Safety-aware Location Privacy in VANET: Evaluation and Comparison

Karim Emara *Member, IEEE*

***Abstract*—VANET safety applications broadcast cooperative awareness messages (CAM) periodically to provide vehicles with continuous updates about the surrounding traffic. The periodicity and the spatiotemporal information contained in these messages allow a global adversary to track vehicle movements. Many privacy schemes have been proposed for VANET, but only few schemes consider their impact on safety applications. Also, each scheme is evaluated using inconsistent metrics and unrealistic vehicle traces, which makes comparing the actual performance of different schemes in the wild more difficult.**

In this paper, we aim to fill this gap and compare different privacy schemes not only in terms of the privacy gained but also their impact on safety applications. A distortion-based privacy metric is initially proposed and compared with other popular privacy metrics showing its effectiveness in measuring privacy. A practical safety metric which is based on Monte Carlo analysis is then proposed to measure the QoS of two safety applications: forward collision warning and lane change warning. Using realistic vehicle traces, six state-of-the-art VANET privacy schemes are evaluated and compared in terms of the proposed privacy and safety metrics. Among the evaluated schemes, it was found that the coordinated silent period scheme achieves the best privacy and QoS levels but fully synchronized silence among all vehicles is a practical challenge. The CAPS and CADS schemes provide a practical compromise between privacy and safety since they employ only the necessary silence periods to prevent tracking and avoid changing pseudonyms in trivial situations.

***Index Terms*—C2X communication, IVC, pseudonym change scheme, privacy metric, safety metric, privacy scheme comparison**

I. Introduction

VEHICULAR ad hoc networks (VANETs) provide wireless communication among vehicles to exchange information autonomously. It is evident that VANETs will be implemented in the near future to minimize traffic fatalities and support self-driving cars [1]. To attain the benefits of safe and efficient traffic flow, VANET applications broadcast Cooperative Awareness Messages (CAM) periodically. A CAM (aka Basic Safety Message (BSM) or beacon) contains, among other information, time stamp, position, speed and heading. Since this information is broadcast publicly [2], a serious privacy threat arises if these CAMs are collected and analyzed.

Preserving different forms of privacy has been investigated in the past decade and several research projects are considering privacy risks and countermeasures from both technical and legal perspectives. For example, Privacy Flag project [3] combines crowd sourcing, ICT technology and legal expertise to protect citizen privacy when visiting websites, using smartphone applications, or living in a smart city. Moreover, numerous research works have been published that address security and privacy issues in a smart city that deploys VANET [4], [5]. In spite of the diversity of security and privacy schemes in VANET, there is a consensus towards adopting public key infrastructure (PKI) for securing VANETs [6] demonstrated by the current standardization activities (ETSI TS 102 941 [7] and IEEE 1609.2 WG [8]). In this vehicular PKI, vehicles are provided with a long-term certificate to ensure accountability, along with short-term unique pseudonyms associated with private keys. A vehicle digitally signs outgoing messages to ensure the integrity and authenticity of the exchanged information. The pseudonym and its corresponding certificate are attached to the signed message to allow any vehicle verify it. To avoid continuous linkability, pseudonyms are changed periodically according to a privacy (i.e., pseudonym-change) scheme.

The essential vulnerability of CAMs is that they are linkable, whether through matching similar pseudonyms or by exploiting the contained spatiotemporal information [9]. This vulnerability permits eavesdroppers to reconstruct vehicle traces[1] from CAMs with perfect accuracy, as shown in our previous work [10], [11]. Although the exchanged CAMs contain no personal information, further inference attacks can be performed to de-anonymize the reconstructed traces. De-anonymization can be achieved using work/home pairs [12] or even with the help of geosocial networks [13]. Therefore, an adversary can identify the driver's sensitive whereabouts, social activities and personal preferences remotely without control or knowledge of the driver. These privacy risks must be handled to ensure the public acceptance of VANETs.

Although there are several privacy schemes that prevent the continuous tracking of CAMs, only a few consider their impact on safety applications. These schemes usually reduce the quality or frequency of the exchanged information and may hinder the functionality of safety applications. Therefore, when designing or evaluating a privacy scheme, it is important to analyze its impact on the quality of service (QoS) of safety applications. The trade-off between privacy and safety is sporadically studied in the literature and still considered to be an open research and deployment challenge [4]. In addition, a comprehensive assessment of privacy schemes with consistent privacy metrics using realistic vehicle traces is needed to judge

K. Emara is with University of Luxembourg (SnT) and Faculty of Computer and Information Sciences, Ain Shams University, Egypt. e-mail: karim.emara@uni.lu, karim.emara@cis.asu.edu.eg. This work was mainly done while the author was affiliated with the Department of Informatics, Technical University of Munich, Germany

[1]Hereafter, a *trace* refers to the original vehicle trace and a *track* refers to the reconstructed trace by the adversary.

the actual performance of different schemes [4].

In this paper, we consider those issues by 1) proposing privacy and QoS metrics and 2) comparing state-of-the-art privacy schemes consistently using realistic vehicle traces. On the one hand, location privacy is quantified by measuring how accurately an adversary can reconstruct vehicle traces from the collected CAMs. For this purpose, our vehicle tracker [10], which is based on a multi-target tracking algorithm, is employed to act as a global adversary. The reconstructed traces by the tracker are then compared with the original vehicle traces to calculate the distortion which expresses on the privacy level. The more distorted the reconstructed traces, the greater is the privacy gained by the driver. On the other hand, the QoS of safety applications is evaluated by estimating the probability of calculating the fundamental requirements of a safety application using CAMs altered by a privacy scheme. We initially proposed this QoS metric in previous works [14], [15], but we extend it here by considering two safety applications, namely forward collision warning (FCW) and lane change warning (LCW) applications. These applications are chosen because they require the most precise location information ($<$1 m) and the highest beaconing rate (10 Hz) [16]. Using these privacy and QoS metrics, six privacy schemes are discussed and compared using realistic traces. Thus, our **contributions** in this paper can be summarized as follows:

- Propose a distortion-based privacy metric and compare it with other popular privacy metrics such as anonymity set size, entropy and traceability.
- Extend our previously-proposed QoS metric, which facilitates evaluating the impact of privacy schemes on VANET safety applications.
- Compare six popular privacy schemes in terms of their privacy and safety levels against a robust global adversary using realistic vehicle traces.

The rest of the paper is organized as follows. After reviewing related work in Section II, we discuss the assumed system and adversary models in Sections III and IV, respectively. In Section V, we explain our methodology, including the employed vehicle tracker and traces. In Section VI, location privacy metrics are discussed and evaluated in comparison with the proposed metric. The QoS metric for FCW and LCW safety applications is presented in Section VII. In Section VIII, several privacy schemes are discussed and consistently compared.

II. Related Work

The basic concept of privacy schemes in VANET is to change pseudonyms periodically in *unobserved mix-contexts* to prevent linkability of CAMs. Unobservability is required to prevent an adversary from using the CAM spatiotemporal information to correlate the two consecutive messages of old and new pseudonyms. Mix-context means that several nearby vehicles change their pseudonyms simultaneously to avoid a sole pseudonym change which is easy to correlate. Unobserved mix-contexts are usually realized by using a silent period before a pseudonym change or by changing pseudonyms in cryptographic mix-zones (e.g., at road intersections). In fact, changing pseudonyms without these unobserved mix-contexts cannot prevent vehicle tracking, as shown in [10], [17].

Sampigethaya et al. [18] apply silent periods in VANETs when vehicles are merging or changing lanes when joining or leaving a freeway. Freudiger et al. [19] introduce cryptographic mix zones (CMIX) which allow vehicles to obtain a symmetric key from the Road-Side Unit (RSU) that controls the mix zone and to use it to encrypt all messages while they drive within the zone. Keys are also forwarded upon request to vehicles outside the range of the RSU to allow them decrypt received messages from vehicles within the zone. Buttyán et al. [20] propose ceasing sending messages when the vehicle speed becomes low, for example at intersections. The idea behind choosing low speed events is that fatal accidents are less likely to occur at low speed, and places like intersections are natural mix areas where many vehicles are in close proximity. Wei and Chen [21] propose obfuscating position, speed and heading of vehicle within the radius of the safe distance calculated by a safety analysis algorithm. They also propose changing the length of the silent period based on the distance from other vehicles. Thus, the closer the vehicles are to one each other, the shorter the silent period.

Palanisamy et al. [22] propose the MobiMix framework, which is a construction and placement model for mix zones that is robust against timing and transition attacks. Yu et al. [23] recently proposed MixGroup, which is capable of efficiently exploiting the sparse meeting opportunities among vehicles for pseudonym change. They also utilize group signature to construct extended pseudonym-changing regions, in which vehicles can successively exchange their pseudonyms.

