IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Survey of Location Privacy Preservation in Social Internet of Vehicles

XIAOFAN JIA^1, LING XING^1, JIANPING GAO^2, HONGHAI WU^1.

^{1}School of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China
^{2}School of Vehicle and Traffic Engineering, Henan University of Science and Technology, Luoyang 471023, China

Corresponding author: Jianping Gao (e-mail: gaojpcar@163.com).

This research is supported by National Natural Science Foundation of China (Grant No. 62071170, Grant No. 61771185, Grant No. 61772175, Grant No. 62072158).

ABSTRACT Social Internet of Vehicles (SIoV) is an emerging complex network where the features of Social Networks are applied to the SIoV system. User location data forms the basis for the implementation of SIoV functions. However, this type of data contains a large amount of user personal information, which may cause privacy leakage if it is stolen. Protecting the privacy of the user location can eliminate concerns about the leakage of user personal privacy data, increase users' viscosity, and help to contribute to the improvement of the SIoV system. This paper systematically analyzes the location privacy protection technology utilized in recent years in the field of SIoV, proposes three types of user data location privacy protection technology, and evaluates the performance of these technologies. We further present some potential future research directions for location privacy protection technology through the analysis and summary of existing work.

INDEX TERMS Social Internet of Vehicles; location privacy preservation; big data; Internet of Vehicles; Social Network

I. INTRODUCTION

SOCIAL Network (SN) is the most promising virtual product in the Internet era, as it allows users to share data, exchange information [1] and liaise [2] with other users anytime and anywhere through mobile devices. As an important branch of the Internet of Things (IoT) [3], the Internet of Vehicles (IoV) provides for the safety and convenience of user travel, and has consequently become an important component of intelligent transportation systems [4]. This is an emerging form of network that combines the two network paradigm types of IoV and SN and is referred to as SIoV; this network turns smart vehicles into the next carrier of mobile SNs [5], while also enabling owners to abandon mobile phone social functions after they get into the cars. However, due to the popularization of SIoV systems, user location privacy issues may arise. Since these functions are implemented at the cost of user location data, they can provide users with more convenient services, but may also reveal user private information. Therefore, the question about how to avoid user location data being leaked has become a new research direction that has attracted widespread attention among researchers.

The purpose of protecting user location privacy in the SIoV context is to reduce the risk of user private information being disclosed. Solving to this problem of great significance in many fields, as is primarily reflected in the following aspects:

(1) Protecting user identity privacy [6]. There is a specific connection between the location and identity information generated by the same users, and attackers can use their location information to speculate about the user identity information. To a certain extent, protecting user location privacy can reduce the probability of user identity information being disclosed.

(2) Increasing users' viscosity. Protecting user location privacy improves the performance of SIoV system, reduces users' concerns about its security, attracts more users to use SIoV functions, increases users' viscosity, and promotes innovation and development in the automobile industry.

(3) Smart cities. SIoV system can guarantee the safety and convenience of user travel, reduce property damage and casualties caused by car accidents, and contribute beneficially to the building of smart transportation systems and smart cities [7].

(4) Personalized service recommendations. The system

can recommend some more reliable personalized services to users by analyzing user interests [8] and location [9]. Once the problem of location privacy disclosure is solved, users will be able to safely use the SIoV function to generate more information; moreover, the system will be able to make full use of this information to provide users with more personalized service content [10].

While protecting user location privacy is of great significance to the application of SIoVs, it is also associated with certain disadvantages. The realization of SIoVs functionality is based on user location, while the location privacy protection research is based on fuzzy positioning. On the one hand, in order to avoid their location being guessed by attackers, users need to protect their location privacy; on the other hand, users who want to enjoy better location-based services (LBSs) must provide their accurate location information to service providers and other physical users. There is thus a contradiction between the degree of location privacy protection and user service demands. However, most users are willing to submit their information provided that the security of their private information is guaranteed.

SIoV will be a core part of intelligent transportation in the future. As consumers of services, users should pay their private information to service providers or other users if they want to get better service experience. This kind of "payment" behavior has attracted wide attention, because it brings privacy risks to users themselves. Therefore, many researchers have proposed varieties of algorithms to protect the user location privacy. However, the existing SIoV is developing towards the direction of cross-platform integration, especially the rapid development about 5G technology in recent years, the information types generated by users become more and more diversified and complicated, which brings several challenges to the privacy protection algorithms in the following aspects:

(1) Combining with non-location data. In the era of big data, attackers can obtain other data types related to user location data from various channels. For example, attackers can make a match between the user location data and non-location data by using the personality or behavior pattern. In order to protect the user location privacy information, it is necessary to study the mapping relationship between the user location data and non-location data, and make the mapped personality vector as fuzzy as possible under the condition that the service availability is available.

Researches into SIoV is still in its infancy, the introduction of new, deeply integrated applications can strengthen customers' viscosity and provide convenience for users in daily life. As the same time, it may also create new challenges for user location privacy protection. In the era of big data, attackers can indirectly find some of the user privacy information by analyzing user preferences. After matching these data with the user location data, user personality vectors can be successfully mapped. In order to better protect user personal privacy, it is necessary to combine this nonlocation-related data with user location data, and subsequently analyze the mapping relationship between them in order to protect user privacy data to a greater extent [11].

(2) Mining and analyzing user information in the SIoV context. The integration of IoV and SN expands the potential application scenarios while also making user data types and relationships between users more complex and diversified. Therefore, privacy protection and trust mechanism research focused on how to efficiently, safely and reliably extract user information sets. Through machine learning and other methods, the public information set in SIoV can be mined from the perspective of different hierarchical structures, so as to solve the privacy problems of users in SIoV from a multilevel perspective.

