Geoinformatica (2014) 18:135–164
DOI 10.1007/s10707-013-0194-y

Effective mix-zone anonymization techniques for mobile travelers

Balaji Palanisamy · Ling Liu

Received: 30 May 2013 / Revised: 4 October 2013 /
Accepted: 10 October 2013 / Published online: 16 November 2013

Abstract Mix-zones are recognized as an alternative and complementary approach to spatial cloaking based location privacy protection. Unlike spatial cloaking techniques that perturb the location resolution through location *k*-anonymization, mix-zones break the continuity of location exposure by ensuring that users' movements cannot be traced while they are inside a mix-zone. In this paper we provide an overview of some known attacks that make mix-zones on road networks vulnerable and discuss a set of counter measures to make road network mix-zones attack-resilient. Concretely, we categorize the vulnerabilities of road network mix-zones into two classes: one due to the road network characteristics and user mobility, and the other due to the temporal, spatial and semantic correlations of location queries. We propose efficient road network mix-zone construction techniques that are resilient to attacks based on road network characteristics. Furthermore, we enhance the road network mix-zone framework with the concept of delay-tolerant mix-zones that introduce a combination of spatial and temporal shifts in the location exposure of the users to achieve higher anonymity. We study the factors that impact on the effectiveness of each of these attacks and evaluate the efficiency of the counter measures through extensive experiments on traces produced by GTMobiSim at different scales of geographic maps.

Keywords Location privacy · Mix-zone · Location-based services

1 Introduction

Advances in sensing and positioning technology, fueled by wide deployment of wireless local area networks (WLAN), have made many devices location-aware. Location-based

B. Palanisamy (✉)
School of Information Sciences, University of Pittsburgh, Pittsburgh PA, USA
e-mail: bpalan@pitt.edu

L. Liu
College of Computing, Georgia Institute of Technology, Atlanta GA, USA
e-mail: lingliu@cc.gatech.edu

services (applications that require geographic location information as input) are becoming increasingly common. The collection and transfer of location information about a particular subject can have important privacy implications. Concrete examples of location-based services (LBSs) include searching nearest points of interest (*"Where is the nearest gas station to my current location?*"), spatial alerts (*"Remind me when I drive close to the grocery store*"), location-based social networking ("*Is my colleague Tom currently at his office?*"). Such services require the Location-based Service Provider to track the location information of their mobile users in order to deliver location based services. Continuous location based services represent queries that are *continuously evaluated* along the trajectory of a mobile user either periodically or aperiodically. Examples of continuous queries (CQs) are "inform me the nearest gas stations coming up along the highway I-85 south every 3 min in the next 30 min" or "show me the restaurants on highway I85 north within 5 miles every two minutes during the next hour". Although LBSs offer users many interesting and life enhancing experiences, they also open doors for new security risks that can endanger the location privacy of mobile clients [3, 27].

Location privacy is a particular type of information privacy. According to [11], location privacy is defined as the ability to prevent other unauthorized parties from learning one's current or past location. In LBSs, there are conceivably two types of location privacy – personal subscriber level privacy and corporate enterprise-level privacy. Personal subscriber-level privacy must supply rights and options to individuals to control when, why, and how their location is used by an application. With personal subscriber-level privacy, each individual has liberties to "opt in" and "opt out" of services that take advantage of their mobile location. Corporate enterprise-level privacy is fundamentally different in that corporate IT managers typically control when, why, and how mobile location capabilities provide application benefits to the organization as a whole.

Location privacy threats refer to the risks that an adversary can obtain unauthorized access to raw location data, derived or computed location information by locating a transmitting device, hijacking the location transmission channel, and identifying the subject (person) using a mobile device. In the United States, privacy risks related to location information have been identified in the Location Privacy Protection Act of 2001 [4]. On one hand, public disclosure of location information enables many useful services such as improved emergency assistance. Mobile users can obtain a wide variety of location-based information services, and businesses can extend their competitive edges to mobile commerce and ubiquitous service provisions. On the other hand, without safeguards, extensive deployment of location based services may risk location privacy of mobile users and to expose LBSs to significant vulnerabilities for abuse. For example, location information can be used to spam users with unwanted advertisements or draw unwanted inferences from victims' visits to clinics, doctors' offices, entertainment districts, religious activities or political events. In extreme cases, unauthorized disclosure of private location information can lead to physical harm, for example in stalking or domestic abuse scenarios. Even though some Location based Service providers (such as Google maps) have a well-stated privacy policy statement, such privacy statement is primarily for not exposing the collected information to public and commercial uses. Thus, there are still inherent risks in continuous collection of location information by the LBS provider as there are channels of attacks beyond the control of the LBS provider and the protection of the privacy policy statement, including insider attacks. For instance, there was a recent incident in Google where a Google engineer spied on four underage teens for months before the company was notified of the abuses [5].

In the past, a fair amount of research efforts have been dedicated to protecting location privacy of mobile travelers. The first category is represented by location cloaking techniques [9, 20, 24, 31, 40]. Spatial location cloaking typically adds uncertainty to the location information exposed to the location query services by increasing the spatial resolution of a mobile user's locations while meeting location k-anonymity and/or location l-diversity [9]. More specifically, the spatially cloaked region is constructed to ensure that at least k users (*location k anonymity*) are located in the same region, which contains l different static sensitive objects (locations). However, the use of spatially cloaked resolution instead of exact position of users does not prevent continuous exposure of location information and thus may lead to breaches of location privacy due to statistics-based inference attacks [28]. Moreover, spatial cloaking is effective for snapshot queries but vulnerable to CQ-attacks.

In contrast, mix-zone based techniques anonymize user identity by restricting when and where the exposure of users' positions are allowed [11]. **Mix-zones** are regions in space where no applications can trace user movements. Mix-zones enable users to change pseudonyms such that the linking between the old and new pseudonyms is not revealed. The idea behind using pseudonyms instead of the real identities is to disassociate the exposure of location information from the actual identity of the person. However, when a pseudonym is used by a user for a continued duration of time, the adversary can link a pseudonym to the user's actual identity through the inference of user's personal locations such as home address, office location and other known favorite locations. For instance, if a pseudonym α is located often at the home location and office location of user *Tom*, then the adversary can infer with high confidence that the pseudonym α belongs to *Tom*. To prevent such inference of real identities from pseudonyms, pseudonyms need to be changed from time to time. However, simply changing the pseudonyms in a user's path of travel can leave the traces of the user trajectory and therefore the linking between the old and new pseudonyms can be easily inferred using a simple connect-the-dots approach.

Mix-zones securely enable users to change pseudonyms in an anonymous fashion such that the linking between the new and old pseudonyms can not be inferred. The anonymity in mix-zones is guaranteed by enforcing that a set of users enter, change pseudonyms and exit a mix-zone in a way such that the mapping between their old and new pseudonyms is not revealed [11]. In this paper, we assume that the mix-zones are managed by a trusted third party that is independent of location-based service providers and mobile users. One such third party player will be the mobile networking service provider as mobile users use their cellphones to request LBSs through location privacy protected channels via the networking service provider. We note that the mobile networking service provider has access to the locations of the users.[1] Therefore, in this paper we assume that the anonymizer is hosted by the networking service provider which acts as the trusted third party.

The idea of building mix-zones at road intersections was first proposed in [18] and [13]. An optimal placement of mix-zones on a road map was formulated in [19]. These earlier techniques for road network mix-zones follow a straightforward refinement of basic mix-zones [11] by using rectangular or circular shaped zones. Both the definition and the construction methodologies of these mix-zones fail to take into account the effect of timing and transition attacks.

Several factors impact on the effectiveness of mix-zone approaches, such as user population, mix-zone geometry, location sensing rate and spatial resolution, spatial and temporal

[1] The mobile networking service provider has access to the user location information through techniques such as cell tower triangulation.

constraints on user movement patterns as well as semantic continuity of the information requested by the LBSs. Mix-zones constructed on the road networks are vulnerable to timing and transition attacks due to the inherent nature of the road network and the mobility patterns of the users. Concretely, the timing information of users' entry and exit into the mix-zone provides information to launch a timing attack and the non-uniformity in the transitions taken at the road intersection provides valuable information for a transition attack. Both of these attacks aid the attacker in guessing the mapping between the old and new pseudonyms.

Mix-zones are also prone to CQ-attacks when the mobile clients obtain continuous query services. The CQ-attack refers to the risk that an adversary can perform inference attacks by correlating the semantic continuity in the time series of query evaluations of the same CQ and the inherent trajectory of locations. We note that neither spatial cloaking nor mix-zone techniques are inherently resilient to CQ attacks. In this paper, we introduce the various attacks that road networks are vulnerable to and illustrate the possible counter measures to deal with them. We first describe and analyze the timing and transition attacks on road network mix-zones and then study the continuous query correlation attacks (CQ-attacks) that perform query correlation based inference to break the anonymity of road network-aware mix-zones. We describe three types of the continuous query correlation attacks (CQ attacks for short): (i) the basic CQ attacks in which only query correlation based inference is performed, (ii) the CQ-timing attacks in which inference attack is performed based on both query correlation and timing correlation, and (iii) CQ-transition attacks in which inference attack is performed based on both query correlation and transition correlation.

We then discuss in detail the various road network mix-zone construction techniques that are resilient to these attacks. Finally, we present an enhancement of the road network mix-zone framework namely the concept of delay-tolerant mix-zones that introduce a combination of spatial and temporal shifts in the location exposure of the users to achieve higher anonymity than conventional mix-zones. We show that the delay-tolerant mix-zone model offers greater level of anonymity under sophisticated attack models such as the continuous query correlation attacks described above. We study the effectiveness of the mix-zones attacks and the proposed techniques through extensive experiments conducted using traces produced by GTMobiSim [33] on different scales of geographic maps.

The rest of the paper is organized as follows: We first introduce the concept and definition of mix-zones in Section 2 and provide an overview of various attacks to mix-zones in Section 3. In Section 4, we introduce attack resilient mix-zone design and construction techniques and analyze the privacy strength against the set of attack models described in Section 3. We highlight the effectiveness of our attack-resilient mix-zones through experimental evaluation in Section 5. The related work is discussed in Section 6 and we conclude in Section 7.

2 Mix-zones

In this section we introduce the concept and notations for basic mix-zones and road network mix-zones.

2.1 Mix-zone concepts

A mix-zone of k participants refers to a k-anonymization region in which users can change their pseudonyms such that the mapping between their old and new pseudonyms is not revealed. In a mix-zone, a set of k users enter in some order and change pseudonyms but none leave before all users enter the mix-zone. Inside the mix-zone, the users do not report their locations and they exit the mix-zone in an order different from their order of arrival, thus, providing unlinkability between their entering and exiting events.

