Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks

Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung

Department of Electrical and Computer Engineering

The University of British Columbia, Vancouver, BC, Canada, V6T 1Z4

E-mail: {jooahans, vincentw, vleung}@ece.ubc.ca

Abstract—Advances in mobile networks and positioning technologies have made location information a valuable asset in vehicular ad-hoc networks (VANETs). However, the availability of such information must be weighted against the potential for abuse. In this paper, we investigate the problem of alleviating unauthorized tracking of target vehicles by adversaries in VANETs. We propose a vehicle density-based location privacy (DLP) scheme which can provide location privacy by utilizing the neighboring vehicle density as a threshold to change the pseudonyms. We derive the delay distribution and the average total delay of a vehicle within a density zone. Given the delay information, an adversary may still be available to track the target vehicle by a selection rule. We investigate the effectiveness of DLP based on extensive simulation study. Simulation results show that the probability of successful location tracking of a target vehicle by an adversary is inversely proportional to both the traffic arrival rate and the variance of vehicles' speed. Our proposed DLP scheme also has a better performance than both Mix-Zone scheme and AMOEBA with random silent period.

I. INTRODUCTION

Recently, significant progress has been made in Intelligent Transportation Systems (ITS) to create a safe and efficient driving environment. The DSRC (Dedicated Short Range Communications) [1] is a short to medium range wireless technology for vehicle-to-roadside (V2R) and vehicle-to-vehicle (V2V) communications. Vehicular ad hoc network (VANET) is an important component in ITS, and is expected to play a crucial role in various applications such as safety, driver assistance, and infotainment. In safety enhancing applications, each vehicle needs to periodically broadcast an authenticated safety message, which includes its verifiable identity, its current location, speed, and acceleration. Although these safety messages can help to prevent accidents, they may also be used by the adversaries for unauthorized location tracking of vehicles. By using an external WiFi network, an attacker can eavesdrop on all the broadcast messages and determine the locations visited by the vehicles (or users) over a period of time. The location history information (or mobility traces of the target vehicles) can be exploited for advertisement or surveillance. Thus, protecting the location privacy of vehicles is important because the lack of privacy may hinder the wide acceptance of VANET technology.

In general, location privacy protection schemes for mobile networks can be classified as policy-based [2] and anonymity-based [3]. In policy-based schemes, vehicles specify their location privacy preferences as policies and trust that the

third party location-based service (LBS) providers adhere to these policies. In the anonymity-based approaches, the location tracking of a target vehicle can be mitigated by using a randomly chosen and changing identifier, called the *pseudonym* [4]. Pseudonyms can either be a set of public keys, network layer addresses [5], or link layer addresses [6]. Pseudonyms are generated in a predefined way such that the adversaries cannot link a new pseudonym to previous ones of the same vehicle. The change of pseudonym denotes that the vehicle either changes its public key or addresses on the different layers (i.e., network and link). This approach regards anonymity as being untraceable between two successive locations of the target. Since pseudonyms cannot be linked to each other, they can provide a certain degree of privacy. In general, frequently changing pseudonyms are accepted as a solution to protecting the privacy of VANET [7]. Note that changing the pseudonym only at one layer may still pose a risk that an attacker can link two pseudonyms from the unchanged address at the other layer.

We now summarize some of the location privacy enhancement schemes proposed in the literature. AMOEBA [8] can mitigate the unauthorized location tracking of vehicles by using the concept of group navigation for V2R communications and by introducing the random silent period between update of pseudonyms [9] for V2V communications. In [10], the road network is divided into observed zones and unobserved zones from the viewpoint of the adversaries. Observed zones are those areas where the adversaries can track the locations of the target vehicles. The unobserved zones (also called the mix zones) are some predetermined locations (e.g., road intersections) where the vehicles vary their directions, speeds, and their pseudonyms. The adversaries would have difficulty in linking the vehicles that emerge from the mix zone to those that entered it earlier. Since the locations of mix zones are predetermined, the adversaries may still attempt to eavesdrop on transmissions originating from the mix-zone area. In the CMIX (Cryptographic MIX-zone) [11], each vehicle obtains a public/private key pair from certificate authority (CA) via the road-side unit (RSU), and utilizes these keys to encrypt all messages while they are within the mix zone.

