Towards an Efficient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks

Abdelwahab Boualouache, Sidi Mohammed Senouci, Samira Moussaoui,

Towards an Efficient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks

Abdelwahab Boualouache*, Sidi-Mohammed Senouci**, and Samira Moussaoui*
*Department of Computer Science, RIIMA laboratory, USTHB University, Bab Ezzouar, Algiers, Algeria
**DRIVE EA1859, Univ. Bourgogne Franche-Comté, F58000, Nevers, France
Email: aboualouache@usthb.dz, Sidi-Mohammed.Senouci@u-bourgogne.fr, smoussaoui@usthb.dz

Abstract— **Protecting the location privacy is still one of the main challenges in Vehicular Ad-hoc Networks (VANETs). Although, standardization bodies such as IEEE and ETSI have adopted the pseudonymous scheme as a solution to this problem, an efficient pseudonym changing and management is still an open issue. In this paper, we propose a complete and efficient pseudonym management and changing scheme based on Vehicular Location Privacy Zone (VLPZ). We define VLPZ as a roadside infrastructure designed to pseudonyms management and changing. This scheme considers that the vehicular geographic area is partitioned as a grid, where each cell contains one or many VLPZs. The location privacy protection level provided by the scheme depends on the VLPZ capacity and the number of vehicles that are inside it at the same time. For this reason, we also propose a reputation mechanism to stimulate vehicles to enter to the VLPZ, and finally evaluate the performances of the proposed scheme using Veins Framework based on OMNet++ network simulator and SUMO mobility. Simulation results demonstrate the effectiveness of the proposed scheme.**

Keywords—VANETs; Security; Location privacy; Pseudonym Changing; Pseudonym Management..

I. INTRODUCTION

On of the keys of a success deployment of Vehicular Ad-Hoc Networks (VANETs) is to consider the location privacy protection of their users [1]. A common approach to avoid this problem is that vehicles use multiple identifiers, called pseudonyms, instead of static identifiers in broadcasting safety messages. Current security standards such as IEEE 1609.2 standard [2] and ETSI 102941-v1.1.1 [3] are based on a public key infrastructure (PKI), where the pseudonyms represent a set of certified public keys stored in the vehicle's On-Board Unit (OBU). Vehicles can then periodically change their pseudonym to mitigate the tracking of their positions. The frequency of pseudonyms changing is then an important factor in the level of location privacy protection provided by this approach i.e. the higher frequency of pseudonyms changing is, the more level of location privacy protection is provided. However, this frequency should not exceed a certain threshold to do not affect the communication performances [4]. In addition, the change of pseudonym should be accompanied by the change of the identifiers of all communication protocols stack layers such as the MAC and the IP addresses [5]. Although, this approach is adopted by both of the academia and the industry to be applied in the near future of VANETs' deployment, several challenges are still to be addressed [6]. We cite for example that: (i) several works that have been conducted on the pseudonym changing approach efficiency (e.g. [7]) demonstrated that, due to the pseudonym linking attacks, a simple changing of pseudonym is ineffective to provide the required level of location privacy protection for VANETs' users. For this reason, several pseudonym changing strategies have been proposed to provide an efficient pseudonym changing (e.g. [8] [9][10][11]). However, an effective strategy is still an open problem of the literature [12], (ii) due to their rationality behavior, vehicles refuse to cooperate by changing their pseudonyms simultaneously with other vehicles [13], which has a negative impact on the privacy protection level provided by the pseudonym changing approach, and last but not least (iii) the existing solutions to distribute the pseudonyms sets and the certificates (pseudonyms) revocation lists (CRLs) requires that the VANET area should totally be covered by Roadside Units (RSUs), which generates a high deployment costs and is hard to be achieved, especially in the first phase of the VANETs' deployment [14].

To address these issues and in contrast to the existing works that only focus on one (e.g. [8] [13] [15]) or some issues (e.g. [16][10]) of the pseudonym changing approach, this paper proposes a complete and efficient pseudonym changing and management scheme. This scheme is mainly based on the Vehicular Location Privacy Zone (VLPZ). We define the VLPZ as a roadside infrastructure designed not only for the changing of pseudonyms [17] but also for the management of them. VLPZ can easily be implemented in the existing roadside infrastructures such as gas stations, electric vehicles charging stations and toll booths or new independent roadside infrastructures deployed for VANETs. The proposed scheme supports a synchronized changing of all identifiers of the communication stack layers and the user-centric location privacy model. In addition, to well manage the pseudonyms, the proposed scheme considers that the vehicular geographic area is partitioned as a grid, where each cell contains one or many VLPZs. The location privacy protection depends on the capacity of the VLPZ and the number of vehicles that exist inside it at the same time. For this reason, we also propose a reputation mechanism to stimulate vehicles to enter to the VLPZ, and finally, evaluate the performance of the proposed scheme using Veins Framework that is based on OMNet++ simulator and SUMO mobility engine.