In terms of the network topology structure of SIoV users, each node represents a user. Because the vehicles are moving at high speed most of the time, the network topology of SIoV users is constantly changing. Therefore, it is necessary to model and analyze the user network topology structure in the SIoV, then find effective algorithms to analyze the user network topology information set, this will lay a foundation for subsequent research into privacy protection mechanisms.

(3) Mechanisms for measuring degrees of privacy protection. Since these methods cannot be measured by a uniform standard, it is impossible to effectively compare and analyze existing location privacy protection methods.

If there a detailed and unitive standard was developed that would allow these methods to be compared and analyzed accurately, users could judge the merits and demerits of these methods more intuitively, and choose appropriate methods that suited their own needs. Moreover, researchers could assess the advantages and disadvantages of these methods more intuitively and clearly, which would facilitate their improvement. Therefore, the research methods used to evaluate location privacy protection from a privacy protection measurement mechanism perspective remains a challenging issue.

(4) Processing of SIoV data. The SIoV social environment is more complex than that of the general SN in terms of user attribute information, connection and application environment. SIoV system can generate large amount of data and different types of data. The question about how to unify the data generated by users remains a research issue that should be considered in the future.

For data transmission, data integrity needs to be guaranteed as far as possible to ensure data security. Especially in 5G era, these characteristics that faster data transmission speed and shorter delay tolerance put forward higher requirements for the location privacy protection technology in SIoV. In terms of data management, another problem worth studying is that of how to manage a large amount of data, so as to maximize its utilization and avoid theft by attackers. Therefore, in response to the user data information processing problem in 5G era, it is crucial to build a security model that can unify, transmit and manage data.

The goal of this paper is to provide a comprehensive review of location privacy preservation technology research, as well as outline guidance for future research directions in SIoV. The contributions of our work can be summarized as follows:

(1) We describe in detail the positive significance of location privacy preservation in various fields, and further summarize the challenges and possible solutions associated with user location privacy protection.

(2) The location privacy problem has various models and preservation frameworks, which we divide into three models according to the different types of user data.

(3) We summarize the preservation methods utilized for different data types and analyze the complexity between protecting algorithms.

(4) The research status of three location privacy preservation algorithms are analyzed in detail, after which their privacy preservation performance is compared and analyzed.

(5) Location privacy preservation remains an active research area, and there are many issues still to be solved. Accordingly, we further discuss the future research directions of location privacy preservation in SIoV.

The remainder of this paper is organized as follows. In Section II, we introduce the model and framework of location privacy preservation in the SIoV context. In Section III, we summarize the basic location privacy protection techniques for SIoV. We review the state-of-the-art methods and compare the performance of different location preservation technologies in Section IV. Finally, we discuss the future directions in Section V and conclude this paper in Section VI.

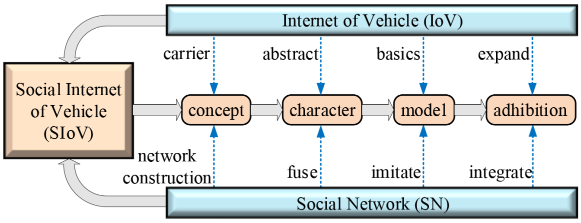

Fig. 1 Research framework of SIoV

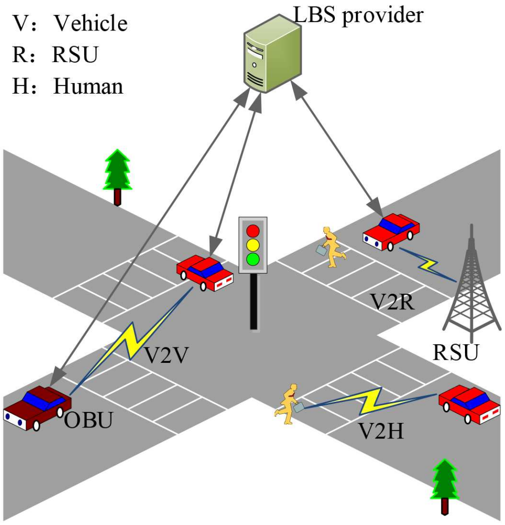

Fig. 2 SIoV model

II. THEORETICAL CONCEPT OF LOCATION PRIVACY PROTECTION TECHNOLOGY FOR SIOV

A. PROBLEM DEFINITION

SIoV is applied to the IoV system by referring to the SN model. This approach can not only improve the functions of the IoV, but also solve the research problems related to the IoV connection, and promote the realization and application of the IoV. As illustrated in Fig. 1, SIoV, as combination of SN and IoV, can be seen as a fusion of the concepts, features, models and applications of the two approaches; accordingly, SIoV has its own unique properties [12]. This paper uses the concept of social IoT [13] to redefine the concept of the SIoV.

Definition 1. The Social Internet of Vehicles is a subset of the IoV. Taking the moving intelligent cars as the nodes, and adopting the composition of SN, the vehicles' communication function can be utilized to realize the connection between V2X (vehicle and vehicle, person, roadside unit and service provider), as shown in Fig. 2. Information is exchanged with other communication-capable entities on the roadside in order to form a model with SN features; this enables the realization of the connection and application of SIoV, which is a form of SN-assisted realization with the car network as the main body.

The realization of these functions in SIoV is achieved through facilitating the cooperation between vehicles. This can help us to achieve unmanned driving, accident warning, the finding of alternate routes and other functions, which will enable the owner to have a better driving experience. The realization of these functions is based on real-time vehicle data, including some location or behavior data, such as *ID*, position coordinates, driving trajectory, etc. [14].

These data contain important information about the user location privacy and user individual privacy. User location privacy refers to the relevant user location data, which may contain the user location and travel trajectory. And the user personal privacy information refers to the users' home addresses, company addresses, physical conditions, hobbies and other sensitive information. There is a certain connection between user location privacy information and user personal privacy information generated by each user, and attackers may use the location information collected to infer more user individual privacy. Therefore, it is very necessary to protect the user location privacy information.

