MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks

Yan Zhang, Senior Member, IEEE, Jiawen Kang, Xumin Huang, Shengli Xie, Senior Member, IEEE, Rong Yu, Member, IEEE, Jiawen Kang, Xumin Huang, Shengli Xie, Senior Member, IEEE, and Stein Gjessing, Member, IEEE

Abstract—Vehicular social network (VSN) is envisioned to serve as an essential data sensing, exchanging and processing platform for the future Intelligent Transportation Systems. In this paper, we aim to address the location privacy issue in VSNs. In traditional pseudonym-based solutions, the privacy-preserving strength is mainly dependent on the number of vehicles meeting at the same occasion. We notice that an individual vehicle actually has many chances to meet several other vehicles. In most meeting occasions, there are only few vehicles appearing concurrently. Motivated by these observations, we propose a new privacy-preserving scheme, called MixGroup, which is capable of efficiently exploiting the sparse meeting opportunities for pseudonym changing. By integrating the group signature mechanism, MixGroup constructs extended pseudonym-changing regions, in which vehicles are allowed to successively exchange their pseudonyms. As a consequence, for the tracking adversary, the uncertainty of pseudonym mixture is accumulatively enlarged, and therefore location privacy preservation is considerably improved. We carry out simulations to verify the performance of MixGroup. Results indicate that MixGroup significantly outperforms the existing schemes. In addition, MixGroup is able to achieve favorable performance even in low traffic conditions.

Index Terms—Location privacy, vehicular social network, pseudonym, group signature

1 INTRODUCTION

By leveraging the Dedicated Short Range Communications (DSRC) technology, vehicular networks have become a dispensable data transmission platform and significantly facilitated the realization of Intelligent Transport System (ITS). In vehicular networks, there are vehicles of advanced sensing and communication capability and smart roadside infrastructures of compact computation and storage capability. With the assistance of vehicular Onboard Unit (OBU) and RoadSide Units (RSUs), communications in vehicular networks is resiliently extended to include vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) data exchanges [1], [2]. This scenario has been conventionally depicted as Vehicular Ad hoc Network (VANETs). Prospectively, vehicular networks are envisioned to integrate advanced computing intelligence (e.g., cloud computing) and social networking perspective, to efficiently support vehicle-, road- and traffic-related data sensing, transmitting and processing for ITS applications, and eventually evolve towards the new paradigm of VSNs [3].

Although VSN is expected to have a wide-range applications in future ITS services, there are considerable challenging technical issues. As a crucial data transmitting and processing platform for ITS, VSN should inherently protect security and privacy from cyber physical systems to ITS users [4], [5], [6].

However, for the sake of safety, vehicles are required to periodically broadcast their current position, speed and acceleration in authenticated safety messages to surrounding neighbors. These messages increase the awareness of vehicles about their neighbors’ whereabouts and warn drivers of dangerous situations, which poses potential threats to the location privacy of vehicles. To address the problem, efficient schemes such as Mix-zone [7], [8] and group signature [9] have been proposed for location privacy preservation. The central idea behind these schemes is to create opportunities for vehicles to obscure the eavesdropping of the adversary. However, Mix-zone is limited by the number of vehicles appearing at the pseudonyms changing occasions. Mix-zone may not perform very well in the places of few vehicles or low traffic. The group signature approach is restricted by the group size. A large-scale group has low efficiency in managing the signatures while a small group is weak in preserving privacy.

By observing traces of vehicles, we find that an individual vehicle actually has many chances to meet a lot of other vehicles. However, in most meeting occasions, there are only few vehicles appearing concurrently. This fact implies that, if the vehicle could accumulatively aggregate these meeting occasions together, it has indeed sufficient opportunities for pseudonym mixture. Otherwise, if the vehicle performs pseudonym changing merely at places of crowded neighbors, a major portion of opportunities will be wasted. In this paper, we are motivated to propose
a new privacy-preserving scheme which is capable of efficiently exploiting the potential opportunities for pseudonym mixture. By creating a local group, we construct an extended region with multiple road intersections, in which pseudonyms are allowed to successively take place. Consequently, for the tracking adversary, the uncertainty of pseudonym mixture is accumulatively enlarged, and hence location privacy preservation is substantially improved.

1.1 Related Work
For driving safety, vehicles have to broadcast periodical messages, which consists of 4-tuple information \{Time, Location, Velocity, Content\}. If real identities of vehicles are used in the safety messages, the location privacy will be easily eavesdropped. For this reason, vehicles should use pseudonyms instead of their real identities. However, under a consecutive adversary tracking, the pseudonym scheme is still vulnerable if vehicles keep using identical pseudonyms for a long time. To address this privacy protection problem, previous work have proposed three major types of schemes: 1) Mix-zone, 2) group signature and 3) silent period [10].

The nature of all these schemes is to obscure the mapping relationship between vehicles’ real identities and their fictitious identities.

The concept of Mix-zone is firstly presented in the context of location privacy in [11], and its variants are discussed in [7], [12]. The vehicle uses different pseudonyms to guarantee location privacy by the unlinkability of pseudonyms. However, if a vehicle changes its pseudonyms in an improper occasion, the scheme will fail to protect location privacy. The adversary could still link a new pseudonym with the old one by continuously overhearing the surrounding vehicles and inferring the pseudonym changing. In [7], the Mix-zone constructs an appropriate time and location for vehicles to change their pseudonyms. Typically in intersection of multiple entries, the vehicles are allowed to change their pseudonyms and separately depart from different exits, which achieves the unlinkability of pseudonyms. The road intersections or parking lots can naturally be assigned as Mix-zones [13]. The limitation of Mix-zone scheme is the concurrent appearance of vehicles in a same intersection. In roads with low traffic, the scheme may not perform well.

For the group signature scheme, a vehicle joins a group and signs for messages by using the group identity, and hence protects its location privacy. Only the group leader is the trusted entity, which knows about the true identities of vehicles, and meanwhile has the right to track down any of the group members if necessary. However, if the size of a group is too large [14], it is challenging to manage all the group members efficiently.

For the silent period scheme, a target vehicle entering a region of interest, it initially broadcasts safety messages, then keeps silent and updates its pseudonym for a random silent period during moving from locations $L_1$ to $L_2$, and finally broadcasts in $L_2$. At the same time, if one of its neighboring vehicles happens to update pseudonyms from proximity locations $L_3$ to $L_4$, then the adversary will be misled to treat the neighboring vehicle as the target. The random silent period scheme is efficient in resisting the adversary tracking. However, the maximum silent period is limited by

the safety message broadcast period [15]. With maximum silent period constrained to the order of hundredths of milliseconds, it is still possible to track vehicles by inferring the temporal and spatial relationship of vehicles.

1.2 Contributions and Organization of the Paper
In this paper, we aim to address the problem of location privacy preservation in VSNs. The main contributions of our work are presented as follow.

- First, we have observations on vehicle traces: although there exist social spots crowded by vehicles, each vehicle tends to meet others sporadically and mostly outside the social spots. Following the observations, we propose a new scheme MixGroup, to accumulatively exploit the meeting opportunities for pseudonym changing and improve the location privacy preservation.

