RESEARCH ARTICLE

Thwarting location privacy protection in location-based social discovery services

Minhui Xue¹³, Yong Liu², Keith W. Ross²³ and Haifeng Qian¹ *

¹ East China Normal University, Shanghai, 200241, China
² New York University, NY 11201, U.S.A.
³ NYU Shanghai, Shanghai, 200122, China

ABSTRACT

Location-based social discovery (LBSD) services enable users to discover their geographic neighborhoods to make new friends. Original LBSD services were designed to provide the exact distances to nearby users. It has been shown that it is easy to pinpoint any target user’s location by using trilateration based on the exact distances from three fake Global Positioning System locations to the target user. To defend against the trilateration attack, contemporary LBSD services then began to report distances of nearby users in concentric bands, for example, bands of 100 meters, rather than exact distances. In this paper, we investigate the user location privacy leakage problem in LBSD services reporting distances in discrete bands. Using number theory, we analytically show that by strategically placing multiple virtual probes with fake Global Positioning System locations, one can nevertheless localize user locations in band-based LBSD. Our methodology is guaranteed to localize any reported user within a circle of radius no greater than one meter, even for LBSD services using large bands (such as 100 m as used by WeChat). Eventually, countermeasures are proposed to reduce location privacy leakage to the very minimum. To the best of our knowledge, this is the first work that explicitly exploits and quantifies user location privacy leakage in band-based LBSD services. We expect our study to draw more public attention to this serious privacy issue and expectantly motivate better privacy preserving LBSD designs. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS
location-based social discovery (LBSD); location privacy; number theory

*Correspondence
Haifeng Qian, East China Normal University, Shanghai, 200241, China.
E-mail: hfqian@cs.ecnu.edu.cn

1. INTRODUCTION

The skyrocketing growth of location-based social networks (LBSNs) has gained billions of users driven by the wide proliferation of both smartphone technology and ubiquitous location-based services. A popular location-based service, named as location-based social discovery (LBSD) services, provides a smartphone user a list of nearby people (not necessarily friends) along with some measure of how far away they are from the user. The smartphone user can then exchange messages with the discovered nearby users, thereby attempting to make new friends and possibly meeting up with them. There has been a plethora of prevalent LBSD applications including WeChat, Tinder, and Yik Yak, and so on. WeChat†—which provides other services in addition to LBSD—boasts more than 600 million users and is currently used by essentially all smartphone users in China on a daily basis. As one of the fastest-growing dating application in the United States, Tinder‡ is soon approaching 50 million active users who log into the application 11 times a day on average. Yik Yak creates an anonymous social network experience and enjoys enormous popularity on US college and university campuses [1].

In order to protect users’ privacy, these LBSD services generally do not report the exact longitude and latitude locations of the nearby users. In the first generation, they instead report to the smartphone user exactly how far away each nearby user is. For example, suppose Alice is a smartphone user and runs the LBSD application. The first
generation applications would report to Alice information like ‘Bob is 176 meters away and Clark is 227 meters away’. This information would not provide Bob’s and Clark’s exact locations but instead locate them on circles centered at Alice’s current location and with radius of 176 and 227 meters, respectively. Unfortunately, as we will review in Section 2, it has been shown that it is easy to pinpoint any reported user’s location by using trilateration based on the exact distances from three fake Global Positioning System (GPS) locations to the reported user. (Fake GPS is an App that lets any smartphone user—such as Alice—to configure her longitude and latitude locations to any place in the world.) Recent work has demonstrated trilateration attacks against services with exact distances [2].

To defend against the trilateration attack, contemporary LBSD services then began to report distances of nearby users in concentric bands, for example, they might say ‘Bob is between 100 and 200 meters away, and Clark is within 200 and 300 meters away’. This would put Bob in a large circular band with area of \( \pi 200^2 - \pi 100^2 \) square meters and Clark in an even larger circular band with area of \( \pi 300^2 - \pi 200^2 \) square meters. By reporting distances in bands, one can no longer directly apply trilateration to pinpoint the locations of the discovered users. WeChat, for example, currently uses this concentric band approach when reporting distances. This band-based approach therefore seemingly protects users’ privacy to a much greater extent.

We show, nevertheless, that by using fake GPS to carefully place multiple virtual probes, we can still pinpoint the discovered users’ locations, even when band-based privacy protection mechanisms are used. In this work, we adopt a generic approach to prove our methodology is guaranteed to pinpoint any reported user within a circle of radius no greater than one meter, even for LBSD services using large bands (such as 100 m used by WeChat). The attack not only can target a specific individual but also can be launched from any geographical location (such as Washington D.C.), to monitor all users in any other target geographical region (e.g., Beijing). Obviously, if a weak adversary can monitor a region in a city, then so can a stronger adversary such as a government intelligence agency. We emphasize, however, that a person can only be discovered if he actively uses LBSD service. For example, if a WeChat user only uses WeChat for messaging friends and posting photos, and never uses WeChat’s LBSD service, then the user is not vulnerable to the attack described in this paper. And a user’s mobility is only traceable if the user repeatedly uses the LBSD service (e.g., repeatedly querying ‘People Nearby’ in WeChat).

In this paper, we first consider a one-dimensional (1-D) version of the problem. We employ the number theory to prove that under some easily satisfiable conditions, we can locate a reported user within a half meter. We then extend the methodology to the two-dimensional (2-D) setting by placing virtual probes as a lattice of equidistant points (honeycomb). Our approach combines the distances observed by several probes to locate the target user within a circle of radius no greater than one meter. Therefore, we can use such information to pinpoint the users, and even identify their mobility patterns if they repeatedly use the LBSD service. Our analysis therefore shows that current band-based LBSD services fail to protect users’ location privacy.

The rest of the paper is organized as follows. In Section 2, we present the problem statement. In Section 3, we formalize the 1-D adversarial model and present the algorithms for identifying the locations of users. We then proceed to present the main algorithm for 2-D case in Section 4. Section 5 shows the architecture for our adversarial models and generalizes the hypothesis. Section 6 analyzes the computational complexity and proposes the countermeasures. Section 7 surveys related work. Finally, Section 8 concludes the paper.

2. PROBLEM STATEMENT

In this section, we first overview the state-of-the-art of LBSD services and summarize the trilateration attack when LBSD services report the exact location. We then define the problem when LBSD services use band-based distances. Finally, we introduce some preliminary notation.

