Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 5, No. 3, 2023

A Sensitivity-based Location Privacy Protection Scheme in Vehicular Networks

Han Jiang, Hequn Xian *

College of Computer Science and Technology, Qingdao University, Qingdao, China
* **Corresponding author**: Hequn Xian (Email: xianhq@126.com)

Abstract: In recent times, the issue of vehicle location privacy has received increasing attention. Location-based services (LBSs) require users' location information to be constantly updated to service providers, which causes the location information to be speculated and attacked by malicious entities. The pseudonym schemes offer a viable solution to the aforementioned problem, but existing pseudonym schemes do not provide differentiated protection for users' varying locations, thereby increasing the possibility of location information leakage. To address this concern, we propose a sensitivity-based pseudonym exchange mechanism, which leverages the vehicle's historical track record to extract features and enable customized location privacy protection. Performance evaluation results demonstrate that our approach significantly outperforms existing approaches in achieving location privacy.

Keywords: Location Privacy Protection; Pseudonym; Vehicular Networks; Sensitivity.

1. Introduction

The Internet of Vehicles (IoV) has gained significant attention due to the advancements in intelligent sensors, big data, artificial intelligence, and mechanical manufacturing technology. It plays a vital role in enabling vehicles to understand the surrounding environment and achieve autonomous navigation [1]. As a distributed self-organized network, IoV allows mobile nodes (vehicles) to communicate with other vehicles equipped with On-Board Units (OBUs) through Vehicle-to-Vehicle (V2V) communication, or with Road-Side Units (RSUs) [2-3]. According to the Regulation of the Standardization Development Organization [4], a vehicle's current state should be broadcast at a frequency of 1-10 Hz when it is in motion, in the form of beacons that include information such as vehicle identification, location, speed, and direction. This aids drivers in anticipating potential hazards, preventing accidents, and enhancing driving safety. However, this information is broadcast to everyone, making it vulnerable to collection by attackers using technical means. Attackers can infer sensitive personal information from a vehicle's historical behavior records, such as the driver's occupation, health status, and daily routines. Consequently, privacy protection is crucial in the IoV.

In order to solve the problem of location privacy in the IoV, the pseudonym schemes [5] are widely used, where multiple pseudonyms are utilized to conceal the identity of the vehicles. A pseudonym scheme based on public key infrastructure (PKI) is described in the ETSI102941-v1.1.1 vehicle security standard [6]. Under this scheme, when the vehicle is registered, the vehicle receives pseudonyms and private key from the Trusted Authority (TA), allowing for the pseudonym to be changed while the vehicle is in operation, and a new set of pseudonyms will be requested once the current set has been exhausted. This approach allows for various identifiers to fulfill network requirements for beacon broadcasting. However, adversaries can still track a vehicle if it maintains a single pseudonym for an extended period or if the pseudonyms are linkable, making unlinkability a critical requirement for pseudonyms in location privacy protection. Additionally, pseudonyms must be changed after being used for a period of time, but changing them at an inappropriate time or location may still enable adversaries to track the vehicle. As a result, the pseudonym change mechanism must be thoughtfully designed to prevent pseudonyms association attacks [7]. The time and location of pseudonym changes directly impact the pseudonym scheme's anonymity performance, making the safe, efficient, and effective use of pseudonyms to protect vehicle track privacy a significant challenge.

The existing research usually provides consistent protection, meaning that identical privacy standards are applied to all users in the Internet of Vehicles. For instance, the literature [8] pays their attention to the location where pseudonyms are changed. If a vehicle alters its pseudonym in a sparse location, the adversary can easily detect this change. To overcome this issue, scholars have proposed changing pseudonyms in mix-zones [9-10], social hotspots, and other areas, such as parking lots, shopping malls, and intersections. The fundamental concept behind this approach is to change pseudonyms in designated pseudonym change areas when the age of the pseudonym reaches a certain threshold, enabling multiple vehicles to simultaneously alter their pseudonyms to confuse attackers. It is evident that different locations, and times require varying degrees of privacy protection need for individual users, requiring different pseudonym change strategies [11]. We believe that the privacy needs of users at frequently visited locations, such as their workplace, should be greater than those in other regions.