- Second, by leveraging group signature, we construct an extended pseudonym-changing region, namely, group-region, in which vehicles are allowed to use group identity instead of pseudonyms, and meanwhile, accumulatively exchange their pseudonyms with each others. The usage of group identity efficiently covers the procedure of pseudonym exchange.

- Third, in order to facilitate the operations of pseudonym exchange among vehicles, we devise an entropy-optimal negotiation procedure. In the procedure, each vehicle will evaluate its benefit and risk in taking part in pseudonym exchange. The benefit and risk during pseudonym exchange are quantitatively measured by the predefined pseudonym entropy.

The rest of this paper is organized as follows. In Section 2, we introduce the network model, threat model and the location privacy requirements. In Section 3, the proposed location privacy-preserving scheme, called MixGroup, is presented. Firstly, two observations from vehicle traces are described. Then, we have a brief overview of MixGroup. After that, the detailed operations and protocols of MixGroup are elaborated. In Section 4, the performance analysis and optimization are discussed. Performance evaluation is provided in Section 5. Finally, we conclude our work in Section 6.

2 System Model
2.1 Network Model
As shown in Fig. 1, we consider a vehicular social network that deployed in an urban area. The VSN consists of a number of vehicles, roadside infrastructures and an Intelligent Transportation System data center. These components are explained as follows.

- Vehicle. There are a large number of vehicles running on the roads in the urban area of interest. Each vehicle is equipped with an OBU, which allows the vehicles to communicate with other vehicles or with the roadside infrastructures for data exchange. Each vehicle will periodically broadcast its location information for the purpose of driving safety. To protect its location privacy, each vehicle should indicate itself by a predefined
In this sense, if a place is a common individual social spot of many vehicles, it is indeed a global social spot. Note that, for a specific vehicle, its individual social spots are candidate places for pseudonyms changing, if it happens to meet enough vehicles there.

2.2 Threat Model

To broadcast safety-related messages periodically, the radio of the OBU can not be switched off when a vehicle is running on the road. As a result, an eavesdropper may track a specific vehicle and monitor its location information by leveraging these periodical safety messages [13], [17]. Location privacy protection is, therefore, necessary to deal with the potential adversaries. In our threat model, we consider both the external and internal adversaries. More specifically, two types of external adversaries, namely, global passive adversary and restricted passive adversary, and two types of internal adversaries, namely, internal betrayal adversary and internal tricking adversary are considered.

- **Global Passive Adversary** (GPA). The global passive adversary (e.g., “Big Brother” surveillance [15]) can locate and track any vehicle in a region-of-interest by eavesdropping its broadcasts.
- **Restricted Passive Adversary** (RPA). The restricted passive adversary (e.g., a compromised service provider) is limited in its location tracking capability in a region-of-interest, since it can only exploit the deployed infrastructure RSUs for eavesdropping and estimating locations of vehicle broadcasts. Hence, the region over which the RPA can track vehicles is dependent on the vehicle transmission range and the distance between any two successive deployed RSUs.
- **Internal Betrayal Adversary** (IBA). For the group signature based scheme, an internal adversary is a compromised group member, who becomes an adversary after being a group member. The internal betrayal adversary will collude with GPA or RPA to track a target vehicle. After exchanging privacy-related information (e.g., the pseudonyms) with the target vehicle, an IBA will leak out the information to the GPA and RAP resulting in reconstruction of target vehicle’s trace in the case of the target vehicle only exchanges once in the MixGroup.
- **Internal Tricking Adversary** (ITA). Unlike the IBA, the internal tricking adversary will tautologically use the pseudonyms, which had been exchanged with others for more than one times. The victim gets useless pseudonyms and may exchange with others unconsciously. The number of victims depends on the number of vehicles that exchange information with the ITA.

There exist other approaches for an eavesdropper to track a target vehicle. For example, a video-based approach using traffic monitoring cameras is able to visually identify the target. Another physical-layer approach may use specialized hardware to capture and process electromagnetic signatures. However, these approaches require significant efforts like expensive cameras with sufficient high resolution to track even a single target vehicle. The adversary has to undertake overwhelming cost of the entire system. In this
paper, we consider the adversary using the aforementioned radio-based eavesdropping, which involves only a moderate system expense.

To preserve the location privacy of vehicles in vehicular social networks against the four types of adversaries mentioned previously, the requirements should be satisfied [15] as below. 1) The vehicles should use pseudonyms instead of a real identity to broadcast their safety messages for identity privacy preservation. 2) The vehicles should choose appropriate time and locations to periodically change the pseudonyms for avoiding continuous adversary tracking. 3) The pseudonyms of vehicles should be trackable to the trusted register authority (RA). The RA is capable of disclosing the real identity as well as the location of any vehicle in the VSN.

In the following section, a location privacy-preserving scheme, which achieves the above requirements, is proposed and discussed for VSNs.

3 The Proposed Location Privacy Preservation Scheme: MixGroup

In this section, we present the design of MixGroup for preserving the location privacy of vehicles in VSNs. Our discussion starts from two interesting and intuitive observations from the real vehicle traces. The notations used in this paper are listed in Table 1.

3.1 Two Observations from Real Vehicle Traces

Through trace-based experiment and analysis [18], we have the following two observations.

3.1.1 Observation One

Only a few vehicles meet in global social spots, while most vehicles meet sporadically. The mobility of vehicles is spatially restricted by the shape and distribution of the roads. Usually, vehicles gather in parking lots or road intersections when the traffic lights are red. In this paper, we choose 40 major road intersections as social hot spots in San Francisco and observe the number of vehicles which pass by the observed intersections from 8 o’clock in the morning to 12 : 10 at noon every 10 minutes. As shown in Fig. 2a, during the 250 minutes of interest, there are about 13 percent of observed vehicles collectively passing by the social hot spots as a crowd every 10 minutes (an aggregation of more than 10 vehicles is viewed as a crowd). Moreover, the vehicles in geographical proximity tend to meet frequently. The other 87 percent vehicles navigate sparsely. Each of these vehicles meets other vehicles sporadically in different road intersections, but not necessarily in the social hot spots.

3.1.2 Observation Two

Most vehicles always visit their individual social spots, where they meet most other vehicles that they may meet in one day. For most vehicles, they are moving with highly regular patterns everyday. Each vehicle usually passes by several fixed places, marked as individual social spots. Furthermore, the time when they arrive at each of these places is fairly close in every day. This is because people’s social behavior patterns usually remain stable within a relatively long interval [19]. We focus on the meetings of the vehicles and find that, each vehicle tends to meet 64 percent of other vehicles that it may meet in one day in its individual social spots (see Fig. 2. Statistics of vehicles in social spots.)
Fig. 2b), but only 13 percent of other vehicles in global social spots. The above two observations jointly reveal the fact that, vehicles have individual social features as well as common social features. The individual social features have major impact on vehicles’ moving patterns.

