Location and trajectory privacy preservation in 5G-Enabled vehicle social network services

Dan Liao, Hui Li, Gang Sun, Ming Zhang, Victor Chang

PII: S1084-8045(18)30039-0

DOI: 10.1016/j.jnca.2018.02.002

Reference: YJNCA 2061

To appear in: *Journal of Network and Computer Applications*

Received Date: 10 April 2017

Revised Date: 16 January 2018

Accepted Date: 2 February 2018

Please cite this article as: Liao, D., Li, H., Sun, G., Zhang, M., Chang, V., Location and trajectory privacy preservation in 5G-Enabled vehicle social network services, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.02.002.

Location and Trajectory Privacy Preservation in 5G-Enabled Vehicle Social Network Services

Dan Liao[1], Hui Li[1,2], Gang Sun[1,3], Ming Zhang[2], Victor Chang[4]

[1]Key Lab of Optical Fiber Sensing and Communications (Ministry of Education), University of Electronic Science and Technology of China, Chengdu, China
[2]Chendu Research Institute of UESTC, Chengdu, China
[3]Center for Cyber Security, University of Electronic Science and Technology of China, Chengdu, China
[4]Xi’an Jiaotong Liverpool University, Suzhou, China

Abstract: 5G-based Vehicular Social Networks (VSNs) demand an advanced location and trajectory privacy preserving scheme for vehicles. Because VSNs present the characteristics of high mobility and multiple hop relays, we design a 5G-based VSN framework that incorporates Mobile Femtocell (MFemtocell) technology. Then, we propose the Dynamic Group Division algorithm (DGD), which is suitable for the dynamic properties of 5G and meets the real-time demands of VSN. To preserve privacy, the DGD algorithm increases the likelihood of exchanging pseudonyms via the proposed Group Generating Protocol and Pseudonym Exchanging Protocol. Then, we adopt the composite metric KDT (where *K* is the average anonymity set size, *D* is the average distance deviation, and *T* is the anonymity duration) and pseudonym entropy to quantify the degree of privacy. We evaluate and validate the effectiveness of our proposed algorithm based on the following three aspects: anonymity set size, distance deviation and pseudonym entropy. The simulation results show that our DGD algorithm better protects the location and trajectory privacy of VSNs while sustaining higher real-time demand than current approaches.

Key words: Location privacy; Trajectory privacy; 5G; Mobile Femtocell; VSN

1. Introduction

Vehicles now represent “the biggest mobile terminal” in the context of the Internet. The 5GAA committee (5G Automotive Alliance) has published research on the Internet of Cars in 2017 [1], and with the development of cloud computing [2-7] and big data [8-13], vehicles represent intelligent devices that can connect to the Internet and present sensing and computing abilities. Thus, vehicles are now the main carriers for mobile social networks. The Vehicular Social Network (VSN) has emerged, and vehicles can now be connected to wireless networks to improve traffic safety and promote the development of smart cars. However, the convenience of VSNs may lead to privacy concerns. The problem of privacy disclosure primarily stems from two aspects. First, for the users, certain data transmitted over the VSN are highly sensitive, such as location, trajectory, and identity information. If these sensitive data are revealed, the location privacy, trajectory privacy and identity privacy can be leaked [14]. Second, the topology of the VSN changes quickly because of the vehicle's high-speed mobility. Thus, data transmission exploits the multiple hop relay method. However, multiple hop relays are prone to data leakage risks, which may lead to the leakage of private information. Furthermore, people are paying increasing attention to their own privacy and data security [15-21]. Therefore, this paper addresses the problem of privacy leakage in VSNs. Combined with modern communication technology (5G), the method in this paper effectively protects the vehicles’ location and trajectory privacy in the VSN.

With the increasing number of connected devices and demand for data rate, the 5G wireless communication system has been a popular research area in recent years [22-23]. The next 5G can serve all types of applications/systems with extremely high user rates anytime and anywhere [24]. As a Wireless Sensor Network (WSN), VSNs will inevitably lead to extraordinary developments with the application of 5G. Compared with other WSNs, VSNs realize the modern Intelligent Transport System (ITS). However, VSNs have inherent characteristics, such as high mobility and multiple hop relays. Thus, Mobile Femtocell (MFemtocell) has been introduced for 5G technology [25]. The use of MFemtocell can significantly maximize performance, such as by realizing dynamic linking, enhancing user throughput, and reducing response times and signal overhead [26-27].

To reduce traffic accidents, vehicles send safety message periodically. The safety message includes information about the location, speed and direction of the vehicles. Although the VSN can be plugged into the 5G network seamlessly, the 5G-based VSN does not consider privacy preservation. If a malicious attacker continuously eavesdrops on the safety message, the location and trajectory privacy may be leaked. To address this problem, researchers have proposed efficient schemes that include K-anonymity [28], Mix-zone [29], MixGroup [30], and Encryption [31-32]. The basic ideas behind these schemes are consistent. Each vehicle is assigned a pseudonym in the VSN, and then vehicles exchange the pseudonyms with each other to obscure the vehicles' real identities. Therefore, the attacker cannot link the real identity to the corresponding vehicle, and the location privacy is protected.

Thus far, the MixGroup method is the most advanced and effective for preserving privacy among the existing schemes. By combining the Mix-zone and group signature technology, the MixGroup algorithm extends the group region and increases the opportunities for exchanging pseudonyms to protect location privacy as shown in Fig. 1 [30]. Nevertheless, the division of the group region in the MixGroup method has three main shortcomings. First, the response time of MixGroup cannot meet the real-time demand of the VSN. Second, the static division of the group region (as shown in Fig. 1) cannot be applied perfectly in future 5G architecture, because 5G MFemtocell technology is dynamic and allows the vehicle to adaptively access the core network. Third, because the division of the group region is based on the vehicles' routes while moving, the MixGroup method cannot effectively protect the vehicles' trajectory privacy. User behavior is known to have certain regular characteristics over a long period of time. Because of work or family circumstances, vehicles regularly drive past a number of fixed locations or traverse along fixed trajectories. Because of this certain regularity, the division of the group region is vulnerable to leak trajectory privacy in the MixGroup method.

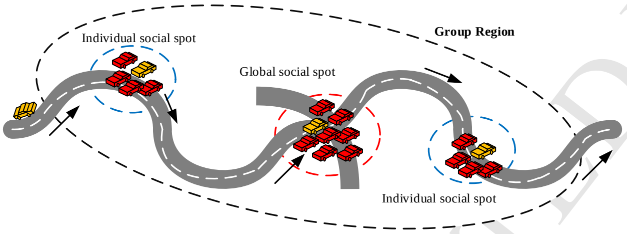

Fig. 1: MixGroup method

To address the main shortcomings of the MixGroup method, we design a novel 5G-based VSN architecture and propose the Dynamic Group Division algorithm (DGD) for the protection of vehicle location and trajectory privacy. The main contributions of this paper are as follows.

- To improve the real-time demand of the VSN, we combine 5G wireless communication systems and VSNs. This paper includes MFemtocell technology and designs a novel system model, the 5G-based VSNs.
- To quantify the location and trajectory privacy that can be suitably applied in the 5G-based VSNs, this paper improves the composite metric KDT, where K is the average anonymity set size, D is the average distance deviation, and T is the anonymity duration.
- To more effectively protect privacy, we propose the DGD algorithm for the 5G-based VSNs. Based on social/individual hot spots, the DGD algorithm designs the Group Generating Protocol and the Pseudonym Exchanging Protocol to dynamically divide the group region and increase the probability of exchanging pseudonyms.

The remainder of this paper is organized as follows. In Section 2, we review related works on the development of integration between 5G networks and VSNs and schemes for preserving privacy in VSNs. In Section 3, we describe the basic concepts and relative definitions. In Section 4, the motivation, objective and system model are revealed. In Section 5, a detailed description of the DGD algorithm is provided. In Section 6, the simulation environment and results are presented. In Section 7, the conclusions of this paper are provided.

