Pseudonym Inference in Cooperative Vehicular Traffic Scenarios

Xu Chu[†], Na Ruan[*†], Ming Li[‡], and Weijia Jia[§†]
[*]Corresponding author, Email: naruan@cs.sjtu.edu.cn
[†]Dept. of CSE, Shanghai Jiao Tong University, Shanghai, P. R. China
[‡]Dept. of ECE, University of Arizona, Tucson, AZ, USA
[§]Dept. of CIS, University of Macau, P. R. China

***Abstract*—Vehicle platooning is a promising technique to enhance travel safety and road capacity. A common form of platooning is Cooperative Adaptive Cruise Control (CACC), where cars communicate their states with each other to maintain a constant gap between them. CACC can further reduce the headway between adjacent vehicles. However, the frequently broadcast safety messages with precise location and time information impose a significant threat to the location privacy of cars. Mix-zone based approaches are traditionally used to obfuscate vehicles' identities by mixing their pseudonyms. However, vehicles' movement is tightly coupled with each other inside a vehicular platoon, which introduces high predictability and spatial-temporal correlation for trajectories of vehicles. In this paper, we show how an adversary can exploit vehicles' platooning states to better infer their pseudonyms by observing their broadcast states before and after entering a mix-zone. We propose a novel attack strategy using a maximum likelihood estimator and expectation-maximization algorithm, and demonstrate the effectiveness of this attack through extensive simulations based on the real data from U.S. Highway 101. Our strategy achieves 30% higher inference accuracy compared with traditional non-platooning traffic scenarios. We also suggest a few possible approaches to mitigate such privacy threat in a platooning environment.**

***Keywords*—Location privacy, mix-zone, vehicle platoon, vehicular ad-hoc networks (VANETs).**

I. Introduction

With the development of automobile industry and urbanization, more and more vehicles are on the highway linking adjacent cities. As a result, a series of critical issues are becoming more severe in modern transportation systems, such as traffic congestion, traffic accidents, energy waste, and pollution. Although the investment on road construction can alleviate traffic congestion to some extent, it is not sustainable because of the enormous construction cost and limited availability of land. A practical approach is to change the driving pattern from individual driving to a platoon-based driving. In general, the platoon-based driving pattern is a cooperative driving pattern, in which a car follows another one, communicates with others, and maintains a small and nearly constant distance to the preceding vehicle. This approach has been proved to be a feasible technology to increase road capacity, traffic safety and reduce energy consumption.

CACC is introduced taking advantage of Vehicle to Vehicle (V2V) communication to realize longitudinal automated vehicle control, with Global Positioning System (GPS) and the sensing module as the complement of the communication structure in case of 802.11p-based V2V communication error. The lead vehicle specifies platoon characteristics including inter and intra platoon spacing, acceleration and velocity interval. The followers only communicate with its directly preceding one, taking communication delay and heterogeneity of the traffic into account to enable the vehicles driving at smaller inter-vehicle distances while the platoon stability is guaranteed. The communicating message is periodically (e.g., every 100 to 300 ms) broadcast to continuously offer the activity of the driver, while such beacons may increase safety as they are transmitted via a wireless channel they may be eavesdropped upon.

High safety though it provides, the use of safety message can cause huge problems. Beacons broadcast through the wireless channel are rich in information about the vehicles, most importantly, the location information of the vehicle itself. With the information, it is possible for an adversary to get the location of the home or working place, and may further find out the real identification of the drivers. Given this, location privacy should be guaranteed before the public widely accepts VANETs.

The solution is to use a pseudonym, which is a kind of identifier used to authenticate safety messages. The pseudonym changes are aiming to break the linkability between the vehicle and its identity [3]. However, improper ways of changing pseudonym may fail to provide location privacy, for the safety messages can still link the two pseudonyms together [4]. Changing pseudonym in a region together breaks the linkability between the vehicles entering and leaving aliases and is a more feasible solution. Such mixed region is called a mix-zone [4]. An external attacker can only eavesdrop communications outside the mix-zone, and the trajectory inside the mix-zone is hidden in the "black box".

Though there are studies focusing on location privacy under VANETs [5], [22], few efforts have been paid to the privacy issues of the vehicular platoon. The problem of location privacy is severe in platoon scenario because the movement of vehicles inside a platoon is more ordered. Designing a scheme to reveal the trajectory of each vehicle in a platoon scenario is challenging. Firstly, vehicles inside a platoon will have different behaviors alongside the road compared to ordinary vehicles. The mixture of platoons and free vehicles introduces complexity to the traffic model. Secondly, an adversary can hardly obtain specific traffic parameters, and the upper bound of attack is difficult to approach. Thirdly, when revealing the mapping between pseudonyms before and after the mix-zone, not all the overall mapping is valid. It has to be noticed that vehicles tend not to shuffle their relative position inside a platoon. In summary, our work makes the following contributions:

(1) We demonstrate an attack framework to infer the pseudonym mapping, and show how our framework takes advantage of this information. We proposed an iterative algorithm for the adversary to update traffic parameters while inferring pseudonym mapping.

978-1-5386-4586-4/18/$31.00 ©2018 IEEE

(2) We analyze from the perspective of adversaries holding different levels of traffic information. Besides attackers carrying zero knowledge and complete knowledge, we also study the attacker with incomplete traffic information and prove that our scheme can be applied to the scenario without platoons.

(3) We develop a simulation platform that considers a general scenario with both platoons and free vehicles to support our scheme and demonstrate the effectiveness of our attack through extensive simulations based on the real data from U.S. Highway 101.

(4) We provide solutions to enhance the location privacy in platoon scenarios according to the simulation results. Our countermeasures focus on increasing the achievable location privacy by adding randomness to the vehicle movements.

II. RELATED WORK

Platoon structures that leverage VANET has been studied for an increased traffic throughput. CACC extends the Adaptive Cruise Control (ACC) system by introducing V2V communications. CACC deployments have been successfully demonstrated, for example, [18], [19]. With a general design proposed in [18] by Naus *et al.*, a CACC system is proved feasible. Milanés *et al.* further implement and validate the system by experiment in real traffic situation in [19]. In [17], Amoozadeh *et al.* apply CACC system to platoon by specifying a longitudinal control logic based on beacons. In [13], Sinan *et al.* investigated the impact of imperfect wireless communication on the platoon stability in a CACC system, including some factors such as the sampling frequency, zero-order-hold and constant network delays.