It is obvious that the location data is important for SIoV system. On the one hand, if these data are added or tampered with (for example, by adding false information), this will not only affect users' driving experience, but also cause safety problems. On the other hand, once these data are stolen by attackers [15], this will pose a threat to the privacy of the user information if data analysis and other related methods are applied [16]; accordingly, privacy becomes an important factor influencing the development of SIoV [17].

The purpose of protecting user location privacy is to minimize the risk of user privacy information being disclosed while ensuring the quality of relevant location-based services.

As illustrated in Fig. 3, due to the large number of SIoV users, the amount of data generated is huge, while there are also certain differences in the forms of data. Therefore, the location privacy protection technology of big data-based SIoV can be roughly divided into three categories: location privacy protection based on user attribute information (user personal information), location privacy protection based on user behavior information (users' behavior while driving), and location privacy protection based on user relationship network (the relationships of connection between users and other nodes in the social processes).

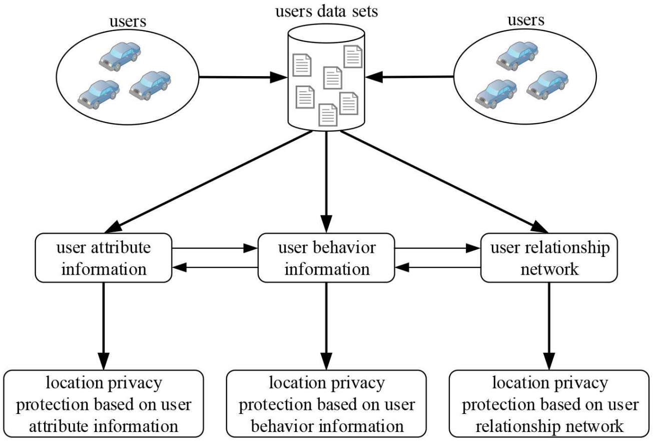
users
users data sets
users
user attribute information
user behavior information
user relationship network
location privacy protection based on user attribute information
location privacy protection based on user behavior information
location privacy protection based on user relationship network

Fig. 3 Information classification framework in the SIoV context

B. LOCATION PRIVACY PROTECTION MODEL BASED ON USER ATTRIBUTE INFORMATION

The attribute information generated by users in the SIoV context is similar across different platforms. User attribute information comprises the vehicle identification information and the user identity information (including the user personal *ID*, vehicle information and other archival information); these are used to represent the user identities during the processes of user information communication. Since the user attribute information is stored at the time the car is purchase and is also unique, the user identities can be more quickly identified with reference to the user attribute information; thus, the user attribute information is likely to become the target of attackers.

We define the type model of motor vehicles as *S*, which refers to the name given by the manufacturer to vehicles of the same genre, brand, type, series and body type, the license plate number as *N*, and the name on the vehicle's identity documents as *ID*. The user attribute information set is written as *{S,N,ID}*, When using the function of SIoV, the information obtained can help the system to accurately identify the entity users. The physical properties of the vehicle, such as its model and license plate numbers, have already been stored and cannot be changed. The user *ID* is equivalent to the user name, which is a code name in the processes of information interaction and can be changed according to the user needs.

In order to prevent attackers from guessing the user private location information through user attribute information, we need to protect the vehicle user *ID* when sending messages [18]. The method adopted here is to change the user *ID* or hide the user *ID* among other irrelevant users; this can hide the user real identities, interrupt the attackers' line of sight, and reduce the probability of the user real location being exposed.

C. LOCATION PRIVACY PROTECTION MODEL BASED ON USER BEHAVIOR INFORMATION

In the SIoV context, users need to send and receive messages continuously during the course of normal driving. Sensor devices and communication devices on the vehicle can digitize users' communication behavior and driving behavior. This behavioral information can be used to infer user personality habits, social status and other sensitive information. In this paper, these behaviors are summarized as the user behavior information set: here, *M* is defined as the set of SIoV message content, which contains all behavior information generated by users (for example, location information, request content, etc.). *M* can be divided into two subsets *L* and *Q* according to the user behavior information type.

Q stands for published content, which is the service requested content by users, such as points of interest, navigation or automatic parking and other required service types. *L* stands for location, which is the real-time positioning and interest points exposed while driving, and is a collection of single location points. Besides, a new behavior information set *T* is derived, *T* stands for trajectory, which means the track of user journeys, even if attackers have not taken all of the user location data information, it is possible to connect a rough trajectory through the multiple locations. The user behavior information set is written as *{L,T,Q}*.

The user behavior information set contains a large amount of private user information, which consequently attract attackers' attention. By analyzing the correlation between user attribute data and behavior data, researchers have built a multi-modal user data mapping model for use in further analyzing user behavior patterns. As can be seen from Fig. 4, based on several different application scenarios, this paper divides the location privacy protection methods based on user behavior information into three categories: positioning, trajectory and published content. This method is primarily designed to remove the correlation between user behavior and location privacy in order to achieve the goal of protecting location privacy.

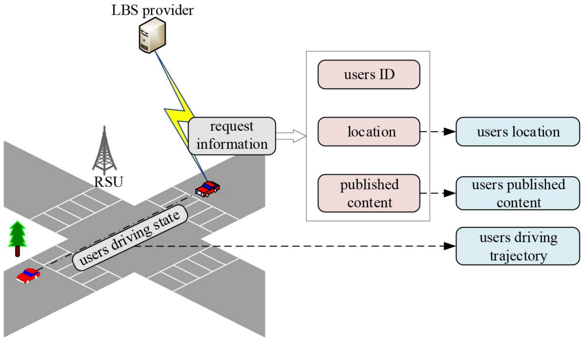

Fig. 4 Location privacy protection model based on user behavior information

D. LOCATION PRIVACY PROTECTION MODEL BASED ON USER RELATIONSHIP NETWORK

Intelligent connected cars move at high speeds; as a result, the connection and disconnection between users occurs very quickly, users need to interact constantly with other nodes while driving, and there is no guarantee that every node encountered on the road are trustworthy and will not betray the user. Even if the nodes are trusted, attackers may be able to infer private user information through real-time interaction and node behavior.