2.1. LBSD services and the trilateration attack

LBSD applications enable a user to find nearby users. In the example of WeChat, which has attracted 600 million users globally because the service was released in January 2011, it provides a ‘People Nearby’ LBSD service, which reads in the current geolocation of the mobile device and returns a list of other WeChat users in geographical proximity, establishing on-the-spot connection among nearby users. One option is to report the exact distance to the nearby users. With Tinder, as with all LBSD services that report exact distances, they are vulnerable to the so-called Trilateration Attack.

In Euclidean geometry, trilateration is the process of determining relative locations of points by measurement of exact distances, using the geometry of circles. To perform the attack, when a target user is known to lie on three circles from known locations, then the centers of the three circles with their exact radii provide sufficient information to pinpoint the location of the target user [3]. One example of trilateration attack is illustrated in Figure 1.

To defend against the trilateration attack, contemporary LBSD applications, such as WeChat, Momo, and Tinder, adopt obfuscation techniques to blur the location information. Specifically, when Alice submits her location to the LBSD server, the server does not provide Bob with

---

<sup>1</sup> https://www.techinasia.com/wechat-monthly-active-users-q2-2015/

<sup>2</sup> http://blog.inclucdesecurity.com/2014/02/how-i-was-able-to-track-location-of-any.html
Thwarting location privacy protection in LBSD services
M. Xue et al.

Figure 1. Trilateration attack.

Figure 2. An example of WeChat obfuscation technique.

her exact location but instead indicates that she is somewhere in a circular band. For example, WeChat reports the relative distance in bands of 100 m. As illustrated in Figure 2, when WeChat shows to Bob that Alice is 500 m away from him, it means that Alice is located in a band centered at Bob’s location with radius \( r \) ranging from 400 to 500 m. We outline the distance report accuracy and coverage of some prevalent LBSD applications in Table I [4].

In general, in this paper, we assume that LBSD applications provide relative distances in bands of \( K \) meters. Then, the relation between the reported relative distance \( \omega_d \) and the actual relative distance \( d \) can be determined as follows:

\[
\omega_d = \left( \left\lceil \frac{d}{K} \right\rceil + 1 \right) \times K
\]

Table I. Location-based social discovery applications.

<table>
<thead>
<tr>
<th>App</th>
<th>Accuracy limit</th>
<th>Coverage limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>WeChat</td>
<td>100 m</td>
<td>1km</td>
</tr>
<tr>
<td>Momo</td>
<td>10 m</td>
<td>N/A</td>
</tr>
<tr>
<td>Tinder</td>
<td>100 feet</td>
<td>N/A</td>
</tr>
<tr>
<td>Skout</td>
<td>0.5 mile</td>
<td>N/A</td>
</tr>
<tr>
<td>Whoshere</td>
<td>100 m</td>
<td>N/A</td>
</tr>
<tr>
<td>Topface</td>
<td>100 m</td>
<td>N/A</td>
</tr>
<tr>
<td>SayHi</td>
<td>10 m</td>
<td>1000 km</td>
</tr>
<tr>
<td>iAround</td>
<td>10 m</td>
<td>N/A</td>
</tr>
<tr>
<td>U +</td>
<td>10 m</td>
<td>N/A</td>
</tr>
<tr>
<td>LOVOO</td>
<td>100 m</td>
<td>27.8 km</td>
</tr>
<tr>
<td>KTalk</td>
<td>10 m</td>
<td>N/A</td>
</tr>
</tbody>
</table>

2.2. Adversary model

The simple trilateration attack no longer works when LBSD uses band distances. In this paper, we develop a new location privacy attack for LBSD applications that report band distances. In the adversary model, an attacker places multiple virtual probes in an arbitrary remote geographical region (for example, attacker in New York but probes in Shanghai), which can be easily carried out with fake GPS locations. Each virtual probe collects nearby LBSD users with the corresponding relative distance bands to the probe. While virtual probes can be deployed in arbitrary locations, we assume that virtual probes are positioned to form a lattice of equidistant points. The attacker then attempts to pinpoint the target user in the lattice by using relative band
distances provided by virtual probes, using the methodology developed in this paper. We analytically show that by ‘strategically’ placing multiple virtual probes with fake GPS locations, a target user’s location can be determined to an area within a circle of radius no greater than one meter. More concisely, we consider

- a geographical region as a lattice of equidistant virtual probes, the distance between one probe and any adjacent probe is \( x \);
- each probe reports the relative distance to the target user in bands of \( K \) (For example, if \( K = 100 \) m, a probe reports a target user is between 400 and 500 m away.);
- \( x \) is chosen to be relatively prime to \( K \), where \( x \) and \( K \) are positive integers (i.e., \( \gcd(x, K) = 1 \) which is defined in Section 2.3).

The lattice is illustrated in Figure 3.

### 2.3. Preliminary number theory

In this section, we introduce some basic notation and the definition from number theory.

**Division:** Consider two integers \( a, b \in \mathbb{Z} = \{ \ldots, -1, 0, 1, 2, \ldots \} \), we say that \( b \) divides \( a \) if there exists \( a \in \mathbb{Z} \), such that \( ab = c \), and write \( b \mid a \).

**Common divisor:** For \( a, b \in \mathbb{Z} \), we call \( d \) a common divisor of \( a \) and \( b \) if \( d \mid a \) and \( d \mid b \); moreover, we call such a \( d \) a **greatest common divisor** of \( a \) and \( b \) if \( d \) is non-negative and all other common divisors of \( a \) and \( b \) divide \( d \), and write \( \gcd(a, b) = d \).

**Congruence:** For a positive integer \( n \) and for \( a, b \in \mathbb{Z} \), we say that \( a \) is congruent to \( b \) modulo \( n \) if \( n \mid (a - b) \), and write \( a \equiv b \pmod{n} \).

**Definition 2.1.** For any given pair \( x, K \in \mathbb{Z} \) with \( \gcd(x, K) = 1 \), we define function \( f^K_x(N) = N \cdot x(\text{mod}K) \), for all \( N \in \mathbb{Z} \).

**Lemma 2.1.** For any given pair \( x, K \in \mathbb{Z} \) with \( \gcd(x, K) = 1 \), there always exists an \( s \in \mathbb{Z} \) such that \( \gcd(s, K) = 1 \), and \( f^K_x(f^K_s(N)) = N(\text{mod}K) \), for all \( N \in \mathbb{Z} \). Note that function \( f^K_x(\cdot) \) is an inverse function of function \( f^K_s(\cdot) \).