The concept of location k -anonymity [12] is proposed for protecting the location information through spatial and temporal cloaking. In spatial cloaking, a vehicle broadcast its coarse-grained spatial range information when the number of

Fig. 1. An example of a VANET with three density zones. The solid black lines denote the road. The shaded areas correspond to the density zones.

vehicles within its range is greater than a certain threshold. In temporal cloaking, the beacon message will not be broadcast by the vehicle until a certain number of other vehicles have visited the same location.

In this paper, we generalize the concept of both grouping and mix-zone by using the neighboring vehicle density. By monitoring the neighboring vehicle density, each vehicle updates its pseudonym only when there are at least $k-1$ distinct neighboring vehicles. To the best of our knowledge, it is the first approach that considers the neighboring vehicle density as the triggering factor for updating the pseudonym. The goal of our proposed scheme is to minimize the probability of successful location tracking of a target vehicle by an adversary. The contributions of this paper are as follows:

- 1) We propose the vehicle density-based location privacy (DLP) scheme, which can mitigate the location tracking of vehicles by changing pseudonyms based on a threshold in neighboring vehicle count within a density zone.
- 2) We derive the delay distribution and the expected total delay of a vehicle within the density zone. Given the delay information, an adversary may still be available to track the target vehicle based on a selection rule.
- 3) Simulation results show that the probability of successful location tracking by an adversary is inversely proportional to the intensity of the traffic and the variance of the vehicles' speed. Our proposed DLP scheme outperforms both AMOEBA (with random silent period) [8] and Mix-Zone [10] schemes in reducing the probability of successful tracking by an adversary.

This paper is organized as follows. The system model is described in Section II. Our proposed DLP scheme is described in Section III. Performance evaluations and comparisons are presented in Section IV. Conclusions are given in Section V.

II. SYSTEM MODEL

We define the k -density zone of vehicle v as the area where at least $k-1$ distinct neighboring vehicles always exist around v . The density zone consists of M ports and N intersections. All vehicles can enter and exit the density zone only via these

Fig. 2. Topology of a road intersection.

ports. An intersection is a road junction where two or more roads either meet or cross. Fig. 1 shows an example of three density zones with different values of M and N . We study the privacy protection of the vehicle operation under a global passive adversary (GPA) [8]. GPA aims to locate and track the target vehicles within a region-of-interest by eavesdropping on their authenticated safety broadcast messages with verifiable identity and location information. GPA leverages the deployed infrastructure (e.g., WiFi network) and utilizes the adversarial RSU deployed to track the movement of the target vehicles within the region-of-interest.

Although the GPA cannot distinguish the target vehicle from other vehicles within the density zone due to the change of pseudonym [10] [11], it can still eavesdrop on all the broadcast messages within the density zone. By installing radio receivers at opportune locations, the GPA can observe entering and exiting events of vehicles where an event is a pair consisting of a port number and a time stamp. In addition, a GPA can either measure (via extensive real measurements [10]) or estimate the probability distribution of the delay of vehicles within the density zone. Given the delay distribution, a GPA can attempt to link an entering vehicle and an exiting vehicle with certain success probability. In the following subsections, we describe how the GPA obtain the delay distributions via estimation.

A. Road Traffic Model

From Fig. 2, after entering the density zone via port i , each vehicle travels at a distance d_i with constant speed S_i which is chosen independently from a normal distribution $f_{S_i}(s_i)$ with mean μ_i and variance σ_i^2 [13] as:

$$f_{S_i}(s_i) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(s_i - \mu_i)^2}{2\sigma_i^2}}, \quad s_i > 0. \quad (1)$$

From an empirical study on the real freeway traffic (i.e., 5-lane highway at California for 24 hours) [14], we can assume that the inter-arrival time A_i of vehicles to port i has an exponential distribution $f_{A_i}(a_i)$ with parameter λ_i :

$$f_{A_i}(a_i) = \lambda_i e^{-\lambda_i a_i}, \quad a_i > 0 \quad (2)$$

Fig. 3. Total delay in a density zone.

