Enabling Location Privacy Preservation in MANETs Based on Distance, Angle, and Spatial Cloaking

Nanlan Jiang, Sai Yang and Pingping Xu *

National Mobile Communications Research Laboratory, Southeast University, Nanjing 211189, China; jiangnanlan@seu.edu.cn (N.J.); 220180904@seu.edu.cn (S.Y.)

* Correspondence: xpp@seu.edu.cn

Received: 12 December 2019; Accepted: 3 March 2020; Published: 8 March 2020

Abstract: Preserving the location privacy of users in Mobile Ad hoc Networks (MANETs) is a significant challenge for location information. Most of the conventional Location Privacy Preservation (LPP) methods protect the privacy of the user while sacrificing the capability of retrieval on the server-side, that is, legitimate devices except the user itself cannot retrieve the location in most cases. On the other hand, applications such as geographic routing and location verification require the retrievability of locations on the access point, the base station, or a trusted server. Besides, with the development of networking technology such as caching technology, it is expected that more and more distributed location-based services will be deployed, which results in the risk of leaking location information in the wireless channel. Therefore, preserving location privacy in wireless channels without losing the retrievability of the real location is essential. In this paper, by focusing on the wireless channel, we propose a novel LPP enabled by distance (ranging result), angle, and the idea of spatial cloaking (DSC-LPP) to preserve location privacy in MANETs. DSC-LPP runs without the trusted third party nor the traditional cryptography tools in the line-of-sight environment, and it is suitable for MANETs such as the Internet of Things, even when the communication and computation capabilities of users are limited. Qualitative evaluation indicates that DSC-LPP can reduce the communication overhead when compared with k-anonymity, and the computation overhead of DSC-LPP is limited when compared with conventional cryptography. Meanwhile, the retrievability of DSC-LPP is higher than that of k-anonymity and differential privacy. Simulation results show that with the proper design of spatial divisions and parameters, other legitimate devices in a MANET can correctly retrieve the location of users with a high probability when adopting DSC-LPP.

Keywords: location privacy preservation; MANETs; wireless channel; Distance; Ranging; Spatial cloaking

1. Introduction

Location information makes wireless devices become location-aware data collection instruments, such as smartphones in Mobile Ad hoc Networks (MANETs) or vehicles in Vehicular Ad hoc Networks (VANETs) [1]. The applications of location information include Mobile Crowd Sensing (MCS) [2,3], geographic routing [4], Location-Based Service (LBS) [5], Online Social Networks (OSN) [6], Internet of Things (IoT) [7], mobile Wireless Sensor Networks (WSN) [8], etc. In these applications, mobile users report their locations to the server through the Access Point (AP) or the Base Station (BS) to acquire services. However, unexpected eavesdroppers could obtain users’ location information during the reporting process, leading to a significant challenge for location information: how to protect users’ location privacy [9]?

The system which needs to preserve the location privacy includes the server-side and the user-side. On the server-side, the attacker will try to capture the location information by attacking the
server, the AP/BS, or by eavesdropping the communication link between devices on the server-side. However, the capabilities of devices on the server-side allow them to protect their messages based on conventional cryptography.

On the user-side, the attacker acquires the location information by invasion attack, Location Estimation (LE), or eavesdropping the wireless channel between the user and the AP/BS. Fortunately, the invasion attack is more costly when compared with eavesdropping, and more and more security technologies can defend against the invasion attack. In the LE attack, the attackers can estimate the location of users by ranging, and the hardware overhead of the LE attack is higher than that of eavesdropping, which makes the LE attack not as common as eavesdropping. Therefore, preventing the leakage of location privacy on the user-side is vital due to the open nature of the wireless environment, especially for applications in which the retrievability of locations is essential. For instance, in the initial stage of some $k$-anonymity or spatial cloaking methods, the locations of users are transmitted to a trusted third party [10], which provides the chance for the attacker to eavesdrop users’ locations through the wireless channel. Furthermore, it is expected that the development of caching technology will result in more distributed LBS/OSN servers or location verifiers [11,12], e.g., the AP. In conclusion, the privacy protection of locations in the wireless channel is essential for the pervasive public networks.

In this paper, by focusing on the wireless channel, we propose an LPP scheme for MANETs based on Distance, angle, and the idea of Spatial Cloaking (DSC-LPP) to prevent eavesdropping attack. DSC-LPP utilizes the AP-user distance as the primary key to transform the location of the user into a cloaking space, and the ranging result enables the AP to retrieve the location of the user. Different from conventional cryptography, the AP receives the key (dynamically) by ranging, and the storage of the key is not necessary, which reduces the risk of eavesdropping based on the revealing key. Compared with conventional cryptography and $k$-anonymity methods, DSC-LPP can reduce the overhead of communication and computation when preserving location privacy in the wireless channel, and the retrievability of the user’s location on the server-side is retained. Meanwhile, polar coordinates are adopted instead of Cartesian coordinates to improve the feasibility of DSC-LPP, i.e., it is adaptable for applications that need only the direction from AP to the user. Another advantage is that the circular coverage of AP can be easily divided into small zones according to the security requirement due to the utilization of polar coordinates. Finally, DSC-LPP is suitable for some sparse networks, and even there is only one AP and one user.

The main contributions of this paper are as follows:

- To our best knowledge, this is the first work that can protect location privacy in the wireless channel based on distance and ranging, while the retrievability of users’ locations on the server-side can be retained without conventional cryptography.
- The scheme of redundancy check for DSC-LPP has been proposed to improve the accuracy of retrieval.
- The application of DSC-LPP in irregular areas has been investigated.
- The solutions to improve the robustness of DSC-LPP in the harsh environment has been investigated.
- The performance of the proposed methods has been evaluated by simulation, qualitative evaluation, and comparison.

In the following, we outline the related work in Section 2. We present the system and threat model in Section 3, and the detail of DSC-LPP is presented in Section 4. Section 5 depicts the performance evaluation of DSC-LPP based on simulation. The discussion of special cases, security evaluation, and the comparison between DSC-LPP and other LPPs are included in Section 6. At last, we conclude the paper in Section 7.

2. Related Work

To preserve location privacy, researchers have proposed different techniques. Spatial cloaking methods blur the locations of the users into a cloaked space, e.g., $k$-anonymity employs a trusted
anonymizer to blur the locations of a group of at least \( k \) users, and then any user’s location cannot be distinguished from at least \((k - 1)\) other locations [10,13,14]. Space transformation transforms the locations of users into an encoded space such that the locations are irreversible for any devices without the transformation key; meanwhile, some spatial properties of the locations are maintained [15]. Dummy-based methods generate a group of dummies aside with the real location, and then the server cannot distinguish which one is the real location [16]. Differential privacy-based methods transform the locations of the users to an obfuscated location according to a preconfigured probability function, and for any two locations, their probability of being mapped to the obfuscated location are similar, such that the attacker cannot distinguish whether the obfuscated location is transformed from which location [17–20].

