MobiMix: Protecting Location Privacy with Mix-zones over Road Networks

Balaji Palanisamy, Ling Liu

College of Computing, Georgia Tech
`{balaji, lingliu}@cc.gatech.edu`

Abstract—This paper presents MobiMix, a road network based mix-zone framework to protect location privacy of mobile users traveling on road networks. In contrast to spatial cloaking based location privacy protection, the approach in MobiMix is to break the continuity of location exposure by using mix-zones, where no applications can trace user movement. This paper makes two original contributions. First, we provide the formal analysis on the vulnerabilities of directly applying theoretical rectangle mix-zones to road networks in terms of anonymization effectiveness and attack resilience. We argue that effective mix-zones should be constructed and placed by carefully taking into consideration of multiple factors, such as the geometry of the zones, the statistical behavior of the user population, the spatial constraints on movement patterns of the users, and the temporal and spatial resolution of the location exposure. Second, we develop a suite of road network mix-zone construction methods that provide higher level of attack resilience and yield a specified lower-bound on the level of anonymity. We evaluate the MobiMix approach through extensive experiments conducted on traces produced by GTMobiSim on different scales of geographic maps. Our experiments show that MobiMix offers high level of anonymity and high level of resilience to attacks compared to existing mix-zone approaches.

I. INTRODUCTION

Location privacy is a system-level capability of location systems, which controls the access to location information at different spatial granularity and different temporal and continuity scale, rather than stopping all access to location information. Several strategies have been suggested to protect personal location information.

- The first strategy is to restrict access. Users who do not want location based services should be provided an option to refuse being tracked [2]. The Geographic Location Privacy (Geopriv) Working Group [1] provides a rule-based policy architecture to allow users to control the delivery and the accuracy of their location information.
- Location *k-anonymization* is an alternative approach that degrades information in a controlled fashion before releasing it through location *k-anonymity* guarantee. A subject is considered *k-anonymous* if its location is indistinguishable from that of $k-1$ other users [8], [15], [17], [23], [24]. Location $k-anonymization$ approaches are targeted at applications that can operate completely anonymously and thus do not require true identity of users, such as finding nearby gas-stations or restaurants, and notifying the sale price of items of interest when

we pass a shopping mall. 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.

- An alternative and complementary approach to spatial cloaking based location privacy protection is to break the continuity of location exposure by introducing techniques, such as mix-zones. Mix-zones anonymize user identity by restricting the positions where users can be located [10]. Mix-zones are regions in space where no applications can trace user movements. The anonymity 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 [10], [12], [13], [14].

Several factors impact on the effectiveness of mix-zone approach, such as user population, mix-zone geometry, location sensing rate and spatial resolution, as well as spatial and temporal constraints on user movement patterns. None of the existing mix-zone approaches consider these factors effectively. Most existing mix-zone proposals fail to provide effective mix-zone construction algorithms that are effective for mobile users traveling on road networks and yet resilient to timing and transition attacks.

In this paper we present MobiMix, a road network based Mix-Zone framework to protect location privacy of mobile users traveling on road networks. In a road network, mix-zones can be constructed at road intersections where there is high uncertainty in the trajectories followed by the users. However, compared to the theoretic mix-zones [10], the road networks impose many challenges that limit the anonymity provided by the mix-zones constructed independently of the spatially constrained road networks. For instance, the timing information of users' entry and exit into the mix-zone and the non-uniformity in the transitions taken at the road intersection provide valuable information to the attacker to guess the mapping between the old and new pseudonyms [12]. In MobiMix, we develop a general framework and a suite of algorithms for constructing mix-zones in road networks, taking into account the constraints and limitations imposed by the road networks, the timing of users entering and exiting a mix-zone, and the transitioning probability of users in terms of their movement trajectory.

This paper makes two original contributions. First, we formally study the impact of the theoretic mix-zone model on the obtained anonymity when some assumptions are violated. We argue that effective mix-zones should be constructed and placed by carefully taking into consideration of multiple factors, such as the geometry of the zones, the statistical behavior of the user population, the spatial constraints on movement patterns of the users, and the temporal and spatial resolution of the location exposure. Second, we present the MobiMix Road Network Mix-zone model for constructing Road Network mix-zones. Based on the model, we develop a suite of mix-zone construction techniques that take into consideration the inherent characteristics of the road networks to guarantee a certain level of privacy in terms of unlinkability between the old and new pseudonyms. We evaluate the proposed techniques through extensive experiments conducted on traces produced by GTMobiSim [22] on different scales of geographic maps. Our experiments show that MobiMix provides higher level of attack-resilience compared to existing mix-zone approaches and yet efficient and scalable.

The rest of the paper is organized as follows: Section II describes the constraints of ideal mix-zones and the anonymity provided by them. In Section III, we explain the characteristics of road networks and the challenges imposed by them for constructing mix-zones. Section IV presents our road network mix-zone model to analyze the anonymity obtained under the spatial constraints of the road network. We introduce our attack-resilient mix-zone construction techniques in section V and our experimental evaluation in Section VI and we conclude in Section VIII.

II. MIX-ZONE MODEL

In this section, we review the concept of theoretical mix-zone and the implications of its assumptions on the level of anonymity it provides.

A. The Mix-zone Model

A mix-zone of k participants refers to a k-anonymizaton region in which users can change their pseudonyms such that the mapping between their old and new pseudonyms is not revealed. A mix-zone is analogous to a mix node in anonymous communication systems [10], where each mix node collects n equal-length packets as input and reorders them randomly before forwarding them, thus providing unlikability between incoming and outgoing messages. 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. These k users exit the mix-zone in an order different from their order of arrival, providing unlinkability between their entering and exiting events. We formally present the theoretic model of a mix-zone and illustrate the strong assumptions used by the model to ensure high privacy guarantee.

Definition 1: A mix-zone Z is said to be k-anonymized with 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 an uniform distribution. i.e., an user entering through an entry point, $e \in E$, is equally likely to exit in any of the exit points, $o \in O$.