Location privacy cannot be protected without cost. Changing pseudonyms and remaining silent for a period of time may degrade the performance of applications. In related work, the quality of service (QoS) is measured from different perspectives and can be grouped into three metric categories: communication quality, data quality (position error), and application requirements. In the communication quality category, Schoch et al. [24] analyze the impact of pseudonym changes on the performance of geographic routing. Their results confirm serious performance degradation in case of low-density traffic and frequent pseudonym changes ($<$ 30 s). Calandriello et al. [25] measure the impact of pseudonym change in terms of the reception timing of the new pseudonym at several distances and relative speeds. For data quality metrics, Hoh et al. [26] present a QoS metric for traffic monitoring applications characterized as the error applied to each individual location sample. For metrics based on the application requirements, Hoh et al. [27] measure the data quality through the relative weighted road coverage. They consider a road segment to be covered if a data sample with 100 m accuracy is available. Papadimitratos et al. [28] study the impact of different VANET security and privacy schemes on an emergency braking alarm application. They simulate a dense platoon of vehicles moving at relatively high speed and count the occurrences of vehicle collisions upon an emergency braking of the leading vehicle. Lefevre et al. [29] analyze the influence of the duration of the silent period on the effectiveness of intersection collision

avoidance (ICA) systems. They propose an ICA system and evaluate a silent period scheme in terms of missed and avoided collisions. They claim that the ICA system can function well with silent periods of less than two seconds.

III. System Model

We assume that each vehicle is equipped with an on board unit (OBU), which used to communicate with other vehicles and broadcast CAMs periodically (1-10 Hz). The CAM contains a pseudonym, a timestamp, and the current vehicle state (i.e., position, speed and heading). Vehicles use a pseudonym acquisition policy [6] to retrieve a pool of pseudonyms to be used one by one in V2X communication. Pseudonyms are attached to anonymous credentials authenticated by a certification authority to ensure trustworthiness among vehicles. A vehicle uses a pseudonym for a *minimum pseudonym time* (to ensure stable communication), then the pseudonym is changed according to the adopted privacy scheme. The European standard ETSI TS 102 867 [30] recommends changing a pseudonym every five minutes, while the American SAE J2735 [31] standard recommends changing it every 120 s or 1 km, whichever comes last.

Since CAMs are primarily used by safety applications, the broadcast information must be as precise as possible. Thus, we assume each vehicle is equipped with a GPS receiver and combines the obtained GPS measurements with its internal sensors to minimize the position error to 50 cm. This small error is recommended in [32] and also realized in systems such as [33] in order to provide useful Cooperative Collision Warnings (CCW). We assume that a vehicle maintains the states of its nearby vehicles located within its communication range (e.g., 300 m) using a multi-target tracking (MTT) algorithm, similar to [34]. The utilization of a MTT algorithm allows a vehicle to predict the state of nearby vehicles even if their CAMs are delayed or missed due to a communication error or a silence period. As a result, the MTT algorithm can enhance the effectiveness of safety applications.

IV. Adversary Model

For the adversary model, we assume a global passive adversary (GPA) that deploys low-cost receivers over a large part of the road network and eavesdrops on all exchanged messages. Having an external adversary that can cover the whole network may seem far-fetched, but we assume the worst case scenario. Also, this model is realizable, for example, by an untrusted service provider through its deployed roadside units. The main objective of the GPA is a *tracking attack* or reconstructing all vehicle traces from their CAMs. Thus, we assume that the drivers' location privacy is determined by the protection level against this attack. Although breaching the driver's location privacy requires de-anonymization of the reconstructed traces, the de-anonymization process is out of scope of this paper. However, we presume that the more complete and correct the reconstructed traces, the more successful the de-anonymization process.

The GPA achieves its objective by correlating the CAMs of a vehicle by pseudonym matching. When a vehicle changes its pseudonym, the adversary uses a multi-target tracking algorithm to correlate the messages of the old and new pseudonyms. If the adversary covers only a small part of the road network, it can still track vehicles within this limited area, but such tracking may not be valuable for de-anonymization as it does not reflect complete traces. Although powerful adversaries can track vehicles using already-deployed cameras spread over the road network, the cost and inefficiency of global camera-based attacks will be much higher than those for global CAM-based attacks [19].

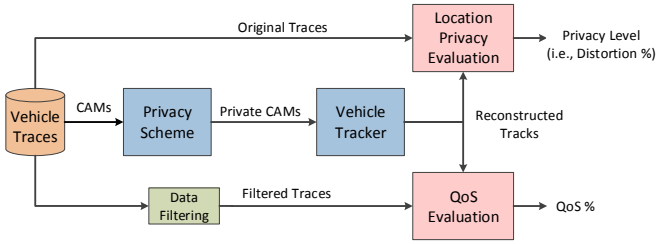


Fig. 1. Block diagram of the evaluation methodology. Privacy schemes are applied to the CAMs obtained from vehicle traces. The adversary tracker tries to reconstruct vehicle tracks which, in turn, are compared to the original traces to obtain privacy and QoS metrics.

The other adversary model that may threaten a privacy scheme is active attacks which tries to prevent a vehicle from changing its pseudonym or to force it to change pseudonyms frequently until the pseudonyms pool depletes so quickly. This adversary model usually affects cooperative privacy schemes where the pseudonym change decision is based on an external trigger (e.g., when k-neighbors surround a vehicle) or requires an inter-vehicle coordination (e.g., a simultaneous pseudonym change). Since we are seeking a holistic comparison of both cooperative and non-cooperative schemes, we do not consider active attacks in this paper and leave it for future work. Readers interested in active attacks can check our previous work [35], which evaluates the effect of a local active attack on the CADS cooperative privacy scheme.

V. Methodology

We evaluate privacy schemes and their impact on safety applications empirically using vehicle traces. As illustrated in Figure 1, vehicle traces are used in generating CAMs as if they were broadcast by vehicles in a fully penetrated VANET and collected by a global adversary. The generated CAMs are then modified according to the specifications of the privacy scheme such as changing pseudonyms and suppressing some messages during obligatory silent periods. These pseudonymous CAMs obtained from a privacy scheme are passed to a vehicle tracker to be reconstructed into anonymous tracks. The reconstructed tracks are then compared with the original traces to calculate the distortion percentage indicating the privacy level. Also, they are compared with the filtered traces to obtain the QoS for safety applications. Given the unified distortion and QoS percentages, we can flexibly compare different privacy schemes with respect to their compromises between privacy and safety levels.

A. Vehicle Tracker

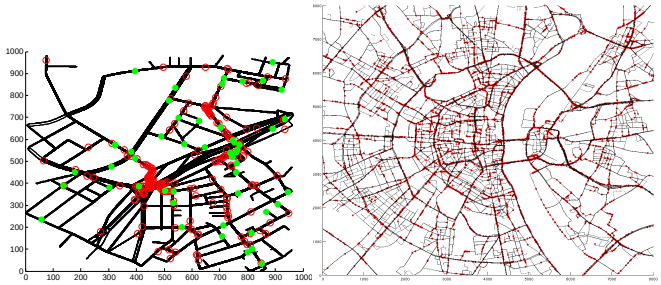
We use an empirical tracker as a global adversary for evaluation of privacy schemes. This tracker is originally proposed in [10], [11], and shows promising effectiveness in tracking anonymous CAMs with various vehicle densities, transmit rates, and position noise levels. Basically, the vehicle tracker consists of four iterative phases as follows:

- *State estimation* using a Kalman filter, which is used to obtain an accurate state for vehicles using both inaccurate measurements gained from vehicle sensors and the estimated states obtained from a predefined kinematic model.
- *Data association* using a nearest neighbor probabilistic data association (NNPDA) algorithm, which tries to associate each CAM to its originating vehicle by calculating an assignment probability matrix. This phase is only applied when there are two or more vehicles changing their pseudonyms in the same time. Otherwise, consecutive CAMs are linked by matching similar pseudonyms.
- *Gating* phase which is performed prior to the data association phase to prevent unnecessary computations for unlikely associations.
- *Track maintenance* phase, which is needed to handle track initiation, confirmation and deletion since the number of vehicles is dynamic. This phase is tuned relative to that proposed in [11] to cope with the silent periods usually imposed by privacy schemes. Originally, the tracker holds a vehicle track without updating it until *time-to-live* time steps, and deletes it afterwards. We added an extra parameter for the maximum silence period (*max-silence*) that can be used by a privacy scheme. The tuned tracker only marks a vehicle track as inactive after *time-to-live* time steps, and then holds it for additional *max-silence* time steps. When the tracker assigns CAMs of unmatched (new) pseudonyms to the current tracks list, it only considers inactive tracks. This tweak increases the linkability of CAMs, since it eliminates the matching of CAMs for new pseudonyms with unrelated tracks.

B. Vehicle Traces

1) STRAW Traces: We employ two sets of vehicle traces. The first traces were generated by Wiedersheim et al. [17]. They have a road map of 1 km^2 and are generated from the STreetRAndom Waypoint (STRAW) mobility model [36] on the Central Boston map for 1000 s. The vehicles in each road lane periodically calculate the acceleration or deceleration for the next time step. Because no collision recognition is implemented, vehicles that simultaneously cross an intersection may collide. The vehicle density is kept constant in each trace file by making vehicles route within road segments and never exit. This constant density per scenario allows evaluating the performance of privacy schemes in each traffic density.

The original traces contain the vehicle ID, time stamp, and position with a second stepping. We calculate the velocity assuming a constant velocity between every two consecutive time steps and interpolate the samples to generate traces of 0.5 s stepping. The maximum vehicle speed ranges from 11 to 26 m/s depending on the road, the maximum acceleration is 2.23 m/s^2 and the maximum deceleration is 11.15 m/s^2. The road map of these traces is shown in Figure 2a, where snapshots of the sparsest case of 50 vehicles and densest case of 200 vehicles are represented by green points and red circles, respectively. Each vehicle density has 10 variations with different routes.



(a) STRAW traces (b) Realistic TAPASCologne traces

Fig. 2. The road maps of the vehicle traces employed.

