Attacks and Defenses in Location-Based Social Networks: A Heuristic Number Theory Approach

Jiawen Peng*, Yan Meng*, Minhui Xue†§, Xiaojun Hei*, Keith W. Ross‡§
*Huazhong University of Science and Technology, Wuhan, 430074, China
†East China Normal University, Shanghai, 200241, China
‡New York University, NY, 11201, USA
§NYU Shanghai, Shanghai, 200122, China
Email: {pessis, mengyan, heixj}@hust.edu.cn; {minhuixue, keithwross}@nyu.edu

***Abstract*—The rapid growth of location-based social network (LBSN) applications – such as WeChat, Momo, and Yik Yak – has in essence facilitated the promotion of anonymously sharing instant messages and open discussions. These services breed a unique anonymous atmosphere for users to discover their geographic neighborhoods and then initiate private communications. In this paper, we demonstrate how such location-based features of WeChat can be exploited to determine the user's location with sufficient accuracy in any city from any location in the world. Guided by the number theory, we design and implement two generic localization attack algorithms to track anonymous users' locations that can be potentially adapted to any other LBSN services. We evaluated the performance of the proposed algorithms using Matlab simulation experiments and also deployed real-world experiments for validating our methodology. Our results show that WeChat, and other LBSN services as such, have a potential location privacy leakage problem. Finally, k-anonymity based countermeasures are proposed to mitigate the localization attacks without significantly compromising the quality-of-service of LBSN applications. We expect our research to bring this serious privacy pertinent issue into the spotlight and hopefully motivate better privacy-preserving LBSN designs.**

I. Introduction

The pervasive utilization of smart phones has drawn billions of users and spawned the development of many popular location-based services (LBSs). In order to obtain a user's geographical location of a mobile-user's device, LBS is accessible through mobile wireless networks (such as cellular networks and WiFi networks) with external means for positioning (such as GPS). An important subcategory of LBSs, namely location-based social network (LBSN) services, provide a unique function and breed an anonymous atmosphere for users to discover their geographic neighborhoods along with some distance measure of how far away they are from the user and then initiate private communications. A mobile user can then connect with new discovered strangers and possibly intends to find potential candidates for dating, which in principle facilitates the promotion of anonymously sharing instant messages and open discussions. Location-based social network applications have enormously become popular worldwide – applications that help to find nearby friends (e.g., WeChat); applications that help to recommend nearby restaurants and points of interest (e.g., Yelp); applications that help to find potential nearby candidates for dating (e.g., Momo); and applications that create an anonymous social network experience for college students (e.g., Yik Yak [1]). For these services to function properly, the integrity of user location privacy must be preserved.

Among all the aforementioned applications, we focus our study on WeChat, a popular online social network application with over 600 million registered users. WeChat has become the largest user group that provides an instant messaging service for intelligent terminals in Asia. It supports inter-communications operators and cross-operating system through the network to send free messages including video, pictures, and texts. WeChat also provides LBSN services by sharing instant data such as *"Shake", "Drift Bottles", "Circle of Friends", and "People Nearby"*. These location-based features facilitate WeChat to breed controversial discussions [2] – such as political rumors, fake news, materialistic and ostentatious messages – that are relatively closed, relationship and geographic based.

In this paper, we attempt to show how the location-based features of WeChat can be exploited to determine the user's location with sufficient accuracy in any city from any location in the world. The basic idea of this localization attack is to use multiple fake GPS, scattered in a target area, to probe for the geo-locations of the probing user accounts, and then predict the location of the target user by leveraging multiple band-based relative distance readings corresponding to each probe. To repel the WeChat rumors discussed previously, our localization attack experiments demonstrate the possibility to determine the location of the source of rumors and safeguard national security.

To achieve the above goal, we utilized an Android emulator, BlueStacks, to simulate multiple Android devices. Within each emulator we ran a WeChat application. The emulator enables us to probe at each location by faking the phone's GPS coordinates. We conducted our real-world experiments to validate our methodology in the field. Guided by the number theory, we propose two generic localization attack algorithms, named as the fundamental algorithm and the two-dimensional algorithm, which can be potentially adapted to any other LBSN services. By demonstrating its efficacy of the algorithms via simulation and the real-world experiments, we show that by strategically placing multiple virtual probes and running these two algorithms, one can nevertheless localize

978-1-4673-8420-9/15 $31.00 © 2015 IEEE
DOI 10.1109/SocialSec2015.19

user locations with high accuracy. Our results demonstrate that WeChat, and other LBSN services as such, have a potential privacy leakage problem. By knowing the exact location of the users, other side knowledge – neighborhood distribution, places of employment, and personal living habits – may help narrow down to identify specific users. Finally, we develop a k-anonymity-based cloaking algorithm that provides location for mobile users to mitigate the localization attacks. These users, called "cloak users", replaced with dummy identifiers in a given area, notably obfuscate the accuracy of attacks. Our experiments show that the location k-anonymity model achieves promisingly high resilience to location privacy threats without significantly compromising the quality-of-service of LBSN services.