2. Related Work

Significant attention has been focused on the problems of privacy preservation and real-time demand in VSNs [33-35]. With the constant development of communication technology, higher speeds and greater bandwidth have promoted the development of integration between the 5G network and VSNs. Through IEEE 802.11p, the work in [36] proposes a 5G-VANET (Vehicular Ad Hoc Network) architecture to realize adaptive clustering, which can reduce the system response time and improve the real-time demand of VANET. The authors in [37] address the security and privacy issues in 5G-enabled vehicular networks and propose the scheme of a real-time video reporting service in a 5G network framework. For protecting the privacy of a video reporting service in vehicular networks, the authors exploit the method of pseudonym management combined with the high speed and low delay characteristics of the 5G network. The study presented in [38] presents a 5G-enabled vehicular network and introduces 5G technologies, such as Device-to-Device (D2D), Enhanced Cloud Radio Access Network (EC-RAN) and Heterogeneous Network (HetNet), into the vehicular network. Moreover, C. Wang, et al. [25] propose a MFemtocell network. MFemtocell is a 5G technology that combines mobile relays with Femtocells. MFemtocell can be deployed in vehicular networks to provide enhanced throughput and spectrum efficiency. With the integrated application of the 5G and vehicular network, MFemtocell allows for the demands of VSNs to be met in real-time and with heavy data traffic.

In VSNs, vehicles can easily access location-based services for the convenience of drivers [39-40], such as finding the nearest gas station or supermarket. Therefore, protecting the location and trajectory privacy of vehicles has received increasing attention recently. With the technology of homomorphic encryption, the work in [41] realizes privacy preservation through the sharing of encryption and trajectories between vehicles. However, because of this sharing, the approach [41] works on the condition that the density of vehicles is high. Other approaches [42-48] have adopted the authentication mechanism to meet the requirement of privacy protection. Facing the challenges of real-time demand in VSNs, researchers have also proposed lightweight authentication mechanisms. For example, Wang [44] proposes a Two-Factor Lightweight Privacy-preserving authentication scheme (2FLIP) that employs the decentralized CA and biological-password based two-factor authentication. Although the 2FLIP scheme can reduce the costs of authentication and realize conditional privacy protection, the safety of the whole scheme heavily relies on the unique system key of the CA. Abbas [46] proposed a hierarchical pseudonymous authentication protocol that divides pseudonyms into two sub-ranges, primary and secondary, based on the time. The lifecycle of the primary pseudonym is longer than that of the secondary pseudonym. The primary pseudonym is used to communicate with partially trusted institutions, whereas the secondary pseudonym is used between vehicles. This scheme is beneficial to reduce the system burden of the VSN, and it is no longer dependent solely on the CA.

Although the schemes mentioned above have addressed preserving the privacy of the VSN under certain conditions, they are inefficient when the VSN is applied in 5G networks. Moreover, most studies have barely focused on location privacy preservation and have ignored the trajectory privacy of moving vehicles. Under the synthetic consideration of real-time demands and privacy preservation, this paper addresses the issue of location and trajectory privacy in 5G-based VSNs.

3. Preliminaries

In this section, we provide a detailed introduction to certain basic concepts relevant to MFemtocell technology and social/individual hot spots. The definition of KDT used in this paper is subsequently provided.

A. Mobile Femtocell

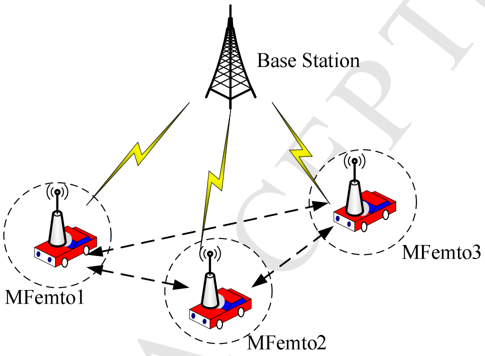

Fig. 2: Vehicles with MFemtocell

To meet the high-mobility demand of users, the architecture of the 5G network incorporates the technology of MFemtocell, which combines the mobile relay and femtocell network. The wireless interface of MFemtocell is backwards compatible with all the existing terminal equipment. Thus, MFemtocell can be seamlessly connected to VSNs. As shown in Fig. 2, MFemtocell is always deployed on fast-moving vehicles, such as cars, trains, buses, etc. With the help of MFemtocell, vehicles can adaptively communicate with other vehicles or the Base Station. Therefore, this technology can improve the throughput and reduce the system response rate. Furthermore, MFemtocell can dynamically access the wireless network and effectively resolve the problems caused by the topology of VSNs, which do not have a center node and change quickly.

B. Social hot spots and individual hot spots

A hot spot is a location that users are interested in. In this paper, all locations can be classified into two categories: social hot spot and individual hot spot. Social hot spots are characterized by a location with a high density of vehicles, such as crossroads, parking lots, etc., where vehicles easily encounter each other. Because many meeting opportunities occur for vehicles in social hot spots, existing privacy protection methods (e.g., Mix-Zone) usually take advantage of social hot spots for exchanging the pseudonyms of vehicles. Then, malicious attackers cannot guess the vehicle's real identity, and the vehicles' location and trajectory privacy are protected.

Although individual hot spots are characterized by frequent vehicle visits, most people generally drive to and from their places of work and their homes over a long period of time. Therefore, most drivers regularly visit certain fixed locations, such as the supermarket near the driver's home or the gas station on the way to work as shown in Fig. 3. Of course, one location may be an individual hot spot as well as a social hot spot for certain drivers, and when this occurs, we define the location as a social hot spot by default.

In this paper, the location of a hot spot (including social hot spot and individual hot spot) is denoted by *PL* (*x*, *y*), where *x* and *y* represent the latitude and longitude of the area of the hot spot, respectively. To effectively protect vehicle location and trajectory privacy in the 5G-based VSNs, our paper dynamically divides the group area by the definition of *PL*.

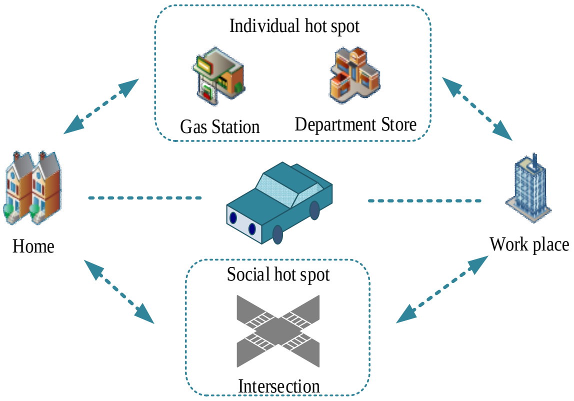

Fig. 3: Social/individual hot spot

C. Quantification for trajectory privacy

Trajectory privacy is the degree to which an entity cannot be linked to the vehicles' trajectory over a consecutive time. In this paper, we adopt a composite metric KDT [49] to quantify the trajectory privacy, where *K* refers to the average anonymity set size, *D* is the average distance deviation, and *T* is the anonymity duration. Considering realistic demands, we redefine KDT as follows.

(1) Anonymity Duration *T*: In our paper, for a better description of the trajectory privacy, we define *T* as a constant. *T* is a set of time $\{t_0, t_1, \ldots, t_i, \ldots, t_n\}$. Therefore, a vehicle is driven for a continuous time *T* (starting from t_0 to t_n), and generates a trajectory.

(2) Average Anonymity Set Size *K*: Assume that K_{ti} represents the number of vehicles in a group area at time t_i. Then, we can find the expression of average anonymity set size *K*.

$$K=\frac{K_{t_0}+K_{t_1}+\ldots+K_{t_i}+\ldots+K_{t_n}}{n+1}, t_i>0, i=0,1,2,\ldots,n \qquad (1)$$

According to the knowledge of random processes, we know that the number of vehicles that arrive at the group region follows a Poisson distribution $\{N(t)\}$. The one-dimensional probability distribution of $N(t)$ is as follows:

$$P\{N(t)=k\}=\frac{(\lambda t)^k}{k!}e^{-\lambda t}, k=K_{t_0}, K_{t_1}, \ldots, K_{t_n} \qquad (2)$$

Therefore, we can calculate the expectation $E\{N(t)\}=\lambda t$, where $t \in [t_0, t_n]$, and λ is the average number of vehicles arriving in the group area per unit time.