The properties of a mix-zone can be formally stated as follows:

Definition 1 A mix-zone Z is said to provide k-anonymity to a set of users A iff

1. The set A has k or more members, i.e., $|A| \geq k$.
2. All users in A must enter the mix-zone Z before any user $i \in A$ exits. Thus, there exists a point in time where all k users of A are inside the zone.
3. Each user $i \in A$, entering the mix-zone Z through an entry point $e_i \in E$ and leaving at an exit point $o_i \in O$, spends a completely random duration of time inside.
4. The probability of transition between any point of entry to any point of exit follows a uniform distribution. i.e., a user entering through an entry point, $e \in E$, is equally likely to exit in any of the exit points, $o \in O$.

Figure 1 shows a mix-zone with three users entering with pseudonyms a, b and c and exiting with new pseudonyms, p, q and r. Given any user exiting with a new pseudonym, the adversary has equal probability of associating it with each of the old pseudonyms a, b and c and thus this example mix-zone provides an anonymity of $k = 3$. The uncertainty of an adversary to associate a new pseudonym of an outgoing user i' to its old pseudonym is captured by entropy, $H(i')$ which is the amount of information required to break the anonymity.

$$H(i') = -\sum_{j \in A} p_{i' \to j} \times log_2(p_{i' \to j})$$

where $p_{i' \to j}$ denotes the probability of mapping the new pseudonym, i' to an old pseudonym, j. When users change pseudonyms inside mix-zones along their trajectories, an adversary observing them loses the ability to track their movements.

2.2 Road network mix-zones

Unlike the theoretical mix-zones, mix-zones constructed at road intersections (Fig. 2) may violate some conditions. For instance, in a road network mix-zone, users do not stay random time inside while entering and exiting the mix-zone [18, 34]. Such violations provide additional information to the adversary in inferring the mapping between the old and new pseudonyms. Mix-zones constructed at road intersections have a limited number of ingress

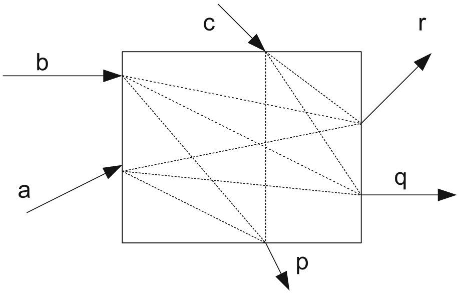


Fig. 1 Mix-zone model

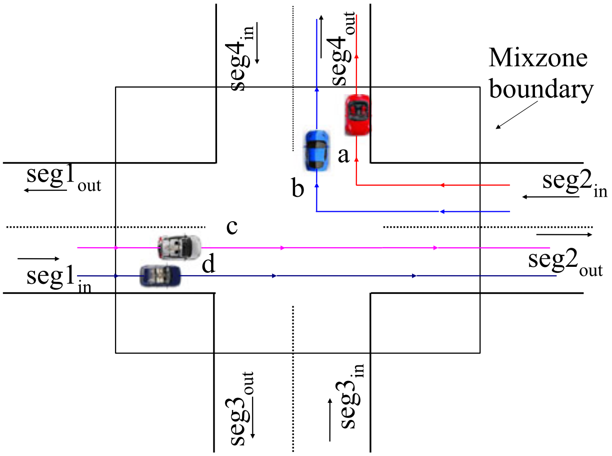


Fig. 2 Road network mix-zone

and egress points corresponding to the incoming and outgoing road segments of the intersection. Furthermore, users in a road network mix-zone are also constrained by the limited trajectory paths and speed of travel that are limited by the underlying road segments and the travel speed designated by their road class category [2]. Thus, users are not able to stay random time inside a road network mix-zone and no longer follow uniform transition probability when entering and exiting the mix-zone.

For example, in Fig. 2, users *a* and *b* enter the road intersection from segment 2 and turn on to segment 4. Users *c* and *d* enter from segment 1 and leave on segment 2. When user *a* and *b* exit the mix-zone on segment 4 with their new pseudonyms, say α and β, the attacker tries to map their new pseudonyms α and β to some of the old pseudonyms *a*, *b*, *c*, and *d* of the same users. The new pseudonym α is more likely to be mapped to two of the old pseudonyms, *a* or *b*, than the other pseudonyms because users *a* and *b* entered the mix-zone well ahead of users *c* and *d* and it is thus less probable for *c* and *d* to leave the mix-zone before users *a* and *b* given the speed and trajectory of travel. Here, the limited randomness on the time spent inside a road network mix-zone introduces more challenges to construct efficient mix-zones. Similarly, in Fig. 2, in order for the attacker to map α and β to *c* and *d*, the old pseudonyms, users *c* and *d* should have taken a left turn from segment 1 to segment 4 and users *a* and *b* should have taken a *U-turn* on segment 2. Based on common knowledge of inference, the attacker knows that the transition probability of a *U-turn* is small and the mapping of α and β to *c* and *d* is much less probable.

Thus, unlike theoretical mix-zones, the mapping probabilities in a road network mix-zone may violate the uniform probability distribution assumption. Thus, measuring just the entropy of mix-zone may not be sufficient for an accurate estimate of the achieved user privacy. Two systems can be shown to have the same entropy, but may provide different levels of anonymity when considered from an individual user's perspective [39]. In order to ensure that the distribution of the mapping probabilities approximates the uniform distribution, we argue to evaluate the quality of road network mix-zones, in addition to entropy. In other words, it is important to measure the deviation of the mapping probabilities in a pairwise fashion using pairwise entropy: for any two users *i* and *j* entering the mix-zone and exiting with new pseudonyms i' and j', the pairwise entropy for the mapping of an exiting user with pseudonym i' to an entering user with pseudonym *j* is defined as the entropy obtained by considering i and j to be the only members of the anonymity set. In that case, we have only two mapping probabilities: $p_{i' \to i}$, corresponding to the probability of mapping the new pseudonym i' to i and $p_{i' \to j}$, corresponding to the probability of mapping i' to j. If the probabilities $p_{i' \to i}$ and $p_{i' \to j}$ are equal, then i' is equally likely to be i or j. The attacker has the lowest certainty of linking the outgoing user i' to i or j (50 %). However, if one of the probabilities is much larger than the other, then the exiting user with the new pseudonym i' can be associated with the old pseudonym whose mapping probability is higher. Formally, let i and j denote the pseudonyms that the two users carry when entering a road network mix-zone, and i' and j' be the pseudonyms that the same two users carry when exiting the mix-zone. Then the pairwise entropy $H_{pair}(i, j)$ between users i and j is defined as follows:

$$H_{pair}(i, j) = -\left(p_{i' \to i} log p_{i' \to i} + p_{i' \to j} log p_{i' \to j}\right)$$

Note that $H_{pair}(i, j)$ and $H_{pair}(j, i)$ are not the same. $H_{pair}(i, j)$ measures the pairwise entropy between users i and j for the event of user i exiting as i' whereas $H_{pair}(j, i)$ measures the pairwise entropy between the users i and j during the exit of user j as j'.

In comparison, by Definition 1, a theoretical mix-zone ensures a uniform distribution for all possible mappings between old and new pseudonyms and the highest pairwise entropy of 1.0 for all pairs of users in the anonymity set. We argue that an effective road network mix-zone should provide a pairwise entropy close to 1.0 for all possible pairs of users in the anonymity set.

Next, we define the road network mix-zone as proposed by the MobiMix road network model [34] as follows:

Definition 2 A road network mix-zone offers k-anonymity to a set A of users if and only if:

1. There are k or more users in the anonymity set A.
2. Given any two users $i, j \in A$ and assuming i exiting at time t, the pairwise entropy after timing attack should satisfy the condition: $H_{pair}(i, j) \geq \alpha$.
3. For any two users $i, j \in A$, the pairwise entropy after transition attack should meet the condition: $H_{pair}(i, j) \geq \beta$.

3 Threat models and attacks

This section is dedicated to illustrate the vulnerabilities of basic mix-zones, such as road network based timing and transition attacks and continuous query correlation attacks (*CQ-attacks*) and present a formal analysis of the mix-zone anonymization problem.

3.1 Attacks based on road network characteristics

We describe three attack models based on the characteristics of road networks: (1) Timing Attack, (2) Transition Attack and (3) Combined timing and transition attack. The effect of attacks based on real world constraints had been studied ever since Beresford et.al. [11] proposed the mix-zone model. Freudiger et. al. [18] studied the effectiveness of the mix-zones on road networks and identified that the timing information and transition probability at the road intersection provide valuable information to the attacker for mapping the new pseudonym to the old pseudonym. Similarly, Buttyan et. al. [13] showed that the privacy obtained in the road network mix-zones is impacted by attacks related to the timing of the entry and exit events in a road network. The MobiMix road network mix-zone framework [34] developed a formal model of these attacks in road network mix-zones which are described below.

3.1.1 Timing attack

In timing attack, the attacker observes the time of entry, $t_{in}(i)$ and time of exit $t_{out}(i)$ for each user entering and exiting the mix-zone. When the attacker sees an user i' exiting, he tries to map i' to one of the users of the anonymity set, A_i. The attacker assigns a probability, $p_{i' \to j}$ that corresponds to the probability of mapping i' to j, where $j \in A$. The mapping probabilities are computed through inference based on the likelihoods of the rest of the users to exit at the exit time of i', denoted by $t_{out}(i')$. Once the mapping probabilities are computed, the attacker can utilize the skewness in the distribution of the mapping probabilities to eliminate some low probability mappings from consideration and narrow down his inference to only the high probable mappings. Consider an example anonymity set, $A = \{a, b, c\}$, let user a exit with a new pseudonym a' at $t_{out}(a')$ and let the likelihoods of a, b and c exiting at time $t_{out}(a')$ be 0.1, 0.09 and 0.05 respectively. In this case, we show that it is easy to compute the mapping probabilities based on these likelihoods: $p_{a' \to a} = \frac{0.1}{0.1+0.09+0.05} = 0.416$, $p_{a' \to b} = \frac{0.09}{0.1+0.09+0.05} = 0.375$ and $p_{a' \to c} = \frac{0.05}{0.1+0.09+0.05} = 0.208$. Thus, with the timing information, the attacker is able to find that $a' \to a$ is the most probable mapping and $a' \to c$ is least probable.

3.1.2 Transition attack

In transition attack, the attacker estimates the transition probability for each possible turn in the intersection based on previous observations. On seeing an exiting user, i', the attacker assigns the mapping probability $p_{i' \to j}$ for each $j \in A$ based on the conditional transitional probabilities $T((ingress(j), egress(i'))$. Transition attack can equally affect the effectiveness of road network mix-zones as timing attack if not handled with care.