This paper's primary contributions are presented as follows:

1) We define a measurement called sensitivity to quantify the location privacy requirements of each vehicle in each location. Based on this, we defined our pseudonym age growth model, so that the age growth rate of the vehicle's pseudonyms is different with different sensitivity.
2) A sensitivity-based pseudonym exchange mechanism is proposed for protecting the location privacy of vehicles in vehicular networks. We construct an extended pseudonym-exchanging region called the

"group-region", which enables vehicles to exchange their pseudonyms using a group identity. The usage of group identity protects the procedure of pseudonym exchange effectively.

The subsequent sections of the paper are structured as follows: Sect.2 provides an overview of the related work. Sect.3 introduces the network model and threat model. Sect.4 describes the privacy protection mechanism and sensitivity calculation method. In Sect.5, the performance analysis is presented. Finally, we conclude our work in Sect.6.

2. Related Work

With the growing concern over privacy disclosure related to the location of IoV, several methods have been developed to address the problem, including mixed zone [9-10], silence period [12]and group signature [13]. The fundamental concept underlying these approaches is that when a vehicle transmits information, it employs a pseudonym instead of its actual name. Consequently, many studies concentrate on the strategy of changing pseudonyms, including the time and location of such changes.

Li et al. proposed the Swing&Swap scheme [12], which aims to prevent opponents from predicting the position of vehicles through sudden changes in location. The scheme updates vehicle pseudonyms when the speed drastically drops or accelerates, while maintaining the same pseudonym for nearly constant speeds. Buttyan et al. [14] proposed Slow, a pseudonym replacement method that considers driving speed as a factor affecting pseudonym replacement. When the speed falls below a specific threshold, the vehicle stops sending messages and performs pseudonym replacement. Chen et al.[15] identified pseudonym age as a critical factor in pseudonym changing. Specifically, when a vehicle's pseudonym age exceeds a specified threshold ff, it attempts to change its pseudonym.

The process of changing pseudonyms should occur in a proper occasion as vehicles can still be tracked when they change their pseudonyms in areas with few vehicles. To address this limitation, a hybrid zone scheme has been proposed as a solution. The fundamental principle of hybrid zones involves the use of RSU public key encryption when all vehicles within the hybrid zone exchange information. Consequently, when the hybrid zone is of sufficient size, attackers are unable to predict the location of vehicles. The concept of hybrid zones was first introduced by Beresford et al. [16], and further improved in [9]. Yu et al. [13] introduced an approach named MixGroup that integrates social gathering spots with other events where a vehicle can encounter a considerable number of vehicles. In MixGroup, vehicles can engage with each other to decide whether to participate in the pseudonym change procedure. Li et al. [17] proposed a method called TLAS, which uses the area in front of the red light as a mixing zone, uses the cycle of the street light to predict traffic flow, and adaptively adjusts the size of the mixing zone. This scheme can achieve better anonymity at lower vehicle speeds.

Inspired by these efforts, we designed a pseudonym exchange scheme based on vehicle history records using a group signature technology and using pseudonym age as a basic factor that affects pseudonyms exchange.

3. System Model

3.1. Network Model

The model of our network model is illustrated in Figure. 1. There exist four types of entities, including vehicles, RSUs, TA, and LBS provider.

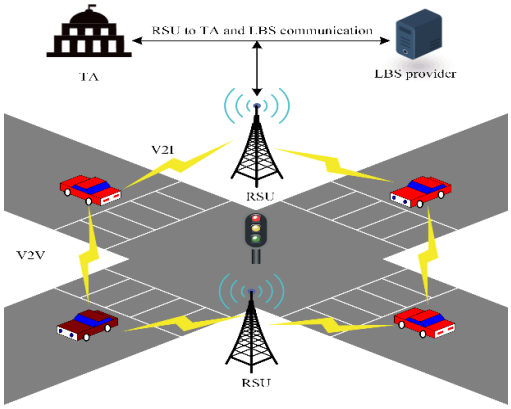


Figure 1. Architecture of vehicular networks

1) TA: TA is a reliable entity with robust computing and processing capabilities in the context of the IoV. Its primary responsibility is to generate the public key, private key, and certificate for secure communication before the vehicle's operation. At the same time, TA will generate a set of pseudonyms along with their corresponding public and private keys, certificates according to the registration information, and distribute them to vehicles applying for pseudonyms. Additionally, TA maintains a tracking table, which enables the identification of the true identity of each vehicle, thereby facilitating investigations into any illegal activities.
2) RSU: RSUs are fixed infrastructure, vehicles communicate with LBS through RSUs for location updates and communicate with TA to access certificates for verification and authentication.
3) Vehicle: Each vehicle is equipped with OBUs for wireless communication, global positioning system for location service, and sensitivity management module. After registering with the TA, vehicles will receive sufficient pseudonyms and corresponding information to be used for broadcasting safety messages. The sensitivity management module is tasked with the computation and retention of sensitivity data