To protect users from the LE attack, Sanaa et al. utilized the fake point to confuse the attackers [21]. Arana et al. increased the localization error of attackers by controlling the transmission power [22]. Conventional cryptography is a primary method to protect location privacy from eavesdropping. However, computing overhead and the exchange of secret keys are the challenges for low power networks such as sensor networks [23]. \( k \)-anonymity and dummy techniques can be utilized for LPP in the wireless channel. Unfortunately, the retrieval of locations of users on the AP/server is challenging, making it not suitable for location reports such as location verification and geographic routing.

K. P. N. Puttaswamy et al. partitioned location data based on users’ social groups, and a user will transform its location into the virtual coordinate system before storing the location on untrusted servers. On the other hand, the member in the same group know the key of transformation, and then the other members can transform the virtual location into the real coordinate system [24].

T. Peng et al. enhanced the LPP by utilizing a Function Generator, which is responsible for generating the spatial transformation parameters in \( k \)NN queries. The user transforms its location into a pseudolocation, and, theoretically, other devices can retrieve the real location of the user by connecting the Function Generator [25].

The methods in [24,25] can maintain the retrievability of locations on the server-side, however, the utilization of cryptography and the third party limits the application environment of them. Therefore, the environments that DSC-LPP is adaptive should be as many as possible. An efficient way to achieve the above goal is to limit the computation and communication overhead of DSC-LPP. Moreover, the utilization of a third party should be limited.

### 3. System and Threat Model

Without the loss of generality, we consider a MANET with an AP. The AP needs to retrieve the specific location of the user, and it can estimate the distance between the user and itself via ranging technologies such as Time of Flight (TOF), Time of Arrival (TOA) [26], Received Signal Strength (RSS) [27], etc. A mobile user, which can localize itself with the assistance of a localization system such as the Global Positioning System (GPS), in the same MANET shares its location with the AP for certain desired services, and the location of AP is known. Additionally, all the unencrypted responses from the AP exclude any information that is strictly related to the user’s real location, i.e., the trajectory tracking attack is limited. It worth noting that, in practice, any neighbouring node trusted by the user can retrieve the location of the user based on DSC-LPP.

We assume that conventional cryptography is not applied to the transmission of locations on the user-side. An eavesdropper in a public area is assumed to collect the locations of the user via eavesdropping the wireless channel between the user and the AP. The LE and other attacks are not included in our model. However, we will discuss some enhanced methods to limit the LE attack in Section 6.

Figure 1 shows an example of the privacy attack in wireless channels, where the Attacker can eavesdrop the wireless channels of both User 1 and User 2 simultaneously. Since it is easy to achieve encrypted communication between APs and servers in most environments, the discussion
and evaluation in the following of this paper is also adaptable to scenarios that the location of the user retrieved on the server.

![System and threat model.](image)

**Figure 1.** System and threat model.

4. Proposed Scheme for Location Privacy Preservation

The key idea of DSC-LPP is to transform the user’s location into a cloaking space based on the user-AP distance. Then, the AP retrieves the user’s location based on the ranging result.

4.1. DSC-LPP

Distance between the user and AP is the primary key for transforming and retrieving the location of users. Therefore, the distance information should not be included in any message to preserve the user’s location privacy. That is, the user can transform its location into the cloaking space by calculating the distance between AP and itself, and AP can retrieve the user’s location based on ranging only. The ranging result is with some deviation when compared with the real distance. Therefore, we utilize the normalized distance rather than the exact distance to transform the location to reduce the impact of ranging deviation on retrieving the location of the user.

In DSC-LPP, we divide the AP’s coverage into $m$ ($m > 1$) annuli. A group of annuli-based divisions compose a related space. Furthermore, any location in the related space will be transformed into cloaking space (a division in the same related space). To obfuscate locations in related space and to retrieve locations from the cloaking space correctly, the following requirements of DSC-LPP should be satisfied:

(i) For any transformed location, its possible retrieved locations should not be unique.
For locations in the same annulus, their normalized distances are the same, and each division has only one transformation scheme.

Locations in some cloaking space use the same retrieving method, that is, a cloaking space has only one associate related space and vice versa.

Requirement (i) ensures the obfuscation of transformed locations, i.e., any location in the cloaking space has two or more corresponding real locations. Requirements (ii) and (iii) avoid the ambiguity of retrieved locations, i.e., for any transformed location, its retrieved result is unique once the normalized distance is observed.

The commonly used notations we used in the following of this paper is shown in Table 1.

| Notation | Denotation |
|----------|------------|
| m        | Number of annuli |
| n        | Number of sectors |
| X_u      | Real location of the user |
| X̃_u     | Transformed location of the user |
| ˙X_u     | Retrieved location of the user |
| r_u      | Real radial coordinate of the user |
| ˆr_u     | Ranging result between AP of the user |
| ˜r_u     | Transformed radial coordinate of the user |
| ˆṙ_u    | Retrieved radial coordinate of the user based on primary divisions |
| ˆr̈_u    | Retrieved radial coordinate of the user based on subdivisions |
| ̂r_u     | Final retrieved radial coordinate of the user |
| φ_u      | Real angular coordinate of the user |
| ˆφ_u     | Retrieved angular coordinate of the user based on primary divisions |
| ̇φ_u     | Retrieved angular coordinate of the user based on subdivisions |
| ̋φ_u     | Final retrieved angular coordinate of the user |
| N_d      | Normalized operator for radial coordinate |
| W        | Operator to export the width of division (radial coordinates) |
| N_c      | Normalized operator for angular coordinate |
| ˆα        | Operator to export the included angle of division (angular coordinates) |
| L        | Obfuscation level |
| M_{i,j}  | Primary division in annulus i and sector j |
| S_{p,q}  | Subdivision in annulus p and sector q |
| d_i      | Lower bound of radial coordinates of annulus i |
| w_i      | Width of radial coordinates of annulus i |
| a_j      | Lower bound of angular coordinates of sector j |
| γ_j      | Included angle of angular coordinates of sector j |
| k        | Number of primary divisions in each related space |
| b        | b^2 denotes the number of subdivisions in each primary division |
| T        | Iteration times of redundancy check |

4.2. Primary Scheme

The relationship between Cartesian coordinates and the user-AP distance is non-linear, and then the requirements of DSC-LPP cannot be satisfied in some environments. Besides, the Cartesian coordinates will significantly increase the complexity of designing the divisions in practice. Instead of Cartesian coordinates, the polar coordinates and user-AP distance have a linear relationship, that is, it is feasible to let the transformation meets the requirements of DSC-LPP.

For the polar coordinates, the normalized distance is, in fact, the normalized radial coordinate. Then, the angular coordinate can be transformed based on the radial coordinate. A simple way to transform the angular coordinate is to divide the AP’s coverage into n (n > 1) sectors based on angular coordinates, and each sector has a normalized angular coordinate. For instance, in Figure 2, division $M_{i,j}$ is generated based on annulus $i$ and sector $j$, where $i \in [1,m]$, $j \in [1,n]$, and the lower bounds of radial and angular coordinates of each division are the normalized coordinates.
The divisions we present above are the critical elements to DSC-LPP to enable location privacy preservation. In the rest of this paper, we assume that locations in the same related space use the same transformation scheme, an AP locates at the origin of the polar coordinate system. Specifically, suppose that the real location of the user is $X_u = (r_u, \phi_u)$, where $r_u$ and $\phi_u$ are the radial and angular coordinates, respectively, and then the transformed location of the user is

$$\tilde{X}_u = T(X_u, N_d(r_u), N_c(\phi_u)),$$ \hspace{1cm} (1)

where $T$ is the transformation function, $N_d$ and $N_c$ normalize the radial and angular coordinates based on $r_u$ and $\phi_u$, respectively. With $\hat{r}_u$, the ranging result between user and AP, the retrieved location can be achieved as follows:

$$X_u = R(\tilde{X}_u, N_d(\hat{r}_u)),$$ \hspace{1cm} (2)

where $R$ retrieves the location of the user from the cloaking space. Equations (1) and (2) show that DSC-LPP can retrieve the location of the user without error even $\hat{r}_u \neq r_u$ except that $\hat{r}_u$ falls into another annulus. A redundancy check can reduce the influence of ranging results as it is shown in Sections 4.4 and 5.