Inside the mix-zone, the location of users cannot be tracked.
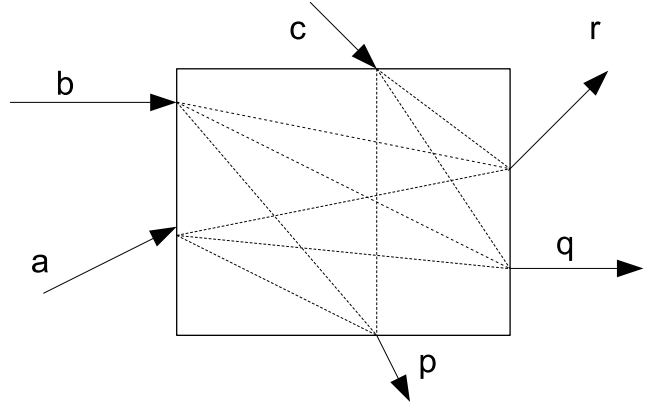

Fig. 1. Mix Zone Model

In the theoretical mix-zone model, the anonymity is measured in terms of the unlinkability between the old and new pseudonyms. For user i, exiting with a new pseudonym, i', let $p_{i' \to j}$ denote the probability of mapping i' to j, where $j \in A$. According to Definition 1, the theoretical mix-zone ensures an equi-probable distribution of mapping i' to $j \in A$. In other words, for every outgoing user, i', it is equiprobable for i' to be any of the k users in the anonymity set A, having $p_{i' \to j} = \frac{1}{|A|}$. Therefore, the entropy of each outgoing user i' is computed according to the information theoretic measure of anonymity

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

The Entropy is a measure of the amount of information required to break the anonymity provided by the system.

In the next subsections, we discuss the significance of the two important assumptions in the mix-zone model namely (1) users stay random time inside (2) users follow uniform transition probability when entering and exiting a mix-zone and illustrate how the failure of these assumptions may affect the entropy measure.

1) Mix Zones without Random time inside: When the users inside the mix-zone spend random time, it ensures a random reordering between the entry and exit orders providing a strong unlinkability between their old and new pseudonyms. However, a mix-zone that does not ensure random duration of time inside for its users usually leaks information. Such leakage may aid attackers to infer the mapping between the

TABLE I

MIX-ZONE WITH RANDOM TIME INSIDE

Id	Old Pseudonym	New Pseudonym	t_{in}	t_{out}	t_{inside}
α	a	p	5	21	16
β	b	q	10	19	9
γ	c	r	15	17	2

TABLE II

MIX-ZONE WITH CONSTANT TIME INSIDE

Id	Old Pseudonym	New Pseudonym	t_{in}	t_{out}	t_{inside}
α	a	p	5	9	4
β	b	q	10	14	4
γ	c	r	15	19	4

old and new pseudonyms of users. For example, when all users spend a constant time inside, the system would simply function in a FIFO (first-in-first-out) style, with the first exit event corresponding to the first entry event and so on. In that case, even though the users might have changed pseudonyms inside, their mapping from the old and new pseudonmys can still be inferred.

Consider the following example in Table I for the mix-zone shown in figure 1 where three users with real identities α, β, and γ enter with pseudonyms a, b and c at time $t_{in}(a) = 5$, $t_{in}(b) = 10$ and $t_{in}(c) = 15$ respectively. If each of them spends a random time inside, (say 16 sec, 9 sec and 2 sec respectively), their order of exits based on their exit times, $t_{out}(p) = 21$, $t_{out}(q) = 19$, and $t_{out}(r) = 17$ would be $(\gamma \rightarrow \beta \rightarrow \alpha)$. We notice that it bears no correlation to their arrival order, $(\alpha \rightarrow \beta \rightarrow \gamma)$, based on their entry times, thus maintaining a strong unlinkability. However, for the example in Table II, with a constant time inside the mix-zone, say 4 sec for each user, their order of exit, $(\alpha \rightarrow \beta \rightarrow \gamma)$, decided by their exit times, $t_{out}(p) = 9$, $t_{out}(q) = 14$, and $t_{out}(r) = 19$, would possess a strong correlation to their order of arrival, $(\alpha \rightarrow \beta \rightarrow \gamma)$, making it simple to guess the mapping of the old and new pseudonyms. A good mix-zone should therefore ensure sufficient randomness in the time spent inside it in order to obtain a high anonymity in terms of unlinkability after the pseudonym change process.

2) Mix-zones without uniform transition probability: Recall Definition 1, the probability of transition between an entry point and an exit point follows a uniform distribution in a theoretical mix-zone. By relaxing this assumption, some transitions between entry and exit points may be more probable than the others. The attacker can use such knowledge to infer the mapping between the old and new pseudonyms. For example, if some transitions are less probable, the attacker may eliminate the pseudonym mappings corresponding to those transitions and thereby improve the success rate of his inference. Based on the probabilities of transition, let us compute $T(ingress(x), egress(y))$, the conditional probability of user, x entering at the entry point, $ingress(x)$ given that the user exits at the exit point, $egress(y)$. Let us assume the conditional transition probability for the example shown in Figure 1 follows: $T(ingress(a), egress(q)) = \frac{2}{3}$, $T(ingress(b), egress(q)) = \frac{1}{3}$, $T(ingress(c), egress(q)) = $

0. Therefore, the probabilities inferred by the attacker about the possible mappings are: $p_{q \rightarrow a} = \frac{2}{3}$, $p_{q \rightarrow b} = \frac{1}{3}$ and $p_{q \rightarrow c} = 0$. The entropy corresponding to the exiting user q, assuming these mapping probabilities, becomes $H(q) = 0.9186$. However, the theoretical mix-zone's entropy value, assuming an uniform mapping probability would be $H(q) = 1.585$. A value of entropy lower than that of the theoretical mix-zone entropy indicates the additional confidence of the attacker in the inference process. In short, the higher the skewness in the transition probabilities, the greater is the information leak to aid the attacker.

III. ROAD NETWORK MIX-ZONES

Theoretical mix-zones assume mobile users move in an Euclidian space without any spatial constraints. In real world, mobile users always move on a spatially constrained space, such as road networks or walk paths. Each road network mix-zone corresponds to a road intersection on a road network. The decision of which intersections are suitable for building mix-zones is usually made based on a number of factors such as the number of road segments at the intersection, the travel speed and trajectory constraints of mobile users inside the mix-zone. Mix-zones constructed at road intersections have a limited number of ingress 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 [3]. 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.
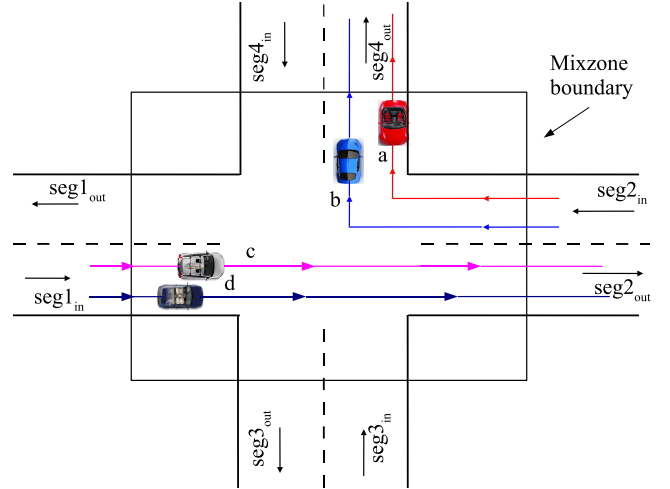

Fig. 2. Road Network Mix Zone

For example, in figure 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 pseudonmys 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 figure 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 very less probable. Thus, an efficient road network mix-zone should be resilient to such transition attacks. Next, we introduce the attack models and the anonymity measures for road network mix-zones.