(3) Average Distance Deviation *D*: At time t_i, suppose that there are two vehicles (u_m, u_k) in a group area and the number of vehicles in the group is Kt_i. Here, we define the distance d_{mk} between two vehicles (u_m, u_k):

$$d_{mk}=\sqrt{(x_m-x_k)^2+(y_m-y_k)^2} \qquad (3)$$

where (x_m, y_m) is the location of vehicle u_m and (x_k, y_k) is the location of vehicle u_k. Assume that P_{mk} is the probability of identity confusion between vehicles. That is, an attacker guesses that vehicle u_m is vehicle u_k with probability P_{mk}.

Thus, we can obtain the distance deviation d_{t_i} at time t_i:

$$d_{t_i}=\frac{1}{(K_{t_i})^2}\sum_{m=1}^{K_{t_i}}\sum_{k=1}^{K_{t_i}}d_{mk}P_{mk} \qquad (4)$$

Then, the average distance deviation *D* is calculated at the anonymity duration *T*:

$$D=\frac{d_{t_0}+d_{t_1}+\ldots+d_{t_i}+\ldots+d_{t_n}}{n+1}, t_i>0, i=0,1,2,\ldots,n \qquad (5)$$

For the best trajectory preservation, we must maximize the average anonymity set size *K* and the average distance deviation *D* for a continuous time *T* (Anonymity Duration). Greater average anonymity set sizes and average distance deviations correspond to better operability of anonymous schemes for vehicles. Therefore, this scheme can more effectively protect the trajectory privacy. However, *K* and *D* are not infinite values. Therefore, assume that the upper limit of Kt_i and d_{ti} are K_{max} and d_{max}, respectively. The values of K_{max} and d_{max} are substituted into formula (1) and (5). In addition, the maximum of *K* and *D* are also K_{max} and d_{max}, respectively.

4. MOTIVATION AND SYSTEM MODEL

This section provides the motivation and objective of this paper. Then, we design a 5G-based VSN system model for solving the problem of real-time demand and privacy preservation.

4.1 Motivation

The construction of the MixGroup framework [30] extends the pseudonym-changing regions with the Mix-zone and group signature mechanism, and it addresses the location privacy issue in VSNs. However, the MixGroup framework does not consider a method of protecting trajectory privacy. According to the vehicles' paths while moving, MixGroup statically generates a group region. Assume that a malicious attacker has joined in the group region. Then, he/she will constantly exchange pseudonyms with other vehicles located in the same group region and will keep trying to exchange pseudonyms until leaving the group region. The malicious attacker can draw the outline of the group region. By matching group regions with the map (e.g., Google Maps), the attacker learns the trajectories of vehicles. If the attacker obtains other information, such as the work location, personal interests, etc., he/she can easily know the real trajectory of the vehicles. There is no guarantee that the users' trajectories will not be exposed; thus, the users' trajectory privacy is leaked. Therefore, preserving privacy is insufficient in the MixGroup framework. In this paper, we aim at protecting the location and trajectory privacy in VSNs.

Furthermore, the real-time demand of the VSN is significant. Therefore, using a VSN does not make sense unless the vehicles obtain a quality-of-service guarantee for real-time services. To improve the pseudonym exchange opportunities, the MixGroup framework generates group regions with the static methods. The MixGroup framework does not consider the time cost. However, because of the development of mobile communication technology, an increasing number of vehicles have accessed VSNs. Therefore, the static division of the group region is not appropriate for the rapid development of the Internet. To support the large amount of data traffic and meet real-time demands, this paper introduces 5G MFemtocell technology. MFemtocell can dynamically connect to an operator's core network. This dynamic characteristic will greatly improve the system response time and meet the real-time demand in VSNs.

4.2 Objective

In this paper, we aim to propose the DGD algorithm for protecting location and trajectory privacy in 5G-based VSNs. First, we build a novel system model with the introduction of the MFemtocell. Then, with the help of MFemtocell, the vehicles can be dynamically brought together for generating a group in time T (Anonymity Duration). The average anonymity set size K and the average distance deviation D of the group must meet certain conditions for reaching the degree of privacy required by the users. Finally, the DGD algorithm exchanges the identities in the same group with pseudonym entropy principle. By increasing the opportunities to exchange vehicle identities, the ability of an attacker to determine the real identity of a vehicle is hindered.

Thus, based on the MFemtocell technology, hot spot concept and composite metric KDT, the problem of protecting a vehicles' location and trajectory privacy is resolved by maximizing the average anonymity set size K and the average distance deviation D for a continuous time T (Anonymity Duration) in the 5G-based VSNs.

4.3 System model

To meet the real-time demand of vehicles and preserve vehicular privacy, we introduce the MFemtocell technology and design a VSN model, and its framework is shown in Fig. 4. The framework consists of three key components: Vehicles, Registration Authority (RA) and Base Station.

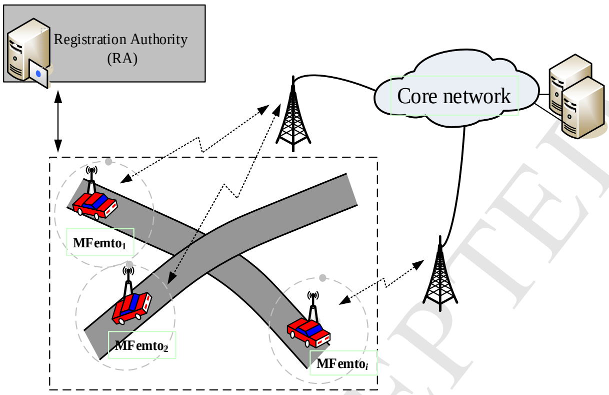

Fig. 4: Framework of the 5G-based VSNs

Vehicles: the moving entities in the VSN. Each vehicle is equipped with a MFemtocell for communication between vehicles or with the users inside the vehicle.

RA: In this paper, the RA is a strictly trusted third party entity, and it can potentially benefit the system security by generating secure parameters {*PID*, *PK*, *SK*, *Cert*} for the entities in the proposed system model, where *PID* is the pseudonym identity for the entities, such as vehicles, groups, etc.; *PK/SK* is the public-private key pair used to encrypt or decrypt messages to ensure information security; and *Cert* is the certification parameter applied in the group signature mechanism for preventing the information from being tampered with, forged or imitated.

Base Station: located between the vehicular network and the core network. The Base Station can directly communicate with the MFemtocell for collecting information from vehicles. Then, the Base Station sends the gathered messages to the core network where they are processed, and then they are fed back to the Base Station.

Fig. 4 shows that the framework of the 5G-based VSN has been divided into four main stages: system initialization, group generating, pseudonym exchange, and group cancellation.

1) *System initialization*: In our proposed system model, the RA is a fully trusted entity and it boots and initializes the whole system. The RA can verify the legitimacy of each entity in the VSN and assign the corresponding secure parameters *PID*, *PK/SK*, *Cert* for the legal entities. Of course, the RA server stores the vehicles' true identities and pseudonym identities, which contributes to tracking offenders for law enforcement. Because the RA is a trusted entity, the problem of privacy leakage from the RA server is not an issue.

2) *Group generating*: If a moving vehicle v_i sends the safety message periodically, MFemtocell technology allows the vehicle v_i to dynamically generate group regions along the vehicle's trajectory. If the vehicle v_i sends a safety message in one location, then the group region is generated based on the values of K_{max} and d_{max}.

3) *Pseudonym exchange*: In the group region, vehicles communicate with a group identity between the Base Station and vehicles. To protect the location and trajectory privacy, vehicles located in the same group region need to exchange pseudonyms with each other constantly. Thus, vehicles will obtain a different pseudonym after moving out of a group region every time, which increases the difficulty for a malicious attacker to guess the real identity of the vehicles.

