Mobile Netw Appl (2010) 15:172–185
DOI 10.1007/s11036-009-0175-4

REP: Location Privacy for VANETs Using Random Encryption Periods

Albert Wasef · Xuemin (Sherman) Shen

Published online: 27 May 2009

Abstract It is well recognized that security is vital for reliable operation of vehicular ad-hoc networks (VANETs). Location privacy is one of the main security challenges in VANETs, which is concerned with preventing an attacker from tracking a specific vehicle. In this paper, we propose a novel location privacy preservation scheme for VANETs using random encryption periods (REP). REP is based on a privacy preserving group communication protocol, which has a conditional full statelessness property. In addition, REP ensures that the requirements to track a vehicle are always violated. By conducting detailed analysis and simulation, REP is demonstrated to be reliable, efficient, and scalable.

Keywords VANETs · security · location privacy

1 Introduction

Recently vehicular ad-hoc networks (VANETs) have become a hot spot as a promising technology for increasing the efficiency and the safety levels of the transportation systems. VANETs consist of network entities, mainly including vehicles and road-side infrastructure units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are two basic vehicular communication modes, which respectively allow vehicles to communicate with each other or with the roadside infrastructure.

Due to the open essence of wireless communications and the high-speed mobility of large number of vehicles in spontaneous vehicular communications, message authentication, integrity, and non-repudiation, as well as privacy preservation are identified as the primary security requirements. Privacy is mainly related to protecting the real identity and location information of the drivers. Any external eavesdropper should be kept from neither recognizing the real identity of the driver nor tracking a specific vehicle [1–7].

One possible solution to protect the real identity of the drivers is to provide each vehicle with a set of anonymous digital certificates. Each vehicle periodically changes its anonymous certificate to mislead attackers. However, those anonymous certificates cannot guarantee location privacy for VANETs.

According to the Dedicated Short Range Communications (DSRC) specifications [8], each vehicle periodically broadcasts a message every 300 ms. Those messages are not intended to a specific vehicle, but multicasted to neighboring vehicles on the road. Unfortunately, the multicasted messages contain critical information such as location, speed, and direction of the transmitting vehicle. An adversary can manipulate this information to track a vehicle even if anonymous certificates are employed. For example, an eavesdropper can use the current location of a targeted vehicle and its current speed to calculate the expected time for receiving another message from the same vehicle at another location on the road. Even if the targeted vehicle changed its anonymous certificate, the eavesdropper may still able to track it. One possible solution to achieve location privacy for VANETs is to prevent

A. Wasef (✉) · X. (Sherman) Shen
Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Ontario, Canada
e-mail: awasef@bbcr.uwaterloo.ca

X. (Sherman) Shen
e-mail: xshen@bbcr.uwaterloo.ca

attackers from gaining any useful information from the multicasted messages. Group communication is one of the promising approaches to achieve such goal [6, 9]. However, the most challenging issue in any group communications protocol for vehicular networks is how to update the group key in a secure and reliable way.

Most of the existing works of group key update for ad hoc networks [10–14] take neither the mobility nor the privacy of nodes into account. The group key update works in [15, 16] are the only ones that consider the mobility of nodes. However, how to preserve the privacy of drivers is overlooked in the existing works.

In this paper, we propose a novel location privacy scheme for VANETs based on random encryption periods (REP) and privacy preserving group communications protocol. The proposed location privacy scheme relies on a probabilistic key distribution approach and a security threshold scheme. Moreover, it provides an efficient and scalable group communications while having conditional full statelessness property. Given that the number of the revoked nodes does not exceed a certain number, each vehicle can calculate the new group key and update its revoked keys even if it misses some previous group rekeying processes. By combining the proposed group communication protocol and random encryption periods, we achieve a salient location privacy for VANETs.

The remainder of the paper is organized as follows. In Section 2, the related work is discussed. Section 3 presents some preliminaries. The proposed REP is introduced in Section 4. REP performance is analyzed in Section 5. Section 6 concludes the paper.

2 Related work

There are several proposals in the literature addressing the problems of location privacy and group communication in VANETs. Sampigethaya et al. [6] combine random silent periods and group communications to achieve location privacy in VANETs excluding safety-related applications. Each group of neighboring vehicles forms a communication group, where the group leader acts as a proxy to all the group members. Combined group communications and random silent periods help in reducing the number of messages broadcasted by the vehicles, hence, reducing the probability of being tracked. During the formation of a new group, there is a need to contact with a central registration authority. Hence, the proposed technique requires an online registration authority. Such requirement may not be feasible in a large scale network like VANET. In addition, when a vehicle updates its pseudonym, it has to leave the group and send a request to the group leader to rejoin the group. This may cause a large number of joining requests.

Freudiger et al. [9] use Cryptographic MIX-zones (CMIXes) at selected road intersections to provide location privacy. In CMIXes, an RSU at an intersection securely provides a symmetric key to any approaching vehicle to establish what is called mix zone. All the data exchanged in a mix zone are encrypted by that symmetric key. In addition, all the vehicles in the mix zone are forced to change their anonymous certificates. As a result of the forced certificate change and the random direction change of each vehicle at road intersections, an attacker on the roadside cannot link a certificate to a particular vehicle, hence, providing location privacy. The accumulation of CMIXes throughout the vehicular network forms what is called mix-network, which maximizes the degree of the location privacy.

Wasef et al. [17] propose an Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV) based on a Public Key Infrastructure (PKI). In ECMV, each node has a short-lifetime certificate, which can be updated from any RSU. The scheme depends on frequent update of the certificates to provide privacy-preserving authentication.

Kaya et al. [10] adopt the Public Key Infrastructure (PKI) to establish group communications. In this protocol, each node possesses a unique certificate, which is used for authentication. The GPS location information of nodes is used to connect new nodes to the physically closest node. In this way, the communication cost is reduced by localizing the group operation. The main drawback of this protocol is the increased computation cost because at each hop the received message has to be decrypted and re-encrypted before being forwarded to the next hop. In [11], Chiang et al. establish group key protocol by exploiting the Group Diffie-Hellman (GDH) protocol [12] and flooding the network with the GPS location information of each node to construct a multicast tree. The main disadvantage of the protocol is the high cost of the GPS information dissemination and the GDH calculations.

The probabilistic approach is a promising technique for the key management in ad hoc networks [13, 14]. Zhu et al. [15] use the probabilistic approach to establish a pairwise key between the network nodes. Later, they introduce the GKMPAN protocol [16], which is considered the most complete work in the context of key management for ad hoc networks. The GKMPAN adopts a probabilistic key distribution approach, which is based on pre-deployed symmetric keys. The GKMPAN is efficient and scalable for wireless mobile networks because it takes node mobility

into consideration. In addition, GKMPAN is dependent neither on the topology of the network nor the node location. GKMPAN has a partial statelessness property, where a node that missed certain number of group rekeying processes can compute the new group key. However, it cannot update the revoked keys corresponding to previously missed rekeying processes. As the number of the non-updated revoked keys increases, it may be necessary for the node to contact the Key Distribution Center (KDC) to reload a new set of keys. Although the GKMPAN protocol has many attractive features, it does not consider privacy preservation of nodes. At some point during the group rekeying process, it may be necessary for a node to transmit its ID clearly. In this way, an attacker can easily track a specific node, which is considered a serious violation of the privacy of the drivers.