The rest of the paper is organized as follows. In Section II, we formalize the localization attacking problem. In Section III, we present a basic one-dimensional algorithm for determining the locations of users in practice. We then proceed to present the fundamental algorithm for the general two-dimensional case in Section IV. Furthermore, we propose an improved version of the fundamental algorithm in Section V. Section VI analyzes the computational complexity and Section VII reports our real-world experiments. Section VIII proposes the countermeasures and Section IX surveys related work. Finally, we conclude the paper in Section X.

II. Problem Statement

In this section, we first formulate the localization attacking problem when LBSN services use band-based distances for location obfuscation. We then further interpret the model assumptions in the case of WeChat.

A. Location Obfuscation

To defend against the trilateration-based localization attacks, contemporary LBSN applications, such as WeChat, Momo, and Tinder, have adopted various obfuscation techniques to blur the location information. Specifically in WeChat, when Alice submits her location to the LBSN server, the server does not provide Bob with 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. Particularly, when WeChat shows to Bob that Alice is 800 m away from him, it means that Alice is located in a band centered at Bob's location with the radius ranging from 700 m to 800 m. Importantly, we found that the distances displayed in WeChat are not completely accurate. For example, when WeChat shows to Bob that Alice is 800 m away from him, WeChat might display the distance as within 900 m instead of the actual distance within 800 m. This error could be attributed to the GPS error. It may be also possible that WeChat intentionally introduces random distance errors in the server responses to protect user privacy. Or it could simply be the data synchronization issues. In summary, we outline the distance report accuracy and coverage of some prevalent LBSN applications in Table I [3].

Following the methodology of [3], we also assume that LBSN applications provide relative distances in bands of K meters. Then, in the case of WeChat, the relation between the reported relative distance W_d and the actual relative distance d can be computed as follows:

$$W_d = \left(\left\lfloor \frac{d}{K} \right\rfloor + 1 \right) \times K, \tag{1}$$

where

$$K = \begin{cases} 100, & 0 \le d < 1000, \\ 1000, & d \ge 1000. \end{cases} \tag{2}$$

TABLE I
Location-based Social Network Applications

App	Accuracy Limit	Coverage Limit
WeChat	100 m (resp. 1 km)	1 km (resp. >1 km)
Momo	10 m	N/A
Tinder	100 feet	N/A
Skout	0.5 mile	N/A
Whoshere	100 m	N/A
Topface	100 m	N/A
SayHi	10 m	1000 km
iAround	10 m	N/A
U+	10 m	N/A
LOVOO	100 m	27.8 km
KKtalk	10 m	N/A

B. Localization Attack

In this section, we develop a new localization attack for LBSN applications that report band distances. In this localization attack, an attacker places multiple probes in an arbitrary remote geographical region (e.g., Wuhan), which can be easily achieved by configuring smart phones with fake GPS locations. Each probe collects nearby LBSN users with the corresponding relative distance bands to this probe. Without losing much generality, we make the following assumptions:

- A priori estimate that the target user is located in a known squared area of size $1,000\mathrm{m} \cdot 1,000\mathrm{m}$;
- A lattice of equidistant probes are placed in the above geographical square region, and the distance between one probe and any adjacent probe is x;
- A Cartesian coordinate system with its origin placed at the bottom left corner of the aforementioned squared area, measured in unit of 1 m;
- Each probe reports the relative distance to the target user in bands of K (e.g., $K = 100$ m as used by WeChat).

Motivated by the general observation that if two points are farther away from each other, the distance error reported by Wechat is larger. In our simulation experiments, we assume that the random localization error generated by the WeChat system is approximated by a segment-wise exponential distribution. Specifically, the random error ϵ (generated by the WeChat system) follows an exponential distribution with mean λ^{-1}, i.e., $\epsilon \sim \exp(\lambda)$, where the probability density function of an exponential distribution is characterized as follows:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x}, & x \ge 0, \\ 0, & x < 0. \end{cases}$$

For clarity, we replace the notation $\exp(\lambda)$ with $exprnd(\lambda)$, where the function $exprnd(\lambda)$ generates a random number from the exponential distribution $\exp(\lambda^{-1})$ with the mean λ in Matlab, as shown in Equation (3). Note that it is worthwhile

investigating a more accurate location error model based on a measurement study in the field, because such a deep understanding of this random error may be helpful to design effective localization attacks and also the defense mechanisms.

$$\epsilon = \begin{cases} 0, & d \leq 400, \\ exprnd(50), & 400 < d \leq 800, \\ exprnd(100), & 800 < d \leq 1200, \\ exprnd(150), & 1200 < d \leq 1600, \\ exprnd(200), & \text{otherwise.} \end{cases} \tag{3}$$

III. One-dimensional Algorithm

A. Overview

In this section, following the methodology of [3], we attempt to further incorporate the location error generated by WeChat into the one-dimensional (1-D) case of the problem. We then simulate the one-dimensional (1-D) algorithm and evaluate its accuracy using simulation experiments.