2) Realistic Traces: The second trace set is obtained from Uppoor et al. [37]. This dataset is originally based on the data made available by the TAPASCologne project [38]. This dataset reproduces vehicle traffic in the greater urban area of the city of Cologne, Germany with the greatest possible level of realism. The street layout of the Cologne urban area is obtained from the OpenStreetMap (OSM) database. The microscopic mobility of vehicles is generated using the Simulation of Urban Mobility (SUMO) traffic simulator. The sources and destinations of vehicle traces are derived through the Travel and Activity PAtterns Simulation (TAPAS) methodology. Uppoor et al. [39] pointed out several problems when combining these data sources to produce traffic data. Among these problems, vehicles are moving rapidly to large traffic jams, travel times are unrealistic and vehicle speeds tend to very low values. Uppoor et al.resolved these problems so that the synthetic traffic matches that observed in the real world, through real-time traffic information services. This is why we call this dataset as realistic traces. We processed the dataset to calculate the heading and velocity in xy coordinates using consecutive time steps for each vehicle. The last heading value was preserved when the vehicle stopped and was changed when it started to move again.

We obtained the two-hour sample published online [37] and selected 30 min (from 6:15 AM till 6:45 AM) for the middle 64 km^2 region, as shown in Figure 2b. We selected this time period because the vehicle density increases dramatically, which provides a challenging evaluation environment for the operation of privacy schemes over different densities. There are 19,704 distinct traces with increasing density, ranging from 1,929 to 4,572 simultaneous vehicles in the first and last time steps, respectively. The vehicle positions in the last time step are shown as red spots in Figure 2b.

VI. Privacy Metric

Several location privacy metrics are utilized in related work. We present and compare here four popular metrics, showing

how effective they are. We then formally define our proposed metric, which will be used in comparing privacy schemes.

A. Anonymity Set Size

The anonymity set of a target vehicle is the vehicles among which this target vehicle is not identifiable or distinguishable with respect to its location. An anonymity set can be formed when two or more nearby vehicles change their pseudonyms at the same time. In this case, the adversary may confuse about the actual location of the target vehicle, since it may be any vehicle from the anonymity set. One disadvantage of anonymity set size is that it cannot deal with nonuniform probability distributions of the anonymity set [40], [41].

B. Entropy

To handle the shortcomings of the anonymity set size, Serjantov and Danezis [40] and Díaz et al. [41] propose an information theoretic metric, the entropy, to measure the anonymity. Let $\mathcal{A}$ represent the anonymity set and p_i the probability assigned by the adversary for each member in $\mathcal{A}$ to be the target such that $\sum_{i=1}^{|\mathcal{A}|} p_i = 1$, then the entropy $\mathcal{H}$ can be defined as:

$$\mathcal{H} = -\sum_{i=1}^{|\mathcal{A}|} p_i \cdot \log p_i \tag{1}$$

According to this definition, the entropy of a vehicle is zero when the same pseudonym is used for several CAMs. Upon a pseudonym change, the entropy is calculated based on the probability distribution assigned by the adversary. The entropy achieves its maximum value when the probability distribution is uniform (i.e., $\mathcal{H}_{max} = \log_2 |\mathcal{A}|$). Since $\mathcal{H}$ is unbounded, Díaz et al. [41] propose an extended metric, the *normalized entropy* $\mathcal{H}_n$, to measure the degree of anonymity:

$$\mathcal{H}_n = \frac{\mathcal{H}}{\mathcal{H}_{max}} \tag{2}$$

Fischer et al. [42] argued that entropy-based metrics are not suitable for measuring unlinkability because they do not distinguish among different probability distributions of linking subsequent messages estimated by different attackers. Moreover, Shokri et al. [43] claim that the entropy and, of course, the anonymity set size metrics are not suitable for quantifying location privacy. The entropy shows how uniform versus condensed the estimated distribution is and, in consequence, how certain the adversary is about its decision. However, the entropy does not provide any clue about the correctness of this decision. It may happen that the adversary is certain about its estimate with a high probability but, at the same time, this estimate is largely different from the actual user's location.

C. Traceability

Another approach for measuring the location privacy is to calculate how long an adversary can track vehicles. Success in tracking vehicles is inversely proportional to the location privacy. Identifying user trajectories and movement patterns is an essential step for privacy breaches (i.e., re-identification and localization attacks) [27].

There are several approaches to measuring traceability. Huang et al. [44] measure how long a node can be tracked continuously in evaluation of silent period schemes in mobile networks. Sampigethaya et al. [18] define the maximum tracking time as the maximum cumulative time that the target anonymity set size remains as one. Hoh et al. [27] propose the time-to-confusion metric, which is the tracking time until the adversary uncertainty (i.e., entropy) rises above a preset threshold. They also proposed another similar metric based on distance rather than time in [45].

In the context of fixed mix zones at road intersections, Buttyán et al. [9] and Freudiger et al. [19] evaluate mix zones by the success probability of an adversary in tracking vehicles. This success probability is calculated as the ratio of the number of successfully mapped vehicles (before and after the mix zone) to the total number of vehicles passed through a mix zone, averaged over all mix zones. Furthermore, Buttyán et al. [20] use the spatiotemporal information in pairs of CAMs to calculate the acceleration of the vehicles to accurately predict their next position. Then, they measure the tracking success rate as the proportion of vehicles tracked from their departure to their destination. Wiedersheim et al. [17] measure the traceability as the average duration over which a vehicle is correctly tracked. However, they allow the reconstructed traces to include false samples from traces of other vehicles. We have used traceability in our previous work [15], and defined it as the percentage of vehicle traces whose tracking percentage is more than a preset threshold (e.g., 95%).

D. Distortion

The distortion-based metric calculates the error or distortion of the reconstructed tracks compared to the actual traces. Hoh and Gruteser [26] propose the expected distance error, which captures the adversary's accuracy in estimating a user position. Similarly, Shokri et al. [46] define an expected distortion metric which can be calculated as follows. First, they find the latest position from a user observed at or before a time step t, which is denoted by e_t. Then, all paths that start from e_t and end at t are identified to calculate the expected user positions and their corresponding probabilities. Finally, the expected distortion at time step t is the total weighted distance between the expected positions and the actual position multiplied by their corresponding probabilities. The authors also define the distortion-based traceability, which is the tracking time until the distortion exceeds a preset threshold.

E. Proposed Metric

As discussed above, anonymity set size and entropy are not suitable privacy metrics. Traceability- and distortion-based metrics are more representative but their definition in related works is not accurate, as we will show later. Thus, we adopt here a combined privacy metric that is based on traceability and distortion. It is important to measure both aspects to determine how long the adversary can track a vehicle and how accurate the reconstructed tracks are related to the actual

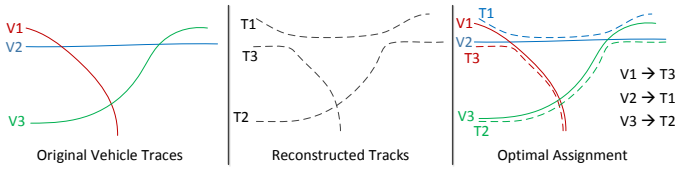


Fig. 3. The reconstructed tracks should be optimally and globally matched to the original traces to reflect the actual capability of the adversary. In this example, each track is matched to the trace of the longest match rather than that initially assigned.

traces. We hypothesize that reconstructing the entire vehicle trace is necessary to breach the driver privacy. This hypothesis is inferred from research aimed at re-identifying anonymous traces which use work/home location pairs [12], top N locations [47] or geosocial networks [13]. All these works depend on finding the places frequently visited by the user over a long period (e.g., several weeks). In VANETs, these places can be identified by correlating the source and destination of each trip, which necessitates the ability to reconstruct the entire vehicle traces. If the adversary is unable to reconstruct complete traces, then clustering techniques used in the re-identification process will fail to find the driver places.

We investigate traceability thoroughly since comparing the reconstructed tracks with the original vehicle traces is not trivial, as illustrated in Figure 3. In this example, there are three traces V1, V2 and V3 (drawn as solid lines on the left) that are reconstructed into three tracks T1, T2 and T3 (drawn as dashed lines on the middle). By visually comparing both sets, it is clear that each track is reconstructed from partial segments of the original traces. For example, T1 is reconstructed from segments of V1, V2 and V3. Traceability metrics, presented in Section VI-C, may fail to reflect the actual tracking capability of this adversary. The main issue for their definition is that they assign tracks to vehicle traces during the tracking process. In other words, they assume the track first assigned to a vehicle trace should continue with this trace until its end, as in [18], [26], [48]. However, this early assignment underestimates the length of the reconstructed tracks. For example, if the traceability of V1 is measured by assigning T1 to V1, then this metric shows a very short tracking time, although V1 is reasonably reconstructed by T3. Therefore, it is more effective if tracks are assigned to the vehicle traces globally after the tracking process is complete. The track-to-trace assignment is basically a nonlinear *assignment problem* where the total benefit should be maximized. The benefit represents the tracking period when a track t assigned to a vehicle trace v continuously. Let $l(v,t), \forall v,t \in V,T$ be the maximum continuous tracking period when the track t is assigned to the vehicle trace v. Note that t can be assigned to v for disconnected segments at different times. In this case, $l(v,t)$ represents the longest segment. The disconnected segments are not summed together because the tracking is discontinued and the track may be assigned to another vehicle trace during this discontinuity. The Let τ_v be the maximal tracking period of v; this can be obtained by solving the following assignment problem:

$$\begin{aligned} &\text{maximize} \sum_{v\in V} \tau_v \\ &\text{subject to } \tau_v = \sum_{t\in T} l(v,t)\cdot a_{v,t}, \quad a_{v,t} \in \{0,1\}, \\ &\qquad \sum_{v\in V} a_{v,t} \le 1 \quad \forall t \in T, \sum_{t\in T} a_{v,t} \le 1 \quad \forall v \in V. \end{aligned} \tag{3}$$