In this paper, based on a novel group communication protocol, we propose REP. The proposed group communication protocol adopts a probabilistic key distribution. Also, it preserves the privacy of drivers during the group key update, and it provides conditional full statelessness property, which enables each vehicle to calculate the new group key and update its revoked keys even if it misses some previous group rekeying processes, provided that the number of the revoked nodes in the missed rekeying processes does not exceed a certain number. Finally, it is combined with random encryption periods to provide robust location privacy preservation.

3 Preliminaries

3.1 System model

As shown in Fig. 1, the system model under consideration consists of the following.

- A Trusted Authority (TA), which is responsible for providing anonymous certificates, and distributing symmetric keys to all vehicles in the network;
- Roadside Units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA;
- On-Board Units (OBUs), which can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

It should be noted that the system model under consideration is mainly a PKI system, where each OBU has a set of short-lifetime certificates used to secure its communication with other entities in the network. Also, each OBU is pre-loaded with a set of symmetric keys. Those symmetric keys are necessary for the proposed group communications protocol. Finally, we consider that a revoked OBU is instantly detected by the TA.

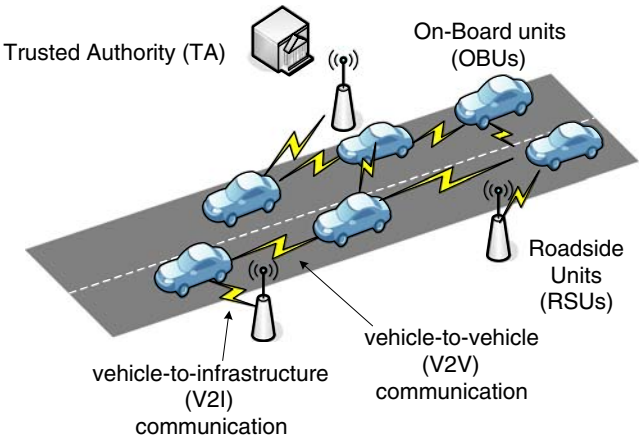


Fig. 1 The system model

3.2 Threat model

We consider an external passive global observer, which can overhear and correlate any message broadcasted in clear in the network. The anonymity set is defined as the set of all possible OBUs which simultaneously change their anonymous certificate between two observation points controlled by an attacker [18]. Consider an OBU moving between two observation points controlled by the global observer as shown in Fig. 2 [1]. The observer can track an OBU if two anonymous certificates can be correctly correlated. This correlation can be achieved by capturing at least one message at each observation point from the OBU, while it is moving with the same speed and in the same lane for some distance between observation points controlled by the observer. For example, a message is captured at the first observation point from an OBU moving with speed v, in lane L, and using anonymous certificate $cert1$. Given the speed of the OBU and the distance between the two observation points, the observer can expect the time to receive a message from that OBU at the second observation point, say after time t. If a

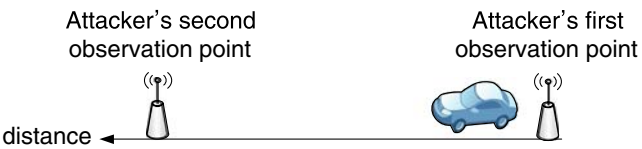


Fig. 2 The threat model

message is captured at the second observation point after time t from an OBU moving with the same speed v, in lane L, and using anonymous certificate $cert2$, the observer can conclude that $cert1$ and $cert2$ belong to the same OBU. Also, if the OBU under attack is the only OBU, which changes its certificate in the area between the two observation points, i.e., it has anonymity set size equals one, the observer can track that OBU even if it changes its speed or lane. It can be seen from the threat model that location privacy can be achieved only if the anonymity set size is greater than one and the OBUs, which changed their certificates, change their speeds and/or their lane locations. In addition, it can be seen that periodically changing the anonymous certificate of each OBU in PKI security architectures is insufficient to provide location privacy for VANETs. Consequently, PKI architectures should be combined with other methods to achieve robust location privacy. In this paper, we use symmetric keys to provide location privacy for VANETs with PKI architecture.

4 The proposed scheme

We consider a PKI system combined with a probabilistic symmetric key distribution. Each OBU has a set of anonymous certificates used to achieve authentication, non-repudiation, and liability. According to the previous threat model, although each OBU periodically changes its anonymous certificate to protect its privacy, it still can be tracked by a global observer. To overcome this tracking attack, each OBU is loaded with a set of symmetric keys used to provide a shared secret key between all legitimate OBUs. When an OBU needs to change its certificate, it uses the shared secret key to surround itself by an encrypted zone with the aid of its neighboring OBUs. Throughout the rest of the paper the notion id is used to denote a symmetric key identity, and the notion ID is used to denote an OBU identity.

4.1 System initialization

The TA issues a set of anonymous certificates for each OBU. Each anonymous certificate contains a pseudo ID (PID). For each OBU, its PID is a function in its real ID. Only the TA can relate PID to the real ID of an OBU. Each OBU periodically changes its anonymous certificate to reduce the probability of being tracked. Moreover, each OBU can update its certificate either from the TA or from any RSU as in [17].

The TA also has a symmetric key pool P, which consists of l keys. Each OBU in the network randomly picks from the key pool a set of keys R, consisting of m distinct keys. In addition, an initial group key k_g is loaded in each OBU. Moreover, the TA authenticates the revocation messages, broadcasted to revoke an OBU, using digital signature. For the sake of intermediate key regeneration (to be discussed later), we use (t, n) threshold scheme [19, 20], where n is the total number of participants, and t is the minimum number of participants that can collude to reveal the shared secret. The TA chooses a large prime P_{TA}, and a polynomial of degree $t-1$ as follows:

$$f_{\mathrm{thresh}}(x) = \left(a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}\right) \bmod P_{\mathrm{TA}} \tag{1}$$

where $(a_0, a_1, a_2, \cdots, a_{t-1}) \in \mathbb{Z}^*_{P_{\mathrm{TA}}}$, and $\mathbb{Z}^*_{P_{\mathrm{TA}}}$ is a finite multiplicative group with its elements relatively prime to P_{TA}.

The TA also selects a set of deterministic functions $(g_1, g_2, \cdots, g_{t-1})$, which are used to generate the coefficients $(a_0, a_1, a_2, \cdots, a_{t-1})$. Finally, each OBU is loaded with P_{TA} and the set $(g_1, g_2, \cdots, g_{t-1})$.

By the end of the system initialization phase, each OBU should have the following:

- A set of anonymous certificates;
- A set of m symmetric keys;
- An initial group key k_g;
- A set of deterministic functions $(g_1, g_2, \cdots, g_{t-1})$;
- The numbers P_{TA} and t.

It should be noted that the TA records a database of the symmetric key set loaded in each OBU. Also, each symmetric key has a unique id. All the OBUs are not allowed to reveal the real values of the symmetric keys loaded in them, however, they can reveal only some keys ids at a time. In addition, it should be noted that the group key k_g is not used to permanently encrypt the communications between OBUs, but it is used to encrypt the communications between a group of neighboring OBUs for random periods as it will be discussed in the next section.