TABLE II
Notations for the 1-D algorithm

Symbol	Meaning
K	the length of band
x	the distance between one probe and any adjacent probe
ϵ	the reported location error generated by WeChat
d_i	the actual distance between probe P_i and the target
W_{p_i}	the reported distance between probe P_i and the target
D_{p_1}	the estimated distance between probe P_1 and the target
$OneDim$	one-dimensional localization function
$\mathbb{Z}$	the set of integers
$\gcd(\cdot,\cdot)$	the greatest common divisor

We summarize the notation for the 1-D algorithm in Table II. The inputs of the 1-D algorithm include the distance x, the relative distances $\{W_{p_i}\}_{i=1}^{i=n}$ reported by the probes, and the length of band K, with the following procedure:

1) Use the Extended Euclidean Algorithm to find s and t such that $s \cdot x + t \cdot K = 1$.
2) Find the largest T ($1 \leqslant T \leqslant K-1$) such that

$$\frac{W_{p_N}}{K} = \frac{W_{p_1}}{K} + \left\lfloor \frac{f_s^K(T) \cdot x}{K} \right\rfloor, \tag{4}$$

where $f_s^K(T) = T \cdot s \pmod K$. Note that the random error ϵ has already been incorporated in Equation (4).
3) The estimated distance from the probe P_1 to the target point O is then given by

$$D_{p_1} = W_{p_1} - T - \frac{1}{2}. \tag{5}$$

Algorithm 1: 1-D Algorithm

We eventually denote $D_{p_1} = OneDim(x, \{W_{p_i}\}_{i=1}^{i=n}, K)$.

B. Simulation Results

The simulation results of the 1-D algorithm are shown in Table III. By inspecting Table III, we show that over 90% of the errors are less than 10 m. Therefore, the 1-D algorithm is accurate enough for further research.

TABLE III
Simulation Results of the 1-D Algorithm

Actual Distance (m)	Predicted Distance (m)	Error (m)
728.82	733.50	4.68
85.51	85.50	0.01
851.80	855.50	3.70
108.97	108.50	0.47
113.76	113.50	0.26
435.19	435.50	0.31
49.38	49.50	0.12
499.26	498.50	0.76
616.56	622.50	5.94
370.03	370.50	0.47

IV. Fundamental Algorithm

A. Overview

In this section, we consider a general case that the target user is located in a two-dimensional (2-D) area. Based on the 1-D algorithm, we further propose the fundamental algorithm (FundALG). The basic idea of the FundALG is to place multiple probes around the intersection of two probe lines where the target user is. Since we only have a priori knowledge that the target user is supposed to appear in a known squared area, we study two FundALG variants, namely "FundALG with positioning probes" and "FundALG without positioning probes", as two subcategories of the FundALG. We summarize the notation for the fundamental algorithm in Table IV.

TABLE IV
Notations for the Fundamental Algorithm

Symbol	Meaning
(m,n)	the coordinate of intersection obtained by edge detection
E_r	the coordinate of the first horizontal positioning probe
E_c	the coordinate of the first vertical positioning probe
C_{p_i}	the reported distance of the ith horizontal edge probe
R_{p_i}	the reported distance of the ith vertical edge probe
W_{pm_i}	the reported distance of the ith probe on line m
W_{pn_i}	the reported distance of the ith probe on line n
C_{min}	the minimum reported distance from horizontal edge probes
R_{min}	the minimum reported distance from vertical edge probes
C_{mark}	the first horizontal edge probe with the minimum reported distance
R_{mark}	the first vertical edge probe with the minimum reported distance
top	the ordinate of the top boundary of the target area
$bottom$	the ordinate of the bottom boundary of the target area
$left$	the abscissa of the left boundary of the target area
$right$	the abscissa of the right boundary of the target area
$OneDim$	one-dimensional localization function
$Fundamental$	fundamental localization function with positioning probes

B. Basic Idea

In FundALG, two types of probes are introduced. As shown in Fig. 1, edge probes are placed on the boundary of the target area. As shown in Fig. 2, positioning probes are placed perpendicular to the boundary of the target area. The basic idea of the algorithm is as follows:

1) We first place 41 edge probes along the horizontal edge and 41 edge probes along the vertical edge of the target area, respectively. Then from each probe line we obtain

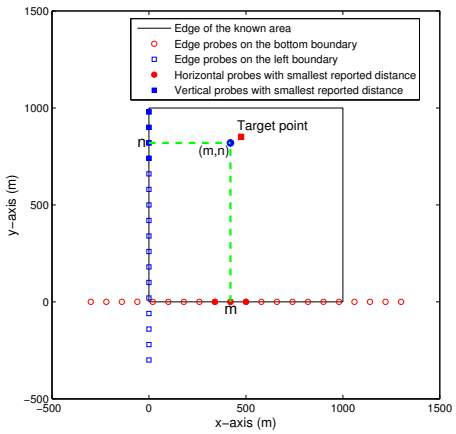

Fig. 1. FundALG without positioning probes: the estimated coordinates of the target are returned by the intersection point of line m and n.