It is obvious that in DSC-LPP, a real location is obfuscated with other $\min(m,n)$ locations. Then the number of locations that are obfuscated can reflect the level of security. Inspired by the anonymity level of $k$-anonymity [28], we utilize $L$ to reflect the obfuscation level of DSC-LPP:

$$L = \min(1 - P_d, 1 - P_c),$$ \hspace{1cm} (3)

where $P_d$ and $P_c$ are the probabilities that an eavesdropper can guess out the real radial and angular coordinates, respectively, based on the transformed location. Then, the higher $L$ means higher security of privacy.

**Lemma 1.** In a related space, the maximum obfuscation level can be achieved if the divisions fall into different annuli, and $L \leq (1 - \frac{1}{m})$. 
Proof. Suppose that a related space includes \( k \) divisions, and all the divisions except \( M_{i,j} \) and \( M_{i,j+1} \) fall into different annuli apart from \( i \). If \( \tilde{X}_u = (\tilde{r}_u, \tilde{\phi}_u) \), then \( \tilde{r}_u \) and \( \tilde{\phi}_u \) are the transformed radial and angular coordinates, respectively. \( u = 1, 2, \ldots, X_1 \in M_{i,j}, X_2 \in M_{i,j+1} \), and then, the retrieved radial coordinate is:

\[
\tilde{r}_u = \mathbb{R}_d (\tilde{r}_u, \mathbb{N}_d (\tilde{r}_u)) ,
\]

where \( \mathbb{R}_d \) retrieves \( \tilde{r}_u \) from the cloaking space. It is evident that, without ranging error, \( \mathbb{N}_d (\tilde{r}_1) = \mathbb{N}_d (\tilde{r}_2) \), then we have \( \tilde{r}_1 = \tilde{r}_2 \) if \( \tilde{r}_1 = \tilde{r}_2 \). Equation (4) indicates that the retrieved result in some annulus is unique for the same transformed radial coordinate. Consider that \( M_{i,j} \) and \( M_{i,j+1} \) belong to the same annulus, according to Equation (4), we can retrieve at most \( (k - 1) \) different radial coordinates based on \( \tilde{r}_u \), i.e., \( P_d = \frac{1}{k} \). Note that the divisions can fall into at most \( k \) annuli, then we have \( P_d \geq \frac{1}{k} \), and similarly, \( P_c \geq \frac{1}{k} \).

The above inequalities indicate that \( L \leq (1 - \frac{1}{k}) \). Consider that \( k \leq m \), we have \( L \leq (1 - \frac{1}{m}) \).

4.3. Transformation and Retrieval

Suppose that \( X_u \in M_{i,j} \), then \( \mathbb{N}_d (r_u) = d_i \) and \( \mathbb{W}(r_u) = w_i \) are the lower bound and width of radial coordinates of \( M_{i,j} \), respectively. Correspondingly, \( \mathbb{N}_c (\phi_u) = \alpha_j \) and \( \mathbb{A}(\phi_u) = \gamma_j \) are the lower bound and included angle of angular coordinates of \( M_{i,j} \), respectively, where \( \phi_u \in [0, 360^\circ) \). The cloaking space of \( M_{i,j} \) is \( M_{i,j}' \), and the coordinates in each related space are continuous. Consider the requirements in Section 4.1 and the general case; scale transformation is adopted to calculate the transformed coordinates as follows:

\[
\tilde{r}_u = \frac{r_u - \mathbb{N}_d (r_u)}{\mathbb{W}(r_u)} \mathbb{W}(d_i') + d_i' ,
\]

\[
\tilde{\phi}_u = \phi_u \mod 360^\circ ,
\]

where

\[
\phi_u' = \begin{cases} 
\frac{\phi_u - \mathbb{N}_c (\phi_u)}{\mathbb{A}(\phi_u)} \mathbb{A}(\phi_u) \alpha_j + \alpha_j , & \phi_u \geq \mathbb{N}_c (\phi_u) \\
\phi_u + 360^\circ - \mathbb{N}_c (\phi_u) + \alpha_j , & \text{others}
\end{cases} .
\]

In Equations (5) and (7), \( d_i' \) and \( \alpha_j \) can be extracted based on the related space determined by \( \mathbb{N}_d (r_u) \) and \( \mathbb{N}_c (\phi_u) \).

In practice, the lower bounds, the widths, and the included angles can be configured by either the AP or the user, and thus Equations (5) and (6) can be calculated once \( M_{i,j} \) is determined.

It is easy to retrieve the radial coordinate from cloaking space once the ranging result, \( \tilde{r}_u \), is known. That is

\[
\tilde{r}_u = \frac{\tilde{r}_u - d_i'}{\mathbb{W}(d_i')} \mathbb{W}(r_u) + \mathbb{N}_d (r_u) .
\]

For a specific division, the lower bound of angular coordinate can be implied by the lower bound of the radial coordinate. Let \( \mathbb{D} \) extract the lower bound of angular coordinate based on the ranging result and cloaking space, then the retrieved angular coordinate in the general case is

\[
\tilde{\phi}_u = \phi_u' \mod 360^\circ ,
\]

where

\[
\phi_u'' = \begin{cases} 
\frac{\phi_u - \alpha_j}{\mathbb{A}(\alpha_j)} \mathbb{A}(\alpha_j) + \alpha_j , & \tilde{\phi}_u \geq \alpha_j \\
\phi_u + 360^\circ - \alpha_j , & \text{others}
\end{cases} .
\]
\[ \alpha_{\gamma'} = D (d_{\gamma'}, \alpha_{\gamma'}, r_u) \quad . \] (11)

The transformation process of DSC-LPP (primary divisions) in the general case is shown in Algorithm 1, where the primary search method is adopted to demonstrate the transformation process clearly. It worth noting that the computation overhead can be reduced in practice by adopting other search methods such as the binary search. The primary divisions can be varied according to the environment and the security requirement, and a typical process of designing the primary divisions is as follows:

**Step 1:** Determine the number of annuli \((m)\) and sectors \((n)\), the width of each annulus \((w_i)\) and the included angle of each sector \((\gamma_j)\) according to the requirement of security (e.g., obfuscation level), the characteristics of devices (e.g., mobility) and the environment (e.g., ranging accuracy), and let \(m \leq n\).