4.2 Random encryption periods

From the threat model previously discussed, location privacy can be achieved only if the anonymity set size of the OBUs changing their certificates is greater than one, and those OBUs change their speeds and/or their lane locations. The main idea of the proposed random encryption periods is to provide location privacy for an OBU changing its certificate by ensuring that the aforementioned conditions are met. Random encryption period is triggered when an OBU needs to change

its certificate. The random encryption period uses the secret group key k_g, shared between all the OBUs, to create an encryption zone around the OBU which needs to change its certificate as follows:

- Any OBU_i, before changing its certificate, sends a message $\text{msg} = \{\text{request}_{\text{REP}}||\text{PID}_i||T_{\text{REP}}\}$ to its neighbors moving in the same direction to announce itself as the random encryption period coordinator, where $\text{request}_{\text{REP}}$ is a request to start a random encryption period in the transmission range of OBU_i, PID_i is the pseudo ID of OBU_i, and T_{REP} is a random time specifying the encryption duration;
- All the OBUs receiving msg start encrypting their broadcasted messages using the group key k_g. We term the OBUs encrypting their messages as the encryption group;
- After encryption starts, OBU_i starts monitoring all the OBUs in the encryption group. Also, it changes its certificate;
- Any OBU in the encryption group checks the remaining validity period of its current certificate. If the remaining validity period is less than T_{REP}, it changes its certificate immediately;
- OBU_i monitors the encryption group for the following conditions:

  1. more than one OBU in the encryption group change their certificates;
  2. the OBUs which changed their certificates change their speeds;
  3. the OBUs which changed their certificates change their lanes or directions;

  If the first condition and either the second or the third condition is met by the end of T_{REP}, OBU_i terminates the encryption period by broadcasting a message informing the encryption group to stop encrypting their messages. It should be noted that the required anonymity set size can be increased in the first condition to increase the location privacy level;
- If the conditions to terminate the encryption period are not met before T_{REP}, OBU_i broadcasts another msg requesting to extend the encryption period.

It should be noted that any legitimate OBU outside the encryption group can decrypt the received messages since it has k_g. Also, it can be seen that random encryption period prevents the global observer from overhearing messages in the areas where a certificate update takes place, hence, decreasing the probability of tracking an OBU.

4.3 Revocation

The revocation is triggered by the TA when there is an OBU_u to be revoked. The certificates of OBU_u must be revoked. In addition, the symmetric key set R_u of OBU_u and the current group key k_g are considered revoked. Hence, each non-revoked OBU should securely update its symmetric key set. Also, a new group key should be distributed to all the non-revoked OBUs. In other words, a group rekeying should be securely performed.

4.3.1 Group rekeying

Assume an OBU_v needs to update its symmetric key set R_v and gets the new group key. The proposed group rekeying is based on [16], and described as follows:

- The TA searches its database to determine the id (M) of the non-revoked symmetric key that is shared by the majority of the non-revoked OBUs. After that, it generates an intermediate key $k_{\text{im}} = f_{k_M}(k_g)$ and a new group key $k_g^{\setminus} = f_{k_{\text{im}}}(0)$, where f_k is a family of pseudo-random functions. Finally, it broadcasts a revocation message containing the certificate of OBU_u to be revoked, M, the ids of the symmetric keys loaded in OBU_u, and $f_{k_g^{\setminus}}(0)$. This message is digitally signed by the private key of the TA;
- After receiving the revocation message, each OBU verifies the received message, and if it has k_M, the OBU computes the intermediate key k_{im} independently;
- If any OBU_v does not have the key k_M, it randomly selects r keys from its symmetric key set R_v, and broadcasts the ids of the selected keys to the neighboring OBUs. Moreover, it starts a timer $T1$;
- Each OBU of the neighbors of OBU_v searches its key set to find a shared key with OBU_v. If any OBU of the neighboring OBUs finds a shared key, it uses this shared key to encrypt the intermediate key k_{im}, and it sends the encrypted k_{im} to OBU_v;
- If the timer $T1$ is timed out without receiving the required data, OBU_v selects a different r keys from its key set R_v, and it retries again;
- If OBU_v receives the data necessary to update its keys, it computes the new group key $k_g^{\setminus} = f_{k_{\text{im}}}(0)$. In addition, it verifies the calculated group key $k_g^{\setminus}$ by checking if $f_{k_g^{\setminus}}(0)$ equal to that in the received revocation message or no. The revoked OBU_u cannot compute $k_g^{\setminus}$ since it does not have k_M. Also, it cannot receive k_{im} from others since the revocation

message contains the ID of OBU_u, which stops others from forwarding k_{im} to it;
- After generating the new group key, each OBU performs an update process to all the keys in its symmetric key set. For example, OBU_v updates every key k_i in its key set as

$$k_i^{\backslash} = f_{k_i}(0) \qquad \forall\, k_i \in R_v \tag{2}$$

- If an OBU has a revoked key, i.e., $k_i \in R_u$, an additional update process must be performed as follows: $k_i^{\backslash} = f_{k_{im}}(k_i^{\backslash})$;
- After updating its symmetric key set, each OBU sets $a_0 = k_{im}$ in Eq. 1, and uses k_{im} as the input to the set of deterministic functions $(g_1, g_2, \cdots, g_{t-1})$ to obtain $(a_1, a_2, \cdots, a_{t-1})$, respectively. In addition, each OBU generates a random number rnd $\in \mathbb{Z}^*_{p_{TA}}$, and it calculates $f_{thresh}(rnd)$ as in Eq. 1. The shadow generation process is shown in Fig. 3. After that, it saves the shadow (rnd, $f_{thresh}(rnd)$) and the timestamp corresponding to the start of the rekeying process. Finally, it erases k_{im}, $(a_1, a_2, \cdots a_{t-1})$, and the original k_i's.

Each OBU counts the number of the revoked OBUs since its shadow is generated. If the number of revoked OBUs equals $t-1$, all the OBUs must erase the corresponding shadow to prevent the revoked OBUs from colluding and regenerating the corresponding intermediate key.

It is clear that OBU_v, which does not have k_M, cannot be tracked since at each try to get k_{im}, it only sends a different collection of r keys identities to the neighboring OBUs. In addition, OBU_v does not send any ID or certificate during its trials to get k_{im}. Consequently, the proposed group communication protocol preserves the privacy of the OBUs.

The intermediate key is sent over channels secured by non-revoked keys. Consequently, the revoked OBU_u cannot get k_{im} since the ids of the symmetric keys loaded in the revoked OBU_u are sent in the revocation message. It should be noted that after each OBU updates its symmetric key set, the value of each symmetric key is changed, however, the ids of all the symmetric keys do not change. Consequently, the TA can still know the symmetric keys loaded in each OBU.

By the end of the group rekeying process, all the non-revoked OBUs should update their group key from k_g to $k_g^{\backslash}$, and their symmetric key sets. Also, each non-revoked OBU should store a shadow (rnd, $f_{thresh}(rnd)$).

