Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 377 – 384

Procedia
Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

HPDM: A Hybrid Pseudonym Distribution Method for Vehicular Ad-hoc Networks

Abdelwahab Boualouache[a,*], Sidi-Mohammed Senouci[b], Samira Moussaoui[a]

[a]Department of Computer Science, RIIMA laboratory, USTHB University BP 32 El Alia Bab Ezzouar, Algiers, Algeria
[b]DRIVE Laboratory, University of Burgundy, 58027 Nevers, France

Abstract

Protecting the location privacy of drivers is still one of the main challenges in Vehicular Ad-hoc Networks (VANETs). The changing of pseudonym is commonly accepted as a solution to this problem. The pseudonyms represent fake vehicle identifiers. Roadside Units (RSUs) play a central role in the existing pseudonyms distribution solutions. Indeed, the VANET area should totally be covered by RSUs in order to satisfy the demand of vehicles in terms of pseudonyms. However, the total coverage is costly and hard to be achieved, especially in the first phase of VANETs deployment. In addition, RSUs could be overloaded due to the large number of pseudonyms requests that could be received from vehicles. In this paper, we propose a new hybrid pseudonyms distribution method, called HPDM that relies not only on RSUs but also on vehicles to perform the pseudonyms distribution. The analysis demonstrate that HPDM is privacy and accountability preserving. The performance evaluation of the proposed method is carried out using veins framework based on OMNet++ network simulator and SUMO mobility engine and shows its feasibility.

Peer-review under responsibility of the Conference Program Chairs

Keywords: VANETs; Security; Location privacy; Pseudonyms distribution.

1. Introduction

Vehicular Ad-hoc networks (VANETs) are considered as a subclass of Mobile Ad-hoc networks (MANETs)[1]. The mobile nodes represent the vehicles, which communicate to each other and to fixed infrastructure points, called Road-side Units (RSUs). Many interesting applications are enabled due to these communications. The existing applications allow not only to preserve road safety (e.g., emergence reporting and collision warning) but also to provide traffic efficiency and entertainment[2].

The VANETs are exposed to a variety of attacks that could cause serious damages both on VANET system and users. Location tracking is one of the attacks that can hinder the deployment of VANETs[3]. The problem is coming from the authenticated safety-related messages that are broadcasted with a high frequency and in clear text. Indeed, several studies demonstrated that a simple passive adversary could collect these messages and relate them according

* Corresponding author. Tel.: +213-21-24-76-07 ; fax: +213-21-24-76-07
E-mail address: aboualouache@usthb.dz

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.199

to vehicles' identifiers[4]. The adversary could then generate a movement trajectory of each vehicle to know the emplacements visited by the driver over time, which violates the driver's privacy[5].

The changing of pseudonym is accepted as solution to this problem. The pseudonyms represent fake vehicle identifiers. The vehicle is equipped by a set of pseudonyms, where each pseudonym is used for a limited period of time. An expiry pseudonym is changed by a new one and cannot generally be reused again. The current 1609.2 standard is based on a public key infrastructure (PKI)[6]. The pseudonyms are public keys certified by the trusted authority (TA) and generated using one of the following methods[7]. (i) They could be generated by vehicles themselves, sent to TA to be signed and sent back to vehicles through RSUs, (ii) They could be generated by RSUs instead of vehicles, sent to TA to be signed, and then distributed by RSUs to the vehicles, (iii) They could be generated by a third party, sent to TA to be signed, and distributed by RSUs, and finally (iv) They could generated and singed by TA, and distributed to vehicles by RSUs. In addition, due to the accountability (liability) issues only the TA can still know the link between the real identifier of a vehicle and the set of pseudonyms associated to it.