**Step 2:** Let the location of the receiver (e.g., base station) be the center, plot circles to divide the coverage of the receiver into \(m\) annuli according to \(w_i\), and plot radial lines from the center to divide the coverage of the receiver into \(n\) sectors according to \(\gamma_j\).

**Step 3:** Adjust and/or merge divisions according to the environment, and the essential requirement of adjusting/merging divisions is to ensure each related space includes \(m\) divisions (an example of this step is shown in Section 6.1).

**Step 4:** Label each related space and cloaking space according to the requirements of DSC-LPP, and it is suggested to let all the cloaking spaces in the same annulus such that the communication overhead can be limited due to that the parameters for transformation is limited.

**Algorithm 1** Transformation process of DSC-LPP (primary divisions)

1. **INPUT**: \(r_u, \phi_u\), primary divisions, related space(s), cloaking space(s);
2. **OUTPUT**: transformed location;
3. **if** \(w_i = w_i + 1 \quad \forall i \in [1, m)\) **then**
4. \(N_d(r_u) = w_i \lfloor \frac{r_u}{w_i} \rfloor ;\)
5. \(W(r_u) = w_i ;\)
6. **else**
7. **if** \(N_c(0^\circ) = 0^\circ\) **then**
8. \(N_c(\phi_u) = \phi_u \lfloor \frac{\phi_u}{\gamma_j} \rfloor ;\)
9. **else**
10. \(N_c(\phi_u) = \phi_u \lfloor \frac{\phi_u}{\gamma_j} \rfloor - (360^\circ - N_c(0^\circ)) ;\)
11. **if** \(N_c(\phi_u) < 0^\circ\) **then**
12. \(N_c(\phi_u) = N_c(\phi_u) + 360^\circ ;\)
13. **end if**
14. **end if**
15. **end if**
16. **if** \(\gamma_j = \gamma_{j+1} \forall j \in [1, n)\) **then**
17. **if** \(N_c(0^\circ) = 0^\circ\) **then**
18. \(N_c(\phi_u) = \phi_u \lfloor \frac{\phi_u}{\gamma_j} \rfloor ;\)
19. **else**
20. \(N_c(\phi_u) = \phi_u \lfloor \frac{\phi_u}{\gamma_j} \rfloor - (360^\circ - N_c(0^\circ)) ;\)
21. **if** \(N_c(\phi_u) < 0^\circ\) **then**
22. \(N_c(\phi_u) = N_c(\phi_u) + 360^\circ ;\)
23. **end if**
24. **end if**
25. **else**
26. **while** \(|\phi_u - \alpha_j| > \gamma_j\) and \(|\phi_u - (\alpha_j) \mod n\) - \(\phi_u| > \gamma_j\) **do**
27. \(j = -1 ;\)
28. **end while**
29. \(N_c(\phi_u) = \alpha_j ;\)
30. \(\alpha_{\gamma_u} = \gamma_j ;\)
31. **end if**
32. Calculate the transformed location according to Equations (5)–(7);
4.4. Redundancy Check

A division can be further divided into subdivisions. Then a related space of primary divisions is covered by some related spaces of subdivisions, as it is shown in Figure 3, where we use the equivalent matrix to demonstrate the divisions in the coverage of AP. The transformation and retrieval of locations in a subdivision are the same as those in a primary division. The subdivisions are designed as the redundancy check for primary division to limit the deviations of retrieved locations.

![Figure 3. Subdivisions of DSC-LPP.](image)

The retrieved locations of the user should be the same in different types of divisions. Suppose that the retrieved radial coordinates of the user in subdivisions is \( \hat{r}_u \). Then, \( \hat{r}_u \) is the final retrieved results if \( \hat{r}_u = \dot{r}_u \). Otherwise, the AP will measure the distance again or use other methods to achieve the final result. The pseudo-code of the retrieving process of DSC-LPP with a redundancy check is shown in Algorithm 2, where \( \tilde{R}_u \) includes the transformed radial coordinates of \( X_u \) in both the primary divisions and the subdivisions, and \( \tilde{\Phi}_u \) includes the transformed angular coordinates correspondingly. \( \dot{r}_{u,t} \) and \( \dot{\phi}_{u,t} \) are the retrieved results of \( r_u \) and \( \phi_u \) of iteration \( t \) (\( t > 0 \)) in primary divisions, respectively, and similarly, \( \tilde{r}_{u,t} \) and \( \tilde{\phi}_{u,t} \) are the retrieved results of iteration \( t \) in subdivisions. Recent \( c \) \( (c \leq T) \) retrieved results are utilized to estimate the final results if \( T \), the maximum iteration times, is reached.
Algorithm 2: Retrieving process of DSC-LPP with redundancy check

```
1: INPUT : \( \hat{R}_u, \Phi_u \), primary divisions, subdivisions, related space(s), cloaking space(s);
2: OUTPUT : final retrieved result;
3: \( t = 0; \)
4: \( \hat{R}_{u,0} = 0; \)
5: \( \hat{\Phi}_{u,0} = 1; \)
6: while \( \hat{R}_{u,t} \neq \hat{R}_{u,t-1} \) and \( t < T \) do
7: \( t++; \)
8: Get a new ranging result \( \hat{R}_u \), and then calculate \( \hat{R}_{u,t}, \hat{\Phi}_{u,t}, \phi_u \) according to \( \hat{R}_u, \Phi_u, \hat{R}_u \), Equations (8) and (9);
9: if \( \hat{R}_u = \hat{R}_{u,t} \) then
10: \( \hat{R}_u = \hat{R}_{u,t}, \phi_u = \phi_{u,t}; \)
11: break;
12: else if \( t = T \) then
13: \( \hat{R}_u = \left( \frac{1}{T} \right) \sum_{t' = t - c + 1}^{t} \hat{R}_{u,t'}; \)
14: \( \hat{\Phi}_u = \left( \frac{1}{2T} \right) \sum_{t' = t - c + 1}^{t} (\hat{\Phi}_{u,t'} + \phi_{u,t'}); \)
15: break;
16: end if
17: end while
18: The final retrieved result is \((\hat{R}_u, \hat{\Phi}_u)\)
```

A well-designed subdivisions cannot reduce the obfuscation level achieved by the primary divisions.

**Lemma 2.** The subdivisions will not reduce the obfuscation level of DSC-LPP if \( M \subseteq \sum_{v} S_v \) and any division of \( M \) includes at least one division of \( S_v \). \( S_v \) and \( M \) are the related spaces of subdivisions and primary divisions, respectively, \( v \geq 2 \).

**Proof.** Suppose that \( L = (1 - \frac{1}{m}) \) for \( M \)-based DSC-LPP. If any division of \( M \) includes at least one division of \( S_v \), then at least \( m \) different coordinates can be retrieved from any location in the cloaking space of \( S_v \). Consider that \( M \subseteq \sum_{v} S_v \), then the obfuscation level of \( S_v \) will not exceed \( (1 - \frac{1}{m}) \). \( \square \)

The designing process of subdivisions is similar to that of primary divisions except that the adjusting/merging process is not necessary for designing subdivisions, as each subdivision is a part of some primary division, and all the subdivisions should conform to the assumption in Lemma 2.

