Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

k-Trustee: Location injection attack-resilient anonymization for location privacy

*Lei Jin, Chao Li**, Balaji Palanisamy, James Joshi*

School of Computing and Information, University of Pittsburgh, USA

ARTICLE INFO

Article history:
Received 20 December 2017
Revised 5 June 2018
Accepted 2 July 2018
Available online 10 July 2018

Keywords:
Location privacy attack
Location privacy protection
Trust
k-Anonymity
k-Trustee

ABSTRACT

Cloaking-based location privacy preserving mechanisms have been widely proposed to protect users' location privacy when using location-based services. A fundamental limitation of such mechanisms is that users and their location information in the system are inherently trusted by the Anonymization Server without any verification. In this paper, we show that such an issue could lead to a new class of attacks called location injection attacks which can successfully violate users' in-distinguishability among a set of users. We propose and characterize location injection attacks by presenting a set of attack models and quantifying the costs associated with them. We present and evaluate *k-Trustee*, a trust-aware location cloaking mechanism that is resilient to location injection attacks and guarantees a lower bound on the user's in-distinguishability. *k-Trustee* guarantees that each user in a given cloaked region can achieve the required *k-Anonymity* by including at least *k-1* other trusted users in the cloaked region. We demonstrate the effectiveness of *k-Trustee* through extensive experiments in a real-world geographic map and our experimental results show that the proposed cloaking algorithm guaranteeing *k-Trustee* is effective against various location injection attacks.

1. Introduction

The rapid development of high-speed mobile networks and the growing usage of advanced mobile devices have made location-based services to be indispensable in people's lives. Users' location privacy threats refer to the risks that an attacker can obtain unauthorized access to raw location data by locating a transmitting device and identifying the subject (person) using it. Examples of such risks include spamming users with unwanted advertisements, drawing sensitive inferences from victims' visits to various locations (e.g., clinics and doctors' offices) and learning sensitive information about them (e.g., diseases, religious and political affiliations, etc.). Hence, preserving location privacy is a critical problem.

Various cloaking-based location privacy-preserving mechanisms (CLPMs) have been proposed for protecting users' location privacy from location-based service providers (Bamba et al., 2008; Gruteser and Grunwald, 2003; Mokbel et al., 2006). As shown in Fig. 1, CLPMs are usually implemented through a trusted third party called Anonymization Server (AS) that collects users' location information and performs an anonymization prior to releasing the sensitive location information to location-based service providers (LBSPs), which are assumed to be either curious-but-honest or malicious. In some cases, the location-based service providers (LBSPs) are also vulnerable to insider threats. When a user *u* with a mobile device requests a location-based service (e.g. searching for the nearest coffee shop) from an LBSP, the mobile user first sends the request including his exact location (e.g., longitude and latitude values) to AS. AS then runs a location cloaking

* Corresponding author.
E-mail addresses: lej17@pitt.edu (L. Jin), chl205@pitt.edu (C. Li), bpalan@pitt.edu (B. Palanisamy), jjoshi@pitt.edu (J. Joshi).

https://doi.org/10.1016/j.cose.2018.07.002
0167-4048/© 2018 Elsevier Ltd. All rights reserved.

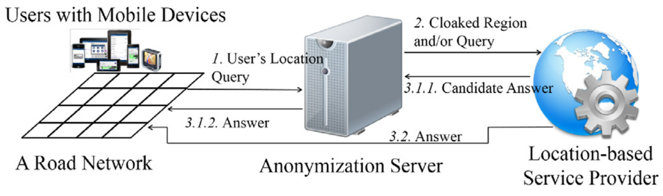

Fig. 1 – Architecture of a cloaking-based location privacy preserving mechanism.

algorithm to reduce the precision of u's location to satisfy the required privacy level (e.g., k-*Anonymity*). After that, AS sends the cloaked region associated with u to the LBSP which finally generates the answer to u's request based on the information from AS. This answer is sent back to u either directly, or through AS as an intermediate tier that delivers the answer to u later.

One way to protect the location privacy of u is to enhance the in-distinguishability of u among a group of users, which is defined as k-*Anonymity* (Bamba et al., 2008; Gruteser and Grunwald, 2003). Specifically, k-*Anonymity* guarantees that the location of a given user is indistinguishable from those of at least $k-1$ other users. In addition to k-*Anonymity*, several extended CLPMs have been proposed, such as POI (*points of interest*) *l-Diversity* (Bamba et al., 2008), which ensures the in-distinguishability of a user's location from a set of POIs, and road segment *s-Diversity* (Wang and Liu, 2009), which guarantees the in-distinguishability of a user's location from a set of road segments. However, one fundamental limitation of these CLPMs is that all users and their location information have to be trusted by AS, which makes the CLPMs vulnerable in practice. Specifically, by exploiting this implicit assumption, an attacker can create fake users with carefully manipulated location information to forcibly reduce the privacy level guaranteed by CLPMs and significantly increase the chance of identifying a targeted user's location. Due to the limitation mentioned above, AS is unaware of the privacy level reduction caused by the injected fake users and therefore no precautionary measure or remedial measure can be implemented. In this paper, we first show that such vulnerability can lead to a new class of attacks called *location injection* attacks, which can successfully compromise privacy of the users' location and trajectory information. After characterizing the location injection attacks, we present various attack models and discuss the cost associated with them. Then, to mitigate the location injection attacks, we further propose a trust based mechanism called k-*Trustee*, which combines trust management with k-anonymity to distinguish fake users (untrusted users) from real users (trusted users) to make it resilient to location injection attacks. The resilience of the proposed k-*Trustee* approach is theoretically analyzed and experimentally evaluated. In summary, the contributions of this paper are as follows:

- We first propose and characterize location injection attacks that can compromise users' privacy setting of k-*Anonymity* in an existing CLPM. We experimentally demonstrate the effectiveness of such attacks through simulations.
- Second, we propose the notion of trust in CLPMs and design a suite of trust-based location cloaking algorithms that can mitigate the impact of location injection attacks.
- Finally, we present the theoretical and experimental analyses of the proposed approaches to demonstrate and validate their effectiveness and resilience against location injection attacks.

The rest of the paper is organized as follows. In Section 2, we review the basic concepts of CLPMs. We then define the notion of location injection attacks in CLPMs and introduce the attack models. In Section 3, we define the concept of trust between users and introduce the notion of k-*Trustee* and design a cloaking algorithm that guarantees the k-*Trustee* property. In Section 4, we demonstrate the effectiveness of location injection attacks and experimentally evaluate the resilience of our proposed cloaking algorithms against location injection attacks. Finally, we summarize the related work in Section 5 and conclude the paper in Section 6.

2. Location injection attacks

In this section, we first model the road network and present the location cloaking techniques based on it. We then propose the location injection attacks and attack models.

2.1. *Road network model*

In various cloaking approaches, users are assumed to travel in a road network (Wang and Liu, 2009) which is modeled as a graph $G(J, S)$, where J represents the set of road junctions and S represents the set of road segments. A junction is defined as the crossover point of any two roads or the end of a road segment. A road segment is defined as the direct road connecting any two adjacent junctions, which may include several point-of-interest (POI) venues. Each segment is uniquely determined by the two junctions associated with it while each junction is associated with one or more adjacent road segments. A road segment s_i that connects two road junctions j_p, j_q can be denoted by $s_i = (j_p, j_q)$. An example road network is shown in Fig. 2 where there are 24 road junctions and 37 road segments.

In particular, for each road segment $s_i = (j_p, j_q)$ in the road network, we define the set of segments sharing either junction j_p or junction j_q with s_i to be the neighbor set of s_i, which is denoted by NS^{s_i}. For example, in Fig. 2, $NS^{s_1} = \{s_2, s_4, s_5\}$. Similarly, given a region R including several road segments, NS^R indicates the neighbor set of R, which consists of segments sharing at least one junction with the segments in R. In Fig. 2, assuming that $R = \{s_1, s_2\}$, we have $NS^R = \{s_3, s_4, s_5, s_6\}$.

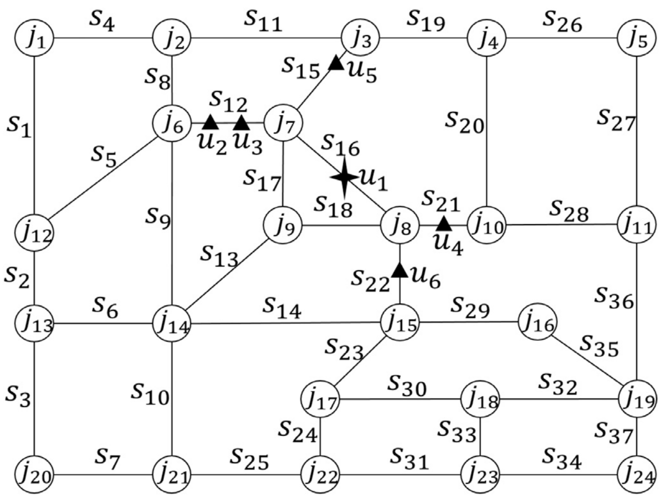

Fig. 2 – A road network example with 24 junctions and 37 road segments.

2.2. *Location cloaking models*

In a road network, the objective of cloaking-based location privacy protection mechanisms (CLPM) is to preserve users' location privacy during their travels in the road network. The fundamental privacy notion behind conventional location cloaking models is *location k-Anonymity* (Gedik and Liu, 2005; Ghinita et al., 2007; Gruteser and Grunwald, 2003), which guarantees the in-distinguishability of a user among a set of users. In other words, a user's location information exposed after the location cloaking process is indistinguishable from that of at least $k-1$ other users. Several extensions have also been proposed to enhance the privacy protection offered by cloaking based solutions, such as POI *l-Diversity* (Bamba et al., 2008) which additionally ensures the in-distinguishability of a user's location from a set of POIs and road segment *s-Diversity* (Wang and Liu, 2009) which additionally guarantees the in-distinguishability of a user's location from a set of road segments. In this paper, we focus on the location cloaking models guaranteeing *k-Anonymity* and/or *s-Diversity*. We present the basic definitions below.

Definition 1. *k-Anonymity* (Gedik and Liu, 2005; Ghinita et al., 2007; Gruteser and Grunwald, 2003). A user *u*'s location is said to satisfy the *k-Anonymity* at time *t*, if there are at least $k-1$ other users present at the same cloaked region at *t*.

Definition 2. *s-Diversity* (Wang and Liu, 2009). A user *u*'s location satisfies *s-Diversity* at time *t*, if there are at least $k-1$ other users at the same cloaked region at *t* and there are at least *s* road segments in the cloaked region.

Note that in this paper we set the atomic element of a cloaked region as a road segment in a road network (Wang and Liu, 2009); *i.e.*, a cloaked region consists of only road segments. For example, in Fig. 2, we assume that there are 6 users, u_1, u_2, u_3, u_4, u_5 and u_6, in the road network. We also assume that both the *k-Anonymity* and the *s-Diversity* requirements are 4 ($k = s = 4$) for u_1 and 3 ($k = s = 3$) for other users. In a CLPM that only guarantees the *k-Anonymity*, the cloaked region for u_1 can be the area consisting of s_{12}, s_{15} and s_{16}. When the *s-Diversity* is supported by a CLPM, the cloaked region for u_1 can be the area composed of s_{12}, s_{15}, s_{16} and s_{17} as it ensures at least 4 segments in the cloaked region.

In the next section, we define the location injection attacks aiming to compromise the location privacy of mobile users, which work by manipulating locations of fake and/or compromised users.[1] We consider a user's location privacy is compromised when an attacker can either identify the road segment where the user is (e.g. find s_{16} from s_{12}, s_{15}, s_{16} for u_1 in Fig. 2) or shrink the cloaked region to a smaller size (e.g. shrink s_{12}, s_{15}, s_{16} to s_{12}, s_{16} for u_1 in Fig. 2), which breaches the user's privacy requirements (*k-Anonymity* and/or *s-Diversity*). We also refer to the violation of a user's trajectory privacy as the case where an attacker can identify a series of consecutive road segments a user visits.

2.3. *Attack definition*

To define the location injection attack, we assume, without loss of generality, that there is a road network G(*J*, *S*), an attacker, a trusted user *u* who travels in G and requests a location-based service from an LBSP through an Anonymization Server (AS). The user *u* has a privacy setting k^u for *k-Anonymity* and AS guarantees the privacy requirement in the generated cloaked region using a cloaking-based location privacy preserving algorithm (e.g., PrivacyGrid Bamba et al., 2008, Casper Mokbel et al., 2006, XStar Wang and Liu, 2009). We also assume that the attacker is the LBSP or a part of the LBSP that tries to compromise *u*'s privacy requirement of k^u, indicating a form of insider attack. The attacker (LBSP) knows the initial cloaked region including *u* before launching the attacks from *u*'s recent location requests sent to the LBSP. Let a fake user be a user that does not physically exist but the attacker

[1] In this paper, a compromised user refers to an authentic user whose location information can be arbitrarily manipulated by an attacker. In the rest of this paper, we simply use the notion of fake users to indicate the set of fake as well as compromised users utilized in location injection attacks.