In[8], Raya and al. estimated the number of pseudonyms needed by a vehicle. They suggested to provide about 43,800 pseudonyms per year for a vehicle that is used 2 hours, in average, per day and changes its pseudonym every 1 minute. However, the number of needed pseudonyms mainly depends the frequency of pseudonym changing and the use of vehicle. Obviously, the more pseudonym changing frequency is, the more location privacy protection is achieved. This is on condition that pseudonym chaining frequency is not less then a certain threshold[9]. Therefore, a huge number of pseudonyms should be stored by vehicles, which can exceed vehicle storage capabilities. For this reason, the existing solutions suggested that pseudonyms should be requested according to the vehicle demand. Indeed, the RSUs play a central role in these solution because they are not only used to request the pseudonyms but also to distribute them. These solutions assume that the VANET area is already covered by RSUs. This assumption might generate a high deployment costs and it is hard to be achieved, especially in the first phase of the VANET deployment. In addition, the RSUs could be overloaded due to frequent pseudonyms requests and distributions operations.

To address these limitations, in this paper, we propose a new hybrid pseudonyms distribution method, called HPDM. HPDM is based not only on RSUs but also on vehicles to distribute the pseudonyms. It aims to involve vehicles in the pseudonyms distribution to ensure the availability of pseudonyms (e.g. in the case of luck in the number of deployed RSUs) and to reduce the overload on RSUs. The analysis demonstrated that proposed method is privacy and accountability preserving. The performance evaluation is carried out using veins framework based on OMNet++ network simulator and SUMO mobility engine. The simulation results show the feasibility of the proposed method.

Our contribution is then threefold:

- We propose a new pseudonym pseudonyms distribution method, called HPDM that is based both on vehicles and RSUs.
- We suggest to integrate HPDM with Urban Pseudonym Changing Strategy (UPCS)[10 11].
- We evaluate the performance of HPDM using veins framework based on OMNet++ network simulator and SUMO mobility engine.

The remainder of this paper is organized as follows. Section 2 describes some related work. The proposed method (HPDM) is presented in Section 3. HPDM analysis are given in Section 4 and performance evaluations are presented in Section 5. The conclusion is given in Section 6.

2. Related work

In[12], the authors investigated the optimal strategy for refilling pseudonyms. Two pseudonyms refill strategies were then identified : refilling a large number of pseudonyms at one time (strategy 1) or refilling a small number of pseudonyms several times (strategy 2). After citing the benefits and the drawbacks of each strategy, the authors concluded that the strategy 2 has more benefits than the strategy 1. For this reason, they proposed a new pseudonym refill solution called pseudonym-on-demand (POD). POD is based on the strategy 1, where vehicles send their requests to the pseudonym provider (PP) through RSUs when they need new pseudonyms. However, as mentioned by the authors themselves the strategy 1 has a high cost of deployment. In[7], the authors evaluated the amount of data that can be acquired by a vehicle during a single pass of a RSU using NS3 simulator. The purpose is to determine whether a single pass over a RSU is enough to a vehicle to get the number of needed pseudonyms. The authors found the amount of data that can be downloaded from the RSU is depended on several parameters such as the speed of the vehicle, the distance between the vehicle and the RSU, and the traffic density. They then concluded that vehicles need several contacts with RSUs to satisfy their demand of pseudonyms. For this reason, they proposed Pseudonym distribution Protocol (PNDP) that allows to RSUs to collaborate for distributing the totality of pseudonyms needed by vehicles.[13] noted that RSUs can be overloaded due to the large number of vehicles' requests. The authors in[14] pointed out the performance impacts that can be created due to pseudonyms refill operations. They then aimed to free up the networks from the unneeded refill operations. For this reason, they investigated the preferred moment to vehicles to request for a pseudonym. They compared three techniques.(i) The baseline technique, where a vehicle requests for pseudonym whenever it meets an RSU, (ii) the threshold technique, where a vehicle requests for pseudonyms only if it has less than a certain threshold, and (iii) the probabilistic technique, where a vehicle requests for pseudonyms as function as the number of pseudonyms that it stores. In[15], the authors considered the pseudonyms as costly resources. As a consequence, they proposed to view the pseudonym as a service i.e. instead of providing pseudonyms pro-actively to all vehicles, the pseudonyms are only provided to the vehicles that requested them. In addition, they developed a stochastic model to estimate the number of pseudonyms needed by vehicles. In[10 11], the authors developped a new pseudonym changing strategy called UPCS based on the creation of silence mix zones at signalized intersection. Simulation results showed that a level of location privacy protection can be achieved using this strategy.