A. Attack Models

We describe two attack models based on the characteristics of road networks: (1) Timing Attack and (2) Transition Attack

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, $p_{i' \rightarrow j}$ 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 probable 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: $p_{a' \rightarrow a} = \frac{0.1}{0.1+0.09+0.05} = 0.416$, $p_{a' \rightarrow b} = \frac{0.09}{0.1+0.09+0.05} = 0.375$ and $p_{a' \rightarrow c} = \frac{0.05}{0.1+0.09+0.05} = 0.208$. Thus, with the timing information, the attacker is able to find that $a' \rightarrow a$ is the most probable mapping and $a' \rightarrow c$ is least probable. Such timing attack can be detrimental if not handled appropriately in the mix-zone construction and usage model.

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 $p_{i' \rightarrow j}$ for each $j \in A$ based on the conditional transitional probabilities $T((ingress(j), egress(i')))$. Recall, $T((ingress(j), egress(i')))$ denotes the conditional probability of an user i' entering through the entry point, $ingress(j)$ given that the user exited at the exit point, $egress(i')$. Transition attack can equally affect the effectiveness of road network mix-zones as timing attack if not handled with care.

B. Measuring Anonymity in Roadnet mix-zones

In this section, we discuss four quantitative metrics and their appropriateness for measuring the level of anonymity provided by road network mix-zones

1) Anonymity set size: The size of anonymity set is the most straight forward measure of anonymity. However, this metric alone is insufficient given the mapping probabilities may not be uniform in a road network mix-zone. Here, the low probable mappings do not effectively count for the anonymity. Therefore, merely measuring the size of the anonymity set may not provide a good estimate of the anonymity achieved in a roadnet mix-zone.

2) Entropy: An alternate measure of anonymity in cases with non-uniform mapping probabilities would be based on Entropy that captures the attacker's uncertainty in guessing the mapping between a new and old pseudonym. However, a high value of entropy may not necessarily represent strong anonymity when a significant part of the entropy is contributed by a large number of low probable mappings that may be ignored from consideration. Hence, we cannot consider that a mix-zone provides good anonymity for a user if its entropy is greater than a certain value. Two systems can be shown to have the same entropy, but however may provide different levels of anonymity when considered from an individual user's perspective [11]. In summary, the entropy measure may not be used as an accurate estimation of the privacy when the mapping probabilities are non-uniform [11].

3) Normalized Entropy: Normalized entropy, also called Degree of Entropy, is defined as the ratio of the entropy obtained from the road network mix-zone to the entropy obtained from a theoretical mix-zone with the same anonymity set. In other words, it is a measure of how close is the entropy of the roadnet mix-zone as compared to a theoretical mix-zone. Although the normalized entropy may capture the uniformity of the mapping probability distribution in several cases, there are still cases, such as when the normalized entropy is close to 1, it is known that some mapping probabilities may significantly deviate from the others [11].

4) Pairwise Entropy: In order to ensure that the distribution of the mapping probabilities does not deviate much from the uniform distribution, we argue that it is important to measure the deviation of the mapping probabilities in a pairwise fashion. Pairwise entropy between two users i' and j is 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: $p_{i' \rightarrow i}$ and $p_{i' \rightarrow j}$. If the probabilities $p_{i' \rightarrow i}$ and $p_{i' \rightarrow j}$ 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 new pseudonym i' is more likely to be associated with one of the two old pseudonyms with high certainty ($> 50\%$) by eliminating the low probable one. In comparison, by Definition 1, a theoretical mix-zone ensures a uniform distribution for all possible mappings between old and new pseudonyms and a high pairwise entropy of 1.0 for all pairs of users in the anonymity set. We argue that an effective mix-zone should provide a pairwise entropy close to 1.0 for

all possible pairs of users in the anonymity set. In MobiMix, we use the pairwise entropy metric in combination with the anonymity set size to measure the anonymity.

IV. ROAD NETWORK MIX-ZONE MODEL

In this section, we present the MobiMix model for road network mix-zones and discuss the level of anonymity offered in terms of pairwise entropy and the anonymity set size, k. We model the road network as a directed graph $G = (V_G, E_G)$ where the node set V_G represent the road junctions and the edge set E_G represent the road segments connecting the junctions. In this work, we consider only the road junctions that connect three or more road segments as candidate junctions for mix-zones. Consider a mix-zone constructed at a road intersection v as shown in Figure 3. Assume that each user i enters the mix-zone at time $t_{in}(i)$ and exits at time $t_{out}(i)$ with a new pseudonym i'. Let $iseg(i)$ denote the incoming segment of user i through which i enters the mix-zone, $oseg(i)$ denote the outgoing road segment of user i through which i leaves the mix-zone. The speed followed by the users in a road segment is assumed to follow a Gaussian distribution with a mean μ and standard deviation σ, where μ and σ are specific to each road class category. For user i, the set of all other users who had entered the mix-zone during the time window defined by $t_{in}(i) - \tau$ to $t_{in}(i) + \tau$, forms the anonymity set of i, denoted as A_i where τ is a small value. We
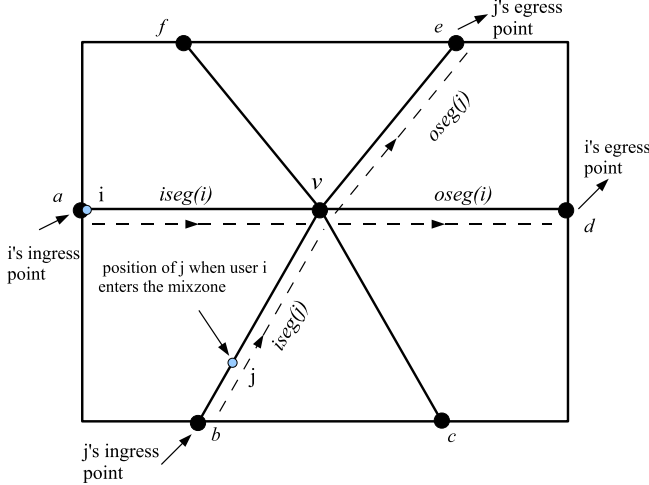