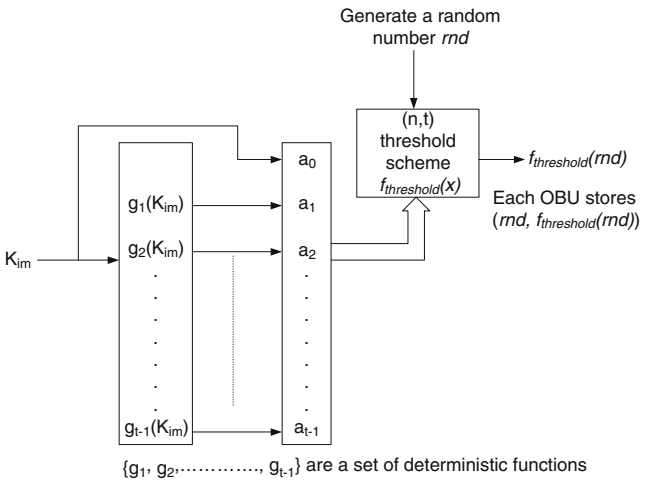


Fig. 3 The shadow generation process

4.4 Intermediate key regeneration

If any OBU_y misses a rekeying process, it has to regenerate the corresponding intermediate key to get the new group key and to update its revoked keys as follows:

- OBU_y selects r keys from its symmetric key set, and it broadcasts an intermediate key request, the selected keys ids, and the timestamp corresponding to the last successfully performed rekeying process;
- Any OBU receiving that message verifies that the ids of those r keys are not revoked. In addition, it compares the request timestamp with the timestamps corresponding to each rekeying process to determine the specific shadows to be sent. After that, it encrypts those shadows with the current group key $k_g^{\backslash}$ and broadcasts them. It should be noted that the requesting OBU_y does not have $k_g^{\backslash}$, therefore, it cannot decrypt those shadows;
- Any OBU receiving shadows from other OBUs starts its own timer $T2$;
- Any OBU receiving different $t-1$ shadows can now, using the received shadows and its own shadow, regenerate the corresponding intermediate keys and transmit them to OBU_y over channels secured by one of the shared keys between itself and OBU_y. It should be noted that OBU_y can update its non-revoked keys, since it does need any intermediate keys as indicated in Eq. 2. Consequently, there is still a considerable probability of sharing some keys with the neighboring OBUs;

– After receiving all the missed intermediate keys and updating its revoked keys, OBU_y broadcasts a confirmation message encrypted with the new group key $k_g^{\setminus}$;
– Upon receiving the confirmation message, each OBU must erase the received shadows and the regenerated intermediate keys;
– If any OBU, which received shadows from other OBUs, does not receive a confirmation message, it waits until the timer $T2$ is timed out, and it erases all the received shadows and the regenerated intermediate keys.

In this way, any legitimate OBU can recover any missing intermediate keys and update its revoked symmetric keys, provided that the number of the revoked OBUs does not exceed $t-1$ from the beginning of the rekeying process in which the intermediate key was used. Consequently, the proposed group communications has a conditional full statelessness property. In other words, the OBUs should never go to the TA to update their symmetric key sets provided that the number of revoked OBUs does not exceed $t-1$ for any rekeying process.

5 Performance analysis

The notations used throughout the rest of this section are given in Table 1.

5.1 Symmetric key sharing probability

In this section, we calculate the probability of directly sharing a symmetric key between an OBU and its neighboring OBUs. First, P_l and P_n can be calculated as follows:

$$P_l = \begin{cases} \frac{\binom{m-n}{r}}{\binom{m}{r}} & \forall\ 0 \le r \le m-n \\ 0 & \forall\ m-n < r \le m \end{cases} \tag{3}$$

$$\begin{aligned} P_n &= \frac{\binom{l}{m} \cdot \binom{m}{n}\binom{l-m}{m-n}}{\binom{l}{m}^2} \\ &= \frac{\binom{m}{n}\binom{l-m}{m-n}}{\binom{l}{m}} \quad \forall\ n = 0, 1, 2, \cdots, m \end{aligned} \tag{4}$$

then, we can get P_r as follows:

$$\begin{aligned} P_r &= 1 - \sum_{n=0}^{m} (P_l \cdot P_n) \\ &= 1 - \sum_{n=0}^{m-r} \frac{\binom{m-n}{r}}{\binom{m}{r}} \cdot \frac{\binom{m}{n}\binom{l-m}{m-n}}{\binom{l}{m}} \quad \forall\ r = 1, 2, \cdots, m \end{aligned} \tag{5}$$

Table 1 Notations

Symbol	Notation
r	The number of randomly selected keys out of vehicle key set
l	The key pool size of the TA
m	The key set size stored in each vehicle
P_r	The probability that at least one key out of r is directly shared between any pair of nodes
N	The number of the neighboring OBUs of an OBU
P_{rN}	The probability that at least one key out of r is directly shared between an OBU and one of its neighboring OBUs
P_l	The probability that the selected r keys are not shared between any pair of nodes given that n keys are shared between them
P_n	The probability that n keys are shared between any pair of nodes
$P_r(w)$	The probability that at least one key out of r is directly shared between any pair of nodes when w keys revoked simultaneously
$P_{rN}(w)$	The probability that at least one key out of r is directly shared between an OBU and one of its neighboring OBUs when w keys revoked simultaneously
$P_l(w)$	The probability that the selected r keys are not shared between any pair of nodes given that n keys are shared between them when there are w keys revoked simultaneously
$P_n(w)$	The probability that n key are shared between any pair of nodes when there are w keys revoked simultaneously
N_s	The number of safe keys in a OBU
$P_s(k)$	The probability that N_s equals k

Finally, the probability of sharing at least one key with one of the N neighboring OBUs is

$$P_{rN} = 1 - \left(\sum_{n=0}^{m} (P_l \cdot P_n) \right)^N$$
$$= 1 - \left(\sum_{n=0}^{m-r} \frac{\binom{m-n}{r}}{\binom{m}{r}} \cdot \frac{\binom{m}{n}\binom{l-m}{m-n}}{\binom{l}{m}} \right)^N \quad \forall\, r = 1, 2, \cdots, m \tag{6}$$

Figure 4 shows the key sharing probability P_{rN} vs. the number of randomly selected keys r. It can be seen that P_{rN} increases with r, m and N. However, increasing r increases the probability of selecting the same r keys twice, thus, increasing the tracking probability. Also, increasing m increases the vulnerability of the system because the more keys a single OBU has, the more information the attacker can get by compromising a single OBU. Also, it can be seen from Fig. 4 that P_{rN} increases as l decreases. Yet, decreasing l lowers the security level of the system because an attacker gets more information about the key pool l if a few numbers of OBUs are revoked.

From the aforementioned discussion, a tradeoff between the values of l, m, r, and the desired security level should be made to achieve the desired value of P_{rN}.