3. HPDM Description

3.1. VANET System Model

We consider that the VANET system is composed of vehicles and Road-Side Units (RSUs). Each vehicle has an On-Board Unit (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 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 trusted authority (TA) that provides public and private keys to vehicles and RSUs. TA has a communication link with all roadside units. The TA is responsible for the generation and management of pseudonyms used by vehicles.

3.2. System Initialization

Before joining the VANET, each vehicle registers with the TA with its vehicle identifier ID_v. During the registration, each vehicle V_i is equipped with a public and a private keys and Q_v sets of pseudonyms. Q_v is the maximum number of pseudonyms sets that can be stored by the vehicle. Each set contains n pseudonyms $K_{j,k}$ where $k \in 1,..., n$. The pseudonyms are public keys certified by the TA. For each pseudonym $K_{j,k}$ of vehicle V_i, the TA provides a certificate $Cert_{j,k}(K_{j,k})$. The private key $K^{-1}_{j,k}$ corresponding to the pseudonym $K_{j,k}$ is used by the vehicle V_i to digitally sign messages. The pseudonym is attached to each message to enable other vehicles an RSUs to verify the sender's authenticity. Each pseudonyms set is identified by a unique identifier (ID_{ps}). Due to accountability issues, the TA stores the details of each issued pseudonyms set such as its identifier and its owner on a table. In the initialization phase TA also identifies the vehicles that will be used to carry out the pseudonyms sets distribution. These vehicles are called the Pseudonym Provider Vehicles (PPVs). The list of all PPVs is also stored by the TA.

Typically, the PPVs are chosen from the vehicles that are frequently used to travel for long distances. This is basically depends on the nature of the vehicle such as (.e.g, buses, cars, and trucks) and the behaviour of the driver. We will investigate more the strategies on the choose the PPVs in our future works.

After installing RSUs, TA provides to each RSU a couple of certificated keys consisting of a public key with an associated certificate $Cert_{RSU}$ and a private key for digitally sign the broadcasted messages and a symmetric key P_{RSU} to encrypt communication between the TA and the RSU. The RSU has a pseudonyms pool that supports only Q_{RSU} sets of pseudonyms. The TA generates and sends Q_{RSU} encrypted sets of pseudonyms with their corresponding private keys. The RSU contacts the TA each time it needs new sets of pseudonyms. The TA temporary assigns the RSU as the owner of each delivered pseudonyms set. In order to check the validity of the public key certificates, the TA also provides for each RSU and for each vehicle its own public key P_{CA}.

3.3. Pseudonyms Distribution

In contrast of the existing pseudonyms distribution solutions, which are only based on RSUs, HPDM relies both on vehicles and RSUs to carry out the pseudonyms distribution. The HPDM method consists thus of two protocols: RSU-based pseudonyms distribution protocol and Vehicle-based pseudonyms distribution protocols. These two protocols are presented in following subsections.

3.3.1. RSU-based Pseudonyms Distribution Protocol

The RSU periodically broadcasts a notification ($Notif_{pds}$) to announce the availability of pseudonyms distribution service. These notifications are authenticated and the RSU's public key certificate ($Cert_{RSU}$) is attached to every notification. When a vehicle receives such notification, it contacts the RSU only if one or more of these conditions are met :

1. If the number of pseudonyms sets stored by the vehicle is less or equal than a certain threshold C_1, the vehicle then requests for new pseudonyms sets. This authenticated request includes the vehicle identifier (ID_v), and is encrypted by the RSU public key. As soon as the RSU receives the request, it starts delivering the set of pseudonyms to the vehicle. The delivery messages are encrypted using the current pseudonyms of the vehicle. The vehicle should send an acknowledgment each time it receives a complete pseudonyms set. In addition, to keep the system updated, the RSU sends to the TA an information about each delivered pseudonyms set and the vehicle that obtained that set. After receiving these information, the TA then updates the pseudonyms sets' owners in its table. Algorithm 1 describes the pseudo-code of the RSU-based pseudonyms distribution protocol.