To facilitate more convenient analysis, we abstract the user relationship network structure into a more intuitive undirected graph $G = \{V, E\}$, where V represents the set of user nodes in SIoV ($V = \{v_1, v_2, v_3, ..., v_i, ..., v_n\}$), *n* is the number of nodes, and v_i is any node; moreover, *E* is the set of edges, $E = \{(v_i, v_j)|v_i, v_j \in V\}$, such that (v_i, v_j) represents the connection edge between the two nodes v_i and v_j, which represents the existence of a social relationship to the two nodes. When an information interaction occurs between the two nodes, an edge is generated.

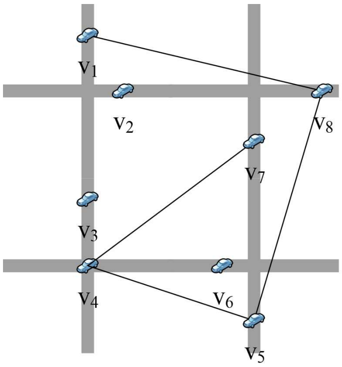

Fig. 5-a Real road map

In Fig. 5, Fig. 5-a illustrates the driving conditions of eight users on the road at a particular time. Moreover, Fig. 5-b represents the network structure. The user set $V = \{v_1, v_2, v_3, ..., v_8\}$, vehicles v_1 and v_8, v_4 and v_7, v_4 and v_5, v_5 and v_8 communicate with each other, while other users do not participate in the communication process, meaning that there will be no additional connection edge.

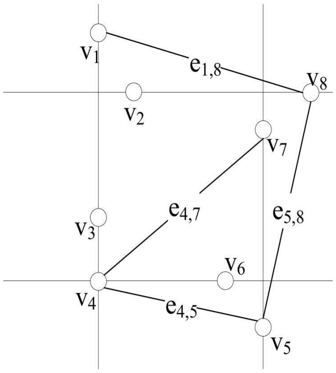

Fig. 5-b Road traffic network structure diagram

The user relationship network structure includes both direct and indirect connection relationships between users. Here, we study the evolution of the user relationship strength and analyze multi-hop users in the SIoV context; this is conducted through the analysis of the user behavior patterns and correlation content, as well as the discussion of the existence of potential relationships between the multiple hops users can in order to avoid attackers speculating indirectly about user private location information.

The social anchor model [19] fully proves that the social process may reveal the user attributes information, but it can also be a means for us to protect the user privacy. The same is true of SIoV, preventing attackers from guessing user real social processes by protecting users' social objects and social processes.

In the process of protecting user location privacy, entity users in SIoV are equivalent to network nodes. *A* is defined as the set of relations between users, it is defined here as:

$$A = (a_{ij})_{N\times N} = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & a_{ij} & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{bmatrix} \quad (1)$$

which is a connected matrix, and represents the friend relationship between two user nodes in the network. If a friend relationship exists between node *i* and node *j*, this is represented by 1; otherwise, it is represented by 0, represented as:

$$a_{ij} = \begin{cases} 1, & if\ there\ is\ a\ connection \\ 0, & if\ there\ is\ no\ connection \end{cases} \quad (2)$$

III. THE BASIC STRATEGY OF SIOV LOCATION PRIVACY PROTECTION

SIoV combines the characteristics of IoV and SN, and the application scenarios and relationship networks are more complex. SIoV has its own unique characteristics, which create more restrictions for the location privacy protection. Vehicles move quickly than ordinary pedestrians, and the connections and interrupts between users are very fast, so the topology change is faster of the whole SIoV. Besides, vehicles need to follow the road topology and traffic rules during driving, so the driving track is easier to be inferred. These limiting factors must be taken into account when designing the user location privacy protection algorithms. Therefore, user location privacy protection technology is more demanding than SN.

The basic strategy of SN such as *k*-anonymous, fake location methods and the generalization method can be used in location privacy protection of SIoV, but SIoV is so special, these basic technologies can not produce great protection. In order to achieve better performance of location privacy protection, researchers have made improvements based on these basic technologies. Crowdsourcing technology, social intimate fogs, ring signature and other methods are based on these basic strategies. After the simulation and comparison by researchers, these methods have better performance.

Every method gives full play to its performance only in the most appropriate scenarios. Users need to choose the most suitable method according to their overhead, delay tolerance, service precision requirements and scenarios, so as to fully protect their location privacy.

A. LOCATION PRIVACY PROTECTION POLICY BASED ON USER ATTRIBUTE INFORMATION

Since the vehicles' physical attributes cannot be changed, location privacy protection based on user attribute information can only be achieved through user *ID*. The main technologies utilized include anonymity [20] [21] and concealment [22].

Anonymous methods mean that users don't use the real *ID* name, instead, when sending information, a false *ID* is created or someone else's *ID* is used to obscure their real identities. This will interfere with the attackers' guessing processes and achieve the protection of user attribute information. The most representative method employed to hide user identity is *k*-anonymity. As illustrated in Fig. 6. When users need to access location-based services, they can send their demand information together with that of other *k-1* users, i.e. $\{M_1, M_2, M_3, ..., M_i, ..., M_k\}$, or send *k* user *IDs* $\{ID_1, ID_2, ID_3, ..., ID_i, ..., ID_k\}$ at the same time, which allows them to hide their *ID* names among those of other users.