Fig. 3. Road Network Model

first derive the pairwise entropy corresponding to user i and its anonymity set A_i under timing attack. Then, we discuss the anonymity obtained under transition attack. We define $d_i(i)$ as the distance travelled by i inside the mix-zone. It is the sum of the lengths of the mix-zone regions on the incoming and exiting segments ,$iseg(i)$ and $oseg(i)$. $d_i(j)$ is defined as the distance that j needs to travel inside the mix-zone if it were to exit on the outgoing segment of i namely $oseg(i)$ instead of its actual outgoing segment, $oseg(j)$. $d_i(j)$ is the sum of the lengths of the mix-zone regions on the segments, $iseg(j)$ and $oseg(i)$. If $l_{iseg(i)}$ and $l_{oseg(i)}$ represent the lengths of the mix-zone on the incoming and outgoing segments of i, then

$d_i(i)$ is given by

$$d_i(i) = l_{iseg(i)} + l_{oseg(i)}$$

Similarly,

$$d_i(j) = l_{iseg(j)} + l_{oseg(i)}$$

Let $speed_i$ and $speed_j$ denote the random variables of the speed of users i and j. As the speed is assumed to follow a Gaussian distribution, the variables $speed_i$ and $speed_j$ become Normal variables. We also assume that time is slotted and let t be the time of exit of user i, that is $t_{out}(i)$. Let $p_{i' \to j}$ be the probability that the exiting user i' is j and $p_{i' \to i}$ be the probability that the exiting user is i. Users i and j become anonymous from each other if the probability, $p_{i' \to j}$ is exactly equal to the probability, $p_{i' \to i}$ which happens when users i and j enter the mix-zone at the same time and travel the same distance to exit the mix-zone. In short, the more one of these probabilities differs from the other, the higher confidence the attacker will have in linking the old and new pseudonyms.

Let $P(j, t)$ denote the probability that user j exits the mix-zone in the time interval, t to $t + 1$. $P(j, t)$ numerically equals to the probability that user j takes time in the interval $(t - t_{in}(j))$ to $(t + 1 - t_{in}(j))$ to travel the distance $d_i(j)$. Accordingly, j needs to travel with an average speed in the range $s_1 = \frac{d_i(j)}{(t - t_{in}(j))}$ to $s_2 = \frac{d_i(j)}{(t+1-t_{in}(j))}$ in order to exit during the time interval between t to $t + 1$. Therefore, we have

$$P(j, t) = \int_{s_2}^{s_1} speed_j(s)ds$$

Similarly,

$$P(i, t) = \int_{s_2}^{s_1} speed_i(s)ds$$

where $s_1 = \frac{d_i(i)}{(t - t_{in}(i))}$ to $s_2 = \frac{d_i(i)}{(t+1-t_{in}(i))}$

We have

$$P(i', t) = P(i, t) + P(j, t)$$

Therefore, the probability of i' being j when i' exits at time t, denoted as $p_{i' \to j}(t)$ is given by the following conditional probability

$$p_{i' \to j}(t) = P((j, t)/(i', t))$$

$$p_{i' \to j}(t) = \frac{P(j, t)}{P(i', t)}$$

Similarly, the probability of i' being i, $p_{i' \to i}(t)$ is given by

$$p_{i' \to i}(t) = P((i, t)/(i', t)) = \frac{P(i, t)}{P(i', t)}$$

The pair-wise entropy between users i and j when i exits as i' is given by

$$H_{pair}(i, j, t) = -(p_{i' \to i}(t)logp_{i' \to i}(t) + p_{i' \to j}(t)logp_{i' \to j}(t))$$

Similarly, the pair-wise entropy between users i and j when j exits as j' is given by

$$H_{pair}(j, i, t) = -(p_{j' \to i}(t)logp_{j' \to i}(t) + p_{j' \to j}(t)logp_{j' \to j}(t))$$

Here, we notice that even though when i' exits, it might resemble both i and j with a closely equal probability and a high pairwise entropy, when user j' exits, it might reveal that j' is more likely to be one of i and j than the other as these are mutually exclusive events. Therefore, although the pair-wise entropy between i and j may be close to 1 when i' exits, it may happen that the pair-wise entropy of j when j' exits is well below 1. Hence, it is important that both of the two pair-wise entropies are high enough to make the attacker harder to guess the mapping. Also, we find that the pairwise entropy is a function of the exit time, t of i'. As the exit time depends on the time spent inside the mix-zone which is inversely proportional to the speed of the user inside the mix-zone, the pairwise entropy becomes a function of the speed of the user inside the mix-zone. A good mix-zone should offer high pairwise entropy for a wide range of user speeds, for example, say 0 to 90 mph on a highway road and 0 to 40 mph on a residential road. The lowest pairwise entropy offered by the mix-zone within this speed range would define the lowerbound pairwise entropy of the mix-zone. A good mix-zone should therefore offer a high lowerbound, α on the pairwise entropy for a wide range of user speeds.

We now extend our discussion with the pairwise entropy under transition attack. Based on the transition probabilities of the road junction, let $T(seg_l, seg_m)$ be the conditional transition probability computed by the attacker on exit of i'. $T(seg_l, seg_m)$ represents the conditional probability of user i' entering through an incoming segment seg_l given that i' exited on the outgoing segment seg_m. The mapping probabilities, $p_{i' \to i}$ and $p_{i' \to j}$ under the transition attack are therefore given by

$$p_{i' \to i} = \frac{T(iseg(i), oseg(i'))}{T(iseg(i), oseg(i')) + T(iseg(j), oseg(i'))}$$

and

$$p_{i' \to j} = \frac{T(iseg(j), oseg(i'))}{T(iseg(i), oseg(i')) + T(iseg(j), oseg(i'))}$$

Hence, the pairwise entropy under transition attack will be

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

In order for the mix-zone to be resilient to transition attacks, the mix-zone should offer a high lowerbound, β on the pairwise entropy after transition attack for all pairs of users in the anonymity set.

Next, we define the criteria for a roadnet mix-zone to function as an effective mix-zone based on the lowerbounds α and β on the pairwise entropies after timing and transition attacks.