3.1.3 Combined timing and transition attack

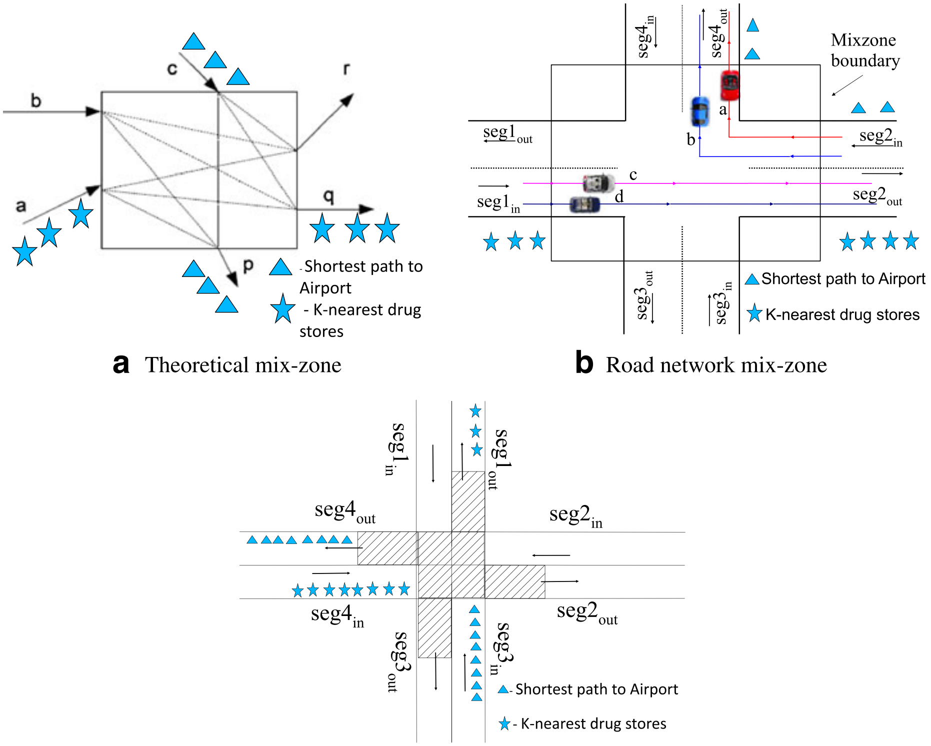
In the combined timing and transition attack model, the attacker is aware of both the entry and exit timing of the users and as well the transition probabilities at the road intersection for a given road network mix-zone. One can estimate the mapping probabilities $p_{i' \to j}$ for each $j \in A$ based on both the likelihoods of every user j exiting at time $t_{out}(i')$ and the conditional transition probabilities $T(ingress(j), egress(i'))$. This combined attack is often more powerful than the timing and transition attacks in isolation as it utilizes the information leaked by both timing and transition attacks.

3.2 Continuous query correlation attacks

We next discuss the class of attacks that are based on continuous query correlation. As discussed earlier, road network mix-zones are prone to CQ attacks when mobile users obtain continuous query services. When a user is executing a continuous query, even though her pseudonym is changed whenever she enters a road network mix-zone, an adversary may simply utilize the consecutive snapshots of the query to reveal the correlation between the old and new pseudonyms. To the best of our knowledge, all road network mix-zones are prone to CQ-attacks.

3.2.1 *Basic CQ-attack*

We first illustrate the basic CQ-attack which uses only query correlation between the consecutive snapshots of the continuous query to infer the mapping between the old and new pseudonyms. Consider the example in Fig. 3a where three users enter with pseudonyms a, b and c and exit with new pseudonyms p, q and r. The attacker finds that before entering the mix-zone, users a and b run continuous queries on obtaining nearest drug store and shortest path driving directions to the airport respectively. Upon their exits, the attacker again finds more instances of their corresponding continuous queries with different pseudonyms, q and r. Here, although users a and c change their pseudonyms to q and r, the continuous exposure of their CQ information breaks their anonymity. Similar attack can happen in a road network mix-zone as shown in Fig. 3b where three users with pseudonyms, a, b and c enter and leave the mix-zone. As users a and b are running continuous queries, the attacker finds an instance of $a's$ continuous query before entering the mix-zone and when user a exits with a new pseudonym, say α and receives another instance of the same query, the attacker infers that the new pseudonym α must correspond to the old pseudonym a. To the best of our knowledge, no existing road network mix-zone technique is free from CQ-attacks. For instance, we find in Fig. 3c that even the non-rectangular mix-zone [34] that is most effective against road network timing



a Theoretical mix-zone

b Road network mix-zone

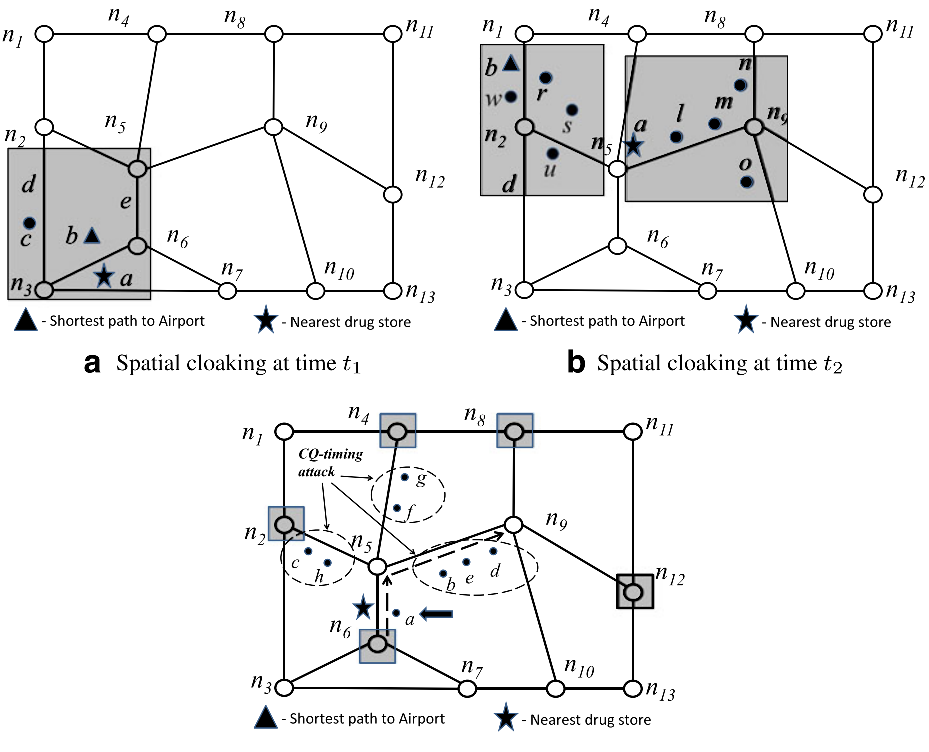
c Non-rectangular mix-zone

Fig. 3 Mix-zone anonymization and its risks under CQ-attack

attack is also prone to the CQ-attack. Next we briefly discuss the CQ-attacks on Spatial cloaking based solutions and describe how Spatial and temporal cloaking based techniques over Mix-zone networks lead to CQ-timing and CQ-transition attacks.

3.2.2 Spatial cloaking

In the spatial cloaking technique, the granularity of location exposure is reduced by exposing a larger spatial region containing the locations of k mobile users instead of the user's actual location [9, 20, 21]. In other words, the exposed location is indistinguishable from the locations of k or more users. However, for continuous queries, the spatial cloaking technique is vulnerable to query correlation based on the information across different snapshot instances of the continuous query. For example in Fig. 4a, we find users a and b asking continuous queries for nearest drug store and shortest path to airport at some time instance t. The conventional spatial cloaking algorithm finds a cloaking box encompassing the locations of a and b with the locations of three other users, c, d and e so that the users obtain *location k-anonymity* corresponding to a k value of 5. As the spatial cloaking algorithm lacks knowledge of the continuous query correlation attack, at a later point in time, say time $t + \delta t$, when users a and b have moved far from each other, it may cloak users a and b using different cloaking boxes that only ensures location k anonymity (Fig. 4b). Therefore, we find user a's location is cloaked with the locations of l, m, n and o and similarly, the location



a Spatial cloaking at time t_1 **b** Spatial cloaking at time t_2

c CQ Cloaking on Mix-zones

Fig. 4 Continuous query: spatial cloaking based techniques

of user b is cloaked using the locations of users r, s, u and w. Using query correlation, the attacker will be able to compare consecutive cloaking boxes and infer that user a is issuing the continuous query to nearest drug store as a is the only common user between the two cloaking boxes. Similarly the adversary can infer that b is the user executing the continuous query on the shortest path driving directions to the airport. Next we discuss a similar cloaking based approach for anonymizing continuous queries in a mix-zone framework and show how it leads to CQ-timing and CQ-transition attacks.

3.2.3 Mix-zone based CQ anonymization

In the CQ-cloaking approach in a mix-zone framework, the continuous queries are either temporally or spatially perturbed while the snapshot queries continue to be unperturbed. The locations used by the CQ is perturbed such that a continuous query originating from a mix-zone is indistinguishable from at least k users traversing the mix-zone. While this technique does not make changes to the mix-zone model, we show that it makes the CQ anonymization susceptible to CQ-timing attack and CQ-transition attack.

Consider the example shown in Fig. 4c where we have a CQ labeled as star. The square nodes represent road network mix-zones. We observe the star CQ trace starting from the mix-zone at road junction n_6. Each star represents one snapshot execution of the corresponding CQ. Intuitively, if we delay the execution of the individual CQ snapshots of CQ users starting at mix-zone n_6 such that at least k_c users leave the mix-zone within the temporal delay, it will make it harder for an adversary to associate the CQ-induced trajectory with the corresponding CQ user. For instance, in Fig. 4c, if the continuous query on the shortest path to the airport (marked by stars) originating from the mix-zone n_6 is perturbed spatially or temporally in such a way that there are k or more users coming out of the mix-zone at road junction n_6 within the continuous query's spatial cloaking region (or temporal cloaking window), then from the attacker's perspective, the query could have originated from any of the k users who entered the mix-zone within the time window. Both CQ-spatial cloaking (CQ-s) and CQ-temporal cloaking (CQ-t) are similar in principle, however in CQ-spatial cloaking, instead of delaying the snapshots, the CQ exposes a larger spatial region such that there are k or more users within the spatial region.

CQ-timing attack CQ-cloaking techniques are vulnerable to CQ-timing attack when users in the anonymity set violate the steady motion assumption, i.e., if all users do not travel at the imposed speed of the road segment. In the example shown in Fig. 4c, we find that users with pseudonyms a, b, c, d, e, f, g and h enter the mix-zone during the continuous query's temporal cloaking window, d_{tmax}. When the steady motion assumption fails, user a travels slowly and stays on segment $\overline{n_5n_6}$ while other users move ahead of the segment, $\overline{n_5n_6}$. If user a is the issuer of the continuous query, then the continuous query would stay on segment, $\overline{n_5n_6}$ even though it is executed with a temporal delay while other users of the anonymity set move ahead. By observing this, the attacker can eliminate the low probability members and identify the issuer of the continuous query with high confidence.

