# EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks

Messaoud Babaghayou[1][0000−0001−9508−7134], Nabila Labraoui[1][0000−0002−5135−8972], and Ado Adamou Abba Ari[2,3][0000−0001−5660−0660]

[1] STIC Lab, Abou Bakr Belkaid University of Tlemcen, P.O. Box 230, chetouane Tlemcen 13000, Algeria
babaghayoumessaoud@hotmail.com, nabila.labraoui@mail.univ-tlemcen.dz
[2] LaRI Lab, University of Maroua, P.O. Box 814 Maroua, Cameroon
adoadamou.abbaari@gmail.com
[3] LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, 45 Avenue des États-Unis 78035 Versailles cedex, France

**Abstract.** The main purpose of designing Vehicular Ad-hoc Networks (VANETs) is to achieve safety by periodically broadcasting the vehicle's coordinates with a high precision. This advantage brings a threat represented in the possible tracking and identification of the vehicles. A possible solution is to use pseudonyms instead of real identities. However, even by changing pseudonyms, the vehicle can still be tracked if the adversary has knowledge about the potential start and end points of a particular driver who has social interactions (e.g., with neighbors) which introduces the concept of Vehicular Social Networks (VSNs). In this work we propose a location privacy scheme, namely: Extreme Points Privacy (EPP) for trips and home identification in VSNs by exploiting the nature of the end points that are common between many VSN users bringing the option to create shared zones to anonymize these users. An analytical study accompanied by a simulation using the realistic vehicular traffic mobility generator SUMO are presented to show the effectiveness of the proposed scheme.

**Keywords:** Location Privacy · Anonymity · Home Identification.

## 1 Introduction

The humain behaviour and social interactions were almost apparent in drivers moving patterns which lead to the emergence of VSNs. The evolution and enhancement of VANET capabilities have significant influence on the successfulness of the Intelligent Transportation Systems (ITSs) [1, 2]. In VANETs, there exist two kinds of communications: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). In order to be able to communicate, vehicles are equipped with On Board Units (OBUs); specific devices that allow vehicles to: communicate,

process date, receive GPS signal and use variant sensors. Vehicles may often communicate with central infrastructures. Such infrastructures may be Road Side Units (RSUs) [4]. VANET applications may be diverse; however, the number one reason for what it was proposed is to reduce the number of crashes and fatalities [4] by enabling periodic broadcasts (also called beacons or heartbeat messages). This requires the vehicle to include its status in kind of location, speed, velocity and other information that allow a better environment knowledge like Basic Safety Messages (BSMs). The standard SAE J2735 sets the frequency of BSMs to be each 100ms with a 300 meter transmission range radius [5].
The frequent and precise location provided by BSMs helps enormously the safety-related applications but, at the same time, reduces dramatically the privacy of VSN users since the BSMs location is not encrypted for fast reaction and less delay. Thus, any adversary willing to monitor the VSN users can do that in real time with just some eavesdropping station(s). Among the possible solution there exist: the use and the change of pseudonyms instead of one real identity, the cooperation of vehicles during the pseudonym change, the use of silent periods [6] and other techniques that will be seen in the next section.
In this paper, we demonstrate the model of EPP by giving an analytical study for the privacy level achieved by the VSN users of a particular district taking into account the number of gates and the possible headings from each gate; the definition of the above concepts will be further explained. This analytical study is accompanied by simulations in order to evaluate the effectiveness of EPP scheme. The rest of this paper is organized as follows. Sect. 2 presents some related works. In Sect. 3, we describe the proposed EPP strategy. The experimental results are presented in Sect. 4 and we conclude the paper in Sect. 5.

## 2 Related Works

In what follows we briefly describe some of the potential solutions to defend against location privacy and identification: (1) Hiding the location: It is described as turning the radio off so that the vehicle does not expose itself and be located. This solution negatively affects security and entertainment services since the vehicle cannot communicate while it is silent.(2) Obfuscating the location: It aims at letting the VSN users be anonymous while using the Location Based Services (LBSs). Using LBSs require sending queries with the location of the VSN user. It consists of send a non-precise location to the LBS thus the VSN users cannot be easily re-identified. The user can still be identified by isolation [7].(3) Anonymization: The VSN users trend toward using anonymizers such as proxies. The goal is to hide their identity while using the different services. Anonymization adds additional latency and overhead.(4) Making dummies (or dummifying as called in [7]): Aims at using fake locations in addition to the correct one in order to let the adversary be confused. Sending false locations is absolutly dangerous in VANETs (sybil attacks [4]).