See proof in Appendix A.1.

### Table II. Summary of notation.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( K )</td>
<td>The length of band</td>
</tr>
<tr>
<td>( x )</td>
<td>The distance between one probe and any adjacent probe, satisfying ( \gcd(x, K) = 1 ), where ( x, K \in \mathbb{Z} ) and ( x, K \geq 1 )</td>
</tr>
<tr>
<td>( O )</td>
<td>The target point (the location of the target user)</td>
</tr>
<tr>
<td>( P_i )</td>
<td>The ( i )-th probe, indexed from left to right along a line</td>
</tr>
<tr>
<td>( d_{p_i} )</td>
<td>The actual distance between the probe ( P_i ) and the target point ( O )</td>
</tr>
<tr>
<td>( \omega_{p_i} )</td>
<td>The reported distance between the probe ( P_i ) and the target point ( O )</td>
</tr>
<tr>
<td>( D_{p_i} )</td>
<td>The estimated distance between the probe ( P_i ) and the target point ( O )</td>
</tr>
<tr>
<td>( r_{p_i} )</td>
<td>The remainder of the distance to the probe ( P_i ), i.e., ( r_{p_i} = d_{p_i} \pmod{K} )</td>
</tr>
</tbody>
</table>

### Figure 4. One-dimensional line.

**3. ONE-DIMENSIONAL ADVERSARIAL METHODOLOGY**

In this section, we consider a special 1-D case of the problem. In particular, we try to determine the target user’s location along a line, which is composed of a set of evenly spaced probes. We prove that the accuracy of the prediction of the 1-D case is bounded by half meter.

We summarize the notation introduced throughout this section in Table II.

In the 1-D case, we consider

- a line of equidistant virtual probes, the distance between one probe and any adjacent probe is \( x \); \( x \) is chosen such that \( \gcd(x, K) = 1 \), where \( x, K \in \mathbb{Z} \) and \( x, K \geq 1 \);
- each probe reports the relative distance to the target user in multiples of \( K \) along a line (the actual distance is between \( (n - 1)K \) and \( nK \) for some integer \( n \), where \( 1 \leq n \leq K - 1 \)).

The problem under study is illustrated in Figure 4. All the virtual probes are evenly spaced along a line. As a direct result of Figure 4, we have the following equation

\[
d_{p_i} = d_{p_{i-1}} + x = d_{p_1} + (i - 1) \cdot x, \quad \text{where} \quad i \geq 1 \quad (3.1)
\]

In addition to Equation 3.1, the following two equations are used throughout this paper:

\[
x = \left\lfloor \frac{x}{K} \right\rfloor \times K + r_x, \quad \text{where} \quad 0 \leq r_x < K, r_x \in \mathbb{Z},
\]

\[
\omega_{p_i} = \left( \left\lfloor \frac{d_{p_i}}{K} \right\rfloor + 1 \right) \times K, \quad \text{where} \quad \forall i \in \mathbb{N}
\]
The 1-D algorithm (Algorithm 1) takes as input the distances \( \{ \omega_p \} \) reported by the probes and does the following:

1. Uses the extended Euclidean algorithm to find \( s \) and \( t \) such that \( s \cdot x + t \cdot K = 1 \). (Appendix A.1)
2. Finds the largest \( T (1 \leq T < K - 1) \) such that
   \[
   \frac{\omega_{p_1}}{K} = \frac{\omega_p}{K} + \left\lfloor \frac{f_s^K(T) \cdot x}{K} \right\rfloor
   \]  
   (3.2)
3. The estimated distance from the probe \( P_1 \) to the target point \( O \) is then given by
   \[
   D_{p_1} = \omega_{p_1} - T - \frac{1}{2}
   \]  
   (3.3)

**Theorem 3.1.** For any target user, there always exists a \( 1 \leq T \leq K - 1 \) such that Equation 3.2 holds.

See proof in Appendix A.2.

To find \( T \) in Equation 3.2, one can do iterative search, starting with \( K - 1 \), then moving downward. To reduce the computation time, we further develop a binary search algorithm. On input \( x \), \( \{ \omega_p \} \), Algorithm 1 can be modified as follows:

- Compute \( s \) such that \( s \cdot x + t \cdot K = 1 \) by executing the extended Euclidean algorithm;
- Let \( j = \lfloor \log_2 K \rfloor, T = 2^\lfloor \log_2 K \rfloor \), and \( N = f_s^K(T) + 1 \), and we define
  \[
  \Delta(T) = \begin{cases} 
  1, & \frac{\omega_N}{K} = \frac{\omega_p}{K} + \left\lfloor \frac{f_s^K(T) \cdot x}{K} \right\rfloor \\
  0, & \text{Otherwise.}
  \end{cases}
  \]
- \( \text{CASE A,} \ (\Delta(2^\lfloor \log_2 K \rfloor) = 1) \land \leq (\Delta(2^\lfloor \log_2 K \rfloor) + 2^\lfloor \log_2 K \rfloor - 1) = 0) \):
  - \( j = \lfloor \log_2 K \rfloor - 2, \ T = 2^\lfloor \log_2 K \rfloor + 2^\lfloor \log_2 K \rfloor - 1 \)
  - While \( j \geq 0 \) do:
    1. Compute \( N = f_s^K(T) + 1 \) and \( \delta = \Delta(T) \)
    2. \( T = T + (-1)^{1-\delta} \cdot 2^j \)
    3. \( j = j - 1 \)
    - Return \( \omega_{p_1} - T - \frac{1}{2} \)
- \( \text{CASE B,} \ (\Delta(2^\lfloor \log_2 K \rfloor) + 2^\lfloor \log_2 K \rfloor - 1) = 1) \):
  - \( j = 1, \ T = 2^\lfloor \log_2 K \rfloor + 2^\lfloor \log_2 K \rfloor - 1 \)
  - While \( j \geq 0 \) do

\[ \begin{align*}
\text{(1) Compute } N &= f_s^K(T) + 1 \\
\text{(2) } T &= T + (-1)^{1-\delta} \cdot 2^j \\
\text{(3) } j &= j - 1
\end{align*}\]
- Return \( \omega_{p_1} - T - \frac{1}{2} \)

As a result, we need only \( \mathcal{O}(\lfloor \log_2 K \rfloor) \) points to identify the target point by adopting iterative binary search method. The complexity of simple iterative method and binary search method are later numerically evaluated in Section 6.

