhao [76] assumes that all users(dummies) involved are trustworthy and report their real locations. However, it is often not the case in reality. There are untrusted users who conduct location injection attacks (LIAs) in continuous LBS queries. Zhen [77] found that the trajectory data were published without proper processing. A great amount of work has been devoted to merging one's own trajectories with those of others, without protecting the semantic information about the location. In continuous LBS queries, users can obfuscate their true query location by selecting dummy locations and predicted locations, thus improving their privacy. However, selecting a large number of dummies for each query can increase the query cost of the system and influence the accuracy of the predicted location [78].

Funding: This research was funded by the National Natural Science Foundation of China (No. 61702180), the Research Foundation of Education Bureau of Hunan Province (No. 21B0493), and the Hunan Province Science and Technology Project Funds (2018TP1036).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

LTTP	location privacy protection techniques
LoP	the level of privacy protection
RM	representative method
QoS	the quality of service
CO	computation overhead
AoQ	attack of query probability
Q	query probability
AoD	attack of location distribution
D	location distribution
AoS	attack of semantic similarity
S	semantic similarity

References

1. Statista Research Department. Share of U.S. smartphone Owners Using Geosocial and Location-Based Services from 2011 to 2015. 2016. Available online: https://www.statista.com/statistics/224949/mobile-geosocial-and-location-based-service-usage-by-age/ (accessed on 15 May 2022).
2. Auxier, B. Pew Research Center: Internet and Technology-How Americans See Digital Privacy Issues Amid the COVID-19 Outbreak. 2020. Available online: https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/ (accessed on 15 May 2022).
3. Laricchia, F. Bluetooth Location Services Device Shipments Worldwide from 2016 to 2026. 2022. Available online: https://www.statista.com/statistics/1226718/global-bluetooth-location-device-shipment-forecast/#statisticContainer (accessed on 15 May 2022).
4. Security, R.B. Year End Data Breach QuickView Report. 2022. Available online: https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (accessed on 14 May 2022).
5. Association, C.C. Investigation Report on App Personal Information Leakage. 2018. Available online: https://www.cca.org.cn/jmxf/detail/28180.html (accessed on 10 May 2022).
6. Kido, H.; Yanagisawa, Y.; Satoh, T. An anonymous communication technique using dummies for location-based services. In Proceedings of the International Conference on Pervasive Services, 2005, Santorini, Greece, 11–14 July 2005; pp. 88–97.
7. Hara, T.; Suzuki, A.; Iwata, M.; Arase, Y.; Xie, X. Dummy-Based User Location Anonymization Under Real-World Constraints.k *IEEE Access* **2016**, *4*, 673–687. [CrossRef]
8. Niu, B.; Zhang, Z.; Li, X.; Hui, L. Privacy-area aware dummy generation algorithms for Location-Based Services. In Proceedings of the IEEE International Conference on Communications, Sydney, NSW, Australia, 10–14 June 2014; pp. 957–962.
9. Chen, S.H.; Shen, H. Semantic-Aware Dummy Selection for Location Privacy Preservation. In Proceedings of the Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 752–759.
10. Magkos, E. Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey. *Int. J. Inf. Technol. Syst. Approach* **2011**, *4*, 48–69. [CrossRef]
11. Shin, K.G.; Ju, X.; Chen, Z.; Hu, X. Privacy protection for users of location-based services. *IEEE Wirel. Commun.* **2012**, *19*, 30–39. [CrossRef]
12. Chatzikokolakis, K.; ElSalamouny, E.; Palamidessi, C.; Pazii, A. Methods for Location Privacy: A comparative overview. *Found. Trends® Priv. Secur.* **2017**, *1*, 199–257. [CrossRef]
13. Zhang, S.; Wang, G.; Alam, B.; Qin, L. A Dual Privacy Preserving Scheme in Continuous Location-Based Services. *IEEE Internet Things J.* **2018**, *5*, 4191–4200. [CrossRef]
14. Ma, M.; Du, Y.; Li, F.; Liu, J. Review of semantic-based privacy-preserving approaches in LBS. *Chin. J. Netw. Inf. Secur.* **2016**, *2*, 10–13.
15. Wan, S.; Li, F.; Niu, B.; Sun, Z.; Li, H. Research progress on location privacy-preserving techniques. *IEEE Internet Things J.* **2016**, *37*, 18.