The problem of location tracking and re-identification of VANET users was studied delicately in a lot of works. In [4], the CARAVAN scheme was proposed which consists of changing pseudonyms over time by combining the silent period and the group concepts. The authors in [8] namely swing & swap used the pseudonym change after ensuring the increase of the neighbors(swing), swap aims at letting vehicles exchange their pseudonyms instead of a normal change. The exchange of pseudonyms enhances privacy but it highly relies on the infrastructures for the accountability requirement. In CMIX [9] the vehicles are supposed to change their pseudonyms at mix-zones [10] (e.g. the intersections, at traffic lights, etc.) in addition of the encryption of safety messages once the vehicle enters the mix-zone. Density-based location privacy (DLP) [11] scheme uses the neighborhood number as a parameter to decide whether to change the pseudonym or not. Pseudonym change at social spot (PCS) [1] was proposed to let vehicles change their pseudonyms at dense places such as intersections or parking lots. However, the map does not always have such places. To better-choose the moment of the pseudonym change, cooperative pseudonym change (CPN) [12] was proposed. CPN uses different triggers in order to achieve a high level of privacy. The neighbors' number is one of these triggers. In [5], Endpoit Protec-tion Zone (EPZ) deals effectively with the location privacy in the domain of LBSs where users query the appropriate LBS. Authors suggested that the users have to be grouped spatially and have to use the same login credentials in addition to keep silent until leaving the EPZ. The scenario of the colluding between an LBS and an RSU dishonest owners is also investigated. EPZ deals mainly with the problem of dishonest LBS owners. In our work we give more attention to the scenario of a dishonest RSU owner or a potential external eavesdropper who may attempt to monitor a region of interest while using backward knowledge represented in: the starting point, exiting point (called gateway here) and potential direction (called heading)at a given time. We also study the different possible scenarios (described in more details in the coming section) in order to investigate the successfulness of the adversary to determine whether his target(s) had quited or not.

## 3 The Proposed EPP Strategy

In this section we outline the principals of the proposed scheme EPP which is a zone division-based that exploits the nature of the VSNs and we give the possible behavior of any VSN user and its implications on the privacy of these users.

Since the pseudonym change strategy is not working in all scenarios, new techniques must be deployed to fill this gap. An example is when vehicles start from a predefined spot. Here, if the adversary has some knowledge (represented by social engineering), he can match the used pseudonym with the real identity of its driver whatever the strength of the deployed pseudonym change strategy is (it goes in vain). We suggest the use of the EPP scheme which is built basing on the characteristics of the end points that, in general, do belong to specific zones that have specific nature as: (1) the speeds of vehicles are low since they are in

the starting status. Also, due to the capabilities of the new generation of vehicles, (2) they provide high environment sensing and movement/objects detection by using, the distance sensors, radars, ultrasonic sensors, high definition cameras, etc. [13] letting the BSMs be an option instead of a must. By this definition and assumptions, we present the different zones and techniques used in combination with the pseudonym change strategies used for the location tracking and re-identification. The next subsection shows the zones division and elements.

### 3.1 Deployment of Zones

As shown in Figure 1.a, the map, according to EPP, is divided into: District zones, Gateway zones and the Outside Environment and are explained in details in what follows:

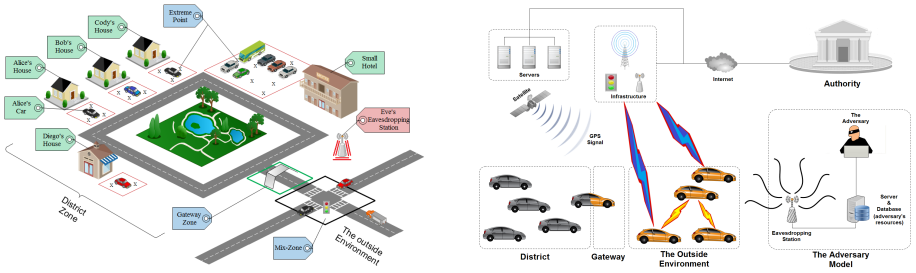
**A. District Zones:** They contain the start and end points of specific VSN users who use these points (spots) more frequently (the home for example). The nature of such zones, allows dispensing with BSMs because of the vehicle's efficiency in dealing with the environment and neighborhood vehicles. The vehicles then will be authorized to stay silent while they are inside the district zone(s) without safety dangers and threats.