4) *Group cancellation*: With the moving of the vehicle, the group region will be changed constantly along the trajectory of the vehicle. Therefore, the group region is generated and revoked alternately. When a group cannot meet the requirements of the system (e.g., anonymity entropy), the group will be revoked automatically with the help of MFemtocell and the source of the group will be recycled by the RA.

5. Algorithm Design

In this section, we first present the framework of the DGD algorithm. Then, we introduce three protocols in the DGD algorithm accordingly: Group Generating Protocol, Pseudonym Exchanging Protocol and Group Revocation Protocol.

5.1 DGD algorithm

Fig. 5 describes the framework of the DGD algorithm. The DGD algorithm addresses the location and trajectory privacy in the 5G-based VSNs. When a vehicle sends the safety message periodically from one location, the location privacy is protected. First, the vehicle generates a group region using the method that is introduced in the Group Generating

Protocol. Then, to protect the location privacy, all vehicles exchange pseudonyms with each other in the same group. When a vehicle is moving, location privacy as well as trajectory privacy should be considered. To dynamically generate group regions along the trajectory, the DGD algorithm calls the Group Generating Protocol and Pseudonym Exchanging Protocol alternately.

Algorithm 1 describes the pseudo code of the DGD algorithm.

***Algorithm* 1: Dynamic Group Division (DGD)**

```
if (vehicle is moving)
    Call for the Group Generating Protocol alternately;
    Dynamically obtain group regions;
    if (One group region is unsuccessful)
        Go to the scheme of location privacy;
    else
        Call for Pseudonym Exchanging Protocol alternately;
    end if
else
    Generate a group region for the vehicle;
    Exchange pseudonyms with each other;
end if
Call for Group Revocation Protocol.
```

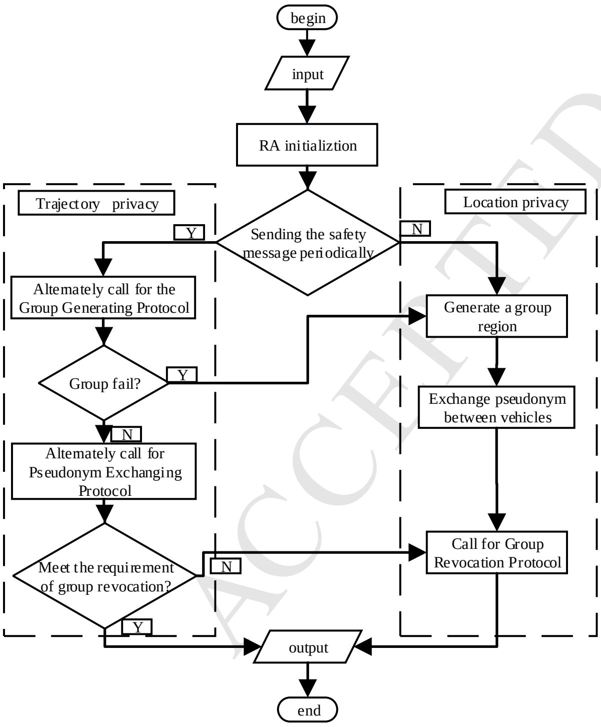
begin
input
RA initializtion
Trajectory privacy
Location privacy
Sending the safety message periodically
Y
N
Alternately call for the Group Generating Protocol
Group fail?
Y
N
Alternately call for Pseudonym Exchanging Protocol
Meet the requirement of group revocation?
N
Y
Generate a group region
Exchange pseudonym between vehicles
Call for Group Revocation Protocol
output
end

Fig. 5: Framework of the DGD algorithm

5.2 Group Generating Protocol

If a vehicle has been accessing the VSNs, then the RA will validate the identity of the vehicle. After finishing system initialization, the MFemtocell can help the vehicle automatically interact at the same social/individual hot spot. According to the area size of the hot spot, different cells are generated as shown in Fig. 6. To preserve privacy, we propose the Group Generating Protocol to expand the area of the group constantly, and then a group region is dynamically generated.

Here, we explain the main procedure of group generating. First, when a vehicle v_1 enters a social/individual hot spot, it will monitor whether there are other vehicles in the same hot spot that are sending the Cell-Generate-Request message. If a vehicle v_2 has initiated the request message for cell generating, vehicle v_1 will join the cell. Otherwise, vehicle v_1 initiates the request message. Within a timestamp t_{stamp}, the cell is finished and the vehicle that first sends the request message becomes the Cell Leader. Second, the Cell Leader broadcasts the Group_Generte_Request message to find the other vehicles. When the number of vehicles in the group is larger than the maximum value K_{max} (that is, $Kt_i>K_{max}$) or the distance deviation between vehicles is larger than the maximum value d_{max} (that is, $d_{ti}>d_{max}$), then the group is finished. Otherwise, the area of group will be extended to find appropriate vehicles for the time t_{stamp}. Fig. 6 describes the generative process of the group region. Because the social hot spot is generally an intersection, the trajectory map in the group region is complicated because of different directions of the trace intersection. Therefore, the group division mechanism in the DGD algorithm can more effectively protect the vehicles' trajectory privacy compared with the privacy-preserving scheme MixGroup.

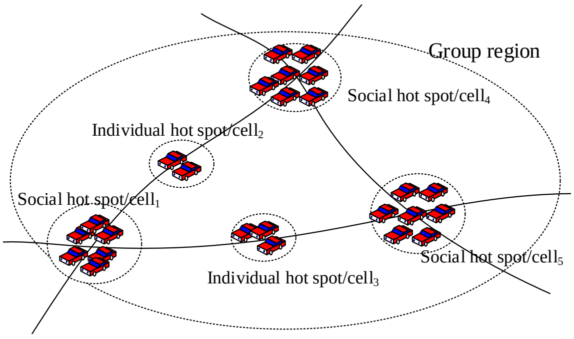

Fig. 6: Group division mechanism

Algorithm 2 describes the pseudo code of the Group Generating Protocol in details.

***Algorithm* 2: Group Generating Protocol**

```
Input: $PID_v$, $PK_v$, $SK_v$, $Cert_v$, $PL$, $t_{stamp}$, $K_{max}$, $d_{max}$
Output: $GID$, $PK_G$, $SK_G$, $Cert_G$
A vehicle $v_i$ enters a hot pot and listens for the request
  message for cell generating;
for ($t_{stamp}$ >=0)
    if (vehicle $v_i$ receives the message Cell_Generte_Request)
        Join in the cell;
    end if
    else
        Initiate the request message Cell_Generte_Request=$PID_v$,
        &$PK_v$, &$SK_v$, &$Cert_v$;
    The vehicle $v_i$ becomes the Cell Leader and waits for other vehicles to join;
Cells are finished;
Select a cell leader as the group leader by the principle of first come first service;
Broadcast the request message Group_Generte_Request;
for ($Kt_i$<=$K_{max}$ && $d_i$<=$d_{max}$)
    for (PL (the cell leader nearby group leader)∈ social hot spot)
        The cell leader agrees to join group;
        Calculate $Kt_i$ and $d_i$;
        if ($Kt_i$>=$K_{max}$||$d_i$>=$d_{max}$)
            break;
        end if
    end for
    The cell leader (PL∈ individual hot spot) agrees to join group;
    Calculate $Kt_i$ and $d_i$;
end for
if ($t_{stamp}$ <0)
    Group generation fails;
end if
else
Group is finished;
Group leader sends the message to the RA;
RA judges its legitimacy and distributes GID, $PK_G$, $SK_G$, $Cert_G$ for valid groups;
end for
```

As shown in *Algorithm 2*, group generation consumes a certain amount of time (within the timestamp t_{stamp}). Thus, time is the key point for the Group Generating Protocol. If the time setting is shorter, then Kt_i and d_i are accordingly smaller and cannot reach the requirements of privacy preservation. If the time setting is longer, then procedure of group generation will waste too much time waiting and cannot meet the user's requirements.