Several previous works on mix-zones have been done to protect location privacy. Beresford *et al.* [4] first address the concept of mix-zones, in which all the vehicles stop transmitting any information. Communication is resumed when a vehicle exits the mix-zone and change its pseudonym. This mechanism cuts off the linkage between vehicles and their pseudonyms, and the location privacy is thus protected. Freudiger *et al.* [11] propose cryptographic mix zones (CMIX) as a practical implementation of the mixzone notion. The CMIX protocol uses traditional asymmetric cryptography to distribute symmetric keys to establish the cryptographic mix zone within the broadcast distance of an RSU. Gao *et al.* [6] take the factor of time spent inside the mix-zone into consideration and constructed the mix-zone using graph theory to analyze the performance of the mix-zone. Buttyn *et al.* [14] analyze the effectiveness of mix-zones and conclude that the optimal frequency of pseudonym change depends on the characteristics of the mix-zone (size, location, number of entry points), which are difficult to determine in practice.

For VANETs, Choi *et al.* [15] first showed the feasibility of symmetric authentication in vehicular networks with balanced privacy and accountability. Lu *et al.* [7] proposed a useful pseudonym changing at social spots strategy for a guaranteed location privacy. Social spots are places with vehicles gathering, e.g., a parking lot, or a road intersection when the traffic light turns red. It is proved that if all vehicles change pseudonyms when they leave, the social spot will become a mix-zone to break the linkage between pseudonyms. Moreover, X. Liu *et al.* [8], Jadliwala *et al.* [9] and Sun *et al.* [10] proposed to deploy mix-zones in a region by formulating graph optimization problems. These schemes enhance the mixing effectiveness as well as location privacy with lowered cost.

On the privacy metrics, Shokri *et al.* [22] proposed to use the distance estimation error to quantify location privacy, which can evaluate the concrete privacy level under specific attacks. It is shown to be more accurate than entropy in some cases. We also adopt this metric in our simulations. Freudiger *et al.* [23] proposed a system-level anonymity metric for anonymous communication systems, which considers multiple messages sent by each sender. However, it is not directly applicable to mix-zones.

On the attacking model, a probability distribution attack [22] is based on gathered traffic statistics and environmental context information. Here, the attacker tries to derive a probability distribution function of the user position over the obfuscation area. Ghinita *et al.* [24] proposed a special kind of the personal context linking attack, where the attacker has user knowledge gathered through observationand retrace all prior locations of the user for the same pseudonym by a single correlation. As it is shown in [26], the attack on a trusted third party (TTP) is realistic and not negligible. Therefore, it is at least questionable to assume the trustworthiness of a TTP. However, this attack is not considered in approaches that rely on a TTP, as it would undermine every approach using a TTP. Particle filter [25] techniques provide a well-established methodology for generating samples from the required distribution without requiring assumptions about the state-space model or the state distributions. It uses a genetic mutation-selection sampling approach, with a set of particles to represent the posterior distribution of some stochastic process given noisy or partial observations.

III. PROBLEM DEFINITION

In this section, the network and threat models are defined. Our model considers all possible situations and determine a mapping with the likelihood maximized.

A. Network Model

1) Communication Model : A VANET with free vehicles and platoons based on vehicles are considered in this part and the traffic scenarios are defined as follows.

- *Vehicles.* Each vehicle is equipped with a GPS device, to provide precise location information, and an On-Board Unit (OBU) device, which allows communication with other vehicles and Road Side Units (RSUs). The process is done by vehicle-to-vehicle (V2V) communications, which is shown in Figure 1(a) between two vehicles. According to the reference [17], a typical beacon includes pseudonyms, position, acceleration, maximum deceleration, lane ID, row ID, and row depth. All vehicles, or at least vehicles in communication, must have different pseudonyms, and all other information must be real as they are used in the CACC.
- *Platoons.* A platoon consists of a leader and several followers. The leader needs to create and manage the platoon. It is assumed that all vehicles on the road are qualified to join a platoon as long as they share the same trajectory. There are three kinds of maneuvers considered including vehicle leaving a platoon, platoon splitting, and vehicle or platoon merging into another platoon. In our paper, only maneuvers taken place in a mix-zone will be considered.
- *Traffic scenarios.* The following scenarios are considered. Figure 1(a) shows our traffic scenario on a

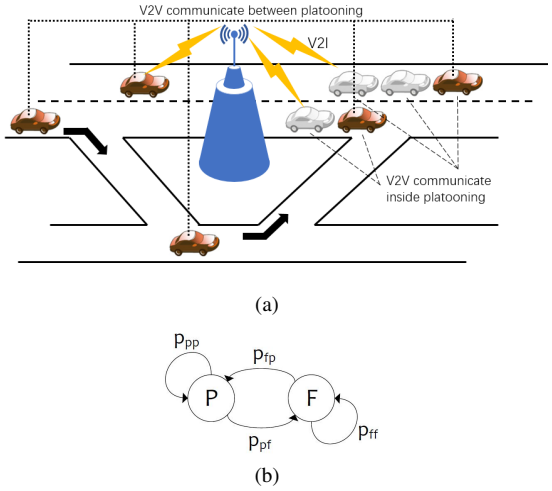


Fig. 1. (a) Network Model. (b) Markov chain to describe vehicle status.

highway, with a side road and the main road. Vehicles from the side road may enter the highway, and those from the main road may exit.

Furthermore, we assume a two-state Markov chain to describe the behavior of vehicles. As shown in Figure 1(b), a vehicle can either be in a platoon or be a free agent when traveling from one intersection to another. The transition matrix can be presented as:

$$P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} \quad (1)$$

Where the label of each probability stands for the transition of the first state to the second, 0 for a platoon state, and 1 for a free state.

2) Mix-zone Model: A mix-zone is an area where an adversary cannot obtain any sensitive information about users by eavesdropping the broadcast information. The pseudonyms of vehicles are changed when they exit the mix-zone. Hence the timing information is the delay characteristic of each direction, and the location information is the trajectory inside the mix-zone and the platoon structure when leaving the mix-zone. It is assumed that vehicles within a platoon must maintain their relative position if they remain together in a platoon after exiting the mix-zone. Also, in our model, the vehicles do not communicate with each other in the mix-zones.

B. Threat Model

Through beacons from the OBU, an eavesdropper can monitor the location information and learn the trajectory of any vehicle. In our threat model, an adversary is considered to be external, passive, and global, that means is considered by the network members as an intruder and hence is limited in the diversity of attacks. Nevertheless, we assume he/she can eavesdrop the communication.

An external adversary deploys signal receivers alongside the road. Considering the cost, only the signal receiver is allowed in this attack model. The receivers passively eavesdrop on beacons from passing vehicles and try to acquire information. The receivers are limited in range, so the strength of an adversary is determined by the area its receiver device can cover. Global means the adversary is fully aware of all safety messages from the monitored vehicle network.