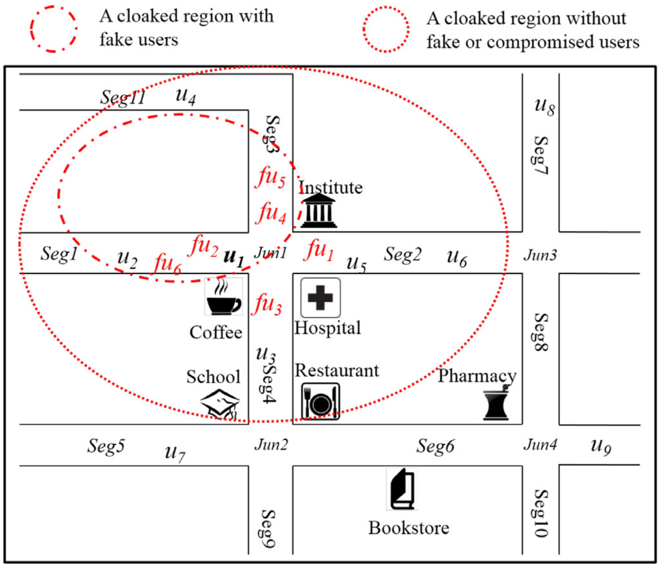

Fig. 3 – An instance of a location injection attack.

has created an account for him in the system, or an authentic user whose location can be manipulated by the attacker.

Adversary's Action: Let u_i be a targeted user. An adversary's attack involves intelligently manipulating a number of fake users' locations using various schemes to identify u_i's location. Let R^{u_i} be the cloaked region created in response to a request from u_i. Let $U(R^{u_i})$ be the set containing all the users including u_i in R^{u_i} and $U_f(R^{u_i})$ be the set of fake users in R^{u_i}.

Location injection attack: We say that u_i is a victim of a location injection attack, when $|U(R^{u_i})| - |U_f(R^{u_i})| < k^{u_i}$. Here $|U|$ indicates the number of users in a user set U.

In a location injection attack, an attacker can distinguish the fake users since these users are either created or controlled by the attacker. As a result, the number of remaining users in the cloaked region, namely $|U(R^{u_i})| - |U_f(R^{u_i})|$, becomes less than the user's privacy requirement of k^{u_i}. When this happens, a user's privacy requirement is compromised. In addition, the size of the cloaked region constructed for u_i or the number of POIs in the cloaked region may also be controlled (e.g., decrease its size) by placing fake users in strategic locations. For example, as shown in Fig. 3, there are six trusted users u_1, u_2, u_3, u_4, u_5 and u_6 traveling in a road network. An attacker can utilize six fake users $fu_1, fu_2, fu_3, fu_4, fu_5$ and fu_6 and report their locations in the road segments around the road junction, $Jun1$. We assume that u_1 has the *k-Anonymity* requirement of $k^{u_1} = 6$ and let the *k-Anonymity* requirements of other users be less than or equal to 6. Without the presence of fake users, AS may generate a cloaked region containing users u_1, u_2, u_3, u_4, u_5 and u_6. The probability of inferring u_1 from that of others in the cloaked region is 1/6. However, when the attacker launches a location injection attack, AS may generate a cloaked region including segments $Seg1$ and $Seg3$ where there are only two authentic users $\{u_1, u_2\}$ and four fake users $\{fu_2, fu_4, fu_5, fu_6\}$. Since the attacker can distinguish fake users in the constructed cloaked region, the probability of identifying u_1 from others is now reduced to 1/2, which compromises u_1's privacy requirement of *k-Anonymity*. Hence, the attacker now has a higher probability of identifying u_1's exact location; *i.e.*, u_1 could be traveling in $Seg1$, $Seg2$, $Seg3$, $Seg4$ or $Seg11$ without the attack but when the location injection attack is launched, u_1 would be associated with either $Seg1$ or $Seg3$.

Note that a location injection attack is successful only when the number of trusted users is less than that required to support a user's *k-Anonymity* requirements. For example, in Fig. 3, if $k^{u_1} = 2$, then u_1's privacy requirement is not violated even under the location injection attack. Detailed analysis of this attack model is provided in Section 3.4. In addition, a location injection attack can be targeted at multiple users simultaneously. It can be also used to infer a targeted user's trajectory when a sequence of location injection attacks for the targeted user are successful.

In our previous work (Jin et al., 2014), we simply defined the location injection attack where attackers can arbitrarily set their locations and thus their trajectories appear suspicious. In addition, we assume that fake users have the lowest *k-Anonymity* requirement supported by AS. This is because an attacker does not expect to trigger the expansion of a cloaked region and aims to induce the CLPM to construct a cloaked region as small as possible. In the next section, we model the location injection attacks.

2.4. *Attack models*

We present the following three different location privacy attacks: *stalking attack*, *fixed-location attack* and *fixed-trajectory attack*. Generally speaking, location privacy attacks involve inferring a relationship between a user and his private location information based on the locations he has visited. Depending on the motive, an adversary may want to find out either '*the locations that have been visited by a targeted user*' or '*the users who have visited a chosen location of interest*'. In the first case, an adversary is more interested in learning private information about the user, so he can launch the stalking attack to continuously stalk the locations of that user and infer private information from collected locations. In the second case, an adversary may target a specific kind of private information (e.g., health information, political inclination) and be more interested in learning about the users associated with this private information. Here, the adversary can launch the fixed-location attack to continuously monitor the users visiting a specific location (e.g., a hospital) or the fixed-trajectory attack using a specific trajectory (e.g., a parade route) to monitor the users following that trajectory. These will help infer the relationship between the users and some private information. The main difference between the fixed-location attack and the fixed-trajectory attack is that in the first case private/sensitive information is implied by a visit to a specific location while in the second case private information is implied by a user's movement along a specific trajectory.

2.4.1. *Stalking attack*

When a location injection attack targets a specific user u, its main purpose is to compromise u's privacy requirement for *k-Anonymity* and identify/infer more accurately his location at a specific time; e.g., the road segment where u is located at time t. When the attacker has obtained a series of more accurate locations of u, he can infer or even identify the detailed trajectory of u. We call such an attack scenario *stalking* attack and we define it as follows.

Assumption. We assume that the attacker is the LBSP or a part of the LBSP that tries to compromise u's privacy requirement of k^u, indicating a form of insider attack. Like many previous work (Gedik and Liu, 2005; Kido et al., 2005; Mokbel et al., 2006), we assume that each LBS query contains a user ID (or pseudonym), so the attacker (LBSP) has the ability to track u's cloaked regions. In addition, we assume that u sends LBS queries with a high frequency, so that the attacker (LBSP) can frequently receive u's cloaked regions and use them to stalk u. Finally, we assume the attacker (LBSP) can generate an arbitrary number of fake users to be located at any segment.

Identifying Initial Road Segment of the Target: To explain the identification of initial position of a user, we assume a user u keeps sending LBS queries (with cloaked regions) to the attacker (LBSP) at $t = -1, 0, 1, 2\ldots$ At $t = -1$, the attacker (LBSP) received u's cloaked region R^u_{-1}, which contains no fake users. Then, between $t = -1$ and $t = 0$, the attacker (LBSP) decides to stalk u. For each road segment in R^u_{-1} and its neighbor set $NS^{R^u_{-1}}$, the attacker places a number of fake users (e.g., the number of fake users deployed to each segment could be equal to the maximum value of k that AS allows a user to declare, so $k \geq k^u$). All these fake users should periodically query the attacker (LBSP) through the anonymization server to be involved in u's future cloaked regions. Later, when $t = 0$, u sends the next LBS query to the attacker (LBSP) through the anonymization server, which will generate the next cloaked region containing u, denoted by R^u_0. We define the segment containing u in R^u_0 as u's initial segment, denoted by s^u_{init}. Since segment s^u_{init} contains k fake users and $k \geq k^u$, R^u_0 will be $\{s^u_{init}\}$, so s^u_{init} can be identified.

Stalking Attack: After s^u_{init} has been identified, the attacker starts to stalk u. Specifically, the attacker makes the fake users move only within $NS^{s^u_{init}}$. Later, when u moves to a new segment from s^u_{init} and queries AS at $t = i$ $(i > 0)$ to generate the cloaked region R^u_i, which is different from R^u_0, the attacker makes the fake users move into R^u_i as soon as possible to identity u's new position s^u_i inside R^u_i. Similarly, when u moves to another segment from s^u_i and queries AS at $t = j$ $(j > i)$ to generate the cloaked region R^u_j, the attacker tries to manipulate the trajectories of the fake users to identity u's new position s^u_j inside R^u_j. By repeating these steps, the attacker can keep stalking u.

Example. We show a comprehensive example of location injection attack in Fig. 4, a part of the road network in Fig. 2. We assume the target user u_1 moves along the trajectory $s_{16} \to s_{12} \to s_9$. We assume u_1 sends three queries to AS at $t = -1, 0, 1$ when it moves along s_{16}, three queries to AS at $t = 2, 3, 4$ when it moves along s_{12} and finally three queries to AS at $t = 5, 6, 7$ when it moves along s_9. We also assume the cloaked region at $t = -1$ is $R^{u_1}_{-1} = \{s_{16}, s_{21}\}$. At time $t = -1$, $R^{u_1}_{-1} = \{s_{16}, s_{21}\}$ is known by the attacker, so the attacker can place 5 fake users at each road segment within $R^{u_1}_{-1}$ and $NS^{R^{u_1}_{-1}}$. Then, at $t = 0$, since $R^{u_1}_0 = \{s_{16}\}$, the initial segment is identified. Please notice that we only show the 5 fake users (fu_1, fu_2, fu_3, fu_4 and fu_5) assigned to segment s_{16} and omit other fake users. After that, to stalk the user u_1, the attacker can dynamically create trajectories for the deployed fake users to make them always run after u_1. That is, given that the cloaked regions of u_1 at time $t = 2$ and $t = 5$ are $R^{u_1}_2 = \{s_8, s_{11}, s_{12}, s_{15}\}$ and $R^{u_1}_5 = \{s_9, s_{13}\}$, respectively, the attacker can control the deployed fakes users to enter the two regions to shrink them to $\{s_{12}\}$ and $\{s_9\}$, respectively, so that the trajectory $s_{16} \to s_{12} \to s_9$ can be disclosed.

2.4.2. *Fixed-location attack*

As another class of location injection attacks, an attacker may cast anchor at a specific location and aim to identify users who visit the targeted location, thus compromising the location privacy of the visitors. That is, instead of stalking a user to incrementally collect his sensitive locations, the attacker can select a fixed sensitive place (e.g., a hospital) and wait for the victims to fall into a snare. An attacker can manipulate the locations of the fake users to the targeted sensitive locations that are close to the targeted location. When users visit the targeted location, users' privacy requirements for the *k-Anonymity* are compromised with a higher probability. This is because the cloaked region has fake users who are controlled by the attacker. The probability of identifying a user is determined by the ratio of real users to fake users. To obtain a probability close to 100%, the adversary should estimate the number of real users and adjust the number of fake users based on that. We call such an attack *fixed-location* attack and it works as follows.

Assumptions. The assumptions are same as the ones presented in Section 2.4.1.

Fixed-location Attack: The attacker places m fake users at the targeted road segment s and makes these fake users stay at s (*e.g.*, visiting POIs at s) during the attack.

