Effectively Changing Pseudonyms for Privacy Protection in VANETs

Jianxiong Liao and Jianqing Li
Faculty of Information Technology
Macau University of Science and Technology
Macau SAR, China
liaojianxiong@gmail.com, jqli@must.edu.mo

***Abstract*—As a technology to improve safety, efficiency and convenience in transportation, Vehicular ad hoc Networks (VANETs) attract more and more attentions of researchers. VANETs will achieve a series of applications by periodically broadcasting beacons containing vehicular status information such as position, velocity and direction. However, some attackers might also utilize the information to track users' whereabouts. Therefore, the lack of privacy protection might impede the further success of VANETs in the future.**

Frequently changing pseudonyms are commonly accepted as a solution to protect privacy in VANETs, but most pseudonym change algorithms are ineffective. This paper proposes a pseudonym change algorithm, called *synchronous pseudonym change algorithm*, where both simultaneity of changing pseudonyms and vehicular status information are taken into consideration. Simulation results show that the algorithm can improve the effectiveness of changing pseudonyms to protect privacy in VANETs.

***Index Terms*—changing pseudonyms, privacy, VANET**

I. Introduction

VANETs consist of two kinds of network nodes, which are vehicles and road-side infrastructure units (RSUs). By means of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, vehicles share safety-related information to achieve a series of applications to improve safety and efficiency in transportation. These applications rely on the periodic broadcast of vehicular status information, such as position, velocity and direction, etc. For instance, cooperative safety application uses information shared among vehicles to avoid collisions.

Unfortunately, the information can also be used by eavesdroppers to track vehicle users. Many researchers propose frequently changing pseudonyms to avoid being tracked [1,2,3,4,12], but these solutions are fairly ineffective under the presence of global attackers. Solutions in [1,2,3] consider neither vehicular status information nor simultaneity of changing pseudonyms, and the solution in [12] only considers vehicular status information. Two vehicles can be clearly distinguished either by their different status information even if their pseudonyms are changed at the same time or by their time information of changing pseudonyms even if their status are similar. An attacker can utilize vehicular status information or time information of changing pseudonyms for linking pseudonyms to track vehicles. Simply changing pseudonyms in arbitrary time or in arbitrary status wastes pseudonyms, thus the number of needed pseudonyms for a vehicle increases, and accordingly, resources for storing or calculating them increase. For a VANET with a great number of vehicles, it is a big challenge to manage such a huge number of pseudonyms. Thereby, the main focus of this paper is to take into consideration vehicular status information and simultaneity of changing pseudonyms to improve the effectiveness of changing pseudonyms, and thus to reduce the total number of used pseudonyms.

The rest of this paper is organized as follows: related work is discussed in Section II. In Section III, attacks on changing pseudonyms are analyzed and our threat model is defined. Then *synchronous pseudonym change algorithm* is proposed in Section IV and three pseudonym change algorithms are evaluated for comparison in Section V. Finally, the conclusion is given in Section VI.

II. Related work

In [5,6], Beresford discusses position privacy in details and proposes the concept of Mix-zone. Mix-zones are anonymous regions of the network where mobile nodes change their identifiers to obfuscate the relation between entering and exiting events.

In [7], in order to reduce the rate of being tracked, J. Freudiger et al. propose an approach of using symmetry key to encrypt the beacons to make intersection areas to become mix-zones, and to combine several mix-zones to be a mix-network.

By utilizing the group navigation for V2I communications and by introducing the random silent period between update of pseudonyms for V2V communication, K. Sampigethaya et al. propose a scheme to provide location privacy, called AMOEBA[8].

In [9], Z. Ma et al. propose the pseudonym-on-demand scheme to support the functionalities of pseudonyms in terms of secure and privacy-preserved vehicular communications. In [10], they develop a quantitative metric to measure and quantify location privacy in VANETs.

In [11], M. Burmester et al. propose a set of cryptographic mechanisms that balance the tradeoff between privacy and accountability in VANETs and propose a strategy to strengthen location privacy in VANETs.

978-0-7695-3908-9/09 $26.00 © 2009 IEEE
DOI 10.1109/I-SPAN.2009.103

In [15], Joo-Han Song et al. propose a vehicle density-based location privacy scheme which can provide location privacy by utilizing the neighboring vehicle density as a threshold to change the pseudonyms.