The remainder of this paper is organized as follows. Section 2 describes some related work. The proposed pseudonym changing and managing scheme is presented in

Section 3. Section 4 describes the reputation mechanism that is used to stimulate vehicles to enter to the VLPZ. The performance evaluation results are presented in Section 5. Finally, the conclusion is given in Section 6.

II. Related Work

Several conducted studies have been demonstrated that a simple pseudonym changing is inefficient to provide the required privacy protection [7]. This is due to the pseudonyms linking attacks that can be classified into two categories [17]: (i) the syntactic linking of pseudonyms: this attack can be performed if there is no synchronization in changing the pseudonyms between vehicles. Indeed, if the target is the only vehicle that changes its pseudonym among the vehicles that are running on the road at time t, the adversary can easily link the old and the new pseudonyms used by the vehicle, (ii) the semantic linking of pseudonyms: this attack can be performed even if the vehicles change their pseudonyms simultaneously. Indeed, by exploiting the information included in safety messages and using some advanced tracking algorithms, the adversary can easily link the vehicle's pseudonyms. To prevent such attacks, several pseudonym changing strategies have been proposed, which can be sorted in terms of their efficiency to prevent the pseudonyms linking attacks into three categories: (i) strategies that rely only on a mechanism to synchronize the changing of pseudonym processes between vehicles (e.g. [8][9]). These strategies showed their weaknesses against a passive adversary that uses the contents of the safety messages to link the pseudonyms using the semantic linking attack, (ii) strategies that propose to encrypt the safety messages for some periods of time (e.g. [10]). These strategies are also broken since it may exist some internal passive adversaries that have the decryption keys. Hence, the contents of the safety messages are disclosed to these adversaries, which can also provide a clue to the external global passive adversary to perform the semantic linking of pseudonyms. In addition, decrypting these messages adds a processing latency, which may not meet with real-time requirements of safety-related applications [18], and finally (iii) strategies that use the radio silence technique (e.g. [11]). The strategies of this category are more effective than the previous ones since they can provide the protection against both external and internal passive adversaries. However, using the radio silence technique in VANETs is challenging since safety-related applications may get affected due of this [19].

Besides of this, the cooperation of vehicles is a key factor in a successful pseudonym changing strategy. Rational vehicles tend to do not change their pseudonyms if they achieved their desired location privacy levels. This is due to the cost generated by pseudonym changing like the impact on geographic routing protocols [4]. [13] proposed a game-theoretic based solution to change the pseudonym in a non-cooperative environment. The authors developed a user-centric privacy model, where vehicles change their pseudonyms if their payoffs will be maximized after pseudonyms changing. However, this solution motivates vehicles to not change their pseudonyms if they have achieved their desired location privacy levels, which has negative consequences on vehicles that do not have achieved their desired location privacy levels yet. In [10], the authors proposed DMPL (Dynamic Mix-Zone for Location Privacy) to dynamically create mix-zones: if a vehicle wants to create a mix zone, it sends a request to a strategy control server (CS); after receiving the request from the vehicle, the CS determines the length of the vehicle's DMPL area and sends a command to all vehicles found in this area in order cooperate in creating vehicle's DMPL. The authors also proposed a mechanism to stimulate rational vehicles to cooperate on creating DMPL. However, this strategy is vulnerable to the semantic linking of pseudonyms and has many other drawbacks like the huge generated overhead.

[16] pointed out that the existing solutions have only focused on how to provide an efficient pseudonym changing and ignore the implementation challenges of pseudonyms changing approach. For this purpose, they proposed RSUs- based scheme to generate and distribute pseudonym sets to the vehicles and an exchange of pseudonyms sets between RSUs mechanism to increase the anonymity. However, this scheme strongly depends on RSUs, which generates high deployment costs. In addition, it is still exposed to the semantic linking attack of pseudonyms.

III. PSEUDONYM CHANGING AND MANAGEMENT SCHEME DESIGN

In this section, we present the design of the proposed scheme. This section is structured as follows. We first describe the considered adversary model. We then present the system model, the VLPZ model, and the VLPZ-based pseudonym changing strategy. After that, we present the VLPZ-based pseudonyms sets and revocation lists distribution. Finally, we describe the used privacy evolution model and the mechanism of generating the communication layers identifiers from the pseudonym.