3.2. Threat Model

To ensure periodic broadcast of safety-related messages, the OBU's radio cannot be switched off while the vehicle is on the road. However, this makes the vehicle vulnerable to eavesdroppers who can track its location information by intercepting these messages. Therefore, safeguarding location privacy is crucial to counter potential threats. The adversary that we mainly consider is global passive adversary (GPA), which can eavesdrop all safety messages in the network, locate and track all vehicles through the safety messages which they broadcast. Then analyze the obtained user information to acquire the user's personal sensitive information.

4. Pseudonym Exchanging Strategy

In this section, we will introduce the sensitivity defined in this paper, along with the pseudonym age growth model and pseudonym exchanging strategy based on the sensitivity. Furthermore, a list of notations used in this article is given in Table 1.

Table 1. The meaning of the symbols in the scheme

Symbol	Description
v_i	The i^{th} vehicle in the scheme
R_l	The l^{th} region in the scheme
RSU_k	The k^{th} RSU in the scheme
TS	Timestamp
$Location_i$	Position information of v_i
$Z_i(t)$	The pseudonym age of v_i at time t
S_i^l	The sensitivity of v_i in R_l
G_l	The l^{th} group in the scheme.
GM_l	The group leader of the l^{th} group
ID_i	The true identity of v_i
$PID_{i,k}$	The k^{th} pseudonym of v_i
$PK_{GID_l}, Cert_{GID_l}$	Public key and corresponding certificate of GM_l
$SK_{G_{l,i}}, Cert_{G_{l,i}}$	Group private key of group ID and corresponding certificate for v_i
$PK_i, SK_i, Cert_i$	Public and private key pair of v_i, and corresponding certificate
$PK_{PID_{i,k}}, SK_{PID_{i,k}}, Cert_{PID_{i,k}}$	Public and private key pair of $PID_{i,k}$ and corresponding certificate
$E_k(m)$	Message m is encrypted with key k
$v_i \rightarrow v_j$	v_i sends a message to v_j
τ	Threshold of pseudonym age
$PK_i^{'}, SK_i^{'}, Cert_i^{'}$	Public and private key pair of v_i's temporary identity, and the corresponding certificate
$Sign_k(m)$	Digital signature on message m with k

4.1. Growth Model of Pseudonym Age

Upon analyzing the track dataset of the vehicle, we discovered that it strictly adheres to the owner's daily activities. As humans exhibit certain social behaviors, such as having a job, maintaining a home, and hanging out with a circle of friends, they frequently visit specific areas, including workplaces and accommodations. If the location privacy of the vehicle in these sensitive areas cannot be protected safely, the personal privacy of the vehicle owner will be endangered. As such, location privacy protection is more critical in these areas than in ordinary ones, and the pseudonym exchanging frequency should be increased. Therefore, we have developed a pseudonym exchanging strategy based on having a job, maintaining a home, and hanging out with a circle of friends.

Most of the existing studies believe that the growth rate of pseudonym age of each vehicle is the same, but it is obvious that different vehicles have different location privacy requirements. Thus, each vehicle's pseudonym growth rate should vary from that of others, and a specific vehicle's growth rate in a given area should also differ from that of other areas. The control center uses historical behavior records of each user to divide their personal sensitive areas and propose a sensitivity metric that quantifies different location privacy requirements

In this paper, we consider a set of vehicles, which are represented as $N_v = \{v_1, v_2 \cdots v_n\}$ and a set of regions, which are represented as $R_l = \{R_1, R_2 \cdots R_n\}$. Each vehicle uses its pseudonym that has been used for a period of time when broadcasting its safety message. When the vehicle v_i is in R_l, assume that the basic speed of the vehicle's pseudonym age growth is k. Then, it's pseudonym age can be calculated as formula (1). Where x, y, a, b is optional constant determined by user.