In [12], M. Gerlach et al. propose a pseudonym change algorithm that uses a mix context model, and their algorithm assumes that a vehicle changes its pseudonym when a mix context is found. The mix context means a vehicle finds several vehicles with similar status around. However, their algorithm discusses an individual behavior and it is a low probability that at least two vehicles with similar status change pseudonyms at the same time. In addition, the mix context at best represents all the information that an attacker may use to link pseudonyms, but the simulation in [12] only considers vehicular partial status information - position information - to deduce the number of neighboring vehicles then to decide if changing pseudonym is needed. In this paper, the simultaneity of changing pseudonyms and more comprehensive status information which includes position, velocity and heading direction are taken into consideration.

III. Attacks on changing pseudonyms

Compared with tracking vehicles by cameras or manual tracking, the cost of using VANETs to track vehicles is greatly reduced because vehicular status information can be eavesdropped. If the current pseudonym of a target vehicle is linked with the next one by an attacker, its mobility trace is easily disclosed.

Attackers might utilize three major aspects which include non-volatile data, protocol information and data in beacon to link changing pseudonyms [4]. How to prevent attackers from using non-volatile data and protocol information to link pseudonyms is beyond our discussion scope. We only focus on data in beacon.

The status of a vehicle *i* is defined as $\{P_i, V_i, D_i\}$, P_i, V_i and D_i denote its position, velocity and heading direction respectively. Two vehicles with similar status is defined that their heading directions are the same, their velocities differ under *d* meters/second, the distance between them is smaller than *range* meters and they are in a same road segment (a road segment is defined that a road area between two intersections). The definition of our threat model is that: when vehicle *i* changes its pseudonym, if at least *n* ($n \geq 1$) other vehicles whose status are similar to vehicle *i* also change pseudonyms at the same time, the attack on vehicle *i* fails and the change of pseudonym is successful, otherwise, the change of pseudonym is failed.

IV. Synchronous pseudonym change algorithm

Currently, the most common pseudonyms change algorithm are *periodical pseudonym change algorithm* and *random pseudonym change algorithm*[12]. Both algorithms keep the pseudonym stable for a minimum stable time which is the requirement of position based routing[13], such as one minute. The *random pseudonym change algorithm* usually generates a random number before broadcasting a beacon. The pseudonym is changed if the random number is less than a *threshold* which is set in advance.

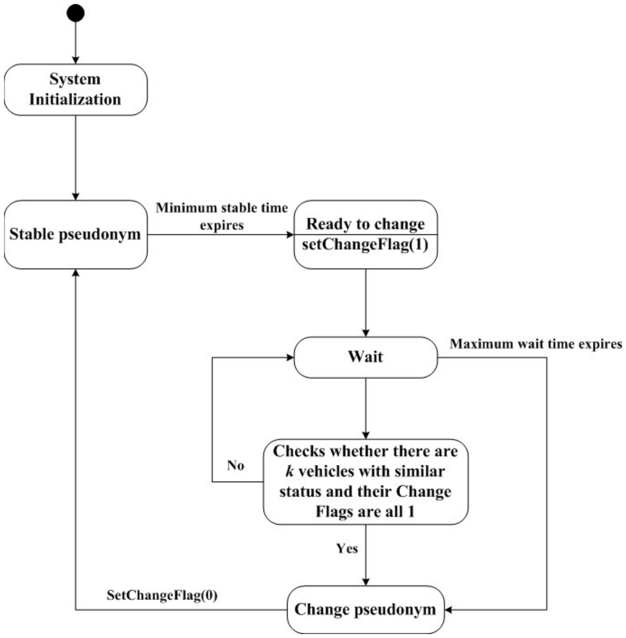

System Initialization
Stable pseudonym
Minimum stable time expires
Ready to change
setChangeFlag(1)
Wait
Maximum wait time expires
Checks whether there are k vehicles with similar status and their Change Flags are all 1
No
Yes
SetChangeFlag(0)
Change pseudonym

Fig. 1. Synchronous pseudonym change algorithm

If we do not take into consideration vehicular status information and simultaneity of changing pseudonyms, but simply periodically or randomly change its pseudonyms, the effectiveness is low. The purpose of changing pseudonyms can not be achieved once attackers successfully link the current pseudonym with the next one, by obtaining the whole or part of information in beacons which are periodically broadcasted. For example, if two vehicles are in the same area and change pseudonyms simultaneously, and they are near each other but different in velocity, an attacker is able to distinguish them based on their respective velocities, thus the changed pseudonyms are wasted.