CQ-transition attack CQ-cloaking techniques are prone to another vulnerability namely CQ-transition attack. When the transitions taken by a subset of the users in the anonymity set differ from that of the user executing the query, then those members can be eliminated from consideration. For example, in Fig. 4c, at road intersection n_5, users c and h take a left turn on to the road segment, $\overline{n_2n_5}$ whereas users f and g move straight on segment, $\overline{n_4n_5}$

and users b, e and d turn right on to segment, $\overline{n_5n_9}$. When the continuous query uses CQ-temporal cloaking or CQ-spatial cloaking and follows the querying user after a temporal delay or using a spatial cloaking region, from the transition taken by the continuous query, from segment, $\overline{n_6n_5}$ to $\overline{n_9n_5}$, the adversary will be able to eliminate the users, c, h, f and g from consideration as their transitions differ from that of the continuous query.

4 Attack-resilient mix-zone techniques

In this section, we discuss the techniques for mix-zone construction, which are resilient to the above mentioned attacks. We first discuss how to construct road network mix-zones with resilience to road network based timing attack.

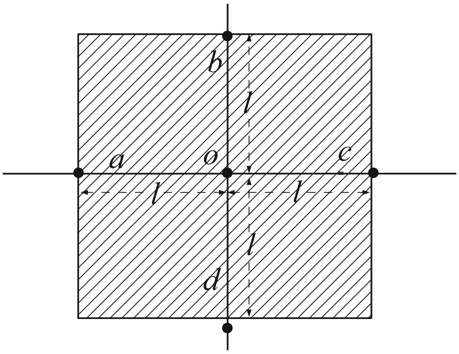
4.1 Constructing mix-zones resilient to timing attack

A majority of existing mix-zone proposals adopt a straightforward approach to construct mix-zones around the road junction using a rectangular or circular region centered at the road junction as shown in Fig. 5. We argue that such a straightforward approach has detrimental effects on the level of anonymity and privacy obtained. We first analyze the weaknesses of the straightforward naive rectangular mix-zone approach and then discuss three MobiMix mix-zone construction techniques that consider the geometry of the zones and their impact on the resilience to timing attack in the mix-zone construction process. Concretely, we discuss: (i) Time Window Bounded(TWB) Rectangular, (ii) Time Window Bounded(TWB) Shifted Rectangular and (iii) Time Window Bounded(TWB) Non-rectangular mix-zones. All perform better than the naive Rectangular mix-zones under timing attack.

4.1.1 Naive rectangular mix-zones

A straightforward approach to construct mix-zones around the road junction is to define a rectangular region centered at the road junction as shown in Fig. 2. The size of the rectangle is defined based on some system supplied default value. For each exiting user i', the set of users that were inside the mix-zone at any given time during user i''s presence in the mix-zone forms its anonymity set, A_i. Thus, any two users that were present together at any given time, become members of each other's anonymity sets.

Fig. 5 Rectangular mix-zone



Timing attack is highly effective in such Naive Rectangular Mix-zones. This is because in Naive Rectangular mix-zones, even when the anonymity set size is typically large, a majority of members of the anonymity set become low probable under the timing attack. For instance, in Fig. 5, consider two users i and j entering from the segments a into the mix-zone. Let user i exit with a new pseudonym i' on segment c and assume the four road segments in the mix-zone, a, b, c and d, have the same speed distribution. If the arrival times of i and j differ by a large value, then even though users i and j might have been present together in the mix-zone for some amount of time, the attacker may infer that the user who entered first is more likely to exit first and that it is unlikely for j to exit before i exits the mix-zone. Therefore, the pairwise entropy of the naive rectangular mix-zones is low under timing attack, making such naive rectangle mix-zones more vulnerable under timing attacks.

4.1.2 TWB rectangular mix-zones

To overcome the problem inherent in the naive rectangle mix-zones, a time-window bounded approach is proposed [13, 18, 19]. In the time window bounded approach, the rectangle is constructed in the same way as in the naive rectangular mix-zone, however, the anonymity set for each user i is assumed to comprise of only users who had entered the mix-zone within a time window in the interval, $t_{in}(i) - \tau_1$ to $t_{in}(i) + \tau_2$. Here, $t_{in}(i)$ is the arrival time of user i and τ_1 and τ_2 are chosen to be small values so that the time window ensures that the anonymity set of i comprises of only those users who are entering the mix-zone with a closely similar arrival time as the arrival time of i, defined by the time window. Hence, when i exits the mix-zone as i', the attacker would have hard time to differentiate i' from all members of i's anonymity set, A_i, as they are all likely to exit at the same time when i exits.

A challenge to the time window based rectangular mix-zones is how to determine the right size of the time window. Although, the notion of mix-zone time window has been adopted in several existing mix-zone proposals [13, 18, 19], they all use a system-supplied default value for the time window length for all the junctions. We argue that it should be decided based on a number of factors including the characteristics of the road junctions, the mix-zone size, the speed distribution of users on the road segments and the level of anonymity users expect, so as to guarantee a lower-bound pairwise entropy. Concretely, for road intersections that have segments with the same speed distributions, we can precisely guarantee a lower-bound on the pairwise entropy for the members of the anonymity set by constructing the anonymity set with the right length of time window based on our MobiMix road network model [34].

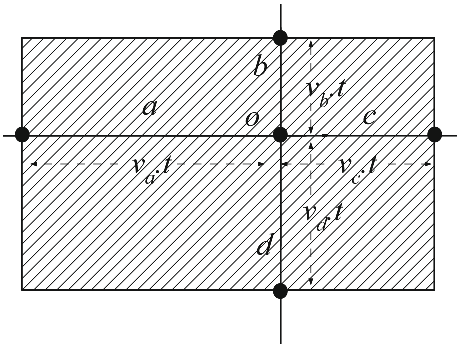
However, when the segments of the road intersection have different mean speeds (e.g., when they belong to different road classes), the attacker may be able to eliminate some mappings based on the timing information. For example, in Fig. 5, let us assume a mix-zone of size 0.5 miles × 0.5 miles with segments a and c of residential road category having a mean speed of 20 mph and segments b and d of highway roads with a mean speed of 60 mph. Consider two users i and j entering the mix-zone at the same time. Let user i enter through the highway segment b and exit through the highway segment d, and let user j enter though the residential segment a and exit through the residential segment c. If both i and j travel around the mean speed of their respective road segments, then i and j would exit approximately in 30 sec and 90 sec respectively. When user i exits the mix-zone with a new pseudonym i' in 30 sec, the attacker can infer that i' is more likely to be i than j. Thus, even though the anonymity set consists of users entering with closely similar arrival times, the difference in the speed distribution on the roads causes the default window size to be ineffective, making the window based rectangular mix-zones vulnerable to the timing attacks.

4.1.3 TWB shifted rectangular mix-zones

To address the above mentioned vulnerabilities against timing attacks, a time window bounded shifted rectangular approach is proposed [34]. In the Time window bounded shifted rectangular approach, the rectangle is not centered at the center of the junction, instead it is shifted in such a way that for all users in the anonymity set, from any point of their entry into the mix-zone, it takes the same amount of time for them to reach the center of the road junction when traveling at the mean speed of the road segments. Similarly, from the center of the junction, it takes the same amount of time for the members of the anonymity set to reach any exit point when travelling at the mean speed of the road segments. In a shifted rectangular mix-zone, a set of users entering within the short time window, $t_{in}(i) - \tau_1$ to $t_{in}(i) + \tau_2$, are likely to exit the mix-zone at the same time. Hence, when user i exits as i', the attacker could not infer which member in the anonymity set, A_i, will be the best match for i' since i' is likely to be any of the members of A_i. If t represents the average time to reach the center of the road junction from an entry point which is the same as the average time to reach an exit point from the junction center, then the mix-zone lengths on the segments will be given by the product of their mean speed, say v and the average time, t as shown in Fig. 6. Compared to naive rectangular and time window bounded rectangular mix-zones, shifted rectangular mix-zones provide good pairwise entropy for many cases, however, they remain to be vulnerable and leak information when the speed of the users deviates from the mean speed.

For example, in Fig. 6, consider a mix-zone of size 0.5 miles × 0.5 miles in a road intersection with a slow residential road segment, a having mean speed 20 mph and three other highway segments, b, c, and d having mean speed 60 mph. Let all road segments have a standard deviation of 10 mph from their mean speed. The computation would yield $v_a.t = 0.375$ miles and $v_b.t = v_c.t = v_d.t = 0.125$ miles. Let users i and j enter the mix-zone at the same time. Let user i enter through the highway segment, b and exit through the highway segment, d and let j enter through the residential road segment, a and exit through the highway segment, c. Let us assume user j travels with a speed of 10 mph on segment a and travels at 60 mph on segment, c. In this case, the attacker would see j' exiting in 2 min, 32.5 sec. With this timing information, the attacker can find that j' is more likely to be mapped to j than i because if j' is i, then i should have travelled really slow on the highway segments b and c, with an average speed of 5.9 mph in order to exit after 2 min,

Fig. 6 Shifted rectangular mix-zone



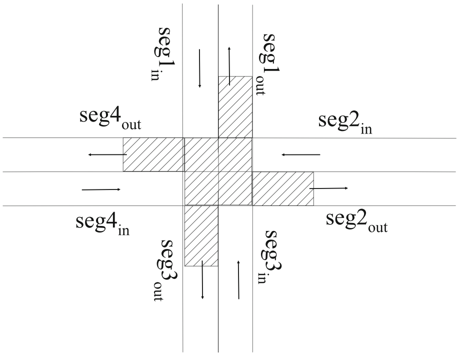


Fig. 7 Non-rectangular mix-zone

32.5 sec. However, if j' is j, then j needs to have travelled only at 10 mph on the residential road segment, a which is more likely to happen. Thus, the attacker can guess that j' is j with high confidence. In general, the shifted rectangular approach performs badly when the user's speed deviates from the mean speed of the road segments.

4.1.4 TWB non-rectangular mix-zones

A more effective way to construct mix-zones would be to have the mix-zone region start from the center of the junction only on the outgoing road segments as shown in Fig. 7. We refer to this technique as non-rectangular approach. The non-rectangular approach is free from timing attacks caused by the heterogeneity in the speed distribution on the road segments. As in the rectangular approaches, the anonymity set for each user, i comprises of users who had entered the mix-zone within a time window in the interval, $|t_{in}(i) - \tau_1|$ to $|t_{in}(i) + \tau_2|$. The length of the mix-zone along each outgoing segment is chosen based on the mean speed of the road segment, the size of the chosen time window and the minimum pairwise entropy required.