Now, we analyze the error bound of estimation returned by our iterative or binary search algorithms.

**Theorem 3.2.** For \( D_{p_1} \) returned by Algorithm 1 in Equation 3.3, we have
\[
|D_{p_1} - d_{p_1}| \leq \frac{1}{2}
\]

Furthermore, if \( d_{p_1} \in \mathbb{Z}^+ \), we can find the exact target point with a slight modification to the algorithm by simply returning \( D_{p_1} = \omega_{p_1} - T - 1 \).

See proof in Appendix A.3.

This suggests that for 1-D case, the estimation error is bounded by half meter, and if the actual distance is an integer, our algorithm can pinpoint the exact location of the target user.

### 4. TWO-DIMENSIONAL ADVERSARIAL METHODOLOGY

In this section, we suppose that the target user \( O' \) is located in a 2-D array, as shown in Figure 3. We consider

- a geographical region as a lattice of equidistant virtual probes, the distance between one probe and any adjacent probe is \( x \);
- each probe reports the relative distance to the target user in bands of \( K \);
- \( x \) is chosen to be relatively prime to \( K \), where \( x \) and \( K \) are positive integers (i.e., \( \gcd(x, K) = 1 \)).
Let $O_1$, $O_2$, and $O_3$ be the projections to the nearest lines for each of three axes. To be specific, we first denote the direction from $O_1$ to $P_1$ as $X_1$, and the direction from $O_1$ to $Q_1$ as $X_2$. As the probe layout is a lattice of equidistant points, when we make a 60 degrees clockwise rotation for both directions $X_1$ and $X_2$, we obtain new directions $Y_1$ and $Y_2$: when we make a 120 degrees clockwise rotation about $O_1$, we obtain new directions $Z_1$ and $Z_2$. We are going to use the probe readings to estimate the positions of $O_1$, $O_2$, and $O_3$ on their respective lines.

**Theorem 4.1.** Suppose we know that $O_1$, $O_2$, and $O_3$ each reside in a given one-meter band on their respective lines, as shown in Figure 5. Then, we can locate the target user $O'$ within a circle of radius no greater than one meter.

**Proof.** By inspecting Figure 5, the proof is immediate. □

In order to automatically determine the target user as stated in Theorem 4.1, we then develop a main algorithm, denoted as **Algorithm 5**. It is constructed by concurrently calling Algorithm 4, as shown later in this section, three times and does the following:

1. Executes Algorithm 4 from directions $X$, $Y$, and $Z$, respectively.
2. Finds the shadow points $O_1$, $O_2$, and $O_3$.
3. Returns the overlapping area containing the target point $O'$.

**4.1. One-dimensional projection**

Our main Theorem 4.1 assumes that we can estimate $O_1$, $O_2$, and $O_3$ on each of its respective lines within one-meter bands. In this section, we will prove that the assumption is correct. Before presenting our 2-D algorithms, we summarize the notation introduced throughout the rest of the paper in Table III. For the determination in this table, see Figure 6.

The problem under study is illustrated in Figure 6. To determine the location of a target user located at position $O'$ on a 2-D plane, we focus on virtual probes along a line close to the target point $O'$ (we can identify those probes by comparing their reported band distances with the target). Without loss of generality, we choose one virtual probe line out of three lines. Let $O_1$ be the projection of $O'$ onto this line, as shown in Figure 6. We also refer $O_1$ as the shadow point. We then name the probes to the left of $O_1$ as $P_1$, $P_2$, ..., $P_N$, and the probes to the right of $O_1$ as $Q_1$, $Q_2$, ..., $Q_N$ (where subscript $N$ is defined in Appendix A.4).

We denote the direction from $O_1$ to $P_N$ as $X_1$, and the direction from $O_1$ to $Q_N$ as $X_2$. Similar to the 1-D case, we assume the distance between two adjacent probes is a constant $x$. We define a problem termed shadow point problem as the problem of finding point $O_1$, the projection of target point $O'$ onto a probe line. Without loss of generality, we can assume $|O_1O'| \leq h$ where $h = \frac{\sqrt{3}}{2}x$. Since $O'$ is close to the line, we determine the shadow point $O_1$ from two opposite directions $X_1$ and $X_2$, respectively. (As above-mentioned subscript $N$ becomes large enough, the reported distance from $O_1$ to the probe $P_1$ is equal to the reported distance from $O'$ to the probe $P_1$. See proof in Appendix A.5.)

The first 2-D algorithm (Algorithm 2) takes as input the distances $\{w_{pi}\}$ reported by the probes from direction $X_1$ and does the following:

1. Uses the extended Euclidean algorithm to find $s$ and $t$ such that $s \cdot x + t \cdot K = 1$.
2. Finds the largest integer $1 \leq T \leq K - 1$ such that
   \[ \frac{w_{p1}}{K} = \frac{w_{p1}}{K} + \left\lfloor \frac{K(T \cdot x)}{K} \right\rfloor + x \cdot \left( \frac{x}{K} + 1 \right) \quad (4.1) \]
3. The estimated distance from the probe $P_1$ to the target point $O'$ is then given by $D_{p1} = w_{p1} - T - \frac{1}{2}$.

In Appendix A.4, we prove that there always exists such a $T$ that satisfies Equation 4.1.

---

**Table III. Summary of notation.**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>$O'$</td>
<td>The target point (the location of the user)</td>
</tr>
<tr>
<td>$O_1$</td>
<td>The first projection of the target point to a line of virtual probes</td>
</tr>
<tr>
<td>$d_{p1}$</td>
<td>The actual distance from $O_1$ to the probe $P_1$</td>
</tr>
<tr>
<td>$d_{q1}$</td>
<td>The actual distance from $O_1$ to the probe $Q_1$</td>
</tr>
<tr>
<td>$D_{p1}$</td>
<td>The estimated distance from $O'$ to the probe $P_1$</td>
</tr>
<tr>
<td>$D_{q1}$</td>
<td>The estimated distance from $O'$ to the probe $Q_1$</td>
</tr>
<tr>
<td>$w_{p1}$</td>
<td>The reported distance from $O'$ to the probe $P_1$</td>
</tr>
<tr>
<td>$w_{q1}$</td>
<td>The reported distance from $O'$ to the probe $Q_1$</td>
</tr>
</tbody>
</table>

