# RSSI-Based User Centric Anonymization for Location Privacy in Vehicular Networks

Yu-Chih Wei[1,2], Yi-Ming Chen[1], and Hwai-Ling Shan[2]

[1] Department of Information Management, National Central University
[2] Information & Communication Security Lab., Chunghwa Telecommunication Labs
{964403007,cym}@cc.ncu.edu.tw, shanhl@cht.com.tw

**Abstract.** In Vehicular Networks, for enhancing driving safety as well as supporting other applications, vehicles periodically broadcast safety messages with their precise position information to neighbors. However, these broadcast messages make it easy to track specific vehicles and will likely lead to compromise of personal privacy. Unfortunately, current location privacy enhancement methodologies in VANET, including Pseudonymization, K-anonymity, Random silent period, Mix-zones and path confusion, all suffer some shortcomings. In this paper, we propose a RSSI (Received Signal Strength Indicator)-based user centric anonymization model, which can significantly enhance the location privacy and at the same time ensure traffic safety. Simulations are performed to show the advantages of the proposed method. In comparison with traditional random silent period method, our method can increase at least 47% of anonymity in both simple and correlation tracking.

**Keywords:** VANET, Location Privacy, Tracking, Anonymity.

## 1 Introduction

Nowadays, more and more vehicles are equipped with navigation systems that can provide drivers with the directions to the destination. To fulfill their safety functions, many safety-related applications require that the vehicles broadcast their current position, speed, and direction periodically. Because these safety messages are broadcasted wirelessly in plaintext for safety applications, they are vulnerable to eavesdropping, and the location information of the vehicles can then be extracted from either position related data or identification related data. Therefore, although the broadcast safety messages could in principle improve driving safety, unauthorized parties or attackers may exploit the vulnerabilities of these VANET application systems and compromise the location privacy of the interested vehicles [1].

To solve the problem mentioned above, the authors in [2-5] proposed schemes to remove the correlation between locations and identifiers by periodically or randomly updating vehicles' pseudo identifiers. Although these methods could make vehicles unidentifiable within an anonymity set in motionless states, it can still be traced by movement tracking [6]. Furthermore, the locations visited by the vehicles can be associated with the places of interests [7] by firstly accumulating the driving paths, then by cross-referencing the accumulation results with geographical maps or other

Q. Gu, W. Zang, and M. Yu (Eds.): SEWCN 2009, LNICST 42, pp. 39–51, 2010.

location based services. Existing methodologies to enhance location privacy can be classified into several categories: *k*-anonymity [8-10], path confusion [11, 12], and Mix-Zones [13, 14]. These approaches are either of the type of centralized or partially centralized control and present two obvious drawbacks. One is the system bottleneck, the other is the potential privacy breach when the centralized control node is compromised [15].

In this paper, we propose a user-centric RSSI-based anonymity (R-Anonymity) model which can overcome the shortcomings of the previous approaches. In the aspect of adversary model, we focus on studying privacy protection of the vehicle operators under global passive adversary (GPA), which can locate and track any vehicle in a region-of-interest by eavesdropping (or intercepting) the broadcast message and utilize the adversarial RSUs deployed to estimate the locations of all broadcast message in the region-of-interest.

The rest of this paper is organized as follows. Section 2 describes the related work about location privacy enhancement. Section 3 depicts the proposed methodology of four R-Anonymity models and the anonymity algorithm. Section 4 describes how to evaluate the privacy enhancement of the proposed methodology. Section 5 discusses the simulation results of the proposed anonymity models and Section 6 presents our conclusions and future work.

## 2 Related Work

### 2.1 Identity-Based Anonymity

The idea of Identity-based anonymity approaches is to make vehicles not identifiable. According to Rongxing [1], there are two basic models for identity-based anonymity approaches: one is huge anonymous keys based(HAB), the other is group signature technique based (GSB).

In HAB [2], on board unit(OBU) stores a lot of anonymous keys, which are signed by CAs and used to sign safety messages. By changing the signing key constantly, it becomes harder to track the vehicles. The main advantage of HAB is its simplicity and straightforwardness. However it has some problems: one of these problems is that OBU needs a large storage space for the anonymous keys; another is that the key management will become a problem. Besides, processing a long list of certificate revocation list (CRL) will take a long time. In GSB [1, 16], the key idea is to allow a group member to sign messages anonymously on behalf of the group. The advantages of GSB are twofold: it reduces the number of anonymous keys and it has a shorter revocation list. But the verification time of safety messages will grow linearly with the number of revoked identities in the revocation list [1].