Time information of changing pseudonyms can also be utilized by attackers. For instance, suppose vehicles send a beacon per second. Vehicle A broadcasts two beacons A_1 and A_2 with pseudonyms P_{A1} and P_{A2} at the first time slot and the second time slot respectively while vehicle B broadcasts two beacons B_1 and B_2 with pseudonyms P_{B1} and P_{B2} at the second time slot and the third time slot respectively. An attacker can use the time information to easily link P_{A1} with P_{A2}, and P_{B1} with P_{B2}. This motivates our idea to simultaneously change pseudonyms of more than two vehicles with similar status. "simultaneously" mentioned above means in the same time slot.

Next we propose a pseudonym change algorithm called *synchronous pseudonym change algorithm*. Our purpose is to provide a high probability that at least two vehicles with similar status change their pseudonyms simultaneously.

A general state diagram of *synchronous pseudonym change algorithm* is depicted in figure 1. When the system boots up,

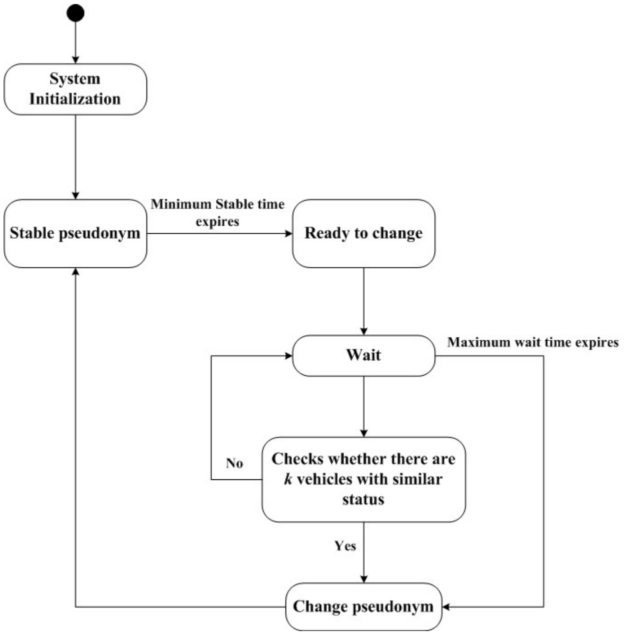

System Initialization
Stable pseudonym
Minimum Stable time expires
Ready to change
Wait
Maximum wait time expires
No
Checks whether there are *k* vehicles with similar status
Yes
Change pseudonym

Fig. 2. Similar status algorithm

the vehicle chooses a pseudonym from the TPD device where pseudonyms were installed in advance. After that, the system enters the pseudonym update cycle and waits for expiry of the minimum stable time. When the minimum stable time expires, the system sets *change flag* to 1. The *change flag* is additionally inserted in beacons which is used to announce that the vehicle is ready to change its pseudonym. Then the system enters a *wait-check* subcycle. The vehicle waits for a trigger to change pseudonym, checks if there are *k* vehicles whose status are similar to itself and whose *change flags* are all 1. If a trigger is found, the vehicle changes its pseudonym and then sets *change flag* to 0. If a vehicle does not find a trigger within a *maximum wait time*, it changes pseudonym by force.

A vehicle *i* can receive beacons from other vehicles within its communication range. When vehicle *i* finds *k* vehicles with similar status and their *change flags* are all 1, some or all of the *k* vehicles may also find the trigger because they are in neighborhood, thus the probability of one or more vehicles change pseudonyms simultaneously with vehicle *i* is high. The probability is related to the number *k* and traffic conditions, and it is left for discussion in the future.

If we do not consider the simultaneity, the "setChange-Flag()" component in figure 1 should be deleted, the *synchronous pseudonym change algorithm* becomes *similar status algorithm* which is depicted in figure 2. There are two differences between *similar status algorithm* and *mix-contexts algorithm* proposed in [12].

The first one is the mechanism in *mix-contexts algorithm* which assesses whether the change of pseudonym is successful after a pseudonym is changed. If the change is not successful, the system ignores the process of waiting for expiry of the minimum stable time and tries to change the pseudonym again. The minimum stable time of a pseudonym is not guaranteed and thus in an extremely worst case the system may change pseudonyms continually, and more pseudonyms are wasted. For *similar status algorithm*, after one pseudonym is changed, no matter whether the change of pseudonym is successful or not, the system enters the process of waiting for expiry of the minimum stable time.