A. Adversary Model

In this paper, we are interested to study the location privacy protection against a strong passive adversary model. This adversary is composed of an external global passive adversary and few internal local passive attackers. It aims to track the target vehicle by eavesdropping all communications of any vehicle within a region of interest. The adversary model is well aware of the system model and the proposed scheme design. However, it has no control on the VLPZ. In addition, this adversary is not able to perform tracking using cameras, because the cost of the global eavesdropping with cameras is much higher than the radio-based eavesdropping. Therefore, camera-based global eavesdropping is beyond the scope of this paper.

B. System Model and assumptions

As illustrated in Figure 1, to facilitate the management of pseudonyms and CRLs, we consider that the vehicular geographic area is partitioned as a grid. The cells of the grid have a same predefined size. Each cell may comprise the entire downtown area of a small town or few city blocks. The VANET system is composed of vehicles and Road-Side Units (RSUs).

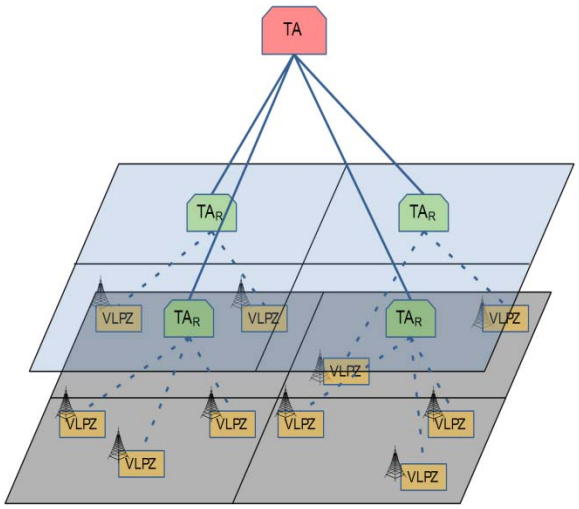


Fig. 1. An example of the proposed system model.

Each vehicle has an OBU device that is equipped with a wireless technology based on the IEEE 802.11p/WAVE standard. The OBU allows the vehicle not only to communicate with other vehicles but also with RSUs. Each vehicle is also equipped with a map and a GPS receiver that allows obtaining the position and the current time. Each vehicle periodically broadcasts a safety message every t milliseconds, where each message includes information about the vehicle such as its position and its speed. We also assume the existence of a central trusted authority (TA) that provides public and private keys to vehicles and RSUs. Before joining the VANET, each vehicle registers with the TA with its vehicle identifier, denoted by ID_v . During the registration, each vehicle Vi is equipped with a public and a private keys and sets of pseudonyms. Each set contains n pseudonyms $K_{i,j}$, where $j \in 1,...,$ n. For each pseudonym $K_{i,j}$ of vehicle Vi , the TA provides a certificate $Cert_{i,j}$ ($K_{i,j}$). The private key K_{ij}^{-1} corresponding to the pseudonym $K_{i,j}$ is used by the vehicle Vi to digitally sign messages. The pseudonym is attached to each message to enable other vehicles and RSUs to verify the sender's authenticity. Each vehicle changes its pseudonym each δ minutes. Each cell contains one regional trusted authority (TA_R), and one or more Vehicular Privacy Zones (VLPZs). TA_Rs act as intermediates between the TA and the VLPZs. They aim to manage the pseudonyms sets and the CRLs distribution and control the location privacy protection level provided the VLPZs within the cells. Indeed, all the TA_Rs are connected to the TA, and each TA_R regional is contacted to the VLPZs within its cell via secure communication links.

C. VLPZ Model

We define the Vehicular Location Privacy Zone (VLPZ) as a roadside infrastructure managed by trusted regional authorities like municipalities or directly by the country transportation department. Each cell of the grid can contain one or more VLPZs. The VLPZ aims not only to increase the location privacy protection level of vehicles within the cell by providing an effective pseudonym changing [17], but also to distribute pseudonyms sets and CRLs to them. The design of VLPZ is seemingly similar to the existing roadside infrastructures like gas stations. As illustrated in the Figure 2, a basic VLPZ consists of one entry point called the router, one exit point called the aggregator and a limited number of lanes l where $l > 1$. Each VLPZ is equipped by an RSU denoted by RSU_{vz} and used to: (i) periodically announce the existence of a VLPZ, (ii) stimulate vehicles passing through the VLPZ to enter, (iii) request pseudonyms sets from the TA_R and distribute them to the vehicles inside the VLPZ according to their requests, (iv) request the CRLs from the TA R and distribute them to the vehicles inside the VPLZ, and finally (v) get information from vehicles, which helps the VLPZ to take certain decisions. The VLPZ can easily be implemented in the existing roadside infrastructures such as gas stations and toll booths. However, due to the increasing interest of users to protect their location privacy, we do not rule out that the VLPZ can be created as an independent roadside infrastructure in the future VANETs deployment. VLPZs emplacements should be shown on the map to help vehicles to enter them, when it is needed.