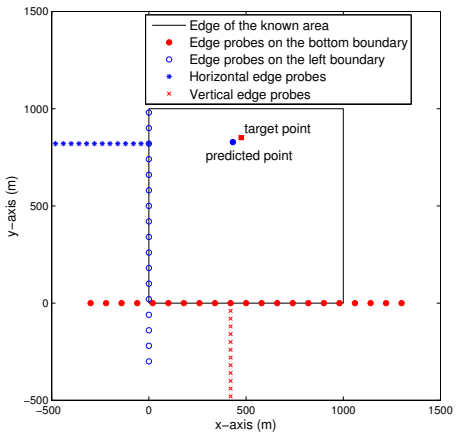

Fig. 2. FundALG with positioning probes: multiple orthogonal positioning probes are placed on two line m and n, respectively. The estimated coordinates of the target are then obtained by executing the 1-D algorithm on each line.

41 reported distances by WeChat, which are denoted as follows:

$$\{C_{p_i}\}_{i=1}^{i=41}, \quad \{R_{p_i}\}_{i=1}^{i=41}.$$

2) Select the minimum reported distances out of 41 horizontal and 41 vertical edge probes, respectively.

$$C_{min} = \min\{C_{p_1}, \ldots, C_{p_{41}}\},$$
$$R_{min} = \min\{R_{p_1}, \ldots, R_{p_{41}}\}.$$

3) Among all the reported distances, we choose the middle probe of which has the minimum horizontal (resp. vertical) reported distances as probe n (resp. m). We attempt to determine the intersection of line m and n that pass through the probes with minimum reported distances. Note that both line m and line n are perpendicular to the boundary of the target area.
4) For FundALG without positioning probes, the intersection of line m and n is returned as the predicted point;
5) For FundALG with positioning probes, we place the first two positioning probes on the boundary of the target area with coordinates $E_r = (0, n)$ and $E_c = (m, 0)$, respectively. After executing the 1-D algorithm on line m and n, respectively, we obtain the estimated coordinates of the target. Finally, we denote the basic idea of the FundALG as follows:

$$Fundamental(C_{p_i}, R_{p_i}, W_{pm_i}, W_{pn_i}, E_r, E_c)$$
$$= (OneDim(x, W_{pm_i}, K), OneDim(x, W_{pm_i}, K))$$

C. Simulation Results

For FundALG without positioning probes, we choose 100 target points to test the overall localization accuracy. As shown in Fig. 3, we observe that except for several estimated points with abnormal errors, 69% of all the target points can be determined within the visual distance (< 60 m).

V. Two-Dimensional Algorithm

In this section, we first show the weakness of the fundamental algorithm when tackling a series of target points with abnormal errors. In order to further improve the localization accuracy, we revise the fundamental algorithm into a so-called two-dimensional (2-D) algorithm.

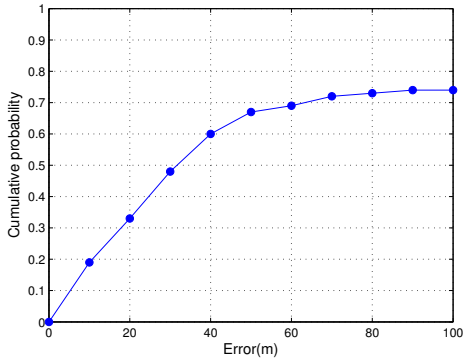

Fig. 3. The cumulation distribution function of the localization errors generated by the FundALG

A. Weakness of the Fundamental Algorithm

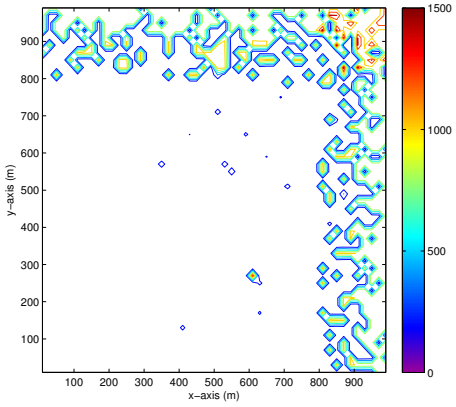

Fig. 4. Distribution of localization errors by FundALG (Contour Map)

In the simulation results of the FundALG proposed in Section IV, 26% of all the errors occurred are excessively larger than 100 m. To visualize this error abnormally, we generate 2,500 target points that are uniformly distributed within the target area. The distance between any two adjacent target points is set as 20 m. The distance between any two

adjacent probes is set as 40 m. We then test the FundALG and obtain the corresponding $2,500$ localization errors by utilizing these $2,500$ uniformly distributed target points.