Figure 5 shows the key sharing probability P_{rN} vs. the number of neighboring OBUs (N). For the cases where $m = 100$ keys, it can be seen that for $N = 30$ OBUs, we achieve P_{rN} higher than 95%, which demonstrates the feasibility of the proposed group communication protocol. According to DSRC, the transmission range of an OBU is around 1 km [8]. If we consider

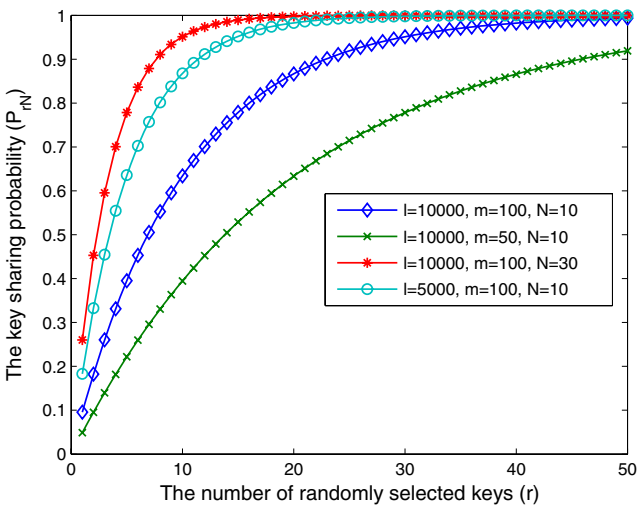


Fig. 4 The impact of changing r on the key sharing probability (P_{rN})

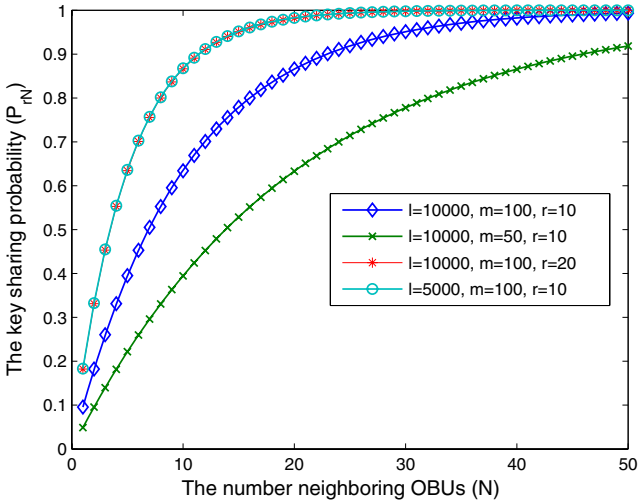


Fig. 5 The impact of changing N on the key sharing probability (P_{rN})

the OBUs moving in both directions, the availability of 30 OBUs within the transmission range of an OBU is feasible.

5.2 Impact of the number of revoked keys

We analyze the effect of simultaneously revoking w symmetric keys on the key sharing probability between an OBU and its neighboring OBUs. $P_l(w)$ and $P_n(w)$ can be calculated as follows:

$$P_l(w) = P_l = \begin{cases} \frac{\binom{m-n}{r}}{\binom{m}{r}} & \forall\, 0 \le r \le m-n \\ 0 & \forall\, m-n < r \le m \end{cases} \tag{7}$$

$$P_n(w) = \sum_{k=n}^{m} P_n(w/N_s = k) \cdot P_s(k)$$
$$= \sum_{k=n}^{m} \frac{\binom{k}{n}\binom{l-k}{m-n} \cdot \binom{l-w}{k}\binom{w}{m-k}}{\binom{l}{m}^2}$$
$$\forall\, n = 0, 1, \cdots, m, \forall\, w = m, m+1, \cdots, l-m \tag{8}$$

then, we get $P_r(w)$:

$$P_r(w) = 1 - \sum_{n=0}^{m} (P_l(w) \cdot P_n(w))$$
$$= 1 - \sum_{n=0}^{m-r} \sum_{k=n}^{m} \frac{\binom{m-n}{r} \cdot \binom{k}{n}\binom{l-k}{m-n} \cdot \binom{l-w}{k}\binom{w}{m-k}}{\binom{m}{r} \cdot \binom{l}{m}^2}$$
$$\forall\, w = m, m+1, \cdots, l-m, \forall\, r = 1, 2, \cdots, m \tag{9}$$

Finally, $P_{rN}(w)$ can be calculated as follows:

$$P_{rN}(w) = 1 - \left(\sum_{n=0}^{m} (P_l(w) \cdot P_n(w)) \right)^N$$

$$= 1 - \left(\sum_{n=0}^{m-r} \sum_{k=n}^{m} \frac{\binom{m-n}{r} \cdot \binom{k}{n} \binom{l-k}{m-n} \cdot \binom{l-w}{k} \binom{w}{m-k}}{\binom{m}{r} \cdot \binom{l}{m}^2} \right)^N$$

$$\forall\, w = m, m+1, \cdots, l-m, \forall\, r = 1, 2, \cdots, m \tag{10}$$

Figure 6 shows the key sharing probability $P_{rN}(w)$ vs. the number of simultaneously revoked keys (w). It can be seen that $P_{rN}(w)$ decreases as w increases. In addition, if l, m, and r are properly selected, the proposed group communication protocol can still perform well even if a relatively large number of keys, compared to the key pool size l, is simultaneously revoked. Consequently, the proposed group communication protocol is robust and reliable.

5.3 Intermediate key regeneration delay

In vehicular networks, the longest transmission delay (T_{delay}) equals 6.47 ms [21]. Let $T_{\text{intermediate}}$ denote the duration between an OBU sending a request to regenerate an intermediate key and the reception of the regenerated intermediate key. Also, let $T_{\text{threshold}}$ denote the time required to regenerate the intermediate key from t shadows. We implement the threshold scheme in Eq. 1 using Matlab. Based on Fig. 5, the value of t is selected to be 30 participants, which ensures high key sharing probability. The implementation is executed on an Intel Centrino Cor2Duo 2.0 GHz machine. Based on our implementation, we have $T_{\text{threshold}} = 1$ ms. For an OBU to regenerate an intermediate key, it has to broadcast a request for key regeneration which takes T_{delay}. In addition, we consider the time required for any OBU sharing in the regeneration process to receive t shadows equal to $2T_{\text{delay}}$ to account for the time shifts between different transmissions. Furthermore, the OBU, which regenerates the intermediate key, needs T_{delay} to deliver the regenerated intermediate key to the requesting OBU. Consequently, we have

$$T_{\text{intermediate}} = 4T_{\text{delay}} + T_{\text{threshold}} = 26.88 \text{ ms}$$

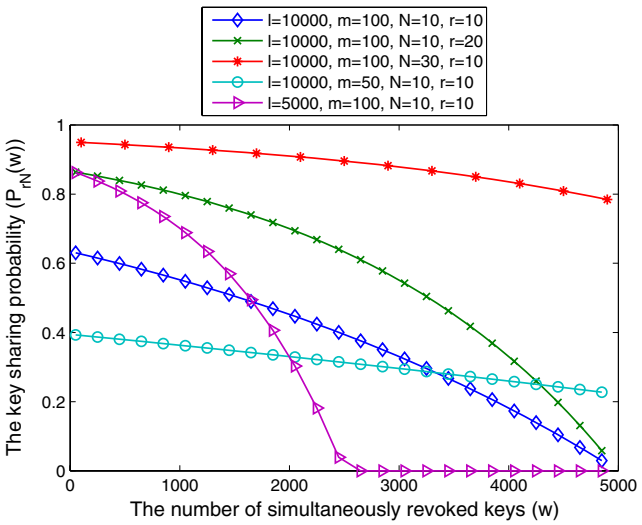


Fig. 6 The effect of key revocation on the key sharing probability ($P_{rN}(w)$)

5.4 Computations complexity

In this section, we evaluate the computation complexity imposed by the REP protocol on an OBU, which is mainly due to the shadows generations and intermediate key regeneration in the group rekeying process.