TABLE I. NOTATIONS

Notation	Description
P	pseudonym entering
s	vehicle state entering
a	entering direction
t	entering time
pid	entering platoon ID
$u = (P, s, a, t, pid)$	an entering event
P'	pseudonym leaving
s'	vehicle state leaving
b	leaving direction
t'	leaving time
pid'	leaving platoon ID
$v = (P', s', b, t', pid')$	an leaving event

Information including time, location, speed, and acceleration are used to track vehicles.

IV. PSEUDONYM INFERENCE IN PLATOON SCENARIOS

In this section, we propose a method with which the adversary can threaten the location privacy in platoon scenarios in the previously mentioned communication model. Further, we show that our proposed method can also be applied to ordinary VANET.

Notations are listed in TABLE I. Any vehicle passing through the mix-zone enters with a pseudonym provided by the Certificate Authority (CA) and leaves with another one. Let u represent an entering event of a vehicle with pseudonym P, state s, platoon ID pid at time t on direction a, denoted by $u = (P, s, t, a, pid)$. Similarly, v refers to an leaving event with pseudonym P', state s', platoon ID pid' at time t' on direction b, which is given by $v = (P', s', t', b, pid')$. The state of a vehicle, s or s', is 0 for a platoon state, and 1 for a single free vehicle.

In a time interval T, the number of ingress and egress vehicles is denoted by k to meet the need of *k-anonymity*. Assume that the number of vehicles entering the mix-zone in a time interval T follows a Poisson distribution with parameter λ, i.e., $N \sim \mathcal{P}(\lambda)$. The time instances of vehicles' arrival is uniformly distributed, $\tau_i \sim \mathcal{U}(T)$. To reveal the pseudonym mapping of a mix-zone, the adversary will perform three steps as follows.

A. Traffic Graph Construction

With the notations in Table I, the mix-zone can be modeled as a weighted directed bipartite graph $G = \{U, E, V\}$. The set of vertexes U and V represents the entering and leaving events respectively. During a time interval T, vehicles pass through the mix-zone, generating k ingress and egress events, which can be denoted as $U = \{u_1, u_2, ..., u_k\}$ and $V = \{v_1, v_2, ..., v_k\}$ respectively. The set of edges E denotes the mapping between the entering and leaving events in the mix-zones. Specifically, the graph is a complete bipartite graph as shown in Figure 2.

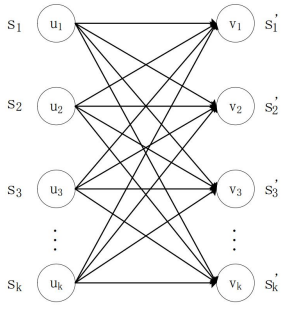


Fig. 2. Platoon mix-zone graph model.

It serves as a structural representation of the mix-zone, and the basis of revealing the pseudonym mapping.

Indexes of entering and exiting vertexes are sorted according to platoon ID and time. Entering vertexes within the same platoon will have a consecutive ascending sequence of indexes, assigned in an ascending order of entering time. The single free vehicle will be regarded as a platoon of length 1. This sorting process can be guarantee $u_i > u_j$, for all $(i,j) \in \{(i,j)|t_i > t_j\}$. Similarly, we have $v_i > v_j$, for all $(i,j) \in \{(i,j)|t'_i > t'_j\}$.

Vertexes in the graph are constructed by pseudonyms of each entering and leaving events. Because adversary tracks pseudonyms of each, each vehicle should change its pseudonym to cut off the linkage between its entering event and leaving events. A one-to-one mapping algorithm is called to calculate the one-to-one mapping probability, which is also the weight on each edge in the traffic graph. The process of the platoon mix-zone graph goes as Algorithm 1.

Algorithm 1 GraphConstruct

Require: Mix-Zone M, entering and leaving pseudonym set P, P'
Ensure: A series of platoon mix-zone graph G
k vehicles in the mix-zone as vertexes;
Sort P and P' according to platoon ID and time.
for $i = 1$ to k **do**
  $u_i \leftarrow (P_i, s_i, a_i, t_i, pid_i)$;
  $v_i \leftarrow (P'_i, s'_i, b_i, t'_i, pid'_i)$;
end for
for $i = 1$ to k **do**
  for $j = 1$ to k **do**
    $e_{ij} \leftarrow \langle u_i, v_j \rangle$;
  end for
end for
$W \leftarrow OneToOneMapping$;
Return $G = \langle U, V, E, W \rangle$;

Algorithm 2 OneToOneMapping

Require: Platooning status S, S', entering and leaving time t, t' and direction a, b
Ensure: Edge Weight W
for $i = 1$ to k **do**
  $sum \leftarrow 0$;
  for $j = 1$ to k **do**
    $P(v_j|u_i) \leftarrow p_t(s_i, s'_j) p_{a_i,b_j} f_{a_i,b_j}(t'_j - t_i)$;
    $sum+ = P(i,j)$;
  end for
end for
for $i = 1$ to k **do**
  for $j = 1$ to k **do**
    $p_{i,j} \leftarrow P(v_j|u_i)/sum$;
  end for
end for
Return $W = \{p_{i,j}|p_{i,j}$ for $e(u_i, v_j), i, j = 1, 2, ..., k\}$;

B. One-to-one Mapping Probability Calculation

A vehicle pass through the mix-zone with an entering event $u = (P, s, a, t, pid)$ and an leaving event $v = (P', s', b, t', pid')$. $p_{a,b}$ is the probability of a vehicle entering at direction a and leaving at b, which is also known as the direction transition probability. Specifically, $a, b \in 1, 2$ stands for the two entering and exiting directions respectively. The combination of a and b indicates the trajectory a vehicle takes in the mix-zone, and the direct transition probability is determined by this trajectory. The probability is denoted by:

$$p_{a,b} = P(Dir_{leave} = b | Dir_{enter} = a) \tag{2}$$

This probability is also related to the platoon states before and after passing through the mix-zone such that $\sum_{Dir_{leave}} p_{a,b} = 1$ for any entering direction a.