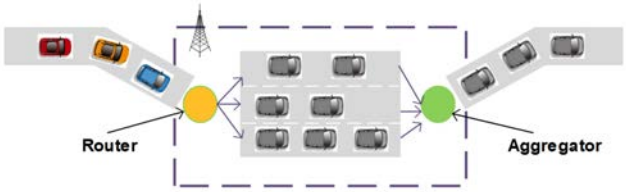


Fig. 2. The VLPZ basic model

D. VLPZ-based Pseudonym Changing Strategy

The strategy of pseudonym changing is executed as follows[17]. The RSU_{vz} periodically broadcasts notifications to inform the vehicles that are passing through a VLPZ its existence. If a vehicle wants to access to the VLPZ, it sends a request to the RSU_{vz}. As Figure 2 shows vehicles arrive to a VLPZ, one after another, on a one-lane. They keep broadcasting safety messages until they enter the VLPZ. When a vehicle reaches the router, it stops broadcasting safety messages and heads for an assigned VLPZ's lane. The assigned lane is randomly and privately selected by the router. The vehicle can then reside inside a VLPZ for a random period of time. This period mainly depends on the service time. For example, if we assume that a VLPZ is implemented in a gas station, the service time is the time taken by the driver to fill the fuel tank of its vehicle. A vehicle must change its pseudonym before it exits the VLPZ and all vehicles exit a VLPZ through the aggregator. However, the exit order is different from the entering order since the residency periods of vehicles are random. We also assume that the aggregator can intervene to select a certain order in random and private way. As discussed in [17], this strategy provides the protection not only against both of the syntactic and the semantic linking of pseudonyms, but also against the FIFO attacks. In addition, differently from the strategies that

rely on the radio silence technique, the road safety is preserved in this strategy.

E. Pseudonyms Sets and Revocation Lists Distribution

In contrast to the existing solutions that rely only on RSUs that are spread over roads to distribute pseudonyms sets (e.g. [16]) and pseudonyms revocation lists (CRLs) (e.g. [20]), we propose in this paper that the distribution of pseudonyms sets and CRLs is performed inside the VLPZ and the RSU_{vz}s are the only roadside units that are used for this purpose. This helps to reduce the number of required RSUs to carry out these operations, which significantly reduces the deployment costs. However, on the one hand, the CRLs should quickly and widely be distributed in order to provide a reasonable revocation time. On the other hand, as the demand of vehicles in terms of pseudonyms is permanent, vehicles should be able to refill pseudonym sets each time they require them. For these reasons, we propose that vehicles: (i) can exchange small CRLs updates through V2V communications. A method like [20] can be used for this purpose, (ii) can be involved in the distribution of pseudonyms sets [21]. In order to request new pseudonyms sets, the vehicle sends a request, which includes its identifier (ID_v), to the RSU_{vz}. This request will immediately be forwarded to the TA_R. When a TA_R receives such request, it first checks if it has enough number of pseudonym sets to satisfy the demand of the vehicle. If this is the case, TA_R sends back the requested pseudonyms sets to the RSU_{vz}. Else, the TA_R forwards the request to the TA that will satisfy the demand as soon as it receives the request. In the same the way, the pseudonyms sets will be sent back to TA_R and from it to the RSU_{vz}. Finally, the RSU_{vz} sends the requested pseudonyms sets to the vehicle as soon as receives them. All exchanges between vehicles and the RSU_{vz} should be encrypted in order prevent the adversary to get access to these messages. We still mention that the pseudonyms sets are generated by the TA and distributed to the TA_Rs according to their estimations of the number of required pseudonyms sets in each cell.

F. Privacy Level Evolution

The location privacy level of a vehicle changes over the time. It can decrease due to the pseudonym linking attacks and increase each time that a vehicle enters to a VLPZ. To capture the evolution that occurs to the location privacy level of ma vehicle over time, we adapt the user-centric location privacy model introduced by [13]. The location privacy level of a vehicle i is modeled using a location privacy loss function $\beta_i(t, T_i^{vz})$: $(\mathbb{R}^+, \mathbb{R}^+) \rightarrow \mathbb{R}^+$ where t is the current time and $T_i^{vz} \leq$ t is the time of the last pseudonym change of vehicle i inside a VLPZ. The privacy loss is set to 0, each time that i changes its pseudonym inside a VLPZ and increases with time according to a sensitivity parameter, $0 < \lambda_i < 1$ until it reaches a maximum value $A_i(T_i^{vz})$, which is the location privacy protection level achieved at last pseudonym change of vehicle i inside a VLPZ. The privacy loss function is defined as follows:

$$\beta_i(t, T_i^{vz}) = \begin{cases} \lambda_i(t - T_i^{vz}) & \text{for } T_i^{vz} \leq t < T_i^{max} \\ A_i(T_i^{vz}) & \text{for } t \geq T_i^{max} \end{cases}$$