The computation complexity incurred in the shadows generations is mainly due to the modular exponentiation in Eq. 1. Consequently, the computation complexity of a shadow generation incurred by an OBU is $O(t \log^3(P_{\text{TA}}))$ bit operations, where $log(P_{\text{TA}})$ is the size of each variable in Eq. 1. Since t is constant in the (t, n) threshold scheme previously discussed, an algorithm of computation complexity $O(t \log^3(P_{\text{TA}}))$ can run efficiently in polynomial time. In addition, the shadow generation is done offline, i.e., there is no time constraint on the shadows generation. Consequently, the delay due to the shadows generation has no effect on the performance of the proposed protocol.

The computation complexity of the intermediate key regeneration is mainly due to reconstructing an intermediate key from t shadows according to the (t, n) threshold scheme previously discussed. In [19], it is shown that the computation complexity of reconstructing a secret value from t shadows using Lagrange polynomial interpolation requires $O(t \log^2(P_{\text{TA}}))$ bit operations. Since t is constant, $O(t \log^2(P_{\text{TA}}))$ algorithms can run efficiently in a polynomial time by the currently available computers. Moreover, since OBUs in vehicular networks are continuously self-charging their batteries, they do not suffer from the power limitation which is common to ad hoc networks. From the aforementioned discussion, it can be seen from the computational complexity point of view that REP is feasible since the additional computation complexity imposed by REP can be efficiently computed by the OBUs.

5.5 Simulation

In this section, we evaluate the communication cost for the group rekeying and the achieved anonymity set size under REP.

5.5.1 Group rekeying communication cost

We are interested in the group rekeying communication cost, which is defined as the average number of symmetric keys an OBU has to transmit and receive during the group rekeying process.

We simulate a highway and Manhattan mobility models using Matlab. The simulation parameters are given in Table 2. In each mobility model, OBUs arrive according to a Poisson random process, where the arriving OBU randomly selects an entry port from predefined entry ports. When an OBU reaches one of the output entries, it disappears. The highway model consists of 6 lanes (3 in each direction). For the Manhattan mobility model shown in Fig. 7, each street consists of 4 lanes (2 in each direction). At each intersection, each OBU has a probability of 25% to turn right or left. In this simulation, we only consider the case that an OBU, which does not have k_M, can get the intermediate key from another OBU through a single hop.

Figure 8 shows the average communications cost vs. the number of simultaneously revoked OBUs for the highway and Manhattan mobility models. It can be seen from the low average communications costs for the highway and Manhattan models that the proposed protocol is feasible and reliable. Also, the average communication cost for the Manhattan model is lower than the highway model, as in the Manhattan model the OBUs arrival rate is higher than that of the highway model. As a result, the total number of OBUs in the Manhattan simulation area is higher than that of the highway model, which results in decreasing the average communication cost for each OBU. Figure 9 shows the average number of trials the OBUs perform to get the intermediate key vs. the number of simultaneously revoked OBUs for the highway and Manhattan mobility models. It can be seen that for the highway model the average number of trials is almost one. Also, the average number of trials for the Manhattan model is higher than that of the highway model as the Manhattan OBUs density is low compared to that of the highway model.

Table 2 Simulation parameters

Simulation parameter	Highway model	Manhattan model
l	10000	10000
m	100	100
r	10	10
Road length (km)	3	3×3
Arrival rate (/ms)	0.01	0.05
OBUs speed(km/h)	80	50
Simulation time (min)	4	6

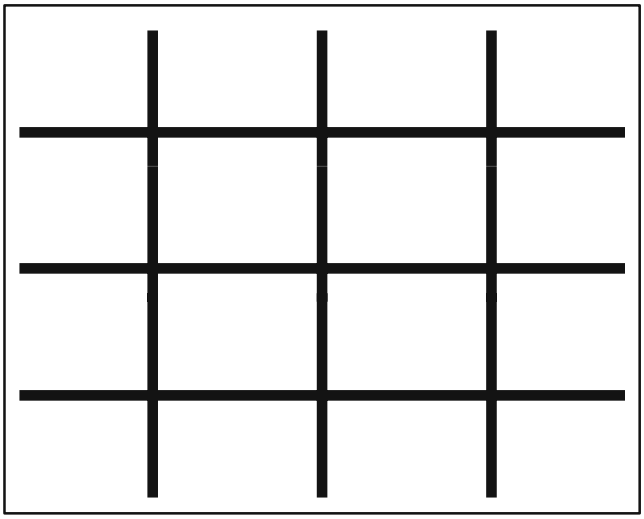


Fig. 7 Manhattan road model

5.5.2 Anonymity set size

We use the highway and Manhattan mobility models to investigate the achieved average anonymity set size using REP. Each OBU has a probability of 10% to change its certificate every 300 ms. Also, we consider that the criteria to terminate the encryption period is that the anonymity set size is greater than one. Figures 10,