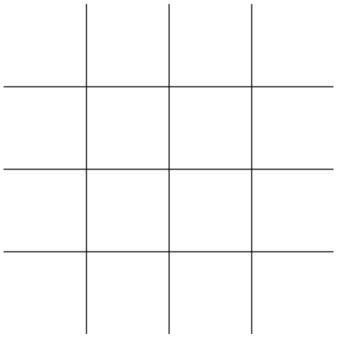


Fig. 3. Road map

The second one is *maximum wait time* mechanism which is added in *similar status algorithm*. Without maximum wait time mechanism, *mix-contexts algorithm* can not handle the extreme instance when a vehicle can not find a mix context to change pseudonym for an extremely long time because of lack of mix contexts.

For comparison, we simplify the component of "checks whether there are *k* vehicles with similar status" in figure 2 to the component of "checks whether there are *k* vehicles with similar position information", thereby it becomes *position algorithm*, whose assumption is the same as simulation conditions in [12].

V. SIMULATIONS

By using C++ language we write a simulation engine according to vehicular mobility model STRAW [14] which offers advanced vehicular behavior and simplifies traffic control mechanisms. We simulate three pseudonym change algorithms which are all described in the last section to compare their effectiveness of changing pseudonyms.

A. Road model

Figure 3 depicts a simple road map used in our simulations. Line section between two intersections denotes a road segment. All segments have two directions and each direction has two lanes. Each segment's length is set to 1 km and its width is set to 14m for four lanes. There are 9 intersections, 12 entrances and 12 exits in this road map region.

B. Traffic light model

We assume that only vehicles in one segment can pass through (turn left, turn right, go straight) if the segment's traffic lights turn green. Green lights are set to last for 30 seconds, so the cycle of traffic lights is 120 seconds.

C. Vehicular behavior model

When a vehicle approaches an intersection, the probability of turning left, turning right or going straight is the same. Its behavior follows STRAW mobility model and the maximum velocity is set to 10∼15 meters/second. Vehicles are evenly distributed in the road map region with their maximum velocity at the initial time, and the number of vehicles is determined according to the corresponding traffic density. The communication range of vehicle is set to 250 meters. If a vehicle moves out of the road map region, its pseudonym update is terminated.

D. Simulation parameters

During our simulations, we conduct a comparison among three pseudonym change algorithms by changing the following parameters:

1) *Traffic density*

2) *Penetration rate*

The *traffic density* defines how many vehicles averagely could be found on one kilometer street length. The five traffic density ranges[12] are chosen as follows:

< 16	vehicles/km	low traffic density
16 - 23	vehicles/km	medium traffic density
24 - 31	vehicles/km	high traffic density
32 - 45	vehicles/km	very high traffic density
> 45	vehicles/km	overload

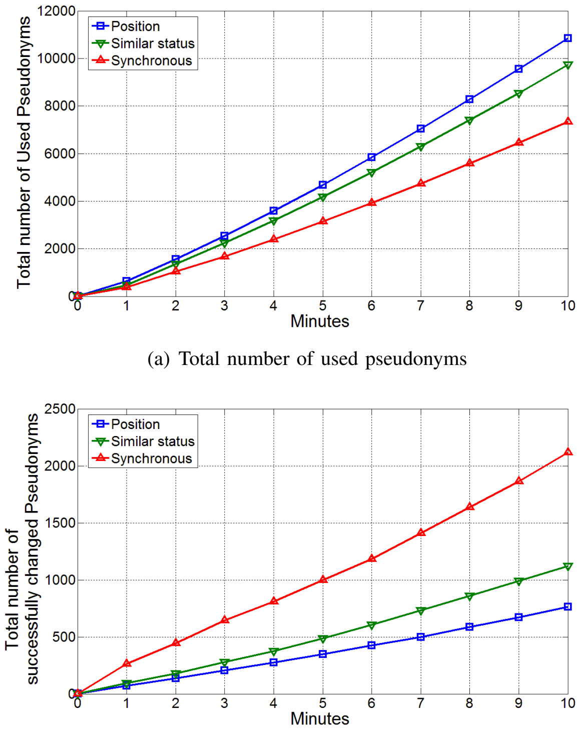
According to different traffic density ranges, we set corresponding frequencies of vehicles entering the road map region.