Where $T_i^{max} = \frac{A_i(T_i^{vz})}{\lambda}$ is the time when the function reaches the maximal privacy loss. The location privacy level of vehicle i at time t is :

$$A_i(t) = A_i(T^{vz}) - \beta(t, T^{vz}), t \geq T^{vz}$$

Figure 3 illustrates the evolution of the location privacy level of a vehicle i. Its privacy level (A_i (t)) is initially equal to 0 and its desired location privacy level is A_d. The vehicle is then looking to enter to a VLPZ each time when its location privacy is below than its desired level. For this reason, it enters to a VLPZ at times t1, t2, and t3. However, at t4, i enters to a VLPZ, although its location privacy level is greater than the desired level. This is because the vehicle enters to cooperate with other vehicles to increase their location privacy levels. This is due the proposed reputation mechanism described in Section 4.

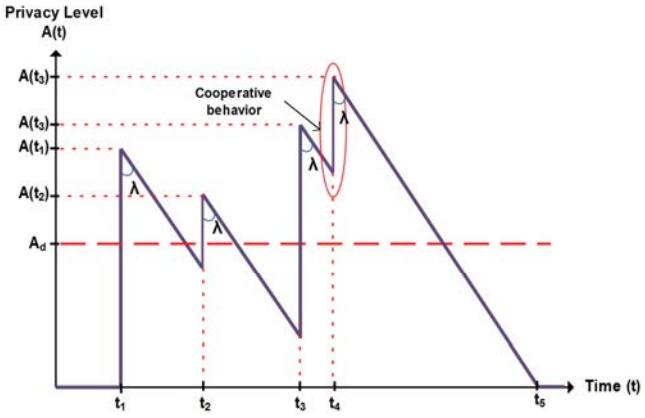


Fig. 3. Evolution of the location privacy level of a vehicle i over time.

G. Generating The Communication Layers Identifiers

In order to prevent the pseudonyms linking attack, the change of pseudonym should be accompanied by the change of the identifiers of all communication stack layers such as the MAC and the IP addresses [5]. In this scheme, we propose that vehicles use the Cryptographically Generated Address (CGA) protocol [22] to generate the IP addresses from the pseudonyms and to generate the MAC addresses from the generated IP addresses. As described in [23], CGA uses a pseudonym (public key) and a random 128-bit number to generate the interface identifier, which is concatenated with a subnet prefix to build an IPv6 address. The concept of CGA can also be used to generate a MAC address from the pseudonym. Indeed, [16] proposed to generate the hash value of (Random 128-bit number || Subnet prefix || Collision count || Public Key || Extension fields). The collision count and the extension are described in [23].

IV. MOTIVATING VEHICLES TO ENTER TO THE VLPZ

The location privacy protection level provided by a VLPZ mainly depends on its capacity and its occupancy i.e. the number of vehicles inside it at the same time. The capacity of the VLPZ, denoted by K, is a static parameter that can be set by the system designer. However, the occupancy of the VLPZ, denoted by $|AS|_t$, can be impacted by several parameters. First, the number of vehicles that request to enter to the VLPZ definitively depends on the road traffic density i.e. more vehicles exist on the road, more vehicles enter to the VLPZ. In addition, in this paper, we assume that vehicles are rational. In other words, they look to ensure their location privacy protection with a minimum possible cost, which represents the cost taken by a vehicle to move to a VLPZ. This cost can be expressed by the time to reach the VLPZ and quantified by the lost of pseudonyms during this time. Therefore, if a vehicle have reached its desired location privacy protection level (A_d), it will not look to enter a VLPZ again to cooperate with other vehicles to increase their location privacy protection levels, until its privacy protection level goes under A_d . For this reason, we assume that the VLPZ uses a reputation system to increase its occupancy. The VLPZ then broadcasts invitation requests to motivate the vehicles to enter to the VLPZ. If a vehicle positively responds to enter to the VLPZ, its reputation value will then increase. However, if a vehicle refuses to enter to the VLPZ, its reputation value will decrease. The increase or the decrease of the reputation value depends on the VLPZ occupancy at t_j, where t_j is time when the vehicle exits the VLPZ, if the vehicle accepts the j^{th} invitation of the VLPZ or the time when the vehicle receives the invitation, if the vehicle refuses the invitation. The reputation value $\mathbb{R}_i^j$ of a given vehicle i after j^{th} invitation is then given by following formula.

$$\mathbb{R}_i^j = \begin{cases} \mathbb{R}_i^{j-1} + |AS|_{t_j} & \text{if v cooperates} \\ \mathbb{R}_i^{j-1} - |AS|_{t_j} & \text{if v defeats and } \mathbb{R}_i^{j-1} \geqslant |AS|_{t_j} \\ 0 & \text{if v defeats and } \mathbb{R}_i^{j-1} < |AS|_{t_j} \end{cases}$$

Where $\mathbb{R}_i^{j-1}$ is the old reputation value of vehicle i. The reputation value of the vehicle increases as much as it cooperates. The accumulated reputation value is then used by the vehicle when it needs to access to the VLPZ.