**Lemma 3.** If the situation in Lemma 2 is real, the false retrieval probability of \( X_u \) is reduced when compared with primary division-only DSC-LPP. Suppose that each primary division includes \( b^2 \) subdivisions with the same width and included angle, then if \( X_u \in M_{i,j} \cap S_{p,q} \) and \( T \to \infty \), the false retrieval probability of \( X_u \) is

\[
P_f(X) = \sum_{i=1}^{m-1} P \left( l_{p+eb} \leq \hat{R}_u < l_{p+eb} + s_{p+eb} \right) + \sum_{c=1}^{m-1} P \left( l_{p+eb} \leq \hat{R}_u < l_{p+eb} + s_{p+eb} \right),
\]

(12)

where \( i \in [2, m - 1] \), \( l_p \) and \( s_p \) are the lower bound and width of radial coordinates of subdivision \( S_{p,q} \), \( d_i < d_{i+1} \), \( l_p < l_{p+1} \), and \( P \) denotes probability.

**Proof.** According to Equations (8) and (10), if \( \hat{R}_u \) falls into annulus \( i \), the retrieved result has no deviation if \( \mathbb{N}_d(\hat{R}_u) = d_i \). Consequently, without subdivisions, the false retrieval probability of \( X_u \) is

\[
P_f(X) = P \left( \hat{R}_u \geq d_i + w_i \right) + P \left( \hat{R}_u < d_i \right).
\]

(13)
If $T \to \infty$, the final retrieved result will be achieved if $\hat{r}_u = \check{r}_u$, that is,

$$\left[ \min (\hat{r}_u, \check{r}_u), \max (\hat{r}_u, \check{r}_u) \right] \subseteq [l_x, l_x + s_x]. \quad (14)$$

Consider that in each primary division, at most an $x$ can let Equation (14) to be true, then we have

$$P_f (\hat{X}) \leq \sum_{h=1}^{i-1} P (l_x \leq \hat{r}_u < l_x + s_x) + \sum_{h=i+1}^{m} P (l_x \leq \hat{r}_u < l_x + s_x) \quad (15)$$

$$s.t. \; l_x \in [d_h, d_h + w_h].$$

If any primary division includes two or more subdivisions, then $P_f (\hat{X}) < P_{\check{g}} (\hat{X})$. Furthermore, suppose that $\hat{r}_u \in [d_{i+c}, d_{i+c} + w_{i+c}], (i + c) \in [1, m]$, then, according to Equation (8), we have

$$\frac{\hat{r}_u - d_{i+c}}{w_{i+c}} = \frac{r_u - d_i}{w_i}, \quad (16)$$

on the other hand, consider that $s_p = \frac{w_j}{b}, s_{p+eb} = \frac{w_{i+c}}{b}$, we have

$$\frac{l_{p+eb} - d_{i+c}}{w_{i+c}} = \frac{l_p - d_i}{w_i}. \quad (17)$$

Equations (16) and (17) indicate that if $r_u \geq l_p$, we have $t_u \geq l_{p+eb}$, and similarly, $\hat{r}_u < (l_{p+eb} + s_{p+eb})$, then we can conclude that the final retrieved result will be achieved if $\hat{r}_u \in [l_{p+eb}, l_{p+eb} + s_{p+eb})$. Finally, we have Equation (12).

In fact, for $i = m$ and $i = 1$, the false retrieval probabilities of $\check{X}_u$ are the first and second parts of the right-hand side of Equation (12), respectively. Lemma 3 indicates that with the same number of primary divisions, more subdivisions means the smaller false retrieval probability if $T \to \infty$.

Consider Figure 3 as an example. Suppose that the user located in $S_{2,1}$, then the retrieved location will be accepted if the ranging result falls into the annuli of $S_{2,1}, S_{4,3}, S_{6,5}$, and $S_{8,7}$. On the other hand, without the redundancy check, any ranging result and retrieved location will be accepted. Therefore, the redundancy check can improve the accuracy of retrieved locations.

Theoretically, the more subdivisions will result in the lower probability of retrieving an incorrect location if there are enough iterations. In practice, the more subdivisions mean the higher probability of ruining a correct retrieved location due to the ranging error. For instance, in the example of the above paragraph, if the ranging result falls into the annulus of $S_{1,1}$, the retrieved result will be rejected. However, the retrieved result of the primary division is correct in such a case, and the later ranging result may achieve the final retrieved result in $S_{4,3}$, which ruins a correct retrieved location. Therefore, it is necessary to design the subdivisions and the threshold of iterations carefully according to the application environment.

Finally, assistant methods, such as the majority vote for the accepted retrieved results, can limit the probability of ruining a correct retrieved location if there are enough iterations. For instance, Algorithm 2 can be repeated for several times, and then several final retrieved results are achieved. It worth noting that for any transformed location, its possible retrieved locations are limited. Consequently, the final retrieved result, which gets the most votes, is the ultimate result. Consider that the ranging deviation of the line-of-sight (LoS) link obeys the Gauss distribution. We can conclude that, in most cases of the LoS situation, the probability of the ranging result falling into an incorrect division is less than that of the ranging result falling into the correct division, and then the retrieval deviation is limited by the majority vote. If the majority vote is adopted, iterations will terminate when some retrieved location gets enough votes or the maximum iteration times are reached.
5. Simulations

We use MATLAB to launch the simulation and then evaluate the performance of DSC-LPP. The maximum communication range of AP is 50 m, besides \( c = 3 \). RSS is adopted as the ranging method, and the transmission power is 20 dbm [29], and the ranging model is as follows:

\[
G(r_u) = G(r_0) - 10K_a \eta \log \left( \frac{r_u}{r_0} \right) + F_c
\]

where \( G(r) \) is the received signal strength at the distance of \( r \), \( r_0 \) is the reference distance and \( G(r_0) = -35 \) dbm. \( \eta = 4 \) is the coefficient of path loss. \( F_c \sim N(0, \sigma^2) \) is the noise variable, and \( \sigma = 1 \) except that in Figure 10.

\( K_a \) is the coefficient of radio irregularity on the direction from the user to the AP (degree \( a \)) [30], \( K_a \) is expressed as:

\[
K_a = \begin{cases} 
1, & a = 0 \\
K_{a-1} \pm \text{Rand}_{\mu, \nu} \cdot \text{DOI}, & a \in (0, 360) \cap \mathbb{Z} \\
\end{cases} 
\]

s.t. \( |K_0 - K_{359}| \leq \text{DOI} \) (19)

where Rand\(_{\mu, \nu}\) is a Weibull random variable with the shape parameter of \( \mu \) and the scale parameter of \( \nu \). DOI > 0 is the indicator of irregularity degree, and \( \mathbb{Z} \) is the set of integers. For degree \( a' \in (a-1, a) \), \( K_{a'} = K_{a-1} + (a' - a + 1)(K_a - K_{a-1}) \). To evaluate the original performance of DSC-LPP, we suppose that AP is stationary, and the user can transmit sequential ranging signal with a small interval. Therefore, the impact of mobility of users and radio irregularity on the ranging result can be incorporated in the noise (i.e., \( K_a = 1 \)) in most cases except that in Figures 7b, 8 and 9. All the results are evaluated based on 10,000 tests. The location of the user in each test is generated randomly, and the maximum distance between AP and the user is 100 m.