Proof of timing attack-resilience The TWB non-rectangular mix-zone is most resilient to timing attacks as it does not encounter any disparity in the speed distributions. Here, as long as a pair of users enter within each other's time window, the mapping probabilities will be similar to each other. For instance, if user i and j enter the mix-zone and exit with new pseudonyms i' and j', the mapping probabilities $p_{i' \to i}$ and $p_{i' \to j}$ corresponding to the exit of i as i' will be similar to each other. Precisely, the length of the mix-zone determines how closely similar are the two mapping probabilities. By suitably choosing a mix-zone region length, one can control the similarity of the two mapping probabilities, $p_{i' \to i}$ and $p_{i' \to j}$. In other words, we can obtain a high lower bound on the pairwise entropy, $H_{pair}(i, j)$. Therefore $H_{pair}(i, j)$ will be always greater than the required minimum value α (refer Definition 2). Thus for any set of k users entering the mix-zone, the mix-zone ensures a high pairwise entropy between each of them, forming an effective anonymity set.

4.2 Resilience to mix-zone transition attack

We next discuss attack-resilient mix-zone construction to deal with transition attacks. As discussed earlier, in a road network, it is possible to launch transition attack to guess the linking between the pseudonyms. For each exiting user, i' the attacker observes the exiting segment of i' and tries to map i' to one of the users, j in the anonymity set based on the conditional transitional probability of exiting in the outgoing segment, $oseg(i)$ given that j entered from the incoming segment, $iseg(j)$. In order to protect against transition attack in cases where the transition probability is skewed, the transition attack resilient technique in [35] proposes that the mix-zone time window should be chosen in such a way that for each outgoing segment, l, there are enough number of users (k or more) entering the mix-zone from the road segments that have similar transitioning probability to the outgoing segment, l, and hence have a higher pairwise entropy, say greater than or equal to β. Therefore, the attacker will have at least k users in the anonymity set that he cannot ignore from consideration.

Proof of transition attack-resilience Given that for each outgoing segment, l, the mix-zone ensures that there are k or more users entering with a similar transitioning probability to segment l, the mapping probabilities $p_{i' \to i}$ and $p_{i' \to j}$ corresponding to the exit of i as i' will be similar to each other. Thus, it results in a high pairwise entropy, $H_{pair}(i, j)$ between each of those k users. Therefore referring to Definition 2, the pairwise entropy $H_{pair}(i, j)$ will be always greater than the required minimum value β and thus the mix-zone protects against transition attack.

4.3 Resilience to CQ-attacks

CQ-attack by far is the most challenging attack in a road network mix-zone. To the best of our knowledge, no road network mix-zone is completely free from CQ-attacks. However, the goal for designing CQ-attack resilient solutions is to increase the anonymity strengths of the mix-zones by considering the fact that the attacker has the continuous query correlation information at the intermediate mix-zones to infer and associate the CQ induced trajectory with its user. Note that the initial anonymity forms the major component of the anonymity under the CQ-attack model as the attacker breaks the anonymity obtained in the intermediate mix-zones and therefore it is important that the mix-zones provide high initial anonymity for the continuous queries so that even when the attacker breaks the anonymity in the subsequent mix-zones, the initial anonymity remains sufficient to meet the required privacy level.

Proof of CQ-attack resilience When a user executes a continuous query, it induces a trajectory corresponding to the movement of the user even though the user's pseudonym is changed whenever she crosses a road network mix-zone. In the proposed mix-zone anonymization model, any mobile user who wishes to obtain CQ service first moves to the nearest mix-zone and starts to run the CQ service from the mix-zone. Since the CQ originates from a mix-zone, the CQ is anonymized with a set of k users in the mix-zone. Here, the attacker becomes confused to associate the continuous query with the actual user as each of the user in the mix-zone has equal likelihood of starting the continuous query. Hence the continuous query obtains an initial anonymity of k. However, it should be noted that at the subsequent mix-zones, the query correlation reveals the mapping between the old and new pseudonyms of the continuous query and hence the intermediate mix-zones do not effectively contribute to the anonynmity.

Thus for a continuous query, its initial anonymity forms the major component and intermediate mix-zones add anonymity only when users in the intermediate mix-zones ask the same query. For instance, if m out of the k users traversing an intermediate mix-zone run continuous queries and if there are R number of unique continuous queries run by the m users and if A^r is the set of users running the continuous query, Q_r, $1 \leq r \leq R$, then the entropy of each continuous query user, i executing the query, Q_r and exiting the mix-zone with a new pseudonym, i' is given by

$$H(i) = -\sum_{j \in A^r} p_{i' \to j} \times log_2 \left(p_{i' \to j} \right)$$

where $p_{i' \to j}$ denotes the probability of mapping the user exiting with the new pseudonym, i' to an old pseudonym, j that runs the same continuous query. Therefore, for a user starting to execute a CQ from mix-zone m_1, if f_i users out of the m_i continuous query users in the i^{th} mix-zone execute the same CQ, then the entropy X of the user executing the continuous query is given by

$$X = log|k_1 - m_1| + \sum_{2 \leq i \leq n} log|f_i|$$

where $log|k_1 - m_1|$ represents the initial anonymity of the user while starting the continuous query in mix-zone, m_1.

The delay-tolerant mix-zones we discuss next combine mix-zone based identity privacy protection with location mixing to achieve high initial anonymity for the continuous queries that is otherwise not possible with conventional mix-zones. In the delay-tolerant mix-zone model, users expose spatially or temporally perturbed locations outside the mix-zone area. However, on the exit of each delay tolerant mix-zone, the mix-zone changes their perturbed locations by introducing a random temporal shift (temporal delay-tolerant mix-zones) or a random spatial shift (spatial resolution-tolerant mix-zones) to their already perturbed locations. While conventional mix-zones only change pseudonyms inside them, the additional ability of delay-tolerant mix-zones to change and mix user locations brings greater opportunities for creating anonymity. Therefore, the anonymity strength of delay-tolerant mix-zones comes from a unique combination of both identity mixing and location mixing. Such high anonymity provides the initial anonymity required to anonymize the continuous queries so that the queries obtain the required anonymity even under the CQ-attack model. Given that the delay-tolerant mix-zone provides a high initial anonymity, k which is the required level of anonymity for the continuous query, the query meets the anonymity levels even though the intermediate mix-zones may not provide any effective anonymity under the CQ-attack model. Thus the proposed CQ-anonymization scheme is CQ-attack resilient.

4.4 Delay-tolerant mix-zones

We first illustrate the concept of delay-tolerant mix-zones with an example temporal delay-tolerant mix-zone. Table 1 shows the entry and exit time of users in a conventional rectangular road network mix-zone. We find that user a enters the mix-zone as $t = 100$ and exits at time $t = 104$. Similarly the other users enter and exit as shown in Table 1. Here the adversary may know that the average time taken by the users to cross the mix-zone is 4 sec. Therefore when user a exits at a' at time $t = 104$, the attacker can eliminate users e and f from consideration as they have not even entered the mix-zone by the time user a exits[2]. Similarly, the adversary can eliminate users o and n from consideration based on timing inference that users o and n have exited the mix-zone by the time a and b enter the mix-zone. Therefore when a exits as a', the attacker has uncertainty only among the users

[2] For the sake of example simplicity, we assume that the users take the average time of 4 s to cross the mix-zone, in a real road intersection, it could actually take slightly longer or shorter time to cross based on the speed of travel.

Table 1 Conventional road network mix-zone

User	t_{in}	t_{inside}	t_{out}
o	94	4	98
n	96	4	100
m	98	4	102
a	100	4	104
b	101	4	105
c	103	4	107
d	103	4	107
e	106	4	110
f	108	4	112

$\{a, b, c, d, m\}$. Also, among the users $\{a, b, c, d, m\}$, the attacker can eliminate more users through sophisticated reasoning based on timing inference described later.

However, in the delay-tolerant mix-zone model, each user uses a temporal delay, d_t within some maximum tolerance, d_{tmax}. Inside the mix-zone, the temporally perturbed location of each user is assigned a random temporal shift. In the delay-tolerant mix-zone example shown in Table 2, we find that user a initially uses a temporal delay, d_{told} of 4 sec and inside the mix-zone it is shifted randomly to 16 sec. Here d_{tmax} is assumed as 20 sec. Therefore when user a exits as a', it becomes possible that many users can potentially exit in the exit time of user a. The example in Table 2 shows one possible assignment of new temporal delays, d_{tnew} for other users in order for them to exit at the same time as a'. Thus, during the exit of user a as a', the attacker is confused to associate the exiting user a' with the members of the anonymity set, $\{a, b, c, d, e, f, g, h, i, j, k, m, n\}$. In principle, users' new temporal delays, d_{tnew} are randomly shifted inside the mix-zone ensuring the possibility of each of the users to exit at the exit time of each other and thus the delay-tolerant mix-zone model provides significantly higher anonymity compared to conventional mix-zones. Such high anonymity provides the initial anonymity required for the continuous queries under the CQ-attack model.

4.4.1 Temporal delay-tolerant mix-zones

In a temporal delay tolerant mix-zone, every mobile user delays the location exposure with a randomly chosen delay, d_t within the maximum temporal tolerance, d_{tmax}. The temporal time window, d_{tmax} is chosen based on the arrival rate of the users in the road junction so as to ensure an expected number of users arriving into the mix-zone within the temporal tolerance, d_{tmax}. Note that the random delay used by a mobile client does not change during its travel between mix-zones. Only when the mobile client enters a new mix-zone, its temporal delay is randomly shifted to a new value within the temporal window, d_{tmax}.

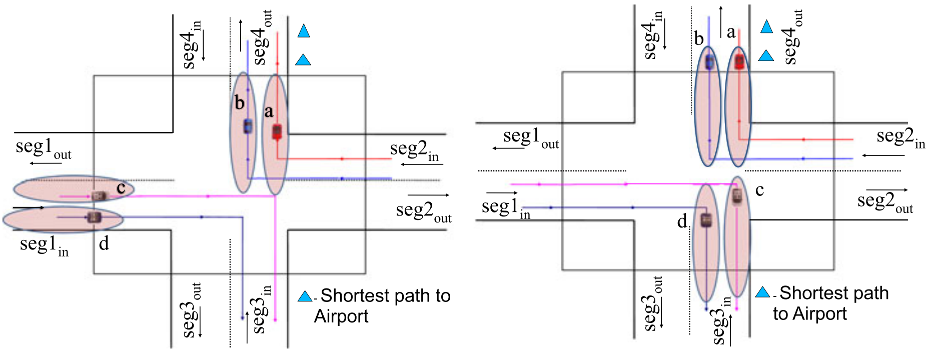
As it is intuitive, for an exiting user, i', the number of users in the effective anonymity set (i.e., those members that have high pairwise entropy with each other and with i') is directly proportional to the temporal tolerance, d_{tmax}, ie., the greater the temporal tolerance value, d_{tmax}, the more the number of users that could possibly resemble i during the exit of i' with a high pairwise entropy. Thus by varying the temporal tolerance, d_{tmax} the temporal delay tolerant-mix-zones can offer any desired level of anonymity to the users.