Definition 2: A roadnet mix-zone acts as a k-anonymized mix-zone for user i if

1) There are k or more users in the anonymity set A_i.
2) For each user $j \in A_i$, the pairwise entropy after timing attack, $H_{pair}(i, j, t) \geq \alpha$.
3) For each user $j \in A_i$, the pairwise entropy after transition attack, $H_{pair}(i, j) \geq \beta$.

In the next section, we present our proposed techniques and approaches to construct road network mix-zones that effectively satisfy the above conditions.

V. ROAD NETWORK MIX-ZONE CONSTRUCTION TECHNIQUES

We compare and analyze the effectiveness of the MobiMix mix-zone construction approaches against timing attack and discuss how the mix-zone geometry and road characteristics impact on the attack-resilience.

A. Mix-zone Approaches

We first describe the weaknesses of the naive rectangular mix-zone approach and then propose three MobiMix mix-zone construction techniques: (i) Time Window Bounded (TWB) Rectangular, (ii) Time Window Bounded (TWB) Shifted Rectangular and (iii) Time Window Bounded (TWB) Non-rectangular mix-zones. All of them perform better than the naive Rectangular mix-zones under timing attack.

1) Naive Rectangular Mix-zones: A straight forward approach to construct mix-zones around the road junction is to define a rectangular region centered at the road junction. The rectangle is defined based on some default size. 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. Here, any two users that were present together at any same given time become members of each other's anonymity sets. Although the anonymity set size of the naive rectangular mix-zones are typically large, a large number of members of the anonymity set become low probable under the timing attack. For instance, in figure 4(a), 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 let us 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 although users i and j might have been present together in the mix-zone for some amount of time, the attacker might infer that the user who entered first is more likely to exit first and that it is unlikely for j to have overtaken i before i exits the mix-zone. Therefore, the pairwise entropy of the naive rectangular mix-zones is low under timing attack, leaking more information to aid the attacker.

2) Time Window bounded Rectangular Mix-zones: In the time window bounded approach, the rectangle is constructed in the same way as in naive rectangular mix-zone, however, the anonymity set for each user, i is assumed to comprise only of users who had entered 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 only of the users entering the mix-zone with a closely similar arrival time as that of i. Hence, when i exits out as i', the attacker would be unable 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. However, the right size of the time window should be decided based on a number

(a) Rectangular Mix-zones   (b) Shifted Rectangular Mix-zones   (c) Non-rectangular Mix-zones
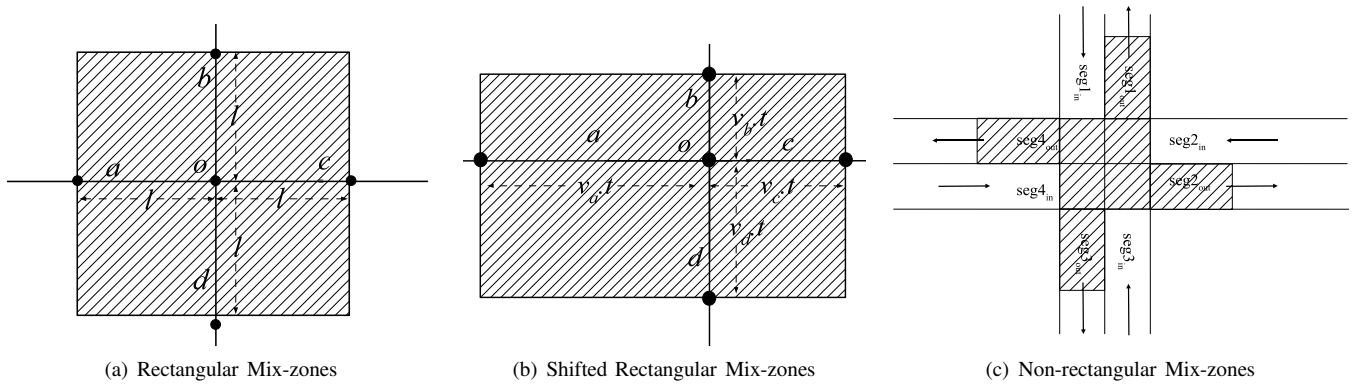
Fig. 4. MobiMix Mix-zone Shapes

of factors including the mix-zone size, the speed distribution of users on the road segments and the level of anonymity users expect. For road intersections that have segments with the same speed distributions, we can precisely guarantee a lowerbound on the pairwise entropy for the members of the anonymity set by constructing the anonymity set with the right value of time window based on our MobiMix road network model. Although, the notion of mix-zone time window has been adopted in many mix-zone proposals [12], [13], [14] where a default value of time window is assumed for the junctions, our approach differs in making the right size of the time window based on the characteristics of the road junction so as to guarantee a lowerbound pairwise entropy.

However, when the segments of the road intersection have different mean speeds, for instance if they belong to different road classes, the attacker may be able to eliminate some mappings based on the timing information. For example, in figure 4(a), let us assume a mix-zone of size 0.5 miles $\times$ 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 seconds and 90 seconds respectively. When user i exits out with a changed pseudonym i' in 30 seconds, 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 leaks information to aid the timing attack.

3) Time Window Bounded Shifted Rectangular Mix-zones: In the Time window bounded shifted rectangular approach, the rectangle is not centered at the centre of the junction, instead it is shifted in such a way that from any point of entry into the mix-zone, it takes the same amount of time to reach the centre of the road junction when travelled at the mean speed. In the same way, from the centre of the junction, it takes the same time to reach any exit point when travelling at the mean speed of the road segments. Here, 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 would find that i' is likely to be any of the members of the anonymity set, A_i. If t represents the average time to reach the centre 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 figure 4(b). Compared to naive rectangular and time window bounded rectangular mix-zones, shifted rectangular mix-zones provide good pairwise entropy for many cases, however, they do leak information when the speed of the users deviates from the mean speed.

As an example, in figure 4(b), consider a mix-zone of size 0.5 miles X 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 minutes, 32.5 seconds. 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 minutes, 32.5 seconds. 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) Time Window Bounded Non-Rectangular mix-zones: A more effective way to construct mix-zones would be to have the mix-zone region start from the centre of the junction only on the outgoing road segments as shown in figure 4(c). 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 distributions 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.