where the average arrival rate λ_i (vehicles/sec) can be estimated via traffic flow measurement. Thus, vehicles arrive at the port i according to a Poisson process with rate λ_i . At the intersection, each vehicle chooses the output port j with probability α_{ij} where

$$\sum_{j=1}^M \alpha_{ij} = 1. \quad (3)$$

B. Delay Model in a Density Zone

In this section, we determine the probability density function (pdf) of the total delay of a vehicle from entering port i to exit port j . From Fig. 3, when the vehicle is on the road segment i , it moves at a constant speed S_i chosen independently from (1). Given the distance of the i^{th} road segment d_i , the delay for traveling on this road segment $T_i = d_i/S_i$. Thus,

$$\begin{aligned} P(T_i \leq t_i) &= P(S_i \geq d_i/t_i) \\ &= 1 - P(S_i \leq d_i/t_i). \end{aligned} \quad (4)$$

By taking the derivative with respect to t_i , we have

$$f_{T_i}(t_i) = \frac{d_i}{t_i^2} f_{S_i} \left(\frac{d_i}{t_i} \right). \quad (5)$$

By substituting (1) into (5), we obtain

$$f_{T_i}(t_i) = \frac{d_i}{\sqrt{2\pi}\sigma_i t_i^2} e^{-\frac{(d_i/t_i - \mu_i)^2}{2\sigma_i^2}}, \quad t_i > 0. \quad (6)$$

The average signal delay p_i is the time it takes for a vehicle from port i waiting at the intersection for the traffic light to turn green. We choose the widely used average signal delay formula from [15]:

$$p_i = \frac{c(1 - g/c)^2}{2(1 - (g/c)x_i)} + \frac{x_i^2}{2\lambda_i(1 - x_i)} - 0.65 \left(\frac{c}{\lambda_i^2} \right)^{1/3} x_i^{2+5(g/c)}, \quad (7)$$

where c denotes the average time (sec) to display all traffic signal indications (i.e., green, red, and yellow) at an intersection, g denotes the average green signal time (sec), x_i degree of saturation on road segment i , and λ_i denotes the arrival rate (vehicles/sec) at port i . Given the estimated values of c , g , x_i , and λ_i , the average signal delay p_i can be determined and be considered as a constant in the subsequent derivation.

As shown in Fig. 3, the total delay that a vehicle experienced in the density zone from entering port i to exit port j , denoted by T_{ij} , is

$$T_{ij} = T_i + p_i + T_j. \quad (8)$$

The cumulative distribution function (cdf) of T_{ij} is

$$\begin{aligned} F_{T_{ij}}(t) &= P(T_{ij} \leq t) \\ &= P(T_i + T_j \leq t - p_i). \end{aligned} \quad (9)$$

Since the random variables T_i and T_j are independent and identically distributed (i.i.d.), we obtain

$$F_{T_{ij}}(t) = \int_0^{t-p_i} \left(\int_0^{t-p_i-t_i} f_{T_j}(t_j) dt_j \right) f_{T_i}(t_i) dt_i, \quad t > p_i. \quad (10)$$

From (6) and (10), the pdf of T_{ij} (i.e., $f_{T_{ij}}(t)$) can be determined numerically. From (10), the average delay for a vehicle to travel from port i to port j is

$$\begin{aligned} \mu_{ij} &= E[T_{ij}] \\ &= E[T_i] + p_i + E[T_j]. \end{aligned} \quad (11)$$

C. The Operation of an Adversary

An adversary can utilize the location information of the target vehicles to infer details about the traveling pattern of the individuals. By installing radio receivers at some sections of the roads, an adversary can eavesdrop on the beacon messages sent by the vehicles with VANET capabilities.

We assume that the adversary has information of the system model of the density zones. It can also observe the entering and exit events corresponding to vehicles entering and exiting the density zone, respectively. An entering event consists of the port where the vehicle entered the density zone, and the time when it happened. Similarly, an exit event consists of the port where the vehicle left the density zone, and the time when it happened.

The objective of an adversary is to relate exit events to entering events. Specifically, in our model, the adversary selects a target vehicle v and tracks its movement until it enters the density zone. Within the density zone, the target vehicle may change its pseudonym if it satisfies the criteria in the DLP scheme (as explained in the next section). In the following, we denote the port at which the target vehicle v entered the density zone by i . Without loss of generality, assume that v entered port i at time 0. The adversary observes the exit events at all ports $j \in \mathcal{J}$ for a time T_{max} such that the probability that the target vehicle v leaves the density zone before T_{max} approaches to 1. The adversary records the time $t_{ij}(v_r)$ for each vehicle v_r which exits port j before T_{max} . Let $\{v_1, \dots, v_R\} \in \mathcal{V}$ be the set of vehicles observed during the time interval $(0, T_{max})$. We propose a selection rule for an adversary to choose a vehicle $v' \in \mathcal{V}$ to be the target vehicle v as follows:

Rule: The adversary chooses a vehicle which minimizes the time difference between the average delay μ_{ij} to the exit time t_{ij} of all candidate vehicles:

$$(v', j') = \arg \min_{\{v_1, \dots, v_R\} \in \mathcal{V}, j \in \mathcal{J}} \alpha_{ij} (t_{ij}(v_r) - \mu_{ij})^2. \quad (12)$$

The multiplication of α_{ij} gives a different weight value depending on the direction of vehicle at the intersection. The adversary is successful in tracking the target vehicle if the selected vehicle v' is indeed the target vehicle v .

III. DENSITY-BASED LOCATION PRIVACY (DLP)

In DLP scheme, each vehicle can provide connectivity information by broadcasting local beacon messages periodically. A beacon message is a short packet with the current pseudonym and location information of the vehicle. At every beacon interval Δt , the vehicle checks whether it has sent a broadcast within the last Δt (e.g., the default beacon interval in 802.11-based networks is 100 ms). If it has not, it will broadcast a beacon message with time-to-live (TTL) value equals to 1. The value of Δt is a configurable parameter for various speed of vehicles. Each vehicle v determines its *neighboring node density* (or *neighboring vehicle count*) by listening for beacon messages from its set of neighbors. If a vehicle v has not received a beacon message from another neighbor m for Δt , the vehicle v assumes that the link to its neighbor m is lost. Therefore, the vehicle v decreases its neighboring vehicle count by 1. On the other hand, whenever vehicle v receives a beacon message from a new neighbor (i.e., with a new pseudonym), v will increase its neighboring vehicle count by 1. Due to the change of pseudonym of neighboring vehicles, the neighboring vehicle count can be greater than the real density for Δt at maximum.

If the deployed network layer protocol does not support the exchange of beacon messages, each vehicle can maintain accurate information about its continued connectivity to its neighboring vehicles by using either link layer or other network layer mechanisms. Any adequate link layer notification, such as those provided by IEEE 802.11, can be used to determine connectivity. For example, the absence of a link layer feedback or failure to receive a clear-to-send (CTS) after sending a request-to-send (RTS) may indicate the loss of the link to its neighboring vehicle. If link layer notification is not available, passive acknowledgment can be used in network layer when the neighboring vehicle is expected to forward the packet, by listening to the channel for a transmission attempt made by the neighboring vehicle. If transmission is not detected within a predefined timeout value, an Internet control message protocol (ICMP) [16] echo request message can also be sent to the target neighboring vehicle. If a link to the neighboring vehicle cannot be detected by any of the above methods, the vehicle assumes that the link is lost.

We assume each vehicle v has been preloaded with S different pseudonyms $\{\psi_{v,1}, \psi_{v,2}, \dots, \psi_{v,S}\}$, where S is a large number. Pseudonyms can either be a set of public keys, network layer or link layer addresses. A pseudonym change is triggered by vehicles only when the neighboring vehicle count is more than or equal to $k - 1$. In other words, DLP prevents a privacy breach by ensuring that each vehicle triggers a pseudonym change only if there are at least $k - 1$ neighboring vehicles.

There are several metrics to quantify the level of privacy provided by DLP. The metric in our model is the *probability of successful tracking of a target vehicle by an adversary* when making its decision as described in Section II-C. If the success probability is large, the density zone and changing

TABLE I
SIMULATION PARAMETERS.

Parameter	Value
Arrival rate λ_1 (arrivals/sec)	0.005 ~ 0.180
Average speed $\mu_1, \mu_2, \mu_3, \mu_4$ (m/sec)	14
Variance $\sigma_1^2, \sigma_2^2, \sigma_3^2, \sigma_4^2$	1, 3, 5, 7, 9
Distance d_1, d_2, d_3, d_4 (m)	500
Probability $\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}$	0, 1/3, 1/3, 1/3
Cycle length c (sec)	60
Average green signal time g (sec)	30
Degree of saturations x_i	0.02 ~ 0.72
Number of simulations	100