Here, $a_{v,t}$ is the assignment function which equals one if the track t should be assigned to the vehicle trace v, and equals zero otherwise. Note that not all tracks must be assigned to a vehicle trace because the number of tracks can be greater than the number of vehicle traces as some tracks are reconstructed from partial vehicle traces. Also, not all vehicle traces have to be assigned to a track because its $l(v,t)$ may not contribute to the maximal $\sum_{v\in V}\tau_v$. In this case, τ_v equals zero. This assignment problem is solved using an auction algorithm considering tracks as the bidders, vehicle traces as the items and $l(v,t)$ as the bidding price. After the optimal assignment is obtained, the traceability of the whole scenario is calculated by counting the percentage of significantly tracked vehicles. Thus, the traceability metric Π is defined as:

$$\Pi = \frac{1}{N}\sum_{v\in V}\lambda_v \times 100, \quad \lambda_v = \begin{cases} 1 & \frac{\tau_v}{L(v)} \ge 0.90 \\ 0 & otherwise \end{cases} \tag{4}$$

where $L(v)$ is the lifetime of v and N is the total number of traces included in the dataset. This metric allows some confusion around the endpoints of a vehicle trace (10% of the trace lifetime) since inaccuracies in endpoints can be smoothed by a clustering technique in a re-identification process, as shown in [49]. According to this definition, the privacy of the driver is considered breached if the adversary is able to continuously track 90% of her trace. Also, this metric reflects the probability of being tracked by calculating the proportion of tracked vehicles rather than how long a tracker can estimate from the actual trace as in [10], [17].

There is a shortcoming in measuring privacy using traceability only: traceability does not consider how distorted the reconstructed tracks are compared to the original traces. In most cases, high traceability necessarily indicates low distortion and vice versa because tracks are reconstructed from precise and frequent spatiotemporal samples exchanged for safety applications. However, this is not always the case, as have been detailed in [50]. Therefore, for better privacy measurement, the distortion of the assigned track should be included in the metric.

The distortion-based metric is measured by calculating how different is the assigned track from the original vehicle trace. The tracks are first assigned to vehicle traces so that the total tracking periods are maximized for the whole scenario, as defined in Equation 3. Then, the ratio of the distorted segments to the total trace length is calculated to indicate the distortion ratio. Formally, let the track t consist of spatiotemporal samples $t_p, t_{p+1}, ..., t_m$. It is assigned to the vehicle trace v, which consists of spatiotemporal samples $v_q, v_{q+1}, ..., v_n$ (i.e., $t \sim v$) where it is not necessary that $p = q$ or $m = n$. We

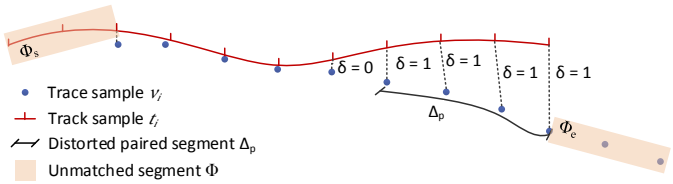


Fig. 4. Components of the proposed distortion metric for a single trace: Δ_p, ϕ_s, ϕ_e

define the distortion of sample pairs $\delta(v_i, t_i)$ at a time step $i, \forall i, max(p,q) \leq i \leq min(m,n)$ as follows:

$$\delta(v_i, t_i) = \begin{cases} 1 & Ed(v_i, t_i) > \varepsilon \quad or \quad \nexists t_i \\ 0 & otherwise \end{cases} \tag{5}$$

where $Ed(v_i, t_i)$ is the Euclidean distance between v_i and t_i and ε is a distortion threshold. According to this definition, $\delta(v_i, t_i)$ qualifies t_i as distorted if it is farther from v_i by at least ε or the adversary cannot reconstruct the sample v_i (i.e., $\nexists t_i$). The distortion threshold ε should be sufficiently large to take into account possible distance errors or time lags between v_i and t_i. We assume that a time lag of 5 s or a spatial distance of 75 m is allowed, assuming an average speed of 15 m/s.

The length of the distorted paired segments of t and v is calculated by taking the longest distorted segment from the reconstructed track or the original trace, as follows:

$$\Delta_p = \max \{ \sum_{i=max(p,q)}^{min(m,n)-1} Ed(v_{i+1}, v_i) \cdot \delta(v_i, t_i), \sum_{j=max(p,q)}^{min(m,n)-1} Ed(t_{j+1}, t_j) \cdot \delta(v_j, t_j) \} \tag{6}$$

Since the track and the original trace may start and end at different times, a penalty should be added to take these unmatched segments into account. Thus, ϕ_s and ϕ_e are defined to count this distortion as follows:

$$\phi_s = \begin{cases} \sum_{i=q}^{p-1} Ed(v_{i+1}, v_i) & p > q \\ \sum_{i=p}^{q-1} Ed(t_{i+1}, t_i) & p < q \\ 0 & otherwise \end{cases} \tag{7}$$

$$\phi_e = \begin{cases} \sum_{i=m}^{n-1} Ed(v_{i+1}, v_i) & m < n \\ \sum_{i=n}^{m-1} Ed(t_{i+1}, t_i) & m > n \\ 0 & otherwise \end{cases} \tag{8}$$

Figure 4 illustrates an example for calculating the distortion for paired and unmatched segments. In this example, the track starts before the beginning of the vehicle trace and ends before the trace end. From their paired samples, there are four distorted samples because their inter-distances are larger than ε. The unmatched segments from the trace and track are highlighted by light orange rectangles.

Given these components, the distortion of the vehicle trace v can be calculated as the ratio of the total length of the distorted segments to the length of the original trace or the length of the reconstructed track, whichever is longer, as follows:

$$D_v = \frac{\Delta_p + \phi_s + \phi_e}{\max \{ \sum_{i=q}^{n-1} Ed(v_{i+1}, v_i), \sum_{j=p}^{m-1} Ed(t_{j+1}, t_j) \}} \tag{9}$$

The distortion D of the whole scenario can be expressed as the percentage of vehicle traces where the distortion exceeds a specific ratio which guarantees preserving the driver's location privacy (e.g., $D_v > 0.25$). Formally, D can be defined as follows:

$$D = \frac{1}{N} \sum_{v \in V} \alpha_v \times 100,$$
$$\alpha_v = \begin{cases} 1 & D_v > 0.25 \quad or \quad t \nsim v \quad \forall t \in T \\ 0 & otherwise \end{cases} \tag{10}$$

Here, the trace is considered distorted if its D_v is more than 0.25 or there is no track assigned to this trace. We assume that traces distorted by at least this ratio are not beneficial in posing further privacy attacks. Since the distortion is calculated based on a track that continuously reconstructs the vehicle trace, the distorted segment will be at the trace endpoints. This means that the source and/or destination of the distorted traces cannot be reconstructed, making re-identification very difficult. Lower distortion ratios may also be sufficient to preserve privacy, but we chose a sufficiently large ratio to ensure a true privacy-preserving level.

Some vehicles never change their pseudonyms during their lifetime, which leads to perfect tracking by repeatedly matching the same pseudonym. Thus, we additionally measure the *normalized distortion* D_n by excluding these traces. This normalized metric considers the effectiveness of the privacy scheme when a vehicle changes its pseudonym at least once and is defined as:

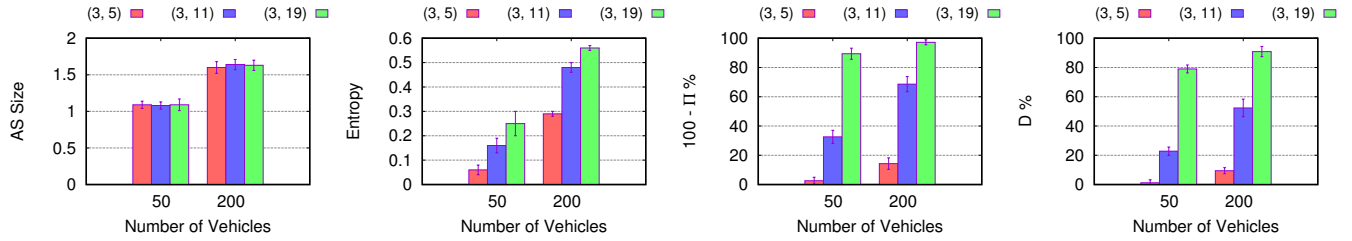
$$D_n = \frac{1}{N} \sum_{v \in V} \alpha_v^{norm} \times 100,$$
$$\alpha_v^{norm} = \begin{cases} 1 & \alpha_v = 1 \wedge psd_v(q) \neq psd_v(n) \\ 0 & otherwise \end{cases} \tag{11}$$

where $psd_v(q)$ and $psd_v(n)$ are the pseudonyms of the trace v at the first and last time steps of its lifetime, respectively.

Based on the metric definitions in Equations 10 and 11, the distortion is calculated as a ratio of the distorted segment to the total trace length, rather than a distance error, which provides a unified scale for privacy measurement. Also, this metric considers traceability implicitly since the track-to-trace assignment is obtained by maximizing the tracking period for the complete vehicle traces.