B. Mix-zone size and Time Window

We now discuss how to set the duration of the mix-zone time window in order to ensure sufficient number of users arriving into the mix-zone. Once the size of the time window is decided, we show how to determine the length of the mix-zone for the given time window so as to ensure a high lowerbound on the obtained pairwise entropy. We assume that the user arrival on the road segments follows a Poisson process. Given the mean arrival rate, λ_l on each incoming segment, l, let λ_L denote the rate parameter corresponding to the sum of the Poisson processes of each incoming segment, l. We have $\lambda_L = \sum_l \lambda_l$ that represents the mean arrival rate of the entire road junction. If $N(t)$ represents the number of users who had entered the mix-zone at time t since the beginning, then the probability of having $N(t) = n$ is given by

$$P[N(t) = n] = \frac{e^{-\lambda_L \tau}(\lambda_L \tau)^n}{n!}$$

$N(t + \tau) - N(t)$ would represent the number of users arrived within the short time interval, τ. The probability that k or more users enter the mix-zone in the time window, τ is

$$P[(N(t + \tau) - N(t) \geq k] = 1 - \sum_{1 \leq n < k} \frac{e^{-\lambda_L \tau}(\lambda_L \tau)^n}{n!}$$

By adjusting the size of the time window, τ, we can lowerbound the number of users arriving at the mix-zone to a desired value. For instance, we may choose the time window, τ such that there are $k = 5$ or more users present in the mix-zone with a probability, say $p = 0.9$. Once the value of τ is decided, we determine the length of the mix-zone so that the mix-zone provides a high lowerbound, α on the pairwise entropy after timing attack for a wide range of user speeds. For example, we might want a lowerbound pairwise entropy of $\alpha = 0.9$ for a wide range of users' speed, say 0 mph to 90 mph. Our algorithm iteratively increments the length of the mix-zone till the expected lowerbound on the pairwise entropy is met for the chosen time window, τ. From our experimental observations, we note that except for the TWB non-rectangular mix-zones, the other approaches suffer from timing attacks and hence it is not possible to have a time window and mix-zone length for them to ensure a high lowerbound on the pairwise entropy. However, the TWB non-rectangular mix-zones offer high lowerbounds even for small mix-zone lengths. As we have a lower bound on the pair-wise entropy and a lower bound on k, the number of users, the mix-zone can now make probabilistic guarantees on the anonymity provided.

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

VI. Experimental Evaluation

We divide the experimental evaluation of MobiMix into two components: the effectiveness of our mix-zone construction approaches in terms of their resilience to attacks and performance in terms of success rate, relative anonymity levels and construction time. Before reporting our experimental results, we first describe the experimental setup, including the road-network based mobile object simulator used in the experiments.

A. Experimental setup

We use the GT Mobile simulator [22] 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 [3]. 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 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 III.

B. Experimental results

Our experimental evaluation consists of two parts. First, we evaluate the effectiveness of the mix-zone construction algorithms by measuring their resilience to timing attack. We then evaluate the effectiveness of the mix-zones in terms of the success rate in providing the desired value of k and study the relative anonymity level which is defined as the ratio of the obtained value of k to the expected value of k. We observe how these parameters behave when we vary the settings of a number of parameters, such as the expected value of k, the expected probability of success, p. Our final set of experiments evaluates the scalability of the algorithms in terms of the monitoring overhead involved and the time taken for constructing the mix-zones. Our results show that the MobiMix construction techniques are effective, fast and scalable and outperform the basic construction methods by a large extent.

1) Resilience to Timing Attack: In our first set of experiments, we analyse the effectiveness of the mix-zones against timing attack. The simulation setting for this set of experiments is listed in table IV. Out of the 6831 road junctions in the map, more than 2000 candidate junctions were chosen to build mix-zones based on their user arrival rate and the number of road segments that connect to them. Figure 5 shows the
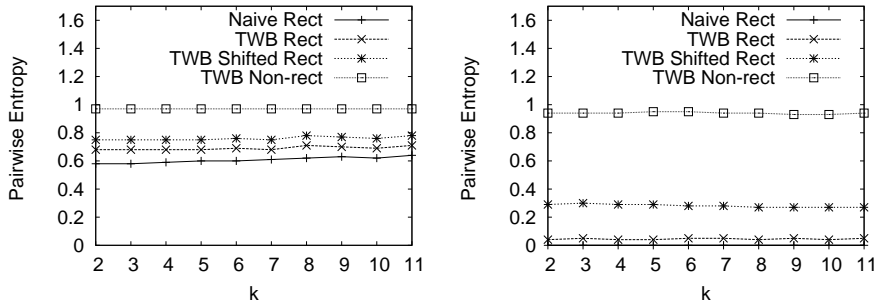
(a) Average Pairwise Entropy   (b) Worst-case Pairwise Entropy

Fig. 5. Resilience to timing attack

TABLE IV
SIMULATION PARAMETERS AND SETTING

Parameter	Value
Map	Northwest Atlanta region
Mobility Model	Random Roadnet Router
Total number of vehicles	10000
Number of Road junctions	6831
Number of Road segments	9187

Fig. 6. Comparison of Entropy after timing attack

average and worst-case pairwise entropy of the mix-zones for various values of k, the size of the anonymity set. In figure 5(a), 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 lowerbound 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, we construct the TWB rectangular and TWB shifted rectangular mix-zones with the same length and time window as used by the non-rectangular mix-zone. Similarly, the size of the naive rectangular 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 figure 5(a), 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 figure 5(b) 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. The other approaches in their bad cases leak a lot information to aid the attacker.

We compare the overall entropy for various values of k in figure 6 for the same experimental setting as in table IV.
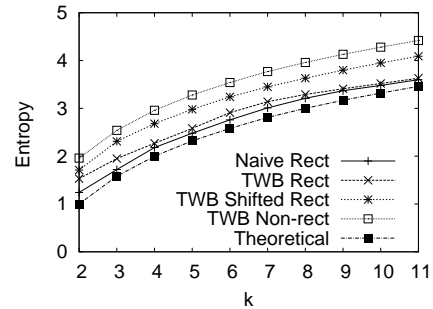
The line showing the theoretical value of entropy corresponds to the actual entropy obtained from an ideal mix-zone for an anonymity set of size k. We find some mix-zones offer higher entropy than the theoretical one, it is because the mix-zones often times have more than k users in them in order to guarantee atleast k users arriving with a probability, p. However, this higher entropy is not necessarily indicative of a better anonymity system than the ideal mix-zone because a large fraction of the entropy could be contributed by low probable mappings that can be ignored from consideration. Our experimental results on pairwise entropy from figure 5 confirm this. However, the TWB non-rectangular approach still has the highest overall entropy.