By incorporating HAB and GSB approaches, Calandriello [5] proposed a hybrid scheme. In this scheme, each vehicle is equipped with a group signing key and a group public key. A vehicle generates its own set of anonymous keys off line. These keys are signed by the vehicle's own private key, the latter is signed by CA to guarantee its validation. With this method, the anonymous keys of the vehicle can be generated on-the-fly and self-certified. In [17], Armknecht also proposed a similar mechanism called PKI+, which has the advantages of traditional HAB methods, but has a smaller size of CRL.

In summary, use of above methods can provide the confidentiality and integrity of messages, but as long as the vehicles need to broadcast messages periodically for the safety sake, they are still identifiable by movement tracking and profile identification of vehicle information. Hence, HAB and GSB are still unable to completely ensure the unlinkability of vehicle movement [9, 18].

### 2.2 Location and Attributes Based Anonymity

**Full Trust Centralized Third Party**

In [9], by use of a centralized third party, Shin proposed a profile based *k*-anonymization model to guarantee anonymity even when profiles of mobile users are known to an adversary. Vehicle privacy can be achieved by a sufficiently large k-anonymous dataset. However, the fully centralized trusted third party could become a system bottleneck or the single point of failure. Furthermore, this may lead to a serious privacy threat when the third party is attacked [15].

Path confusion uses a time-to-confusion approach to enhance location privacy in location dataset. Hoh [11] proposed an uncertainty-aware path cloaking algorithm to hide location samples in a dataset. As processing delay is a significant impediment in this method, Meyerowitz [12] tries to resolve it by predicting which intersection the users will pass through, and proactively retrieve data of the user's locations.

**Partial Trust Centralized Third Party**

In partial trust centralized model, vehicles could be in cooperation with road side unit (RSU) to provide location privacy without a centralized service provider. Freudiger [14] proposed a mix-zones model to enhance the location privacy. All legitimate vehicles within a mix-zone obtain a symmetric key from the RSU of that mix-zone. When a vehicle enters a RSU's mix-zone and stays within it, it uses the key provided by the RSU to encrypt all messages. However, in this scheme, there is a traffic safety concern: when vehicles come nearby a mix-zone but not yet enter the zone, it will not be able to detect its potential collision with other vehicles for lacking the encryption key of RSU.

**User Centric**

With user centric anonymity method, vehicles in the vehicular network are able to independently determine when and where to protect their privacy. In [19], Tang proposed a scheme called P-SRLD, which determines the relative locations of surrounding wireless connected vehicles and uses cryptographic keys to authenticate and protect driver's privacy. However, without GPS or accurate position information, his scheme does not seem to be applicable to all kinds of safety applications.

In [20], the authors propose a random silent period and swap identifiers for the two nearest vehicles. In addition to random silent period, Sampigethaya [7, 21] also proposes a group communication scheme in VANET. The scheme in [15] can also enhance privacy by using group communication. In this scheme, when a node wants to query the location-based database server through a base station, it will give a list of candidate queries that includes the actual ones and some false ones. The advantages

of this method are flexibility and the property of being distributive, as in a peer-to-peer system, there is no need to have a trusted third party to store the vehicles' information. However, this method also has some drawbacks. For example, there are too many broadcast messages over the same channel which will likely cause communication jam. A more serious drawback is that keeping silent in a long time will bring about traffic mishap, especially in highways.

In next section, we propose a RSSI based anonymity method, which cannot only mitigate unauthorized location tracking but also take the vehicle safety into account.

## 3 Methodology

### 3.1 Assumptions

In order to make the proposed method work properly, we make the following assumptions.

- All of the vehicles are equipped with a GPS navigation system.
- A public key infrastructure is available in the vehicular network.
- Pseudonyms have a short validity period and cannot be reused.
- Vehicles periodically broadcast their positions, velocities and directions to the network for the sake of safety and they record these data in their individual Event Data Recorder (EDR).
- There exist fully trustworthy third parties, which conform to privacy policies and keep track of the mapping between the pseudonyms and the corresponding driver's real identity.

### 3.2 R-Anonymity Model

The basic idea of R-Anonymity model is to use a distance metric method to preserve the location privacy while maintaining the traffic safety. The privacy is preserved by selectively disturbing the real values (based on the risk level) of vehicles positions, directions, and velocities. These disturbed data will prevent the adversary from precisely tracking a targeted vehicle.