The width, included angle of primary divisions are the same, and the coverage of AP includes \( k^2 \) primary divisions. The relationship between primary divisions and subdivisions is the same as in Lemma 3, where \( b = 8 \) in Figures 4–6 and 11. The coordinates of each related space are continuous, i.e., \( M \neq \sum S_v \). Consequently, the boundary of primary divisions will be considered if \( t = T \) and \((r_u, \phi_u) \notin M \); that is, the final retrieved result will be modified to let \((r_u, \phi_u) \in M \) in the above case.

Figures 4a,b show the Cumulative Distribution Function (CDF) of the deviation of \( \hat{X}_u \). We set \( T = 5 \), and the user can transmit \( T \) ranging signals to AP continuously. Figure 4a indicates that fewer divisions mean a higher probability of accurate retrieval and lower security, where the deviations of more than 99.57%, 94.79%, 88.53%, and 81.49% tests are less than 10 m for \( k = 2 \), \( k = 5 \), \( k = 10 \), and \( k = 15 \), respectively. It worth noting that we utilize the original RSS to estimate the distance in our simulation, and it is expected that an advanced ranging technology could increase the accuracy of retrieval further. Also, the large number of primary divisions can limit the large deviations. Figure 4b indicates that when \( k \leq 5 \), the deviations of more than 93% retrieved angular coordinates are less than 10°. Therefore, we can conclude that DSC-LPP is also suitable for applications that only concern the direction from AP to the user.
Figure 4. CDF of deviation of: (a) retrieved locations with different primary divisions; (b) $\bar{\phi}_u$ with different primary divisions.

Figure 5 shows the CDF of the deviation of $\bar{X}_u$ with different $T$, where $k = 5$. The deviations of more than 97.07%, 96.39%, 94.79%, and 92.88% tests are less than 10 m for $T = 9$, $T = 7$, $T = 5$, and $T = 3$, respectively. It can be concluded that more iterations result in more correct retrieved results, and the impact of iteration times on large deviations is limited.

In Figure 6, the iterations are terminated when $\ddot{r}_u = \dot{r}_u$. We suppose that the user is stable to analyse the impact of primary division quantity on convergence of DSC-LPP. It is evident that more primary divisions result in more iterations, and the CDF of iterations can help to determine $T$ in practice. Besides, it is feasible to finish the continuous ranging tests within a short time. Figure 6 indicates that 95% tests are converged within 4, 11, 24, and 35 iterations for $k = 2$, $k = 5$, $k = 10$, $k = 15$, respectively.

Figure 5. CDF of deviation of retrieved locations with different $T$. 
In the following simulations, $k = 5$ except that in Figure 11. Figure 7a indicates that the subdivisions can improve the accuracy of retrieved locations effectively, and the best performance is achieved when $b = 2$. Note that Lemma 3 reveals that the deviation of the retrieved location will decrease along with the increasing of $b$ theoretically; however, the limited iterations and ranging error will affect the performance of redundancy check. Therefore, the best performance of the redundancy check will be achieved with different $b$ when the iteration times and environment are changed.

In Figure 7b and the following mobile cases, the impact of radio irregularity cannot be ignored, where $DOI = 0.005, \mu = 0.67, \nu = 0.16$. We suppose the user is a walker with a speed of 3.6 km/h (1 m/s), and its moving direction changed randomly per second. The interval of broadcasting the ranging signal is 1 s. Figure 7b indicates that with the proper value of $b$, the subdivisions can reduce the deviation of retrieved locations in walking cases. Note that $b = 1$ means that only the primary divisions are adopted.

The performance of DSC-LPP in stationary cases and the mobile cases are compared in Figure 8, and we can conclude that, with the appropriate value of $b$, the impact of mobility (walking cases) on the performance of redundancy check is limited. Figure 8b demonstrates the average deviation of the retrieved locations with different numbers of subdivisions, and we can conclude that the redundancy check is useful when $b < 8$. When $b \geq 8$, the average deviation with redundancy check is over that of
the case without redundancy check due to the mobility and the limited iterations, and therefore, it is necessary to design the subdivisions carefully in practice.

Figure 8. Comparison: (a) CDF of deviation of retrieved locations with different subdivisions; (b) Average deviation of retrieved locations with different subdivisions.

Figure 9 shows the deviation of retrieved locations with the speed of walking/robots (3.6 km/h), bicycles (18 km/h), unmanned aerial vehicles (36 km/h), and vehicles (72 km/h), where \( b = 5 \). We can conclude that with the proper design of subdivisions, the impact of mobility on the performance of the redundancy check is limited. It worth noting that, in practice, the interval consecutive transmissions for RSS ranging can be reduced to 100 ms [31], and then the impact of mobility on the performance of the redundancy check can be further suppressed.

Figure 9. CDF of deviation of retrieved locations with different speeds.

The impact of noise on retrieval performance can reflect the robustness of DSC-LPP in different environments and can help to determine the strategy of LPP. Figure 10a shows that the retrieval accuracy of DSC-LPP increases along with the decrease of noise. Therefore, it is necessary to use other methods to improve the performance of DSC-LPP in a harsh environment. For instance, the user can switch its LPP mode from DSC-LPP to cryptography when the link status changes from LoS to non-line-of-sight (NLoS). Another candidate solution is to utilize one or several trusted assistant neighbour(s) to forward the ranging result between the user and its one-hop-neighbour to the AP. It worth noting that because all the nodes utilize DSC-LPP, the AP can retrieve the locations of nodes
from the neighbour of itself to the user sequentially. Figure 10b shows the effectiveness of the assistant neighbour-based solution. In the “one hop” case, the AP retrieves the location of the user based on the signal from the user with much noise (e.g., NLoS link). In the other cases, the AP retrieves the location of the user based on the signal from the assistant neighbour(s). The ranging result from the user to its one-hop-neighbour is forwarded one, two, and three times in the cases of “two hops”, “three hops”, and “four hops”, respectively, and all the links are with limited noise (i.e., LoS link).

Finally, we compare the retrieval performance of DSC-LPP with that of \( k \)-anonymity. Figure 11 indicates that the average retrieval accuracy of DSC-LPP is higher than that of \( k \)-anonymity. In \( k \)-anonymity, the other \((k - 1)\) dummy locations are the other possible retrieved locations in the same related space, and the AP retrieves the locations by guessing.

6. Discussions

6.1. Special Cases

In practice, the division of angular coordinates is optional, and Equations (6) and (9) can be simplified as a transformation based on \( r_u \) and \( \hat{r}_u \), respectively. On the other hand, the division of angular coordinates increases the flexibility of DSC-LPP. For instance, suppose \( M_{4,4} \) in Figure 2 is
the only division available for users in $M_i$, then the eavesdropper can infer the locations of users. To avoid the above weakness of DSC-LPP, we can merge $M_{4,4}$ into other related space(s) to obfuscate the locations of users.