Table 2 An example temporal delay-tolerant mixing

User	Observed t_{in}	t_{inside}	d_{told}	d_{tnew}	Observed t_{out}
w	81	4	4	20	105
v	84	4	7	20	108
u	84	4	7	20	108
s	87	4	10	20	111
r	89	4	12	20	113
q	90	4	13	20	114
p	92	4	15	20	116
o	94	4	18	20	118
n	96	4	19	20	120
m	98	4	20	18	120
a	100	4	4	16	120
b	101	4	4	15	120
c	103	4	7	13	120
d	103	4	7	13	120
e	106	4	10	10	120
f	108	4	12	8	120
g	109	4	13	7	120
h	111	4	15	5	120
i	113	4	18	3	120
j	115	4	19	1	120
k	117	4	20	0	120
l	118	4	20	0	121

4.4.2 Spatial resolution-tolerant mix-zones

The second class of mix-zones based on the concept of delay-tolerance is the spatial resolution-tolerant mix-zone. Unlike the temporal delay-tolerant mix-zones, in the spatial resolution-tolerant mix-zone approach, users' locations are instantaneously sent out using a spatial region instead of the exact point location. Here, the spatial region masks the exact time of traversal of the user inside the mix-zone ensuring the possibility that the user could be located at any point within the spatial region. This ensures that the adversary can not infer the exact time of traversal of the user. The spatial region is constructed by first identifying the temporal window size, d_{tmax} based on the arrival rate of the users in the mix-zone and by translating the user's current location into a spatial region based on the temporal window size, d_{tmax}. A spatial region corresponding to a temporal window size d_{tmax} includes all road segments that can be reached within d_{tmax} units of time (i.e., the corresponding d_l units of length) from the center of the region when travelled at the mean speed of the road segments. The delay-proportional spatial cloaking algorithm described in Algorithm 1 computes the spatial region in such a way that the distance from the center of the spatial region and the location of the mobile user exactly corresponds to the spatial distance, d_l proportional to the temporal delay, d_t of the user in the temporal delay-tolerant approach. Inside the delay-tolerant mix-zone, the spatial regions of the users are randomly changed by introducing a spatial shift (Fig. 8).



a Before spatial location-mixing **b** After spatial location-mixing

Fig. 8 Illustration of spatial resolution-tolerant mix-zones

We note that the spatial resolution-tolerant mix-zone approach does not incur temporal delays, however they lead to higher query processing cost that is directly proportional to the size of the spatial regions. In the next subsection, we discuss spatio-temporal delay-tolerant mix-zones that yield suitable tradeoffs between the incurred delay and the cost of query processing.

Algorithm 1 Delay-proportional Spatial Cloaking

```
$d_{tmax}$: continuous query temporal window
$v$: vertex $v$ corresponds to the road junction $v$
$pathtime_v$: mean travel time to vertex $v$ from starting mix-zone, if $v$ is the mix-zone junction, then $pathtime_v = 0$
$region$: is a global list of road segments representing the cloaking region. It is empty at beginning and represents the cloaking region when the algorithm terminates
procedure FINDCLOAKREGION($d_{tmax}$, $pathtime_v$, $v$)
    for all $segments(v, u) \in segs(v)$ do
        $pathtime_u = pathtime_v + \frac{length(v,u)}{speed(v,u)}$
        if $(pathtime_u < d_{tmax})$ then
            if $(region.contains(v, u) == false)$ then
                $region.add(v, u)$
                FindCloakRegion$(d_{tmax}, pathtime_u, u)$
            end if
        end if
    end for
end procedure
```

4.4.3 Spatio-temporal delay-tolerant mix-zones

In the spatio-temporal delay-tolerant mix-zone approach, user locations are perturbed using both a temporal delay as well as a spatial region instead of the exact point location and the mix-zone introduces both random temporal and spatial shifts to the spatio-temporally perturbed user locations. Therefore, to an adversary observing an user, the user could have been located at any point in the spatial region at any instance of time during the temporal time window. Thus, the spatio-temporal delay-tolerant mix-zones effectively combine temporal delay-tolerant and spatial delay tolerant mix-zones to obtain the highest anonymity for continuous queries while making acceptable tradeoff between anonymous query processing cost and temporal delay incurred in anonymous query processing.

Overall, the road network mix-zones enhanced with the concept of delay-tolerant mixing provides the level of anonymity required to meet the strong privacy requirements under the CQ-attack model.

5 Experimental evaluation

In this section, we present the experiments on the effectiveness of the various attack resilient mix-zone techniques on road networks and discuss the level of privacy provided by them. We first describe the experimental setup and the road-network mobile object simulator used in the experiments.

5.1 Experimental setup

We use the GT Mobile simulator [33] to generate a trace of cars moving on a real-world road network, obtained from maps available at the National Mapping Division of the USGS [2]. The simulator extracts the road network based on three types of roads – *expressway*, *arterial* and *collector* roads. Our experimentation uses maps from three geographic regions namely that of Chamblee and Northwest Atlanta regions of Georgia and San Jose West region of California to generate traces for a two hour duration. We generate a set of 10,000 cars on the road network that are randomly placed on the road network according to a uniform distribution. Cars generate random trips with source and destination chosen randomly and shortest path routing is used to route the cars for the random trips. The speed of the cars are distributed based on the road class categories as shown in Table 3.

5.2 Resilience to mix-zone timing attack

We first measure the resilience of the various techniques to timing attacks based on road network characteristics. Figure 9 shows the average and worst-case pairwise entropy of the mix-zones for various values of k, the size of the anonymity set. In Fig. 9a, we observe that the effect of timing attack is different across various approaches: we find that the TWB non-rectangular mix-zones perform the best under timing attack with the average pairwise entropy close to 1.0. Here, the length of the non-rectangular mix-zone is computed so as to ensure a lower bound pairwise entropy of $\alpha = 0.9$ for the chosen time window size, τ which is computed based on the user arrival rate in the road junction to ensure the expected value of k with a high probability of $p = 0.9$. In order to compare the effectiveness of the other mix-zone approaches with the TWB non-rectangular approach, the TWB rectangular and TWB shifted rectangular mix-zones are also constructed with the same length and time window as used by the non-rectangular mix-zone. Similarly, the size of the naive rectangular

Table 3 Motion parameters

Road type	Expressway	Arterial	Collector
Mean speed (mph)	60	50	25
Std. dev.(mph)	20	15	10
Speed distribution	Gaussian	Gaussian	Gaussian

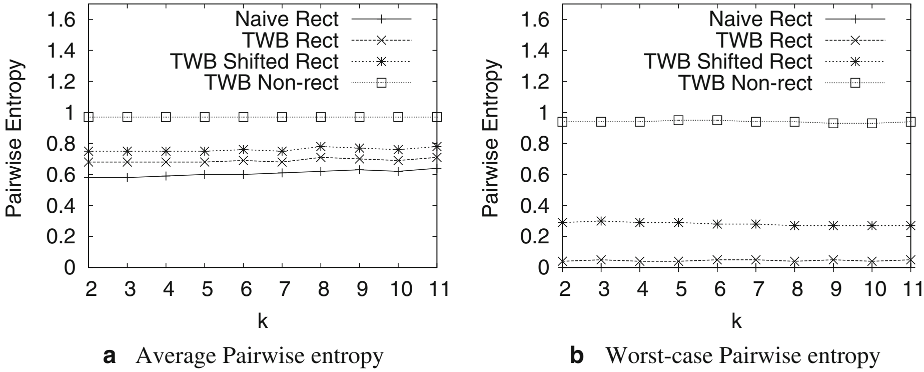


Fig. 9 Resilience to timing attack

mix-zone is fixed in such a way that the mean time to cross the mix-zone equals the time window of the TWB non-rectangular mix-zone.

In Fig. 9a, we also find that the naive rectangular and time window bounded rectangular mix-zones have low pairwise entropies after timing attack but the pairwise entropy of the TWB shifted rectangular approach is relatively higher, close to 0.8 as its geometry is more resilient to timing attack. However, a high pairwise entropy of 0.9 or higher may be often required to ensure strong anonymity. In such cases, the time window bounded non-rectangular approach becomes the most efficient choice. The worst case pairwise entropy in Fig. 9b represents the lowest possible pairwise entropy obtained by the users after timing attack. Here also, only the TWB non-rectangular approach offers a high value for the worst case pairwise entropy.

5.2.1 Success rate and relative anonymity of road-network attack-resilient mix-zones

In order to measure the effectiveness of the mix-zone techniques against road network-specific attacks, we study the success rate of them in providing the expected value of k. Here, the expected probability of getting k or more users, p is taken to be 0.9 and the value of k is varied from 2 to 11. Figure 10a shows the comparison of the success rate among

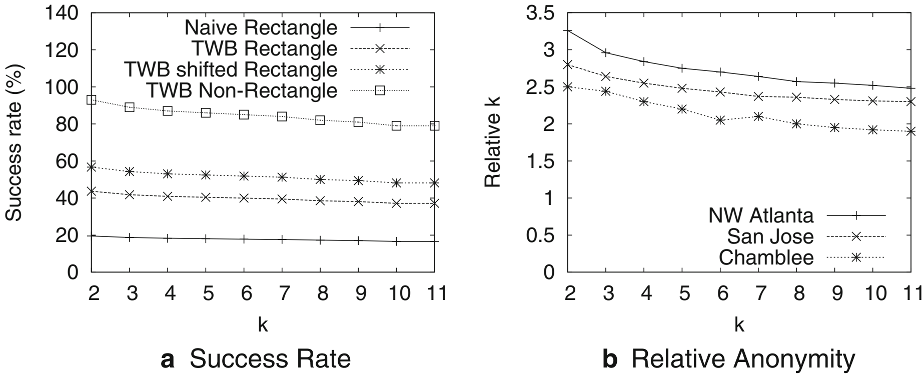
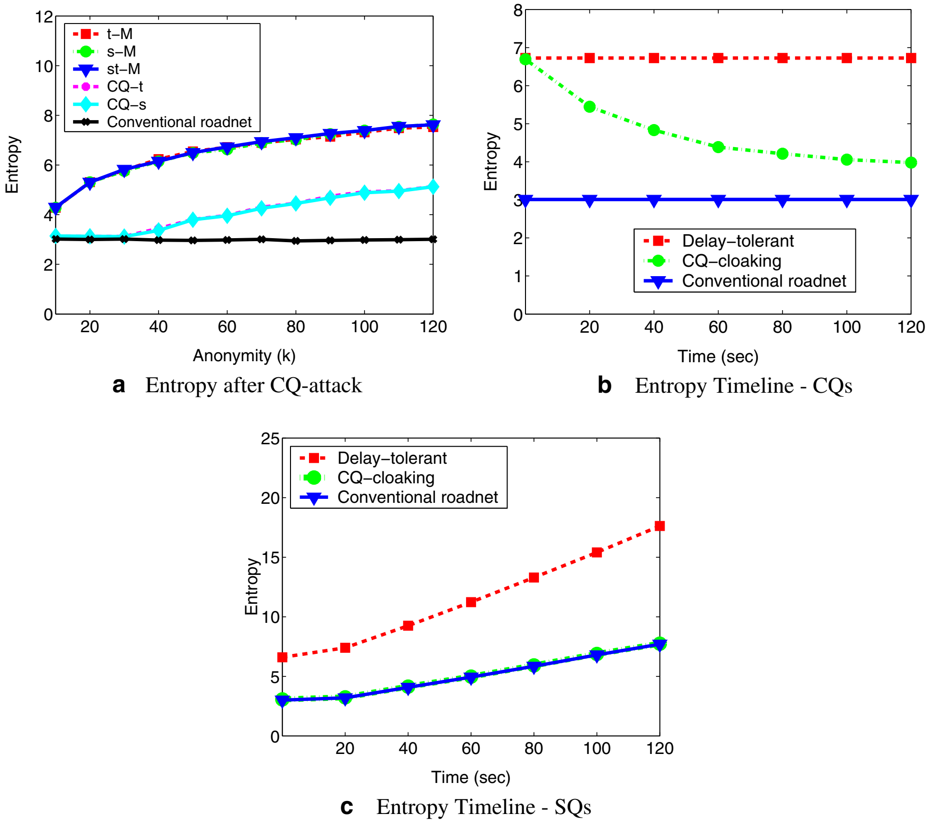