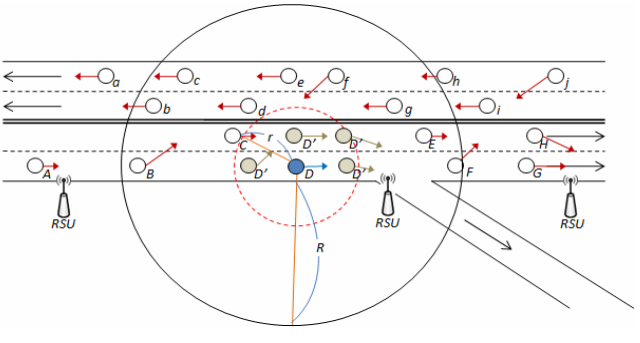



**Fig. 1.** Illustration of R-Anonymity model in pseudo position, direction and velocity

Take Fig. 1. as an example, the wireless transmission diameter of vehicle *D* is *R* and the vehicle *C* is the nearest vehicle to *D* with distance *r*. The proposed pseudo position *D'* will be broadcasted instead of *D*, where *D'* is within the circle centered at *D* with diameter *r*. The value of *D'* is chosen in a way that the pseudo position will not affect the traffic safety. It is clear that the longer the distance of the nearest vehicle, the larger range of variation of pseudo positions we could use. Consequently, as we make it more difficult for the adversary to track the correct position, we can increase the location privacy of vehicle *D*.

**Radio Signal Strength Indication (RSSI)**

The method of received signal strength indication (RSSI) is most widely known for providing a low-cost estimation of distance between vehicles [22-24]. The benefit of RSSI method is that its implementation does not require any specialized hardware. It has been used by many user location tracking applications [25-27] with an estimation error as low as 4.1m [28]. As we need a parameter to be used as a seed and a simple and fast equation to guarantee the anonymity of VANET, therefore in this paper, we leverage the RSSI to propose a user centric anonymity model, which we call R-Anonymity. Because the vehicles are in the driving mode, their moving direction, velocity and acceleration vary, hence the strengths of received signals of the vehicle are changing constantly.

$$RSSI_{ij} = -(10n \log_{10} d_{ij} + A) \tag{1}$$

In the Equation (1), $RSSI_{ij}$ indicates the radio strength from node *i* to node *j*, where *i* is the node of transmitter, *j* is the receiver, *n* is the path loss exponent depending on each network characteristics, $d_{ij}$ is the distance from *i* to *j*, and *A* is the received signal strength at 1 meter distance. For different vendor, the range of value of RSSI is defined differently. For example, Cisco uses a range of 0~100 in their devices, while Atheros-based chipsets use a range of 0~60. In this paper, we will normalize the RSSI indicators to be from 0 to 1.

As $RSSI_{max}$ can be used to represent the distance between the tracked vehicle and its nearest vehicle, we use it to compute a pseudo value to be used in R-Anonymity model. That is, the computation of pseudo value depends on the value of $RSSI_{max}$. The radio strength is reversely proportional to the distance difference between the real value and the pseudo value, which means that when the radio strength is low, there is no vehicle close to the tracked vehicle. Hence we can generate the pseudo value with larger difference to real position to keep this vehicle hard to be tracked.

$$R_d = X \times 10^{-(RSSI_{\max}+A)/10n} / C_R \quad , -1 \le X \le 1 \tag{2}$$

In Equation (2), $R_d$ is the tolerable distance ratio with respect to current $RSSI_{max}$ value, *X* is a random value between -1 to 1, and $C_R$ is the maximum transmission range of a VANET device. With the computation of $R_d$, we can provide four kinds of privacy enhancement: pseudo position, pseudo direction, pseudo velocity and pseudo random silent period, named respectively R-Pseudo position, R-Pseudo direction, R-Pseudo velocity and R-Random silent period.

**R-Pseudo Position**

Equation (3) shows how to generate a pseudo vehicle position value to avoid being tracked by adversaries. Here $(x_r, y_r)$ represents the original position of the tracked vehicle, $d$ is a constant (not greater than transmission radius) chosen to generate acceptable pseudo position.

$$(x_p, y_p) = (x_r + d \times R_d \ , \ y_r + d \times R_d) \tag{3}$$

**R-Pseudo direction**

In addition to vehicle's position, vehicle's driving direction should also be taken into consideration in order to reduce the risk of being tracked. This is because, if we just generate pseudo positions, adversaries can still make use of vehicle driving direction to filter the candidate vehicles and increase the probability of successful tracking.

$$D_p = D_r + C_d \times R_d \tag{4}$$

Equation (4) shows how to generate R-Pseudo direction, where $D_r$ is the original drive direction of the node, $C_d$ is the constant of maximum differential direction, and $C_d$ is 30 degrees for change lane.