pseudonyms are ineffective. On the other hand, if the success probability is small, then tracking is difficult and the system ensures location privacy. The probability of successful tracking cannot be determined analytically due to the complexity of our model. Therefore, we ran simulations to determine its empirical value in realistic situations. The simulation setting and parameters as well as the simulation results are presented in the next section.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the achievable location privacy under various traffic conditions. We first evaluate the performance of our proposed DLP scheme. We then compare the performance between our proposed DLP scheme with Mix-Zone [10] and AMOEBA with random silent period [8] schemes. Table I provides a summary of the simulation parameters. The ns-2 [17] simulator is used for the implementation of our proposed scheme. SUMO [18] is used to generate all the necessary files for the network topology, traffic signal logic, and mobility models for the corresponding density zones. We extended several modules in SUMO so that it can support both the normal distribution of vehicle speed and the Poisson arrival of vehicles. Using TraNS [19], SUMO car movement file is converted to the ns-2 mobility file. The ns-2 source code is also modified to count the number of neighbors with varying beacon intervals. We performed multiple independent simulation runs to obtain an estimation of the probability of successful tracking of a target vehicle by a GPA.

The number of vehicles is 100. Each simulation run takes 30,000 simulated seconds. The average speed of vehicles is 14 m/s (i.e., 50.4 km/hr). For medium access control, the IEEE 802.11 distributed coordination function is used. The nominal data rate is 2 Mb/s and a transmission radio range is 250 m. The propagation model combines both free space propagation model and two-ray ground reflection model. We performed multiple independent simulation runs to obtain an estimation of the probability of successful tracking of a target vehicle by a GPA.

A. Performance of DLP

In the following, we outline the topology and mobility model for the performance evaluation of our proposed DLP scheme.

Fig. 4. Probability of successful location tracking by an adversary under different arrival rate and variance for DLP.

- *Network Topology*: A density zone is composed of one intersection and four road segments in each direction (see Fig. 2). Each segment has one lane that prevents following vehicles from passing the preceding ones.
- *Mobility Pattern*: All vehicles within the density zone are assumed to travel at a constant speed given by (1) at each segment. At the intersection, all vehicles experience the delay based on the signal logic of intersection.

In the first set of simulations, we investigate the success probabilities of the adversary as a function of both arrival rate and the variance σ_i^2 of the vehicles' speed. Fig. 4 shows the success probabilities of the location tracking when both the arrival rate and variance σ_i^2 of vehicles' speed vary. Here, adversary uses the equation (12) to detect a target vehicles. In other words, for each exiting vehicle, the adversary chooses a vehicle which can minimize the time difference between the average delay to the exit time of all candidate vehicles. Each curve matches a different value of σ_i^2 . Results indicate that the success probability of the adversary decreases as the variance of vehicles' speed increases. The main reason is that the total delay is inversely proportional to the speed of vehicles. Therefore, as the variance of vehicles' speed increases, the variance of total delay decreases. This makes it difficult to find a target vehicle with the highest probability as the variance of vehicles' speed increases.

B. Performance Comparison with Other Schemes

The topology for the performance comparison among AMOEBA, Mix-Zone, and DLP is shown in Fig. 5. There are three density zones with different values of AR , which is the arrival rate of vehicles in density zone. Each vehicle is allowed to change its own pseudonym only one time during the whole travel. For example, if a vehicle v changes its pseudonym in the density zone #1, it cannot change its pseudonym in the other two density zones. In AMOEBA, each vehicle can change its pseudonym only when there are new neighboring

Fig. 5. Topology for performance comparison between AMOEBA [8], Mix-Zone [10], and our proposed DLP scheme. AR denotes the arrival rate of vehicles in a density zone.

Fig. 6. Probability of successful location tracking by an adversary under different variance of vehicles' speed for Mix-Zone, AMOEBA, and DLP.

vehicles joining the density zone via the entrance ramp. After a silent period chosen randomly between 0.1 to 3 seconds (recommended values in [8]), each vehicle can update its own pseudonym. In Mix-Zone scheme, each vehicle changes its pseudonym in any density zone with the same probability of $1/3$. In our proposed DLP scheme, each vehicle changes its pseudonym in the density zone only when there are at least $k - 1$ neighboring vehicles on average. The value of k is set to 10 in the simulation.