The two observations on the vehicles’ mobility features could be traced back to the Pareto principle (also known as the “80-20” rule). More specifically, there are roughly 80 percent of the vehicles meet others in 20 percent of the social spots (i.e., the hot spots). Our observations match with the Pareto principle and go a step further to reveal the fact that the hot spots could be divided into global hot spots and individual hot spots. In the roughly 80 percent (it is 77 percent accurately) of the vehicles, 64 percent meet others in the individual hot spots, while only 13 percent meet others in the global social spots.

In designing location privacy preservation schemes, it is important to exploit both the common and individual social features of vehicles’ moving patterns.

3.2 MixGroup: A Brief Overview

As we have pointed out that, the main concern in designing location privacy protection in VSNs is to increase the number of meeting vehicles, and hence maximize the uncertainty of pseudonym mixture. In traditional schemes, pseudonym changing happens only at global social spots. Consequently, a lot of mixture opportunities are wasted, as we know from the aforementioned two observations. In this paper, we are motivated to propose a new location privacy preserving scheme, namely MixGroup, which aims at efficiently aggregating the potential opportunities for pseudonyms changing along vehicles’ moving paths. To be more concrete, let us consider the scenario in Fig. 3. There are global and individual social spots along the path of vehicle $v_i$. In traditional scheme, $v_i$ is allowed to change its pseudonyms in the global social spot $S_g$ where there are 8 other vehicles at the intersection. Actually, there are still 3, 3 and 4 other vehicles at the intersections of the individual social spots $S_1$, $S_2$ and $S_4$, respectively. To efficiently leveraging these potential opportunities, the proposed scheme strategically combines the spots $S_1$ to $S_4$ to constitute an extended social region $R_1$. Vehicle $v_i$ is then allowed to accumulatively exchanging pseudonyms with vehicles that it meets in $R_1$. For instance, it may exchange pseudonyms with vehicle $v_h$ in $S_1$ and then with $v_i$ in $S_4$ sequently. Theoretically, since $v_i$ will meet totally 18 other vehicles, the opportunities for pseudonym mixture are considerably enlarged from 8 to 18. As a consequence, the privacy preservation is highly increased.

To implement the proposed scheme, four key mechanisms are devised: 1) the pseudonym mechanism, 2) the group signature, 3) temporary in-group identity, and 4) the encryption and authentication mechanisms, as explained below.

- **Pseudonym mechanism.** In MixGroup, the usage of pseudonym is the fundamental mechanism to protect the location privacy of vehicles. For vehicle $v_i$, it will be allocated with $w$ pseudonyms. For example, $PID_{i,k} (k = 1, \ldots, w)$ represents the $k$-th pseudonym of $v_i$. Pseudonym is used out of group-region for safety message broadcasting. In a group-region, vehicles will use group identities instead of pseudonyms. Pseudonyms are changed among vehicles in group-region.

- **Group signature.** By leveraging the mechanism of group signature, MixGroup constructs extended pseudonym-mixing regions (i.e., group-regions), in which vehicles are allowed to perform accumulatively change their pseudonyms. Each group has a group identity $GID_i$, and a group leader $GL_i$. When vehicle $v_i$ enters a group-region, the group leader $GL_i$ will deliver the group identity $GID_i$ and the corresponding group private key $SK_{G_i}$ and certificate $Cert_{G_i}$ to the vehicle after authentication. Vehicle $v_i$ will use $GID_i$, $SK_{G_i}$ and $Cert_{G_i}$ for broadcasting safety messages and pseudonyms changing subsequently.

- **Temporal in-group identity.** During the procedure of pseudonym exchange, each vehicle needs a dedicated identity to indicate itself and exchange pseudonyms with others. To avoid associating the real identity with identity of pseudonym exchange and adversary tracking, neither the real identity nor the current pseudonym could be set as the dedicated identity. For this reason, we define a new ID called temporary in-group identity (TID) for each vehicle. When a vehicle $v_i$ enters the group-region, the group leader will allocate a set of TIDs $PK_{G_i,l}$, $SK_{G_i,l}$ ($l = 1, \ldots, L$) to it. After that, TIDs will be used for sending requests and responses in the pseudonym exchanging procedures. Usually, each TID is expected to be used only once for pseudonym exchange. As a result, the adversary cannot establish the mapping relationship between vehicle’s real identity and pseudonym exchanging identity.

- **Encryption and authentication.** To protect wireless communication security and exclude illegal vehicles, MixGroup uses restrict encryption and authentication mechanisms. For each vehicle $v_i$, there are three set of public and private keys and certificates, respectively for real identity, TID and pseudonym exchange. Specifically, $[PK_i, SK_i, Cert_i]$ are used in V2I communications through which the RA can authenticate the vehicle’s real identity; $[PK_i', SK_i', Cert_i']$ are used according to TID for sending requests and responses before pseudonym exchange; $[PK_{G_i}, SK_{G_i}, Cert_{G_i}]$ are used to authenticate the validity of the two sides during pseudonym exchange.

![Fig. 3. Illustration of group-region.](image-url)
3.3 MixGroup: The Detailed Operations

MixGroup mainly consists of six operations: system initialization, key generation, group join, pseudonym exchange, group leaving and revocation. Fig. 4 shows the state diagram of vehicles in MixGroup to explain how the vehicle transits from one state to another.

3.3.1 System Initialization and Key Generation

In MixGroup, we employ the efficient Boneh-Boyen short signature scheme in [14], [20] for system initialization and key generation. In the scheme, vehicle \( v_i \) with identity \( I_D_i \) joins the system and gets its public/private key and certificate, denoted as \( PK_i, SK_i \) and \( Cert_i \), respectively. The RA stores \( (I_D_i, PK_i) \) in the tracking list. The vehicle is provided with a set of pseudonyms \( \{PID_{i,k}\}_{k=1}^{w} \) by RA, and accordingly public/private key pair \( (PK_{PID_{i,k}}, SK_{PID_{i,k}}) \) and certificates \( Cert_{PK_{PID_{i,k}}} \) for each pseudonym \( PID_{i,k} \). The group public key of group \( G_j \) and group private key for vehicle \( v_i \) are denoted as \( \{GID_j, SK_{G_j}, Cert_{G_j}\} \), respectively. In this paper, TIDs are generated by the RSA algorithm. After that, TIDs are delivered through RSUs (which are located at the boundary of MixGroup region) to the vehicles when they enter the MixGroup region. It is noteworthy that TIDs are only used for sending requests and responses during the procedure of pseudonym exchange.

3.3.2 Group Join

Before entering a group-region and joining a group, each vehicle \( v_i \) periodically broadcasts safety messages with its own pseudonyms \( \{PID_i\} \) given by the RA. Upon hearing the broadcast messages from the nearby RSU, say, RSU\(_{k}\), \( v_i \) will propose to the group leader GL\(_j\) through RSU\(_k\), requesting for the membership of group \( G_j \). The group leader, who is responsible for distributing and managing group identity (GID) and the associated keys and certificates, is elected by the RSUs of group \( G_j \). The group leader GL\(_j\) verifies whether the legality of \( v_i \) (identity parameters of \( v_i \), included in the request) with the help of RA. And then, GL\(_j\) provides \( v_i \) with parameters of GID and the associated private key and certificate, and also the parameters of a temporary in-group identity (TID) used during pseudonym exchange with others. After that, \( v_i \) becomes a group member and will broadcast safety message using GID\(_j\), instead of \( \{PID_i\} \) to prevent the possible continuous tracking of pseudonyms from potential adversary. In order to ensure liability of the message originator and safety of message receiver, each vehicle signs its safety message with a time-stamp to ensure message freshness and includes the group private key and certificate to enable verification. The pseudocode of the group join protocol is presented below.