The traffic delay depends on the trajectory inside the mix-zone. $f_{a,b}(\tau)$ stands for the probability that a vehicle spend time $\tau = t' - t$ travelling from a to b. The distribution of traffic delay is an arbitrary distribution with parameters determined by the trajectory and platoon status (a_i, b_j). The probability is given by the PDF of time interval distribution:

$$f_{a,b}(t' - t) = P(\Gamma = \tau | Dir_{leave} = b | Dir_{enter} = a) \tag{3}$$

Generally, the probability follows Gaussian distribution with parameter $\mu_{a,b}$ and $\sigma_{a,b}$. The time spend in the mix-zone can be modelled as $\tau \sim \mathcal{N}(\mu_{a,b}, \sigma^2_{a,b})$:

$$f_{a,b}(\tau) = \frac{1}{\sqrt{2\pi}\sigma_{a,b}} exp(-\frac{(\tau - \mu_{a,b})^2}{2\sigma^2_{a,b}}) \tag{4}$$

Further, a vehicle may choose to join a platoon or travel as a free agent. This process can be described by a Markov chain. Recall our definition for vehicle state s, s' and state transition matrix P. Let $p_t(s, s')$ represent the state transition probability, which is given by the state of entering and exiting vehicles, and the state transition matrix P. In (5), s and s' become indexes of element in matrix P shows in equation (1).

$$p_t(s, s') = P(S_{leave} = s' | S_{enter} = s) \tag{5}$$

Let $P(v|u)$ represent the probability of a vehicle exits with event v given it enters the mix-zone event u. The probability $P(v|u)$ does not depend on the observations and can be used to calculate any event pairs (u, v). Numerically, $P(v|u)$ equals to the product of the lane transition probability, the state transition probability, and the traffic delay characteristic, which takes the form in equation (6). Here the state transition and the direction transition is independent, while the direction transition and delay do not need to be since we have a conditional probability in Eq (3)

$$P(v|u) = p_t(s, s') p_{a,b} f_{a,b}(t' - t) \tag{6}$$

The adversary calculates $P(v_j|u_i)$ for all the observed entering and leaving pairs (u_i, v_j) in the traffic graph. The summation and integration of $P(v|u)$ over all possible s, s', a, b and τ is equal to 1. Normalization is needed to get the linkability between two given observations. From all the leaving events, a vehicle must take only one of them. Let U and V denote all our observed events. The normalized probability that a vehicle with ingress event u_i leaves with event v_j can be given by equation (7):

$$p_{ij} = \frac{P(v_j|u_i)}{\sum_{j=1}^{k} P(v_j|u_i)} \tag{7}$$

Algorithm 2 gives a detailed process of computing edge weights. The weight matrix, together with the two-state matrices, can be used to represent the platoon graph model. The

weight matrix takes a form of the adjacency matrix, which can be represented as follows:

$$\text{Weight } W = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1k} \\ p_{21} & p_{22} & \cdots & p_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ p_{k1} & p_{k2} & \cdots & p_{kk} \end{pmatrix} \tag{8}$$

Graph G can be described by the $k \times k$ edge weight matrix W. Elements in G represent the mapping possibilities between entering and exiting events given by equation (7). The possibilities meets conditions (9) and (10):

$$s.t. \quad \sum_{j=1}^{k} p_{ij} = 1, \quad \forall i \in [1,k] \tag{9}$$

$$0 \leq p_{ij} \leq 1, \quad \forall i \in [1,k] \tag{10}$$

Each vehicle enters the mix-zone with a pseudonym and exits with another different one. The privacy level and uncertainty for adversary depends on the weight on each edge. The construction process is described in Algorithm 2.

C. Overall Mapping Inference

With the edge weight matrix W, the adversary then gives a possible mapping between the ingress and the egress pseudonyms. Consider a mapping $M = m_1, m_2, ..., m_k$, where $m_i = 1, 2, ..., k$ is the mapping for ingress pseudonym i, and its value stands for the corresponding egress pseudonym. Then all the adversary have to do is to determine a mapping with the likelihood $L(M)$ maximized. For certain mapping M, this probability can be given by:

$$L(M) = \frac{\prod_{i=1}^{k} p_{i,m_i}}{\sum_{\hat{M}} \prod_{i=1}^{k} p_{i,m_i}} \tag{11}$$

Where p_{i,m_i} is the probability to link incoming pseudonym i together with outgoing pseudonym m_i. Taking the production of all the probabilities over i, we can get the probability of this mapping M. But this probability is not normalized, and we have to derive this by the summation over all the possible mappings $\hat{M}$. The result $L(M)$ is the normalized probability of given mapping M.

Notice that the summation is not over all the M since there are some overall mappings that violate our assumption of the mix-zone and platoon. As discussed in III-A2, we assume that each vehicle will perform at most one of the four maneuvers in the mix-zone. The relative position between two vehicles is kept unchanged if they stay in the same platoon before entering, and in another one after leaving. Let set C denote all the pair (i,j) such that i and j, m_i and m_j are in the same platoon, and i enters earlier than j. We have:

$$C(M) = \{(i,j) | t_i < t'_j \& pid_i = pid_j \& pid'_{m_i} = pid'_{m_j}\} \tag{12}$$

$$\hat{M} = \{(\hat{m}_1, ..., \hat{m}_k) | \hat{m}_i \neq \hat{m}_j \& (i,j) \in C(\hat{M}) \Rightarrow \hat{m}_i < \hat{m}_j\} \tag{13}$$

Where $\hat{M}$ includes all the valid mappings. The goal of the adversary is to find a mapping to maximize $L(M)$ among all the $\hat{M}$. Notice that all the probability have the term $1/\sum_M \prod_{i=1}^{k} p_{i,m_i}$ in common, so the objective can be further simplified into maximize $\prod_{i=1}^{k} p_{i,m_i}$. Furthermore, we can take log on our objective function, to turn production into summation: $\sum_{i=1}^{k} \log p_{i,m_i}$.

This objective function comes with constraint that the value of all the element in the mapping, $m_1, m_2, ..., m_k$, should be assigned exclusively, which means that $m_i \neq m_j$ for all i, j. we can write the objective:

$$M^* = arg \max_{M \in \hat{M}} \sum_{i=1}^{k} \log p_{i,m_i} \tag{14}$$

Notice that the most likely overall mapping is not only related to the mapping probability p_{i,m_i}, it is also constrained by possible global mapping $\hat{M}$. The set $\hat{M}$ filters out all the global mappings that go against out assumption of vehicles' behavior inside the mix-zone in III-A2. Intuitively, a smaller set indicates that the adversary is more likely to find the best overall mapping.

D. Traffic Parameter Re-estimate

From the perspective of an adversary, pseudonyms and their status are regarded as observations, and overall mapping results are considered hidden variables. The adversary takes advantage of the overall mapping and re-estimate the traffic parameters. The adversary computes the traffic parameters under current overall mapping results and then updates the parameters to maximizes the likelihood given fixed hidden variables. The updated parameters can be further used to again estimate the overall mapping.