F. Metrics Comparison

In this section, we provide an experimental comparison between the presented metrics to verify their effectiveness in quantifying location privacy. The experiment consists of applying a simple privacy scheme with three parameter sets, which are known to result in low, intermediate and high privacy levels, respectively. We used STRAW vehicle traces in both low- and high-density scenarios (i.e., 50 and 200 vehicles). A



(a) Anonymity Set Size (b) Normalized Entropy (c) Reversed Traceability (d) Distortion

Fig. 5. Privacy metrics comparison in random silent period using STRAW vehicle traces. AS size shows no variation among schemes of different strengths. Normalized entropy does not show a unified privacy level among different densities. Traceability and distortion metrics show reasonable variations among different schemes and densities.

good privacy metric should show reasonable variation among different parameter sets and different densities. We chose the random silent period (RSP) privacy scheme, which keeps the pseudonym for a fixed preset time (120 s) and then keeps silent for a random time period and changes the pseudonym afterwards. We selected random silent periods of (3, 5) s[2], (3, 11) s and (3, 19) s to achieve low, intermediate and high privacy levels, respectively. We applied the RSP with each parameter set to the traces dataset of each density 10 times. We then used the vehicle tracker to track pseudonymous CAMs generated by the RSP.

The traceability and distortion metrics are calculated as defined in Equations 4 and 10, respectively. For the anonymity set (AS) size, we calculate the maximum AS size encountered by each vehicle and then taking the average over all vehicles. The maximum AS size of a subject vehicle is obtained by finding the maximum number of nearby vehicles, including itself, that changed their pseudonyms simultaneously with a pseudonym change by this subject vehicle. Two vehicles are considered nearby if they are located within a distance of 100m. For the entropy, we calculate the maximum normalized entropy $\mathcal{H}_n$, defined in Equation 2, of the pseudonym changes made by a vehicle and then take the average over all vehicles.

Figure 5 shows the results of each metric with the three silent periods in low and high density scenarios. In Figure 5a, the AS size is almost the same in all silent periods with a slight difference between low and high densities. This highlights the inability of the AS size to discriminate among the capabilities of different privacy schemes. The normalized entropy overcomes this problem and shows consistent variation among different silent periods, as illustrated in Figure 5b. However, the entropy values are misleading because they do not reflect the true privacy level in different scenarios. For example, the normalized entropy of the RSP (3, 5) in the dense traffic is higher than the RSP (3, 19) in the sparse traffic. This is true regarding the adversary's uncertainty, which will be greater in a dense environment due to, for example, the larger AS size. However, the privacy gained with the RSP (3, 5) in dense traffic is not that high because most of the vehicle traces ($\geq 90\%$) can be reconstructed effectively, as we now demonstrate.

[2](α, β) s refers to a period of α to β seconds. It should not be misinterpreted as reference numbers.

In Figure 5c, we show the reversed traceability (i.e., $100-\Pi$) instead of the traceability metric to reflect the privacy level and to be consistently comparable with other metrics. It shows a significantly different variation from that given by the entropy metric. In contrast to the entropy, it demonstrates a low privacy level in dense traffic when using a short silent period of (3, 5) s. Also, it shows that privacy can effectively be preserved in sparse traffic when using a relatively long silent period of (3, 19) s. This difference in the variation distribution of the reversed traceability arises from the fact that it measures the effectiveness of reconstructing complete vehicle traces rather than the adversary's uncertainty. Last but not least, the distortion metric produces variations similar to the reversed traceability, but it reduces the percentage values, indicating lower privacy. This reduction is a result of the distortion metric filtering out the cases when vehicles are completely tracked but their reconstructed tracks are still different from the original vehicle traces.

VII. Safety Metric

As discussed in Section II, QoS can be measured in various manners. However, we presume that the appropriate QoS metric of a privacy scheme should reflect the deficiency in application performance, rather than absolute distance errors or time delays. The issue in measuring QoS as a distance error or a time delay is that it does not explain the actual robustness of the application against information inaccuracy or delay. We focus on measuring the QoS of safety applications in our analysis because privacy schemes modify the CAMs on which safety applications depend. In addition, safety applications have the most restricted constraints regarding information accuracy, frequency and latency. If a privacy scheme does not hinder the QoS of safety applications, it will not do so for other applications as well. In [14], we proposed formulating application requirements using Monte Carlo numerical analysis to estimate the QoS of a forward collision warning (FCW) application. Here, we apply the same approach to measure the QoS of a lane change warning (LCW) application. But we first briefly explain how the metric is calculated.

A. Proposed QoS metric

The main idea of the proposed QoS metric is to formulate the probability of estimating safety application requirements

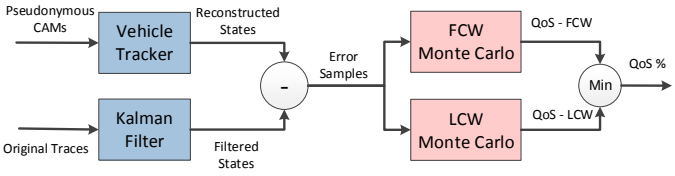


Fig. 6. Block diagram of the QoS metric calculation. Error samples in position are calculated between the reconstructed and filtered traces. These error samples are then used to estimate the probability of accurately calculating the application requirements.

in terms of vehicle states. Examples of these requirements are correctly identifying the lane of the vehicle and calculating the time-to-collision with a leading vehicle. Monte Carlo numerical analysis is used to calculate these probabilities, given the vehicle states altered by a privacy scheme. Once the probability of each requirement is estimated, all these probabilities are combined to express the QoS metric. This QoS measurement method is inspired by the approach presented by Shladover and Tan [32] to determine the probability of providing useful Cooperative Collision Warning (CCWs) as a function of the position and speed accuracy. We apply the same concept with similar assumptions, which are as follows:

1) The position and velocity obtained from vehicle sensors are erroneous and their errors follow a Gaussian distribution.
2) To simplify the formulation of the requirements, it is assumed that vehicles are driving on straight roads, centered in their lanes and have constant speed without changing their lane.
3) Communication and computation delays are ignored.

These assumptions are considered to simplify the Monte Carlo equations without loss of generality. The second assumption applies only during instantaneous Monte Carlo calculations. If this assumption were to be removed, the equations would become complex because it would be necessary to consider the vehicle heading, position and velocity in both lateral and longitudinal coordinates [3].

To produce stable estimations, Monte Carlo analysis requires a large number of samples drawn from the random distribution of the measurement errors. As position and velocity measurements are necessarily erroneous and are sometimes eliminated during silence periods to preserve privacy, generating such samples should be performed carefully to reflect the correct representation of the data. To estimate the error distribution originating from a privacy scheme, we assume that the subject vehicle tracks the surrounding vehicles continuously aiming to enhance their measurements and also predict their states when CAMs are missed. In this case, the safety application works like a local tracker that tracks and filters measurements received from other vehicles.

The error samples of a privacy scheme are generated as follows and illustrated in Figure 6. Initially, we add a basic noise to positions and speeds specified in the vehicle traces dataset. The basic position noise is drawn from a Gaussian distribution with a standard deviation of 0.5 m. The basic speed noise is assumed to have a Gaussian distribution, and its standard deviation equals 2% of the actual speed. Next, the vehicle tracker tries to track the pseudonymous CAMs, containing noised positions and speeds and altered by a privacy scheme. The position and speed errors between the reconstructed tracks and the true traces are then calculated for all vehicles and time steps. These error samples are collected and used directly in the Monte Carlo analysis

The true traces used in calculating error samples are slightly different from the original traces. Generally, the Kalman filter modifies the position and speed from those recorded in the traces dataset to reduce presumed noise even if no noise or privacy scheme is applied. These enhancements will contribute to the extracted error samples if the original traces are used as the ground truth. Thus, we calculate the error samples by taking the *filtered traces* as the ground truth. These filtered traces are obtained by applying the Kalman filter on each vehicle trace individually and taking the position and speed of the estimated state every time step. Thus, the error samples are guaranteed to originate from changes made by the privacy scheme only, not from changes made by the Kalman filter. Moreover, the error samples are measured in the scenario global coordinate, but, according to our assumptions, they need to be in the vehicle coordinates (i.e., lateral and longitudinal). The error sample Δ is formally calculated as follows:

$$\Delta = \begin{bmatrix} \delta x \\ \delta \dot{x} \\ \delta y \\ \delta \dot{y} \end{bmatrix} = \begin{bmatrix} \mathbf{R} & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{bmatrix} \cdot (\hat{\mathbf{x}}_p - \hat{\mathbf{x}}_f), \quad \mathbf{R} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{12}$$

where θ is the vehicle heading, $\hat{\mathbf{x}}_p$ is the estimated vehicle state by the tracker and $\hat{\mathbf{x}}_f$ is the filtered state. Both $\hat{\mathbf{x}}_p$ and $\hat{\mathbf{x}}_f$ consist of position and velocity in xy global coordinates. We will now show how these error samples are used to estimate the QoS of the FCW and LCW applications.