In addition, researchers also use the concept of the logical group [23] to obscure the user identities, allowing them to become members of the group after their real identities are verified. Users belonging to the same logical group or troops can communicate freely with each other without revealing their private information.

This method is relatively simple for the users, and also has lower overhead. However, it cannot resist multiple guessing attacks by attackers; if attackers associate user attribute information with behavioral information, the probability of guessing correctly will be greater.

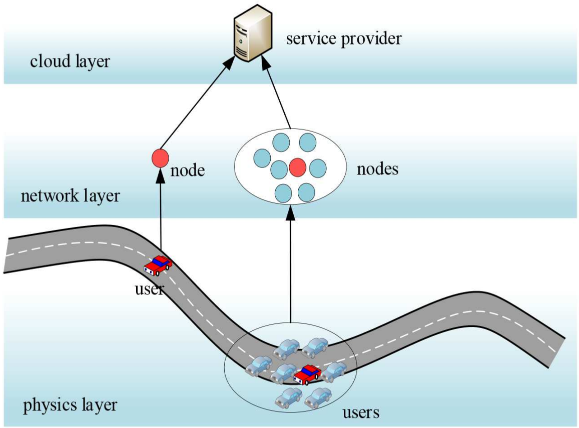

Fig. 6 The model of *k*-anonymity

B. LOCATION PRIVACY PROTECTION POLICY BASED ON USER BEHAVIOR INFORMATION

Location privacy protection technology based on user behavior information can prevent attackers from using the correlation between user attribute information and user behavior information to build a user data model, and can accordingly protect user location privacy more comprehensively. In this paper, user behavior information is divided into three information sets: a user location information set, a user driving track information set, and a user generated content information set.

The main user location-based location privacy protection techniques are similar to the user attribute-based location privacy protection methods, mainly the fake location method and the generalization method. The generalization method operates by obscuring the precise location of the user within an area, and meets the user demands for the protection for his/her location privacy by reducing the accuracy of the position posted by the user. This approach can hide their real location or destination among that of *k-1* other users; alternatively, the user directly sends *k* requests, so that even if the attackers obtain all of this location information, they can only obtain the approximate user location range. In short, the user location information is generalized in order to protect their true location data.

Moreover, the false location method means that the users send false locations when sending out their position information. In addition, the user can also use his/her friend relationship to help him/her forward demand information (although this approach can be easily affected by the credibility of the user's friend list). On this basis, crowdsourcing technology was proposed, and will replace friends who forward messages with "workers" who need to be rewarded, users will send their needs to the package in the crowdsourcing server, the servers will distribute these tasks to "workers", and these "workers" will help users to collect related services based on location in order to obtain the corresponding rewards; this can both stimulate the enthusiasm of "workers" and also ensure the quality of services obtained.

The location privacy protection based on the user travel trajectory is achieved by reducing the correlations between user location information in time and space. The simplest method is the "silent area" method, in which the user turns off his/her communication device and stays in the silent state, then returns to a communicative state after leaving the silent area. If this approach is used, the attackers cannot guess the user trajectory information during the silent period. In addition, false data is also a common method, employed to access other user or trusted third parties' information on the road in order to generate false location information; this will disrupt the attackers' line of sight and achieve the purpose of protecting the user trajectory information.

The location privacy protection based on user-posted comments is employed to prevent attackers from analyzing the users' destinations or other points of interest (PoIs) from the user demand information. The most common method is to use public and private key pairs to encrypt the content that the user needs to publish. The public key is generated by the system in each small area, while the private key is distributed by the system to each user and stored in a tamper-proof device in his/her vehicle. The user encrypts the messages with their own private key before sending, then uses the public key encryption on them, which greatly reduces the probability of attackers being able to access the user's actual published data.

Finally, the virtual trajectory [24] is also a commonly used location privacy protection method. By using the location information from a friend list, or that of other users they encounter, a certain deviation can be formed to distort their own true trajectory; this can disrupt the attackers' line of sight to a greater extent, thereby achieving better privacy protection.

C. LOCATION PRIVACY PROTECTION POLICY BASED ON USER RELATIONSHIP NETWORK

User relationship network-based location privacy protection technology uses the strength of potential relationships between the user and multi-hop users to protect the user privacy data. The most commonly used method is to select trusted users. However, this method is too restrictive, and group signatures are also relatively common. Users who enter the group communicate with each other under false identities, meaning that external attackers cannot infer the real identities of users from among the numerous users in the group. While attackers within a group can glean the destination of users they interact with, they are still unable to connect the users' pseudonyms with their real identities, which protects the location privacy within the user relationship network.

In addition, many researchers have proposed a network trust model [25] that can calculate the credibility of the users and data [26], thereby ensuring that the users and data in this model are sufficiently trusted. Another approach is to establish a trusted routing path [27] to ensure the security of the information during the transmission processes.

IV. CLASSIFICATION AND PERFORMANCE EVALUATION OF LOCATION PRIVACY PROTECTION TECHNOLOGIES IN SIOV

SIoV is a complex network structure that has been developed and perfected continuously in recent years. The amount of data information generated by users is large and diverse, and users have different privacy protection requirements. Therefore, existing location privacy protection methods cannot meet the requirements of all users. After determining a given user privacy protection needs, effective technologies can be identified to provide different services for different users. This article summarizes the current status of location privacy protection from three aspects according to users' differing privacy protection needs.

A. LOCATION PRIVACY PROTECTION BASED ON USER ATTRIBUTE INFORMATION

Every vehicle driven by user has his/her own identity, which can to some extent directly reflect the identity of the user. The physical feature information of the vehicle itself cannot be changed, and nor does it participate in the information exchange process of SIoV. When protecting user attribute information, only the user *ID* name can be protected in order to achieve the goal of privacy protection.