**B. Gateway Zones:** Each district is attached with the outside environment. The role of gateways (GWs) is to let the outside environment vehicles know about the newly coming vehicles from the district. Now, BSMs become a must (instead of being an option in district zones). In addition, a district may have many gateways and headings (HDs). A heading is a direction that a vehicle would take once it leaves the gateway, it then determines the trip of the driver.

**C. The outside Environment:** it is the remaining part of the network in where a privacy mechanism like pseudonym change at mix-zones is used. The vehicle changes its pseudonym and may: (1) stop beaconing, e.g., uses silent periods when it enters the mix-zone, (2) change its pseudonym then (3) emerges from the outside of the mix-zone letting the adversary be confused.

### 3.2 The Privacy Mechanisms in the System

As explained in the previous subsection, a VSN user starts from the district, more precisely from his appropriate spot inside that district. We assume that the adversary is advanced, e.g., is considered as Global Passive Adversary (GPA) [3] with a backward knowledge about all VSN users inside that district. The adversary then knows about each vehicle's potential spots, exiting/entering gateway and its heading. With ordinary strategies, the adversary will know for sure about the events of: (1) quitting the home or the frequent places and (2) entering them. In EPP, VSN users are supposed to be in control of enabling and disabling the radio-silence feature which enhances and removes the inner's privacy respectively.




(a) EPP Zones division (b) Network and threat models in EPP

Fig. 1: An illustration of the proposed scheme

**Definitions and Properties**

In this part we explain the entities of the network with their definitions for better comprehension:
We first define the three possible scenarios (or vehicle classes) that may occur:

- A set of VSN users who are aware of the privacy concept. Thus, they enable the radio-silence feature to protect their privacy. The set is defined as "$X$".
- A set of VSN users who are not aware of their privacy. Thus, they disable the radio-silence feature. The reason may also be that they need to use some services which require a continuous connected. The set is defined as "$Y$".
- A set of VSN users who may not be able or cancel their appointments, works or visits for whatever reason. This kind of vehicles surprises the adversary since they act unexpectedly to his thoughts. This set is defined as "$Z$".
- The adversary is supposed to be aware of the approximate movement time of his target(s) due to the social engineering techniques (Figure 1.b). shows both of the network model and the threat model in EPP scheme.

Let the set of VSN users who belong to the district be:

$$S = \{v_1, v_2, ...v_n\} = X + Y + Z \tag{1}$$

The set of VSN users who are similar in term of gateway and heading:

$$S_{sim(i)} = \{v_j \in S : Similarity(v_i, v_j) = 1\} \tag{2}$$

The set of VSN users who are still inside the district:

$$S_{in(i)} = \{v_j \in S_{sim(i)} : State[v_j] = "Inside"\} \tag{3}$$

The set of VSN users who quitted the district:

$$S_{out(i)} = S_{sim(i)} - S_{in(i)} \tag{4}$$

The set of VSN users who quitted the district for sure in the thoughts of the adversary with a 100% of certainty:

$$S_{Clearly\_out(i)} = \{v_j \in S_{out(i)} : Class[v_j] = "Y"\} \tag{5}$$

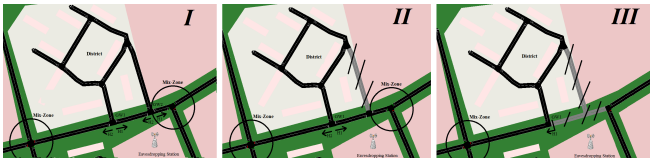



Fig. 2: The three scenarios: $I$, $II$ and $III$

by these definitions, we can formulate the adversary's probability metric to quantify the privacy of VSN users. In other words: the exact probability of quitting the district by his target which is formulated as follows:
Firstly the probability of being inside the district:

$$P_{inside}(v_i) = \begin{cases} 0 & IF(Class[v_i] = "Y")AND(State[V_i] = "Outside") \\ \frac{|S_{sim(i)}|-|S_{out(i)}|}{|S_{sim(i)}|-|S_{Clearly\_out(i)}|} & Else \end{cases} \tag{6}$$