Example. In Fig. 4, an attacker targets the road segment s_{16} and tries to identify users who are traveling in s_{16} by injecting fu_1, fu_2, fu_3, fu_4 and fu_5. We assume that a user u_1 is traveling in s_{16} and she has a privacy setting $k^{u_1} = 4$. When u_1 requests a

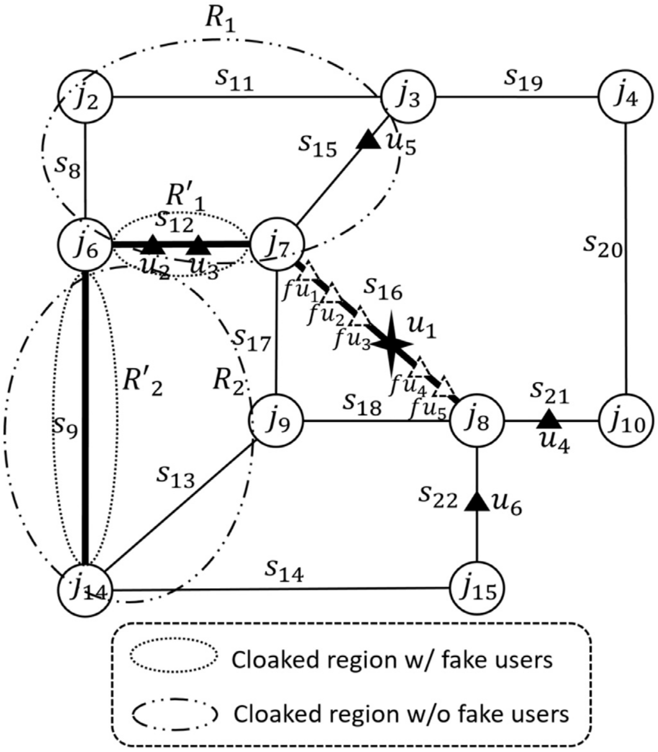

Fig. 4 – An example of the stalking attack. In the example, an adversity keeps using fakes users (fu_1, fu_2, fu_3, fu_4 and fu_5) to stalk the target user u_1 and successfully shrinks the cloaked regions R_1 and R_2 to smaller regions R'_1 and R'_2. Please notice that we only show the 5 fake users (fu_1, fu_2, fu_3, fu_4 and fu_5) assigned to segment s_{16} and omit other fake users assigned to other segments.

location-based service, AS selects s_{16} as a cloaked region such that it satisfies u_1's privacy requirement k^{u_1}. Since there is only u_1 in the cloaked region besides fake users, the attacker can determine u_1 is at s_{16}. Without launching such an attack, the cloaked region constructed for u_1 may consist of s_{12}, s_{15} and s_{16} which includes other three users who are not created by the attacker. In this case, the attacker cannot identify exactly where u_1 is located. It could be s_{12}, s_{15} or s_{16}.

2.4.3. *Fixed-trajectory attack*

In certain situations, an attacker may be interested to identify users who travel at a specific trajectory consisting of a set of connected road segments. We call such an attack *fixed-trajectory* attack and it works as follows. (*e.g.*, $s_{16} \rightarrow s_{12} \rightarrow s_9$ in Fig. 4).

Assumptions. The assumptions are same as the ones presented in Section 2.4.1.

Fixed-trajectory attack. The attacker can first identify the smallest circular region that includes each road segment in the targeted trajectory in the road network. Then, the attacker can simulate the trajectories of fake users continuously traveling in this circle. Note that the attacker has to create an adequate number of fake users at each road segment in the circle continuously in order to best induce AS to construct the cloaked regions that include only one road segment.

Example. In Fig. 4, to identify the users travelling along the trajectory $s_{16} \rightarrow s_{12} \rightarrow s_9$, the attacker can simulate the trajectories of fake users continuously traveling in this circle $s_{16} \rightarrow s_{12} \rightarrow s_9 \rightarrow s_{13} \rightarrow s_{18} \rightarrow s_{16}$.

In summary, we can see that the stalking attack and the fixed-location attack mainly compromise users' location privacy while the fixed-trajectory attack can compromise users' trajectory privacy. In Section 4, we experimentally simulate these three attacks and demonstrate their effectiveness in successfully invading the location privacy of users. Next, we present the ways to mitigate these location injection attacks.

3. Mitigating location injection attacks

In this section, we first discuss potential solutions to defend against location injection attacks. We then introduce various definitions related to trust computations and propose the trust based cloaking-based mechanism against location injection attacks, *k-Trustee*. Notations that will be used in this section are summarized in Table 1.

3.1. *Discussions of potential solutions*

An intuitive approach to defend against location injection attacks is to design a detection mechanism for AS to detect fake

Table 1 – Summary of notations.

Notations	Descriptions
u	Real user.
fu	Fake user.
s	Road segment.
NS^s	Neighbor Set of s.
R_t^u	Cloaked region of u at t.
t; τ	Time point; time duration.
$d_t^u(u_i, u_j)$	Coarse distance between u_i and u_j at t.
$d_t^s(u_i, s_j)$	Coarse distance between u_i and s_j at t.
$\sum_{t\in\tau} cut_t^u(u_i, u_j)$	Coarse-grained user-user trust during τ.
$\sum_{t\in\tau} clt_t^s(u_i, s_j)$	Coarse-grained user-location trust during τ.
$\sum_{t\in\tau} fut_t^u(u_i, u_j)$	Fine-grained user-user trust during τ.
$\sum_{t\in\tau} flt_t^s(u_i, s_j)$	Fine-grained user-location trust during τ.
e^u	e-stalker parameter of u.
f^u	f-stationary parameter u.
(e_l^u, f_l^u)	Local trust parameters of u.
(e_g^u, f_g^u)	Global trust parameters of u.
$U_{lt}^u(t)$	Local trustees of u.
$U_{gt}^u(t)$	Global trustees of u.
$U_T^u(t)$	Trustees of u.
$U_T^u(R_t^u)$	Trustees of u in cloaked region R_t^u.
k^u	k-Anonymity parameter of u.
R_M^u	Maximum acceptable cloaked region size of u.
T_M^u	Maximum acceptable response time of u.
p^u	Privacy parameters of u.
$\overline{U_{lt-e}^u(t)}$	Potential e-stalkers of u.

users. When users are identified as fake by the detection process, their location-based requests can be rejected by AS. Such a detection approach can be based on the characteristics of a user (e.g., IP address) or the user's trajectory (*e.g.*, suspicious or abnormal trajectories). However, it has the following issues:

- It needs a verification process to validate the identified fake users, which incurs additional cost. It is also difficult to design such a process because of users' privacy preferences.
- There will always be false-positives and false-negatives in a detection approach. Trusted users will not be able to request any location-based service when they are identified as false-positives. For example, a trusted user may have a suspicious trajectory around a stadium while trying to find a parking slot (similar to the trajectories of fake users in the fixed-trajectory attack). A detection approach may mistakenly flag the trusted user as a fake user because of her suspicious trajectory. In addition, when the fake users are flagged as false-negatives, they can still be used in location injection attacks.
- It is also very difficult to completely characterize fake users and their suspicious trajectories.

We also note that the encryption-based approaches (Chow and Mokbel, 2007) to encrypt users' information and disconnect their identities with their locations are also feasible approaches to defend against the location injection attack. However, the cost of the encryption and decryption for each request of the location-based service from each user may be high, which makes such an approach less practical.

In this paper, we propose a trust based mitigation approach, named *k-Trustee*, that aims to reduce the impact of the location injection attacks through trust computations. Such a trust based mitigation approach has the following advantages:

- It does not detect nor validate fake users but it will mitigate the impact of suspicious users who could be either trusted users or fake users. Compared with detection approaches where false-positives and/or false-negatives are usually inevitable, the proposed mitigation approach will never forbid real users to request services.
- Users including fake users are always able to request services from AS and LBSPs. However, anonymity service is not free lunch. Users including attackers have to pay for that service. In this case, the attacker has to pay for a cost to conduct location injection attacks irrespective of whether the attacks are successful or not. Such a mechanism can significantly increase the attack cost for the attacker.

3.2. *Trust computations*

In this subsection, we first introduce the computations of the user-user trust and the user-location trust and then apply these trust computations to define *k-Trustee*.

3.2.1. *Trust functions*

The principle behind the computation of trust is that a user u_j is more trusted by another user u_i or a road segment s_i if u_j is always further away from u_i or s_i. When u_j follows u_i (u_j is always close to u_i) or u_j is always traveling around s_i, we say that u_j has a probability to be a fake/compromised user targeting u_i or s_i in the attack. Thus, u_j may not be trusted by u_i or s_i. We first define two types of distances.

Definition 3. *User-User Distance*. Given a road network $G(J, S)$ and two users u_i and u_j, we use $d_t^u(u_i, u_j)$ to represent the coarse distance between u_i and u_j at time t. When u_i and u_j appear together in a same cloaked region R, $d_t^u(u_i, u_j) = 0$. In other cases, $d_t^u(u_i, u_j) = SJ(u_i, u_j)$. Here, $SJ(u_i, u_j)$ is equal to the number of the junctions in the shortest path between the locations of u_i and u_j in a road network.

Definition 4. *User-location distance*. Given a road network $G(J, S)$, a user u_i located at a road segment s_i, and a road segment s_j, we use d_t^s to represent the coarse distance between u_i and s_j at time t. When u_i is in a cloaked region R including s_j, $d_t^s(u_i, s_j) = 0$. Otherwise, $d_t^s(u_i, s_j) = SS(s_i, s_j)$, where $SS(s_i, s_j)$ is equal to the number of junctions in the shortest path between s_i and s_j.

For example, in Fig. 3, $d_t^u(u_1, fu_4) = 0$ since u_1 and fu_4 are in the same cloaked region. $d_t^u(u_1, u_9) = 3$ as there are three junctions in the shortest path between u_1 and u_9. Similarly, $d_t^s(u_1, Seg_3) = 0$ since the cloaked region includes both u_1 and Seg_3; $d_t^s(u_1, Seg_9) = 1$ because there is one junction in the shortest path between u_1 and Seg_9.

Based on the Definitions 3 and 4, we then present two types of user-user trust functions and two types of user-location trust functions. The user-user trust functions present the trust between users while the user-location trust functions indicate the trust values from locations to users.

Definition 5. *Coarse-grained User-User Trust Function*. Given a road network $G(J, S)$, two users u_i and u_j traveling in G and a time interval τ, the coarse-grained user trust between u_i and u_j is $\sum_{t\in\tau} cut_t^u(u_i, u_j)$. Here,

$$cut_t^u(u_i, u_j) = \begin{cases} 1, d_t^u(u_i, u_j) = 0 \\ 0, d_t^u(u_i, u_j) > 0 \end{cases}$$

Definition 6. *Coarse-grained User-Location Trust Function*. Given a road network $G(J, S)$, a user u_i traveling in G, a road segment s_j ($s_j \in J$) and a time interval τ, the coarse-grained location trust function between u_i and s_j is $\sum_{t\in\tau} clt_t^s(u_i, s_j)$. Here,

$$clt_t^s(u_i, s_j) = \begin{cases} 1, d_t^s(u_i, s_j) = 0 \\ 0, d_t^s(u_i, s_j) > 0 \end{cases}$$

Definition 7. *Fine-grained User-User Trust Function*. Given a road network $G(J, S)$, two users u_i and u_j traveling in G and a time interval τ, the fine-grained user trust between u_i and u_j is $\sum_{t\in\tau} fut_t^u(u_i, u_j)$, where

$$fut_t^u(u_i, u_j) = \begin{cases} 1, d_t^u(u_i, u_j) = 0 \\ xd_t^u(u_i, u_j)^{-y}, d_t^u(u_i, u_j) > 0 \end{cases}$$

Here, $x \ge 0, y \ge 0, 0 < xd_t^u(u_i, s_j)^{-y} < 1$.

Definition 8. *Fine-grained User-Location Trust Function*. Given a road network $G(J, S)$, a user u_i traveling in G, and a road segment s_j ($s_j \in J$) and a time interval τ, the coarse-grained location trust function between u_i and s_j is $\sum_{t\in\tau} flt_t^s(u_i, s_j)$, where

$$flt_t^s(u_i, s_j) = \begin{cases} 1, d_t^s(u_i, s_j) = 0 \\ xd_t^s(u_i, s_j)^{-y}, d_t^s(u_i, s_j) > 0 \end{cases}$$

Here, $x \ge 0, y \ge 0, 0 < xd_t^s(u_i, s_j)^{-y} < 1$.

In both Definitions 7 and 8, users outside the cloaked regions are not simply considered to be innocent. Their degree of suspicion can be controlled by adjusting the parameters x and y. Specifically, by choosing a larger x while a smaller y, the user u_i outside the cloaked region containing u_j or s_j obtains higher $fut_t^u(u_i, u_j)$ or $flt_t^s(u_i, s_j)$, thus becoming more suspicious. In contrast, by choosing a smaller x while a larger y, users outside the cloaked regions become less suspicious. In this paper, we set $x = 1$ and $y = 2$, which considers users closer to the cloaked regions to be suspicious but their degree of suspicion is much lower than that of the users inside the cloaked region. Note that the time window τ in the Definitions 5–8 is generally defined by AS. The value is same for all users. An example of such a time window could be 24 hours.