The contour map of the location errors generated by the FundALG is shown in Fig. 4. The shape of the error values is shown by different contour lines, the relative spacing of the lines indicates the relative error values of the surface. We observe that almost all the abnormal errors occur in the vicinity of the plane $X = 1000, Y = 1000, Z = 0$. When the target point moves close to the two boundary lines, the reported distance may accidentally be modified as 1 km or even 2 km, due to its roundup function as show in Equation 2. Thus, in this case the localization errors may increase dramatically.

B. Partition of the Target Area

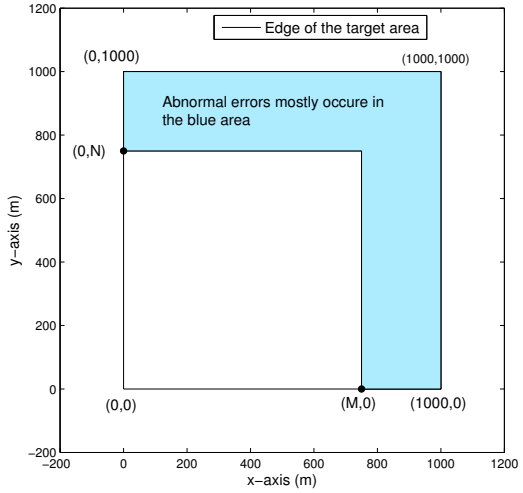

Fig. 5. Partition of the Target Area

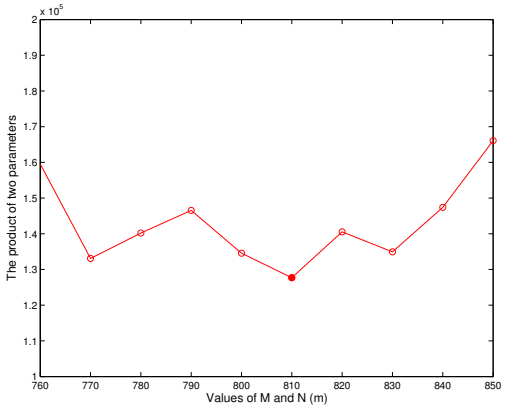

Fig. 6. Performance Indicator w.r.t. M, N

In order to reduce these above-mentioned abnormal errors, we attempt to partition the target area according to the distribution of localization errors as shown in Fig. 5. For the points with abnormal errors occurred in the blue area, we devise the 2-D algorithm (i.e., improved FundALG) to tune the initial positions of the positioning probes to reduce the abnormal errors; for the points occurred in the blank area, we simply call the FundALG. In order to properly determine the optimal values of the partition thresholds M and N, as shown in Fig. 5, and trade off the utility of the 2-D algorithm, we novelly define a performance indicator – the product of the number of points with errors greater than 100 m (in the blank area) and the number of points that need improvement (in the blue area) – to measure the performance of the algorithm. Note that a smaller product indicates a better performance of the algorithm. The performance indicator is shown in Fig. 6, and we conclude that $M = N = 810$ are the optimal values as the partition thresholds.

To sum up, in order to prevent the occurrence of abnormal errors, for the points in the blue area (See Fig. 5), the original location settings of the positioning probes should be initialized in the blank area. We outline the overall 2-D algorithm in Algorithm 2.

Input: $(m, n), M, N$
Output: $P_{predict}$
$top = 1000, bottom = 0, left = 0, right = 1000$
if $m > M$ **then**
  $E_c = (m, 500)$
end
if $n > N$ **then**
  $E_r = (500, n)$
end

$P_{predict} = Fundamental(C_{p_i}, R_{p_i}, W_{pm_i}, W_{pn_i}, E_r, E_c)$

Algorithm 2: 2-D Algorithm

C. Simulation Results

Under the condition of $M = N = 810$, the distribution of the localization errors by the 2-D algorithm occurred in the three-dimensional space is shown in Fig. 7.

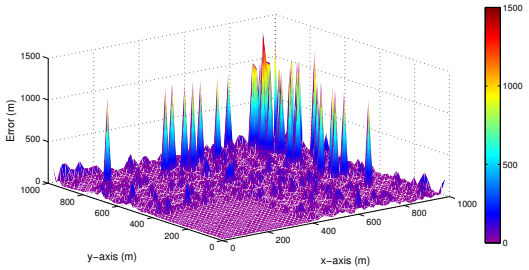

Fig. 7. Distribution of localization errors by the 2-D algorithm (3-D Space)

The contour map of the 2-D algorithm is characterized in Fig. 8. As shown in Fig. 7 and 8, the 2-D algorithm has significantly reduced most abnormal localization errors. We finally show the overall performance of the 2-D algorithm in Fig. 9.