**Group Join Protocol (GROUP_JOIN)**

1. \( v_j \): listen to the messages from neighboring RSU\(_{k_i}\) RSU\(_{k_j}\) in \( G_j \).
2. \( v_j \): verify the legitimate identity of RSU\(_{k_i}\) and change its pseudonyms from PID\(_{i,k-1}\) to PID\(_{i,k}\), PID\(_{i,k}\) ∈ \{PID\(_i\)\};
3. \( v_j \rightarrow GL_j \):
   
   \[request = RSU_{k}\[join\_request]\{|PID_{i,k}\}
   \[\{|Cert_{PID_{i,k}}\}|\{TimeStamp\}\]
   
   where \( join\_request = PK_{PID_{i,k}}|location\_i|\{velocity\_i, acceleration\_i\} \{TimeStamp\} \]
4. if \((\text{verified}\, \text{PID}_{i,k}) \) and \((\text{location}_i \in \text{within range of} \text{RSU}_{k_i}, \text{RSU}_{k_j} \in \text{G}_j)\)
   
   \( GL_j \rightarrow i \):
   
   \[reply = E_{PK_{G_j}}(\text{Group}\_\text{key}|\{TID\_key, Cert_{G_j}\}|\text{GID}_j, \text{TimeStamp}) \]
   
   where \( \text{Group}\_\text{key} = G_{j}\_\text{sk}_{G_j, i}|\text{Cert}_{G_j} \),
   
   \( \text{TID}\_\text{key} = PK_i|\{SK_{G_j, i}, Cert_{G_j}\} \)
   
   else
   
   \( GL_j \): do not reply;

5. if (received reply within \( T_{max} \))
   
   \( v_i \): broadcast by GID\(_j\), instead of \( \text{PID}_{i,k} \);
   
   \( broadcast = GID_j|\{navigation\_data, |Sign_{SK_G_j, i} (navigation\_data), |Cert_{G_j, i}\} |\{TimeStamp\} \)
   
   where \( \text{navigation}\_\text{data} = |\text{location}_i, |\{velocity\_i, acceleration\_i\} \{\text{TimeStamp}\} \)
   
   \( v_i \): go to GROUP\_OPERATION when meeting other vehicles;
   
   else
   
   \( v_i \): go to step 3;

end

3.3.3 Pseudonyms Exchanging

When vehicle \( v_i \) navigates as a group member of \( G_j \), it will periodically broadcast safety messages with the identity GID\(_j\). Once vehicle \( v_i \) meets other group members of \( G_j \), there is an opportunity to exchange their pseudonyms. At this moment, the vehicle will broadcast a pseudonym exchanging request. In traditional Mix-zone [7], vehicles change their pseudonyms in road intersections under the assistance of RSUs. The operations of pseudonym changing in MixGroup are different from that in Mix-zone. Two vehicles of a same group are allowed to directly exchange their pseudonyms without the involvement of RSUs. This means that, pseudonym changing could be performed out of the coverage area of RSUs. Furthermore, the newly exchanged pseudonyms would not be used immediately but after the vehicles leave the group-region. Instead, the group identity is still used for broadcasting safety messages. The usage of group identity is beneficial to “cover” the procedure of pseudonym exchange. By leveraging group signature mechanism, pseudonym changing in MixGroup may take place anywhere as a vehicle meets with other vehicles.

The procedure of pseudonym exchange has several steps. First, if vehicle \( v_i \) finds out that there are other vehicles in proximity (by hearing safety messages) and it attempts to exchange pseudonyms, \( v_i \) will broadcast a pseudonym...
exchanging request message associated with it’s public key of TID $PK'_v$. After receiving the request messages from other vehicles, vehicle $v_i$ will compute its own exchange benefit and decide whether to exchange at this time or not. In this paper, the exchange benefit is quantitatively evaluated by the pseudonym entropy. The procedure of negotiation on the participation of pseudonym exchange will be elaborated later in Section 4. If vehicle $v_i$ decides to exchange with others, it will randomly select a neighbor vehicle, say, $v_j$ (actually indicated by the TID), and send pseudonym exchange proposal to $v_j$ which is encrypted with the public key of $v_j$’s TID (i.e., $PK'_j$) in its broadcast request. With the agreement from $v_j$, $v_i$ will receive and verify the response of $v_j$. $v_i$ will send signing request to it with $PID^i_j=(exchange)$ and go to EXCHANGE_HANDSHAKE protocol.

3. $v_i$ goes to step 1;  
else 

**Exchange Handshake Protocol (EXCHANGE_HANDSHAKE)**

1. $v_i$: receive pseudonym exchanging request from neighbors;  
2. $v_j$: verify and evaluate the benefit to decide whether to exchange right now;  
3. $v_i$: if (exchange) 

3.1 $v_i$: randomly choose a vehicle $v_j$ with $PK'_j$;  
3.2 $v_j$ goes to $v_i$: 

$\text{proposal} = PK'_j[\text{exchange\_proposa}l|PK_i||\text{Cert}_i||\text{Cert}_{G_j}||\text{TimeStamp}]
$  
and go to PSEUDONYM\_EXCHANGE protocol;  
else 

3.3 $v_i$ goes to step 1;  
endif 

3.4 $v_i$: broadcast request $=(\text{exchange\_request}|PK_i||\text{Cert}_i||\text{Cert}_{G_j}||\text{TimeStamp})$;  
3.5 $v_j$: goes to PSEUDONYM\_EXCHANGE protocol;  
else 

3.6 $v_j$: go to step 3.1;  
endif 

3.7 $v_j$: go to step 1;  
endif 

### Pseudonym Exchange Protocol (PSEUDONYM\_EXCHANGE)

1. $v_i \rightarrow v_j$:  

$\text{Pseudonym}_i \rightarrow j = E_{PK}_j(\text{data}_1|\text{Sig}_j)\text{|\text{Cert}_{G_j}||\text{TimeStamp}}$

where $\text{data}_1 = \text{PID}_i||\text{Cert}_{PID}_i||\text{Sign}_{SK_{PID}_i}$  
$\text{Sig}_j = \text{Sign}_{SK_{G_j}}(\text{data}_1)$

2. $v_j$: verify and store data from $v_i$;  
3. $v_j \rightarrow v_i$:  

$\text{Pseudonym}_j \rightarrow i = E_{PK}_i(\text{data}_2|\text{Sig}_i)\text{|\text{TimeRecord}\text{|\text{TimeStamp}}}$

where $\text{data}_2 = \text{PID}_j||\text{Cert}_{PID}_j||\text{Sig}_{SK_{PID}_j}$  
$\text{Sig}_i = \text{Sign}_{SK_{G_i}}(\text{data}_2)$