Based on Definitions 5 and 7, when u_i and u_j are included in the same cloaked region or they are close to each other, the values of $\sum_{t\in\tau} cut_t^u(u_i, u_j)$ and $\sum_{t\in\tau} fut_t^u(u_i, u_j)$ are higher. The smaller distance between u_i and u_j also implies that u_i may stalk u_j or vice versa. Hence, the higher values of $\sum_{t\in\tau} cut_t^u(u_i, u_j)$ and $\sum_{t\in\tau} fut_t^u(u_i, u_j)$ refer to the lower trust between u_i and u_j. Similarly, in the Definitions 6 and 8, the higher values of $\sum_{t\in\tau} clt_t^s(u_i, s_j)$ and $\sum_{t\in\tau} flt_t^s(u_i, s_j)$ refer to the smaller distance between u_i and s_j and this suggests the lower trust from s_j to u_i. In addition, compared to the coarse-grained trust functions (Definitions 5 and 6), the fine-grained trust functions (Definitions 7 and 8) are more restricted; users are probably regarded as potential attacker nodes even when they are just a bit close to a target but they are not included in the same cloaked region with the target. Instinctively, these fine-grained trust functions would be more effective to defend against the attacks, and they are more useful for handling the attack scenarios where fake users are placed a bit far away from a target for the attacks. However, the potential issue with the fine-grained trust functions is that they may consider more trusted users as suspicious users than the coarse-grained trust functions. Such an issue may make AS construct a larger size of a cloaked region and it may lower the quality of the location based services for users. We compare these two types of trust functions in Section 4.

Next, based on the above trust functions, we introduce the definitions of the local trust and the global trust which are used to capture the trust values between users and between users and road segments in a more comprehensive way. Based on these, we define the *k-Trustee*.

3.2.2. k-trustee

In order to define the local trust and the global trust, we first define the notions of *e-stalker* and *f-stationary* based on the proposed trust functions.

Definition 9. *e-stalker*. Given a road network $G(J, S)$, two users u_i and u_j traveling in G and a time interval τ, we say that u_j is an *e-stalker* for u_i when $\sum_{t\in\tau} cut_t^u(u_i, u_j) \ge e_l^{u_i}$ or $\sum_{t\in\tau} fut_t^u(u_i, u_j) \ge e_l^{u_i}$. Here, $e_l^{u_i}$ is a parameter defined by u_i indicating his privacy setting for *e-stalker*.

Definition 10. *f-stationary*. Given a road network $G(J, S)$, a user u_i located at a road segment s_i, another user u_j located at a road segment s_j, and a time interval τ, we say that u_j is an *f-stationary* of u_i when $\sum_{t\in\tau} clt_t^s(u_j, s_i) \ge f_l^{u_i}$ or $\sum_{t\in\tau} flt_t^s(u_j, s_i) \ge f_l^{u_i}$. Here, $f_l^{u_i}$ is defined by u_i specifying the privacy setting for *f-stationary*.

From these two definitions, we can see that *e-stalker* characterizes users who may be utilized by an attacker to identify and/or infer a specific user's location while *f-stationary* characterizes users who may be employed by the attacker to identify users who are visiting a specific location. Next, we define the *Local Trust* specifying whether a user trusts another locally.

Definition 11. *Local trust*. Given two users u_i and u_j traveling in a road network $G(J, S)$, a time window τ, u_i's location s_i at time t ($t \in \tau$), and u_i's local trust parameters $e_l^{u_i}$ and $f_l^{u_i}$, we say that u_j is currently a local trusted user of u_i, denoted as $u_j \in U_{lt}^{u_i}(t)$, only when u_j is neither an *e-stalker* nor an *f-stationary* of u_i. That is, $\sum_{t\in\tau} cut_t^u(u_i, u_j) < e_l^{u_i}$ and $\sum_{t\in\tau} clt_t^s(u_j, s_i) < f_l^{u_i}$, or $\sum_{t\in\tau} fut_t^u(u_i, u_j) < e_l^{u_i}$ and $\sum_{t\in\tau} flt_t^s(u_j, s_i) < f_l^{u_i}$.

Fake users used for a particular target can be reused by an attacker to attack a new target; these fake users may be initially trusted by the new target. To limit re-usability of fake users, we present the notion of *global trust* as follows.

Definition 12. *Global Trust*. Given two users u_i and u_j traveling in a road network $G(J, S)$, a time window τ, u_i's location s_i at time t ($t \in \tau$), and u_i's global trust parameters $e_g^{u_i}$ and $f_g^{u_i}$, we say that u_j is globally trusted by u_i, denoted as $u_j \in U_{gt}^{u_i}(t)$, only when there are less than $e_g^{u_i}$ users who regard u_j as the *e-stalker*, and less than $f_g^{u_i}$ users who regard u_j as the *the f-stationary*.

Now, when a fake user has been adopted for attacking enough users and/or road segments in the past, he is unlikely to be globally trusted by many other users. Hence, the re-usability of this fake user for a new target will be restricted.

We define a trusted user of a specific user by considering both local and global trust as follows.

Definition 13. *A Trustee of a Specific User*. Given two users u_i and u_j traveling in a road network $G(J, S)$, a time window τ, u_i's location s_i at time t ($t \in \tau$), u_i's local trust parameters $e_l^{u_i}$ and $f_l^{u_i}$, and u_i's global trust parameters $e_g^{u_i}$ and $f_g^{u_i}$, we say that u_j is a trustee of u_i, denoted as $u_j \in U_T^{u_i}(t)$, only when $u_j \in U_{lt}^{u_i}(t)$ and $u_j \in U_{gt}^{u_i}(t)$.

In the rest of the paper, when we say u_j is trusted by u_i, it will refer to local and global trust. We next present the notion of *k-Trustee* for a user as follows.

Definition 14. *k-Trustee of a User*. Given a road network $G(J, S)$, an Anonymization Server (AS) and a time window τ, a user u_i travels in G while requesting a location-based service. u_i has a privacy setting k^{u_i} for *k-Anonymity* and AS constructs a cloaked region $R_t^{u_i}$ for u_i at time t ($t \in \tau$). $U_T^{u_i}(R_t^{u_i})$ represents the trusted users of u_i in the cloaked region $R_t^{u_i}$ at t. We say that *k-Trustee* is guaranteed for u_i if and only if there are at least k^{u_i} users in $U_T^{u_i}(R_t^{u_i})$; i.e., $\left|U_T^{u_i}(R_t^{u_i})\right| \geq k^{u_i}$.

Note that we assume that u_i always trusts himself (i.e., $u_i \in U_T^{u_i}(R_t^{u_i})$).

The trustees of a specific user u_i are the least likely to be fake users since these users have the lowest probability of either stalking u_i or attacking the location where u_i is currently is. When there are at least k trustees in a cloaked region for user u_i, the probability of distinguishing u_i in the cloaked region is at most $1/k^{u_i}$. Thus, u_i's privacy requirement for *k-Anonymity* is guaranteed. Note that it is possible that fake users may be identified as trustees of a specific user u_i in the initial stages. However, when these fake users continue to stalk u_i or attack road segments including u_i, their trust values with respect to u_i will keep decreasing, as per the proposed definitions. Eventually, they will not become the trustees of u_i any more in the time window τ. In this case, an attacker has to use new fake users to launch the location injection attacks on u_i. In addition, it is also possible that an authentic and not compromised user may not be always identified as a trustee of any user in terms of his trajectory. It is a false-negative but there is no impact for this authentic user to request anonymity service from AS and various location-based services from LBSPs. The only potential issue is that AS may construct a larger cloaked region for the authentic user and hence the quality of the location-based service may decrease.

Based on the definition of *k-Trustee* of a user, we define the notion of *guarantee of k-Trustee* as follows.

Definition 15. *Guarantee of k-Trustee in a Cloaked Region*. Given a cloaked region R and a time instant t, a user set $U(R)$ indicates a set of users in R. We say that *k-Trustee* is guaranteed in R at t if and only if *k-Trustee* is guaranteed for each user in R at t; i.e., $\forall u_i \in U(R)$, $\left|U_T^{u_i}(R_t^{u_i}, t)\right| \geq k^{u_i}$.

Next, we present the cloaking-based location privacy mechanism that guarantees *k-Trustee* in any cloaked region constructed by AS.

3.3. *Cloaking-based location privacy mechanism guaranteeing* k-trustee

Here, we first present the proposed *k-Trustee* cloaking based privacy framework. We then discuss and compare several expansion schemes and finally show the *k-Trustee* cloaking algorithm.

3.3.1. *k-trustee framework*

The key idea of our proposed cloaking-based location privacy framework is to adopt the notion of *k-Trustee* instead of the *k-Anonymity* to enhance a user's location privacy and mitigate the location injection attacks.

In this framework, a user u first needs to specify his privacy requirement as a 7-tuple $p^u(k^u, e_l^u, f_l^u, e_g^u, f_g^u, R_M^u, T_M^u)$. Here, R_M^u denotes the maximum size of a constructed cloaked region accepted by u; and T_M^u indicates the maximum wait time accepted by u for the response for his location request. R_M^u and T_M^u are usually used by u to specify the quality of service. In this paper, R_M^u refers to the maximum number of road segments in a road network. When the number of road segments in the cloaked region is larger than R_M^u, u's location request will be ignored. p^u needs to be sent to AS before the anonymous service is provided.

The process to compute trustees involves the following steps. First, both *e-stalkers* and *f-stationary* values are computed and labeled by the users through cloaked regions previously received from AS within the past time period τ. Specifically, to compute *e-stalkers*, for a user u_j that appeared at least once in these recent cloaked regions, user u_i should count the number of the recent cloaked regions that contains u_j. If the result is not less than $e_l^{u_i}$, u_j will be labeled as a *e-stalker* of u_i by u_i. Similarly, *f-stationary* values can be computed by counting the number of times that other users have appeared in recent cloaked regions and comparing the results with the threshold. Then, to query AS for a cloaked region, u_i should send both *e-stalkers* and *f-stationary* values to AS along with his current location $s_t^{u_i}$ and privacy parameters p^{u_i}. With the knowledge of both *e-stalker* and *f-stationary*, AS can label a user u_j to be locally trusted by another user u_i if u_j is neither an *e-stalker* nor a *f-stationary* of u_i. In addition, with the global knowledge about the number of times that u_j has been labeled as *e-stalker* and/or *f-stationary* by other users, AS can compare the results with parameters $e_g^{u_i}$ and $f_g^{u_i}$ declared by u_i to determine whether u_j can be globally trusted by u_i or not. Finally, if u_j can be both locally and globally trusted by u_i, AS will label u_j to be a trustee of u_i.

An essential issue in this framework is the strategies for expanding a cloaked region where *k-Trustee* is guaranteed for each user. Generally, there are two approaches for expanding the cloaked region (Bamba et al., 2008) in the literature: the *Bottom-Up* cloaking and the *Top-Down* cloaking. The *Bottom-Up* cloaking approach starts the cloaking process by taking a road segment as a candidate cloaked region. If it cannot satisfy users' privacy requirements, the *Bottom-Up* cloaking approach will start the expansion process to enlarge it by including more neighboring road segments till all the users' privacy requirements in the cloaked region are satisfied. On the other hand, the *Top-Down* cloaking approach first selects the entire graph as an initial candidate cloaked region and it aims to partition it to various smaller cloaked regions where none of the users' privacy requirements is violated. In this paper, we focus on the *Bottom-Up* cloaking approach since we feel that it is more straightforward and easier to be utilized in a road network.

3.3.2. *Expansion Schemes*

We proposed the following three cloaked region expansion schemes in the proposed *k-Trustee* framework: *random* expansion, *greedy* expansion and *hybrid* expansion. Note that these are deployed in AS.

Random expansion. Given a cloaked region R, the random expansion approach randomly picks a road segment from the neighbor set NS^R and adds it to R. This process is repeated until the expanded R guarantees the *k-Trustee* requirement for each user in R.

Greedy expansion. The greedy expansion focuses on constructing a smaller size of the cloaked region at each expansion step. Given a cloaked region R, it first computes the neighbor set NS^R when R does not satisfy the *k-Trustee* requirement of each and every user. After that,in each expansion step, it tries to find the best road segment in NS^R that can satisfy the users' privacy requirements as soon as possible. It then adds the road segment to R. It keeps adding the best road segment to R until every user's requirement of *k-Trustee* is guaranteed. Below, we define the approach to identify the best road segment to add at each step, as follows:

Definition 16. *"Best First"*. Given a road network $G(J, S)$ and a cloaked region R where not all users' *k-Trustee* privacy requirements are satisfied, let NS^R be the neighbor set at time t. For each road segment $s_i \in NS^R$, let $p(s_i)$ be a profit function and let $c(s_i)$ be a cost function. $p(s_i)$ denotes the number of pairs of trusted users between a user in s_i and another user in R. It can be calculated as $p(s_i) = \sum Tr(u_i, u_j), u_i \in U(s_i), u_j \in U(R)$, where

$$Tr(u_i, u_j) = \begin{cases} 1/(k^{u_j} - 1), u_i \in U_T^{u_j}(R \cup s_i, t) \\ 0, \textit{otherwise} \end{cases}$$

$c(s_i)$ indicates the number of additional trusted users required for users at s_i when s_i is added to R. $c(s_i)$ can be computed as $c(s_i) = \sum_{u_i \in U(s_i)} \frac{(k^{u_i}-1)-\left|U_T^{u_i}(R \cup s_i)\right|}{k^{u_i}-1}$. We say that s_i is the best road segment to add to R when the value of $p(s_i) - c(s_i)$ is the largest, compared to other road segments in NS^R. When there are more than one best road segments, we randomly pick one of them and add it to R.