It is common in reality that an irregular area is not available for most users, which results in some irregular areas that are available for users. Then the obfuscation level of some areas will be reduced in such a case. The reduction of obfuscation level can be avoided by merging an irregular area into its neighbouring division, as it is shown in Figure 12. As the unavailable area $B$ divide $M_{4,1}$ into different parts, the obfuscation level of the related space of $M_{4,1}$ is reduced to $\frac{4}{3}$, to avoid the reduction of obfuscation level, the left part of $M_{4,1}$ is merged into $M_{4,4}$. Because the upper bound of the angular coordinates of new $M_{4,4}$ is irregular, $A(\phi_u)$ is calculated as follows:

\[ A(\phi_u) = V(r_u, \phi_u) - N_c(\phi_u), \]  

(20)

where $V(r_u, \phi_u)$ is the upper bound of the angular coordinates of the new $M_{4,4}$ when the radial coordinate is $r_u$. Equation (20) indicates that for irregular boundaries, the transformation and retrieval of coordinates should consider the radial and the angular coordinates simultaneously. On the other hand, it is not necessary to merge the other irregular parts divided by $B$ into their neighboring divisions, and the included angle of angular coordinates of new $M_{4,1}$ and the width of radial coordinates of $M_{3,1}$ can be calculated similarly to Equation (20). It is easy to prove that the obfuscation level in Figure 12 is still 0.75, as same as that in Figure 2. Finally, we can conclude that, in any case, the obfuscation level of DSC-LPP can be maintained if the coordinates of each division are continuous, and the number of divisions in each related space is as same as that in the original case (no irregular division existed).

Figure 12. Primary divisions with irregular area.

6.2. Security Evaluation

Mobility is a primary concern in practice. DSC-LPP is designed for users to report their real-time locations rather than the past locations, and a user should re-localize itself if the delay between the recording and the transmitting time of location reaches some threshold. Thus the impact of mobility on the deviation of retrieved location is limited.
The scheme of “handover” should be designed carefully to avoid the revealing of locations. Any user in the overlapping area of different APs should select the appropriate related space to transform its location. Otherwise, the eavesdropper can infer the location of the user based on the relationship of divisions in different APs. A simple solution for “handover” is to generate the transformed location based on the related space of new AP if the last and current real locations are not in the same primary division of the current AP. Besides, conventional cryptography and $k$-anonymity can also be utilized to assist the “handover”.

It worth noting that if the AP broadcasts the division scheme without any conventional encryption, the location privacy can still be protected in most scenarios. The first exception is that the eavesdropper is very close to the AP, where the eavesdropper can estimate the distance between the user and itself. The second exception is that the eavesdropper-user distance is much different from the distance between the eavesdropper and any other retrieved location. The third exception is the LE attack. Fortunately, once AP can avoid the approaching of an eavesdropper, e.g., AP is mobile, the above weaknesses can be eliminated by adopting TOF/TOA ranging and the dynamic transmission power [22]. Note that with TOF/TOA ranging, the user does not need to inform its current transmission power to the AP. Thus it is almost impossible for the eavesdroppers to estimate the accurate distance between it and the user.

6.3. Comparison

Consider that it is difficult for the attackers to steal the secret keys of a MANET; the location privacy of conventional cryptography is higher than other methods. Based on the system and threat model we assumed, the location privacy of $k$-anonymity and DSC-LPP depend on the anonymity level and the obfuscation level, respectively. The privacy level of differential privacy depends on the privacy budget.

According to the theories of some classic encryption methods and [19], the computation overhead of conventional cryptography is high. On the other hand, we assume that the other $k−1$ locations of $k$-anonymity are generated by dummy techniques (to make it adaptable for sparse MANETs). Then the maximum computation overhead (complexity) of $k$-anonymity is $O(k)$. Differential privacy obfuscates the location of the user to another one according to a pre-configured probability function; therefore, its computation overhead is low. For DSC-LPP, the computation overhead consumes in the process of matching the division (search $i$ and $j$). In the worst case, the included angles of divisions in the same annulus are different from each other. Consider that it is convenient to store the boundaries of annuli in order, then the maximum computation complexity of DSC-LPP is $O(\log_2 n)$ by adopting the binary search (note that $n \geq m$).

Consider that the length of ciphertext is larger than plaintext in some cases, then the communication overhead of conventional cryptography is various. Most of the dummy-based $k$-anonymity methods need to transmit $k$ locations to the AP to avoid the eavesdropping attack. Then the communication overhead of $k$-anonymity is high. Differential privacy and DSC-LPP transmit only the transformed location to the AP; then, their communication overhead is as low as the primary transmission. It worth noting that the comparison here is for uplink only, and for location reports, the resource of uplink in a MANET is less than that of the downlink in typical cases.

With a secret key, the AP can retrieve the location of users directly. Therefore, its retrievability is prefect. In $k$-anonymity and differential privacy, the AP can retrieve the location of the user by guessing only. Then, the retrievability of $k$-anonymity and differential privacy is low. At last, our simulation results show that the AP can retrieve the locations of users with a high probability, and then the retrievability of DSC-LPP is high.

Finally, we can conclude that DSC-LPP can extend the applicable environments of $k$-anonymity as the comparison shows in Table 2.
Table 2. Comparison of different LPP methods

|                      | Loc. Privacy | Comp. Overhead * | Comm. Overhead + | Retr. on AP |
|----------------------|--------------|------------------|------------------|-------------|
| Conventional cryptography [19] | High         | High             | Various          | Perfect     |
| k-anonymity ♦ [10]    | Anonymity level ≤ O(k) | High             | Low              | Low         |
| Differential privacy [18] | Privacy budget | Low              | Low              | Low         |
| DSC-LPP              | Obfuscation level ≤ O(log₂ n) | Low              | High             |             |

Loc. = Location; Comp. = Computation; Comm. = Communication; Retr. = Retrievability; * Applicable for users only; ♦ Use dummy techniques to generate other k – 1 locations; + Applicable for the uplink only, and the scheme of divisions are known by the user and AP.

7. Conclusions

In this paper, we proposed DSC-LPP based on distance, angle, and the idea of spatial cloaking. DSC-LPP is a solution for MANETs to preserve location privacy in the wireless channel while retaining the retrievability of locations on the server-side. DSC-LPP is suitable for sparse MANETs and location reports, and it can enhance the reliability of k-anonymity and other conventional LPPs by increasing the privacy between the user and the trusted third party. Retrievability is one of the main advantages of DSC-LPP, and simulation results show that, with the proper-designed parameters, AP can correctly retrieve the location of users with a high probability, even when the user is mobile. Additionally, the performance of DSC-LPP in the harsh environment can be improved by adopting adaptive strategies such as traditional cryptography or routing. Besides, Qualitative evaluation indicates that DSC-LPP can reduce the communication overhead when compared with k-anonymity, and the computation overhead is limited when compared with conventional cryptography. Meanwhile, the retrievability of DSC-LPP is higher than that of k-anonymity and differential privacy. In the future, we will investigate advanced division and “handover” schemes to improve the performance of DSC-LPP, as well as low-cost solutions for improving the performance of DSC-LPP in the harsh environment. The integration of DSC-LPP with conventional LPP methods is also a candidate topic. Besides, it is necessary to investigate other solutions, except “merging”, for cases of irregular divisions to improve the flexibility of DSC-LPP.