Fig. 6 shows the success probabilities of location tracking by an adversary between AMOEBA, Mix-Zone, and DLP in multiple density zones. Since DLP can choose the density zone where the average number of neighboring vehicles (or the average neighboring vehicle density) is greater than or equal to k , the probability of successful location tracking of a target vehicle by an adversary is lower than those of both AMOEBA and Mix-Zone schemes. Although AMOEBA can provide unlinkability between the new and old pseudonyms by using a random silent period, it cannot always find the density zone with k neighboring vehicles on average.

V. CONCLUSION

In this paper, we studied the effectiveness of changing pseudonyms to provide location privacy in VANETs. The approach of changing pseudonyms to make location tracking more difficult was proposed in prior work, but its effectiveness has not been investigated in either an analytical or numerical manner. In order to tackle this issue, we derived a delay model of vehicles in the density zone. We assumed that the adversary has sufficient knowledge (i.e., the delay distribution of the vehicles) in density zone. Based on this information, an adversary may try to select a vehicle which exits the density zone to the target vehicle that entered it earlier. We proposed the vehicle density-based location privacy (DLP) scheme, which can mitigate the location tracking of vehicles by changing pseudonyms based on a threshold in neighboring vehicle count within a density zone. We performed extensive simulations to study the probability of successful tracking of a target vehicle by an adversary under different scenarios. Simulation results showed that our proposed DLP scheme also has a better performance than both Mix-Zone and AMOEBA with random silent period in terms of a lower probability of successful tracking by an adversary.

In this paper, we assumed that the frequency of the update of pseudonyms has no effect to the privacy. However, in general, frequent updates of pseudonym may give an advantage to the privacy. On the other hand, the higher the frequency, the larger the cost that the pseudonym updates induce on the system in terms of the design of communication protocols between layers. Future work will investigate the optimal frequency of the pseudonym updates, and enhance the analytical studies with different intersection delay models and service time distributions.

ACKNOWLEDGEMENT

This research is funded in part by AUTO21, a member of the Network of Centres of Excellence of Canada program, and by Nokia Products Limited, Canada.

REFERENCES

- [1] "Standard specification for telecommunications and information exchange between roadside and vehicle systems - 5 GHz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications," ASTM E2213-03, Sept. 2003.

- [2] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 56–64, Mar. 2003.
- [3] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of ACM Int'l Conf. Mobile Systems, Applications, and Services (MobiSys)*, San Francisco, CA, May 2003.
- [4] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs," *Lecture Notes in Computer Science (LNCS)*, vol. 4357, pp. 43–57, Mar. 2007.
- [5] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice," in *Proc. of IEEE WCNC*, Hong Kong, China, Mar. 2007.
- [6] M. Lei, X. Hong, and S. V. Vrbsky, "Protecting location privacy with dynamic MAC address exchanging in wireless networks," in *Proc. of IEEE Globecom*, Washington, DC, Nov. 2007.
- [7] M. Garlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in *Proc. of IEEE VTC-Spring*, Dublin, Ireland, Apr. 2007.
- [8] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE J. Select. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
- [9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. of IEEE WCNC*, New Orleans, LA, Mar. 2005.
- [10] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. of European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS)*, Cambridge, UK, July 2007.
- [11] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proc. of Int'l Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, Vancouver, BC, Aug. 2007.
- [12] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: architecture and algorithm," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, Jan. 2008.
- [13] M. Khabazian and M. Ali, "A performance modeling of vehicular ad hoc networks (VANETs)," in *Proc. of IEEE WCNC*, Hong Kong, China, Mar. 2007.
- [14] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in sparse vehicular ad hoc wireless networks," *IEEE J. Select. Areas Commun.*, vol. 25, no. 8, pp. 1538–1556, Oct. 2007.
- [15] "Highway capacity manual," Transportation Research Board, Special Report 20, National Research Council, Washington, DC, 1985.
- [16] S. Deering, "ICMP Router Discovery Messages," 1991. [Online]. Available: <http://www.ietf.org/rfc/rfc1256.txt>
- [17] NS-2 simulator. [Online]. Available: <http://www.isi.edu/nsnam/ns/>
- [18] Simulation of urban mobility (SUMO). [Online]. Available: <http://sumo.sourceforge.net>
- [19] Traffic and network simulation environment VANETs (TraNS). [Online]. Available: <http://trans.epfl.ch>