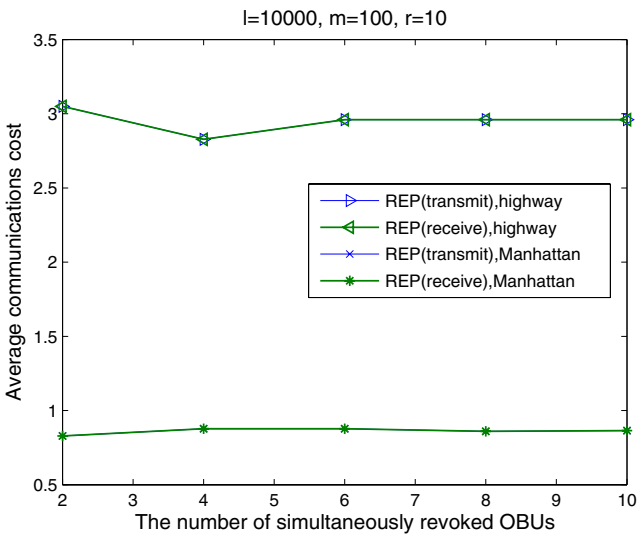


Fig. 8 The average communication cost

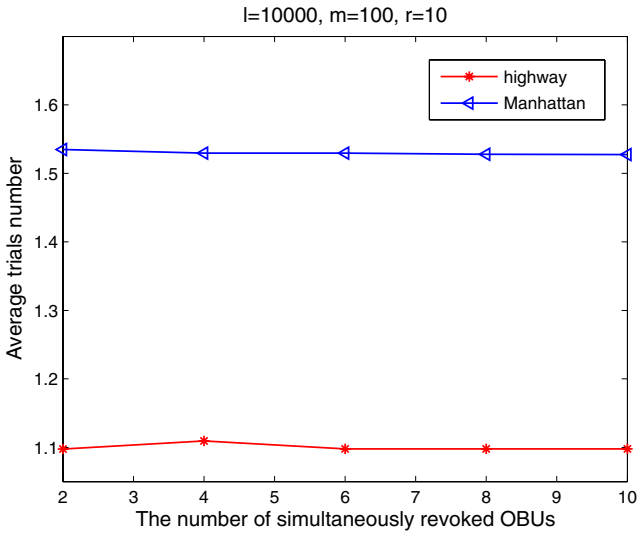


Fig. 9 The average number of trials

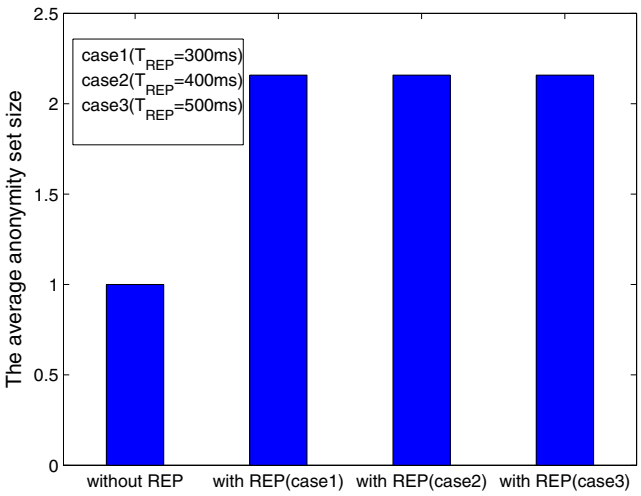


Fig. 11 The average anonymity set size for Manhattan mobility model

11, 12, 13, 14 and 15 show the average anonymity set size, the average REP duration, and the ratio between the number of anonymity sets of different sizes to the total number of anonymity sets for the highway and Manhattan mobility models, respectively. In Figs. 10–11, we compare the average anonymity set size with and without REP. Also, we simulate REP for three cases corresponding to initial T_{REP} values of 300, 400, and 500 ms, respectively. It can be seen that without using REP (which is the current normal mode of VANETs), the average anonymity set size is one since the global observer can capture all the broadcasted messages. As a result, the location privacy of drivers is vulnerable to the tracking attack previously discussed.

In addition, it can be seen that with using REP, the average anonymity set size is always greater than two, which decreases the probability of being tracked by a global observer. Also, the average anonymity set size for the highway model is higher than that for the Manhattan model. The reason can be explained as follows. First, although the arrival rate for the Manhattan model is higher than that for the highway model, the arriving OBUs are distributed between 6 streets (4 lanes each, i.e., 24 lanes) for the Manhattan model, while the arriving OBUs are distributed between 6 lanes in the highway model. Second, the simulation area for the Manhattan model is larger than that for the highway model. From the aforementioned explanation, the OBUs density in the Manhattan model is lower than that in the highway model.

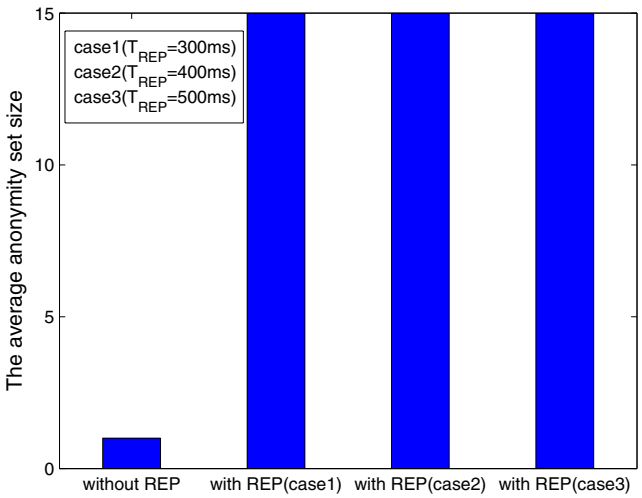


Fig. 10 The average anonymity set size for highway mobility model

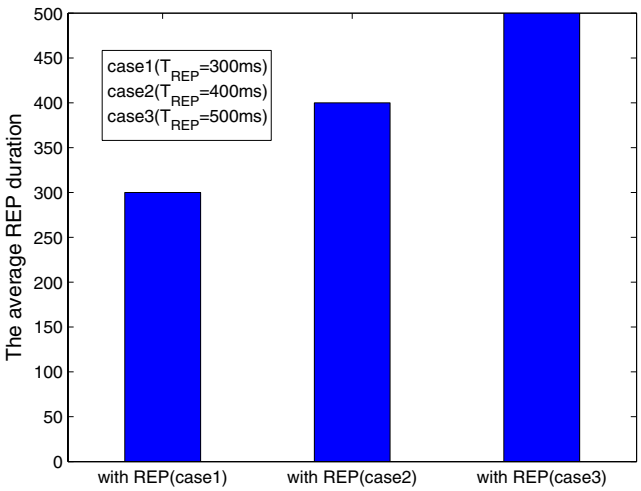


Fig. 12 The average REP duration for highway mobility model

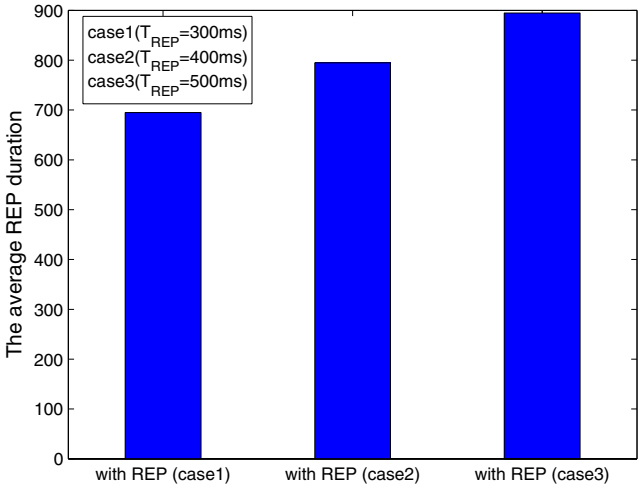


Fig. 13 The average REP duration for Manhattan mobility model

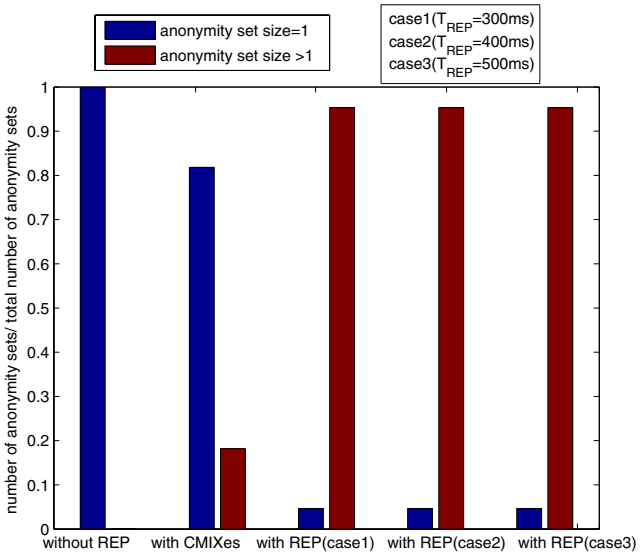


Fig. 15 The impact of REP on the anonymity set size for Manhattan mobility model

It can be seen from Figs. 12–13 that the average REP duration for the highway model is almost the initial value of T_{REP}. Also, the average REP duration for the Manhattan model is higher than that for the highway model as the OBUs density in the Manhattan model is less than that for the highway model. Hence, the OBUs in the Manhattan model needs more than one T_{REP} to have anonymity set size greater than one.

Figures 14–15 show the ratio between the anonymity sets of different sizes and the total number of anonymity sets. For both Manhattan model and highway model, it can be seen that without using REP, the anonymity sets of size one are 100% of the total anonymity sets. In addition, when using REP in the highway model, the ratio of the anonymity sets of size greater than one are 100%. For the Manhattan model, when using REP, 95.35% of the total anonymity sets achieves set size greater than one, while 4.65% of the anonymity sets are still having size one by the end of the simulation time.