**R-Pseudo velocity**

For the similar reason as in above, vehicle velocity is also an important attribute to be considered. Equation (5) shows how to generate pseudo velocity to confuse the adversaries.

$$V_p = V_r + C_v \times R_d \tag{5}$$

In Equation (5), $V_r$ is the original driving velocity of the tracked vehicle, and $C_v$ is the maximum allowable velocity difference between real and pseudo velocity. In this paper, $C_v$ is less than 5 m/sec (18 km/hr).

**R-Random silent period**

By altering broadcast interval, random silent period (RSP) becomes a useful method to enhance location privacy[6, 7, 20]. However, when the vehicles are close to each other, indiscriminately following random silent period rules may result in vehicle collision. To address this issue, we propose a RSSI based random silent period method. In this method, the closer distance between the vehicles, the shorter the random silent period.

$$SP_p = SP_{\min} + (SP_{\max} - SP_{\min}) \times R_d \tag{6}$$

In Equation (6), the $SP_{min}$ is the minimum silent period, and $SP_{max}$ is the maximum silent period.

In order to keep safety, when a vehicle detects that the distance of the nearest vehicle is less than $C_n$, the broadcast messages of this vehicle will not apply the R-Anonymity model, so as to avoid possible vehicle collisions. In addition, after we apply the R-Anonymity model to obtain pseudo position, the new position might be out of the road. In order to solve this problem, we use map matching [29] to verify the pseudo position value. If the coordinates of the vehicle indicate that the pseudo

position is outside of the road, the algorithm will regenerate new one and verify again, until the coordinates fall within the road.

# 4 Evaluation

In order to evaluate the location privacy and compare our model with other models, we first define a reachable area, $A_r$, to represent the next possible positions of a vehicle based on current moving directions, velocity and silent period. Then we use both simple and correlation tracking methods [7] to measure the anonymity of the tracked vehicles. The anonymity of a vehicle is determined by its anonymity set, where the latter is defined as vehicles locating within the reachable area of the tracked vehicles, but is indistinguishable from each other.

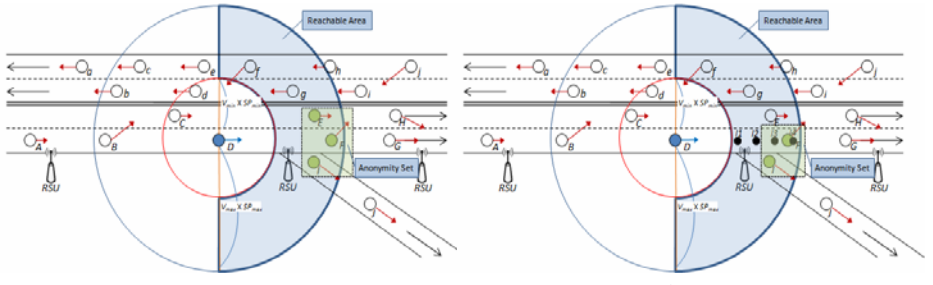
## 4.1 Tracking of Vehicles

**Simple Tracking**

With the simple tracking, it is assumed that each vehicle in the anonymity set has the same probability to be tracked vehicle. The on-coming vehicle in the reachable area is filtered according to the driving direction of vehicle. Fig.2 (a) is an example of simple tracking, in which we find vehicles {*f, g, E, F, I*} are in the reachable area. But as vehicles {*f, g*} are on-coming vehicles, they are filtered out of the anonymity set. Therefore, the result of the anonymity set by simple tracking is {*E, F, I*}.