Finaly the probability of being outside, e.g. had probability of quitting as follows:

$$P_{outside}(v_i) = 1 - P_{inside}(v_i) \tag{7}$$

## 4 Simulation Setup and Results

In this section, we evaluate the effectiveness of the proposed EPP scheme. For this aim, we consider a set of 10 VSN users of a specific district (taken from Tlemcen town, Algeria) that contains two gateways and two headings per each gateway. Our main task is to evaluate the adversary's certainty about the exiting/quitting of a target(s) ($V_i$). Each VSN user may belong to either classes ($X$, $Y$ or $Z$). The number of gateways and headings is manipulated in order to see its effect on the achieved privacy. The simulations were done by taking three scenarios (namely: $I$, $II$ and $III$). In $I$, a real district that contains two gateways and two heading per each gateway was taken. We modify this real map fragment and transform it into $II$ then $III$ (one gateway, two headings and one gateway, one heading respectively).

We use SUMO to make realistic VSN user traces. For this purpose, we generate a vehicular road traffic starting from $7:40$ until $8:15$. The reason we took this interval of time is because users often leave their homes in such a period (rush time) to either: work, study, etc. we then (via a c++ program) randomly generate our ten district vehicles' departure times, the exiting gateways and the headings. We also make four parameters per each scenario by varying the number of vehicles in each class (see Figure 3).

**The simulation runs:**
As explained before, we choose three scenarios and per each one we make four runs, we then evaluate the probability of quitting. The monitored targets are

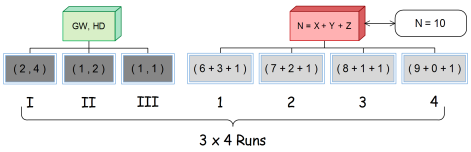
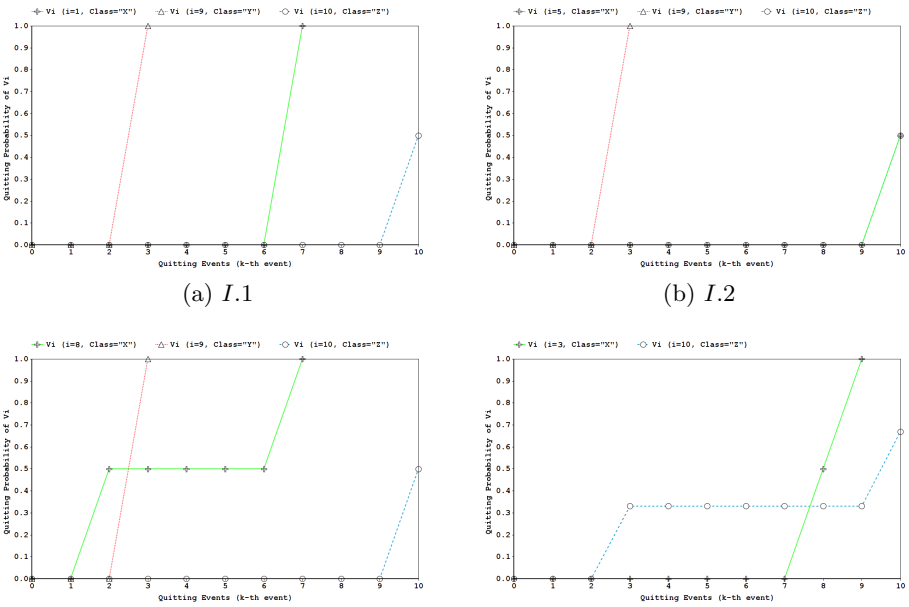



Fig. 3: The simulation runs (scenarios*4)