---

**Figure 5. Illustration of overlapping area.**
Symmetrically, the Algorithm 3 takes as input the distances \( \{w_{qi}\} \) reported by the probes from direction \( \vec{X}_2 \) and does the following:

1. Uses the extended Euclidean algorithm to find \( s \) and \( t \) such that \( s \cdot x + t \cdot K = 1 \).
2. Finds the largest integer \( 1 \leq \tilde{T} < K - 1 \) such that
   \[
   \frac{w_{QN}}{K} = \frac{w_{qi}}{K} + \left\lfloor \frac{f_k^N(\tilde{T}) \cdot x}{K} \right\rfloor + x \cdot \left( \frac{x}{K} \right) + 1
   \] (4.2)
3. The estimated distance from the probe \( Q_1 \) to target point \( O_0 \) is then given by
   \[
   D_{q1} = w_{q1} - \tilde{T} - \frac{1}{2}.
   \]

### 4.2. Determine the shadow point from two directions

In this section, we show that the explicit algorithm to find the shadow point \( O_1 \) from direction \( \vec{X}_1 \) and direction \( \vec{X}_2 \), which is denoted as Algorithm 4, can be graphically interpreted in Figure 6.

In Algorithm 4, we manually set the shadow point \( O_1 \) as the middle point from two points returned by both Algorithms 2 and 3. As a result, by running Algorithm 4, the shadow point \( O_1 \) can always be pinpointed with an accuracy bounded by one meter.

The Algorithm 4 takes as input the distances \( \{w_{pi}\} \) and \( \{w_{qi}\} \) reported by the probes from two directions \( \vec{X}_1 \) and \( \vec{X}_2 \), respectively, and does the following:

1. Executes both Algorithms 2 and 3.
2. Finds the largest input value of \( T(1 \leq T < K - 1) \) from direction \( \vec{X}_1 \) to \( \tilde{T}(1 \leq \tilde{T} < K - 1) \) from direction \( \vec{X}_2 \) such that the shadow point \( O_1 \) is set by the middle point from two points returned from two-opposite directions.
3. Returns the setting of the shadow point \( O_1 \) on the line segment between \( Q_N \) and \( P_N \).

We run Algorithm 4 from two-opposite directions by executing both Algorithms 2 and 3 in order to ultimately pinpoint the shadow point of the target user. The main result for the shadow point problem is as follows:

**Theorem 4.2.** Suppose the estimated distances from the probe to the target point \( O' \) are given by \( D_{p1} = w_{p1} - \tilde{T} - \frac{1}{2} \).

For clarity, the proof of Theorem 4.2 is directly followed by Lemma A.7, which we spell out the details in Appendix A.5.

Hence, taking all the results together in this section, we can prove that the target user is located within a circle of radius no greater than one meter, as formally stated in Theorem 4.1.

### 5. IMPLEMENTATION DISCUSSION

We show the architecture for our attacking methodology in Figure 7. Adversaries gather relative distance samples from the target user’s smartphone, when the target user uses LBSD applications. The data are processed in real time via our attacking algorithms and stealthily pinpoint the target user.
In Figure 7, the initial $s$ satisfying $s \cdot x + t \cdot K = 1$ is computed via extended Euclidean algorithm, which derives Algorithm 1. Algorithms 2 and 3 are constructed from two-opposite directions $X_1$ and $X_2$ respectively based on Algorithm 1. Algorithm 4 combines both Algorithms 2 and 3 and executes three times from direction $X$, $Y$, and $Z$ respectively, which derives Algorithm 5. Finally, the Algorithm 6 returns the overlapping area containing the target user for tracking or stalking.

In the aforementioned analysis, we assumed that the probe layout satisfies $\gcd(x, K) = 1$. If we generalize the hypothesis and consider

- a geographical region as a lattice of equidistant virtual probes, the distance between one probe and any adjacent probe is $x$;
- each probe reports the relative distance to the target user in bands of $K$;
- $x$ is chosen such that $\gcd(x, K) = \ell$, where $x, \ell, K \in \mathbb{Z}$ and $x, \ell, K \geq 1$.

The corresponding results will be revised as follows.

1. Given $4 \cdot \lceil \log_2 K \rceil$ virtual probes, the target user can be determined in an area bounded by $\left(\frac{2 \sqrt{3}}{3} \cdot \ell^2\right) m^2$;
2. Given $6 \cdot \lceil \log_2 K \rceil$ virtual probes, the target user can be determined in an area bounded by $\left(\frac{2 \sqrt{3}}{2} \cdot \ell^2\right) m^2$.

### 6. PERFORMANCE ANALYSIS AND COUNTERMEASURES

In this section, we first numerically contrast the computational complexity of both binary search method and simple iterative method. We finally show the countermeasures from a technical perspective.

#### 6.1. Computational complexity

We numerically evaluate the performance of two executing algorithms binary search method and simple iterative method in terms of their complexity. Our main goal on performance is to reduce computational cost of the attack as much as possible. For simplicity, we summarize the detailed computational cost in Table IV.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Computational cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary search method</td>
<td>$O(\lceil \log_2 K \rceil)$</td>
</tr>
<tr>
<td>Simple iterative method</td>
<td>$O(K)$</td>
</tr>
</tbody>
</table>

#### 6.2. Countermeasures

Gurevich et al. [5] recently define two different concepts of privacy, namely, an item of your personal information is *private* if you have it but no other party does; it is *inversely private* if some party has it but you do not. Having access to geolocation information that is absolutely in the inverse privacy bucket would allow a person to have a better recommendation by commercial institutions or a better social messaging experience with a swatch of nearby people. Hence, we here incorporate LBSD services into the framework of inverse privacy issue to show that technology can reduce inverse privacy to a minimum.

From a technical perspective, LBSD services appear to add a degree of randomness to the reported users and distances. However, the aforementioned attack cannot simply be mitigated by adding more noise into the system due to the law of large numbers. Adversaries can always apply increasingly sophisticated statistical tools to eliminate noise and pinpoint a user even in the situation that the fake GPS sensors introduce errors. Instead, the key to defense is to restrict user access to extensive distance measurements, limit the rate on queries to the nearby lists, and stop displaying the same user in the nearby lists of multiple requests in the vicinity. Finally, the ultimate defense for LBSDs is to simply remove the ‘relative distance’ field or allow users to configure the service that only the city or the zone the user is currently in is reported. Fortunately, as we later review in Section 7, various other privacy protection mechanisms could also be proposed to enhance the privacy for LBSD services.