Equations (7) are the tracking criteria for simple tracking, where $V_{min}$ ($V_{max}$) is the minimum (maximum) velocity of this vehicle; $SP_{min}$ ($SP_{max}$) is the minimum (maximum) silent period. Let ($x_i$, $y_i$) be the location of tracked vehicle; ($x_j$, $y_j$) be a vehicle in the transmission area. Equation (7a) is use to determine whether vehicle $j$ is within the transmission area of vehicle $i$.; Equation (7b) is used to determine whether vehicle $i$ and $j$ are in the same driving direction.

$$\begin{cases} V_{\min} \times SP_{\min} \le \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \le V_{\max} \times SP_{\max} & \forall j \in \{A_t\} \quad (7a) \\ \left| \arctan 2\left( {}^{(x-x_j)}/_{(y-y_j)} \right) \right| \le {}^{\pi}/_{2} & (7b) \end{cases}$$




(a) (b)

**Fig. 2.** (a) Simple Tracking of vehicles (b) Correlation Tracking of vehicles

**Correlation Tracking**

With the correlation tracking, the adversary will estimate locations of the tracked vehicle in the reachable area constantly, and then select the closest vehicle in the reachable area. The number of vehicles selected by the correlation tracking is less or equal to that selected by simple tracking. Fig.2 (b) is an example of correlation tracking, by the estimated location of tracked vehicle *D* in different time points from $l_1$ to $l_4$. As *E* is not the nearest vehicle to $l_1$, $l_2$, $l_3$, $l_4$, compared with *I* and *F*, vehicle *E* will be filtered out, and the result of anonymity set found by correlation tracking is {*F, I*}.

Equations (8) are the tracking criteria for correlation tracking, where $(x_t, y_t)$ is the estimate positions in time *t*, time t is between $SP_{min}$ and $SP_{max}$, $V_s$ is the vehicle velocity between $V_{min}$ and $V_{max}$,θis driving direction of the tracked vehicle, and $l_{est}$ is the nearest vehicle in the reachable area $A_r$ comparing with estimation positions.

$$\begin{cases} (x_t, y_t) = (x + t \times V_s \times \cos\theta,\ y + t \times V_s \times \sin\theta) \\ l_{est} = Min\ (\sqrt{(x_t - x_j)^2 + (y_t - y_j)^2}) \quad \forall j \in \{A_r\} \\ SP_{min} \le \mathrm{t} \le SP_{max} \\ V_{min} \le V_s \le V_{max} \end{cases} \tag{8}$$

## 4.2 Evaluation of Anonymity

Entropy of the vehicle distribution in the anonymity set is the most popular method to evaluate the level of anonymity [7, 14]. Equation (9) is used to measure the entropy. It is assumed that the elements of the anonymity set have a uniform distribution [30]. In Equation (9), $P_i$ is the probability of vehicle *i* to be selected to track, $S_A$ is the anonymity set of vehicles, and $|S_A|$ is the number of vehicles in the anonymity set. When H(*p*)=0, it means that the tracked vehicle could not provide any anonymity set and it is easy to be tracked. The higher the value of H(*p*), the higher the location anonymity.

$$H(p) = -\sum_{i=1}^{|S_A|} P_i \log_2 P_i\ ,\ \sum_{i=1}^{|S_A|} P_i = 1 \tag{9}$$

For a given time *t*, if there is no vehicle found during t+ $SP_{min}$ and t+ $SP_{max}$, it means that the tracking fails under simple or correlation tracking. This emptiness of the anonymity set makes the entropy value to become infinite. In order to resolve the infinite entropy problem, when the size of anonymity set is zero under both simple and correlation tracking, we change from the anonymity set of reachable area to the anonymity set of coverage area $A_c$.

Equation (10) is the criteria to get the anonymity set in the coverage area $A_c$, where $(x_j, y_j)$ represents the positions of vehicles *j* in the transmission area $(A_t)$, and $(x_r, y_r)$ is the real position of the tracked vehicle.

$$\begin{cases} \sqrt{(x - x_j)^2 + (y - y_j)^2} \le \sqrt{(x - x_r)^2 + (y - y_r)^2} \\ \left|\arctan 2(^{(x-x_j)}/_{(y-y_j)})\right| \le \pi/2 \end{cases} \quad \forall j \in \{A_t\} \tag{10}$$

$$H(p) = \log_2(|S_A|) \tag{11}$$

The number of vehicles in the coverage area of a specific vehicle is always greater or equal to 1 (this vehicle itself). Therefore, new entropy value of anonymity set (see Equation (11)) will never be infinite.

### 4.3 Simulation

In order to evaluate the RSSI based location privacy method, we simulate the vehicular network with two types of topology: grid and cobweb. Grid topology is a 2x2 grid, whose total length is 2196 meters with 9 intersections. Cobweb topology is a 2-circle cobweb topology with the total length of 7566 meters and 27 intersections.