Example. We illustrate the working of the above expansion scheme as follows. Fig. 5 shows the steps of a greedy expansion for u_1. fu_1, fu_2 and fu_3 in the figure are fake users. We first assume that every fake user has a very low privacy requirement ($k^{fu_1} = k^{fu_2} = k^{fu_3} = 2$) and trust any other user locally and globally in order to achieve the best attack results. Authentic users (u_i, $i \in [1, 12]$) do not trust these fake users globally but they trust any other authentic user globally; *i.e.*, $U_{gt}^{u_i} = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9, u_{10}, u_{11}, u_{12}\}, i \in [1, 12]$. Authentic users have privacy settings for the *k-Trustee* as: $k^{u_3} = k^{u_4} = k^{u_6} = k^{u_7} = k^{u_9} = k^{u_{10}} = k^{u_{11}} = 3$, $k^{u_1} = k^{u_2} = k^{u_5} = 4$, $k^{u_8} = k^{u_{12}} = 5$. Their current trustees are: $U_{lt}^{u_1} = U_{lt}^{u_9} = U_{lt}^{u_{10}} = \{u_4, u_5, u_6, u_7, u_8\}$, $U_{lt}^{u_2} = \{u_6, u_7, u_{10}\}$, $U_{lt}^{u_3} = \{u_5, u_7, u_{12}\}$, $U_{lt}^{u_4} = \{u_5, u_6\}$, $U_{lt}^{u_5} = \{u_1, u_4, u_6\}$, $U_{lt}^{u_6} = \{u_1, u_4, u_5, u_7, u_9\}$, $U_{lt}^{u_7} = \{u_4, u_6, u_8\}$, $U_{lt}^{u_8} = \{u_1, u_2, u_4, u_5, u_6\}$, $U_{lt}^{u_{11}} = \{u_2, u_5, u_6, u_7, u_8\}$, $U_{lt}^{u_{12}} = \{u_2, u_5, u_6, u_7, u_9\}$.

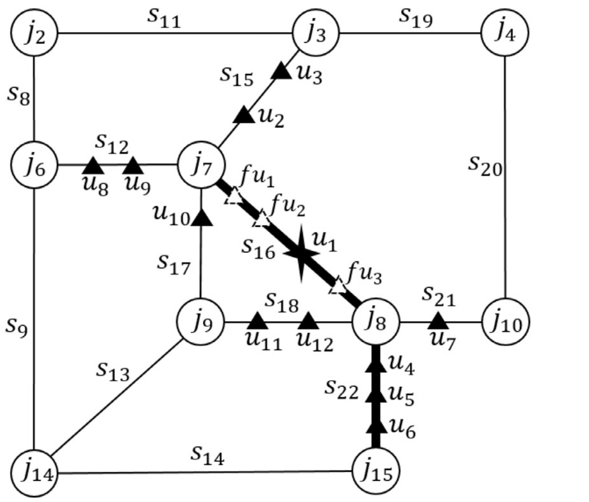

Fig. 5 – An example of the greedy expansion. In this example, u_1 requires a cloaked region that should satisfy $k^{u_1} = 4$. Initially, the candidate cloaked region $R^{u_1} = \{s_{16}\}$ and $NS^{R^{u_1}} = \{s_{12}, s_{15}, s_{17}, s_{18}, s_{21}, s_{22}\}$. To expand the cloaked region to satisfy $k^{u_1} = 4$, the greedy expansion computes the difference between profit and cost when each segment in $NS^{R^{u_1}}$ is added into R^{u_1} and selects the segment s_{22} with the largest difference.

To construct a cloaked region for u_1, initially, in Fig. 5, AS sets the candidate cloaked region $R^{u_1} = \{s_{16}\}$ and $NS^{R^{u_1}} = \{s_{12}, s_{15}, s_{17}, s_{18}, s_{21}, s_{22}\}$. Since $k^{u_1} = 4$ and there are less than 4 trustees in R^{u_1}, AS needs to expand R^{u_1} by adding the best road segment in $NS^{R^{u_1}}$. Given s_{12}, $U(s_{12}) = \{u_8, u_9\}$, $p(s_1) = 1/3$ since only u_8 is one of the trusted users of u_1. $c(s_1) = 3/4 + 1/2 = 5/4$ as u_8 needs 3 more trusted users and u_9 needs 1 more trusted user. $p(s_{12}) - c(s_{12}) = -11/12$. Similarly, $p(s_{15}) - c(s_{15}) = 0 - 2 = -2$, $p(s_{17}) - c(s_{17}) = 0 - 1 = -1$, $p(s_{18}) - c(s_{18}) = 0 - 2 = -2$, $p(s_{21}) - c(s_{21}) = 1/3 - 1 = -2/3$, $p(s_{22}) - c(s_{22}) = 1 - 0 = 1$. Hence, s_{22} is selected according to Definition 16 and $CR^{u_1} = \{s_{16}, s_{22}\}$. We also find that every user's privacy requirement is satisfied in R^{u_1} now and hence $R^{u_1} = \{s_{16}, s_{22}\}$ is selected as the cloaked region for u_1.

We can see that the greedy expansion tends to minimize the size of a cloaked region while the random expansion may generate a cloaked region with a larger size that can decrease the quality of the location-based services (QoS). However, the greedy expansion may be more vulnerable to the replay attack (Wang and Liu, 2009) where an attacker knows the preference of the expansion process and he can possibly replay the anonymization process to identify a user's exact location. To balance the QoS and the resilience against the replay attack, we further propose a hybrid expansion that combines the random expansion and the greedy expansion.

Hybrid expansion. When a cloaked region R needs to be expanded, AS randomly adopts either the random expansion or the greedy one to add a road segment to R in the hybrid

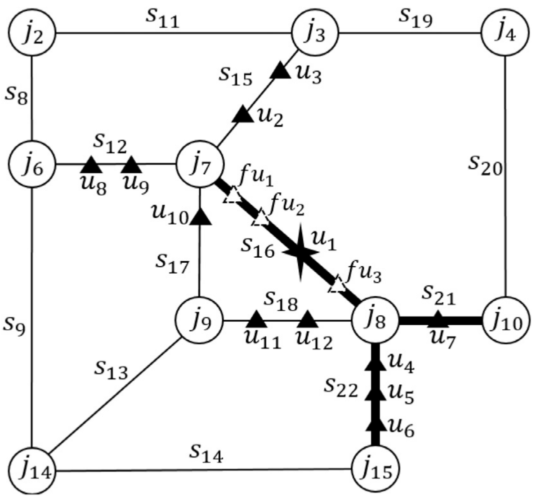

Fig. 6 – An example of the hybrid expansion. In this example, to expand the cloaked region $R^{u_1} = \{s_{16}\}$ to satisfy $k^{u_1} = 4$, in the first step, the hybrid expansion randomly selects the random expansion and therefore randomly selecting s_{21} from $NS^{R^{u_1}}$. Then, since $k^{u_1} = 4$ is still not met, in the second step, the hybrid expansion randomly selects the greedy expansion and therefore selecting s_{22} according to the 'best first' computation.

Algorithm 1: Cloaking Algorithm Guaranteeing *k-Trustee*.

```
Input: A road network $G(J, S)$, active users in a user set $U$
       traveling in G, a time instant t, and a privacy
       setting $p^{u_i}(k^{u_i}, e_l^{u_i}, f_l^{u_i}, e_g^{u_i}, f_g^{u_i}, R_M^{u_i}, T_M^{u_i})$ of each user
       $u_i \in U$
Output: An anonymized set $RS\langle u_i, R_t^{u_i}\rangle$
1  $CU \leftarrow \emptyset$;
2  $RS \leftarrow \emptyset$;
3  $es \leftarrow$ getExpansionScheme();
4  foreach $u_i \in U$ do
5      getTrustees($u_i$, $p^{u_i}$, t);
6  while $CU \neq U$ do
7      $u_i$ = pickAnUnprocessedUser($U$, $CU$);
8      $CR_t^{u_i} \leftarrow s_t^{u_i}$;
9      while !PrivacyMet($CR_t^{u_i}$) do
10         $s_j \leftarrow$ getExpanded($CR_t^{u_i}$, $es$);
11         $CR_t^{u_i} \leftarrow CR_t^{u_i} + s_j$;
12     $R_t^{u_i} \leftarrow CR_t^{u_i}$;
13     foreach $u_j \in R_t^{u_i}$ do
14         $CU \leftarrow u_j$;
15         if Size($R_t^{u_j}$) > Size($R_M^{u_j}$) then
16             $R_t^{u_j}$ = unavaliable;
17         else
18             $RS \leftarrow (u_j, R_t^{u_j})$;
```

expansion scheme. AS continues to do the same expansions until every user's privacy requirement is satisfied in *R*.

For example, in Fig. 6, every user's privacy setting is same as the one in Fig. 5. Initially, $R^{u_1} = \{s_{16}\}$ and $NS^{R^{u_1}} = \{s_{12}, s_{15}, s_{17}, s_{18}, s_{21}, s_{22}\}$. In the first expansion, we assume that the random expansion is employed and s_{21} is added into R^{u_1}, so $R^{u_1} = \{s_{16}, s_{21}\}$. In the second expansion, the greedy expansion is adopted. s_{22} is chosen based on Definition 16 and it is added to R^{u_1}. Now, we can see that *k-Trustee* is guaranteed for every user in $R^{u_1} = \{s_{16}, s_{21}, s_{22}\}$.

3.3.3. k-trustee *cloaking algorithm*

The cloaking algorithm that guarantees *k-Trustee* is shown in Algorithm 1. In this algorithm, the cloaking process, run by AS, first initializes a user set *CU* indicating users who have been processed by the algorithm, the output set and the expansion scheme adopted by the algorithm (line 1–3). It then computes the trusted users for each user at *t* based on the user's privacy setting p^{u_i} (line 4–5). After that, it randomly selects one user who has not been processed and starts to construct a cloaked region where each user's privacy requirement is satisfied using the selected expansion scheme (line 6–12). If the size of the cloaked region is larger than the required one for a user in the constructed cloaked region, the anonymity service is not available for that user (line 13–16). However, the AS will continuously include that user into future cloaked regions until the maximum response time R_M^u of that user has passed. In that case, the query of that user is rejected (i.e., if its k-trustee requirement is not met). Since only the query of that user fails, we believe its influence to other users is not big. Lastly, the cloaking process stops when all the users have been processed. Note that, to simplify, the restriction of the time $T_M^{u_i}$ defined by a user u_i are not involved in this algorithm. We recommend that it be handled by a user's mobile device.

Note that the guarantees of POI *l-Diversity* (Bamba et al., 2008) and road segment *s-Diversity* (Wang and Liu, 2009) can be additionally ensured by the *k-Trustee* cloaking-based location privacy preserving mechanism. The *k-Trustee* cloaking process can first satisfy *l-Diversity* or *s-Diversity* requirement for every users in the region and then it satisfies the *k-Trustee* requirement. It can also first satisfy every user's *k-Trustee* requirement and then it guarantees the *l-Diversity* or *s-Diversity* requirement. We argue that the latter approach may be more appropriate when most of the users are strict to their trusted users by setting high values for *k-Trustee* requirements. It is because the guarantee of *k-Trustee* usually also ensures *l-Diversity* and *s-Diversity*. On the other hand, the former probably works more efficiently when there are fewer fake users in the road network and users are less strict in defining their trusted users.

4. Simulations

In this section, we first present the results of location injection attacks in the cloaking mechanism (called the general cloaking) guaranteeing only *k-Anonymity* and the one supporting both *k-Anonymity* and *s-Diversity* (referred as XStar Wang and Liu, 2009). We choose the general cloaking algorithm as the baseline approach and the XStar algorithm as the advanced approach. We want to demonstrate that the location injection attack is effective for both *k*-anonymity and *s*-diversity. We also want to compare the performance of a location injection attack when it is launched over a cloaking algorithm purely designed for k-anonymity and a cloaking algorithm designed for both k-anonymity and s-diversity. After evaluating the location injection attacks, we simulate the proposed k-*Trustee* cloaking algorithm and demonstrate its effectiveness against the location injection attacks.