### 7. RELATED WORK

The field of location privacy in LBSNs has been examined in recent years. In addition, location verification and location privacy protection in LBSNs are long-standing topics and have received much attention in the past few years.

#### 7.1. Location verification

Narayanan et al. [6] propose location tags for proximity verification protocols. Lin et al. [7] explore the use of GSM cellular networks for creating location tags. While a promising approach, it presents significant practical limitations, as users must be connected to the same base station tower. Marforio et al. [8] propose the use of smartphones in a location verification scheme for sales transactions, which could potentially be employed by proximity services for location verification.

#### 7.2. Location privacy protection

The need to enhance location privacy for LBSNs users is understood, and various solutions have been proposed, falling roughly into three categories: centralized, user-collaborative, and user-centric.
(1) Firstly, centralized approaches protect user privacy in a trustworthy third party system which is used to anonymize or obfuscate queries by hiding any information about the users’ identities [9–11].

(2) Secondly, a user-collaborative approach does not require a third party to be reliable; it instead improves users’ location privacy through collaborative peers in the vicinity keeping their context information in a buffer and passing it to others who need information [12]. Such a scheme ensures the user to remain hidden from the server.

(3) Finally, user-centric approaches operate directly on mobile devices. Typically they aim to develop a general protection mechanism to blur the information by having the user’s smartphone submit vague or noisy GPS coordinates to the location-based server. For example, obfuscation techniques are built according to different design principles. The most popular approach to achieving location privacy is to adopt the spatial-obfuscation or temporal-obfuscation techniques of the users’ real locations [13–16]. Changing user pseudonyms when passing through pre-defined spots, that is, mixzones, enable to hide users’ locations [17,18]. However, users do not communicate with the provider and must keep silent inside the mixzones of which the size is kept small [19]. This mechanism limits the unlinkability of users’ queries and prevents the adversary from tracking the users. Another technique proposed to protect location privacy is to distort the users’ queries by adding some dummy queries, indistinguishable from real requests, camouflaged from the location-based services [20], [21]. Many novel differential privacy protection for location-based system have recently been proposed [11,22–24].

In addition to the three aforementioned privacy protection mechanisms, there also exist some cryptographic approaches that redesign the LBSNs: the service provider can reply to the users’ queries but remain zero-knowledge to them [11]. The lack of incentives for LBSNs operators to implement these methods and high computational overhead reduce the utility and have made them impractical [25].

7.3. Our work

Recent studies show that human mobility traces are highly unique, and four spatio-temporal points are enough to uniquely identify the individuals [26]. By empirically observing the basic scaling laws characterizing human trajectories, a self-consistent microscopic model offers a framework that predicts future human mobility [27]. Even though anonymizing or obfuscating shared location data, target users can still be determined given an obtained social network graph [28,29]. Furthermore, fully implemented Android’s security design and well-protected smartphone applications still can leak user’s location information without any permission [30]. In [31], Mascetti et al. present an attack against users that obfuscate their location with dummy queries; it uses clustering and trilateration, to bound users within an area. The attack only works for users located in large cities, and the bounding area is too large to locate users.

In all the aforementioned mechanisms, very little work exists on LBSDs. To the best of our knowledge, the following three approaches are the closest to ours. Le Blond et al. [32] discuss that a third party is used to track plenty of users’ whereabouts. Li et al. [4] develop a novel automated user location tracking system and test it on leading LBSD applications including WeChat, Skout, and Momo. They demonstrate its effectiveness and efficiency in achieving high-accuracy geo-locating. While Ding et al. [33] develop a generic and automated measurement methodology—combining many off-the-shelf softwares—that can be adapted to any LBSD service without relying on an application programming interface or on reverse engineering. They monitor midtown Manhattan for 7 days and gather location information relevant to 1745 distinct users moving in the targeted geographical region.

However, based on [33], we proceed to quantify its accuracy and develop number theory-based algorithms to accurately pinpoint a target user within one square meter. Our approach is the first work to rigorously formulate the attacking model within the realm of number theory and prove that a victim can be pinpointed in band-based LBSD services.

8. CONCLUSION

To defend against the trilateration attack, contemporary LBSD services have begun to report distances of nearby users in concentric bands. In this paper, we investigate the user location privacy leakage problem in LBSD services reporting distances in concentric bands. Using number theory, we analytically show that by strategically placing multiple virtual probes as pre-determined fake GPS locations, one can nevertheless localize user locations in band-based LBSD. Our methodology is guaranteed to localize any reported user within a circle of radius no greater than one meter, even for LBSD services using large bands. We emphasize, however, that a person can only be discovered if he is a user of the LBSD service. For example, if a WeChat user only uses WeChat for messaging friends and posting photos, and never uses WeChat’s LBSD service, then the user is not locatable by the methods described in this paper. Finally, countermeasures are proposed to mitigate the attack.

To the best of our knowledge, this is the first work that explicitly exploits and quantifies user location privacy leakage in band-based LBSD services. We expect our
study to draw more public attention to this serious privacy issue and confidently motivate better privacy preserving LBSD designs.

Acknowledgements

*This paper is an extended version of [34]. This work was supported in part by the NSF under Grant CNS-1318659. This work was also supported in part by the National Natural Science Foundation of China, under Grant 61571191, in part by the Science and Technology Commission of Shanghai Municipality under Grant 13JC1403502.

REFERENCES


### A. APPENDICES

#### A.1. Preliminary number theory

**Lemma A.1.** For $a, b \in \mathbb{Z}$, there exist $s, t \in \mathbb{Z}$ such that $as + bt = 1$ if and only if $\gcd(a, b) = 1$.

For simplicity, by using extended Euclidean algorithm to compute $s$ and $t$ where $|a| \leq |b|$ and $|b| \leq |a|$, the proof of Lemma A.1 is trivial [35].

**Lemma A.2.** For any $y \in \mathbb{Z}$ such that $1 \leq y \leq K – 1$ and any positive integer $x$ such that $\gcd(x, K) = 1$, there exists $n \in \mathbb{Z}$ where $1 \leq n \leq K – 1$, such that

$$n \cdot x \equiv y \pmod{K}$$

**Proof.** For any positive integer $x$ such that $\gcd(x, K) = 1$, there exist $s, t \in \mathbb{Z}$ such that

$$s \cdot x + t \cdot K = 1$$

(A.1)

Observe $y \cdot s \cdot x + y \cdot t \cdot K = y$. It implies $y \cdot s \cdot x \equiv y \pmod{K}$. Let $n = y \cdot s \pmod{K}$, then we have $n \cdot x \equiv y \pmod{K}$.