Dietzel *et al*. [28] proposed *k*-anonymity [29] to the study of location privacy protection in the SIoV context first. This involves hiding the user *ID* names among that of *k-1* other users nearby. Attackers thus cannot steal the user location information based on their *ID* names, which facilitates the protection for the user attribute information. When the difference between the *k* users is large, however, the attackers can infer the user *ID* through analysis. Accordingly, in order to reduce the degree of identification between users, Wu *et al*. [30] proposed using a BP neural network to calculate the similarity quickly and accurately between vehicle attributes and establish a communication group based on attribute similarity, thereby improving the stability of the group topology. The base stations generate pseudonyms and keys for the vehicles; using these pseudonyms for communication not only can prevent other attackers in the group from discerning their identities, but also protects the user attribute information.

It is difficult to search for users with similar attributes and close proximity; thus, this method is not universal and can only be used in scenes with a dense group of users. In allusion to the multi-user collaborative collision avoidance system proposed in literature [31], a broadcast anonymous method has been proposed to solve the efficiency and scalability problems associated with anonymous authentication. Through using the certificateless aggregate signature, anonymous and batch authentication technologies, users can employ a combination of digital signatures and group signatures when transmitting data. Moreover, batch verification with fog equipment [32] can effectively facilitate the confidentiality of user attribute information in the cooperation process and protect the user location privacy information. Lu *et al*. [33] made improvements on the basis of anonymous authentication by proposing a blockchain-based anonymous authentication scheme (BAAS). According to this approach, the vehicles use the public keys as pseudonyms for authentication purposes during the communication process. This not only ensures the authenticity of the source and the integrity of the news, but also realizes certificate transparent in order to avoid leaking of the user real identity information.

When the attackers are hidden among the *k* users, however, the system cannot accurately identify the attacker. For this reason, Mei *et al*. [34] proposed an anonymous access control scheme based on pseudonymous authentication. Users need to register fake identity information and tokens from traffic management agency authority before obtaining services; when user uses the false identification application services, the token can generate a false certificate for the session before each communication takes place. This method can protect the user attribute information. When a dispute occurs, the authority also can reveal the user real identity at any time. In order to further impact malicious nodes, Caballerogil *et al*. [18] used the concept of logical groups to propose a new method of *k*-anonymity: according to this method, each user has a certificate to prove his/her identity, and users in the logical group share a pair of keys, meaning that attackers will be unable to distinguish a specific user from the other *k-1* users in the group. The system can track nodes which are complained according to the user signatures, and can therefore revoke the malicious nodes in time while also protecting the user attribute information.

In order to accurately measure the degree of user privacy information protection provided by the anonymous method, researchers have proposed *k*-anonymous entropy [35] differential privacy [36] and other methods. However, because these methods fail to consider the changes in anonymous collection size and anonymous duration, the measurements are inaccurate. Corser *et al*. [37] summarized the existing anonymous measurement research standards and proposed the comprehensive performance index KDT after considering the factors related to the anonymous methods. Here, *K* means the size of the average anonymous collection, *D* represents the average distance of the anonymous user location deviation, while *T* represents the time of anonymity. Compared with the traditional *k*-anonymous entropy, this method can more accurately measure the degree of privacy protection provided by an anonymous method.

When there are few neighbors around a user, this user is unable to cannot hide their identities effectively. Accordingly, in order to reduce the influence of the number of adjacent nodes on the degree of user privacy protection, Li *et al*. [38] devised a novel identity management method. Considering a target user, when other users and the target user are in the same group, they exchange pseudonym information between each other. When there are no other users within a certain distance, the user can apply for a new fake identity for communication purposes. Because this fake identity is randomly obtained from the system, it can effectively resist malicious attacks. When this service is no longer reliable, however, the user identity information will be directly exposed. Moreover, Yu *et al*. [39] proposed a method that does not rely on the servers, and instead integrates the concept of mixed space into the method of exchanging pseudonyms, such that the concept of MixGroup was proposed. During the driving process, exchanging pseudonyms is continuously performed with other users that the user encounters; this can greatly increase the number of pseudonyms that can be utilized, meaning that the probability of attackers using the *ID* to track the user is greatly reduced. Even in cases where vehicles are sparse, this approach is better able to protect the user attribute information and achieves the good performance.

While anonymous schemes can effectively hide user attribute information, changing pseudonyms at inappropriate times and places may result in private information being exposed. In order to facilitate better performance of these methods, it is therefore necessary to consider the appropriate timing. Lu *et al*. [40] proposed a social spots strategy (PCS) for changing the user names (which has accessed to more unique properties of users), using the size of the anonymous set as the standard of location privacy measurement, and using game theory methods to demonstrate that the method is practical in real-world applications. Better results are achieved when this method is used to change the pseudonym at a specific place. To make the method of changing pseudonyms more flexible, one research scholar combined pseudonyms with ordinary Mix-zone technology [41] [42] to improve performance, Xia *et al*. proposed a dynamic traffic-adaptive Mix-zone [43]. According to this method, users can measure the protection level of the Mix-zone based on joint entropy, then decide whether to dynamically create the Mix-zone that will allow vehicles to change their pseudonyms at any time. This system can achieve differentiated protection that can flexibly accommodate the needs of different users.