We use the SUMO [31] to generate the topology of maps and use TraNS [32] to leverage the NS2 to simulate the movement of vehicles. In order to observe the effectiveness of different density of vehicles on the roads to our method, for each topology, the number of vehicles entering the topology is from 50 to 700 nodes per seconds. After NS2 finished, we import the output file of NS2 trace file to Matlab and compute the entropy in different fixed/random silent period and R-random silent period.

## 5 Simulation Result

In our experiments, we simulate both grid and cobweb topologies with two lanes and two drive directions. It is assumed that the maximum message transmission radius is 100 m, and the simulation is done with the range of fixed silent period from 300 to 900 ms and with random/R-random silent period from 1 to 3 seconds.

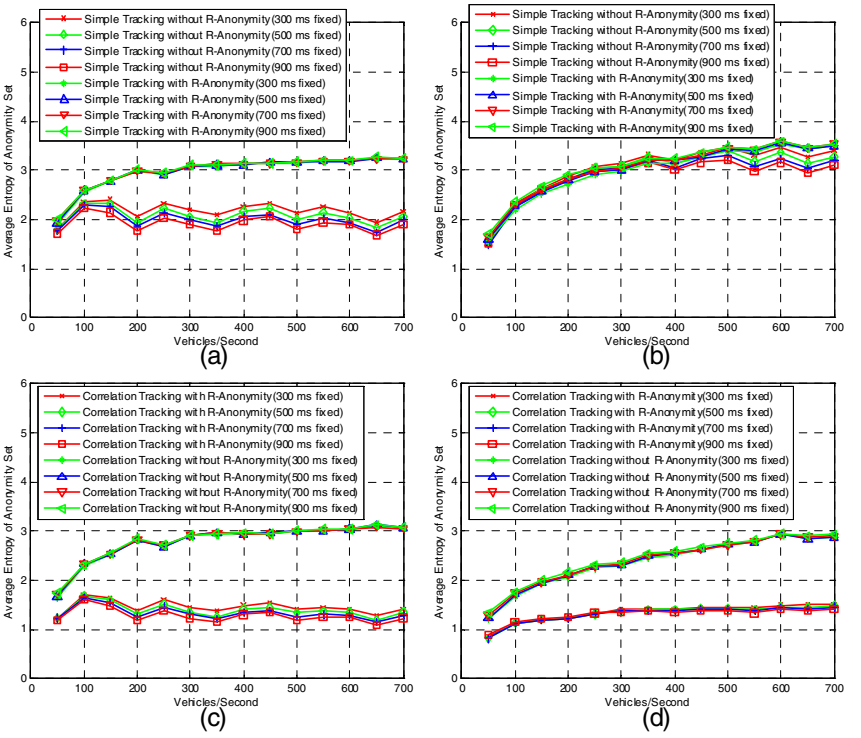



**Fig. 3.** Vehicle tracking to fixed silent period from 300 ms to 900 ms (a) Grid topology with simple tracking (b) Cobweb topology with simple tracking (c) Grid topology with correlation tracking (d) Cobweb topology with correlation tracking

The experimental results of fixed silent period are shown in Fig.3. The level of anonymity increases with the number of vehicles per second in the road under simple tracking. After R-Pseudo is applied in position, direction and velocity to produce interference in the simple tracking in grid topology (shown in Fig.3 (a)) and cobweb topology (shown in Fig.3 (b)), we observe that the resulting entropies in cobweb topology are higher than those in the grid topology. This is because that the number of intersections of cobweb topology is greater than that of the grid topology, which increases the difficulties of simple tracking. The entropy in the cobweb topology is relatively high so that the improvement of location privacy by R-pseudo position, direction and velocity seems less obvious.

Fig.3 (c) and (d) show the correlation tracking results of fixed silent period. From these two figures, we can find that the differences of the result in both two types of topologies are not significant in correlation tracking. It follows that the correlation tracking has higher tracking capability than simple tracking. The experimental results in both topologies with correlation tracking show that by adopting R-Pseudo method the entropy can be increased substantially.