These parameters are replaced by the statistical expectations. Specifically, parameters including turning probability, mean and variance of passing time are updated. Denote $\delta(i, m_i, a, b)$ as an binary identifier indicating if pseudonym i is on direction a and m_i is on b:

$$\delta(i, m_i, a, b) = \begin{cases} 1 & a_i = a \text{ and } b_{m_i} = b \\ 0 & \text{other} \end{cases} \tag{15}$$

Let the label t denote the number of iteration and $\tau(i, m_i)$ denote time the vehicle arrival. The update rule of the parameters can be given by (16), and (17) respectively.

$$p_{a,b}^{(t)} = \frac{1}{k} \sum_{i=1}^{k} \delta(i, m_i, a, b) \tag{16}$$

$$\mu_{a,b}^{(t)} = \frac{\sum_{i=1}^{k} \delta(i, m_i, a, b) \tau(i, m_i)}{\sum_{i=1}^{k} \delta(i, m_i, a, b)} \tag{17}$$

E. Iterative Mapping Inference

After updating the parameters, the adversary again re-estimates the overall mapping following the strategies introduced in IV-B and IV-C. The process works like an EM algorithm towards maximizing the likelihood of overall mapping, with the overall mapping computed in the E-step, and the traffic parameters updated in the M-step. As the iteration goes on, the estimation of the traffic parameters and the overall mapping will both get converged.

Algorithm 3 IterativeInference

Require: Initial estimation of parameters $p_{a,b}$, $\mu_{a,b}$, $\sigma_{a,b}$
Ensure: Overall mapping and estimated parameters.
$G \leftarrow$ GraphConstruct;
Calculate all the valid overall mappings $\hat{M}$;
repeat
  E-step, estimate best overall mapping
  One to one mapping probability W;
  Max log-likelihood $l^* \leftarrow 0$
  Best overall mapping $M^{*(t)}$
  for M in $\hat{M}$ **do**
    if $l^* < \sum_{i=1}^{k} \log p_{i,m_i}$ **then**
      $M^{*(t)} \leftarrow M$
    end if
  end for
  M-step, update parameters
  $p_{a,b}^{(t)} \leftarrow \frac{1}{k}\sum_{i=1}^{k} \delta(i, m_i, a, b)$;
  $\mu_{a,b}^{(t)} \leftarrow \frac{\sum_{i=1}^{k} \delta(i,m_i,a,b)\tau(i,m_i)}{\sum_{i=1}^{k} \delta(m_i,a,b)}$;
  $W^{(t)} \leftarrow OneToOneMapping$;
  if Maximum iteration reached **then**
    return M^*, $p_{a,b}$, $\mu_{a,b}$
  end if
until Overall mapping and parameters converged **return** M^*, $p_{a,b}$, $\mu_{a,b}$

V. PRIVACY ANALYSIS

In this section, we will analyze the reachable location privacy of adversary. Three kinds of attackers and a special case are considered, which are classified according to the traffic knowledge they hold. Entropy and success probability to evaluate our system. The proposed oblivious adversary just provides a lower bound of an attacker, which is only related to the number of cars in the mix-zone, while the strong adversary makes decisions based on perfect parameters and be regarded as an upper bound of the adversary.

A. Oblivious Adversary

An oblivious adversary knows vehicles were moving in and out the mix-zone. Other information including time, trajectories and platoons are limited.

The direction transition probability $p_{a,b}$ takes a uniform distribution $p_{a,b} = 1/d$. The time consumption of vehicle is given uniformly by $f_{a,b}(\tau) = 1/T$. The platoon transition each vehicle takes will be regarded as random, where $p_t(s, s') = 1/2$ for all ingress and egress states s and s'.

The entropy of a mix-zone indicates the uncertainty of the adversary towards several individuals, which can formulate as the sum of all vehicles in the mix-zone during a given time interval (18).

$$H_M = -\sum_{i=1}^{k}\sum_{j=1}^{k} p_{i,j}\log_2(p_{i,j}) \tag{18}$$

To further quantify the level of privacy in a mix-zone, we use the average entropy. This factor is useful comparing privacy level with different car numbers. The entropy is determined by the number of vehicles in the mix-zone.

$$\bar{H} = \frac{H_M}{k} = -\frac{1}{k}\sum_{i=1}^{k}\sum_{j=1}^{k} p_{i,j}\log_2(p_{i,j}) \tag{19}$$

Since all the three components are identical among all pseudonym pairs. $p_{i,j} = 1/(2Td)$ is given by the product of these components, which is also a constant. According to Algorithm 2, weights of the egdes $w_{i,j}$ in the bipartite graph shown in Figure 2 is $w_{i,j} = 1/k$. Consequently, the mapping probability takes a uniform distribution, and the location privacy is:

$$H(M_i) \leq k\log_2 k \tag{20}$$

As shown in (20), the oblivious adversary provides a lower bound of an attacker, which is only related to the number of cars in the mix-zone.

To carry out the overall mapping probability, the oblivious adversary first enumerates all the possible mapping $\hat{M}$. For each valid mapping $\hat{M}$, the overall mapping likelihood is given by

$$L(\hat{M}) = \frac{\prod_{i=1}^{k} p_{i,\hat{m}_i}}{\sum_{\hat{M}}\prod_{i=1}^{k} p_{i,\hat{m}_i}} \tag{21}$$

Since $p_{i,j}$ is given by a constant $1/(2Td)$, the likelihood $L(\hat{M}) = 1/|\hat{M}|$ is also constant which is inversely proportioned to the number of valid overall mapping.

According to this result, the privacy is also related to the complexity of the traffic scenario. Intuitively, if all the vehicles are free before and after the mix-zone, the size of set $\hat{M}$ reaches its maximum $|\hat{M}|_{max} = k!$. While in another case, if only one platoon is observed entering and leaving the mix-zone, there can be only one overall mapping, which means that the platoon remains unchanged inside the mix-zone.

From these two cases we can see that even for the oblivious adversary without adequate information, the privacy of a mix-zone will be significantly jeopardized if the number of vehicles and platoons in the mix-zone is small.

B. Strong Adversary

A strong adversary is fully aware of the temporal and spatial information. The sequentiality of events and platoon information will be taken into consideration to assigning a mapping probability.

Also, the strong adversary holds a prior knowledge about all the traffic parameters. The direction transition probability $p_{a,b}$ is perfectly learnt by long-term observation. The time spent on the entering direction to the left follows the Gaussian distribution. The strong adversary can take advantage of this term by capturing the statistic of entering and leaving time for each vehicle. The platoon statistics can also be perfectly learned by the adversary. This includes all the parameters in the Markov chain in (1).