Algorithm 1 RSU-based Pseudonyms Distribution

```
  RSU periodically broadcasts a notification ($Notif_{pds}$)
  if (vehicle.notif_received = true) then
      if (vehicle.pseudossets_number)$\leq C_1$ then
          Vehicle sends a request to the RSU for new pseudonyms sets
          if rsu.request_received = true then
              RSU sends an encrypted pseudonyms set to the vehicle
              while (rsu.acknowledgment = true) do
                  RSU sends an encrypted pseudonyms set to the vehicle
              end while
          end if
      end if
  end if
```

2. If the vehicle is a Pseudonym Provider Vehicle (PPV) and has already distributed pseudonyms sets but it did not inform the TA about them yet. Then, the vehicle sends a message to the RSU that includes its identifier and the information about each distributed pseudonyms set such as its identifier ID_{ps}, the identifier of the new owner of the pseudonyms set, and the time when the distribution occurs. The identifier of the owner represents the pseudonym that is used to contact the PPV. The message is then authenticated and encrypted using the RSU's public key, and will immediately be transferred to the TA as soon as the RSU receives it. After the that, the RSU sends an acknowledgment encrypted by the current pseudonym of the PPV. The TA uses the information included in the message to update its table that keeps the detail of each distributed pseudonyms set. Algorithm 2 describes the pseudo-code that describes this process.

Algorithm 2 Updating The Information about the distributed PS

```
RSU periodically broadcasts a notification ($Notif_{pds}$)
if (vehicle.notif_received = true) then
    if (vehicle.IamPPV= true) and (vehicle.PS_distributed=true) then
        Vehicle sends a message that includes the detail of each performed distributed PS
        if rsu.received_message = true then
            RSU transfers the received message to the TA.
            RSU sends an acknowledgement to the PPV
        end if
    end if
end if
```

3.3.2. Vehicle-based Pseudonyms Distribution Protocol

Algorithm 3 describes the pseudo code of vehicle-based pseudonyms distribution protocol. The pseudonym provider vehicle (PPV) starts the distribution process only if the number of pseudonyms sets that possesses is grater or equal than a certain threshold C_2. If the condition meet, the PPV starts broadcasting notifications to announce the availability of pseudonyms distribution service. If a neighboring vehicle receives such notification, it checks if the number of remaining pseudonyms sets is less or equal than a threshold C_1. If this is the case, the vehicle then requests for new pseudonyms sets. The authenticated request is encrypted by the current pseudonym of the provider vehicle. As soon as the *PPV* receives the request, it starts delivering pseudonyms sets to the vehicle. The delivery messages are encrypted using the current pseudonyms of the vehicle. The vehicle should send an acknowledgment each time it receives a complete pseudonyms set. This acknowledgment is encrypted using the current PPV pseudonym. After receiving the acknowledgment, the PPV deletes the distributed pseudonym set and should only store the detail of each performed pseudonyms set distribution such as the identifier (pseudonym) of the new owner of the pseudonym and the time of the distribution. These information will be sent to the TA as soon as the PPV has a contact with a RSU as described in Subsection 3.3.1.