B. Forward Collision Warning Application

The FCW application aims to provide the driver of the subject vehicle (SV) a sufficiently early alert that a possible collision with another vehicle (OV) in the same lane is likely to happen. To achieve this functionality, the application must be able to (1) identify the correct lane of OVs and (2) estimate the time to collision (TTC) within a small tolerance. To satisfy the first requirement, accurate lateral positions of the SV and OVs must be known. To satisfy the second requirement, knowledge of the longitudinal positions and speeds of the SV and the next OV in the same lane is necessary. As explained in [14], the true and false positive probabilities for correctly identifying lanes of the OVs can be calculated by:

$$P_{true+} = P(|y_{OV1} - y_{SV}| \leq 1.8) \tag{13}$$

$$P_{false+} = P(|y_{OV2} - y_{SV}| \leq 1.8) \tag{14}$$

For the second requirement, we assume that the SV is approaching the OV1 at speed differences Δs of 5 m/s and 15

[3]The lateral and longitudinal coordinates are perpendicular and parallel to the road direction, respectively. Hereafter, the longitudinal coordinate is referred to by x while the lateral coordinate is referred to by y.

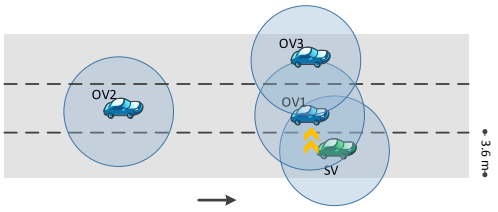


Fig. 7. Lane change warning scenario. SV needs to change to the left lane while OV1 is located in the blind spot, OV2 may cause a rear collision if it is moving too fast; OV3 is located in the third lane and should not pose any collision threat.

m/s. The assumed true TTC is set to three seconds as an example; thus, the true position of OV1 is generated to be three seconds distant from the true position of SV. Here, there is no binary classification to calculate false positives; instead, we calculate the probability of calculating TTC within a small tolerance of 500 ms. This 500 ms tolerance is chosen by Shladover and Tan [32] as the maximum tolerance for issuing a useful warning. Therefore, the TTC and the probability of correctly estimating it within 500 ms can be calculated by:

$$TTC = \frac{x_{OV1} - x_{SV}}{\dot{x}_{SV} - \dot{x}_{OV1}} \tag{15}$$

$$P_{TTC} = P(|TTC - 3| \leq 0.5) \tag{16}$$

In this equation, we determine how frequently the difference between the calculated TTC and the true TTC (i.e., 3 s) is less than the tolerance threshold of 0.5 s. Finally, the probability of an accurate FCW application (P_{FCW}) can be obtained by multiplying all three probabilities together, assuming they are independent, as follows:

$$P_{FCW\Delta s} = P_{true+} \times (1 - P_{false+}) \times P_{TTC\Delta s} \tag{17}$$

C. Lane Change Warning Application

There are two main scenarios that concerns LCW application: *blind spot* and *overtaking*, as shown in Figure 7. In the blind spot scenario, OV1 moves in the adjacent lane of the SV at approximately the same speed and slightly behind it, which poses a threat of collision when the SV changes its lane. Therefore, the LCW application deployed in the SV should give an alert about OV1, but not about OV3 as it is located in the third lane and does not threaten the SV. In the overtaking scenario, the approaching OV2 comes from the rear with a high closing speed, such that it arrives adjacent to the SV at the same time as the lane change. If OV2 is moving at a speed that allows it to reach the adjacency of the SV at the time of lane change, then a warning should be issued as it is an overtaking threat. This shows that, the overtaking scenario is just like that of FCW, but the positions of SV and OV are reversed. Thus, we will only analyze the blind spot scenario here.

To handle the blind spot scenario, three requirements must be correctly identified by the SV. The first requirement is to identify the lateral position of OV1 in the adjacent lane (i.e., its true center is 3.6 m away from the SV). Additionally, its longitudinal position should be estimated slightly behind the SV, say between 1.5 m and 6 m from the longitudinal position of the SV. Thus, its true longitudinal position is assumed to be in the middle of this range (i.e., 3.75 m from the SV). The second requirement is to recognize OV3 as not located in the adjacent lane, which means its true lateral position is 7.2 m away from the SV. The last requirement is that the speeds of OV1 and SV should be recognized to be similar within a small margin of 3 m/s as an example. Therefore, the true speeds of SV and OV1 are assumed to be the same. In our analysis, we assume that the errors of the SV measurements are just the basic error in position and speed, as the SV obtains these values through its own sensors, rather than through VANET communication. According to these requirements, the measured positions and speeds of SV, OV1 and OV3 are defined as follows:

$$\begin{aligned} y_{SV} &= 1.8 + \mathcal{N}(0, 0.5) \\ x_{SV} &= 3.75 + \mathcal{N}(0, 0.5) \\ \dot{x}_{SV} &= \hat{x}_{SV} + \mathcal{N}(0, 0.02 \cdot \hat{x}_{SV}) \\ y_{OV1} &= 5.4 + \delta y \\ x_{OV1} &= \delta x \\ \dot{x}_{OV1} &= \hat{x}_{OV1} + \delta \dot{x} \\ y_{OV3} &= 9 + \delta y \end{aligned} \tag{18}$$

where $\hat{x}$ is the filtered longitudinal speed and $\hat{x}_{SV} = \hat{x}_{OV1}$. The Monte Carlo equations of each requirement need some further analysis. Assuming 2 m wide SV and OV1, OV1 must leave enough space for the SV to enter the adjacent lane. This means that when the SV changes its lane, the center of OV1 should be 3 m away from the right edge of the lane. Thus, the warning of a blind spot should be fired if the estimated distance between SV and OV1 less than or equal to 4.8 m. To avoid a false alert about OV3, assume a 3 m wide vehicle moving just along the edge of the third lane. Then, its center is 1.5 m away from the lane boundary. Thus, when the distance between centers of SV and OV3 is more than 6.9 m, the system must not warn. Therefore, the true positive probability is calculated when OV1 is estimated within a distance less than 6.9 m. The false positive probability is calculated when OV3 is estimated within a distance less than or equal 4.8 m. Additionally, the longitudinal position of OV1 must be estimated within the blind spot so that it is not easily visible to the SV driver (i.e., 1.5 - 6 m behind the SV). Also, the speeds of SV and OV1 should be estimated to be similar within small tolerance of 3 m/s. These probabilities can be formulated as follows:

$$P_{true+} = P(y_{OV1} - y_{SV} < 6.9) \tag{19}$$

$$P_{false+} = P(y_{OV3} - y_{SV} \leq 4.8) \tag{20}$$

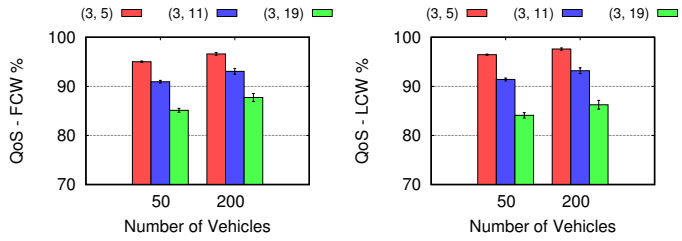
$$P_{long} = P(x_{SV} - x_{OV1} < 6 \wedge x_{SV} - x_{OV1} > 1.5) \tag{21}$$

$$P_s = P(|\dot{x}_{OV1} - \dot{x}_{SV}| \leq 3) \tag{22}$$

The probability of an accurate LCW application (P_{LCW}) can be obtained by multiplying these probabilities together, assuming they are independent as follows:

$$P_{LCW} = P_{true+} \times (1 - P_{false+}) \times P_{long} \times P_s \tag{23}$$

To measure the impact of a privacy scheme on the QoS of safety applications, both P_{FCW} and P_{LCW} are calculated, and then the minimum value is taken and multiplied by 100



(a) Forward Collision Warning (b) Lane Change Warning

Fig. 8. The QoS of FCW and LCW applications in STRAW traces modified by random silent period privacy scheme and CAM rate = 2 Hz. In all cases, QoS of more than 90% can be achieved when a silent period of (3, 11) s is employed.

to express on the final QoS percentage. Formally, the QoS of a privacy scheme is defined as:

$$QoS = min\{P_{FCW}, P_{LCW}\} \times 100 \quad (24)$$

D. QoS of random silent period

We evaluate the QoS of the random silent period (RSP) privacy scheme on STRAW vehicle traces using the proposed metric. Similar to the experiment in Section VI-E, we selected silent periods of (3, 5) s, (3, 11) s and (3, 19) s which should achieve high, intermediate and low QoS, respectively, since the longer the silence, the harder to predict vehicle states and the lower the QoS. Figure 8 shows that a QoS of at least 91% can be achieved for both applications and traffic densities if a silent period up to (3, 11) s is used before a pseudonym change. The QoS is expected to be slightly higher in dense traffic because vehicles drive at lower speeds which, in turn, results in lower absolute speed noise (Note that speed noise is assumed to be 2% of vehicle speed).

This experiment shows a different result from that claimed by Lefevre et al. [29]. They claim that an intersection collision system can function only with silent periods of less than two seconds. This difference comes from our assumption that an in-vehicle tracker is utilized to predict vehicle states during silence. Results shown in Figures 5 and 8 confirm that it is possible to preserve location privacy without hindering the functionality of safety applications. For example, an RSP of (3, 19) s can achieve a privacy level of 80% in terms of tracking distortion with a loss of about 15% in the QoS of safety applications. Advanced privacy schemes will compromise this trade-off more effectively, as explained in the next section.

VIII. Comparison of Privacy Schemes

In this section, selected privacy schemes are evaluated and compared using proposed privacy and QoS metrics. The selected schemes are RSP [48], SLOW [20], CSP [51], CPN [52], CAPS [15] and CADS [35]. We first explain briefly these schemes and then show their evaluation.