According to all the information, a strong adversary can get, the normalized mapping probabilities are shown as a weight matrix in Section IV-B can be derived by (7). Specifically, the mapping probability is given by:

$$p_{ij} = \frac{p_t(s_i, s'_j)p_{a_i,b_j}f_{a_i,b_j}(t'_j - t_i)}{\sum_{j=1}^{k}(p_t(s_i, s'_j)p_{a_i,b_j}f_{a_i,b_j}(t'_j - t_i))} \tag{22}$$

For the overall mapping, the strong adversary chose the most likely one, $M^* = arg \max_{M \in \hat{M}} \sum_{i=1}^{k} \log p_{i,m_i}$ as the final overall pseudonym mapping. Denote the actual mapping as $M = m_1, ...m_k$, the mapping accuracy can be given by $\frac{1}{k}\sum_{i=1}^{k} \delta(m_i = m_i^*)$. Where $\delta(X)$ is a function that outputs 1 if statement X is true and 0 if X is false. The strong adversary makes decisions based on perfect parameters and can thus be regarded as an upper bound of the adversary.

C. Weak Adversary

The weak adversary holds partial traffic information about the mix-zone. The adversary knows roughly the platoon transition probability and the turning probability. Also, the attacker uses Gaussian distribution to model the time spent going through the mix-zone.

The initialization of these parameters is based on simple observations. The attacker obtains a weight matrix with the form (8), by calculating the one-to-one mapping probability given by:

$$p_{ij} = \frac{p_t(s_i, s_j')p_{a_i,b_j} f_{a_i,b_j}(\tau(i,j))}{\sum_{j=1}^{k}(p_t(s_i, s_j')p_{a_i,b_j} f_{a_i,b_j}(\tau(i,j)))} \tag{23}$$

The attacker goes on to calculate the overall mapping. Since the traffic parameters the weak attacker uses is not perfect, the resulting overall mapping is also flawed. But the weak adversary re-estimates the traffic parameters, approaching the true values a bit. Iteratively, the weak adversary adjusts its parameters and the overall mapping. The accuracy of each step rises as the iteration goes on, and stops as the process get converged.

A weak adversary is the most realistic one with reasonable initial parameters. With the corrected traffic information, the weak adversary should have a lower but close performance compared with the strong adversary.

D. Scenario without platoon

An ordinary VANET without platoon is a special case for our scheme. This scenario can be treated as all vehicles passing through the mix-zone with platoon status fixed as free agents.

Hence the mapping probability for no platoon scenario can be calculate according to Equation 23, by just let status transition probability $p_t(s_i, s_j') = p_{11} = 1$.

Though VANET scenario do not include vehicle platooning, we can still treat each vehicle as a platoon of length 1. Since any two vehicles are in different "platoons", $C(M) = \emptyset$. In Equation 13, the predicate expression $\forall i \neq j, (i,j) \in C(\hat{M}) \Rightarrow \hat{m}_i < \hat{m}_j$ is always true. With this observation, the set of possible mappings can be further written as

$$\hat{M} = \{(\hat{m}_1, ..., \hat{m}_k) | \forall i \neq j, \hat{m}_i \neq \hat{m}_j\} \tag{24}$$

This set includes all the possible combination of ingress and egress pseudonyms, whose size is given by $|\hat{M}| = k!$.

VI. SIMULATION

In this section, we will simulate the highway scenario to evaluate the achievable location privacy of our scheme, and our experiments take place on both synthetic data and real data from U.S. Highway 101.

TABLE II. SIMULATION PARAMETERS

Parameter	Values
Mix-zone radius	500m
Maximum speed allowed	20m/s
Minimum inter-platoon gap	20m
Maximum intra-platoon gap	5m
Arrival rate λ: for sparse traffic	$1s^{-1}$
Arrival rate λ: for dense traffic	$1.5s^{-1}$

A. Simulation on Synthetic Data

The simulation platform is based on a discrete-time simulator coded in C++ which implementing a centralized control logic to simulate the behavior of vehicles. In our simulation, the trajectories of each vehicle are generated by a stochastic process, and the simulation parameters are listed in TABLE II.

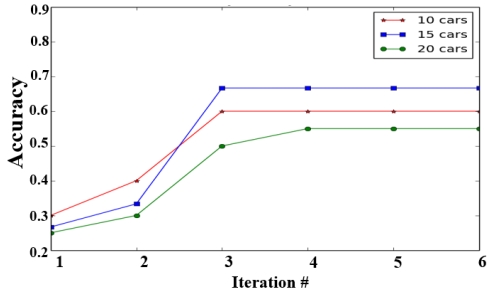
The effectiveness of the attacker is evaluated regarding the average entropy of the whole intersection. The success rate for adversaries is also considered to reflect the effect of our system against attack intuitively. As our simulation takes place in the highway scenario, the mix-zone radius setting as 500 meters is reasonable. Individually, for specific arrival rate λ, we consider the number of vehicles to be $\lceil 2\lambda T \rceil$ to meet the need of *k-anonymity*. With the arrival rate set to be $\lambda = 1s^{-1}$ for low traffic congestion and $\lambda = 1.5s^{-1}$ for high congestion at an intersection, the arrival time of each vehicle is uniformly distributed.

1) Entropy Analysis: We launch our simulation under two different scenarios. Firstly, keep the density of vehicles fixed, adjust the time interval and observe the impact of vehicle numbers on the average entropy. We run the simulation and launch attacks for 15 times, and the result is illustrated in Figure 3(a). From the figures, our proposed scheme significantly outperforms the oblivious adversary, and get results very close to the strong adversary. The growth in average entropy reflects raised uncertainty for the adversary, which is caused by increased number of vehicles in the mix-zone.

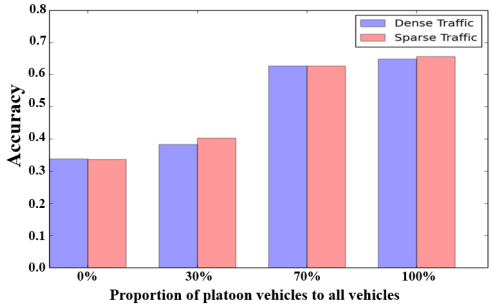
The second series of simulation is for different proportion of platoon vehicles to total vehicles. Keep the number of vehicles fixed and change the proportion of platoon vehicles to all platoons. Figure 3(b) shows the average entropy by our proposed weak adversary in tracking the vehicles in a mix-zone. As demonstrated, with the increasing of the number of platoon vehicle, the average entropy decreases, meaning that the adversary has a higher level of confidence. We also launched the attack against different traffic density. The average entropy is close for dense and sparse traffic, indicating that the sparsity of the traffic flow does not mitigate the power of our proposed attacker.