16. Zhang, J.; Xu, L.; Tsai, P.W. Community structure-based trilateral stackelberg game model for privacy protection. *Appl. Math. Model.* **2020**, *86*, 20–35. [CrossRef]
17. Qiu, Y.; Liu, Y.; Xxuan, L.; Chen, J. A Novel Location Privacy-Preserving Approach Based on Blockchain. *Sensors* **2020**, *20*, 3519. [CrossRef] [PubMed]
18. Ni, L.; Tian, F.; Ni, Q.; Yan, Y.; Zhang, J. An anonymous entropy-based location privacy protection scheme in mobile social networks. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–19. [CrossRef]
19. Palanisamy, B.; Liu, L. Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms. *IEEE Trans. Mob. Comput.* **2015**, *14*, 495–508. [CrossRef]
20. Liu, B.; Zhou, W.; Zhu, T.; Gao, L.; Xiang, Y. Location Privacy and Its Applications: A Systematic Study. *IEEE Access* **2018**, *6*, 17606–17624. [CrossRef]
21. Chen, S.; Fu, A.; Shen, J.; Yu, S.; Wang, H.; Sun, H. RNN-DP: A new differential privacy scheme base on Recurrent Neural Network for Dynamic trajectory privacy protection. *J. Netw. Comput. Appl.* **2020**, *168*, 102736. [CrossRef]
22. Farouk, F.; Alkady, Y.; Rizk, R.Y. Efficient Privacy-Preserving Scheme for Location Based Services in VANET System. *IEEE Access* **2020**, *8*, 60101–60116. [CrossRef]
23. Gupta, S.; Arora, G. Use of Homomorphic Encryption with GPS in Location Privacy. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019; pp. 42–45.
24. Sahai, A.; Waters, B. Fuzzy Identity-Based Encryption. *IACR Cryptol. ePrint Arch.* **2005**, *2004*, 86.
25. Cui, Y.; Gao, F.; Li, W.; Shi, Y.; Panaousis, E. Cache-Based Privacy Preserving Solution for Location and Content Protection in Location-Based Services. *Sensors* **2020**, *20*, 4651. [CrossRef]
26. Khodaei, M.J.; Papadimitratos, P. Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones are Not Enough. *IEEE Internet Things J.* **2021**, *8*, 7985–8004. [CrossRef]
27. Khoshgozaran, A.; Shahabi, C.; Shirani-Mehr, H. Location privacy: Going beyond K-anonymity, cloaking and anonymizers. *Knowl. Inf. Syst.* **2011**, *26*, 435–465. [CrossRef]
28. Jadallah, H.; Aghbari, Z.A. Spatial cloaking for location-based queries in the cloud. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 3339–3347. [CrossRef]

29. Xu, C.; Zhu, L.; Liu, Y.; Guan, J.; Yu, S. DP-LTOD: Differential Privacy Latent Trajectory Community Discovering Services over Location-Based Social Networks. *IEEE Trans. Serv. Comput.* **2021**, *14*, 1068–1083. [CrossRef]
30. Li, W.; Li, C.; Geng, Y. APS: Attribute-Aware Privacy-Preserving Scheme in Location-Based Services. *Inf. Sci.* **2020**, *527*, 460–476. [CrossRef]
31. Ni, L.; Yuan, Y.; Wang, X.; Yu, J.; Zhang, J. A Privacy Preserving Algorithm Based on R-constrained Dummy Trajectory in Mobile Social Network. *Procedia Comput. Sci.* **2018**, *129*, 420–425. [CrossRef]
32. Andrés, M.E.; Bordenabe, N.E.; Chatzikokolakis, K.; Palamidessi, C. Geo-indistinguishability: differential privacy for location-based systems. In Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, Berlin, Germany, 4–8 November 2013; pp. 901–914.
33. Li, H.; Wang, Y.; Guo, F.; Wang, J.; Wang, B.; Wu, C. Differential Privacy Location Protection Method Based on the Markov Model. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 4696455. [CrossRef]
34. Fung, E.; Kellaris, G.; Papadias, D. Combining Differential Privacy and PIR for Efficient Strong Location Privacy. In Proceedings of the International Symposium on Spatial and Temporal Databases, Hong Kong, China, 26–28 August 2015; pp. 1–18.
35. Russell, P.; Golam, K.M.; Xun, Y.; Elisa, B. Privacy-Preserving and Content-Protecting Location Based Queries. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1200–1210.
36. Domingo-Ferrer, J. Microaggregation for Database and Location Privacy. In Proceedings of the International Workshop on Next Generation Information Technologies and Systems, Kibbutz Shefayim, Israel, 4–6 July 2006; pp. 106–116.
37. Shokri, R.; Theodorakopoulos, G.; Papadimitratos, P.; Kazemi, E.; Hubaux, J.P. Hiding in the Mobile Crowd: Location Privacy through Collaboration. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 266–279.