We also study the impact of varying the mix-zone length on the resilience to timing attacks. Figure 7 shows the worst case and average pairwise entropies after timing attacks. We used the same experimental setting as the previous ones except that the time window of the mix-zones is statically set as 4 sec. Here, we compare the worst case and average entropies with the theoretically computed values based on the road network mix-zone model we described in section IV. We find that except for the TWB non-rectangular approach, the mix-zone length does not have a significant impact on the pairwise entropy. The reason is that the rest of the approaches suffer from timing attack due to the heterogeneity in the speed distributions of the road segments. Therefore, irrespective of the mix-zone length, there always exist bad cases in these mix-zones that cause the pairwise entropy to drop down. The TWB non-rectangular mix-zones show a monotonic increase in the
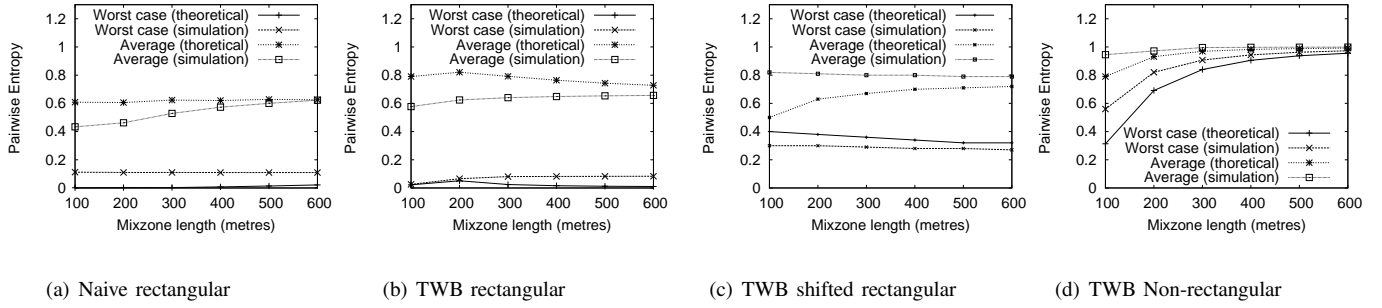
(a) Naive rectangular   (b) TWB rectangular   (c) TWB shifted rectangular   (d) TWB Non-rectangular

Fig. 7.   Effect of mix-zone length on Timing Attack

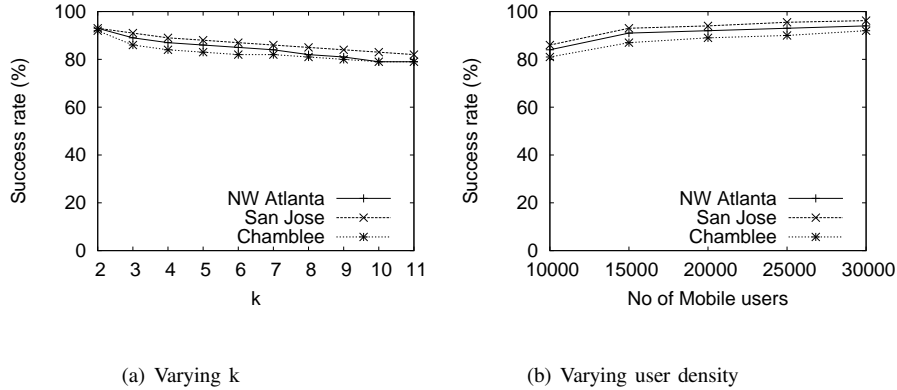(a) Varying k   (b) Varying user density

Fig. 8.   Success rate of TWB Rectangular Mix zones

pairwise entropy with increase in mix-zone length and attains a high lowerbound on the worst case pairwise entropy for even small mix-zone lengths. For the other mix-zones, we do not observe a significant increase with increase in mix-zone size due to their lack of resilience to timing attack.

2) Success Rate and Relative Anonymity: In order to measure the effectiveness of the mix-zones, we study their success rate 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 9 shows the comparison of the success rate among the mix-zone approaches. A mix-zone is considered successful for an user if the user has atleast k other users in its anonymity set with pairwise entropies greater than 0.9. 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. As the TWB non-rectangular mix-zones yield the highest success rate, we present their success rate under more experimental conditions using three geographical maps described earlier. Figure 8(a) shows the obtained success rate of TWB non-rectangular mix-zones for varying values of k. We find that the success rate remains fairly constant for all values of k for all geographic maps and is close to the expected success rate, p which is 90%. Similarly, Figure 8(b) shows the variation of success rate with respect to the total number of users present in the road network. Here also, the obtained success rate matches well with the expected success rate of 90% for a wide range of user densities in the map. 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 10 shows the variation of relative-k of TWB non-rectangular mix-zones with respect to the expected value of k. The expected success rate is set to 90%. The graph shows 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.
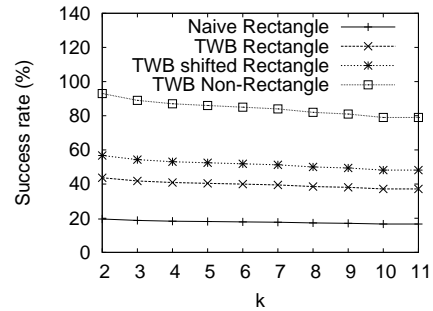

Fig. 9.   Success Rate

3) Scalability and Overhead: Measuring the user arrival rate at the road junctions and dynamically adapting to the changes in traffic conditions require constant monitoring of the road junctions. We study the overhead of monitoring and the time taken for the mix-zone construction process in figure 11. The mix-zone construction time includes the time to compute the time window and the size of the zones by analyzing the pairwise entropy provided by them. Figure 11(a) shows the monitoring time for a 10 minute simulation of road traffic. The monitoring time increases linearly with the total number
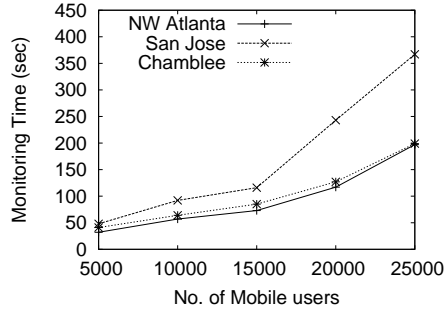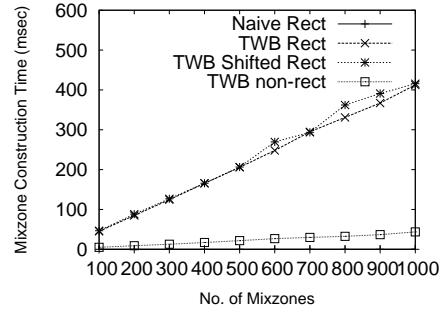
(a) Monitoring Time
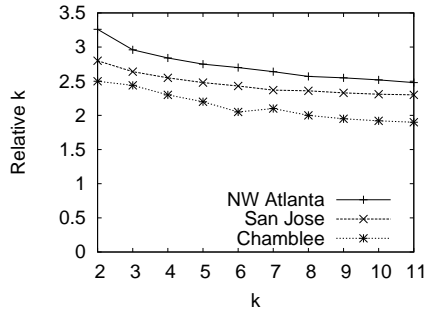(b) Construction Time