$$Z_i(t)=Z_i(t\text{-}1)+\begin{cases} k & S_i^l <= x \\ ak & x < S_i^l <= y \\ bk & S_i^l > y \end{cases} \quad (1)$$

4.2. Sensitivity Calculation Method

Based on an analysis of the user's historical track record, it is evident that users visit various locations with three discernible characteristics, namely access duration, access frequency, and access regularity. Therefore this paper uses these three features to measure the sensitivity of a certain region to users. The following are detailed descriptions of the three features:

1) Access duration: Analyze the user's recent behavior track record, and calculate the average access time of the user to each location. Generally, the location with longer average access time also contains more personal privacy information. Define the access duration from v_i to location R_j as $T_{i,j}$. It can be calculated as formula (2). Where t_i is the start time of track recording, t_j is the end time of track recording. F(t) = 0 indicates that the user is not in the area, and F(t) = 1 indicates that the user is in the area.

$$T_{i,j} = \frac{\int_{t_i}^{t_j} F(t)dt}{t_j - t_i} \quad (2)$$

2) Access frequency: Access frequency refers to the ratio of the number of times users visit a certain location in a certain period of time to the total number of times users travel. If the user visits a location frequently, it can be judged that the location is more important to the user and contains more privacy information. The moving track of user i in the (t_1, t_2) time period is $L_i = (l_1, l_2, \cdots l_j, \cdots l_n)$, 1<= j <=n, l_j indicates a location accessed by the user in (t_1, t_2) time period. Define the access frequency from v_i to location R_j as $P_{i,j}$. It can be calculated as formula (3). Where $N(l_j)$ indicates the number of visits user i to position l_j, $N(L)$ indicates the total number of visits by user i in a period of time.

$$P_{i,j} = \frac{N(l_j)}{\sum_{l \in L_i} N(L)} \quad (3)$$

3) Access regularity: In order to enhance the privacy protection of car owners, it is crucial to consider the regularity of their visits to specific locations such as their homes and workplaces. Such locations are frequently visited for long durations and exhibit predictable patterns of access. These regular factors of access can help determine whether a user's access to a location is routine, thus reducing errors in location privacy demands caused by temporary and sudden events.

To calculate the regularity of users' access to a location, first calculate the average access period of users and locations, which can be calculated as:

$$AVG_{i,j} = \frac{\int_{t_1}^{t_2} o(i)dt}{n_{i,j}} \quad (4)$$

Where t_1 is the start time of track recording, t_2 is the end time of track recording. $n_{i,j}$ indicates the number of separations between user and location. O(i) indicates whether user i is in R_j. O(i) = 0 indicates that the user is not at the location, and O(i) = 1 indicates that the user is at the location. Using Gaussian similarity function to measure $AVG_{i,j}$ normalization, get the relationship strength between user i and location j, as shown in formula (5), σ scaling parameter representing access period.

$$C_{i,j} = e^{\frac{(AVG_{i,j})^2}{-2\sigma}} \quad (5)$$

By calculating the variance of the access period, the irregular metric $I_{i,j}$ indicates the regularity of access cycle fluctuation to determine whether the user's access to the location meets the regularity, which can be calculated as formula (6), $x_{i,j}$ indicates the length of the access cycle.

$$I_{i,j} = \frac{\sum_l (C_{i,j} - x_{i,j})^2}{n_{i,j}} \quad (6)$$

Based on the factors affecting sensitivity described above, this paper proposes a multi-factor model based on multiple linear regression, which organically combines the above factors to form the user's sensitivity evaluation function, sensitivity evaluation function can be calculated as formula (7). Where α, β, γ means the weight value of each feature element, and the value is between [0,1]. The sensitivity obtained is different with the weight of each element.

$$s_i^j = \alpha P_{i,j} + \beta T_{i,j} + \gamma I_{i.j} \quad (7)$$

4.3. Pseudonym Exchanging Protocol

Our mechanism mainly consists of several operations: system initialization, group joining, pseudonym exchanging, pseudonym activating, and group leaving. Figure.2 shows the state diagram of vehicles in our mechanism to explain how the vehicle transits from one state to another.