A. Description of Schemes

In SLOW [20], a vehicle continuously checks its current speed and broadcasts CAMs only when its speed is higher than a preset threshold SP. If a vehicle does not send CAMs for ST time steps, it changes its pseudonym.

Coordinated Silent Period (CSP) is proposed by Tomandl et al. [51] in their comparison of silent period and mix zone schemes. CSP coordinates all vehicles in the network to remain silent and change pseudonyms synchronously. CSP seems to be theoretical, since the coordination overhead in real world situations increases dramatically [51]. However, CSP increases privacy significantly because it maximizes the size of the anonymity set at every pseudonym change.

In the Cooperative Pseudonym change scheme based on the number of Neighbors (CPN) [52], vehicles monitor their neighbors within radius R and wait until they reach a threshold K. When this trigger occurs, the vehicle sets an internal flag $ready\_flag$, broadcasts this flag within the CAM and changes the pseudonym in the next CAM. When a vehicle receives a CAM with a set flag or its internal flag is set already, it changes its pseudonym immediately.

Context-Aware Privacy Scheme (CAPS) [15] monitors surrounding vehicles through their CAMs using an in-vehicle tracker. If the vehicle determines that a previously identified neighbor has become silent, it becomes silent as well. When a vehicle is silent, it resumes broadcasting CAMs if its state could be confused with another silent neighbor.

Context-ADaptive privacy Scheme (CADS) [35] is based on CAPS but allows a driver to choose among privacy preferences of low, normal or high. It optimizes the internal parameters of CAPS dynamically according to the driver's privacy preference and the density of the surrounding traffic.

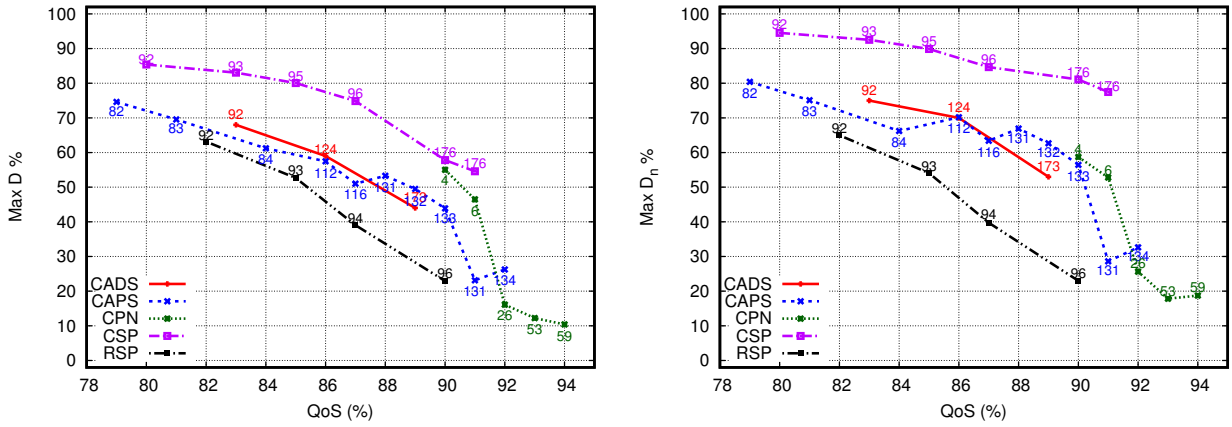
B. Comparison

We implemented the selected privacy schemes in MATLAB as a centralized program, which operates on individual vehicles in parallel. For each time step of the vehicle traces, the program determines if a CAM would be broadcast by a vehicle and when a pseudonym should be changed based on the procedures of the privacy scheme. We employed the realistic traces in this experiment and tested several parameter sets for each scheme as listed in Table I. Recently, we have implemented these schemes in an open-source privacy extension for Veins framework, called PREXT [53][4], which allows readers to verify the presented results and evaluate other schemes using unified privacy metrics.

Since privacy schemes have different assumptions and parameters, they were aligned to their QoS levels rounded to the nearest integer. Then, the maximum (normalized) distortion that can be achieved in each QoS level is selected, along with the average pseudonym lifetime selected by vehicles to achieve this maximum distortion. Figure 9 illustrates this comparison among RSP, CPN, CSP, CAPS and CADS. The SLOW scheme is omitted because it results in very low QoS levels (only 50% on average with speed threshold of 6 m/s). This significantly low QoS occurs because of the large number of eliminated CAMs at low speeds.

CSP provides the highest distortion of all schemes given a similar QoS level. It results in a high QoS of up to 91%

[4]https://github.com/karim-emara/PREXT



(a) Distortion (b) Normalized Distortion

Fig. 9. Distortion versus QoS levels of different VANET privacy schemes in TAPASCologne traces. Numbers written on the graph lines represent the average pseudonym lifetime in seconds. CSP achieves the highest distortion levels with QoS up to 91%. CPN achieves high QoS levels up to 94% but with intermediate distortion levels and short pseudonym lifetimes. CAPS and CADS provide a practical compromise between distortion and QoS while RSP performs worse than the others.

TABLE I
PARAMETER TEST RANGES FOR THE EVALUATED SCHEMES.

Scheme	Parameter (unit)	Test Range
RSP [48]	Pseudonym lifetime (min) Max silence time (s)	2 7, 11, 15, 19
CSP [51]	Pseudonym lifetime (min) Fixed silence time (s)	2, 5 5, 7, 9, 11
SLOW [20]	Speed threshold SP (m/s) Silent threshold ST (s)	3, 6, 8 10, 15, 20, 30
CPN [52]	Neighborhood radius R (m) No. of neighbors K	10, 20, 30, 50 3, 5, 7
CAPS [15]	Pseudonym lifetime (min) Max silence time (s) Neighborhood Radius (m)	2, 5 5, 7, 9, 11 50, 100
CADS [35]	Privacy preference of all vehicles	Low, Normal, High

and requires a reasonable average pseudonym lifetime of about 3 min. However, global coordination among all vehicles in the network is challenging. Also, further investigation is required to study possible implications of or attacks on this globally coordinated silence. The delivery of packets and handling safety-critical situations during the scheduled silence are just two examples that make the CSP unpractical. The next best scheme is the CPN, which results in the highest QoS levels because it does not employ any silence before a pseudonym change. It can result in high distortion levels but with a significantly short pseudonym lifetime of 4 s. This is a serious drawback of CPN because it requires these frequent pseudonym changes to preserve privacy. RSP achieves a good distortion level but at a cost in QoS. Higher QoS levels can be attained but with low distortion levels.

CAPS and CADS provide practical compromises between distortion, QoS and pseudonym lifetime. The performance of CAPS varies according to the provided parameters. CAPS can provide about 60% of normalized distortion when the QoS is 90%. The average pseudonym lifetime ranges from 1.3 min to 2.2 min, depending on the achieved distortion and QoS levels. CADS let drivers choose which privacy level matches their preferences. The normal privacy preference results in distortion of 60% and QoS of 86%. The average pseudonym lifetime ranges from 1.5 min to 3 min.

C. Comparison with Mix Zone

We evaluate mix zones qualitatively because they are usually evaluated against timing and transition attacks. Since the tracker utilized does not support these attacks, quantitative evaluation will not represent the actual performance of these schemes.

Mix zones are usually placed at road intersections since vehicle movements are not predictable. Within a mix zone, the exchanged CAM messages must be encrypted [19], or vehicles must be silent [9]. If vehicles change their pseudonyms within the mix zone, the adversary cannot correlate leaving vehicles with those entering the zone earlier because movement cannot be predicted. Mix zones have the following drawbacks when compared to privacy schemes evaluated above:

- **Timing and transition attacks.** An adversary can utilize additional knowledge about the timing and transition among different entry and exit points of the intersection. Buttyán et al. [9] showed that a tracking success rate of up to 70% can be achieved by covering only half of the mix zones.
- **RSU dependability.** Mix zones depend on RSUs to coordinate silence periods or distribute encryption keys. However, it is not expected that RSUs will be widely deployed, especially in the initial deployment of VANET.
- **Active attacks for cryptographic zones.** An active attacker may participate in the cryptographic mix zones and obtain the shared key. Once the key is obtained, the mix zone becomes useless.
- **Safety concerns for silence-based zones.** Road intersections or joints are risky places in road networks. In fact,

intersection crashes represent 26% of all crashes in the USA [54]. Silence-based mix zones are at variance with this fact because it is inappropriate to remain silent in places where it is important to exchange safety messages.

IX. Conclusion

In this paper, privacy and QoS metrics for privacy schemes in VANET are reviewed in detail and experimentally evaluated. A privacy metric that is based on traceability and distortion is formally defined and compared with entropy and AS size metrics. Based on the comparison of privacy metrics, the proposed distortion metric provides a unified scale when comparing privacy schemes of different strengths at different traffic densities. In addition, a QoS metric for two safety applications FCW and LCW is proposed and verified on the random silent period scheme, showing a reasonable QoS reduction as the silence duration is increased. Finally, six privacy schemes are discussed and compared in terms of the proposed metrics using realistic traces. Based on the experimental comparison, we reach the following conclusion. First, the coordinated silent period (CSP) scheme provides the greatest privacy and QoS levels but global coordination among all vehicles is very challenging and needs further investigation regarding possible attacks or implications. Second, the cooperative pseudonym change (CPN) scheme can result in a good privacy level with a reasonably high QoS but requires very short pseudonym lifetimes, making it impractical. Third, both CAPS and CADS provide a more practical compromise among acceptable privacy and QoS levels and relatively long pseudonym lifetime. Last but not least, mix zones are effective in reducing traceability, but they suffer from some issues such as transition and timing attacks, active attacks and dependability of road-side units. In future work, we will investigate how to deploy different privacy schemes collaboratively over the road network to get benefit of the advantages of each.