(a) $I.1$ (b) $I.2$

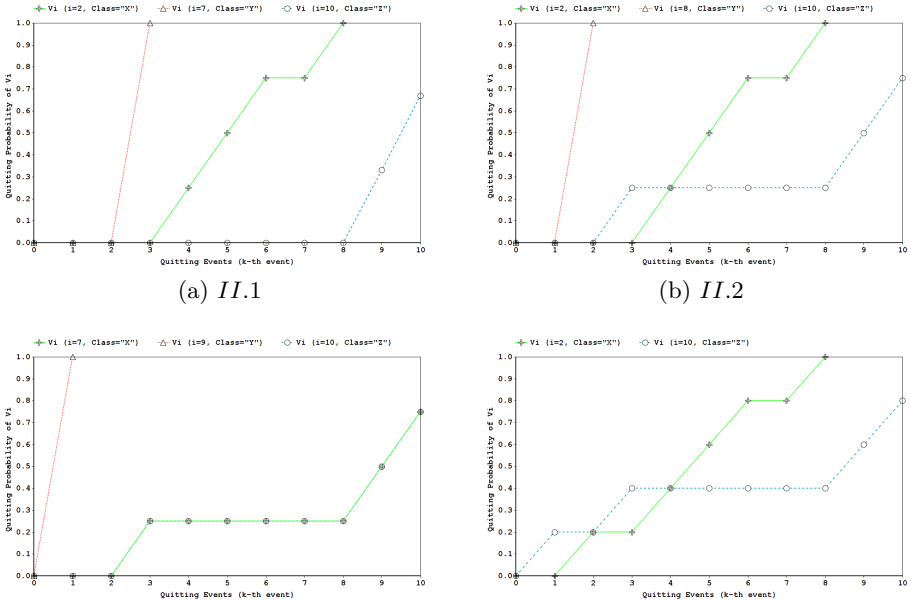
(c) $I.3$ (d) $I.4$

Fig. 4: The four simulations of scenario $I$

taken randomly from each class (i.e. from $X$, $Y$ and $Z$ which is only one since it is 10% from 10).

**Scenario $I$:** We start by the scenario of two gateways with two hidings per each. The taken Vahicles from each class are mentioned in the graphs. The obtained results are as follows:

The results in Figure 4 shows that the VSN user who does not activate/enable the privacy mechanism (class "$Y$") fails both: (a) easily and (b) faster than other classes. The next one is the class "$X$" user, because he does not expose himself by staying silent until he quits the district. However, class "$Y$" VSN users affect him by letting the adversary know about their quitting events. The last category ("$Z$") comes with the best privacy level since it does not quit the district which enhances its and others' privacy (users who share the same similarity as it). A similarity in our scheme reflect the same gateway and heading.




(a) $II.1$ (b) $II.2$

(c) $II.3$ (d) $II.4$

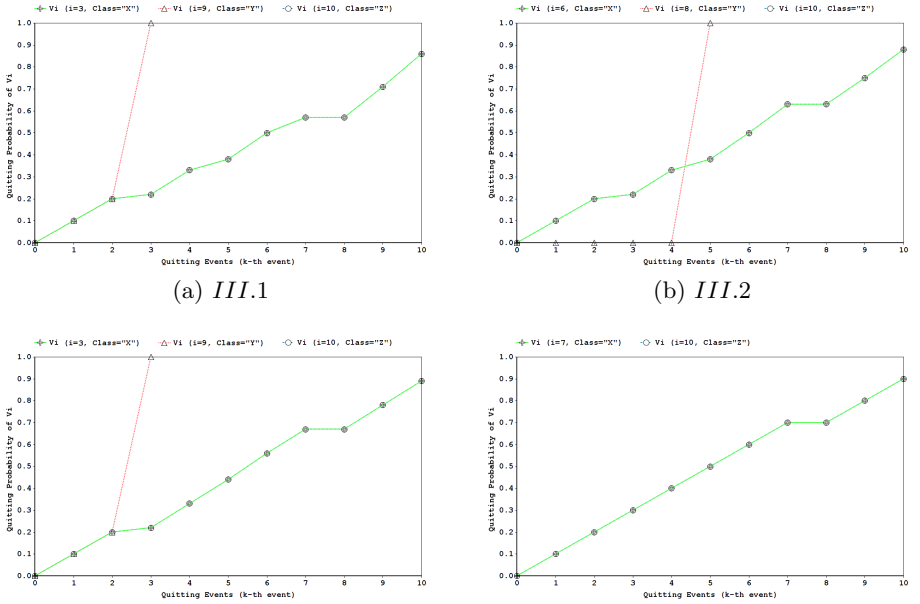
Fig. 5: The four simulations of scenario $II$

Another two observations from the four results in figure 4 indicate that (1) by reducing the number of "$Y$" users and rising the "$X$" users the overall privacy will last longer before the adversary starts identifying the quitting events of VSN users. (2) The change of quitting probability for all VSN users rises rapidly and this is due to the fact that users do not share the same gateway and heading which means that if a user quits, he may be the only user in that district who has such gateway and heading combination.