Algorithm 3 Vehicle-Based Pseudonyms Distribution

```
if (PPV.pseudossets_number)$\geq C_2$ then
    The  the PPV  periodically broadcasts a notification ($Notif_{pds}$)
    if (vehicle.notif_received = true) and (vehicle.pseudossets_number)$\leq C_1$ then
        Vehicle sends a request to the provider vehicle for new pseudonyms sets
        if  PPV.request_received = true  then
            The PPV sends a pseudonyms set to the vehicle
            while (PPV.acknowledgment = true) and (PPV.pseudossets_number)$\geq C_2$ do
                The PPV sends a pseudonyms set to the vehicle
            end while
        end if
    end if
end if
```

3.4. Integration of HPDM with UPCS

In[10,11], a new pseudonym changing strategy, called Urban Pseudonym Changing Strategy is proposed. UPCS aims to achieve a high level of location privacy protection using the pseudonym changing approach. It uses an RSU installed at a signalized intersection for creating a silent mix zone while the traffic light is red. The analysis and performances evaluation show that UPCS allows to avoid the pseudonyms linking attacks and provides a high level of entropy values. Besides of this, UPCS allows to reduce the radio channel load. For this reason and for the reason that a vehicle may still waiting in front of the red traffic light for a period of time between 30s et 60s, we suggest to integrate UPCS with HPDM. Indeed, the low radio channel load and the long period of contact between the RSU and the vehicle, will definitely help the vehicles to increase the number of pseudonyms sets loaded from the RSU.

4. HPDM Analysis

In this section we analyze HPDM in terms of the accountability and the privacy preserving. The accountability is an important security requirement in VANETs because the misbehaving nodes should be identified and excluded from the system. In the pseudonymous schemes, the authorities should be able to resolve the link between the real identifier of a vehicle and its pseudonym. In HPDM, the accountability is preserved at different levels: (i) During the initialization phase, the TA stores the information about the owner each provided pseudonyms set, (ii) The TA also temporally assigns the RSU as an owner of the pseudonyms sets that not distributed yet to the vehicles (iii) If the RSU distributes a pseudonyms set, it sends the identifier of the new owner of the pseudonyms set to the TA. The TA will then update the information about the owner of the pseudonyms set stored in its table, an finally (iv) As distributed in 3.3.1, the pseudonym provider vehicle (PPV), regularly sends a message that contains information about the distributed pseudonyms sets to the RSU. This message includes the pseudonym of new owner of each pseudonyms set. When the TA receives such message, it first resolves the pseudonym to find the real identity of the vehicle. After that, it updates the information about the distributed pseudonyms set.

In the other hand, HPDM is privacy preserving, because the all information exchanged between a vehicle and the RSU and between a PPV and a vehicle are encrypted. In addition, all the pseudonym provider vehicles (PPVs) are monitored by the TA and each distributed pseudonyms set is deleted from the PPVs.

5. HPDM Performances Evaluation

To study the feasibility and to evaluate the performances of the proposed method, we performed a set of simulations. These simulations are conducted using Veins Simulation Framework[16]. Veins is an inter-vehicular communication simulation framework based on OMNet++ bi-directionally coupled with SUMO road traffic simulation[17]. 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 1 summarizes the parameters considered in our simulation.