4.1. *Experiment setup*

In our experiments, we use the GT Mobile simulator (Pesti et al., 2009) to generate trajectories of 30,000 users moving in the DeKalb County in Atlanta regions of Georgia, which contains 37,996 segments and 27,647 junctions. We assume that each user is active during the travel in this road network and he has a location-based request from a specific location service provider every second. The simulator runs for 10 minutes and each user has 600 location-based requests in total. Note that we assume that all of these 30,000 users are authentic users.

4.1.1. *Privacy settings*

Given any authentic user u in the road network, we first set k^u for k-*Anonymity* and k-*Trustee* as a randomly chosen value from 2 to 10. We also set r^u (used by XStar to support s-*Diversity*) as randomly chosen values between 2 and 5. The maximum size R_M^u (the number of the road segments) of the cloaked region accepted by u is a random value chosen from the set $\{20r^u, 30r^u, 40r^u, 50r^u\}$. We then set e_l^u and f_l^u as random values between 20 and 40, respectively. The global privacy requirements, e_g^u and f_g^u are both set as 5 for u. Note that, in the simulations, we assume that each user can get the cloaked results from AS immediately and we do not set the maximum waiting time (T_M^u) for u.

Regarding each fake user fu created by the attacker, we choose the least privacy restrictions for him; *i.e.*, we set $k^{fu} = r^{fu} = 2$, $R_M^{fu} = 250$, $e_l^{fu} = f_l^{fu} = 40$, $e_g^{fu} = f_g^{fu} = 5$.

4.1.2. *Target Selection*

As shown in Section 2.4, the location injection attack has two types of targets: user targets and location targets. In the simulation, we randomly select 1000 out of 30,000 authentic users as the user targets. Regarding location targets, we focus on the road segments which have at least one user during the simulation, *i.e.*, the average traffic of the road segment (the number of users visiting a road segment) is no less than 1. There are 9033 such road segments in the dataset and we randomly select 1000 of them as location targets. In addition, we choose 10 trajectories as the targets for the fixed-trajectory attack. These selected one consist of 10 connected road segments and there are total of 95 authentic users traveling on them.

4.1.3. *Fake user creations*

We simulate fake users according to the proposed three attack models (refer to Section 2.4) as follows:

Stalking Attack. We assume that an attacker initially knows the initial location (a road segment) of the targeted user by injecting enough fake users into the road network (refer to Section 2.4.1). We then generate 6, 8 and 10 fake users, respectively, for a targeted user when the general cloaking is adopted. We also create 10, 15 and 20 fake users, respectively, for a targeted user when the *XStar* is applied. These fake users travel either in the same segment with the targeted user or few segment-based distant away from the targeted user as described in Section 2.4.1.

Fixed-location attack. At a targeted road segment, we generate 2, 4 and 6 fake users, respectively, when the general cloaking is adopted. We also create 6, 8 and 10 fake users placed at a targeted road segment, respectively, when the *XStar* is applied. The location injection attack needs more fake users to compromise the *XStar* algorithm successfully. Unlike the general cloaking algorithm that only guarantee k-Anonymity, the *XStar* algorithm is designed for both k-Anonymity and s-Diversity. It is the s-Diversity that makes the *XStar* algorithm harder to be compromised. These fake users travel at the trajectory described in Section 2.4.2.

Fixed-trajectory attack. Given a targeted trajectory, we put 4, 6 and 8 fake users traveling at every road segment in the trajectory, respectively, in this attack. The goal of such an attack is to identify users who travel exactly on these trajectories.

Note that the times of the attacks conducted for each target is 600 in our simulation since each user has a total of 600 location-based requests during his travel in the road network (refer to 4.1).

4.1.4. *Measurements*

In the simulations, we adopt the following measurements to evaluate the location injection attacks and the cloaking-based mechanism guaranteeing k-*Trustee*:

In-distinguishability D_R: It indicates the in-distinguishability of a user (the number of trusted users) in a cloaked region. Each user has specified its required value (k) in the k-*Anonymity* and in the k-*Trustee* cloaking mechanisms. The location injection attack aims to compromise it by lowering its value. Note that fake users do not contribute to D_R for an attacker since they are distinguishable for the attacker. A lower value of D_R indicates the lower location privacy protection. Thus, the lower value of D_R a location injection attack can achieve the more successful the attack is.

Size of a cloaked region S_R: It represents the in-distinguishability of a road segment in a cloaked region. In the *XStar*, each user specifies the privacy requirement for S_R. The location injection attacks may be able to lower its value. In addition, we use it to demonstrate the quality of service for the k-*trustee* cloaking-based mechanism.

Cloaking failure rate F_R: In the *XStar* and the k-*Trustee* cloaking mechanisms, a user usually needs to define the maximum size of the cloaked region, *i.e.*, the maximum number of road segments in a cloaked region. Given a user, we say the anonymity service is failed when the size of the cloaked region for a user is larger than the defined maximum size by the user. Then, R_R generally indicates how practical the cloaking-based mechanism is.

Attack successful rate A_R: In an attack, given a user and a cloaked region, when the number of the trusted users in the cloaked region is smaller than a specified k by the user, we say the attack is successful. The A_R for a user indicates how successful the location injection attacks work for that user in general.

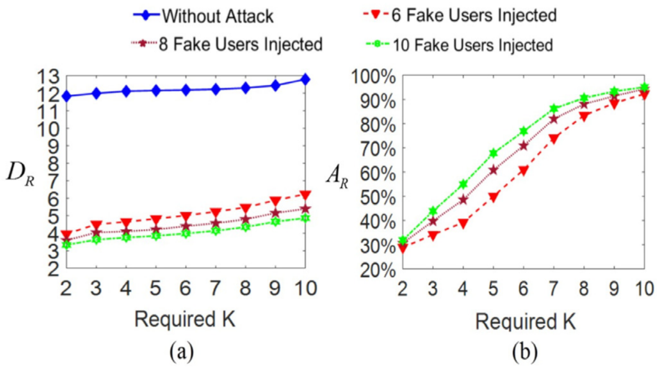

Fig. 7 – Stalking Attacks on the General Cloaking Algorithm.

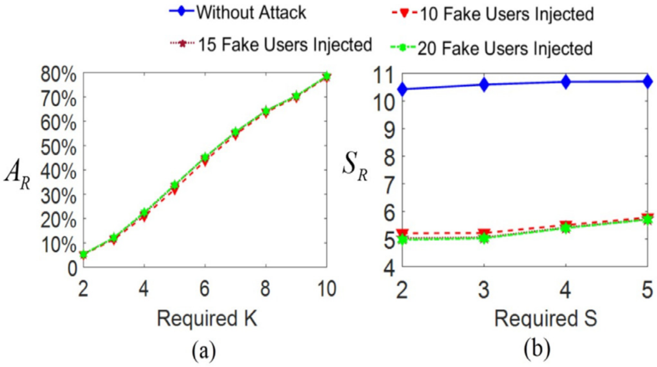

Fig. 8 – Stalking Attacks on the XStar Algorithm.

4.2. *Attack results of location injection attacks*

In the subsection, we present the results of the location injection attacks on two road network-aware cloaking algorithms guaranteeing *k-Anonymity*: (1) the general cloaking algorithm with a random expansion; (2) *XStar* cloaking algorithm (Wang and Liu, 2009) which preserves users' location privacy with the additional guarantee of *s-Diversity*.

Stalking Attacks on a General Cloaking Algorithm. The attack results of the stalking attacks on the general cloaking algorithm are shown in Fig. 7. It demonstrates the average D_R (Fig. 7.a) and the average A_R (Fig. 7.b) for targeted users with their diverse *k-Anonymity* requirements. From Fig. 7.a, we can see that the stalking attacks can significantly downgrade the D_R for targeted users. When the stalking attacks are not launched, the range of the D_R for targeted users is between 12 and 13 with the guarantee of *k-Anonymity* for each user. However, when the attacks are launched, D_R decreases to the range of 3 and 6. When the required *k* in the *k-Anonymity* specified by targeted users is larger than 6, we even find that the average D_R for these users is even lower than 6. Such a result suggests the successes of the attacks. Fig. 7.b also confirms the successes of the attacks by showing that the average A_R is more than 50% when the required *k* of *k-Anonymity* is larger than 6. We also find that A_R increases with the increase of the required *k*. Such a result reflects that the stalking attacks are more successful for users with the more restricted *k-Anonymity* requirements.

Stalking Attacks on the XStar Algorithm. Fig. 8 shows the stalking attack results on the *XStar* cloaking algorithm. Fig. 8.a demonstrates the average A_R for targeted users with their various *k-Anonymity* requirements while Fig. 8.b indicates the average S_R with users' *s-Diversity* requirements. From Fig. 8.a, we can see that A_R has a significant increase from 5% to 80% with the increased value of the required *k* in the *k-Anonymity*. Such a result shows that most attacks are successful. From Fig. 8.b, we find that the attacks can dramatically decrease values of S_R from 10 to 5 causing the targeted users easier to be distinguishable. However, since the required S of *s-Diversity* defined by targeted users are between 2 and 5, the stalking attacks cannot actually compromise the guarantee of *s-Diversity*. Lastly, we also find that the number of fake users used in the attacks for the *XStar* cloaking algorithm may not be able to significantly promote the attack results from both graphs.

Fixed-location attacks. The results of the fixed-location attacks on the general cloaking algorithm are shown in Fig. 9. It shows that the average D_R of users visiting every targeted road segment. We can see that D_R significantly decreases with the increasing number of injected fake users. When 2 fake users are injected at a targeted segment, it seems that the *k-Anonymity* requirements for users visiting the targeted segment are still satisfied in most attack instances. However, when 4 or 6 fake users are placed at a targeted segment, D_R deceases significantly than the required value and users'

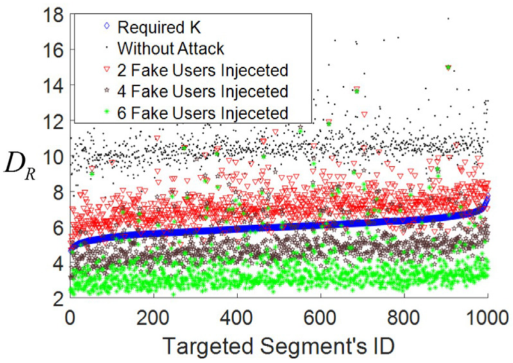

Fig. 9 – Fixed-location Attacks on the General Cloaking Algorithm.

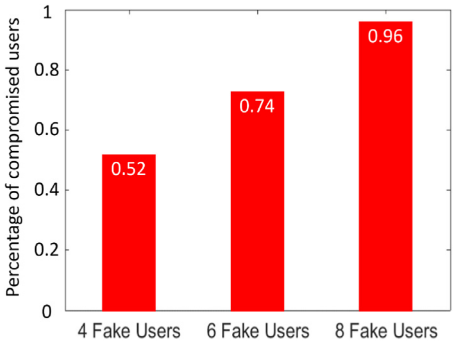

Fig. 10 – Results of fixed-trajectory attacks.

k-Anonymity requirements are compromised. In our simulation, we also find that A_R is between 20% and 40% when 2 fake users are placed. When 4 or 6 fake users are injected, the range of A_R has a remarkable increase and it is between 60% and 90%. These results also confirm the successes of the fixed-location attacks on the general cloaking algorithm. In addition, we simulated the fixed-location attacks on the *XStar* cloaking algorithm. However, such attacks are less successful and the average A_R is below 20%. We believe that the enforcement of the *s-Diversity* can mitigate the fixed-location attacks to some extent.

Fixed-trajectory attacks. We also performed the fixed-trajectory attacks for the chosen trajectories in order to identify users who follow these trajectories. The results of the attacks on a general cloaking algorithm are shown in Fig. 10. Among the 95 targets in the fixed-trajectory attacks, the percentage of compromised users rises from 0.52 to 0.96 when the number of placed fake users are increased from 4 to 8. These numbers reflect the successes of the fixed-trajectory attacks. We also simulated the fixed-trajectory attacks under the *XStar* clocking algorithm. However, the attacks are not successful and we cannot identify the trajectory of any user in terms of the requirements of *s-Diversity* defined by users. To have a successful fixed-trajectory attack, all the constructed cloaked regions from AS for a user should have only one road segment in order to determine the user's trajectory. The cloaked region from the *XStar* includes more than one road segment and hence the attack cannot be successful.