Acknowledgment

The authors would like to thank Björn Wiedersheim for providing his vehicle traces. This work has received funding from the European Union's Horizon 2020 research and innovation programme within the Privacy Flag project under grant agreement No. 653426.

References

[1] N. H. T. S. A. (NHTSA), "Advance notice of proposed rulemaking (ANPRM) (Docket No. NHTSA-2014-0022)," http://www.regulations.gov/#!documentDetail;D=NHTSA-2014-0022-0002, Aug. 2014, [Online; accessed Sep-2015].

[2] European Telecommunications Standards Institute, "ETSI TS 102 940 V1.1.1," *Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*, Jun 2012.

[3] Privacy Flag, "Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments, PN: 653426," http://privacyflag.eu, [Online; accessed Sep-2016].

[4] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 17, no. 1, pp. 228–255, Firstquarter 2015.

[5] A. Boualouache, S. M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–7.

[6] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems," in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, ser. IoV-VoI '16. New York, NY, USA: ACM, 2016, pp. 7–12. [Online]. Available: http://doi.acm.org/10.1145/2938681.2938684

[7] European Telecommunications Standards Institute, "ETSI TS 102 941 V1.1.1," *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, Jun 2012.

[8] "Ieee standard for wireless access in vehicular environments security services for applications and management messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, April 2013.

[9] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of the 4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks*, ser. ESAS'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 129–141. [Online]. Available: http://dl.acm.org/citation.cfm?id=1784404.1784417

[10] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *Fourth International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*, Madrid, Spain, Jun. 2013.

[11] ——, "Beacon-based Vehicle Tracking in Vehicular Ad-hoc Networks," TECHNISCHE UNIVERSITÄT MÜNCHEN, Tech. Rep., Apr. 2013. [Online]. Available: http://mediatum.ub.tum.de/attfile/1144541/hd2/incoming/2013-Apr/691293.pdf

[12] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proceedings of the 7th International Conference on Pervasive Computing*, ser. Pervasive '09. Berlin, Heidelberg: Springer-Verlag, May 2009, pp. 390–397.

[13] A. Cecaj, M. Mamei, and N. Bicocchi, "Re-identification of anonymized CDR datasets using social network data," in *The Third IEEE International Workshop on the Impact of Human Mobility in Pervasive Systems and Applications*. Ieee, Mar. 2014, pp. 237–242.

[14] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Computer Communications*, vol. 63, pp. 11–23, June 2015.

[15] ——, "CAPS: Context-Aware Privacy Scheme for VANET Safety Applications," in *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '15. New York, NY, USA: ACM, 2015.

[16] V. S. C. Consortium, *Vehicle Safety Communications Project: Task 3 Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*. National Highway Traffic Safety Administration, Office of Research and Development, Washington, D.C., 2005.

[17] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, Feb. 2010, pp. 176 –183.

[18] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1569 –1589, Oct. 2007.

[19] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, Vancouver, Aug. 2007.

[20] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," in *2009 IEEE Vehicular Networking Conference (VNC)*. IEEE, Oct. 2009, pp. 1–8.

[21] Y.-C. Wei and Y.-M. Chen, "Safe Distance Based Location Privacy in Vehicular Networks," in *2010 IEEE 71st Vehicular Technology Conference*. Ieee, 2010, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5494209

[22] B. Palanisamy and L. Liu, "Attack-resilient Mix-zones over Road Networks: Architecture and Algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6815691

[23] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 1, pp. 93–105, Jan. 2016. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2015.2399291

[24] E. Schoch, F. Kargl, T. Leinmller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *Security and Privacy in Ad-Hoc and Sensor Networks*, ser. Lecture

Notes in Computer Science, L. Buttyán, V. Gligor, and D. Westhoff, Eds. Springer Berlin Heidelberg, 2006, vol. 4357, pp. 43–57. [Online]. Available: http://dx.doi.org/10.1007/11964254_6

[25] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks - VANET '07*. New York, New York, USA: ACM Press, 2007, pp. 19–28. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1287748.1287752

[26] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, ser. SECURECOMM '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 194–205. [Online]. Available: http://dx.doi.org/10.1109/SECURECOMM.2005.33

[27] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 161–171. [Online]. Available: http://doi.acm.org/10.1145/1315245.1315266

[28] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, "Impact of vehicular communications security on transportation safety," in *INFOCOM Workshops 2008, IEEE*. IEEE, 2008, pp. 1–6.

[29] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in *Vehicular Networking Conference (VNC), 2013 IEEE*, Dec 2013, pp. 71–78.

[30] European Telecommunications Standards Institute, "ETSI TS 102 867 v1.1.1," *Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2*, Jun 2012.

[31] "SAE J2735 V1.1.1 - Dedicated Short Range Communications (DSRC) Message Set Dictionary," *SAE Standard*, 2009. [Online]. Available: http://standards.sae.org/j2735_200911/

[32] S. E. Shladover and S.-K. Tan, "Analysis of vehicle positioning accuracy requirements for communication-based cooperative collision warning," *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, pp. 131–140, Jan. 2006.

[33] R. Sengupta, S. Rezaei, S. E. Shladover, D. Cody, S. Dickey, and H. Krishnan, "Cooperative collision warning systems: Concept definition and experimental implementation," *Journal of Intelligent Transportation Systems: Technology, Planning, and Operations*, pp. 143–155, Jun. 2007.

[34] F. Hrizi, J. Härri, and C. Bonnet, "Can Mobility Predictions Be Compatible with Cooperative Active Safety for VANET?" in *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, ser. VANET '12. New York, NY, USA: ACM, 2012, pp. 111–114. [Online]. Available: http://doi.acm.org/10.1145/2307888.2307909

[35] K. Emara, W. Woerndl, and J. Schlichter, "Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks," *ArXiv e-prints*, Jul. 2016.

[36] D. R. Choffnes and F. E. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*. ACM, Sept 2005, pp. 69–78.

[37] S. Uppoor and M. Fiore, "Vehicular mobility trace of the city of cologne, germany," 2011, [Online; accessed 20-January-2015]. [Online]. Available: http://kolntrace.project.citi-lab.fr/

[38] "TAPASCologne project," 2010, [accessed 20-January-2015]. [Online]. Available: http://sourceforge.net/projects/sumo/files /traffic_data/scenarios/TAPASCologne

[39] S. Uppoor, O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, "Generation and analysis of a large-scale urban vehicular mobility dataset," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 1061–1075, 2014.

[40] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, ser. PET'02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 41–53.

[41] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, ser. PET'02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 54–68. [Online]. Available: http://dl.acm.org/citation.cfm?id=1765299.1765304

[42] L. Fischer, S. Katzenbeisser, and C. Eckert, "Measuring unlinkability revisited," *Proceedings of the 7th ACM workshop on Privacy in the electronic society - WPES '08*, p. 105, 2008. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1456403.1456421

[43] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Security and Privacy (SP), 2011 IEEE Symposium on*, May 2011, pp. 247–262.

[44] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent cascade: Enhancing location privacy without communication qos degradation," in *Proceedings of the Third International Conference on Security in Pervasive Computing*, ser. SPC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 165–180. [Online]. Available: http://dx.doi.org/10.1007/11734666_13

[45] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceeding of the 6th international conference on Mobile systems, applications, and services*, 2008, pp. 15–28.

[46] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy," in *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, ser. WPES '09. New York, NY, USA: ACM, 2009, pp. 21–30. [Online]. Available: http://doi.acm.org/10.1145/1655188.1655192

[47] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '11. New York, NY, USA: ACM, 2011, pp. 145–156.

[48] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, March 2005, pp. 1187–1192 Vol. 2.

[49] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing Security and Privacy in Traffic-Monitoring Systems," *Pervasive Computing, IEEE*, vol. 5, no. 4, pp. 38–46, 2006.

[50] K. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Ph.D. dissertation, München, Technische Universität München, 2016.

[51] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in vanets," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 165–172.

[52] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in {VANETs}," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599 – 1609, 2013.

[53] K. Emara, "Poster: Prext: Privacy extension for veins vanet simulator," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–2.

[54] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," National Highway Traffic Safety Administration, Washington, DC, Tech. Rep., August 2014.

Karim Emara received his PhD in Computer Science from the Technical University of Munich (TUM), Germany in 2016 with Highest degree of Honor. He was awarded a full scholarship from Deutscher Akademischer Austauschdienst (DAAD) to pursue his PhD in Germany. Then, he was a PostDoc Fellow in the Connected Mobility chair in TUM supervised by Prof. Jörg Ott until September 2016. Afterwards, he joined the Networking Research Group (Netlab), headed by Prof. Thomas Engel, as a Research Associate in the Interdisciplinary Centre for Security, Reliability and Trust (SnT), Luxembourg. Currently, he is an assistant professor in Faculty of Computer and Information Sciences, Ain Shams University, Egypt. His research interests include mobile networks, in particular, vehicular networks, location privacy and applications of intelligent transportation systems.