**Lemma A.3.** For any $y \in \mathbb{Z}$ such that $1 \leq y \leq K – 1$ and any positive integer $x$ such that $\gcd(x, K) = 1$, there exists a unique $n \in \mathbb{Z}$ where $1 \leq n \leq K – 1$, such that

$$n \cdot x \equiv y \pmod{K}$$

**Proof.** We assume that there exist $1 \leq n < n' \leq K – 1$ such that

$$n \cdot x \equiv y \equiv n' \cdot x \pmod{K}$$

It follows

$$(n' – n) \cdot x \equiv 0 \pmod{K}$$

which implies $K|(n' – n)$ because $\gcd(x, K) = 1$. However, $1 \leq (n' – n) < K$, implies that $K|(n' – n)$ is impossible. Therefore, $n = n'$.

**Proof of Lemma 2.1:**

**Proof.** From Lemmas A.2 and A.3, we can obtain that $f^K_x(N) = N \cdot x \pmod{K}$ is a permutation over $\mathbb{Z}_K$. For $s$ identified in Equation A.1, it is obvious that $\gcd(x, K) = 1$. Similar to $f^K_x(s)$, we can define $f^K_x(N) = N \cdot x \pmod{K}$. Also from Equation A.1, we have $x \cdot s \equiv 1 \pmod{K}$. Then, $f^K_x(f^K_x(N)) = N \cdot x \cdot s \pmod{K} = N \pmod{K}$. In other words, $f^K_x(N)$ is the inversion of $f^K_x(N)$ over $\mathbb{Z}_K$. 

**DOI:** 10.1002/sec
A.2. Proof of Theorem 3.1

Proof. Using consistent notation to declare variables, we observe that

\[ 1 \leq T \leq K - 1, \]
\[ f^K_s(T) = f^K_s(T) = T \mod K \]

To further interpret Equation 3.2, we have

\[ f^K_s(T) \cdot x = \left( \frac{f^K_s(T) \cdot x}{K} \right) \times K + T \]
\[ = \left( T \cdot s - \frac{T \cdot s}{K} \right) \times x \]
\[ = T \cdot s \cdot x - \left( \frac{T \cdot s}{K} \right) \times x \]
\[ \text{Equation A.2} \]
\[ = \frac{T \cdot s \cdot x}{K} \times K + T - \frac{T \cdot s}{K} \times x \]
\[ = \left( \frac{T \cdot s \cdot x}{K} - \frac{T \cdot s}{K} \right) \times x \times K + T \]

Thus, let \( N = f^K_s(T) + 1 \), it follows

\[ \frac{\omega_{p_N}}{K} = \left[ \frac{d_{p_1}}{K} \right] + 1 \]
\[ = \left[ \frac{d_{p_1} + (N - 1) \cdot x}{K} \right] + 1 \]
\[ = \left[ \frac{d_{p_1} + f^K_s(T) \cdot x}{K} \right] + 1 \]
\[ x = \left[ \frac{d_{p_1}}{K} \right] \times K + r_{p_1} + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \times K + T \]
\[ \text{Equation A.3} \]

We then plug Equation A.2 into Equation A.3 and obtain two cases of a single formula A.2 that makes it almost trivial.

If \( r_{p_1} + T < K \), then

\[ \frac{\omega_{p_N}}{K} = \left[ \frac{d_{p_1}}{K} \right] \times K + r_{p_1} + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \times K + T \]
\[ = \left[ \frac{d_{p_1}}{K} \right] + 1 + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \]
\[ = \frac{\omega_{p_1}}{K} + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \]
\[ \text{Equation A.4} \]

otherwise

\[ \frac{\omega_{p_N}}{K} = \left[ \frac{d_{p_1}}{K} \right] \times K + r_{p_1} + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \times K + T \]
\[ = \left[ \frac{d_{p_1}}{K} \right] + 1 + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \]
\[ = \frac{\omega_{p_1}}{K} + \left[ \frac{f^K_s(T) \cdot x}{K} \right] \]
\[ \text{Equation A.5} \]

\[ \square \]

A.3. Proof of Theorem 3.2

Proof. The first step of the presented Algorithm 1 is to find \( T \) such that: \( \Delta(T) = 1 \) and \( \Delta(T + 1) = 0 \), based on Equations A.4 and A.5, it implies that \( 0 < r_{p_1} + T < K \), and \( r_{p_1} + T + 1 \geq K \). Then, we have

\[ K - 1 \leq r_{p_1} + T < K \]
\[ \text{Equation A.6} \]

which indicates that the target point O almost cuts the edge of the band of probe \( p_N \) where \( N = f^K_s(T) + 1 \). Eventually, the algorithm returns

\[ D_{p_1} = \omega_{p_1} - T - \frac{1}{2} \]
\[ = \left[ \frac{d_{p_1}}{K} \right] \times K + K - T - \frac{1}{2} \]
\[ \text{Equation A.7} \]

As the accurate distance from the target point O to probe \( p_1 \) is

\[ d_{p_1} = \left[ \frac{d_{p_1}}{K} \right] \times K + r_{p_1} \]
\[ \text{Equation A.8} \]

we obtain

\[ D_{p_1} - d_{p_1} = K - T - \frac{1}{2} - r_{p_1} \]
\[ \text{Equation A.9} \]

From Equation A.6, we also have

\[ -\frac{1}{2} < D_{p_1} - d_{p_1} \leq \frac{1}{2} \]

Hence, the error of our algorithm earlier is bounded by \( \frac{1}{2} \).

In particular, if \( d_{p_1} \in \mathbb{Z}^+ \), then \( r_{p_1} \in \mathbb{Z}^+ \). From Equation A.6, we have \( r_{p_1} + T = K - 1 \). Because of Equation A.8, we obtain

\[ d_{p_1} = \left[ \frac{d_{p_1}}{K} \right] \times K + r_{p_1} \]
\[ = \frac{d_{p_1}}{K} \times K + K - T - 1 \]
\[ = \omega_{p_1} - T - 1 \]
\[ = D_{p_1} \]
In a word, the target user’s location can be pinpointed with an accuracy bounded by half meter.