5.3 Pseudonym exchange protocol

To protect the vehicles' location and trajectory privacy outside of the group area, vehicles periodically send safety messages with pseudonym identities. Vehicles directly communicate with the Base Station. Inside of the group area, vehicles employ group identity (*GID*). To ensure that the attacker cannot deduce the vehicles' real identity, this paper increases the pseudonym exchanging opportunities. When a vehicle enters a group region, the vehicle will continuously exchange pseudonyms with other vehicles until the vehicle leaves the group region. A condition for exchanging pseudonyms between vehicles is observed. Assume that each vehicle has the probability of being tracked by a malicious attacker denoted by p_i. Thus, the pseudonym entropy H for the vehicles $\{v_1, v_2, \dots, v_k\}$ in a group region can be expressed as follows:

$$H = -\sum_{i=1}^{k} p_i \log_2 p_i$$

When the vehicle's pseudonym is changed, the probability p_i and the pseudonym entropy H are changed. Therefore, this paper exploits the entropy of the group to exchange the vehicles' PIDs to preserve privacy.

The pseudo code of the Pseudonym Exchanging Protocol is shown in *Algorithm* 3. Here, we consider the privacy preservation of vehicle v_i in group region *Gr*. Before exchanging the pseudonym of vehicle v_i, we first calculate the pseudonym entropy of the *Gr*, which is denoted by the symbol H_{befor}. Thus, H_{before} is the entropy before exchanging. In the valid anonymity duration *T*, if vehicle v_i receives the message pseudonym_exchange_ Request from a vehicle v_j, we will estimate the pseudonym entropy of the group region *Gr* denoted by the symbol H_{after}. Of course, the vehicle v_j also belongs to the group region *Gr*. If the pseudonym entropy H_{after} is greater than H_{before}, the two vehicles v_i and v_j will interexchange pseudonyms. In contrast, vehicle v_i will abandon the opportunity of exchange because smaller pseudonym entropy corresponds to lower the level of privacy protection.

In summary, for privacy preservation in the Pseudonym Exchanging Protocol, we calculate the pseudonym entropy H before two vehicles exchange pseudonyms. If H is increased by exchanging pseudonyms, then the two vehicles will successfully complete the process of pseudonym exchange. Otherwise, the exchange will be abandoned.

***Algorithm* 3: Pseudonym Exchanging Protocol**

Input: *Gr, GID, T*

Output: H_{after}, PID_v, PK_v, SK_v, $Cert_v$,

```
for (a vehicle $v_i$∈Gr)
    Calculate the pseudonym entropy $H_{before}$; // $H_{before}$ is the entropy before exchanging.
    if (T !=0&&vehicle $v_i$ receives the message pseudonym
     _exchange_Request from a vehicle $v_j$) // ($v_j$∈Gr)
        Calculate the pseudonym entropy $H_{after}$; // $H_{after}$ is the entropy after exchanging.
        if ($H_{after}$-$H_{before}$>0)
            Exchange pseudonyms <$v_j$, $v_i$>;
        end if
        else
            Abandon the exchange;
    end if
else
    Send the request message pseudonym_exchange
    _Request and wait the exchanging;
Group Leader sends the exchanged pseudonyms to RA;
end for
```

5.4 Group Revocation

When a vehicle leaves the group region, it will send a message about leaving the group to the Group Leader. If the lifetime of the vehicle is zero (T_{life}=0), then the vehicle will automatically apply to leave the group. When the number of vehicles in a group is less than the minimum value K_{min} (that is, $Kt_i<K_{min}$) or the distance deviation between vehicles is less than the minimum value d_{min} (that is, $d_{ti}<d_{min}$), we determine that the existence of the group is meaningless. Thus, the group will be revoked by the RA. *Algorithm* 4 presents the pseudo code of the Group Revocation Protocol.

Algorithm **4: Group Revocation Protocol**

```
Input: Group region, GID, $T_{life}$, $K_{min}$, $d_{min}$
Output: Resources of group
if (a vehicle $v_i \notin$ Group region || $T_{life}$,<=0)
    Initiate the message leaving_group_ request;
    Calculate $Kt_i$ and $d_i$;
    if ($Kt_i<K_{min}||d_i<d_{min}$)
  Group leader sends message of group revocation 6: to RA;
        RA recovers the corresponding resources of the group;
    end if
end if
```

6. Simulation And Results

In this section, we conduct extensive simulations and evaluate the performance and effectiveness of our proposed DGD algorithm under city and suburban scenarios. We first describe the simulation environment for the city and suburban scenarios. The simulation results from three aspects (anonymity set size *K*, distance deviation *D* and pseudonym entropy *H*) are then presented in charts. Finally, through the analysis of the simulation, we show that our proposed DGD algorithm can effectively protect the location and trajectory privacy in 5G-based VSNs.

6.1 Simulation Environment

Table 1: Simulation parameters

Parameter	Setting
Vehicle Speed	30 km/h
Vehicle density	0.3 v/m for city scenario
Vehicle density	0.2 v/m for suburban scenario
Anonymity Duration	600 s
K_{min}	35
d_{min}	600 m
K_{max}	50
d_{max}	750 m

We first simulate a graph to represent a large real geographic area (3000 m×3000 m) using the Generic Mobility Simulation Framework, GMSF[50]. For emulating the performance of MFemtocell, we add certain functions to the GMSF simulator that are compliant with 3GPP LTE specifications[51]. Then, we divide the graph into 10×10 small cells. Each cell is labeled a social hot spot or individual hot spot according to the real geographic area. To determine whether to exchange pseudonyms, each vehicle is labeled with an ordered pair <PID_{vi}, p_i>, where PID_{vi} represents the vehicle identity and p_i is the tracked probability.

As we know, GMSF supports the import of vehicle traces for three different areas (city, suburban and rural). For simulating the different road information in Chengdu City, Sichuan Province, China, we design a city scenario and a suburban scenario. The only difference between the two scenarios is the vehicle density. We set the vehicle density of the city scenario as 0.3 v/m (that is, 900 vehicles in 3000 m × 3000 m area), whereas we set the vehicle density of the suburban scenario as 0.2 v/m (that is, 600 vehicles in 3000 m × 3000 m area). Table 1 shows the simulation parameters in details.

6.2 Simulation Results

A. Location Privacy

To simplify our experiment, we assume that a vehicle is in the social hot spot and sends a request message for group generating. We analyze the location privacy in the city scenario and suburban scenario from two aspects: anonymity set size and distance deviation.

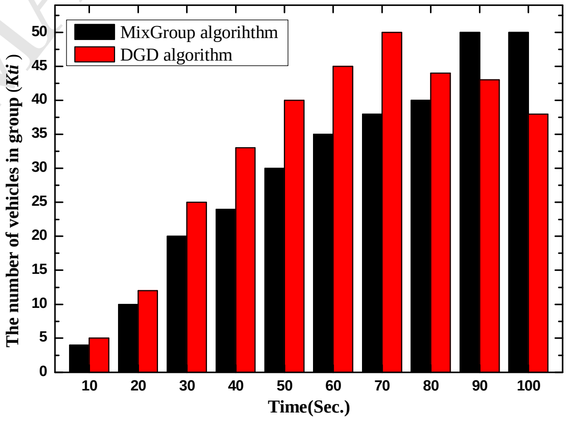

Fig. 7: Anonymity set size of a group region for the city scenario

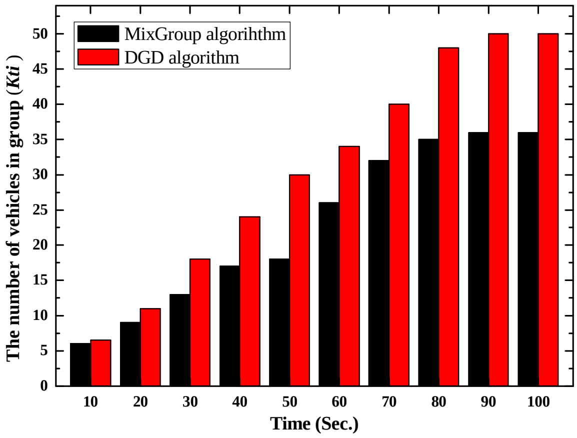

Fig. 8: Anonymity set size of a group region for the suburban scenario

In Fig. 7, we measure the anonymity set size (K_{ti}) of a single group region within 100 s in the city scenario, which shows that the anonymity set size with the DGD algorithm is larger than the MixGroup algorithm when the time t≤80 s. Our proposed DGD algorithm approaches the maximum (K_{max}=50) at t=70 s, whereas the MixGroup algorithm achieves the K_{max} value at t=90 s. Evidently, with the assistance of MFemtocell, the DGD algorithm possesses a faster convergence rate. Hence, from perspective of protecting the location privacy in a city scenario, the DGD algorithm can perform better compared with the MixGroup algorithm.