**Scenario $II$:** This scenario is formed by only one gateway and two hidings. The taken Vahicle from each class is mentioned in the graphs (as in scenario $I$). The obtained results are the followings:

The results' interpretation is almost the same as in scenario $I$ where "$Y$" users are the first to be exposed followed by the class "$X$" then lastly class "$Z$" maintains its privacy perfectly as in Figure 5. The additional observations are: (1) VSN users in $II$ stay longer before being exposed and this is because more vehicles have the same similarity since in such a scenario there is only one gateway. (2) Despite the higher identification probability compared to $I$, VSN users's probability does not change with big amount. Just when a lot of users quit, the privacy of the target will be affected.

**Scenario $III$:** This last scenario is formed by only one gateway and one hiding. The taken Vahicle from each class is mentioned in the graphs. The obtained results are represented as follows:




(a) $III.1$ (b) $III.2$

(c) $III.3$ (d) $III.4$

Fig. 6: The four simulations of scenario $III$

The VSN user in this scenario share the same characteristics as the previous two scenarios and class "$Z$" is the best in privacy preserving followed by class "$X$" then class "$Y$" comes in the last place (see Figure 6). The special characteristic in such a scenario is that all VSN users are similar because of the unique gateway and heading. Our observations are: (1) VSN users stay longer than both the two scenarios ($I$ and $II$) before being exposed. (2) The users' probability of quitting (except "$Y$" users) is not rising with a big amount per quitting event thus the adversary needs more users to quit in order to be able to determine the quitting event of a monitored target.

## 5 Conclusion

In this work we investigated the end points location privacy and the re-identification problem. We first introduced the problem and our EPP scheme. We accompanied this with different simulations where we varied the number of gateways, headings and the number of VSN users who enable, disable and not leave the district. The obtained results showed that the more the users have the same similarity, the more they are protected from quitting-event exposition. The results also showed that the class "$Y$" VSN users affect negatively the privacy of other users. Thus, from all of these we conclude that, in order to ensure a high level of privacy, VSN users have not to be selfish and be aware of the privacy term. With this, not

only they protect their own privacy, but, the others' as well. The nature of the district and the number of gateways and headings have also an impact on the achieved privacy. Finally, EPP has to be accompanied by a pseudonym change strategy such as mix-zones in order to maintain the privacy of VSN users even after leaving the district (e.i. in the outside environment).

## References

1. Lu, Rongxing, et al. "Pseudonym changing at social spots: An effective strategy for location privacy in vanets." IEEE transactions on vehicular technology 61.1 (2012): 86.
2. Mfenjou, M. L., Ari, A. A. A., Abdou, W., & Spies, F. Methodology and trends for an in-telligent transport system in developing countries. Sustainable Computing: Informatics and Systems, 19, 96-111 (2018).
3. Al-Kahtani, Mohammed Saeed. "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)." Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on. IEEE, 2012.
4. Sampigethaya, Krishna, et al. CARAVAN: Providing location privacy for VANET. Washington Univ Seattle Dept of Electrical Engineering, 2005.
5. Corser, George, et al. "Endpoint Protection Zone (EPZ): Protecting LBS user location privacy against deanonymization and collusion in vehicular networks." Connected Vehicles and Expo (ICCVE), 2013 International Conference on. IEEE, 2013.
6. Huang, Leping, et al. "Enhancing wireless location privacy using silent period." Wireless Communications and Networking Conference, 2005 IEEE. Vol. 2. IEEE, 2005.
7. Corser, George P., Huirong Fu, and Abdelnasser Banihani. "Evaluating location privacy in vehicular communications and applications." IEEE transactions on intelligent transportation systems 17.9 (2016): 2658-2667.
8. Li, Mingyan, et al. "Swing & swap: user-centric approaches towards maximizing location privacy." Proceedings of the 5th ACM workshop on Privacy in electronic society. ACM, 2006.
9. Freudiger, Julien, et al. "Mix-zones for location privacy in vehicular networks." ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS). No. LCA-CONF-2007-016. 2007.
10. Beresford, Alastair R., and Frank Stajano. "Location privacy in pervasive computing." IEEE Pervasive computing 1 (2003): 46-55.
11. Song, Joo-Han, Vincent W. Wong, and Victor C. Leung. "Wireless location privacy protection in vehicular ad-hoc networks." Mobile Networks and Applications 15.1 (2010): 160-171.
12. Pan, Yuanyuan, and Jianqing Li. "Cooperative pseudonym change scheme based on the number of neighbors in VANETs." Journal of Network and Computer Applications 36.6 (2013): 1599-1609.
13. Ali, Ahmad, et al. "A comprehensive survey on real-time applications of WSN." Future Internet 9.4 (2017): 77.