As summarized in Fig. 9, the simulation results show that the abnormal errors occurred in the FundALG can be effectively reduced from 25% to 10% using the 2-D algorithm. 84% out of all the errors are less than 60 m. The 2-D algorithm developed in this section can effectively reduce the abnormal

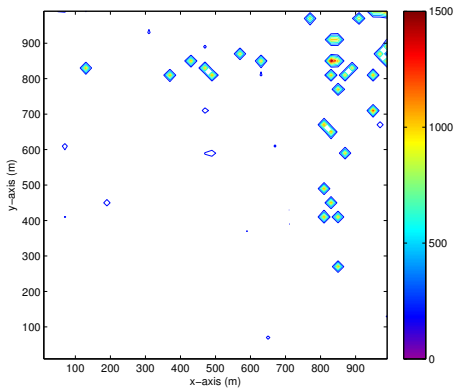

Fig. 8. Distribution of localization errors by the 2-D algorithm (Contour Map)

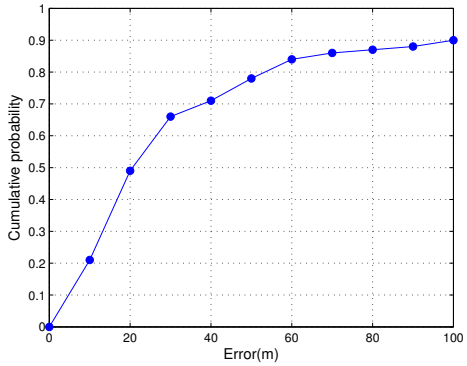

Fig. 9. The cumulation distribution function of the localization errors generated by the 2-D algorithm

errors caused by the FundALG and generally improve its localization accuracy.

VI. Performance Analysis

In this section, we numerically contrast the computational time complexity of different algorithms proposed in this paper. Our main goal on performance is to reduce computational cost of the attacks as much as possible. For simplicity, the time complexity of each algorithm is summarized in Table V.

TABLE V
Time Complexity

Algorithm	Time Complexity
One-dimensional algorithm (1-D algorithm)	$\mathcal{O}(N)$
Fundamental algorithm (FundALG)	$\mathcal{O}(N)$
Two-dimensional algorithm (2-D algorithm)	$\mathcal{O}(N)$

As shown in Table V, all the algorithms proposed in the paper share the same degree of the polynomial-time complexity. In real attack deployments, we estimate that one probe takes roughly 2.5 seconds to detect a target point on average. If only one probe is used, it will take 11.75 minutes for the 2-D algorithm to complete the detection. We can deploy multiple probes in parallel, the detection time may significantly be reduced to several seconds.

VII. Field Test

In this section, we conduct real-world tests to demonstrate the location-tracking performance of the proposed attacking algorithms. We focus on the 2-D algorithm, while the proposed evaluation framework is also applicable for other attacking algorithms because we utilize a smartphone emulator running the WeChat client to mimic user's behaviors without reverse-engineering the WeChat LBSN protocol.

A. Test Setup

We select a geographical area of size 1000 m· 1000 m as our test field, in which various target users are located in this region with known GPS coordinates. Multiple virtual probes are also placed in this area following the requirements of the attacking algorithms. Each probe collects the distance bands of the target user with respect to itself by running the *"People Nearby"* service in WeChat. To facilitate the experiments, we utilize the BlueStacks Android emulator to run the WeChat client, and to run Mock GPS to fake the geographic locations of virtual probes and target users. Fig. 10 shows a typical experiment session setup for the 2-D algorithm, in which the edge probes are placed along the longitude edge and the latitude edge of the test area, and the position probes are also placed following the 2-D algorithm. We randomly placed 10 target users in the test area in total. In order to track one target user in one field test, we deploy 41 edge probes along the longitude edge and 41 edge probes along the latitude edge of the test area. Following the 2-D algorithm, we also deployed 100 position probes along the longitude axis and 100 position probes along the latitude axis. We believe that optimization may exist in reducing the required number of virtual probes worthwhile for further research.

Fig. 10. Field-test setup for the 2-D algorithm

B. Field Results

The detailed experiment procedures can be found in [4]. Table VI tabulates the estimated location of the targets and the corresponding localization errors. All the results show quite

accurate location estimate within the visual distance (< 60 m), which is sufficient for the tracking purpose.

TABLE VI
FIELD TEST RESULTS OF THE 2-D ALGORITHM

Target Point	Predicted Point	Error (m)
(372,519)	(377.5,488.5)	30.99
(382,645)	(388.5,623.5)	22.46
(456,778)	(456.5,779.5)	1.58
(523,871)	(566.5,844.5)	50.94
(820,256)	(822.5,200.5)	55.57
(409,282)	(422.5,288.5)	14.98
(824,867)	(822.5,866.5)	31.54
(266,895)	(288.5,855.5)	45.46
(653,619)	(677.5,602.5)	29.53
(815,377)	(822.5,325.5)	52.04

Note that the 2-D algorithm was motivated and revised based on the fundamental algorithm due to the incurring errors in the edge area. Table VII tabulates the error reduction of the 2-D algorithm with respect to the fundamental algorithm for those target points in the edge area. The average error reduction among these 5 target points are 45.6%, which indicates an effective error reduction of the 2-D algorithm practically.