When the number of pseudonyms is sufficient, the probability of users being able to hide their attribute information will be greatly increased, while the degree of protection provided for their location privacy will also be higher. However, the addition of too many pseudonyms will burden the system and cause a waste of resources. In order to avoid the abuse of pseudonyms, researchers have proposed some conditional cryptography-based anonymous authentication schemes [20] [21]. However, these methods have high computational complexity and high communication cost. Zhang *et al*. [44] proposed a pseudonym distribution managemen-t scheme based on mobile cloud computing, in which a certification center generates vehicle pseudonyms at a constant rate and stores them in the repository, when a user needs to access services, he/she applies to the local cloud for the pseudonym ahead of time. This approach utilizes a pseudonym management scheme based on fog computing, which has abundant network edge resources; accordingly, the method can transfer the pseudonym management system to the fog, which is composed of roadside units (RSUs), and proposes the concept of pseudonyms change choice pseudonyms problem, which can effectively reduce costs and ensure that the user attribute information is safe without creating delays in data transmission. Moreover, in order to solve the problem of computing complexity, Wang *et al*. used the dimension reduction method to manage the pseudonyms [45]; this reduces both the time cost and space complexity of vehicle certifications, while the new condition of anonymous VKPCA (vehicular communication network based on kernel principal component analysis) is also implemented to avoid abuse of the anonymities at the same time. This approach has lower computational complexity, while also being able to protect the user attribute information.

Location privacy protection policy based on user attribute information is mainly to change or hide user *ID* names to achieve the purpose of privacy protection. False *ID* names, hiding in other users may help users confuse the attackers' perceptions to a certain extent and reduce the correlation between the *ID* names and the location information. The attackers cannot associate the user *ID* with real-time location information in time, thereby the probability of being successful guessing was reduced. Moreover, the user *ID* does not affect the accuracy and timeliness of users want to enjoy services, so this method does not affect the availability of the services.

Location privacy protection policy based on user attribute information is relatively simple to implement. However, there is an obvious disadvantage that these methods cannot resist the repeated attacks of attackers. The probability of success will increase gradually and the protection performance of these methods will be greatly reduced if guessing attacks are leveraged many times. Therefore, there may be higher performance to protect user location privacy via user behavior data.

B. LOCATION PRIVACY PROTECTION BASED ON USER BEHAVIOR INFORMATION

The sensor equipment and mobile communication technology contained in the vehicle can digitize a certain amount of user behavior information: this includes the user attribute information, but also implies the user personal habits, social status and other sensitive details. This information can in turn be used to infer private information about the location of the users' home and work addresses, through mining and finishing. In order to protect the user behavior information, this article summarizes the user behavior information set into three aspects location, driving track, and published content and summarizes the status of the contemporary research.

1) Privacy protection based on location

In the SIoV context, users need to continuously broadcast their location in order to obtain LBSs, such as navigation, road advanced alarm, and service query. They need to provide location information for service providers. Since these service providers are untrusted or semi-trusted, these actions will expose the user location information at that time; thus, protecting the precise location of users can effectively protect the user private location information while sending information.

In order to avoid revealing the user location information while information is being sent, researchers hope to hide the user real location during this process. *K* service requirements can be used to confuse the users' real target location. However, because the vehicle moves at high speeds, *k*-anonymity is generally difficult to achieve. Liu *et al*. combined the caching strategy [46] with the *k*-anonymity strategy to propose a location privacy protection strategy based on active caching [47]. Within the RSUs, some services are cached and provided for users freely. Each user sets a *k* value depending on their own needs. Users then send *k* requests while traversing the driving path to the roadside units containing their needs. When the RSUs are unable to satisfy the user needs, users will send their requests to the service providers. This method can satisfy the users' needs at the lowest possible cost, and also protects the privacy of the user behavior data; however, this method also requires a large amount of calculation. Li *et al*. [48] proposed an efficient, energy-saving location privacy protection scheme, which can transfer the users required location-based service requests to the fog and gather close foggy family members in order to form social intimate fogs for two-way transmission; this approach can isolate the direct communication between users and the service providers. Accurate position information can be hidden, and a content caching mechanism is also introduced to help users send queries quickly and flexibly, thereby providing communication delay compensation.

The two above-mentioned methods can reduce the delay to some extent. However, when the pre-cached content is unable to meet the user requirements, the resulting delay will be larger. Researchers examined researches on user queries about the SIoV, and found that this delay is a problem that needs to be urgently solved. For this reason, a new fog computing-based LBS framework is designed [49] that supports mobile queries. Outsourcing some services from the service providers to the fog nodes can compensate for the deficiencies in cloud processing. Moreover, on this basis, two privacy-protected query schemes are proposed: kNN and T-kNN. For the user query request, the system feeds back the *k* closest PoIs to achieve a low-latency query response, while T-KNN supports fine-grained PoI queries. This privacy protection method can ensure that users' queries are immediate and reliable.

Furthermore, using a fuzzy real location will affect the accuracy of obtaining relevant services. Accordingly, the researchers propose using trusted partners to forward these messages; this not only avoids disclosure of the location information, but also ensures the availability of the services. Ying *et al*. proposed a social privacy-based location privacy protection (SLP) method to protect user behavior information [50]. Using multi-hop trusted users in a certain area obfuscates the initial sent location, and also puts forward a social list that helps users in selecting reliable partners, even if there are no trusted partners within the original sender's communication range. The method also achieves a higher level of privacy protection for the user behavior information. Subsequent improvements have been made on this basis, and a social perception-based location privacy protection method was consequently proposed [51] [52]. B-SLP can enable users to obscure their location within a certain area, while I-SLP can conceal users and confuse them with the other *k-1* users located in the same area; moreover, E-SLP can encourage the other *k-1* users to cooperate, which can further protect the user behavior information and help to ensure the user service quality.