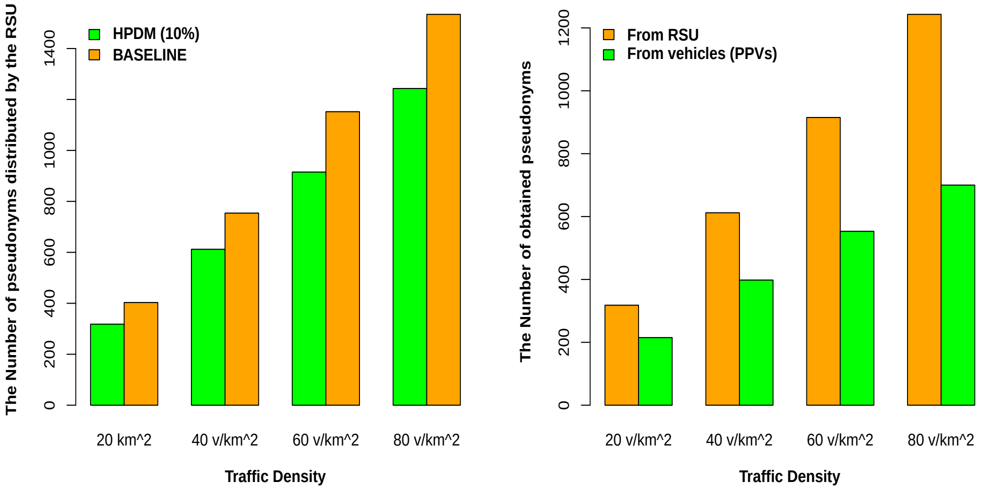
Table 1. Simulation Parameters

Parameter	Value
Simulation duration	30 min
Transmission Range	500 m
Traffic density	20, 40, 60, and 80(vehicles/km^2)
Q_v	6
The number of pseudonyms in each set	10
The frequency of changing of the pseudonym	30 s
$Notif_{pds}$ frequency	1 s
C_1	2
C$_2$	4

In the considered scenario, we have modeled the Manhattan city in Grid of 2km x 2km, three horizontal two-way streets and three vertical two-way streets, with two lanes in each direction, crossed each 1km. The vehicles were generated using SUMO to take trips of 30 min duration. The number of pseudonyms sets that is stored by each vehicle

[0] http://www.omnetpp.org

is randomly selected for the range [C_1 , Q_v]. In our evaluation, we run simulations by changing the traffic density parameter each time, from the low traffic density (20 vehicles/km^2) to the high traffic density (80 vehicles/km^2).



(a) Comparison between HPDM and the Baseline method in terms of the number of obtained pseudonyms sets from RSU.

(b) Comparison between the number of obtained pseudonyms sets both from the RSU and PPVs in HPDM.

Fig. 1. The number of the obtained pseudonyms set versus the traffic density (The percentage of of PPv in HPDM equals 10%.)

We first compare HPD Method with the baseline method. We consider that the percentage of the pseudonym provider vehicles (PPVs) equals only 10%. The baseline distribution method is only based on the RSU. In this method, the vehicles simply request for new pseudonyms if the number of stored pseudonyms sets is less or equal than the threshold C_1.

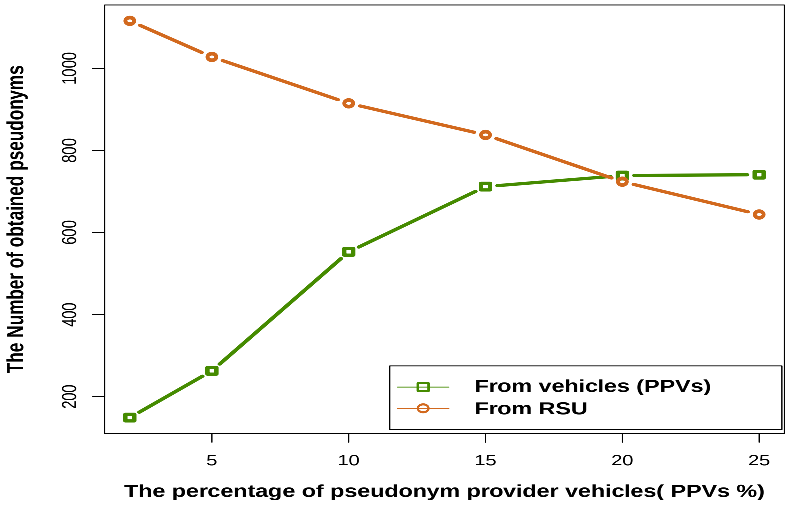


Fig. 2. The number of pseudonyms sets obtained from both of the PPVs versus the percentage of PPVs (Traffic density =60 (veh/km^2))

Figure 1 (a) compares between the number of pseudonyms sets distributed by the RSU in each method versus the traffic density. We can observe that using HPDM, the number of obtained pseudonyms sets from RSUs are reduced whatever the traffic density is. For example, the number of pseudonyms sets distributed by the RSUs is decreased for more than 20% in case of traffic density equals to 20 veh/km^2. Figure 1(b) compares the number the pseudonyms sets received from the RSU with the number of pseudonyms sets received from PPVs in HPDM. We can see that an important number (more than 35%) of pseudonyms sets are obtained from PPVs, which reflects the role played by these vehicles in the pseudonyms sets distribution.