TABLE VII
ERROR COMPARISON: 2-D VS FUNDALG

Target Point	Error (2-D)	Error (FundALG)	Error Ratio
$(523, 871)$	50.94 m	73.71 m	0.69
$(820, 256)$	55.57 m	96.14 m	0.58
$(824, 867)$	1.58 m	31.54 m	0.05
$(266, 895)$	45.46 m	55.27 m	0.82
$(815, 377)$	52.04 m	89.75 m	0.58

The error ratio is defined as the ratio between the localization error generated by the 2-D algorithm and the one generated by the fundamental algorithm.

VIII. DEFENSES

As shown in previous sections, the localization attacks on the current "*People Nearby*" service in WeChat are quite effective in both simulation and real-world experiments. In this section, we aim to examine the cloaking-based countermeasures to mitigate the localization attacks without significantly compromising the quality-of-service of LBSN services.

A. Basic Idea

As discussed in Section II, in order to protect the privacy of users, contemporary LBSN systems introduce the "distance-of-band" to blur the accurate positions of users. However, the protection is still limited. Section V demonstrates that the proposed 2-D algorithm is still able to track target users within 60 m with high probability (84%) in simulation experiments, and Section VII demonstrates that the proposed 2-D algorithm is still able to track all the 10 target users within 60 m.

Previous research has shown that the k-anonymity algorithms are quite effective to protect the user's privacy against malicious attacks. For example, Gedik and Liu in [5] proposed a k-Nearest Neighbors (k-NN) algorithm to introduce the concept of "cloak users" for protecting location privacy. These cloak users are the nearby users around a target user within a certain area. With a careful algorithm design when LBSN services provide the location information to users by integrating the location information of these cloak users, such a k-anonymity algorithm may raise the bar for the potential localization attacks while the positioning accuracy of the service may still be maintained at a certain high-level.

The basic idea of k-anonymity is simple and straightforward, which is to mix one user with the surrounded users, preserving his/her location privacy in the crowd. Each user can find a "cloak user set", which consists of all the users within a circular area with a predefined radius r. When receiving a "*People Nearby*" request from a user, WeChat randomly selects one out of the "cloak user set" of one neighbor user, and uses the location of this selected cloak user instead of the true location of that neighbor user. Because each cloak user set is close to the corresponding user, the quality-of-service of the "*People Nearby*" service will not deteriorate much. Nevertheless, it is interesting to examine the privacy-preserving performance of such a simple anonymity technique combined with the distance-of-band. Note that this radius r of the cloak user set may provide a control knob to balance the trade-off between the accuracy of a LBSN service and its privacy-preservation capability.

B. Simulation Results

Considering the distance band in WeChat is $K = 100$ m when the distance is within 1 km, we set the cloaking radius $r = 100$ m. We assume that $1,000$ users are randomly distributed in the test area of size $1,000\text{m} \cdot 1,000\text{m}$. We randomly select 100 users in the system as the target users and run the 2-D algorithm to track these users with and without the k-anonymity technique. Table VIII shows the localization errors of the 2-D algorithm with/without the k-anonymity technique. Among these 100 target users, the average localization error magnification with defense and without defense reaches up to 15.7, which indicates an effective location-privacy preservation by the cloaking-based countermeasures.

TABLE VIII
LOCALIZATION ERRORS OF THE 2-D ALGORITHM WITH/WITHOUT THE k-ANONYMITY TECHNIQUE.

Target Point	Without k-anonymity	With k-anonymity	Error Ratio
$(372, 519)$	15.91 m	87.92 m	5.53
$(382, 645)$	12.40 m	195.50 m	17.14
$(456, 778)$	34.88 m	113.28 m	3.25
$(523, 871)$	12.69 m	162.95 m	12.84
$(820, 256)$	1.60 m	89.16 m	55.61
$(409, 282)$	19.17 m	141.13 m	7.36
$(824, 867)$	37.00 m	220.16 m	5.95
$(266, 895)$	3.10 m	139.87 m	45.12
$(653, 619)$	82.97 m	114.01 m	1.37
$(815, 377)$	7.41 m	149.94 m	20.23

The error ratio is defined as the ratio between the localization errors with k-anonymity and the ones without k-anonymity.

We take a close look at the cumulation distribution function of the localization errors generated by the 2-D algorithm with the k-anonymity defense in Fig. 11. We observe that after deploying the simple k-anonymity technique, the localization errors of the 2-D algorithm has been dramatically increased. 86% of the localization errors are larger than 100 meters, which tends to beyond the visual distance. It is worth further

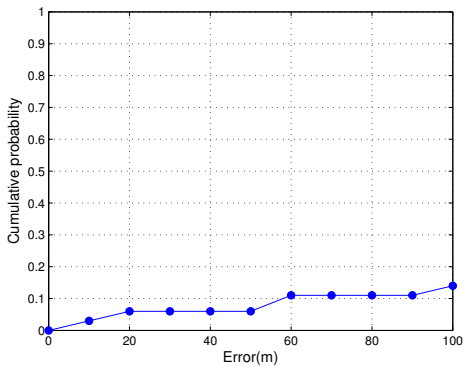

Fig. 11. The cumulation distribution function of the localization errors generated by the 2-D algorithm with the k-anonymity defense.

research how other k-anonymity variants perform against the localization attacks for the LBSN systems with distance-of-band.