However, the MixGroup algorithm approaches the maximum (K_{max}=50) in a lower density area in the suburban scenario. As shown in Fig. 8, although the DGD and MixGroup algorithm obtain their peak almost simultaneously (at approximately t=80 s), the anonymity set size in the DGD algorithm is much larger than that of the MixGroup algorithm. A larger anonymity set size corresponds to a greater intensity of privacy preserving. Thus, our proposed DGD algorithm shows its superior performance of protecting location privacy in the suburban scenario.

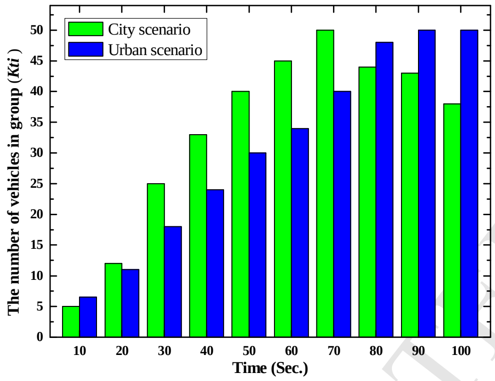

Fig. 9: Anonymity set size of the city vs. suburban scenario

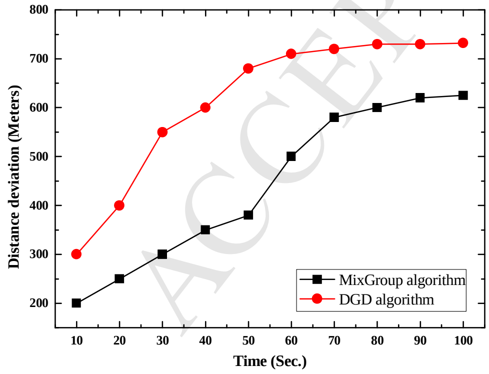

Fig. 10: Distance deviation of a group region for the city scenario

Fig. 9 compares the anonymity set size between the city scenario and suburban scenario in the DGD algorithm. Because the vehicle density is higher in the city scenario than the suburban scenario, the DGD algorithm obtains the maximum anonymity (K_{max}=50) at t=70 in the city scenario and at t=90 in suburban scenario. Therefore, the DGD algorithm can protect location privacy well in both the city scenario and the suburban scenario.

Fig. 10 compares the distance deviation of a single group region between the DGD and MixGroup algorithm in the city scenario. Fig. 10 shows that the convergence rate of the DGD algorithm is faster than that of the MixGroup algorithm. The DGD algorithm achieves the convergence value at approximately t=60 s, whereas the MixGroup algorithm achieves it at 80 s. This finding further demonstrates that our proposed DGD algorithm has faster response speeds and effectively protects location privacy under the city scenario.

The distance deviation of a group region for the suburban scenario is shown in Fig. 11. Two rapid increases are observed at t=30s and t=60s separately in MixGroup algorithm, while the growth of distance deviation shows a smooth increase in our proposed DGD algorithm. These data reveal that there are two social hot spots in the MixGroup algorithm, which may be caused by the leaking of location privacy, whereas the DGD algorithm performs better in preserving location privacy.

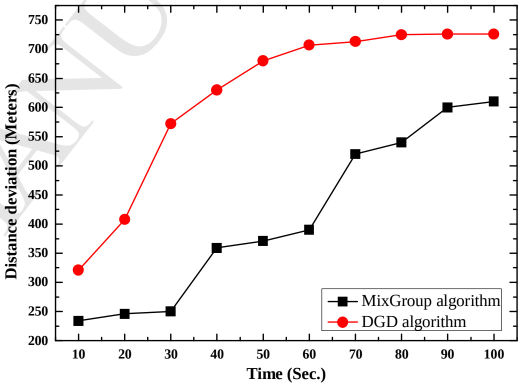

Fig. 11: Distance deviation of a group region for the suburban scenario

Fig. 12 compares the distance deviation of a group region between the city and suburban scenarios. We find that the distance deviation is smaller in the city scenario than in the suburban scenario when t<60 s. However, the distance deviation of the city scenario overlaps the suburban scenario on the end. Both scenarios realize location privacy preservation when the distance deviation falls between 750 m (d_{max}) and 600 m (d_{min}).

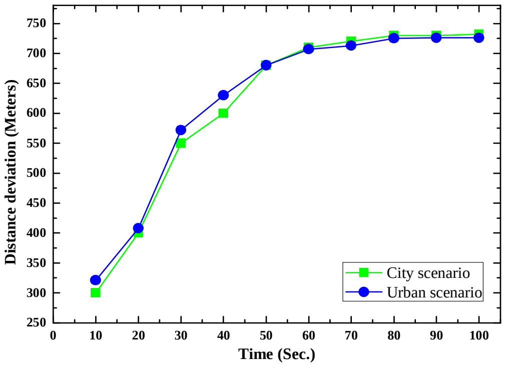

Fig. 12: Distance deviation for the city vs. suburban scenario

B. Trajectory Privacy

To better measure the trajectory privacy, we also assume that a vehicle starts in a social hot spot and sends a safety message periodically with a speed of 30 km/h. Then, a trajectory is generated that includes 6 group regions in the anonymity duration (*T*=600 s). Here, the trajectory privacy is described with the average anonymity set size, average distance deviation and pseudonym entropy.

Fig. 13 shows the anonymity set size of the trajectory under the city scenario. Comparing the DGD and MixGroup algorithm, the *K* in the DGD algorithm is larger than that of the MixGroup overall. Through formula 1, we can calculate the average anonymity set size as *K*=42.33 in the MixGroup algorithm, whereas the *K*=47.20 in the DGD algorithm. Hence, our proposed algorithm can effectively protect the trajectory privacy in the city scenario.

In the MixGroup algorithm for the suburban scenario, three types of time settings {200 s, 500 s, and 600 s} are observed in which the anonymity set size is below the minimum (K_{min}=35). Fig. 14 shows that the average anonymity set size *K* is 34.63. However, the anonymity set size of the DGD algorithm is close to the K_{max}, and the average anonymity set size *K* (*K*=43.62) in the DGD algorithm is much larger than that in the MixGroup algorithm. Thus, we find that the DGD algorithm effectively provides the service of trajectory privacy preservation in the suburban scenario.

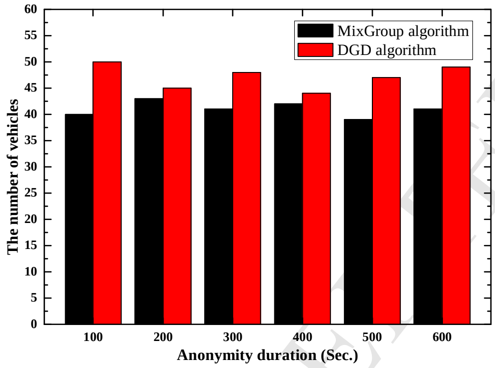

Fig. 13: Anonymity set size of a trajectory in the city scenario

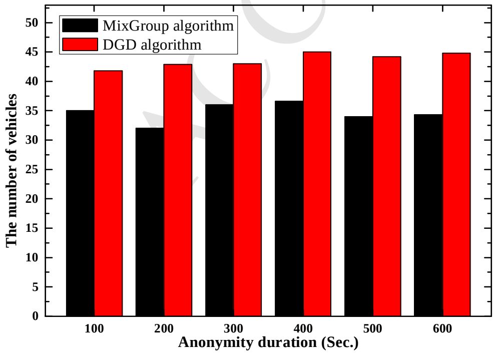

Fig. 14: Anonymity set size of a trajectory in the suburban scenario

Fig. 15 compares the anonymity set size on the trajectory between the city scenario and suburban scenario. In general, the anonymity set size in the city scenario is larger than that in the suburban scenario. Based on the above, the performance of our proposed DGD algorithm for trajectory privacy preservation in the city scenario is superior to that of the suburban scenario.