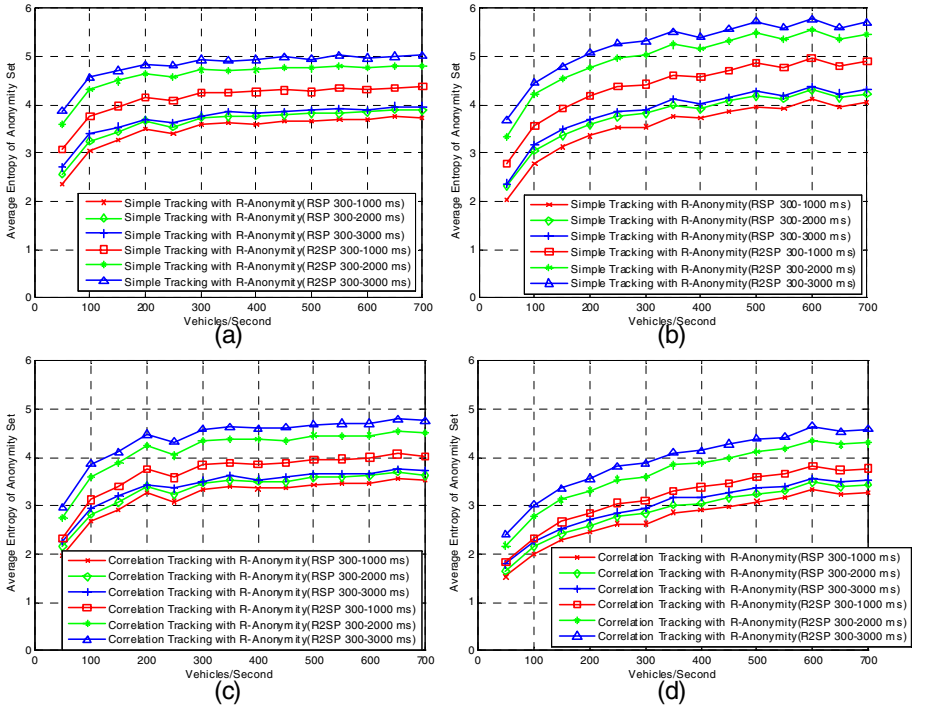



**Fig. 4.** Vehicle tracking to random and R-random silent period from 300ms to 3000ms (a) Grid topology with simple tracking (b) Cobweb topology with simple tracking (c) Grid topology with correlation tracking (d) Cobweb topology with correlation tracking

In regard to simple tracking and correlation tracking, Fig.4. shows that after applying R-Pseudo position, direction and velocity methods and pseudo random silent period, we can improve the anonymity under various conditions. In Fig.4 (c) and (d), the average entropy under correlation tracking is 3.46. Compared with Fig.3 (c) and (d), the overall difference of entropy between our R-pseudo method and pure correlation tracking method in Fig.4 (c) and (d) is greater than 1.91, which is quite significant. We may, therefore, conclude that the vehicular network applying R-Anonymity model can greatly enhance the location privacy and prevent vehicle from being tracked in this simulation.

## 6 Conclusion and Future Work

In this paper, an R-Anonymity model is proposed to cope with location privacy threats in vehicular networks. It is user centric, namely it is without the need of a centralized trusted party. Furthermore, it is simple to implement because it is easy to sample RSSI from the air. Applying R-Anonymity in vehicular networks can actually provide sufficient unlinkability to protect location privacy.

We simulate our R-Anonymity model with two kinds of topology and fourteen sets of network parameters. Simulations manifest that R-Anonymity model can obtain better results than traditional fixed and random silent periods. The results also show that by merely applying either one of R-Pseudo position, velocity, direction or R-Random silent period, the entropy value becomes relatively low, which means that the vehicles are easy to be tracked in some cases. By combining all of the above, we can provide better location privacy than the traditional methods do.

In the future, we intend to evaluate the proposed model by simulation based on the real map integrated with traffic signs. Another interesting future research direction is to address the relation between location privacy and road traffic safety by measuring the RSSI value in various conditions.

## References

1. Lu, R., Lin, X., Zhu, H., Ho, P., Shen, X.: ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. In: INFOCOM 2008. The 27th Conference on Computer Communications, pp. 1229–1237. IEEE, Los Alamitos (2008)
2. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security 15, 39–68 (2007)
3. Dötzer, F.: Privacy Issues in Vehicular Ad Hoc Networks. Privacy Enhancing Technologies, pp. 197–209 (2006)
4. Gerlach, M., Guttler, F.: Privacy in VANETs using Changing Pseudonyms-Ideal and Real. In: IEEE 65th Vehicular Technology Conference, 2007. VTC 2007, pp. 2521–2525 (Spring 2007)
5. Calandriello, G., Hubaux, J., Lioy, A.: Efficient and robust pseudonymous authentication in VANET. In: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19–28 (2007)