Fig. 11. Scalability and Performance

Fig. 10. Relative Anonymity

of users present in the road map and the overhead is well within acceptable limits. Figure 11(b) shows the total mix-zone construction time for constructing the mix-zones. We find that the TWB non rectangular mix-zones take lesser construction time compared to others as their analysis on the road network model involves only the outgoing segments and hence involves only one Gaussian variable in the pairwise analysis as opposed to a combination of two random variables for the other geometries.

VII. RELATED WORK

Location Anonymization has been proposed in [17] and adopted by several others [15], [23], [16], [8]. Some recent work on location anonymity had focussed from the road network perspective [24] and [25]. The *XStar* framework presented in [24] performs location cloaking based on road-network-specific privacy and QoS requirements, striking a balance between the attack resilience of the performed protection and the processing cost of the anonymous query. The *Cachecloak* algorithm proposed in [25] uses cache prefetching to hide the exact location of the user by requesting the location based data along an entire predicted path. While the approaches based on location cloaking do not work for applications that require an exact point location of the mobile user, the approach presented in [25] is not very suitable when users ask different queries as they move.

The concept of mix-zones to change pseudonyms has been introduced in [10] and the idea of building mix-zones at road intersections has been proposed in [12] and [14]. In [13], a formulation for optimal placement of mix-zones in a road map has been discussed. Almost all of these mix-zone techniques follow a straight forward 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. The approaches presented in MobiMix differ from these in two folds: firstly, the mix-zone construction process of MobiMix tries to minimize the effect of attacks based on the characteristics of the underlying road network and secondly, the framework attempts to address the issue of guaranteeing an expected value of anonymity by taking into consideration the statistics of user arrivals and other factors in the road network.

VIII. CONCLUSIONS

This paper presents MobiMix, a framework for building mix-zones on road networks for protecting the location privacy of mobile clients. We first provided a formal analysis of the theoretical mix-zone model and the vulnerabilities of applying them to road networks where some of the assumptions may be violated. We argue that road network mix-zone construction techniques should take into consideration a number of factors such as the mix-zone geometry, the statistics of the user population, and the spatial and velocity constraints on the movement patterns of the users. The construction techniques proposed in MobiMix are efficient and are more attack-resilient than the existing mix-zone approaches. Extensive experiments were conducted on real road networks to study the efficacy and attack resilience of the proposed algorithms. In future, we would investigate on the mix-zone construction and placement problems considering more sophisticated attack models based on background knowledge about the users' trajectory patterns and travel behaviour.

IX. ACKNOWLEDGEMENT

REFERENCES

[1] J.R. Cuellar, J.B. Morris, D.K. Mulligan, J. Peterson and J. Polk. Geopriv requirements. *IETF Internet Draft*, 2003.

[2] U. Hengartner and P. Steenkiste. Protecting access to people location information. In *Security in Pervasive Computing*, 2003.

[3] U.S. Geological Survey. http://www.usgs.gov.

[4] P. Karger and Y. Frankel. Security and privacy threats to its. In *World Congress on Intelligent Transport Systems*, 1995.

[5] USAToday. Authorities: Gps systems used to stalk woman. http://www.usatoday.com/tech/news/2002-12- 30-gps-stalker x.htm.

[6] Foxs-News. Man accused of stalking ex-grilfriend with gps. http://www.foxnews.com/story/0293313148700.

[7] C. Aggarwal. On k-Anonymity and the Curse of Dimensionality. In *VLDB*, 2005.

[8] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid. In *WWW*, 2008.

[9] R. Bayardo and R. Agrawal. Data Privacy Through Optimal k-Anonymization. In *ICDE*, 2005.

[10] A. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *Pervasive Computing, IEEE*, 2003.

[11] G. Toth, Z. Hornak and F. Vajda. Measuring Anonymity Revisited. In Norsec, 2004.

[12] J. Freudiger, M. Raya, M. Flegyhazi, P. Papadimitratos, and J.-P. Hubaux. Mix-Zones for Location Privacy in Vehicular Networks. In WiN-ITS, 2007.

[13] J. Freudiger, R. Shokri and J.-P. Hubaux. On the Optimal Placement of Mix Zones. In PETS, 2009.

[14] L. Buttyan and T. Holczer and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs In ESAS 2007

[15] B. Gedik and L. Liu. Location Privacy in Mobile Systems: A Personalized Anonymization Model. In *ICDCS*, 2005.

[16] G. Ghinita, P. Kalnis, and S. Skiadopoulos. PRIVE: Anonymous Location-Based Queries in Distributed Mobile Systems. In *WWW*, 2007.

[17] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys*, 2003.

[18] M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. *Mobile Networks and Applications*, 2005.

[19] J. Hong and J. Landay. An Architecture for Privacy-Sensitive Ubiquitous Computing. In *Mobisys*, pages 177–189, 2004.

[20] K. LeFevre, D. DeWitt, and R. Ramakrishnan. Incognito: Efficient Full-Domain K-Anonymity. In *SIGMOD*, 2005.

[21] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. l-Diversity: Privacy Beyond k-Anonymity. In *ICDE*, 2006.

[22] P. Pesti, B. Bamba, M. Doo, L. Liu, B. Palanisamy, M. Weber. GTMobiSIM: A Mobile Trace Generator for Road Networks. College of Computing, Georgia Institute of Technology, 2009, *http://code.google.com/p/gt-mobisim/*.

[23] M. Mokbel, C. Chow, and W. Aref. The New Casper: Query Processing for Location Services without Compromising Privacy. In *VLDB*, 2006.

[24] T. Wang and L. Liu. Privacy-Aware Mobile Services over Road Networks In *VLDB 2009*

[25] J. Meyerowitz and R. Choudhury. Hiding Stars with Fireworks: Location Privacy through Camouflage In *MOBICOM 2009*