As described in Algorithm 1, when the VLPZ receives a request to access from a vehicle i, it first checks if the reputation value of i is above or equals to a certain threshold, denoted by ω. If this is the case, the VLPZ then accepts i to enter to the VLPZ. Else, the VLPZ checks if i has already refused an invitation from a VLPZ. The reason of this second check is to verify if the vehicle does not have already an opportunity of cooperation. Indeed, the VLPZ can get this information directly from the TA, which is connected to all VLPZs. If the VLPZ finds that i has already refused an invitation from a given VLPZ, i is detected as a selfish and the VLPZ refuses the access to i . Else, the VLPZ accepts the request of i. The vehicle then always tries to keep its reputation value above ω, which stimulates it to cooperate more when it receives an invitation from the VLPZ. We mention that if the VLPZ is implemented at an existing roadside infrastructure like a gas station, refusing access to the VLPZ means that the vehicle will enter to the infrastructure and will not execute the VLPZ-based strategy and request new pseudonyms sets. We also mention that during the registration, the TA gives to each vehicle a reputation value above to ω, which allows the vehicle to enter to the VLPZ at the beginning. In addition, each time that the vehicle exits a VLPZ, its reputation value will be set to 0.

Algorithm 1: Decision on a vehicle's request

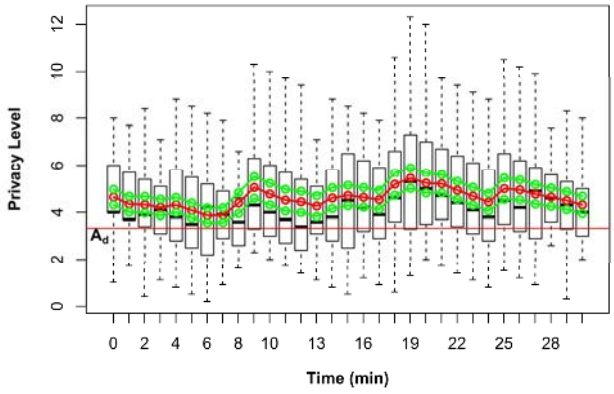
```
Data: Request from a vehicle i
Result: Decision from a VLPZ
Initialize;
RSU_vz periodically broadcasts notification;
if (| AS |_t < K) then
    RSU_vz periodically broadcasts invitations;
end
if (i.privacy_level < A_d^i) then
    if (i.reputaion_level ⩾ ω) then
        Allows access to i;
    else
        if (i has already refused an invitation from a
          VLPZ) then
            i is detected as a selfish ;
            Refuses access to i;
        else
            Allows access to i;
        end
    end
else
    Allows access to i.;
end
```

V. PERFORMANCE EVALUATION

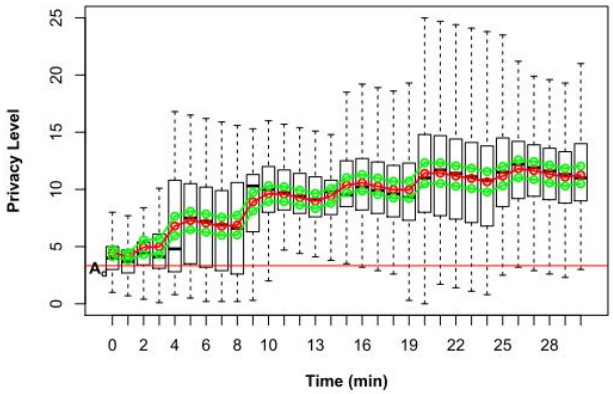
In order to evaluate the performances of the proposed scheme, we performed a set of simulations. These simulations are conducted using Veins Simulation Framework [24]. Veins is an inter-vehicular communication simulation framework based on OMNet++ bi-directionally coupled with SUMO road traffic simulation [25]. OMNet++ and SUMO run in parallel and communicate via a TCP socket. The reason of choosing Veins is its ability to simulation full 802.11p and IEEE 1609.4 DSRC/WAVE network layers. Table I summarizes the parameters considered in our simulations.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation duration	30 min
Transmission Range	500 m
Number of vehicles	100
The VLPZ capacity (K)	10
The desired level (A_d)	K/3
The reputation threshold (ω)	K/2, K/4
The sensitivity parameter (λ)	0.3
Changing peudonym frequency	1 min



(a) Baseline



(b) With the reputation mechanism ($\omega = K/2$)

Fig. 4. The evaluation of the location privacy level of vehicles over time.