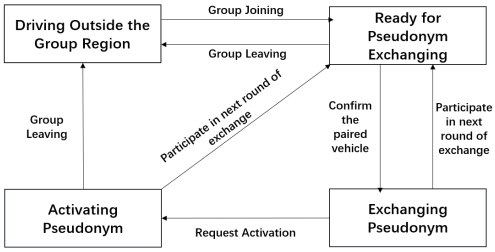


Figure 2. State diagram of vehicles

4.3.1. System initialization

Prior to driving, vehicle vi sends its ID_i and other identity information to TA for registration. Based on the vehicle's provided information, the TA generates a set of public and private keys and certificates denoted by $\{ID_i, Gk_i, Sk_i, Cert_i\}$. Additionally, v_i requests a certain number of pseudonyms $PID_{i,k}(k = 1,2,3\cdots n)$ from the TA, along with the corresponding set of public/private key pairs and certificates $\{PK_{PID_{i,k}}, SK_{PID_{i,k}}, Cert_{PID_{i,k}}\}$. Each vehicle is equipped with a sensitivity calculation module, which utilizes the vehicle's historical track information to calculate the sensitivity of each area and store the data. Moreover, group leader vehicles receive public and private key pairs and certificates of communication.

Protocol 1 Group joining protocol

1: GM_l broadcast group invitation to the neighboring v_i

$invition = R_l \,||\, join \,||\, GM_l \,||\, TS \,||\, Cert_l$

2: if (v_i verified the legitimate identity of GM_l) then

$v_i \rightarrow GM_l$:

$E_{GM_l}(join \,||\, PID_{i,k} \,||\, PK_{PID_{i,k}} \,||\, TS \,||\, Cert_{PID_{i,k}} \,||\, Location_{v_i})$

end if

3: if (GM_l verified the legitimate identity of v_i)&& (v_i is in R_l) then

$GM_l \rightarrow v_i : E_{PK_{PID_{i,k}}}(GID_l \,||\, TS \,||\, PK_i^{'} \,||\, SK_i^{'} \,||\, Cert_i^{'} \,||\, SK_{G_{l,i}} \,||\, Cert_{G_{l,i}} \,||\, Cert_l)$

else GM_l do not response

end if

4: if (v_i received reply within $T_{\max}$) then v_i broadcast information

$broadcast = GID_l \,||\, TS \,||\, Location_{v_i} \,||\, Cert_{G_{l,i}}$

else v_i do not response

end if

4.3.2. Group Joining

During operation, all vehicles are required to broadcast safety beacons periodically to the surrounding area, for instance, every two seconds. The safety beacon should contain the vehicle's pseudonym $PID_{i,k}$, current location $location_i$, TS and other status information. TS can ensure the real time of the information and avoid replay attacks. When vi enter region R_l, it receives an invitation message from GM_l including group identity region information, and other

relevant details. GM_l is selected by nearby RSU. It is responsible for verifying the legitimacy of the identity of vehicles applying to become group member and distributing relevant information required for vehicles to become group member. Upon receiving the invitation message, vi verifies the message from GM_l and sends a request message that includes its identity information and location as a response. If GM_l verifies the response message from v_i, it provides v_i with parameters of GID_l 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_l to prevent continuous tracking by attackers. 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 entire process is described in Protocol 1.

Protocol 2 Pseudonym exchanging protocol

1: GM_l broadcast pseudonym exchanging invitation to v_i which is in the group:
$invition = R_l \| exchange \| Cert_l \| TS \| GID_l$

2: if (vi verified the inviation from GM_l)&&(pseudonym age ≥ τ) then
$v_i \rightarrow GM_l$:
$E_{Pk_{GID_l}}(agree \| PID_{i,k} \| s_i^l \| TS \| Cert_{PID_{i,k}} \| Location_{v_i} \| speed_i)$
else v_i do not response
end if

3: if (GM_l verified the legitimate identity of v_i) then
$GM_l \rightarrow v_i : E_{PK_{PID_{i,k}}}(GID_l \| Cert_{GID_l} \| TS \| Allocation)$
else GM_l do not response
end if