Fig. 10 Success rate and relative-k

the mix-zone approaches. A mix-zone is considered successful for an user if the user has at least *k* other users in its anonymity set with pairwise entropies greater than 0.9 under both timing and transition attacks. As evident from the Figure, the TWB non-rectangular mix-zones have the highest success rate, the other mix-zones have low success rate due to their lack of resilience to timing attack. In order to compare the level of anonymity offered by the mix-zones with the anonymity expected from them, we measure relative anonymity which is defined as the ratio of the value of obtained *k* to the value of expected *k*. Figure 10b shows the variation of relative-*k* of TWB non-rectangular mix-zones with respect to the expected value of *k* for different geographic maps. The expected success rate is set to 90 %. The graphs show that the value of relative *k* lies within the range of 2 to 3, meaning that the mix-zone on an average offers two to three times the anonymity requested by the users.

5.3 Resilience to CQ-attacks

This set of experiments compares the CQ-attack resilient mix-zones namely delay-tolerant mix-zones with the conventional mix-zones and CQ-cloaking techniques in terms of their anonymity under CQ-attack measured by entropy. Here, the delay-tolerant mix-zones are constructed over a conventional road network mix-zone whose size is chosen to offer an anonymity of 4. In Fig. 11a, we compare the average entropy of the temporal delay-tolerant,



a Entropy after CQ-attack

b Entropy Timeline - CQs

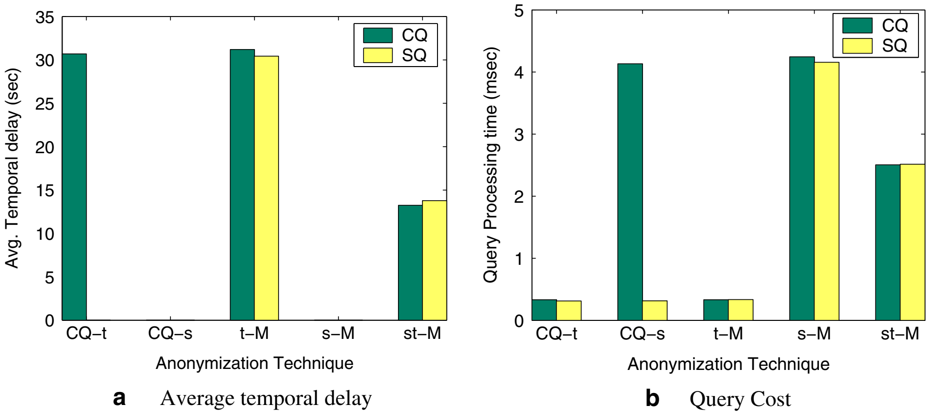
c Entropy Timeline - SQs

Fig. 11 Comparison with conventional mix-zones

spatial resolution-tolerant and spatio-temporal delay-tolerant mix-zone approaches (t-M, s-M, and st-M) with the conventional mix-zone approach and the temporal and spatial CQ-cloaking approaches (CQ-t and CQ-s) for various values of required anonymity, k. Here, the temporal window and spatial region size are chosen based on the arrival rate of the users in the mix-zones to ensure the required number of users, k with a high probability, $p = 0.9$. For the spatio-temporal delay-tolerant mix-zones, the spatial region size is fixed as 800 m and the temporal window is varied according to the required value of k. We find that the average entropy of the conventional mix-zone approach is significantly lower than that of the delay-tolerant mix-zones as they can not adapt to higher levels of anonymity but the delay-tolerant mix-zones always provide the required anonymity level for all values of k as shown by the high entropy. Here, we also note that the CQ-cloaking approaches (CQ-t and CQ-s) have low level of entropy due to the effect of CQ-timing and CQ-transition attacks. In Fig. 11b and c, we plot the timeline of the entropy obtained by continuous queries (CQ) and snapshot queries (SQ) respectively. Here, we use the spatio-temporal mix-zone as the candidate delay-tolerant mix-zone and temporal CQ-cloaking as the candidate CQ-cloaking technique. We find that with conventional mix-zones, the continuous queries obtain low initial anonymity and it stays constant throughout the timeline. With the CQ-cloaking approach, the queries obtain higher anonymity in the beginning but their anonymity is gradually reduced due to the impact of CQ-timing and CQ-transition attacks. However, the delay-tolerant mix-zones offer very high anonymity to meet the privacy requirements of the continuous queries under the CQ-attack model. For snapshot queries, we find that the techniques have a different trend as shown in Fig. 11c. The conventional mix-zone model shows an increasing entropy timeline where users gain more anonymity at the intermediate mix-zones as CQ-attack has no impact on snapshot queries. We also find that the delay-tolerant mix-zone offers greater anonymity to snapshot queries with a much steeper entropy timeline but the CQ-cloaking technique offers only similar anonymity as the conventional mix-zone.

5.3.1 Performance of continuous and snapshot queries

Next, we study the performance impact of the delay-tolerant mix-zone approaches for continuous and snapshot queries individually. We measure the average temporal delay incurred and the average query execution time of the techniques in Fig. 12a and b. Here, all queries



a Average temporal delay

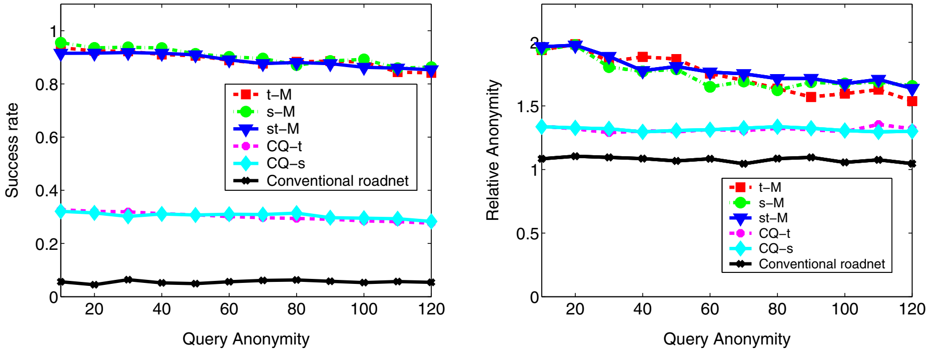
b Query Cost

Fig. 12 Performance of continuous and snapshot queries

are anonymized corresponding to a $k = 50$. The spatio-temporal delay-tolerant mix-zone uses its default spatial region size of 800 m. The query execution time represents the average time to process a snapshot of a k-NN query for a k-nearest neighbor value of ($k_q = 7$) over 14000 uniformly distributed objects on the road network using the road network based anonymous query processor described in [40]. We find that with the CQ-temporal cloaking (CQ-t), only the continuous queries incur delay before getting processed and in CQ-spatial cloaking (CQ-s), neither of the queries incur any delay. With the spatial cloaking approach, we obtain the results of the query for all possible locations within the cloaking region, however the continuous queries in the CQ-spatial cloaking approach result in higher query execution time. In temporal delay-tolerant mix-zones (t-M), both continuous and snapshot queries incur temporal delays but have low query execution time. Conversely, the spatial resolution-tolerant mix-zones (s-M) do not incur any delays for the queries but have increased query execution time for both snapshot and continuous queries. The spatio-temporal delay-tolerant mix-zones technique (st-M) finds a tradeoff between these approaches and has more than 55 % lower average temporal delay compared to the temporal cloaking case as well as a 40 % lower query execution time compared to the spatial resolution-tolerant mix-zones.

5.3.2 Success rate of CQ-attack resilient mix-zones

Our final set of experiments evaluates the performance of the delay-tolerant mix-zones in terms of their success rate in providing the desired level of anonymity given the influence of CQ-attacks. The success rate represents the fraction of the cases where the proposed framework is able to provide an anonymity equal or greater than the requested value, k. In Fig. 13a, the query anonymity level is varied along the X-axis and the Y-axis represents the obtained success rate. Based on the arrival rate of the users in the mix-zone, the expected success rate is chosen as 0.9 so that the delay-tolerant mix-zones provide an anonymity of k or higher in more than 90 % of the cases. We find that all the delay-tolerant mix-zone techniques obtain a success rate close to the expected success rate of 0.9, however the success rate of the CQ-cloaking approach is much lower (less than 0.3) and the conventional mix-zone approach has a even lower success rate of less than 0.06. Similarly, we study relative-k which is defined as the ratio of the anonymity obtained by the queries to the



a Success Rate

b Relative k

Fig. 13 Success rate and relative k

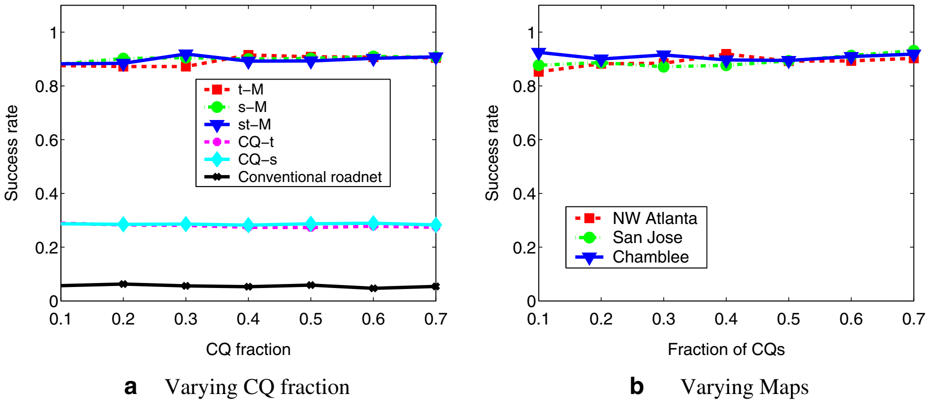
query anonymity requested. In Fig. 13b, we find that the relative anonymity level of delay-tolerant mix-zones ranges from 1.5 to 2.0 showing that the queries on an average obtain an anonymity which is 1.5 to 2.0 times the requested value. The successful cases of CQ-cloaking and conventional mix-zone approaches have a lower relative anonymity as the mix-zones have lower success rate and provides lower value of *k* in general.