The considered scenario represents a simple road course that has a rectangle shape of dimensions 3km x 1.5km. We have installed a VLPZ on one side of this road course. The vehicles were generated using SUMO to take repeated turns of 30 min duration on this road course. The privacy level values and the reputation values of vehicles are initialized according to a normal distribution N (μ,σ) with a mean equal to $\mu = 5$ and with a standard deviation equals to $\sigma = 5/3$. In addition, as shown in Table I, the desired levels of all vehicles and their sensitivity parameters are assumed equals. In our evaluation, we run simulation several times with different random seeds and calculate the average value with 95% confidence interval. Figure 4 illustrates of the evolution of the location privacy protection levels of vehicles over time both when using the baseline version of the scheme and when using the scheme with the reputation mechanism. We can see in the Figure 4(a) that using the baseline version, the average of privacy protection levels still stable over time and more that 30% of vehicles still have privacy protection levels under the desired level (A_d) over time. However, as illustrated in Figure 4(b), when the reputation mechanism is used, the average privacy protection levels gradually increase and at time 30 min, only 2% of vehicles still have privacy protection levels under the desired location privacy level (A_d), which demonstrates the efficiency of the proposed reputation mechanism.

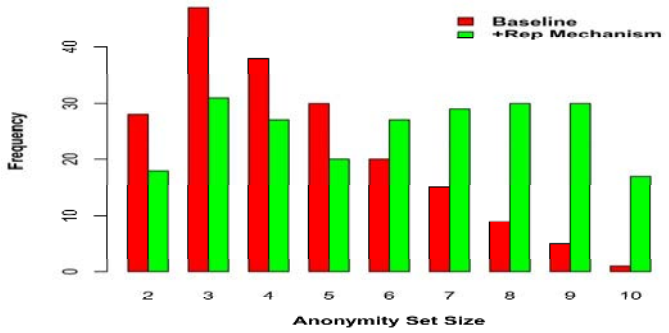


Fig. 5. The anonymity set size frequency over time.

In Figures 5 and 6, we evaluate the location privacy protection level provided by the VLPZ over time. In our evaluation, we use two well-known privacy metrics: the size of the anonymity set and the degree of anonymity. The anonymity set (AS) defined as the set of vehicles that are indistinguishable from the target with the set including the target itself. At a VLPZ, the anonymity set actually includes the target and all vehicles inside a VLPZ. The size of the anonymity set is then the number of vehicles that the anonymity set includes. The capacity of the VLPZ (K) is the maximum value of the anonymity set size that could be taken by a vehicle when it enters to a VLPZ. The degree of anonymity is the normalized value of the level of privacy protection level achieved compared to the maximum privacy protection level that can be achieved [26]. The anonymity degree (d) is given by the following formula:

$$d = \frac{\log_2(|\ AS\ |)}{\log_2(K)}$$

Figure 5 compares the frequency of the anonymity set size over the simulation period between baseline scheme and the scheme using the reputation mechanism (ω = K/2). It shows that the number of times that the anonymity set size achieves high values increase when the reputation mechanism is used, which has a positive impact on the

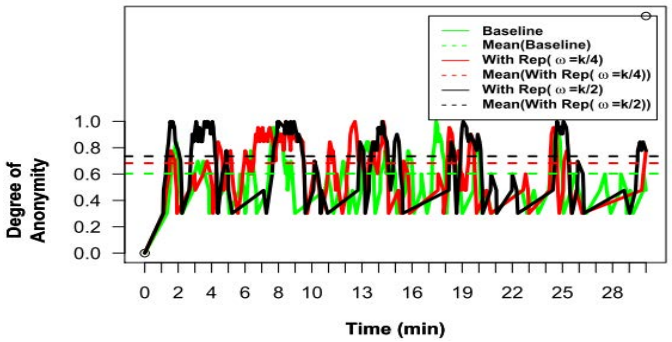


Fig. 6. The degree of anonymity over time.

degree of the anonymity provided by the VLPZ. Indeed, Figure 6 compares between the degree of anonymity of baseline scheme and the scheme using the reputation mechanism, where ω takes the following values respectively: K/4, K/2. The Figure shows that comparing to baseline scheme, the mean of the degree of anonymity increases for more than 0.1 using the reputation mechanism. In addition, the mean of the degree of anonymity slightly increases using the threshold reputation value ω equals to K/2 instead of k/4.