4.3. *Location injection attacks on k-trustee cloaking algorithm*

In this subsection, we utilize the same fake users for the same targeted users and locations as those used in the Section 4.2. We simulate various location injection attacks on the *k-Trustee* cloaking mechanism. Note that, in these simulations, when users additionally specify requirements for the diversity of the road segments, we first guarantee their *k-Trustee* requirements and then meet those for the diversity of road segments.

4.3.1. *General attack results*

We first perform location injections for targets on the *k-Trustee* cloaking mechanism adopting the coarse-grained trust functions and the random expansion scheme.

Fig. 11 shows the results of the stalking attacks on the *k-Trustee* cloaking mechanism. Fig. 11.a indicates the average A_R for targeted users who has different *k-Anonymity* requirements and do not specify the diversity of road segments. Fig. 11.b demonstrates the average A_R for targeted users who do specify the diversity of road segments. From this figure, we can see that less than 5% of the stalking attack instances on the *k-Trustee* cloaking mechanism are successful. Compared to those successful rates shown in Figs. 7 and 8, we can conclude that the *k-Trustee* cloaking mechanism can significantly defend against the stalking attacks.

In addition, our simulation results for the fixed-location attacks on the *k-Trustee* cloaking mechanism demonstrate that less than 4% of the attack instances on average are successful for targeted road segments when users do not specify the diversity of road segments. When users do specify this requirement, our results show that the average A_R is less than 1.5%. Compared to the corresponding results of the same attacks on the general cloaking algorithm in Section 4.2, we can say that the fixed-location attacks become significantly less successful when the *k-Trustee* cloaking mechanism is applied. Furthermore, we performed the fixed-trajectory attacks on the *k-Trustee* cloaking mechanism. However, we cannot identify any user's trajectory in this case.

Based on the above results, we can conclude that the *k-Trustee* cloaking mechanism is indeed effective to mitigate the location injection attacks.

4.3.2. *k-trustee cloaking mechanism with different trust functions*

We next compare the effectiveness of the *k-Trustee* cloaking mechanisms using different trust functions (coarse-grained trust and fine-grained trust functions) as discussed in Section 3.2. We focus on the stalking attacks using 8 fake users for each targeted users. We also assume that a random expansion is adopted in these *k-Trustee* cloaking mechanisms and users do not specify the diversity of road segments. We then perform the stalking attacks for the targeted users using different trust functions in the *k-Trustee* cloaking mechanism and the results are shown in Fig. 12. It shows the average A_R for each targeted users. We can see that both of the coarse-grained and fine-grained trust functions adopted by the *k-Trustee* cloaking mechanisms are effective to mitigate the location injection attacks. As expected, the fine-grained trust

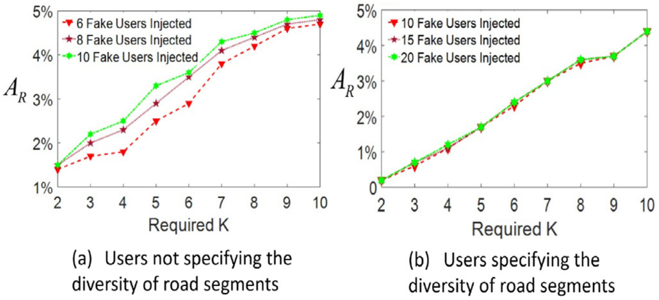

Fig. 11 – Results of the Attacks on the *k-Trustee* Cloaking Mechanism.

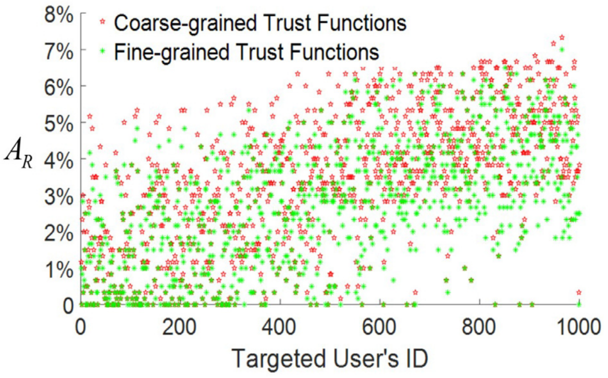

Fig. 12 – Coarse-grained Trust Functions *vs*. Fine-grained Trust Functions.

functions can achieve a better resilience by approximately decreasing 1% of A_R by average.

4.3.3. *k-trustee cloaking mechanism with different expansion schemes*

In Section 3.3.2, we discussed three different expansion schemes for the *k-Trustee* cloaking mechanism and we compare them in this subsection. We first focus on the stalking attacks using 10 fake users for each targeted user who also specifies the diversity of road segments. We then adopt the coarse-grained trust functions for the *k-Trustee* cloaking mechanisms using the random expansion, the greedy expansion and the hybrid expansion. Our results are shown in Fig. 13. Fig. 13.a demonstrates the average A_R for targeted users with different *k-Anonymity* requirements. We can see that attacks on the the *k-Trustee* cloaking mechanism using the greedy expansion can achieve the lowest A_R while those on the *k-Trustee* cloaking mechanism adopting the random expansion have the highest A_R. Fig. 13.b indicates the average size of cloaked regions, S_R, for targeted users with different requirements for the diversity of road segments. We can find that the random expansion induces AS to construct the largest cloaked regions while the greedy expansion induces AS to construct the smallest cloaked regions. Based on these results, we can say that the greedy expansion has the best resilience against location injection attacks and it can achieve the best quality of the location-based services.

5. Related work

Location privacy has been an active area of research for decades. To protect users' location privacy during usage of location based services (LBS), various location privacy protection mechanisms have been proposed. Based on their core ideas, these mechanisms can be broadly categorized into approaches that use dummies (Kido et al., 2005; Liu et al., 2017), space transformation (Ghinita et al., 2008; Khoshgozaran and Shahabi, 2007), mix-zone (Beresford and Stajano, 2004; Palanisamy and Liu, 2015), encryption (Li and Jung, 2013), spatial cloaking (Beresford and Stajano, 2003; Cho et al., 2015; Gedik and Liu, 2005; Gruteser and Grunwald, 2003; Hoh et al., 2007; Kalnis et al., 2007; Li and Palanisamy, 2015; Mokbel et al., 2006; Wang and Liu, 2009; Ying and Makrakis, 2014) and differential privacy (Andrés et al., 2013; Hua et al., 2017; Xiao et al., 2017). The basic ideas behind these techniques are briefly discussed as follows. The dummy-based approaches replace real user locations with fake locations that are related to the real ones. The schemes based on spatial transformation transform data to another space to encode relationship between data and queries. The mix-zone solutions change pseudonyms of users who enter the zones so that adversaries are unable to link leaving users with entering users. The encryption-based schemes use cryptographic techniques to protect privacy of location data. For instance, in Li and Jung (2013), Li *et al.* applied CP-ABE (Bethencourt et al., 2007) to extend binary access to location data to a fine-grained access control model. The spatial cloaking mechanisms, as the most widely studied category, usually generate cloaked regions that satisfy privacy requirements such as *k*-anonymity (Gruteser and Grunwald, 2003) for users and send such cloaked regions to LBS providers. More recent work have introduced the newer privacy paradigm of differential privacy (Dwork et al., 2006), to location privacy protection (Andrés et al., 2013; Hua et al., 2017; Xiao et al., 2017). By carefully applying differential privacy protection mechanisms (e.g. Laplace Mechanism (Dwork et al., 2006), Exponential Mechanism (McSherry and Talwar, 2007)) to the location data, the personal location information in the disclosed statistical output can be protected. Among these techniques, we have focused on studying the spatial cloaking technique in this work because it is the one that has been widely studied with respect to various settings (e.g., centralized (Gedik and Liu, 2005; Mokbel et al., 2006), P2P (Chow et al., 2006; 2011)) as well as various problem statements (e.g., snapshot

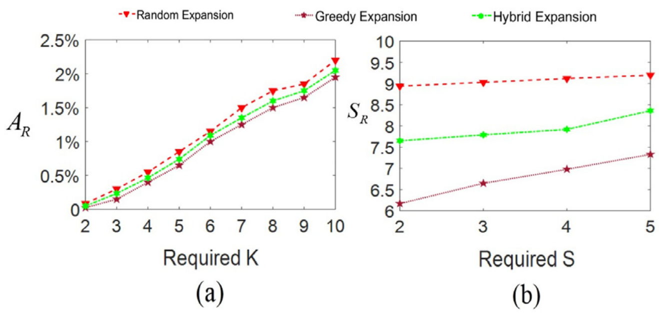

Fig. 13 – Results of the Attacks using Different Expansion Schemes in the *k-Trustee* Cloaking Mechanism.

queries Gedik and Liu, 2005, trajectories Chow and Mokbel, 2011). While differential privacy provides a more formal and rigorous privacy guarantee against background knowledge attacks, it can result in a higher perturbation and may provide a lower data utility compared to spatial cloaking techniques. Thus, in cases where there is a lack of background knowledge and when the risks of such attacks are minimal, the spatial cloaking techniques are likely to provide a higher data utility compared to differential privacy. A unified framework for location privacy that offers a systematic view by formalizing the problem, adversaries, mechanisms and metrics can be found in Shokri et al. (2010).

The notion of spatial cloaking was first introduced by Beresford and Stajano (2003). From then on, many centralized approaches have been proposed, which essentially leverage a centralized anonymization server to deploy the spatial cloaking algorithms. Among these approaches, Gruteser and Grunwald (2003) presented the *Interval Cloak* that guarantees *k-Anonymity* in the cloaked region to preserve users' location privacy from LBS providers. Gedik and Liu (2005) introduced the *CliqueCloak* where users' personalized privacy requirements for *k-Anonymity* are satisfied. Mokbel et al. (2006) designed *Casper* that extended the *Interval Cloak* to the grid network with the privacy-aware query processor. Hoh et al. (2007) developed a time-to-confusion criterion as the duration over which an attacker could track a target. Based on it, they designed an uncertainty-aware path cloaking mechanism that guarantee *k-Anonymity* for all users and hide users' trajectories. Kalnis et al. (2007) improved the previous cloaking algorithms by introducing the *Hilbert Cloak*. The *Hilbert Cloak* satisfies reciprocity that is sufficient for users to achieve the spatial *k-Anonymity* for their location requests. Cui et al. (2016) extended the *Hilbert Cloak* by considering average query density to make anonymity set satisfy both reciprocity and uniformity. Zheng et al. (2014) proposed an approach that selects a sub-area from the clocked region that may or may not include the real user location to prevent side information attacks launched by adversaries.

However, centralized approaches usually suffer from a single point of trust, which motivates the research of decentralized solutions that do not need the anonymization server. As the representative solution, Chow et al. (2006) proposed a peer-to-peer (P2P) spatial cloaking algorithm that leverages single-hop communication and/or multihop routing among peers to generate cloaked region without help from a centralized anonymization server. The algorithm offers two modes. The candidate searching step is triggered by queries in the *demand* mode, whereas it is periodically executed in the *proactive* mode. Later, Chow et al. (2011) improved their scheme with information sharing scheme, historical location scheme and cloaked region adjustment scheme. After that, Che et al. (2012) proposed the *dual-active* mode that allows peers both actively collect location data and actively disseminate collected data to others, which offers better performance than the previous two modes. However, the above P2P approaches are not reliable when there are malicious peers in the network. To secure the P2P scheme, Jin and Papadimitratos (2015, 2017) introduced the pseudonymous authentication technique to provide message authentication and integrity for peer communication, thus significantly suppressing the impact of malicious peers.

Recent work has considered the location cloaking problem under a constrained road network model (Cho et al., 2015; Li and Palanisamy, 2015; Wang and Liu, 2009; Ying and Makrakis, 2014). Wang and Liu (2009) implemented *XStar* which supports the *k-Anonymity* and the road segment diversity in a road network. Li and Palanisamy (2015) further made the *k*-anonymity reversible. However, all of these algorithms guarantee *k-Anonymity* but they are vulnerable to the proposed location injection attacks as shown in Section 2.3.

The fake users/accounts/identities have become a well-known security and privacy issue (Rowaihy et al., 2007). This problem can also pose a threat to data aggregation systems, voting systems, peer-to-peer systems, social networks and misbehavior detection mechanisms. For example, in the peer-to-peer systems, such a problem can lead to the *Sybil attacks* where an attacker forges multiple identities to compromise the network to arbitrarily subvert content storage and acquisition (Rowaihy et al., 2007). In social networks, an attacker can create fake accounts to impersonate victims, deceive the victim's friends and destroy the victims' reputations (Jin et al., 2011). In the literature, the defense approaches against these attacks are usually based on trust among users, position verification, game theory and access control mechanisms. For instance, Yu *et al.* proposed a *Sysbil* defense approach based on the trust in the social networks (Yu et al., 2006). Chen et al. (2010) proposed a generalized attack-detection model using the spatial correlation of RSS inherited from wireless nodes to detect Sybil nodes. In this paper, we identify that fake users can also be utilized in the cloaking-based privacy preserving mechanisms to compromise the guarantee *k-Anonymity* via the proposed location injection attacks. We then design the *k*-

Trustee cloaking-based mechanisms to mitigate such attacks. To the best of our knowledge, our proposed approach is the first work to address this kind of attacks in the cloaking-based privacy preserving mechanisms.