Penetration rate refers to the ratio of the number of vehicles installed with communication modules to the total number of vehicles. Since the deployment of VANETs is a long process, *penetration rate* is an important parameter for comparison among different algorithms. In this paper we assume a fixed beacon update rate of 1 *Hz* and the minimum stable time is set to one minute. The simulation time is 10 minutes in each simulation run and a simulation result is averaged by ten simulation runs.

E. Simulation results

Figure 4 compares the total number of used pseudonyms and the total number of successfully changed pseudonyms among three algorithms. It is observed that when a simulation finishes, compared with *similar status algorithm*, the *synchronous pseudonym change algorithm* reduces up to about 25% of the total number of used pseudonyms while increases up to 90% of the total number of successfully changed pseudonyms.

Figure 5 describes the influence of *penetration rate* on three algorithms. Figure 5(a) shows that for the all three algorithms, the average number of used pseudonyms per vehicle increases as the *penetration rate* increases because the number of events that satisfy the requirements of actively changing pseudonyms increases. It can be seen from figure 5(b) that the successful rate of changed pseudonyms for *synchronous pseudonym change algorithm* increases from 10.5% to 28.9% as *penetration rate* increases. It is important to note that *synchronous pseudonym change algorithm* even has lower successful rate than *similar status algorithm* in low penetration rate. That is because most vehicles following *synchronous pseudonym change algorithm* can not find a trigger to actively change pseudonym and most pseudonyms are changed by force when the *maximum wait time* is expired. Increasing the *maximum wait time* is an optional way to improve the performance of *synchronous pseudonym change algorithm* in low penetration rate.



(a) Total number of used pseudonyms

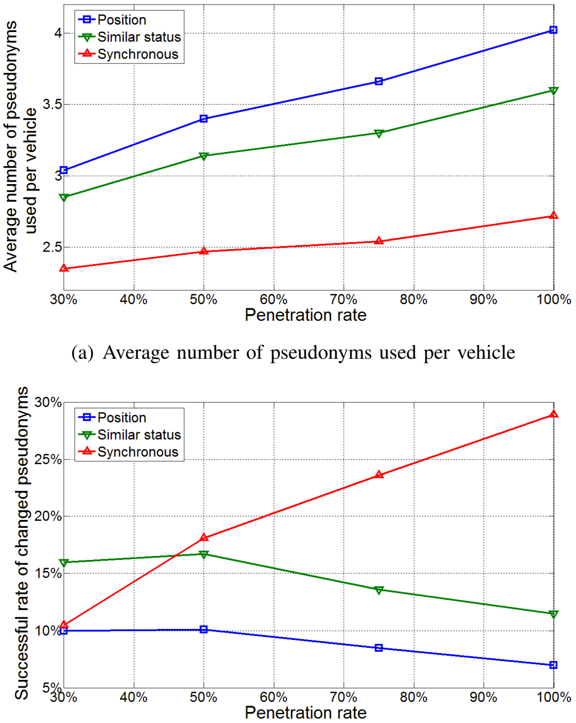
(b) Total number of successfully changed pseudonyms

Fig. 4. Comparison among three algorithms in the total number of used pseudonyms and the total number of successfully changed pseudonyms. *Traffic density* = medium, *Range* = 20 meters, *Penetration rate* = 100%, *d*= 0.5 meters/second, *k* = 2, *n* = 1, *Maximum wait time* = 60 seconds.

Figure 6 describes the influence of *traffic density* on three algorithms. Figure 6(a) shows that more pseudonyms are used as the *traffic density* increases for all three algorithms because there are more opportunities for vehicles to find the corresponding trigger to change pseudonyms. The curves of the three algorithms in figure 6(a) are similar with those in figure 5(a). It can be observed in figure 6(b) that the difference of successful rate of changed pseudonyms between *similar status algorithm* and *synchronous pseudonym change algorithm* increases from 13% to 37.3% as the *traffic density* increases.