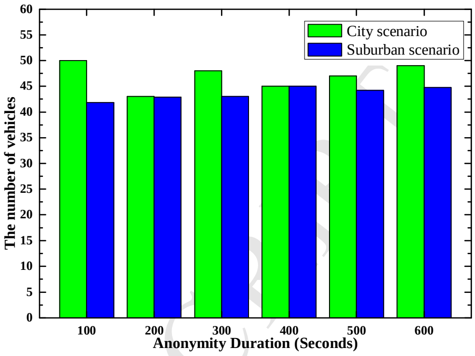

Fig. 15: Anonymity set size for the city vs. suburban scenario

Figs. 16-18 show the distance deviation of the trajectory in the anonymity duration of 600 s. Based on formula 5, the average distance deviation of the DGD algorithm is D=727.67 while that of the MixGroup algorithm is 621.33 in the city scenario (as shown in Fig. 16). In suburban scenario (see Fig. 17), we find that the average distance deviation *D* is 609.17 using the MixGroup algorithm and *D*=723.00 with the DGD algorithm. Thus, the DGD algorithm, which presents a higher average distance deviation, can effectively protect the trajectory privacy both in the city and suburban scenarios.

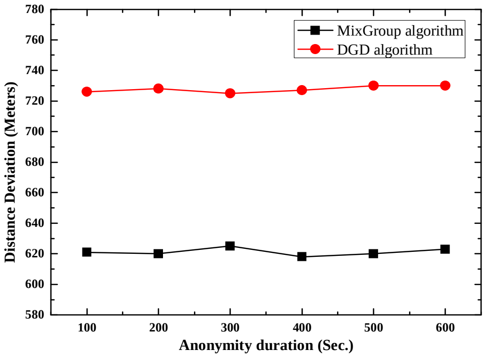

Fig. 16: Distance deviation on the trajectory in the city scenario

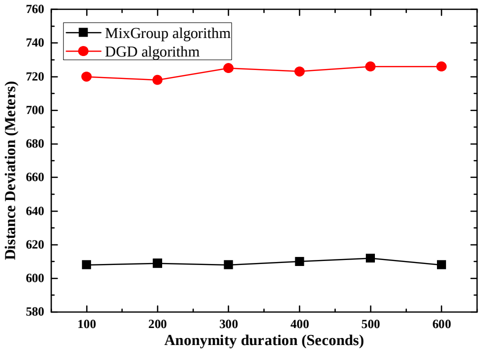

Fig. 17: Distance deviation on the trajectory in the suburban scenario

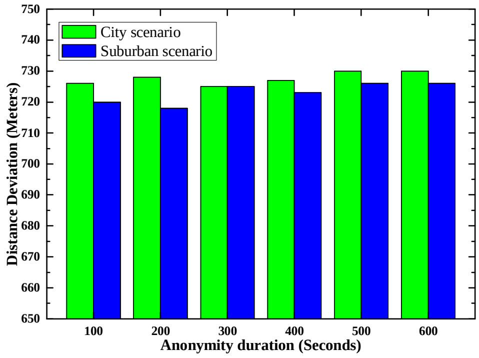

Fig. 18: Distance deviation in the city vs. suburban scenario

We compare the distance deviation between the city scenario and the suburban scenario in Fig. 18. Generally, the distance deviation in the city scenario is larger than that in the suburban scenario. Accordingly, the DGD algorithm is more effective in the city scenario in terms of preserving the trajectory privacy.

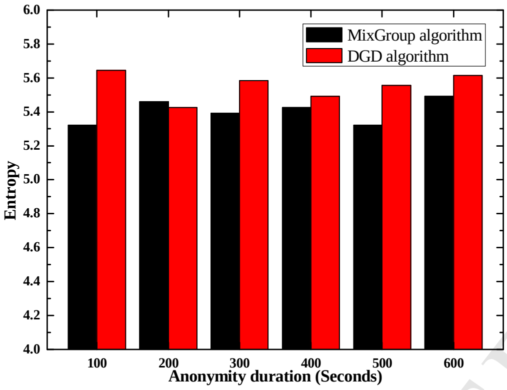

Fig. 19: Pseudonym entropy in the city scenario

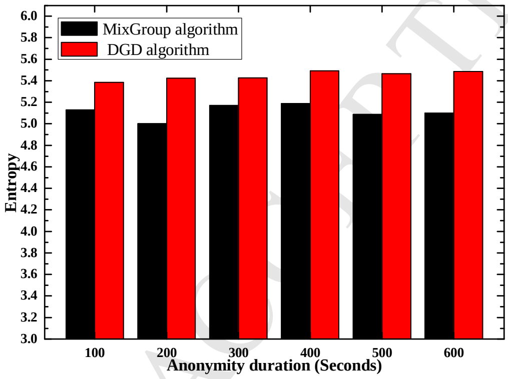

Fig. 20: Pseudonym entropy in the suburban scenario

Fig. 19 compares the pseudonym entropy on the trajectory between the DGD and MixGroup algorithms in the city scenario, and it shows that the pseudonym entropy with the DGD algorithm is larger than that with the MixGroup algorithm. The degree of privacy protection is directly proportional to the pseudonym entropy. From Fig. 20, the same result is found in the suburban scenario. Thus, in both the city scenario and suburban scenario, the DGD algorithm has a strong ability to protect trajectory privacy in the 5G-based VSNs compared with the MixGroup algorithm.

7. Conclusions

In this paper, we studied the problem of protecting location and trajectory privacy in 5G-based VSNs. To dynamically divide the group region and meet the high real-time demands of users, we propose a system model of 5G-based VSNs that applies MFemtocell technology. In our proposed system model, we design an efficient DGD algorithm to protect a vehicle's location and trajectory privacy. The DGD algorithm comprises four stages: system initialization, group generating, pseudonym exchange, and group cancellation. Through the simulations, we show that, compared with existing solutions for generating the group region, our algorithm reduces the time delay and effectively protects the users' location and trajectory privacy in 5G-based VSNs.

Acknowledgement

This research was partially supported by the National Natural Science Foundation of China (61571098), Fundamental Research Funds for the Central Universities (ZYGX2016J217).

References

[1] 5GAA, available on https://www.5gaa.org/, accessed on Mar 9, 2017.

[2] J. Li, Y. Zhang, X. Chen, et al. Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 1-12, 2018.

[3] P. Li, J. Li, Z. Huang, et al. Privacy-preserving outsourced classification in cloud computing. Cluster Computing, 1-10, 2017.

[4] G. Sun, A. Vishal, D. Liao, et al. Power-efficient provisioning for online virtual network requests in cloud-based data centers. IEEE Systems Journal, 427-441, 2015.

[5] J. Li, J. Li, D. Xie, et al. Secure Auditing and Deduplicating Data in Cloud. IEEE Transactions on Computers, 2386-2396, 2016.

[6] P. Li, J. Li, Z. Huang, et al. Multi-key privacy-preserving deep learning in cloud computing. Future Generation Computer Systems, 76-85, 2017.

[7] J. Li, Z. Liu, X. Chen, et al. L-EncDB: A Lightweight Framework for Privacy-Preserving Data Queries in Cloud Computing. Knowledge-based Systems, 18-26, 2015.

[8] G. Sun, D. Liao, D. Zhao, et al. Towards Provisioning Hybrid Virtual Networks in Federated Cloud Data Centers. Future Generation Computer Systems, Available online 18 October, 2017.