**Dual-signature** $\rightarrow i = E_{SK_{G_i}}(\text{data}_1)\text{|\text{TimeRecord}\text{|\text{TimeStamp}}}$

4. $v_i$: verify and store from $v_j$;  
$v_i \rightarrow v_j$:  

$\text{data}_i = E_{PK}_i(\text{data}_1|\text{TimeRecord}\text{|\text{TimeStamp}})$

where $\text{data}_i = \text{PID}_i||\text{Cert}_{PID}_i||\text{AddData}$

5. $v_j$: verify and store data from $v_i$;  
6. $v_j$: $\text{Record}_1 = E_{PK}_j(\text{Cert}_{G_j})\text{|\text{Cert}_{G_i}}$  

$\text{PID}_i || \text{PID}_j \text{|| \text{AddData}}$

$v_j$: $\text{Record}_2 = E_{PK}_j(\text{Cert}_{G_j})\text{|\text{Cert}_{G_i}}\text{|| \text{PID}_i} \text{|| \text{PID}_j} \text{|| \text{AddData}}$

7. $v_j$: send $\text{Record}_1$ to $v_i$;  
8. $v_i$: compare received $\text{Record}_2$ with $\text{Record}_1$, if $\text{Record}_2$ and $\text{Record}_1$ are identical  

$i \rightarrow j$:  

$R_i = E_{PK}_i(\text{Record}_1|\text{TimeRecord})$

where $\text{Sig}_{R_{i-j}} = \text{Sign}_{SK_{G_i}}(\text{Record}_1)\text{|\text{TimeRecord}}$

9. $v_j$: verify and store data from $v_i$;  
10. $v_j$: compare received $\text{Record}_1$ with $\text{Record}_2$, if $\text{Record}_2$ and $\text{Record}_1$ are identical  

$j \rightarrow i$:  

$R_j = E_{PK}_j(\text{Record}_1|\text{TimeRecord})$

where $\text{Sig}_{R_{j-i}} = \text{Sign}_{SK_{G_j}}(\text{Record}_1)\text{|\text{TimeRecord}}$

11. $v_i$: verify and store data from $v_j$.

#### 3.3.4 RSU Signing Protocol

As mentioned above, a vehicle may meet and exchange its pseudonyms and the associated certificates with other vehicles. However, before having permission to use the exchanged pseudonyms, the vehicle should firstly activate the pseudonyms by RA through the RSUs. After pseudonym exchange with the last vehicle, say, $v_i$, $v_j$ will listen to broadcast messages of RSUs nearby. When connected to an RSU, say $\text{RSU}_{m}$, $v_i$ will send signing request to it with $\text{Exchange\_data}$ and $\text{Personal\_data}$ that are encrypted by public key of RA. The Exchange\_data includes exchanged pseudonyms and dual-signature signed by $v_i$ and $v_j$ to prevent from forgery. The RA validates the Personal\_data to verify the legal identity of $v_i$ and $v_j$ and distributes new exchanging key pair for the next exchange and renewed certificates of $\{\text{PID}_i\}$ to $v_i$. The RA will keep record of these data, while $v_i$ will also verify and store them. If the Exchange\_data is invalid, RA will redistribute valid pseudonyms and
certificates in its backup list to $v_i$. The pseudocode of RUSSIGN protocol is illustrated below.

**RSU Sign Protocol (RUSSIGN)**

1. $v_j$: receive and verify broadcast from $RSU_m$ and decide to activate the new pseudonyms ($RSU_m \in G_j$);
2. $v_j \rightarrow RSU_m$ (RA):
   
   request_sign = $RSU_m || E_{PK_{RSU}}(Exchange\_data$
   
   $|| Personal\_data || TimeStamp),$
   
   where $Personal\_data = PK_{v_j} || Cert_{v_j},$
   
   $Exchange\_data = (PID_i || Cert_i$
   
   $|| Dual\_signature_{j-m} || TimeStamp),$
   
   $SigR_{j-m} = Sign_{RSU_m}(Record\_1 || TimeStamp);
3. RA: if (validate $Personal\_data$ and $v_i$)
   
   go to REVOCATION
   
   else
   
   3.1 if (Exchange_data valid)
   
   send new exchanging keys and certificates,
   
   $RA \rightarrow v_i$: update = $E_{PK_{v_j}}(new\_key || new\_certification$
   
   $|| new\_pseudonyms || Cert_{RA} || TimeStamp)$
   
   where $new\_key = Hash(PID_j || SK_{v_j}$
   
   $|| Cert_{j} || TimeStamp)$
   
   $new\_certification = Hash(PID_j || Cert_{j}$
   
   $|| TimeStamp)$
   
   $new\_pseudonyms = PID_j$
   
   3.2 $v_i$: validate and store renewed data;
   
   else
   
   3.3 RA: redistribute pseudonyms for $v_i$
   
   go to REVOCATION;
   
   endif
   
   3.4 go to GROUP_LEAVE;

   endif

**Group Leave Protocol (GROUP_LEAVE)**

1. $v_i$: compute distance from zone boundary of $G_j$;
2. $v_i$: if (before going out of $G_j$ at leave\_time, $t$)
3. $v_i$: randomly choose $t$ to use $PID_j$ instead of $GID_j$
   
   go to GROUP\_JOIN
4. $GL_j$: if (no broadcast received from $v_i$ during $D_{max}$)

**3.3.6 Revocation Protocol**

In MixGroup, any violation of vehicles will be monitored and accused by neighboring vehicles or RSUs. For example, if a compromised vehicle $v_k$ in the group is detected by $v_i$, $v_i$ will record the violation actions of $v_k$ and report to the group leader $GL_j$. There are vital evidences in the report. If $v_i$ is staying in the group-region, the report will include the information such as the type of violation of $v_k$, the group certificates of $v_i$ and $v_k$, and the messages signed by $v_i$. If $v_i$ has left the group, it will integrate the pseudonym $PID_{j,n}$, the public key $PK_{PID_{j,n}}$ and the certificate $Cert_{PID_{j,n}}$ into the report. After receiving the report, the group leader $GL_j$ will check the validity of the report as well as the identity of $v_i$, and then forward to the RA. The RA will validate the report and delete the true identity of $v_i$ by the tracking list. If the violation if confirmed, RA will add $v_k$ into its blacklist and broadcast a new blacklist to all RSUs and vehicles in the VSN.

**3.3.7 Conditional Tracking**

When a vehicle is in a group $G_j$, its periodical broadcasting message includes the safety-related data and the group certificate $Cert_{G_j}$. Although group members of $G_j$ only can verify the validity of the safety message, the RA can link all the messages with certificates to the true identities of vehicles by checking the tracking list. When a vehicle is out of any group and uses its own pseudonyms for communication, its safety message also includes the certificate, which can be identified by RA. In other words, the true identity of each vehicle is totally concealed for the trust RA, but conditionally private for the group leader and unknown for the other common vehicles.