IX. Related Work

The privacy of location-based social networks (LBSNs) is a long-standing topic and has been scrutinized in recent years. Many researchers have been trying to infer the exact location and mobility trajectory of any given user using only limited location information using ad-hoc heuristics [6]. Following the methodology of [6], Wang et al. [7] proceeds to quantify the relationship between user mobility and user anonymity by re-developing an automated attacking methodology for tracking WeChat users on the Wall Street. There are many other works that have taken interests in inferring user's trajectory and anonymity [8]–[10]. These works indicate that a large amount of seemingly non-sensitive information may enable an adversary to locate and re-identify potential targets.

Xue et al. [3] theoretically proves that any location-based social discovery user can be located within a circle of radius no greater than one meter using the number theory without considering the possible location errors reported by the LBSN systems. Following the methodology of [3], we consider these possible location errors in practice and proposed practical localization attack algorithms that are able to pinpoint target users with sufficient accuracy in simulations and real-world experiments. Many researchers have been also proposing location k-anonymity schemes for mobile users to defend against the localization attack [11], [12]. In this paper, we apply the k-anonymity method into practice and devise the scheme of "Cloak users" – replaced with dummy identifiers in a given area – in order to obfuscate notably the accuracy of localization attacks.

X. Conclusion

Contemporary LBSN applications have adopted the band-based approach to report distances of nearby users. In this paper, we demonstrated how the location-based feature of WeChat can be exploited to determine the user's location with sufficient accuracy in any city from any location in the world. Guided by the number theory, we designed and implemented two generic algorithms, namely the fundamental algorithm and the two-dimensional algorithm, which can be potentially adapted to any other LBSN services. We evaluated the performance of the proposed algorithms using Matlab simulations and real-world experiments. Our results show that the two-dimensional algorithm achieves better accuracy and shares the same complexity over time with the fundamental algorithm. By using the Android emulator, BlueStacks, to simulate multiple Android devices and the fake GPS application, Mock GPS, to probe for the geo-locations of target users, we show that by strategically placing multiple virtual probes with two algorithms, one can nevertheless localize user locations with sufficient accuracy. Finally, countermeasures are proposed to mitigate the localization attack without significantly compromising the quality-of-service.

Acknowledgements

This work was supported in part by the National Natural Science Foundation of China, under Grant 61370231, in part by the Fundamental Research Funds for the Central Universities under Grant HUST:2014QN156. This work was also supported in part by the Natural Science Foundation, under Grant CNS-1318659.

References

[1] C. L. Nemelka, C. L. Ballard, K. Liu, M. Xue, and K. W. Ross, "You can yak but you can't hide," in *Proceedings of the third edition of the ACM conference on Online social networks*, 2015.

[2] C. H. Wong and O. Geng, "Rumor has it: Tall tales thrive on chinas wechat, researchers say," http://blogs.wsj.com/chinarealtime/2015/06/29/rumor-has-it-tall-tales-thrive-on-chinas-wechat-researchers-say/.

[3] M. Xue, Y. Liu, K. W. Ross, and H. Qian, "I know where you are: thwarting privacy protection in location-based social discovery services," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2015, pp. 179–184.

[4] J. Peng, Y. Meng, M. Xue, and X. Hei, "Attacks and defenses in location-based social networks: A heuristic number theory approach," Huazhong University of Science and Technology, Tech. Rep., 2015. [Online]. Available: http://itec.hust.edu.cn/~heixj/paper/wechat.pdf

[5] B. Gedik and L. Liu, "A customizable k-Anonymity model for protecting location privacy," in *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2004, pp. 620–629.

[6] Y. Ding, S. T. Peddinti, and K. W. Ross, "Stalking Beijing from Timbuktu: A generic measurement approach for exploiting location-based social discovery," in *ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, 2014, pp. 75–80.

[7] R. Wang, M. Xue, K. Liu, and H. Qian, "Data-driven privacy analytics: A wechat case study in location-based social networks," in *Wireless Algorithms, Systems, and Applications*. Springer, 2015, pp. 561–570.

[8] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, 2013.

[9] C. Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, "Privacy vulnerability of published anonymous mobility traces," *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 720–733, 2013.

[10] M. Li, H. Zhu, Z. Gao, S. Chen, L. Yu, S. Hu, and K. Ren, "All your location are belong to us: Breaking mobile social networks for automated user location tracking," in *ACM international symposium on Mobile ad hoc networking and computing*, 2014, pp. 43–52.

[11] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, 2008.

[12] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *IEEE INFOCOM*, 2014, pp. 754–762.