[9] G. Sun, D. Liao, D. Zhao, et al. Live Migration for Multiple Correlated Virtual Machines in Cloud-based

Data Centers. IEEE Transactions on Services Computing, 1-14, 2015.

[10]G. Sun, D. Liao, S. Bu, et al. The Efficient Framework and Algorithm for Provisioning Evolving VDC in Federated Data Centers. Future Generation Computer Systems, 79-89, 2017.

[11]X. Chen, J. Li, J. Weng, J et al. Verifiable Computation over Large Database with Incremental Updates. IEEE Transactions on Computers, 3184-3195, 2016.

[12]G. Sun, C. Victor, G. Yang, et al. The Cost-efficient Deployment of Replica Servers in Virtual Content Distribution Networks for Data Fusion. Information Sciences, Available online 10 August, 2017.

[13]G. Sun, D. Liao, A. Vishal, et al. A New Technique for Efficient Live Migration of Multiple Virtual Machines. Future Generation Computer Systems, 74-86, 2016.

[14]D. Liao, G. Sun, H. Li, et al. The Framework and Algorithm for Preserving User Trajectory while using Location-Based Services in IoT-Cloud Systems. Cluster Computing, 2283-2297, 2017.

[15]Y. Zhang, X. Chen, J Li, et al. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 42-61, 2017.

[16]Z. Huang, S. Liu, X. Mao, et al. Insight of the Protection for Data Security under Selective Opening Attacks. Information Sciences, 223-241, 2017.

[17]J. Li, X. Chen, M. Li, et al. Secure Deduplication with Efficient and Reliable Convergent Key Management. IEEE Transactions on Parallel and Distributed Systems, 1615-1625, 2014.

[18]J. Li, Y. Li, X. Chen, et al. A Hybrid Cloud Approach for Secure Authorized Deduplication. IEEE Transactions on Parallel and Distributed Systems, 1206-1216, 2015.

[19]J. Li, X. Chen, X. Huang, et al. Secure Distributed Deduplication Systems with Improved Reliability. IEEE Transactions on Computers, 3569-3579, 2015.

[20]J. Li, X.Huang, J. Li, et al. Securely Outsourcing Attribute-based Encryption with Checkability. IEEE Transactions on Parallel and Distributed Systems, 2201-2210, 2014.

[21]X. Chen, X. Huang, J. Li, et al. New Algorithms for Secure Outsourcing of Large-scale Systems of Linear Equations. IEEE Transactions on Information and Forensics Security, 69-78, 2015.

[22]G. Araniti, M. Condoluci, P. Scopelliti, et al. Multicasting over Emerging 5G Networks: Challenges and Perspectives, IEEE Network, 80-89, 2017.

[23]P. Pekka. A Brief Overview of 5G Research Activities. International Conference on 5G for Ubiquitous Connectivity, 17-22, 2014.

[24]D. Panagtiotis, G. Andreas, T. Kostas, K. Serafim. Intelligent 5G Networks. IEEE vehicular technology magazine, 41-50, 2015.

[25]C. Wang, X. Gao, X. You, et al. Cellular Architecture and Key Technologies for 5G Wireless Communication Networks. IEEE Communications Magazine, 123-130, 2014.

[26]H. Fourat, C. Wang. H. Harald, et al. Spectral Efficiency Analysis of Mobile Femtocell Based Cellular Systems. IEEE 13th International Conference on Communication Technology (ICCT), 347-351, 2011.

[27]F. Haider, C. Wang, B. Ai. Spectral/Energy Efficiency Tradeoff of Cellular Systems with Mobile Femtocell Deployment. IEEE Transactions on Vehicular Technology, 3389-3400, 2016.

[28]M. Pramanik, R. Lau, W. Zhang. Cooperative anonymity authentication in Vehicular Networks. IEEE 13th International Conference on e-Business Engineering (ICEBE), 85-91, 2016.

[29]X. Liu, H. Zhao, X. Liang, et al. Traffic-aware multiple mix zone placement for protecting location privacy. IEEE INFOCOM, 972-980, 2012.

[30]R. Yu, J. Kang, X. Huang, et al. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks. IEEE Transactions on Dependable and Secure Computing, 93-105, 2016.

[31]J. Li, X. Chen, F. Xhafa, et al. Secure Deduplication Storage Systems Supporting Keyword Search. Journal of Computer and System Sciences, 1532-1541, 2015.

[32]J. Li, J. Li, X. Chen, et al. Identity-based Encryption with Outsourced Revocation in Cloud Computing. IEEE Transactions on Computers, 425-437, 2015.

[33]M. Azees, P. Vijayakumar, L. J. Deboarhm. EAAP: Efficient Anonymous Authentication With Conditional Privacy- Preserving Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems, 1-10, 2017.

[34]M. Wang; H. Shan; R. Lu, et al. Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System. IEEE Transactions on Vehicular Technology, 1664-1678, 2015.

[35]K. Rabieh, M. Mahmoud, A. Siraj, et al. Efficient Privacy-Preserving Chatting Scheme with Degree of Interest Verification for Vehicular Social Networks. IEEE Global Communications Conference (GLOBECOM), 1-6, 2015.

[36]X. Duan, X. Wang, Y. Liu, et al. SDN Enabled Dual Cluster Head Selection and Adaptive Clustering in 5G-VANET. IEEE 84th Vehicular Technology Conference (VTC-Fall), 1-5, 2016.

[37]M. Eiza, Q. Ni, Q. Shi. Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks. IEEE Transactions on Vehicular Technology, 7868-7881, 2016.

[38]R. Yu, J. Ding, X. Huang. Optimal Resource Sharing in 5G-Enabled Vehicular Networks: A Matrix Game Approach. IEEE Transactions on Vehicular Technology, 7844-7856, 2016.

[39]F. Wu, M. R. Brust, Y. Chen, et al. The Privacy Exposure Problem in Mobile Location-Based Services. IEEE

Global Communications Conference (GLOBECOM), 1-7, 2016.

[40] X. Gong, X. Chen, K. Xing, et al. Personalized location privacy in mobile networks: A social group utility approach. IEEE Conference on Computer Communications (INFOCOM), 1008-1016, 2015.

[41] K. Rabieh, M. Mahmoud, M. Younis. Privacy Preserving Route Reporting Schemes for Traffic Management Systems. IEEE Transactions on Vehicular Technology, 2703-2713, 2016.

[42] G. Sun, Y. Xie, D. Liao, et al. User-Defined Privacy Location-Sharing System in Mobile Online Social Networks. Journal of Network and Computer Applications, 34-45, 2016.

[43] D. Rivas, J. Barceló-Ordinas, M. Zapata, et al. Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. Journal of Network and Computer Applications, 34(6): 1942-1955, 2011.

[44] F. Wang, Y. Xu, H. Zhang, et al. 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET. IEEE Transactions on Vehicular Technology, 896-911, 2016.

[45] G. Sun, V. Chang, M. Ramachandran, et al. Efficient Location Privacy Algorithm for Internet of Things (IoT) Services and Applications. Journal of Network and Computer Applications, 3-13, 2017.

[46] F. Abbas, H. Oh. A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET. IEEE Access, pp.7770-7784, 2016.

[47] J. Shao, X. Lin, R. Lu, et al. Threshold Anonymous Authentication Protocol for VANETs. IEEE Transactions on Vehicular Technology, 1711-1720, 2016.

[48] G. Sun, D. Liao, H. Li, et al. L2P2: A Location-Label based Approach for Privacy Preserving in LBS. Future Generation Computer Systems, 375-384, 2017.

[49] P. George, H. Fu, B. Abdelnasser. Evaluating Location Privacy in Vehicular Communications and Applications. TEEE Transactions on Intelligent Transportation Systems, 2658-2667, 2016.

[50] GMSF, available on https://www.gmsf.nl/, accessed on Mar 17, 2017.

[51] S. Schwarz, T. Philosof, M. Rupp. Signal Processing Challenges in Cellular-Assisted Vehicular Communications: Efforts and developments within 3GPP LTE and beyond IEEE Signal Processing Magazine, 47-59, 2017.