VI. Conclusion

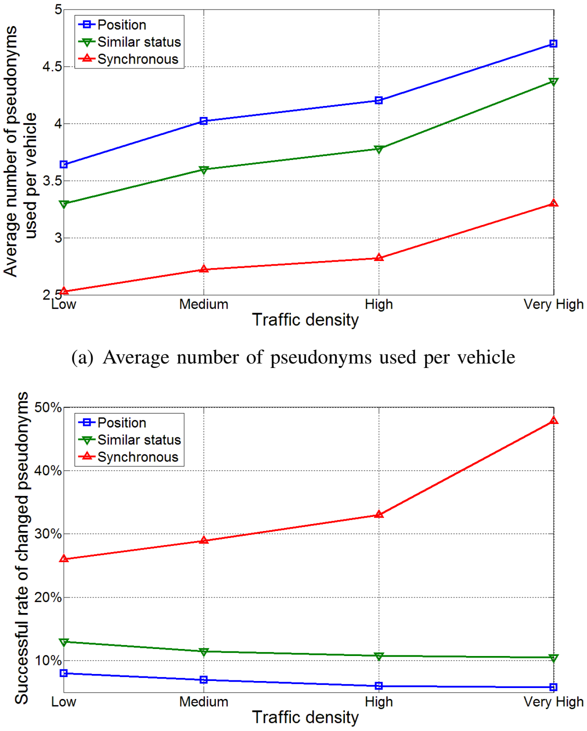
It is shown by the simulations that *synchronous pseudonym change algorithm* has a best performance among the three algorithms and *similar status algorithm* is better while *position algorithm* is last. That is because *position algorithm* and



(a) Average number of pseudonyms used per vehicle

(b) Successful rate of changed pseudonyms

Fig. 5. Influence of *penetration rate* on three algorithms. *Traffic density* = medium, *Range* = 20 meters, *d* = 0.5 meters/second, *k* = 2, *n* = 1, *Maximum wait time* = 60 seconds.



(a) Average number of pseudonyms used per vehicle

(b) Successful rate of changed pseudonyms

Fig. 6. Influences of *traffic density* on three algorithms. *Penetration rate* = 100%, *Range* = 20 meters, *d* = 0.5 meters/second, *k* = 2, *n* = 1, *Maximum wait time* = 60 seconds.

similar status algorithm only consider partial and all vehicular status information respectively while *synchronous pseudonym change algorithm* not only considers vehicular status information but also considers simultaneity of changing pseudonyms. Increasing the *maximum wait time* seems a simple way to improve the performance of *synchronous pseudonym change algorithm* because a vehicle has more time to search a trigger to change pseudonym, but the risk of being tracked increases because an attacker also has more time to track a vehicle, so how to balance the performance and the risk is our future work.

References

[1] P. Papadimitratos et al, "Secure vehicular communication systems: design and architecture," IEEE Communications Magazine, Nov. 2008.

[2] M. Raya and J-P. Hubaux, "The security of vehicular ad hoc networks," in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN), 2005.

[3] M. Raya, P. Papadimitratos, J-P. Hubaux. "Securing Vehicular Networks," IEEE Wireless Communications, Oct. 2006.

[4] F. Armknecht, A. Festag, D. Westhoff, K. Zeng, "Cross-Layer Privacy Enhancement and Non-Repudiation in Vehicular Communication," in Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks (WMAN), March 2007.

[5] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Computing, Mar. 2003.

[6] A. R. Beresford, "Location privacy in ubiquitous computing," Dissertation, University of Cambridge, 2005.

[7] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix-Zones for Location Privacy in Vehicular Networks," in Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), Aug. 2007.

[8] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," IEEE Selected Areas in Communications, Oct. 2007.

[9] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications," in Proceedings of the 2nd IEEE International Symposium on Wireless Vehicular Communications (WiVeC), Sep. 2008.

[10] Z. Ma, F. Kargl, and M. Weber, "A location privacy metric for V2X communication systems," in Proceedings of 2009 IEEE Sarnoff Symposium, Mar. 2009.

[11] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," in Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB), 2008.

[12] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real," in Proceedings of the 65th Vehicular Technology Conference (VTC), April 2007.

[13] I. Stojmenovic, "Position-based routing in ad hoc networks," IEEE Communication Magazine, July 2002.

[14] D. Choffnes and F. Bustamante, "An integrated mobility and traffic model for vehicular wireless networks," in Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, Sep. 2005.

[15] Joo-Han Song, Vincent W.S. Wong and Victor C. M. Leung, "Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks," Mobile Networks and Applications, May 2009.