In order to evaluate the success rate under different fractions of continuous queries in the system, we study the approaches by varying the fraction of users executing continuous queries. Here, each query is anonymized with an anonymity of 50. Figure 14a shows that the obtained success rate is close to the expected success rate for the delay-tolerant mix-zones across different fractions of CQs in the system. However, the CQ-cloaking and conventional mix-zone techniques have much lower success rate. Similarly, the success rate of the techniques is compared across different scales of geographic maps described in Section 5.1. We compare the success rate of spatio- temporal delay-tolerant mix-zones in Fig. 14b that shows that the technique performs well across different geographic maps.

6 Related work

Location privacy has been studied over the past decade along two orthogonal dimensions: spatial cloaking through location *k*-anonymity represented by [8, 9, 15, 20, 31, 40] and mix-zone based privacy protection and its variations represented by [11, 13, 18, 19, 30, 34]. Some of them had identified the additional vulnerability of location disclosure due to mobile users traveling on spatially constrained road networks [34, 40]. The *XStar* approach [40] performs location cloaking by adding road network-specific privacy metrics such as segment diversity and QoS requirements, striking a balance between the attack resilience of the performed protection and the processing cost of the anonymous query.

The concept of mix-zones was first presented in the context of location privacy in [11]. The idea of building mix-zones at road intersections is proposed in [18] and [13]. In [19], a formulation for optimal placement of mix-zones in a road map is discussed. Almost all existing mix-zone techniques follow a straightforward approach of using a rectangular or circular shaped zone and their construction methodologies do not take into account the effect of timing and transition attacks in the construction process.



a Varying CQ fraction **b** Varying Maps

Fig. 14 Success rate

Inspired by the mix-zone concept, the *Cachecloak* algorithm [30] employs an alternate technique for path-mixing by using cache prefetching to hide the exact location of mobile user by requesting the location based data along an entire predicted path. Although these techniques are effective when all users obtain the same service, they are vulnerable to continuous query correlation attacks when the mobile users obtain uniquely different CQ services. Recently, content caching [7] has been proposed as an alternate solution to location privacy. However, caching large amounts of information on tiny mobile devices may not be effective. In addition, they may limit the usability of the services by restricting mobile clients to ask only services that are cached before-hand.

In recent years, there had been research efforts that dealt with location privacy risks of continuous queries. [14] proposes spatial cloaking using the memorization property for continuous queries. This is further used in [36] for clustering queries with similar mobility patterns. However, as discussed earlier, this type of techniques may lead to large cloaking boxes resulting in higher query processing cost as users may not always move together. An alternative thread of research is represented by the *Private information retrieval* techniques as an alternate to location cloaking for anonymous query processing [22, 23]. PIR techniques guarantee privacy of mobile users regardless of which types of queries (continuous or snapshot) they ask. However PIR based solutions are known to be expensive in both computation and storage overheads, even with the recent new techniques such as hardware-assisted PIR techniques [42], developed to improve the scalability and efficiency of the PIR approach. Another general issue with PIR based solutions is its limitation in terms of what kinds of queries can be protected under PIR [41].

To the best of our knowledge, the road network and CQ-attack resilient mix-zone framework discussed in this paper is the first road-network aware attack-resilient mix-zone that guarantees an expected value of anonymity by leveraging the characteristics of both the underlying road network and motion behaviors of users traveling on spatially constrained road networks. Additionally, by performing a combination of both location mixing and identity mixing in the mix-zones, the delay-tolerant mix-zone approach offer greater level of anonymity that is sufficient to meet the anonymity levels of continuous queries under the CQ-attack model while maintaining acceptable quality of continuous query services.

7 Conclusions

This paper investigates the use of mix-zones as an effective alternative approach to location privacy protection, complementary to spatial cloaking [4, 10–12, 18]. We discussed the vulnerabilities and challenges of constructing attack-resilient mix-zones on road networks. For example, on a road network, the timing information of users entry and exit into the mix-zone may lead to timing attacks and the non-uniformity in the mobility patterns taken at the road junctions may lead to transition attacks. When the location based services are continuous in nature, mix-zones will face the challenge of CQ-attacks, which perform query correlation based inference on continuous queries to break the anonymity of the road network mix-zones. We described our road network and CQ-attack resilient mix-zone framework and discussed the solution techniques to counter the effects of road network timing and transition attacks as well as the continuous query correlation attacks. Our extensive experiments on the effectiveness of our approach using traces generated by GTMobiSim [17] shows significant attack-resilience under a wide range of mix-zone attack models.

Acknowledgments This work is partially sponsored by grants from NSF CISE NetSE program, SaTC program, and a grant from Intel ISTC on Cloud Computing and also by an IBM PhD fellowship for the first author.

References

1. Cuellar JR, Morris JB, Mulligan DK, Peterson J, Polk J (2003) Geopriv requirements. IETF Internet Draft
2. U.S. Geological Survey. http://www.usgs.gov.
3. USAToday. Authorities: gps systems used to stalk woman. http://www.usatoday.com/tech/news/2002-12-30-gps-stalkerx.htm
4. Location Privacy Protection Act of 2001. http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp
5. Chen A GCreep: google engineer stalked teens, spied on chats. Gawker, September 2010 http://gawker.com/5637234/
6. Aggarwal C (2005) On k-anonymity and the curse of dimensionality. In: VLDB
7. Amini S, Lindqvist J, Hong J, Lin J, Toch E, Sadeh N (2011) Cache': caching location-enhanced content to improve user privacy. In: Mobisys
8. Ardagna C, Cremonini M, Vimercati S, Samarati P (2011) An obfuscation-based approach for protecting location privacy. In: IEEE TDSC
9. Bamba B, Liu L, Pesti P, Wang T (2008) Supporting anonymous location queries in mobile environments with PrivacyGrid. In: WWW
10. Bayardo R, Agrawal R (2005) Data privacy through optimal k-anonymization. In: ICDE
11. Beresford A, Stajano F (2003) Location privacy in pervasive computing. Pervasive Computing, IEEE
12. Bettini C, Mascetti S, Wang X, Freni D, Jajodia S (2009) Anonymity and historical-anonymity in location-based services. In: Privacy in location-based applications: introduction, research issues and applications, lecture notes of computer science 5599. Springer
13. Buttyan L, Holczer T, Vajda I (2007) On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In: ESAS
14. Chow C, Mokbel M (2007) Enabling private continuous queries for revealed user locations. In: SSTD
15. Chow C, Mokbel M, Bao J, Liu X (2011) Query-aware location anonymization for road networks. In: Geoinformatica
16. Dewri R, Ray I, Ray I, Whitley D (2010) Query m-invariance: preventing query disclosures in continuous location-based services. In: MDM
17. Daz C, Seys S, Claessens J, Preneel B (2002) Towards measuring anonymity. PETS
18. Freudiger J, Raya M, Félegyhazi M, Papadimitratos P, Hubaux J-P (2007) Mix-zones for location privacy in vehicular networks. In: WiN-ITS
19. Freudiger J, Shokri R, Hubaux J-P (2009) On the optimal placement of mix zones. In: PETS
20. Gedik B, Liu L (2005) Location privacy in mobile systems: a personalized anonymization model. In: ICDCS
21. Ghinita G, Kalnis P, Skiadopoulos S (2007) PRIVE: anonymous location-based queries in distributed mobile systems. In: WWW
22. Ghinita G, Kalnis P, Kantarcioglu M, Bertino E (2011) Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection. In: GeoInformatica
23. Ghinita G, Kalnis P, Khoshgozaran A, Shahabi C, Tan K (2008) Private queries in location based services: anonymizers are not necessary. In: SIGMOD
24. Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. In: MobiSys
25. Hengartner U, Steenkiste P (2003) Protecting access to people location information. In: security in pervasive computing
26. Hong J, Landay J (2004) An architecture for privacy-sensitive ubiquitous computing. In: Mobisys. pp 177–189
27. Karger P, Frankel Y (1995) Security and privacy threats to its. In: World Congress on Intelligent Transport Systems
28. Krumm J (2007) Inference attacks on location tracks. In: PERVASIVE
29. Machanavajjhala A, Gehrke J, Kifer D, Venkitasubramaniam M (2006) l-Diversity: privacy beyond k-Anonymity. In: ICDE

30. Meyerowitz J, Choudhury R (2009) Hiding stars with fireworks: location privacy through camouflage. In: MOBICOM
31. Mokbel M, Chow C, Aref W (2006) The new casper: query processing for location services without compromising privacy. In: VLDB
32. Mouratidis K, Yiu M (2010) Anonymous query processing in road networks. In: TKDE
33. Pesti P, Bamba B, Doo M, Liu L, Palanisamy B, Weber M (2009) GTMobiSIM: a mobile trace generator for road networks. College of computing, georgia institute of technology. http://code.google.com/p/gt-mobisim/
34. Palanisamy B, Liu L (2011) MobiMix: protecting location privacy with mix-zones over road networks. In: ICDE
35. Palanisamy B, Liu L Attack-resilient mix-zones over road networks: architecture and algorithms. Georgia Tech Technical Report
36. Pan X, Meng X, Xu J (2009) Distortion based anonymity for continuous queries in location based mobile services. In: GIS
37. Serjantov A, Danezis G (2002) Towards an information theoretic metric for anonymity. PETS
38. Shmatikov V, Wang M (2006) Timing analysis in low-latency mix networks: attacks and defenses. In: ESORICS
39. Toth G, Hornak Z, Vajda F (2004) Measuring anonymity revisited. In: Norsec
40. Wang T, Liu L (2009) Privacy-aware mobile services over road networks. In: VLDB
41. Wang T, Liu L (2010) Execution assurance for massive computing tasks. In: IEICE transactions on information and systems, Vol. E93-D, No. 6, Special session on Info-Plosion
42. Williams P, Sion R (2008) Usable PIR. In: NDSS

Balaji Palanisamy is an Assistant Professor in the School of Information Sciences in University of Pittsburgh. He received his B.Tech from Pondicherry Engineering College and M.S from Georgia Tech both in Computer Science. He obtained his PhD degree in Computer Science from the college of Computing at Georgia Tech in August 2013. His primary research interests lie in scalable and privacy-conscious resource management for large-scale Distributed and Mobile Systems. He is a member of IEEE.

Ling Liu is a full professor in the School of Computer Science at Georgia Institute of Technology. There she directs the research programs in Distributed Data Intensive Systems Lab (DiSL), examining various aspects of data intensive systems with the focus on performance, availability, security, privacy, and energy efficiency. She has published more than 300 International journal and conference articles in the areas of databases, distributed systems, and Internet Computing. She is a senior member of the IEEE.