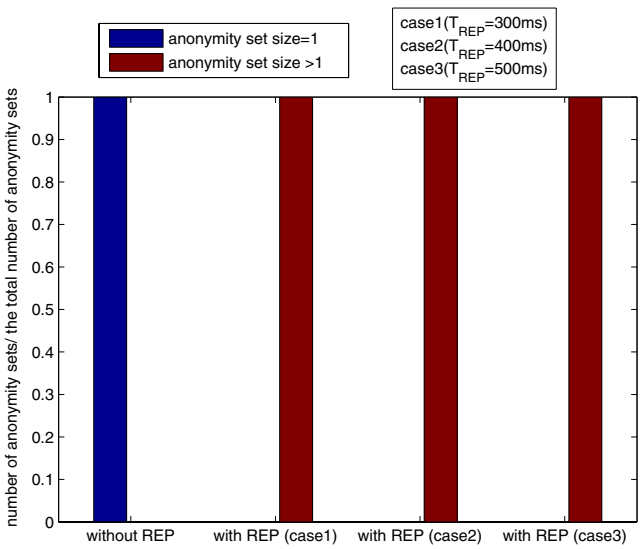


Fig. 14 The impact of REP on the anonymity set size for highway mobility model

Since the work done by Sampigethaya et al. [6] only considers location privacy for non-safety applications in vehicular networks, and REP is mainly used for providing location privacy for safety applications, the only work that can be compared to REP is the Cryptographic MIX-zones (CMIXes) approach [9]. In addition, the authors of CMIXes demonstrate that CMIXes can be applied in a city scenario with the help of RSUs at some selected intersection, however, they do not explain how CMIXes can be applied in a highway scenario. Hence, we only consider CMIXes in the Manhattan model. In the conducted simulation for CMIXes, we consider that there is an RSU with a coverage area of 300 m [8] at each intersection. In addition, when an OBU_i enters the coverage area of an RSU_j at an intersection, it is forced to change its certificate according to [9]. Moreover, we consider all the OBUs within the coverage area of RSU_j to be in the anonymity set of OBU_i. When OBU_i leaves the coverage area of RSU_j, the anonymity set corresponding to OBU_i is terminated, and a new anonymity set is generated at RSU_j for the first OBU enters the coverage area of RSU_j. Figure 15 shows a comparison of the ratio between the anonymity sets of different sizes and the total number of anonymity sets in the Manhattan model

for the case without and with REP, and with CMIXes. It can be seen that for CMIXes, only 18.18% of the total anonymity sets achieves set size greater than one, while 81.82% of the anonymity sets are still having size one by the end of the simulation time, which clearly indicates that the proposed REP protocol outperforms CMIXes.

6 Conclusion

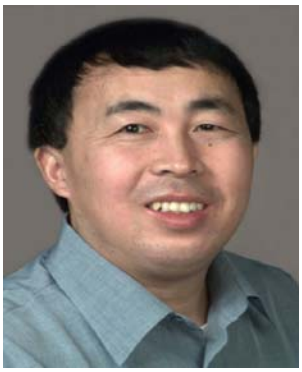
We have proposed REP which provides location privacy for VANETs using random encryption periods. For an OBU changing its certificate, REP triggers encryption zone around the OBU to violate the conditions required to launch a tracking attack, and it creates an ambiguity to any external observer. Extensive analysis and evaluation of REP have been performed to demonstrate its reliability and security. Our future work include providing location privacy against internal malicious OBUs.

Acknowledgement The authors would like to thank Mr. Rongxing Lu for his valuable comments on this work.

References

1. Raya M, Hubaux J-P (2005) The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks, pp 11–21
2. Dötzer F (2006) Privacy issues in vehicular ad hoc networks. In: Proceedings of the 2nd ACM workshop on vehicular ad hoc networks
3. Papadimitratos P, Kung A, Hubaux J-P, Kargl F (2006) Privacy and identity management for vehicular communication systems: a position paper. In: Proceedings of the workshop on standards for privacy in user-centric identity management, Zurich
4. Choi J, Jakobsson M, Wetzel S (2005) Balancing auditability and privacy in vehicular networks. In: Proceedings of the 1st ACM international workshop on quality of service and security in wireless and mobile networks, pp 79–87
5. Sha K, Xi Y, Shi W, Schwiebert L, Zhang T (2006) Adaptive privacy-preserving authentication in vehicular networks. In: Proceedings of the ChinaCom '06, pp 1–8
6. Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K (2005) CARAVAN: providing location privacy for VANET. In: Proceedings of the embedded security in cars (ESCAR)
7. Lin X, Sun X, Ho P-H, Shen X (2007) GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol 56:3442–3456
8. 5.9 GHz DSRC (2002) http://grouper.ieee.org/groups/scc32/dsrc/index.html
9. Freudiger J, Raya M (2007) Mix-zones for location privacy in vehicular networks. In: Proceedings of the WiN-ITS
10. Kaya T, Lin G, Noubir G, Yilmaz A (2003) Secure multicast groups on ad hoc networks. In: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks, pp 94–102
11. Chiang T-C, Huang Y-M (2003) Group keys and the multicast security in ad hoc networks. In: Proceedings of the international conference on parallel processing workshops, pp 385–390
12. Steiner M, Tsudik G, Waidner M (1996) Diffie-Hellman key distribution extended to group communication. In: Proceedings of the 3rd ACM conference on computer and communications security, pp 31–37
13. Chan H, Perrig A, Song D (2003) Random key predistribution schemes for sensor networks. In: Proceedings of the 2003 IEEE symposium on security and privacy, pp 197–213
14. Eschenauer L, Gligor V-D (2002) A key-management scheme for distributed sensor networks. In: Proceedings of the ACM conference on computer and communications security, pp 41–47
15. Zhu S, Xu S, Setia S, Jajodia S (2003) Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach. In: Proceedings of the 11th IEEE international conference on network protocols, pp 326–335
16. Zhu S, Setia S, Xu S, Jajodia S (2006) GKMPAN: an efficient group rekeying scheme for secure multicast in ad-hoc networks. J Comput Secur 14:301–325
17. Wasef A, Jiang Y, Shen X (2008) ECMV: efficient certificate management scheme for vehicular networks. In: Proceedings of the IEEE GLOBECOM 2008
18. Pfitzmann A, KÄhntopp M (2001) Anonymity, unobservability, and pseudonymity- a proposal for terminology. In: Designing privacy enhancing technologies, pp 1–9
19. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
20. Jiang Y, Lin C, Shi M, Shen X (2006) Multiple key sharing and distribution scheme with (n,t) threshold for NEMO group communications. IEEE J Sel Areas Commun 24(9):1738–1747
21. Lu R, Lin X, Zhu H, Ho P-H, Shen X (2008) ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of the INFOCOM 2008, pp 1229–1237

Albert Wasef received the B.Sc. (1998) degree and the M.Sc. (2003) from El Menoufia University (Egypt), both in electrical communications engineering. He is currently working toward his Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Waterloo, Ontario, Canada, where he is working with the Broadband Communications Research (BBCR) Group. His research interest includes wireless network security, privacy preservation in vehicular networks, revocation, and group communications.



Xuemin (Sherman) Shen received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of IEEE Communications Society.