2) Accuracy Analysis: The adversary uses an iterative process to calculate the best overall mapping as well as re-estimating the traffic parameters. In each iteration, the adversary gives an overall mapping with maximum likelihood under current parameters. In Figure 4(a), the accuracy of the overall mapping after each iteration is illustrated. The accuracy rises as the iteration goes, after 4 to 5 iterations, the process converges, giving a final result much better than that of the first iteration. The iterative inference process allows the adversary to hold inaccurate estimation of the traffic parameters, and still guarantees a high accuracy in the overall mapping.

Success probabilities under different platoon proportions are also simulated with the result given by Figure 4(b). A lower success rate is observed without platoon compared with scenarios including platoons under same simulation parameters. The conclusion accords with Figure 3(b) come up that



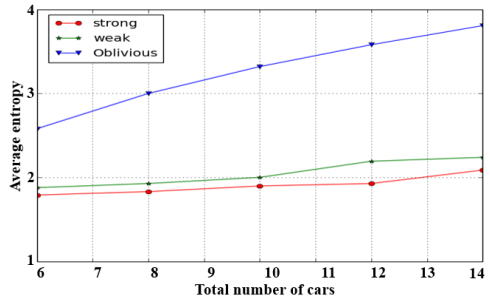
(a)



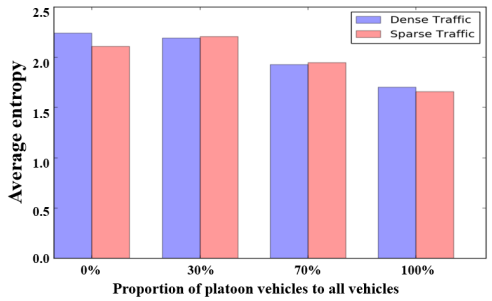
(b)

Fig. 4. Accuracy for adversaries. (a) Accuracy to car numbers for all kinds of attackers. (b) Accuracy to platoon proportion for our proposed weak adversary.

we can get more than 30% accuracy in scenarios of all in platoons than in all free scenarios.



(a)



(b)

Fig. 3. Average entropy of the mix-zone. (a) Accuracy to car numbers by all kinds of attackers. (b) Average entropy to platoon proportion by our proposed weak adversary.

B. Simulation on Real Data

Some of our experiments are based on real data of vehicle traffic data collecting from U.S. Highway 101. This dataset

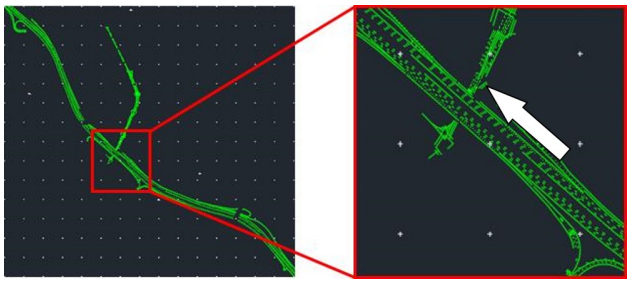


Fig. 5. Scenes of U.S. Highway 101

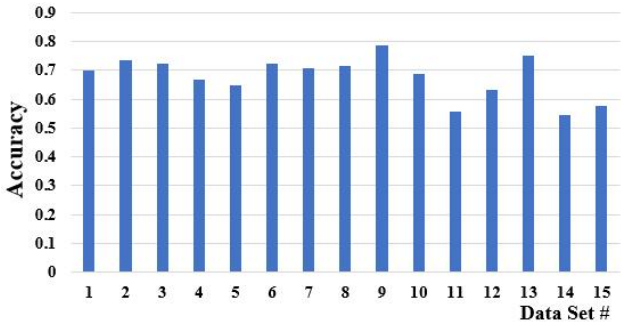


Fig. 6. Mapping Accuracy

contains data transcribed by Cambridge Systematics, Inc. as part of the Federal Highway Administration's (FHWA) Next Generation Simulation (NGSIM) project. The traffic data was collected on a freeway segment of US 101 (Hollywood Freeway) located in Los Angeles, California on June 15th, 2005. One segment of 15min from the dataset is selected in our experiments as it has three in all though. This dataset contains detailed trajectory data, wide-area detector data, and supporting data needed for behavioral algorithm research. The traditional highway scene, which is shown in Figure 5, and we artificially set some of the areas on the road as the mix-zone, which is the part in the red rectangle and is enlarged and shown in the right part of Figure 5. Vehicles do not communicate with each other in the mix-zone in our model so in the data preprocessing we remove the part of the traffic information that generates in the mixed area. To carry out our experiment, the information for vehicle identification, such as vehicle ID, is omitted and the remaining vehicle traffic data is applied to the algorithm we proposed.

1) Mapping probability analysis: 15 different segments of data are extracted from the obtained data set at equal intervals, and all the segments are of the same duration. The information of vehicles entering and leaving the mix-zone are matched by applying our algorithm, getting an overall mapping and then compare it with the actual results of the traffic data. The results are shown in Figure 6, which indicates that the algorithm we proposed can get a relatively high probability of correct mapping in the real scene. The probability of success is relatively stable, most of which are between 0.7, and the best can be up to nearly 0.8, which also proves the reliability of our proposed algorithm.

2) Position error analysis: It is more practical to carry out this analysis on real data than on synthetic data. Based on the overall mapping of the vehicles entering and leaving the mix-zone, an analysis of the position error of the vehicles caused by the vehicle mapping result is introduced . In Figure 7, the summation of the Euclidean distances of the vehicles position errors of each traffic data caused by the mapping results is obtained by our proposed algorithm. From the

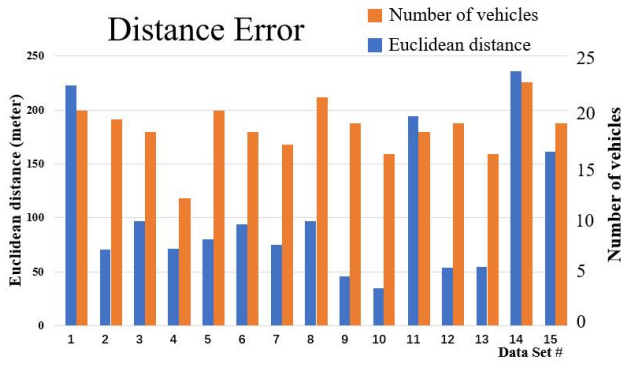


Fig. 7. Distance Error

results in the graph, it is concluded that the vehicle position error is proportional to the number of vehicles that have not been successfully mapping. It is evident that some of the unexpected situation in actual traffic lead to the sudden change of position error, which indicated in segments such as 1, 11, 14, 15. Although some of the sudden situation happens in the actual vehicle driving process may cause a specific range of fluctuations within the field, the position error, averaged to each vehicle, is still in a favorable range which also proves the reliability of our proposed algorithm.