In Figure 2, we evaluate the number of pseudonyms sets obtained both from the RSU end the PPVs as function as the percentage of PPVs. We set traffic density to 60 (veh/km^2). Figure 2 shows that the number of obtained pseudonyms from the RSU decreases with the increase of the percentage of PPVs. It also shows the number of pseudonyms sets obtained from the PPVs increases with the percentage of PPVs. Indeed more that than 50% of pseudonyms sets are obtained from PPVs when the percentage of PPVs only equals to 20%.

6. Conclusion

In this paper, we proposed a Hybrid Pseudonym distribution Method (HPDM) that is based not only on RSUs but also on vehicles to perform the distribution of pseudonyms. We carried out a set of simulation to evaluate the performance of the proposed method using veins framework. The obtained results demonstrated the feasibility of the proposed method. As future works, we will investigate the choosing the pseudonym provider vehicles (PPVs) and carry out extensive simulations.

References

1. C. Sommer, F. Dressler, Vehicular Networking, Cambridge University Press, 2014.
2. G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions, Communications Surveys Tutorials, IEEE 13 (4) (2011) 584–616.
3. F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, L. Wischhof, Research challenges in intervehicular communication: lessons of the 2010 dagstuhl seminar, IEEE Communications Magazine 49 (5) (2011) 158–164.
4. B. Wiedersheim, Z. Ma, F. Kargl, 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, WONS'10, IEEE Press, Piscataway, NJ, USA, 2010, pp. 176–183.
5. D. Eckhoff, R. German, C. Sommer, F. Dressler, T. Gansen, Slotswap: Strong and affordable location privacy in intelligent transportation systems, IEEE Communications Magazine 49 (11) (2011) 126–133.
6. Ieee draft standard for wireless access in vehicular environments - security services for applications and management messages, IEEE P1609.2/D12, January 2012 (2012) 1–266.
7. J. Benin, M. Nowatkowski, H. Owen, Unified pseudonym distribution in vanets, in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on, IEEE, 2010, pp. 529–533.
8. M. Raya, J. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1) (2007) 39–68.
9. E. Schoch, F. Kargl, T. Leinmller, S. Schlott, 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, ESAS'06, Springer-Verlag, 2006, pp. 43–57.
10. A. Boualouache, 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, IEEE, 2014, pp. 70–75.
11. A. Boualouache, S. Moussaoui, Urban pseudonym changing strategy for location privacy in vanets, International Journal of Ad Hoc and Ubiquitous Computing, inderscience (2016) (in press).
12. Z. Ma, F. Kargl, 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.
13. G. M. N. Ali, E. Chan, W. Li, On scheduling data access with cooperative load balancing in vehicular ad hoc networks (vanets), The Journal of Supercomputing 67 (2) (2014) 438–468.
14. J. Benin, M. Nowatkowski, H. Owen, Vehicular network pseudonym distribution in congested urban environments", in: Southeastcon, 2012 Proceedings of IEEE, IEEE, 2012, pp. 1–5".
15. G. Yan, S. Olariu, J. Wang, S. Arif, Towards providing scalable and robust privacy in vehicular networks, Parallel and Distributed Systems, IEEE Transactions on 25 (7) (2014) 1896–1906.
16. C. Sommer, R. German, F. Dressler, Bidirectionally coupled network and road traffic simulation for improved ivc analysis, IEEE Transactions on Mobile Computing 10 (1) (2011) 3–15.
17. D. Krajzewicz, J. Erdmann, M. Behrisch, L. Bieker, Recent development and applications of sumo simulation of urban mobility, International Journal on Advances in Systems and Measurements 5 (3) (2012) 128–138.