38. Zhang, S.; Xiong, L.; Tan, Z.; Tao, P.; Wang, G. A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. *Future Gener. Comput. Syst.* **2019**, *94*, 40–50. [CrossRef]
39. Niu, B.; Li, Q.; Zhu, X.; Cao, G.; Hui, L. Enhancing privacy through caching in location-based services. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Hong Kong, 26 April–1 May 2015; pp. 1017–1025.
40. Sweeney, L. k-Anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness -Knowl.-Based Syst.* **2002**, *10*, 557–570. [CrossRef]
41. Beresford, A.R.; Stajano, F. Location Privacy in Pervasive Computing. *IEEE Pervasive Comput.* **2003**, *2*, 46–55. [CrossRef]
42. Niu, B.; Li, Q.; Zhu, X.; Cao, G.; Hui, L. Achieving k-anonymity in privacy-aware location-based services. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, ON, USA, 27 April–2 May 2014; pp. 754–762.
43. Wernke, M.; Skvortsov, P.; Dürr, F.; Rothermel, K. A classification of location privacy attacks and approaches. *Pers. Ubiquitous Comput.* **2012**, *18*, 163–175. [CrossRef]
44. Chow, C.Y.; Mokbel, M.F.; Liu, X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *Geoinformatica* **2011**, *15*, 351–380. [CrossRef]
45. Mokbel, M.F. Privacy in Location-Based Services: State-of-the-Art and Research Directions. In Proceedings of the International Conference on Mobile Data Management, Mannheim, Germany, 1 May 2007; p. 228.
46. Shokri, R.; Theodorakopoulos, G.; Boudec, J.Y.L.; Hubaux, J.P. Quantifying location privacy. In Proceedings of the IEEE Symposium on Security and Privacy, Washington, DC, USA, 22–25 May 2011; pp. 247–262.
47. Lee, B.; Oh, J.; Yu, H.; Kim, J. Protecting location privacy using location semantics. In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, CA, USA, 21–24 August 2011; pp. 21–24.
48. Jiang, H.; Li, J.; Zhao, P.; Zeng, F.; Xiao, Z.; Iyengar, A. Location Privacy-preserving Mechanisms in Location-based Services. *ACM Comput. Surv.* **2021**, *54*, 1–36. [CrossRef]
49. Gedik, B.; Ling, L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Trans. Mob. Comput.* **2007**, *7*, 1–18. [CrossRef]
50. Vu, K.; Rong, Z.; Jie, G. Efficient Algorithms for K-Anonymous Location Privacy in Participatory Sensing. In Proceedings of the IEEE International Conference on Computer Communications, Orlando, FL, USA, 25–30 March 2012; pp. 2399–2407.
51. Yu, L.; Liu, L.; Pu, C. Dynamic Differential Location Privacy with Personalized Error Bounds. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 26 February–1 March 2017; pp. 1–15.
52. Differential Privacy Team, A. Learning with Privacy at Scale. 2017. Available online: https://machinelearning.apple.com/research/learning-with-privacy-at-scale (accessed on 20 April 2022).
53. Xu, M.; Zhao, H.; Ji, X.; Shen, J. Distribution-Perceptive-Based Spatial Cloaking Algorithm for Location Privacy in Mobile Peer-to-Peer Enviroments. *J. Softw.* **2018**, *19*, 1852–1862.
54. Huang, Y.; Huo, Z.; Meng, X.F. CoPrivacy: A Collaborative Location Privacy-Preserving Method without Cloaking Region. *J. Softw.* **2018**, *19*, 1852–1862. [CrossRef]
55. Sun, G.; Cai, S.; Yu, H.; Maharjan, S.; Chang, V.; Du, X.; Guizani, M. Location Privacy Preservation for Mobile Users in Location-Based Services. *IEEE Access* **2019**, *7*, 87425–87438. [CrossRef]
56. Shaham, S.; Ding, M.; Liu, B.; Lin, Z.; Li, J.Y. Privacy Preservation in Location-Based Services: A Novel Metric and Attack Model. *IEEE Trans. Mob. Comput.* **2021**, *20*, 3006–3019. [CrossRef]
57. Wu, D.; Zhang, Y.; Liu, Y. Dummy Location Selection Scheme for K-Anonymity in Location Based Services. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017; pp. 441–448.
58. Li, L.L.; Hua, J.F.; Wan, S.; Zhu, H.; Li, F.H. Achieving efficient location privacy protection based on cache. *J. Commun.* **2017**, *38*, 148–157.