6. Huang, L., Matsuura, K., Yamane, H., Sezaki, K.: Towards modeling wireless location privacy. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 59–77. Springer, Heidelberg (2006)
7. Sampigethaya, K., Li, M.Y., Huang, L.P., Poovendran, R.: AMOEBA: Robust location privacy scheme for VANET. IEEE Journal on Selected Areas in Communications 25, 1569–1589 (2007)
8. Gruteser, M., Grunwald, D.: Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services, pp. 31–42 (2003)
9. Shin, H., Atluri, V., Vaidya, J.: A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment. In: 9th International Conference on Mobile Data Management, 2008. MDM 2008, pp. 73–80 (2008)
10. Gedik, B., Liu, L.: A Customizable k-Anonymity Model for Protecting Location Privacy. Georgia Institute of Technology (2004)
11. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Preserving privacy in GPS traces via uncertainty-aware path cloaking. In: Proceedings of the 14th ACM conference on Computer and communications security, pp. 161–171 (2007)
12. Meyerowitz, J.T., Choudhury, R.R.: Realtime location privacy via mobility prediction: creating confusion at crossroads. In: Proceedings of the 10th workshop on Mobile Computing Systems and Applications. ACM, Santa Cruz (2009)
13. Beresford, A., Stajano, F.: Mix zones: User privacy in location-aware services. In: Proceedings of First IEEE International Workshop on Pervasive Computing and Communication Security, PerSec (2004)
14. Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., Hubaux, J.P.: Mix-Zones for Location Privacy in Vehicular Networks (2007)
15. Chow, C., Mokbel, M., Liu, X.: A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems, pp. 171–178 (2006)
16. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. IEEE Transactions on Vehicular Technology 56, 3442–3456 (2007)
17. Armknecht, F., Festag, A., Westhoff, D., Zeng, K.: Cross-layer privacy enhancement and non-repudiation in vehicular communication. In: 4th Workshop on Mobile Ad-Hoc Networks (WMAN) (March 2007)
18. Huang, L., Matsuura, K., Yamane, H., Sezaki, K., Japan, N.R.C., Tokyo, J.: Enhancing wireless location privacy using silent period. In: 2005 IEEE Conference on Wireless Communications and Networking, vol. 2 (2005)
19. Tang, L., Hong, X., Bradford, P.G.: Privacy-preserving secure relative localization in vehicular networks. Security and Communication Networks 1, 195–204 (2008)
20. Li, M., Sampigethaya, K., Huang, L., Poovendran, R.: Swing & swap: user-centric approaches towards maximizing location privacy. In: Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 19–28 (2006)
21. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: CARAVAN: providing location privacy for VANET. In: Proceedings of Embedded Security in Cars, ESCAR (2005)
22. Choi, W., Nam, J., Choi, S.: Hop State Prediction Method Using Distance Differential of RSSI on VANET, vol. 1 (2008)

23. Bouassida, M., Guette, G., Shawky, M., Ducourthial, B.: Sybil Nodes Detection Based on Received Signal Strength Variations within VANET. International Journal of Network Security 9, 12 (2009)
24. Bin, X., Bo, Y., Chuanshan, G.: Detection and localization of sybil nodes in VANETs. In: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks. ACM, Los Angeles (2006)
25. Lau, E.E.L., Chung, W.Y.: Enhanced RSSI-Based Real-Time User Location Tracking System for Indoor and Outdoor Environments, pp. 1213–1218 (2007)
26. Choi, W.S., Nam, J.W., Choi, S.G.: Hop State Prediction Method Using Distance Differential of RSSI on VANET, vol. 1 (2008)
27. Saxena, M., Gupta, P., Jain, B.N.: Experimental analysis of RSSI-based location estimation in wireless sensor networks, pp. 503–510 (2008)
28. Whitehouse, K., Karlof, C., Culler, D.: A practical evaluation of radio signal strength for ranging-based localization (2007)
29. Jagadeesh, G.R., Srikanthan, T., Zhang, X.D.: A Map Matching Method for GPS Based Real-Time Vehicle Location. Journal of Navigation 57, 429–440 (2004)
30. Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Dingledine, R., Syverson, P.F. (eds.) PET 2002. LNCS, vol. 2482, pp. 41–53. Springer, Heidelberg (2003)
31. SUMO: Simulation of Urban Mobility, `http://sumo.sourceforge.net/`
32. Trans: Traffic and Network Simulation Environment, `http://trans.epfl.ch/`