**3.3.8 Discussions**

In the proposed scheme, there are two separate procedures related to the pseudonym changing: the pseudonym exchange procedure and the pseudonym activation procedure. These two procedures are efficiently integrated to allow distributed pseudonym changing. The pseudonym exchange procedure only involves vehicles. Vehicles of a same group are allowed to exchange their pseudonyms directly and out of the coverage area of RSUs. Even more, a vehicle is allowed to accumulatively exchange its pseudonym with others without the involvement of RSUs. During the pseudonym activation procedure, vehicles have to activate their pseudonyms through RSUs. After exchanging its pseudonym with others, a vehicle will activate the new pseudonym whenever it meets the RSUs. In this sense, it is unnecessary to have continuous RSUs radio coverage. Eventually, when a vehicle encounters the RSUs at the boundary of the MixGroup region, it will have a final check to ensure the pseudonym activation procedure is carried out.
4 Security Analysis

In this section, we discuss on the possible attacks and the corresponding defense measures in MixGroup. In addition, we present the optimization of pseudonym exchange to improve the pseudonym entropy against location privacy tracking.

4.1 Attack and Defense Analysis

In principle, the strength of location privacy preservation in pseudonym-based schemes depends on the uncertainty (i.e., entropy) in mapping pseudonyms to real vehicle identities from the perspective of adversary. Accordingly, the central idea of MixGroup is to combine the successively located individual hot spots of the target vehicle into an extended pseudonym-changing region. Since the area of the region is considerably enlarge and vehicles are allowed to accumulatively change their pseudonyms, the uncertainty of pseudonyms mixture is significantly improved, and therefore, the privacy preservation is consequently enhanced.

MixGroup has favorable defense ability against many security and privacy attacks. For example, due to the encryption and authentication mechanisms, the adversary is computationally bounded and unable to launch brute-force cryptanalytic attacks on the encrypted messages. Furthermore, since all messages are authenticated, the adversary is hard to emulate the legal vehicles. The replay attacks would not be successful due to the usage of time stamps. Meanwhile, the adversary cannot simulate an RSU or forge the RSU messages, and hence, they cannot create fictitious MixGroup with valid keys it controls.

In the following, we will further discuss on several essential attacks and the defense measures of MixGroup.

4.1.1 GPA and RPA

For GPA and RPA, the adversary passively eavesdrops vehicles' safety messages, and observes the time and the locations of the entering and exiting vehicles in order to derive a probability distribution over the possible mappings. If there are few vehicles in the pseudonym changing place, the adversary will still have high probability to follow the target vehicle. However, MixGroup is not limited in one pseudonym changing in one place. When a vehicle enters a group-zone and meets many vehicles during navigation. By using a uniform group signature, the vehicle is allowed to exchange pseudonym with any vehicle passing by. In this case, for GPA and RPA, it is hard to track a target if it is ‘mixed’ with a sufficient large number of vehicles. All these vehicles look identical under the protection of group signature. As a consequence, the GPA and RPA will be lost in tracking a target.

4.1.2 Incorrect Data Attack

The internal adversary can perform attack on vehicle safety by misbehaving and broadcasting incorrect data to attack neighboring vehicles. However, in MixGroup, since each vehicle signs the safety messages (see Step 5 of GROUP JOIN protocol), the adversary will be held liable for providing incorrect data. In order to detect such attacks, each vehicle must be able to detect the incorrect safety messages. In [21], an efficient scheme is proposed to detect incorrect data, by enabling each vehicle to maintain its own observations of the neighborhood (such as estimated locations of neighboring vehicles) and checking data received from neighbors for any inconsistencies.

4.1.3 Liability Attack

The adversary may perform attack on the vehicle liability. In order to evade liability, the adversary can counterfeit a random pseudonym in the VSN. Actually, such an attack is prevented in MixGroup. It is mentioned that safety messages from each vehicle must contain valid certificates, and furthermore, be signed by a legal group signature if inside the group, or by an authenticated pseudonym if outside the group. The vehicles can authenticate the validity of the safety messages. The adversary can also attempt to impersonate the target vehicle using one of its overheard pseudonyms and the associated certificate [15]. Such impersonation attacks are avoided in our model by making each vehicle sign on the safety message and include a valid certificate from RA according to the pseudonym in usage.

4.1.4 IBA and ITA

In this paper, there are two kinds of special internal adversaries, namely internal betrayal adversary (IBA) and internal tricking adversary (ITA). For IBA, it exchanges its pseudonyms, which had been used, with the target vehicle. The IBA finds out the pseudonyms that target had used and the target vehicle may be tracked if it no longer exchanges the pseudonyms from IBA when it is out of group-regions. The IBA may share the information to GPA that which pseudonyms the target will use when it is out of group-regions and which pseudonyms the target had used before entering group-regions. The GPA can link the locations of vehicles by eavesdropping safety messages signed by these pseudonyms. However, it can be easy to resist if the target vehicle exchanges pseudonyms with one more vehicles. The adversary can’t precisely link the pseudonyms to the target. As we know that, the more vehicles it exchanges to, the less risk it will be, but the higher overhead it will undertake. Additionally, with the help of neighboring group members and the group leader, the compromised group members would be accused. By then, the adversary would be expelled from the system soon.

In ITA, the adversary will tautologically use its pseudonyms that has been exchanged with others and repeatedly perform PSEUDONYMS EXCHANGE protocol. The victim vehicle get overused pseudonyms and exchange with others. The number of victims depends on the vehicles’ number of exchanging with ITA. For this adversary, with the help of dual signature and signed record $\text{SigR}$, the RA can detect these adversaries through $\text{SigR}$ which is unchanged by the adversary because of encryption with RA public key (as shown in the PSEUDONYMS EXCHANGE protocol in Section III-C). When the vehicles detect these adversaries, they will report to RA. The adversaries would be put into blacklist and be charged with responsibility later.

4.2 Entropy-Optimal Pseudonym Exchange

The meetings of vehicles are underlying opportunities for vehicles to enhance their location privacy. However, there are potential threats from internal attacks IBA and ITA, by
which the pseudonym information of a legitimate vehicle may be copied and leaked out. Therefore, it is not always beneficial for a vehicle to exchange its pseudonyms with others. In this paper, we define pseudonym entropy to measure the strength of location privacy protection for vehicles. Consider a road intersection where a collection of vehicles, denoted by \( V = \{ v_1, v_2, \ldots, v_K \} \), will exchange pseudonyms with each other. Let \( p_i \) represent the successful tracking probability of vehicle \( v_i \) after pseudonyms exchanges. The pseudonym entropy for \( v_i \) is represented by

\[
H_i = -\log_2 p_i.
\]

The pseudonym entropy for the collection \( V \) is given by

\[
H_V = -\sum_{i=1}^{K} p_i \log_2 p_i.
\]

Clearly, the successful tracking probability \( p_i \) depends on the number of internal adversaries (IBA or ITA) inside the VSN of interest, and \( B \) of them are internal adversaries, denoted by collection \( V_{IA} \). The probability that \( v_i \) happens to select \( v_j \) which is an internal adversary for pseudonym exchange is derived by

\[
\Pr \{ v_j \in V_{IA} \} = \frac{B(B) \left( \frac{N-1}{K-1} \right) i}{K-1} = \frac{B}{N-1}. \tag{3}
\]