\( \square \)

### A.4. Verification of Equation (4.1)

**Proof.** We let

\[
M = \left( \left\lfloor \frac{n}{K} \right\rfloor + 1 \right) \times K, \quad \text{and} \quad N = M + f_s^K(T) + 1
\]

and define

\[
\Delta(T) = \begin{cases} 
1, & \frac{w_{PN}}{K} = \frac{w_{P1}}{K} + \left[ \frac{f_s^K(T) \cdot x}{K} \right] + x \cdot \left( \left\lfloor \frac{x}{K} \right\rfloor + 1 \right) \\
0, & \text{otherwise.}
\end{cases}
\]

Then, we have

\[
\frac{w_{PN}}{K} = \frac{d_{OP}}{K} + 1
\]

\[
= \left[ \frac{d_{P1} + (N - 1) \cdot x}{K} \right] + 1
\]

\[
= \left[ \frac{d_{P1} + f_s^K(T) \cdot x + M \cdot x}{K} \right] + 1
\]

\[
= \left[ \frac{d_{P1} + f_s^K(T) \cdot x}{K} \right] + x \cdot \left( \left\lfloor \frac{x}{K} \right\rfloor + 1 \right) + 1
\]

\[
= \frac{w_{P1}}{K} + \left[ \frac{r_{P1} + T}{K} \right] + \left[ \frac{f_s^K(T) \cdot x}{K} \right] + x \cdot \left( \left\lfloor \frac{x}{K} \right\rfloor + 1 \right) \tag{A.11}
\]

If \( r_{P1} + T < K \), then

\[
\frac{w_{PN}}{K} = \frac{w_{P1}}{K} + \left[ \frac{f_s^K(T) \cdot x}{K} \right] + x \cdot \left( \left\lfloor \frac{x}{K} \right\rfloor + 1 \right) \tag{A.12}
\]

otherwise

\[
\frac{w_{PN}}{K} = \frac{w_{P1}}{K} + \left[ \frac{f_s^K(T) \cdot x}{K} \right] + x \cdot \left( \left\lfloor \frac{x}{K} \right\rfloor + 1 \right) + 1 \tag{A.13}
\]

\( \square \)

### A.5. Proof of Lemmas in Section 4

For simplicity, we only apply the direction \( X_1 \) to the following lemmas, which also hold for the direction \( X_2 \).

**Lemma A.4.** If \( |O'\Omega| \) is bounded, that is, \( |O'\Omega| = h \leq \sqrt{x^2} \), where \( x \in \mathbb{Z}^+ \) and \( \gcd(x, K) = 1 \), then

\[
|D_{Pn} - d_{Pn}| \rightarrow 0, \quad \text{as} \quad n \rightarrow \infty
\]

**Proof.** Because \( O \) is the projection of \( O' \), it follows

\[
h^2 + d_{Pn}^2 = \frac{D_{Pn}^2}{K} \tag{A.14}
\]

\[
\frac{|D_{Pn} - d_{Pn}| = D_{Pn} - d_{Pn} = \frac{h^2}{D_{Pn} + d_{Pn}} \leq \frac{h^2}{2 \cdot d_{Pn}} \leq \frac{3 \cdot x^2}{8 \cdot d_{Pn}} < \frac{3 \cdot x^2}{(n - 1) \cdot x} < \frac{x}{2(n - 1)}
\]

Therefore, \( |D_{Pn} - d_{Pn}| \rightarrow 0, \quad \text{as} \quad n \rightarrow \infty \).

In particular, as \( n \) becomes large enough, as a direct result of Lemma A.4, the reported distance from \( O_1 \) to the probe \( P_1 \) is equal to the reported distance from \( O' \) to the probe \( P_1 \).

\( \square \)

**Corollary A.5.** If \( n \geq x + 1 \), then

\[
d_{Pn} < D_{Pn} < d_{Pn} + \frac{1}{2} \tag{A.16}
\]

**Lemma A.6.** If \( n \geq x + 1 \), and \( 0 \leq d_{P1} - |d_{P1}| \leq \frac{1}{2} \), then the following holds:

\[
\left[ \frac{D_{Pn}}{K} \right] = \left[ \frac{d_{Pn}}{K} \right] \tag{A.17}
\]

**Proof.** If \( n \geq x + 1 \), then \( d_{Pn} < D_{Pn} < d_{Pn} + \frac{1}{2} \). Because

\[
d_{P1} = d_{P1} + (i - 1) \cdot x, \quad \forall i \geq 1
\]

it follows

\[
0 \leq d_{P1} - |d_{P1}| \leq \frac{1}{2}
\]

We conclude by

\[
d_{Pn} < D_{Pn} < d_{Pn} + \frac{1}{2} \leq \left[ \frac{d_{Pn}}{K} \right] + \frac{1}{2} + \frac{1}{2} = \left[ \frac{d_{Pn}}{K} \right] + 1
\]

Therefore, we obtain

\[
\left[ \frac{d_{Pn}}{K} \right] = \left[ \frac{D_{Pn}}{K} \right]
\]

which implies

\[
\left[ \frac{D_{Pn}}{K} \right] = \left[ \frac{d_{Pn}}{K} \right] \tag{A.18}
\]

\( \square \)

For any \( 1 \leq T \leq K - 1 \), let \( N' = f_s^K(T) + 1 \). We have

\[
d_{Pn'} = d_{Pn'}(f_s^K(T + 1)), \quad D_{Pn'} = D_{Pn'}(f_s^K(T + 1))
\]

Then, we have the following lemma.

**Lemma A.7.** There exists \( T_0 \), where \( 1 \leq T_0 \leq K - 1 \), such that for any \( 1 \leq T \leq K - 1 \), and \( T \neq T_0 \), we have

\[
\left[ \frac{d_{Pn'}(f_s^K(T + 1))}{K} \right] = \left[ \frac{D_{Pn'}(f_s^K(T + 1))}{K} \right]
\]

**Remark A.8.** In fact, Lemma A.7 is directly followed by Theorem 4.2.
学霸图书馆

www.xuebalib.com

本文献由“学霸图书馆-文献云下载”收集自网络，仅供学习交流使用。

学霸图书馆（www.xuebalib.com）是一个“整合众多图书馆数据库资源，提供一站式文献检索和下载服务”的24小时在线不限IP图书馆。

图书馆致力于便利、促进学习与科研，提供最强文献下载服务。

图书馆导航：

图书馆首页 文献云下载 图书馆入口 外文数据库大全 疑难文献辅助工具