VI. CONCLUSION

In this paper, we proposed a complete and efficient pseudonym changing and managing scheme for vehicular ad-hoc networks. This scheme is mainly based on the VLPZ, which is a roadside infrastructure designed for the changing and the management of pseudonyms and can easily be implemented in the existing roadside infrastructures. We also proposed a reputation mechanism to simulate vehicles to enter to the VLPZs. As a future works, we will develop the communication protocols that will be used in this scheme, and propose a stochastic model to predict the optimal number of VLPZs required in a given cell over time. In addition, we will carry out a simulation study using a real map with real traffic mobility measurements.

REFERENCES

[1] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, "Researchchallenges in intervehicular communication: lessons of the 2010 dagstuhl seminar," IEEE Communications Magazine, vol. 49, no. 5, pp. 158–164, 2011.

[2] IEEE, "Ieee standard for wireless access in vehicular environments security services for applications and management messages," IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006), pp. 1–289, April 2013.

[3] ETSI, "Etsi ts 102 941 v1.1.1- intelligent transport systems (its); security; trust and privacy management," Standard, TC ITS, 2012.

[4] E. Schoch, F. Kargl, T. Leinmller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets"," in Proceedings of the Third European Conference on Security and Privacy in Ad-Hoc and Sensor Networks, ser. ESAS'06. Springer-Verlag, 2006, pp. 43–57.

[5] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in Telecommunications, 2007. ITST'07. 7th International Conference on ITS. IEEE, 2007, pp. 1–6.

[6] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," Communications Surveys Tutorials, IEEE, vol. PP, no. 99, pp. 1–32, Aug 2014.

[7] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: why simple pseudonym change is not enough," in Proceedings of the 7th international conference on Wireless on-demand network systems and services, ser. WONS'10. IEEE Press, 2010, pp. 176–183.

[8] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86–96, Jan 2012.

[9] B. Ying and D. Makrakis, "Pseudonym changes scheme based on candidate-location-list in vehicular networks," in Communications (ICC), 2015 IEEE International Conference on, June 2015, pp. 7292–7297.

[10] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," Vehicular Technology, IEEE Transactions on, vol. 64, no. 12, pp. 5631–5641, 2015.

[11] A. Boualouache and S. Moussaoui, "S2si: A practical pseudonym changing strategy for location privacy in vanets," in Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, June 2014, pp. 70–75.

[12] D. Eckhoff and C. Sommer, "Driving for big data? privacy concerns in vehicular networking," IEEE Security and Privacy, vol. 12, no. 1, pp. 77–79, February 2014.

[13] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 2, pp. 84–98, 2013.

[14] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications," in Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th. IEEE, 2008, pp. 1–5".

[15] G. Yan, S. Olariu, J. Wang, and S. Arif, "Towards providing scalable and robust privacy in vehicular networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 7, pp. 1896–1906, 2014.

[16] H. Artail and N. Abbani, "A pseudonym management system to achieve anonymity in vehicular ad hoc networks," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 106–119, Jan 2016.

[17] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," in (to appear in) The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016). Procedia Computer Science Elsevier, 2016.

[18] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient vanet authentication," Communications and Networks, Journal of, vol. 11, no. 6, pp. 574–588, Dec 2009.

[19] S. Lefevre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of v2x privacy strategies on intersection collision avoidance systems," in Vehicular Networking Conference (VNC), 2013 IEEE, Dec 2013, pp.71–78.

[20] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking, ser. VANET '08. ACM, 2008, pp. 86–87.

[21] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Hpdm: A hybrid pseudonym distribution method for vehicular ad-hoc networks," The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016). Procedia Computer Science Elsevier, 2016.

[22] T. Aura, "Cryptographically generated addresses (CGA)," Internet Requests for Comments, RFC Editor, RFC 3972, March 2005. [Online]. Available: https://tools.ietf.org/html/rfc3972

[23] S. Qadir and M. U. Siddiqi, "Cryptographically generated addresses (cgas): A survey and an analysis of performance for use in mobile environment," IJCSNS Int. J. Comput. Sci. Netw. Secur, vol. 11, no. 2, pp. 24–31, 2011.

[24] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 3–15, January 2011.

[25] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo – simulation of urban mobility," International Journal on Advances in Systems and Measurements, vol. 5, no. 3, pp. 128–138, 2012.

[26] C. Díaz, "Anonymity metrics revisited," in Anonymous Communication and its Applications, 09.10. - 14.10.2005, ser. Dagstuhl Seminar Proceedings, vol. 05411, 2005.