59. Fei, F.; Li, S.; Dai, H.; Hu, C.; Dou, W.; Ni, Q. A K-Anonymity Based Schema for Location Privacy Preservation. *IEEE Trans. Sustain. Comput.* **2019**, *4*, 156–167. [CrossRef]
60. Xu, X.; Chen, H.; Xie, L. A Location Privacy Preservation Method Based on Dummy Locations in Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 4594. [CrossRef]
61. Zhou, C.; Chen, Y.; Tian, H.; Cai, S. Location Privacy and Query Privacy Preserving Method for K-nearest Neighbor Query in Road Networks. *J. Softw.* **2020**, *31*, 471–492.
62. Chen, H.; Qing, X. Location-semantic-based location privacy protection for road network. *J. Commun.* **2016**, *37*, 67–76.
63. Bostanipour, B.; Theodorakopoulos, G. Joint obfuscation of location and its semantic information for privacy protection. *Comput. Secur.* **2021**, *107*, 1–22. [CrossRef]
64. Zeng, H.; Zuo, K.; Wang, Y.; Liu, R. Semantic Diversity Location Privacy Protection Method in Road Network Environment. *Comput. Eng. Appl.* **2020**, *56*, 102–108.
65. Tian, C.; Xu, H.; Lu, T.; Jiang, R.; Kuang, Y. Semantic and Trade-Off Aware Location Privacy Protection in Road Networks Via Improved Multi-Objective Particle Swarm Optimization. *IEEE Access* **2021**, *9*, 54264–54275. [CrossRef]
66. Liao, D.; Huang, X.; Anand, V.; Sun, G.; Yu, H.F. k-DLCA: An efficient approach for location privacy preservation in location-based services. In Proceedings of the IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
67. Song, D.; Song, M.B.; Shakhov, V.V.; Park, K. Efficient dummy generation for considering obstacles and protecting user location. *Concurr. Comput. Pract. Exp.* **2021**, *33*, e5416. [CrossRef]
68. Kuang, L.; Wang, Y.; Zheng, X.; Huang, L.; et al. Using location semantics to realize personalized road network location privacy protection. *Eurasip J. Wirel. Commun. Netw.* **2020**, *2020*, 1. [CrossRef]
69. Li, J.; Zeng, F.; Xiao, Z.; Jiang, H.; Zheng, Z.; Liu, W.; Ren, J. Drive2friends: Inferring Social Relationships From Individual Vehicle Mobility Data. *IEEE Internet Things J.* **2020**, *7*, 5116–5127. [CrossRef]
70. Cui, G.; He, Q.; Chen, F.; Jin, H.; Xiang, Y.; Yang, Y. Location Privacy Protection via Delocalization in 5G Mobile Edge Computing Environment. *IEEE Trans. Serv. Comput.* **2021**, *9*, 1–12. [CrossRef]
71. Khalfoun, B.; Mokhtar, S.B.; Bouchenak, S.; Nitu, V. EDEN: Enforcing Location Privacy through Re-identification Risk Assessment: A Federated Learning Approach. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2021**, *5*, 1–25. [CrossRef]
72. Geyer, R.; Klein, T.; Nabi, M. Differentially Private Federated Learning: A Client Level Perspective. *arXiv* **2017**, arXiv:1712.07557.
73. Bagdasaryan, E; Veit, A; Hua, Y; Estrin, D; Shmatikov, V. How To Backdoor Federated Learning. *arXiv* **2018**, arXiv:1807.00459.
74. Yang, X.; Gao, L.; Wang, H.; Li, Y.; Zheng, J.; Xu, J.; Ma, Y. A User-related Semantic Location Privacy Protection Method In Location-based Service. In Proceedings of the IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS), Beijing, China, 14–16 December 2021; pp. 691–698.
75. Sun, G.; Song, L.; Liao, D.; Yu, H.; Chang, V. Towards privacy preservation for "check-in" services in location-based social networks. *Inf. Sci.* **2019**, *481*, 616–634. [CrossRef]
76. Zhao, P.; Li, J.; Zeng, F.; Xiao, F.; Wang, C.; Jiang, H. ILLIA: Enabling k-Anonymity-Based Privacy Preserving Against Location Injection Attacks in Continuous LBS Queries. *IEEE Internet Things J.* **2018**, *5*, 1033–1042. [CrossRef]
77. Tu, Z.; Zhao, K.; Xu, F.; Li, Y.; Su, L.; Jin, D. Protecting Trajectory from Semantic Attack Considering k-Anonymity, l-diversity and t-closeness. *IEEE Trans. Netw. Serv. Manag.* **2018**, *16*, 264–278. [CrossRef]
78. Zhang, S.; Mao, X.; Choo, K.K.R.; Peng, T.; Wang, G. A trajectory privacy-preserving scheme based on a dual-K mechanism for continuous location-based services. *Inform. Sci.* **2020**, *527*, 406–419.