6. Conclusion and future work

In this paper, we identified the vulnerability of location injection attacks in existing cloaking-based location privacy preserving mechanisms. We presented various attack models and demonstrated the effectiveness of these attacks through simulations. We developed cloaking-based mechanisms that guarantee the notion of *k-Trustee* by employing different trust functions and expansion schemes to mitigate the location injection attacks. We demonstrated that the *k-Trustee* cloaking-based privacy preserving mechanisms are effective against these attacks. As future work, we plan to study how to achieve *k-Trustee* in a peer-to-peer (P2P) environment that has no centralized anonymization server. Since P2P spatial cloaking algorithms usually leverage P2P communication to build the cloaked region, the generation of fake users become harder. However, similar attacks can still be launched by malicious users. For example, a fixed-location attack can be launched by malicious users that stay in a particular location, e.g., a hospital. Such an adversary can communicate with nearby peers to form cloaked regions and learn about the peers who are visiting the hospital. Because of the lack of a global view, computing global trustees in the P2P environment becomes a challenging problem. A promising solution to the lack of a global view is to leverage the blockchain (Nakamoto, 2008) technique to build global trust. We believe that it can be adopted as a digital ledger to record the *e-stalker* and *f-stationary* to offer a trusted global view in the P2P environment. A blockchain insures credibility so that all the users are guaranteed that they all see the same *e-stalker* and *f-stationary* when they participate in the location anonymization process. These values, once submitted to the blockchain, become nearly tamper-proof unless someone controls a majority of computation power of the distributed network (Eth, 0000). One potential way to implement this process is to develop a decentralized application over the Ethereum smart contract platform (Wood, 2014), which can collect *e-stalker* and *f-stationary* from mobile users, compute the global *e-stalker* and *f-stationary* values and show these global values to all the mobile users through Ethereum mobile browsers (e.g., Tos, 0000). Another potential future direction of work is to enable our system to distinguish intentional stalking behavior from unintentional stalking. A group of people who travel together within a period of time may label each other as *e-stalkers*. As a result, each of them may be globally labeled as *e-stalker* by many, and thus, it becomes hard to add them into a cloaked region that require members with lower count of being an e-stalker. A potential solution requires each user to maintain a list of trusted user IDs, such as a friend list or family group in many kinds of applications. Then, after receiving the cloaked regions from AS, this list can be used as a filter so that the *e-stalker* values are only computed for the unknown users. Here, it is important that the metadata used should not create additional privacy risks. In order to control and mitigate such potential risks, one approach is to avoid the creation of new metadata each time for the location anonymization process and instead we can leverage existing user relationship information such as a friend list on social networks as the source of metadata. Such an approach significantly reduces the amount of newly generated metadata and mitigates any potential risks associated with the use of metadata.

REFERENCES

Andrés ME, Bordenabe NE, Chatzikokolakis K, Palamidessi C. Geo-indistinguishability: differential privacy for location-based systems. Proceedings of the 2013 ACM SIGSAC conference on computer & communications security. ACM; 2013. p. 901–14.

Bamba B, Liu L, Pesti P, Wang T. Supporting anonymous location queries in mobile environments with privacygrid. Proceedings of the 17th international conference on World Wide Web. ACM; 2008. p. 237–46.

Beresford AR, Stajano F. Location privacy in pervasive computing. IEEE Pervasive Comput. 2003;2(1):46–55.

Beresford AR, Stajano F. Mix zones: User privacy in location-aware services. Proceedings of the second IEEE annual conference on pervasive computing and communications workshops, 2004. IEEE; 2004. p. 127–31.

Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proceedings of the IEEE symposium on security and privacy, 2007. SP'07. IEEE; 2007. p. 321–34.

Che Y, Yang Q, Hong X. A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks. Proceedings of the wireless communications and networking conference (WCNC) IEEE. IEEE; 2012. p. 2098–102.

Chen Y, Yang J, Trappe W, Martin RP. Detecting and localizing identity-based attacks in wireless and sensor networks. IEEE Trans. Vehicular Technol 2010;59(5):2418–34.

Cho HJ, Kwon SJ, Jin R, Chung TS. A privacy-aware monitoring algorithm for moving k-nearest neighbor queries in road networks. Distrib Parallel Databases 2015;33(3):319–52.

Chow CY, Mokbel MF. Enabling private continuous queries for revealed user locations. Proceedings of the international symposium on spatial and temporal databases. Springer; 2007. p. 258–75.

Chow CY, Mokbel MF. Trajectory privacy in location-based services and data publication. ACM Sigkdd Explorations Newslett 2011;13(1):19–29.

Chow CY, Mokbel MF, Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems. ACM; 2006. p. 171–8.

Chow CY, Mokbel MF, Liu X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. GeoInformatica 2011;15(2):351–80.

Cui N, Yang X, Wang B. A novel spatial cloaking scheme using hierarchical hilbert curve for location-based services. Proceedings of the international conference on web-age information management. Springer; 2016. p. 15–27.

Dwork C, McSherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. Proceedings of the theory of cryptography conference. Springer; 2006. p. 265–84.

Ethernodes: The ethereum node explorer. https://www.ethernodes.org/network/1.

Gedik B, Liu L. Location privacy in mobile systems: a personalized anonymization model. Proceedings of the 25th IEEE international conference on distributed computing systems, 2005. ICDCS 2005. IEEE; 2005. p. 620–9.

Ghinita G, Kalnis P, Khoshgozaran A, Shahabi C, Tan KL. Private queries in location based services: anonymizers are not necessary. Proceedings of the 2008 ACM SIGMOD international conference on Management of data. ACM; 2008. p. 121–32.

Ghinita G, Kalnis P, Skiadopoulos S. Prive: anonymous location-based queries in distributed mobile systems. Proceedings of the 16th international conference on World Wide Web. ACM; 2007. p. 371–80.

Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. Proceedings of the 1st international conference on Mobile systems, applications and services. ACM; 2003. p. 31–42.

Hoh B, Gruteser M, Xiong H, Alrabady A. Preserving privacy in GPS traces via uncertainty-aware path cloaking. Proceedings of the 14th ACM conference on computer and communications security. ACM; 2007. p. 161–71.

Hua J, Tong W, Xu F, Zhong S. A geo-indistinguishable location perturbation mechanism for location-based services supporting frequent queries. IEEE Trans. Inf. Forensics Secur. 2017.

Jin H, Papadimitratos P. Resilient collaborative privacy for location-based services. Secure IT systems. Springer; 2015. p. 47–63.

Jin H, Papadimitratos P. Resilient privacy protection for location-based services through decentralization. Proceedings of the 10th ACM conference on security and privacy in wireless and mobile networks. ACM; 2017. p. 253–8.

Jin L, Palanisamy B, Joshi JB. Poster: compromising cloaking-based location privacy preserving mechanisms with location injection attacks. Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. ACM; 2014. p. 1439–41.

Jin L, Takabi H, Joshi JB. Towards active detection of identity clone attacks on online social networks. Proceedings of the first ACM conference on data and application security and privacy. ACM; 2011. p. 27–38.

Kalnis P, Ghinita G, Mouratidis K, Papadias D. Preventing location-based identity inference in anonymous spatial queries. IEEE Trans. Knowl. Data Eng. 2007;19(12): 1719–1733.

Khoshgozaran A, Shahabi C. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. Proceedings of the international symposium on spatial and temporal databases. Springer; 2007. p. 239–57.

Kido H, Yanagisawa Y, Satoh T. Protection of location privacy using dummies for location-based services. Proceedings of the 21st International Conference on Data Engineering Workshops, 2005. IEEE; 2005. p. 1248.

Li C, Palanisamy B. Reversecloak: protecting multi-level location privacy over road networks. Proceedings of the 24th ACM international on conference on information and knowledge management. ACM; 2015. p. 673–82.

Li XY, Jung T. Search me if you can: privacy-preserving location query service. Proceedings of the INFOCOM. IEEE; 2013. p. 2760–8.

Liu H, Li X, Li H, Ma J, Ma X. Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services. Proceedings of the INFOCOM 2017-IEEE conference on computer communications. IEEE; 2017. p. 1–9.

McSherry F, Talwar K. Mechanism design via differential privacy. Proceedings of the 48th annual IEEE symposium on foundations of computer Science, 2007. FOCS'07. IEEE; 2007. p. 94–103.

Mokbel MF, Chow CY, Aref WG. The new casper: query processing for location services without compromising privacy. Proceedings of the 32nd international conference on Very large data bases. VLDB Endowment; 2006. p. 763–74.

Nakamoto S. Bitcoin: A peer-to-peer electronic cash system 2008. Working Paper.

Palanisamy B, Liu L. Attack-resilient mix-zones over road networks: architecture and algorithms. IEEE Trans. Mobile Comput. 2015;14(3):495–508.

Pesti P, Bamba B, Doo M, Liu L, Palanisamy B, Weber M. Gtmobisim: a mobile trace generator for road networks. College Computing, Georgia Inst of Tech; 2009.

Rowaihy H, Enck W, McDaniel P, La Porta T. Limiting sybil attacks in structured p2p networks. Proceedings of the 26th IEEE international conference on computer communications INFOCOM. IEEE; 2007. p. 2596–600.

Shokri R, Freudiger J, Hubaux JP. Technical Report. A unified framework for location privacy; 2010.

Toshi. https://www.toshi.org/.

Wang T, Liu L. Privacy-aware mobile services over road networks. Proc VLDB Endowment 2009;2(1):1042–53.

Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 2014;151.

Xiao Y, Xiong L, Zhang S, Cao Y. Loclok: location cloaking with differential privacy via hidden markov model. Proc VLDB Endowment 2017;10(12):1901–4.

Ying B, Makrakis D. Protecting location privacy with clustering anonymization in vehicular networks. Proceedings of the IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE; 2014. p. 305–10.

Yu H, Kaminsky M, Gibbons PB, Flaxman A. Sybilguard: defending against sybil attacks via social networks. Proceedings of the ACM SIGCOMM computer communication review. ACM; 2006. p. 267–78.

Zheng J, Tan X, Zou C, Niu Y, Zhu J. A cloaking-based approach to protect location privacy in location-based services. Proceedings of the 2014 33rd Chinese control conference (CCC). IEEE; 2014. p. 5459–64.

Lei Jin has been a graduate student at the University of Pittsburgh from 2009 to 2016 and was a member of the Laboratory of Education and Research on Security Assured Information Systems (LERSAIS). He received his MSE in Software Engineering from Tsinghua University and his BS in Computer Software from Tsinghua University in 2009 and 2006, respectively. His research interests include authentication, privacy and security in social computing and in mobile computing, usable privacy and security. He is a student member of the IEEE and the ACM.

Chao Li is currently a 4th year Ph.D. student in the School of computing and information, University of Pittsburgh and a member of the Laboratory of Education and Research on Security Assured Information Systems (LERSAIS). Before that, he got his MSc degree from Imperial College London and BEng degree from both University of Edinburgh and Dalian University of Technology. His current research interests include database privacy, location privacy, social network privacy, differential privacy, distributed system security and IoT privacy.

Balaji Palanisamy is an Assistant Professor in the School of computing and information in University of Pittsburgh. He received his M.S and Ph.D. degrees in Computer Science from the college of Computing at Georgia Tech in 2009 and 2013, respectively. His primary research interests lie in scalable and privacy-conscious resource management for large-scale Distributed and Mobile Systems. At University of Pittsburgh, he codirects research in the Laboratory of Research and Education on Security Assured Information Systems (LERSAIS), which is one of the first group of NSA/DHS designated Centers of Academic Excellence in Information Assurance Education and Research (CAE &CAE-R). He is a member of the IEEE.

James Joshi is a Professor of School of computing and information at the University of Pittsburgh. He received his MS in Computer Science and PhD in Computer Engineering degrees from Purdue University in 1998 and 2003, respectively. He is an elected Fellow of the Society of Information Reuse and Integration (SIRI) and is a Senior member of the IEEE and the ACM. His research interests include Access Control Models, Security and Privacy of Distributed Systems, Trust Management and Information Survivability. He is the director of LERSAIS at the University of Pittsburgh.