4: if (v_i exchange pseudonym with of v_j) then
$v_i \rightarrow v_j : PK_j^{'} \| E_{PK_j^{'}}(data\_1 \| Sig\_1 \| TS \| Cert_{G_{l,i}} \| Sign_{SK_{PID_{i,k}}}(data\_1 \| Sig\_1)$
$data\_1 = PID_{i,k} \| Cert_{PID_{i,k}}, Sig\_1 = Sign_{SK_{PID_{i,k}}}(data\_1)$
v_j verify and store data from v_i
$v_j \rightarrow v_i : PK_i^{'} \| E_{PK_i^{'}}(data\_2 \| Sig\_2 \| TS \| Cert_{G_{l,j}} \| Sign_{SK_{PID_{j,k}}}(data\_2 \| Sig\_2)$
$data\_2 = PID_{j,k} \| Cert_{PID_{j,k}}, Sig\_2 = Sign_{SK_{PID_{j,k}}}(data\_2)$
end if

4.3.3. Pseudonym Exchanging

After becoming a member of group GM_l, v_i will have the opportunity to participate in the pseudonym exchange procedure. GM_l will broadcast an invitation for pseudonym exchange to the vehicles within the group. If v_i needs to conduct a pseudonym exchanging, it will report to GM_l reply message. GM_l will then confirm the participating vehicles for this round of pseudonym exchange, allocate them into pairs based on similar sensitivity, speed and driving direction. Then notify each vehicle of the distribution results separately. The entire process is described in Protocol 2.

4.3.4. Pseudonym Activating

After the pseudonym exchange between v_i and v_j is completed, v_i 's pseudonym is changed to $PID_{j,k}$,but it cannot be used immediately. The vehicle should firstly activate the pseudonyms by TA through the RSUs. To activate the new pseudonym, vi must send an activation request encrypted with the public key of the TA via the RSUs. The request includes the exchanged pseudonyms, personal data, and corresponding digital signature. TA first verifies the legal identity of v_i, then generates and distributes a new public and private key pair and certificates for the new pseudonym. However, it is worth noting that to prevent continuous tracking by attackers and make it more difficult for them to link the old and new pseudonyms, v_i uses the group identity to communicate and broadcast messages before leaving the group. After leaving the group, v_i switches to the new pseudonym.

4.3.5. Group Leaving

Once a vehicle moves out of the group-region, it broadcasts safety messages using newly changed pseudonyms. If GM_l fails to receive any safety messages from v_i with the certificate $Cert_{G_{l,i}}$ within $T_{\max}$ time. GM_l believes that v_i has left the group, and consequently removes vi 's entry from the group member list. When leaving group, v_i independently decides whether to search for a new group in the next group-region or continue using the pseudonyms for a while.

4.4. Conditional Tracking

When a vehicle is part of a group G_l, its periodic broadcast message contains safety-related data and a group certificate $Cert_{G_{l,i}}$. Although only group members of G_l can verify the validity of the safety message, the TA can associate all messages with their certificates to the true identities of the vehicles by contrast the tracking list. When a vehicle is not part of any group and uses its own pseudonyms for communication, its safety message also includes a certificate, which can be identified by the TA. In other words, the true identity of each vehicle is entirely revealed to the trustworthy TA, but conditionally private to the group leader, and unknown to other ordinary vehicles.

5. Experimental Analysis

In this section, we evaluate the performance of this through some existing privacy metrics. Experimental results show that our mechanism is superior to existing methods in achieving location privacy

5.1. Performance Metrics

Entropy represents the degree of uncertainty in the vehicle's identity. In this paper, the entropy of the average anonymous set of vehicles is used to measure the location privacy of vehicles. Consider a group of n vehicles, which are

represented as $G_j = \{v_1, v_2 \cdots v_n\}$. Assume that pi represents the probability that the vehicle v_i will be tracked by an attacker after exchanging a pseudonym. The entropy of the anonymous set G_j can be calculated as:

$$H(G_j) = -\sum_{i=1}^{|G_j|} p_i \times \log_2 {}^{p_i} \tag{8}$$

The probabilistic attack model described in reference [18] assumes that two nodes are involved. Through the exchange of pseudonyms between these nodes, an attacker can calculate the likelihood of the target vehicle being present. This probability is denoted as $\alpha \in [0.5, 1]$. The probability of an attacker successfully tracking a target vehicle can be calculated as:

$$p_i = \frac{\alpha}{\alpha + (|G_j| - 1) \times (1 - \alpha)} \tag{9}$$

Assuming that n represents the number of vehicles in the entire network, after the vehicles exchange the nth pseudonym, the entropy of the average anonymous set of the entire network can be calculated as:

$$H_{ave} = \sum_{i=1}^{n} \sum_{j=1}^{|G|} H(G_j) \tag{10}$$

5.2. Simulation Parameters

The simulation experiment was conducted using the real map of Qingdao City, and was implemented utilizing the OMNeT++ and SUMO simulation platforms. Detailed simulation parameters are shown in Table 2.