Author Contributions: The work presented here was completed in collaboration among all authors. Research conceptualization, N.J. and S.Y.; methodology, N.J.; software, N.J. and S.Y.; validation, N.J. and S.Y.; formal analysis, N.J.; investigation, S.Y. and N.J.; resources, P.X.; data curation, S.Y.; Writing—Original draft preparation, N.J.; Writing—Review and editing, S.Y. and P.X.; visualization, N.J.; supervision, P.X. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science and Technology Major Project, China (No. 2018ZX03001008-002).

Acknowledgments: We would like to thank Qing Wang, KU LEUVEN, Belgium, for his valuable feedback to this paper.

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

References

1. Yu, R.; Kang, J.; Huang, X.; Xie, S.; Zhang, Y.; Gjessing, S. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks. IEEE Trans. Dependable Secur. Comput. 2016, 13, 93–105.
2. Jin, W.; Xiao, M.; Li, M.; Guo, L. If You Do Not Care About It, Sell It: Trading Location Privacy in Mobile Crowd Sensing. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1045–1053.
3. Pourmajaf, L.; Garcia-Ulloa, D.A.; Xiong, L.; Sunderam, V. Participant privacy in mobile crowd sensing task management: A survey of methods and challenges. SIGMOD Rec. 2015, 44, 23–34.
4. Madasamy, B.; Balasubramanian, P. Geographical angular zone-based optimal resource allocation and efficient routing protocols for vehicular ad hoc networks. IET Intell. Transp. Syst. 2018, 12, 242–250.
5. Schlegel, R.; Chow, C.; Huang, Q.; Wong, D.S. User-Defined Privacy Grid System for Continuous Location-Based Services. *IEEE Trans. Mob. Comput.* 2015, 14, 2158–2172.

6. Huguenin, K.; Bilogrevic, I.; Machado, J.S.; Mihaila, S.; Shokri, R.; Bacosta, I.; Hubaux, J. A Predictive Model for User Motivation and Utility Implications of Privacy-Protection Mechanisms in Location Check-Ins. *IEEE Trans. Mob. Comput.* 2018, 17, 760–774.

7. Luo, C.; Ma, B.; Chen, F.; Guan, Q.; Yu, H.; Ji, F. Multicore-Processor Based Software-Defined Communication/Network Platform for Underwater Internet of Things. *Sensors* 2019, 19, 5168.

8. Lee, J.G.; Chim, S.; Park, H.H. Energy-Efficient Cluster-Head Selection for Wireless Sensor Networks Using Sampling-Based Spider Monkey Optimization. *Sensors* 2018, 17, 5281.

9. Nosouhi, M.R.; Pham, V.V.H.; Yu, S.; Xiang, Y.; Warren, M. A Hybrid Location Privacy Protection Scheme in Big Data Environment. In *Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference*, Singapore, 4–8 December 2017; pp. 1–6.

10. Ying, B.; Nayak, A. A Distributed Social-Aware Location Protection Method in Untrusted Vehicular Social Networks. *IEEE Trans. Veh. Technol.* 2019, 68, 6114–6124.

11. Wen, W.; Cui, Y.; Zheng, F.; Jin, S.; Jiang, Y. Enhancing Performance of Random Caching in Large-Scale Heterogeneous Wireless Networks With Random Discontinuous Transmission. *IEEE Trans. Commun.* 2018, 66, 6287–6303.

12. Liu, D.; Lee, M.; Wu, D. A Node-to-Node Location Verification Method. *IEEE Trans. Ind. Electron.* 2010, 57, 1526–1537.

13. Gedik, B.; Liu, L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Trans. Mob. Comput.* 2008, 7, 1–18.

14. Jiang, H.; Zhao, P.; Wang, C. RobLop: Towards Robust Privacy Preserving Against Location Dependent Attacks in Continuous LBS Queries. *IEEE/ACM Trans. Netw.* 2018, 26, 1018–1032.

15. Khoshgozaran, A.; Shirani-Mehr, H.; Shahabi, C. Blind evaluation of location based queries using space transformation to preserve location privacy. *GeoInformatica* 2013, 17, 599–634.

16. Liu, H.; Li, X.; Li, H.; Ma, J.; Ma, X. Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services. In *Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications*, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9.

17. Gong, Y.; Zhang, C.; Fang, Y.; Sun, J. Protecting Location Privacy for Task Allocation in Ad Hoc Mobile Cloud Computing. *IEEE Trans. Emerg. Top. Comput.* 2018, 6, 110–121.

18. Wang, L.; Yang, D.; Han, X.; Zhang, D.; Ma, X. Mobile Crowdsourcing Task Allocation with Differential-and-Distortion Geo-Obfuscation. *IEEE Trans. Dependable Secur. Comput.* 2019, doi:10.30110/TDSC.2019.2912886.

19. Andres, M.E.; Bordenabe, N.E.; Chatzikokolakis, K.; Palamidessi, C. Geo-Indistinguishability: Differential privacy for location-based systems. In *Proceedings of the ACM Conference on Computer and Communications Security*, Berlin, Germany, 4–8 November 2013; pp. 901–914.

20. Yin, C.; Xi, J.; Sun, R.; Wang, J. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* 2018, 14, 3628–3636.

21. Taha, S.; Shen, X. A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs. *IEEE Trans. Intell. Transp. Syst.* 2013, 14, 1665–1680.

22. Arana, O.; Garcia, F.; Gomez, J. Analysis of the effectiveness of transmission power control as a location privacy technique. *Comput. Netw.* 2019, 163, 106880.

23. Wang, D.; Li, W.; Wang, P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* 2018, 14, 4081–4092.

24. Puttaswamy, K.P.N.; Wang, S.; Steinbauer, T.; Agrawal, D.; Abbadi, A.E.; Kruegel, C.; Zhao, B.Y. Preserving Location Privacy in Geosocial Applications. *IEEE Trans. Mob. Comput.* 2014, 13, 159–173.

25. Peng, T.; Liu, Q.; Wang, G. Enhanced Location Privacy Preserving Scheme in Location-Based Services. *IEEE Syst. J.* 2017, 11, 219–230.

26. Jiang, N.; Xu, P.; Yao, Y.; Bui, T.; Chen, Q. Exploiting Radoi Irregularity for Location Verification in Sparse MANETs. *IEEE Commun. Lett.* 2018, 22, 1284–1287.

27. Wu, X.; Yang, P.; Tang, S.; Zheng, X.; Xiong, Y. Privacy preserving RSS map generation for a crowdsensing network. *IEEE Wirel. Commun.* 2015, 22, 42–48.
28. 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.

29. Auer, G.; Giannini, V.; Desset, C.; Godor, I.; Skillermark, P.; Olsson, M.; Imran, M.A.; Sabella, D.; Gonzalez, M.J.; Blume, O.; et al. How much energy is needed to run a wireless network? *IEEE Wirel. Commun.* 2011, 18, 40–49.

30. Zhou, G.; He, T.; Krishnamurthy, S.; Stankovic, J.A. Models and Solutions for Radio Irregularity in Wireless Sensor Networks. *ACM Trans. Sens. Netw.* 2006, 2, 221–262.

31. Zanella, A. Best Practice in RSS Measurements and Ranging. *IEEE Commun. Surv. Tutor.* 2016, 18, 2662–2686.