VII. CONCLUSION

In this paper, we proposed the attack scheme of an attacker against mix-zone with the platoon and an iterative process to learn traffic information while inferring the pseudonym mapping. We proved the compatibility of our scheme with no platoon scenario and designed and implemented a simulation platform supporting platoon control logic. We also demonstrated the effectiveness of our proposed attack scheme by comparing the result with a strong adversary and show how the proportion of platoon vehicles affect the total location privacy of the mix-zone.

In the future, we will compare our framework with previously proposed algorithms for pseudonym inference in ordinary VANET without platooning, study the impact of the length of the platoons on the success probability of the pseudonym mapping, as well as extend our attack scheme to handle platoon-level pseudonyms.

VIII. ACKNOWLEDGMENTS

This work is supported by Chinese National Research Fund (NSFC) No. 61702330, U.S. NSF grant CNS-1410000, DCT-MoST Joint-project No. (025/2015/AMJ), Startup Funds of University of Macau Nos: CPG2018-00032-FST & SRG2018-00111-FST, Chinese National Research Fund (NSFC) Key Project No. 61532013 and National China 973 Project No.2015CB352401.

REFERENCES

[1] L. Xu, L. Y. Wang, G. Yin and H. Zhang, "Communication Information Structures and Contents for Enhanced Safety of Highway Vehicle Platoons", *IEEE Trans. on vehicular Technology*, 2014, vol. 63, no. 9, pp.4206-4220.

[2] C. Bergenhem, E. Hedin and D. Skarin, "Vehicle-to-vehicle Communication for a Platooning Systems", in *Proc. Transp. Res. Arena*, 2012.

[3] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey", *IEEE communications surveys & tutorials*, 2015, vol.17, no.1, pp. 228-255.

[4] A. R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-aware Services", in *Proc. PerCom Workshops*, 2004, pp.127-131.

[5] J. Freudiger, M. H. Manshaei, J.-P. Hubaux and D. C. Parkes, "On Noncooperative Location Privacy: A Game-theoretic Analysis", in *Proc. ACM CCS*, 2009, pp. 324-337.

[6] S. Gao, J. Ma, W. Shi, G. Zhan, C. Sun, "TrPF: A Trajectory Privacy-preserving Framework for Participatory Sensing", *IEEE Trans. on Information Forensics and Security*, 2013, vol.8, no. 6, pp. 874-887.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", *IEEE Trans. on vehicular Technology*, 2012, vol.61, no. 1, pp. 86-96.

[8] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li and Y. Fang, "Traffic-Aware Multiple Mix Zone Placement for Protecting Location Privacy", *IEEE INFOCOM*, 2012 Proceedings IEEE, 2012, pp. 972-980.

[9] M. Jadliwala, I. Bilogrevic b and J.-P. Hubaux, "Optimizing Mix-zone Coverage in Pervasive Wireless Networks", *Journal of Computer Security*, 2013, vol. 21, no. 3, pp. 317-346.

[10] Y. Sun, B. Zhang, B. Zhao, X. Su and J. Su, "Mix-zones Optimal Deployment for Protecting Location Privacy in VANET", *Peer-to-Peer Networking and Applications*, 2015, pp. 1108-1121.

[11] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks", in *Proc. WIN-ITS*, 2007.

[12] M. Dahl, S. Delaune and G. Steel, "Formal Analysis of Privacy for Vehicular Mix-Zones", in *Proc. of ESORICS'10*, 2010, pp. 55-70.

[13] Oncu, S.; Van de Wouw, N. and Nijmeijer, H., "Cooperative adaptive cruise control: Tradeoffs between control and network specifications", in *International IEEE Conference on Intelligent Transportation Systems*, 2011, pp.2051-2056.

[14] Buttyn, L.; Holczer, T. and Vajda, I., "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, Springer-Verlag*, 2007, pp.129-141

[15] Choi, J. Y.; Jakobsson, M. and Wetzel, S., "Balancing auditability and privacy in vehicular networks", in *Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks*, 2005, pp.79-87

[16] D. Jia, K. Lu and J. Wang, "A Disturbance-Adaptive Design for VANET-Enabled Vehicle Platoon", *IEEE Trans. on vehicular Technology*, 2014, vol. 63, no. 2, pp. 527-539.

[17] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang and D. Ghosal, "Platoon Management with Cooperative Adaptive Cruise Control Enabled by VANET", *IEEE Trans. on Vehicular Technology*, 2015, pp. 110-123.

[18] G. J. L. Naus, R. P. A. Vugts, J. Ploeg, M. J. G. van de Molengraft, and M. Steinbuch, "String-Stable CACC Design and Experimental Validation: A Frequency- Domain Approach", *IEEE Trans. on Vehicular Technology*, 2010, vol.59, no. 9, pp. 4268-4279.

[19] V. Milanés, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative Adaptive Cruise Control in Real Traffic Situations", *IEEE Trans. on Intelligent Transportation Systems*, 2014, vol.15, no. 1, pp. 296-305.

[20] Y. Jiang, S. Li, and D. Shamo, "Development of Vehicle Platoon Distribution Models and Simulation of Platoon Movements on Indiana Rural Corridors", *Joint Transportation Research Program*, 2003.

[21] C. E. Shannon, "A mathematical theory of communication", *ACM SIGMOBILE MCCR*, 2001, vol. 5, no. 1, pp. 3-55.

[22] Shokri, R., Theodorakopoulos, G., Le Boudec, J.Y., & Hubaux, J.P. (2011, May). "Quantifying Location Privacy", in IEEE S & P, pp. 247-262.

[23] J.Freudiger, R.Shokri, and J.P.Hubaux. "On the Optimal Placement of Mix Zones", *Privacy Enhancing Technologies Symposium* (PETS), 2009

[24] Ghinita, G., Damiani, M. L., Silvestri, C., & Bertino, E. "Preventing velocity-based linkage attacks in location-aware applications",in *ACM Sigspatial International Conference on Advances in Geographic Information Systems*, 2009, pp.246-255

[25] Moral, P. D. "Nonlinear filtering: Interacting particle resolution",in *Comptes Rendus de l'Acadmie des Sciences - Series I - Mathematics*, 2009, pp.653-658

[26] Shankar, P., Ganapathy, V. & Iftode, L. "Privately querying location-based services with SybilQuery.", 2009, pp.31-40.

[27] B. Gierlichs, C. Troncoso, C. Diaz, B. Preneel, I. Verbauwhede, "Revisiting a combinatorial approach toward measuring anonymity", *WPES 2008*.