By pseudonym exchange, the increase of \( v_i \)'s pseudonym entropy is given by

\[
\Delta h = \sum_{i=1}^{B} \frac{B(N-1)}{N-1} \log_2(K-i). \tag{4}
\]

After the \( k \)-th pseudonym exchange, the pseudonym entropy of \( v_i \) is represented by

\[
H_v(k) = \begin{cases} 
0, & v_j \in V_{IA}, \\
H_v(k-1) + \Delta h, & v_j \notin V_{IA}.
\end{cases}
\]

Following (5), each vehicle will evaluate the benefit and the risk in pseudonym exchange. For vehicles already have high pseudonym entropy, they tend to skip the pseudonym exchange; while for vehicles of low pseudonym entropy, they expect to take the opportunity to enhance their location privacy. More concretely, a vehicle is willing to exchange pseudonym if the possible increase of its pseudonym entropy is sufficiently large, i.e.,

\[
\Delta h > \frac{\Pr \{ v_j \in V_{IA} \} H_v(k-1)}{1 - \Pr \{ v_j \in V_{IA} \}}. \tag{6}
\]

To facilitate the decision making of pseudonym exchange among vehicles, we elaborately devise the following negotiation procedure.

- **Sending pseudonym exchange request.** Vehicles will broadcast pseudonym exchange requests periodically, and meanwhile, listen to other vehicles’ requests. Given a number of vehicles at a road intersection, the negotiation takes several rounds.

- **Evaluating pseudonym exchanging benefit.** In each round of negotiation, the vehicle will firstly observe the number of candidate vehicles for exchange, and then evaluate the benefit by (6). If the condition of (6) is satisfied, it will send out a pseudonym exchange confirmation message; otherwise, it will broadcast a pseudonym exchange ending message to indicate it will skip the opportunity.

- **Observing pseudonym exchanging candidates.** A vehicle observes the pseudonym exchanging candidates by listening to the pseudonym exchange requests and confirmation/ending messages of its neighboring vehicles. Initially, all vehicles are treated as candidates.

- **Selecting pseudonym exchanging candidates.** After receiving the confirmation messages of all candidates, each vehicle will randomly select one of the candidates for exchange. If a vehicle is selected by multiple vehicles, it has the right to choose one from them. Then, the two vehicles send their exchanging public keys and associated certificates to each other. During the procedure of pseudonym exchange, vehicles are paired to exchange pseudonyms.

When there are an odd number of vehicles, the unpaired vehicle may randomly select a paired vehicle for pseudonym exchange. In this case, the selected vehicle will sequentially exchange pseudonyms twice. Alternatively, the unpaired vehicle may also skip the current exchange procedure until meeting other vehicles. As the observations in Section 3.1, each vehicle in MixGroup region has enough chances to meet and exchange pseudonyms with others. Even if a vehicle leaves out of a MixGroup region without exchanging pseudonym with others, the adversary couldn’t identify if the vehicle has exchanged with others. Therefore, the vehicle could also protect its privacy in this case.

## 5 Performance Evaluation

In this section, we study the performance of proposed MixGroup scheme using a self-developed network simulator based on NS-3 [22] and SUMO [23]. We use synthetic vehicle traces and road maps to simulate different traffic conditions and group-region coverage ratios. Specifically, we consider a city region of 20 km². We investigate different traffic conditions: 500 vehicles for low traffic load, 1000 vehicles for medium traffic load and 1500 vehicles for high traffic load. RSUs are placed at road intersections evenly with different density: 0.5/\( \text{km}^2 \) for sparse deployment, 1/\( \text{km}^2 \) for medium deployment, and 2/\( \text{km}^2 \) for dense deployment. The radio coverage radius of RSUs and OBUs is set to be 300 m, which is a typical range of the IEEE 802.11p WAVE protocol. It is noteworthy that, by integrating group signature and pseudonym changing, the proposed scheme is operated in a distributed way. This means that, even if the city road map has a larger size, the proposed scheme still works efficiently when we deploy more MixGroup regions. Table 2 shows the simulation parameters, most of which are common settings in existing work [16].
5.1 Global Pseudonym Entropy of VSN

Fig. 5 shows the global pseudonym entropy of the VSN. For comparison, we set that MixGroup is launched at time 0 while the global pseudonym entropy is reset to 0. We know from Fig. 5a that, the global pseudonym entropy increase rapidly, as vehicles start to exchange their pseudonyms within the group-regions. More importantly, we find that the traffic conditions have significant impact on the increasing rate of the global pseudonym entropy. This fact is easy to understand. The more the vehicles on roads, the more the pseudonym exchanging opportunities. In the case of medium traffic condition of totally 1,000 vehicles, the global pseudonym entropy is 35 percent larger than that in low traffic condition of 500 vehicles. In the case of high traffic condition of 1,500 vehicles, the global pseudonym entropy is only 10 percent larger than that in medium traffic. This is due to the increasing traffic load, the traffic congestion will slow down the frequency of pseudonym exchanges among vehicles.

In Fig. 5b, different tracking attack strength are considered. In the simulation, we suppose that all adversary vehicles are of the four types of attacks: GPA, GRA, ITA and IBA. Regarding the high traffic conditions, the cases of 10, 30 and 50 adversary vehicles are investigated as weak, medium and strong attacks, respectively. We can see that, the global pseudonym entropy under different attack strength initially have same increasing rate, but finally converge to different value. The global pseudonym entropy under weak attack is more than two times of that under strong attack.

The global pseudonym entropy under different group-region coverage are reported in Fig. 5c. The ratio of group-region coverage is set according to RSUs density. For example, 50, 30 and 15 percent coverage of group-region are set to dense, medium and sparse RSU deployment, respectively. We could observe from the figure that, in a large group-region coverage, vehicles tend to meet each others more frequently, and therefore, the resulted global pseudonym entropy is clearly larger than that in a small group-region coverage.

5.2 Pseudonym Entropy of Target Vehicle

The second simulation is carried out to evaluate the pseudonym entropy of a specific target vehicle. Both the expected and actual pseudonym entropy are investigated. We select a vehicle of active social activity and track the variation of its pseudonym entropy. The pseudonym entropy is reset to 0 at the beginning of the simulation. After that, the vehicle enters group-regions for pseudonym exchange.

In Fig. 6a, different tracking attack strength are considered. In the simulation, we suppose that all adversary vehicles are of the four types of attacks: GPA, GRA, ITA and IBA. Regarding the high traffic conditions, the cases of 10, 30 and 50 adversary vehicles are investigated as weak, medium and strong attacks, respectively. We can see that, the global pseudonym entropy under different attack strength initially have same increasing rate, but finally converge to different value. The global pseudonym entropy under weak attack is more than two times of that under strong attack.

The global pseudonym entropy under different group-region coverage are reported in Fig. 5c. The ratio of group-region coverage is set according to RSUs density. For example, 50, 30 and 15 percent coverage of group-region are set to dense, medium and sparse RSU deployment, respectively. We could observe from the figure that, in a large group-region coverage, vehicles tend to meet each others more frequently, and therefore, the resulted global pseudonym entropy is clearly larger than that in a small group-region coverage.