Table 2. Simulation Parameters

Parameter	Value
Simulation duration	0~1800 s
Map Size	4*4 km²
Transmission bandwidth	10 MHZ
Vehicle speed	[0,60] km/h
Communication range for OBU and RSU	500 m
Number of RSU	15
Car-following model	Krauss Model
Beacon message interval	1 s

5.3. Simulation Results

We employ the average anonymous entropy to evaluate and compare the proposed scheme with DMLP [19] and AS [14]. DMLP allows vehicles to dynamically generate mixed regions and exchange pseudonyms in the mixed regions. In AS, the vehicle's pseudonym age is allowed to change only when it reaches the specified threshold. Figure.3 shows the comparison between the proposed scheme and other schemes under different vehicle densities. In any given scenario, the performance of this algorithm is superior to the other two schemes. This is due to the fact that this scheme maximizes the protection of location privacy by utilizing the opportunity of pseudonyms exchange as much as possible, even in situations where there are few vehicles present.

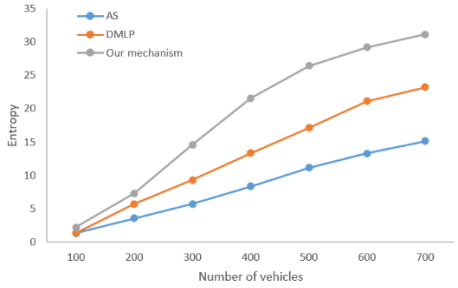
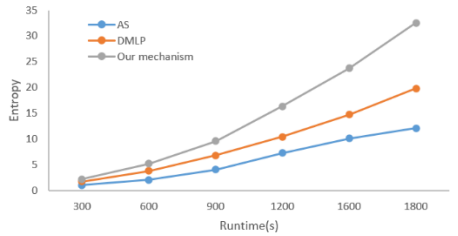
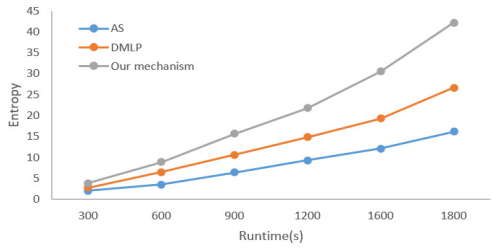


Figure 3. Average anonymous entropy corresponding to different vehicle density

Figure.4 is a comparison of the performance of three schemes under different attack capabilities. The ability of attackers is divided into two types: weak attackers $\alpha = 0.5$ and strong attackers $\alpha = 0.9$. It can be inferred that the proposed scheme presents significant advantages, irrespective of the attacker's capabilities. Because in the AS scheme, the growth rate of the pseudonym age is fixed and only after the pseudonym age reaches a fixed threshold can be replaced, compared to the scheme proposed in this article, the number of pseudonym replacement times is greatly reduced. And in the DMLP scheme, the mixed area size is determined by the vehicle's location and current traffic statistics, which limits the number of simultaneous vehicles in the same location. However, our mechanism increases the number of vehicles exchanging pseudonyms and the number of vehicles participating in the exchange of pseudonyms. Make our average anonymous entropy higher than other schemes.



(a) α=0.8



(b) α=0.5

Figure 4. Average anonymous entropy with different attack capabilities

Figure.5 shows the comparison of tracking rates between different schemes under different vehicle densities. It can be seen that the proposed scheme outperforms other schemes, as the use of group identities masks the process of kana exchange, resulting in a lower tracking rate for vehicles. Overall, the proposed scheme in this article outperforms other schemes in terms of privacy protection.

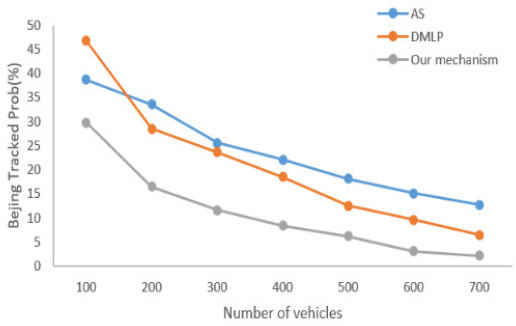


Figure 5. Vehicle tracking rate under different vehicle densities

6. Conclusion

In this paper, we propose a pseudonym management mechanism to protect location privacy in vehicular networks. Our mechanism considers the historical trajectory of the vehicle and proposes a sensitivity to quantify the privacy requirements of the vehicle for each location. And the use of group signature technology reduces the link between pseudonyms and real identities. The results of the analysis demonstrate that in comparison with traditional approaches, our approach not only takes into account the heterogeneity between vehicles, but also provides higher location privacy. In future work, we intend to continue the perfection of the proposed mechanism.

References

[1] C. Chen, Z. Liu, S. Wan, J. Luan, and Q. Pei, “Traffic flow prediction based on deep learning in internet of vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 6, pp. 3776–3789, Jun. 2020.

[2] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, “Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment,” IEEE Trans. Inf. Forensics Secur ., vol. 15,pp. 1654–1667, 2020.

[3] C. Chen, Y . Zhang, Z. Wang, S. Wan, and Q. Pei, “Distributed computation offloading method based on deep reinforcement learning in ICV,”Appl. Soft Comput., vol. 103, May 2021, Art. no. 107108.

[4] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” IEEE Commun. Surveys Tuts., vol. 17,no. 1, pp. 228–255, Mar. 2014.

[5] H. Artail and N. Abbani, “A pseudonym management system to achieve anonymity in vehicular ad hoc networks,” IEEE Trans. Dependable Secure Comput., vol. 13, no. 1, pp. 106–119, Jan./Feb. 2016.

[6] SAE J2735 V1.1.1-Dedicated Short Range Communications (DSRC) Message Set Dictionary. SAE Standard, 200.

[7] X. Li, H. Zhang, Y. Ren, S. Ma, B. Luo, J. Weng, J. Ma, X. Huang, “PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs[J],” IEEE Internet of Things Journal, 2020, 7(12): 11789–11802.

[8] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in V ANETs,” IEEE Trans. V eh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[9] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux,“Mix-zones for location privacy in vehicular networks,” in Proc. ACM Workshop Wireless Netw. Intell. Transp. Syst., 2007, pp. 1–7.

[10] H. Zhong, J. Ni, J. Cui, J. Zhang and L. Liu, "Personalized Location Privacy Protection Based on Vehicle Movement Regularity in Vehicular Networks," in IEEE Systems Journal, vol. 16, no. 1, pp. 755-766, March 2022.

[11] Z. Liu, Z. Liu, L. Zhang, and X. Lin, “MARP: A distributed MAC layer attack resistant pseudonym scheme for V ANET,” IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 869–882, Jul./Aug. 2020.

[12] L. Buttyán, T. Holczer, A. Weimerskirch and W. Whyte, "SLOW: A Practical pseudonym changing scheme for location privacy in VANETs," 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 2009, pp. 1-8.

[13] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, “Mixgroup:Accumulative pseudonym exchanging for location privacy enhancementin vehicular social networks,” IEEE Trans. Dependable Secure Comput.,vol. 13, no. 1, pp. 93–105, Jan./Feb. 2016.

[14] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real," 2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring, Dublin, Ireland, 2007, pp. 2521-2525.

[15] Y.-S. Chen, T.-T. Lo, C.-H. Lee, and A.-C. Pang, “Efficient pseudonym changing schemes for location privacy protection in VANETs,” in Proc. Int. Conf. Connected Veh. Expo., 2013, pp. 937–938.

[16] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,”IEEE Perv. Comput., vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003.

[17] Y. Li, Y. Yin, X. Chen, J. Wan, G. Jia and K. Sha, "A Secure Dynamic Mix Zone Pseudonym Changing Scheme Based on Traffic Context Prediction," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 9492-9505, July 2022.

[18] D. Eckhoff, C. Sommer, T. Gansen, R. German and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," 2010 IEEE Vehicular Networking Conference, Jersey City, NJ, USA, 2010, pp. 174-181.

[19] B. Ying, D. Makrakis and H. T. Mouftah, "Dynamic Mix-Zone for Location Privacy in Vehicular Networks," in IEEE Communications Letters, vol. 17, no. 8, pp. 1524-1527, August 2013.