In Fig. 6b, different tracking attack strength are considered. In the simulation, we suppose that all adversary vehicles are of the four types of attacks: GPA, GRA, ITA and IBA. Regarding the high traffic conditions, the cases of 10, 30 and 50 adversary vehicles are investigated as weak, medium and strong attacks, respectively. We can see that, the global pseudonym entropy under different attack strength initially have same increasing rate, but finally converge to different value. The global pseudonym entropy under weak attack is more than two times of that under strong attack.

The global pseudonym entropy under different group-region coverage are reported in Fig. 5c. The ratio of group-region coverage is set according to RSUs density. For example, 50, 30 and 15 percent coverage of group-region are set to dense, medium and sparse RSU deployment, respectively. We could observe from the figure that, in a large group-region coverage, vehicles tend to meet each others more frequently, and therefore, the resulted global pseudonym entropy is clearly larger than that in a small group-region coverage.
pseudonym entropy is improved faster in heavy traffic conditions. There is a gap between the actual pseudonym entropy and the expected pseudonym entropy. The reason is that the presence of adversary poses a potential risk to the vehicle. Especially for the ITA and IBA, if the target vehicle happens to choose an ITA or IBA for pseudonym exchange, its location privacy will be violated as the pseudonym entropy is reset to 0. We also know from Fig. 6b that, both the expected and actual pseudonym entropy of the target vehicle decrease rapidly with the raising of attack strength. In addition, the denser the group-region coverage, the larger the the pseudonym entropy of the vehicle, as shown in Fig. 6c.

5.3 Comparison with Existing Schemes

We also compare our proposed MixGroup with two existing location privacy protection schemes: Mix-zone and PCSS. Mix-zone [7] is a well-known scheme for preserving vehicle location privacy. PCSS [13], referring to pseudonym changing at social spots, is an efficient scheme that exploits the social feature of vehicles and performs pseudonym changing at social spots (actually mentioned as global social spots in this paper). In the simulation, two types of RSU coverage density are considered, which accordingly have dense and sparse coverage of Mix-zone/group-region.

In Fig. 7, the global pseudonym entropy of the VSN in the three scheme are compared. We observe that, in dense coverage, the global pseudonym entropy in MixGroup is about 56 percent and 5 times higher than that in PCSS and Mix-zone, respectively. While in sparse coverage, the global pseudonym entropy in MixGroup is approximately 28 percent and 4 times higher than that in PCSS and Mix-zone, respectively. In Fig. 8, the actual pseudonym entropy of a target vehicle is investigated. As the figure has shown, in dense coverage, the actual pseudonym entropy in MixGroup is 47 and 96 percent higher than that in PCSS and Mix-zone, respectively. In sparse coverage, the actual pseudonym entropy in MixGroup is 29 percent and 3.8 times higher than that in PCSS and Mix-zone, respectively.

From the above results, we know that MixGroup significantly outperforms the other two schemes. The advantage of MixGroup over the other two schemes remains remarkable in the case of sparse coverage. In low traffic case, only few vehicles appear at road intersections concurrently. However, MixGroup has the natural ability to accumulatively exploit the vehicle meeting opportunities. The number of aggregated meeting vehicles stays at a moderate level, even in low traffic conditions. As a consequence, MixGroup still has satisfying performance in low traffic conditions.

6 Conclusion

In this paper, we address the problem of location privacy protection in VSNs. We propose a new scheme called MixGroup, which integrates the mechanism of group signature and constructs an extended pseudonym-changing region. By accumulatively exchanging pseudonyms, vehicles will have their pseudonym entropy consecutively increased. As a consequence, the location privacy is substantially enhanced. We also propose the entropy-optimal negotiation procedure to facilitate the local pseudonym exchange among vehicles. Simulation results indicate that MixGroup works very well even under low traffic conditions. Meanwhile, through comparison, MixGroup is shown to significantly outperform existing schemes.

Acknowledgments

The work is supported in part by programs of NSFC under Grant nos. 61422201, 61370159 and U1201253, Guangdong Province Natural Science Foundation under Grant no. S201103000286, High Education Excellent Young Teacher Program of Guangdong Province under grant no. YQ2013057, and Science and Technology Program of Guangzhou under grant no. 2014J2200097(Zhujiang New Star Program). Yan Zhang is the corresponding author of the article.

References


Rong Yu received the PhD degree from Tsinghua University, Beijing, China, in 2007. After that, he worked in the School of Electronic and Information Engineering at South China University of Technology, Guangzhou, China. In 2010, he joined the Institute of Intelligent Information Processing at Guangdong University of Technology, Guangdong, China, where he is now a full professor. His research interest mainly focuses on wireless communications and networking, including cognitive radio, wireless sensor networks, and home networking. He is the co-inventor of over 10 patents and author or co-author of over 70 international journal and conference papers. He is currently serving as the deputy secretary general of the Internet of Things Industry Alliance, Guangdong, and the deputy head of the IoT Engineering Center, Guangdong. He is the member of home networking standard committee in China, where he leads the standardization work of three standards. He is a member of the IEEE.

Xumin Huang received the PhD degree in Guangdong University of Technology, Guangdong, China. His research interests mainly focus on network performance analysis, simulation and enhancement in wireless communications and networking.

Jiawen Kang is currently working toward the PhD degree in Guangdong University of Technology, Guangdong, China. His research interests mainly focus on resource management, security and privacy protection in wireless communications and networking.

Yan Zhang received the PhD degree from Nanyang Technological University, Singapore. He is working with the Simula Research Laboratory, Oslo, Norway; and he is an adjunct associate professor in the Department of Informatics, University of Oslo, Oslo. He is a regional editor, associate editor, on the editorial board, or guest editor of a number of international journals. His recent research interests include wireless networks, cyber physical systems, and smart grid communications. He is a senior member of the IEEE.

Shengli Xie received the MS degree in mathematics from Central China Normal University, Wuhan, China, in 1992, and the PhD degree in control theory and applications from South China University of Technology, Guangzhou, China, in 1997. He is presently a full professor and the head of the Institute of Intelligent Information Processing at Guangdong University of Technology, Guangdong, China. His research interests include wireless networks, automatic control and blind signal processing. He is the author or coauthor of two books and more than 150 scientific papers in journals and conference proceedings. He received the second prize in China’s State Natural Science Award in 2009 for his work on blind source separation and identification. He is a senior member of the IEEE.

Stein Gjessing (steing@ifi.uio.no) is an adjunct researcher at the Simula Research Laboratory and a professor of computer science in the Department of Informatics, University of Oslo. He received his Dr. Philos. degree from the University of Oslo in 1985. Dr. Gjessing acted as head of the Department of Informatics for 4 years from 1987–1991. From February 1996 to October 2001, he was the chairman of the national research program “Distributed IT-System,” founded by the Research Council of Norway. He participated in three European funded projects: Macrame, Arches and Ascissa. His current research interests are routing, transport protocols and wireless networks, including cognitive radio and smart grid applications. He is a member of the IEEE.

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.