Although the method of relying on partners to forward messages is effective at helping users to hide their location, it still requires the cooperation of trustworthy partners. Accordingly, crowdsourcing technology was proposed to distribute the content that users need to multiple "workers" through the crowdsourcing servers, after which the relevant results are collected by these "workers" and fed back to the users [53]. "Workers" involved in crowdsourcing may therefore disclose their locations. In order to solve the location privacy problem posed about "workers" in crowdsourcing, Qian *et al.* [54] used location differential privacy to obscure user real location and designs a task assignment strategy based on this disrupted location. This mainly includes three components: participants, task publishers and a task publishing platform. The task publisher publishes tasks, along with the minimum number of subtasks for each task, to the platform. Platforms using differential privacy can protect the location privacy of participants, as well as cause participants' moving distance to be minimized in order to optimize the distribution strategy. Participants use the disturbance mechanism to upload their false positions on the platform; this not only protects the participants' private location information, but also ensures the availability of the collected services.

Another problem associated with crowdsourcing technology is that of how to ensure that the "workers" collection of messages is reliable. Azad *et al.* [55] proposes a collaborative crowdsourcing vehicle location privacy protection system. According to this method, users obtain the required services through feedback from users in the group. Evaluation and scoring can help users to obtain high-quality services. As the encryption and decryption phase of this process does not depend on other third-party systems, it is better able to protect the user private behavior information and avoid the occurrence of single points of failure. Furthermore, the rewards for "workers" need to be borne by users. In order to make the obtained information more reliable and reduce certain expenses, it is necessary to choose higher quality "workers" [56]. Yahiatene *et al.* [57] introduced a blockchain structure and proposed a distributed connected dominating set algorithm; this approach can support a highly dynamic network topology, as well as dynamically select trusted and reliable "workers" for users (the users' mobility will not affect the quality of the selected "workers"). When the users take all the required services package for "workers" in a reliable manner, this does not only protect the user behavior information, but also enables high-quality services to be obtained.

It is not only the sending of information that can reveal the user location information, but also the parking location. As the state of the vehicle when it is stopped is very different from when it is driving, it can be easily stolen by attackers. Regarding the correlation between parking location and user privacy preferences, Ni *et al.* [58] proposed a user social behavior-based privacy protection data forwarding protocol designed to protect user behavior information and send the observed user social behavior to nearby RSUs; when users revisit these social networking sites, they can retrieve information from the RSUs directly, allowing them to avoid contact with service providers and thereby protect their behavior information. Moreover, due to its lower latency and higher delivery rate, this method is suitable for using in shopping malls, as users can receive related services without sending requests. Yin *et al.* divided user related location services into discrete and non-discrete location points according to the crowd density [59], and subsequently proposed a hybrid location privacy protection method based on differential privacy *k*-means, which are improved through the application of differential privacy technology [60] and the clustering algorithm [61]. Generalizing the non-discrete location points and adding noise to the discrete points facilitates the protection for user behavior information.

The main principle of the location privacy protection policy based on location is to utilize the false location or generalize user real location. Forwarding by friends, crowdsourcing policy can help users get more accurate service information through adding rewards, the RSUs caching function not only reduces latency, but also reduces overhead for users. In these methods, the attackers cannot intuitively obtain users' accurate real-time location information, thus user location privacy will be protected from the root directly.

These methods start from the single positioning of users and reduce the probability of tracking to the real-time location by attackers. Users need to send their location continuously in order to get relevant services during driving, when false locations are generated in areas where vehicles are unlikely to appear, such as rivers and buildings, they are easy to be identified. Even if they are multiple false location data, there is a correlation in time and space. If the attackers connect these locations, it will form a rough trajectory of the user's travel history, from which the user location data can be indirectly inferred. Therefore, it is very necessary to protect user position privacy from the direction of the driving trajectory.

2) Privacy protection based on driving trajectory

The user trajectory contains correlations in time and space across multiple locations as they drive, meaning that the user private location information can be inferred based on their driving trajectory. For example, due to work or family commitments, vehicles may regularly pass through the same fixed locations or driving along a fixed trajectory. From this information, attackers can guess at the users' home addresses, workplaces, and other sensitive information based on the starting and ending positions of the users' daily path. Protecting the user driving trajectory can prevent the attackers from speculating on the user personality, habits, preferences and other relevant information, thereby achieving the protection for the user private location information. Over a long time, user behavior characteristics exhibit a certain regularity.

Lu *et al*. divided services into two categories according to the different service types required by users delay tolerant network (VDTN) and non-delay tolerant network (VDNTN) and designed different location privacy protection schemes for each of these. Du *et al*. [62] designed a vehicle privacy protection scheme that combines running and transmission for the VDTN. While driving, the users will pass information to the vehicles or RSUs that they encounter. When considering only the location and time of the RSUs that eventually receive this information, it is very difficult to determine the user driving trajectory; accordingly, the protection for the user behavior information is realized. Basaran at al. [63] designed a location privacy protection scheme for typical application intersections in non-tolerant networks, based on the invisible intersections of the blockchain. The vehicles that will pass through are regarded as a queue, while the driving goals of the vehicles are submitted in RSUs. For the roadside units, the processor executes the traffic scheduling algorithm with reference to the traffic rules and the information collected, controls the color and timing of the signal lights, and is thus better able to manage the traffic flow and protect the user driving trajectory.

Historical location data can reveal the user individual information. Yu *et al*. [39] hoped to protect user driving trajectory information by protecting their parking location information. As the users stopping positions depend on aspects of the user personal identity, when the vehicle stops after a period of time and then begins to move again, it can be easily identified by the attackers; the attackers can then recognize and guess the user's mobile location and carry out a mobile preference attack. Therefore, a method that protects the user trajectory based on the privacy of the parking location was proposed, and the user behavior information was protected by removing the correlation between the users and their parking location. Sun *et al*. [64] found that the user location was related to interests, and proposed a region-of-interest division-based algorithm to preserve the location privacy of mobile device users in location-based cyber services (PPCS) for SN. On this basis, Memon observed the density of vehicles, and found that most vehicles stopped in social hotspots, such as traffic intersections, congested roads, shopping malls, and hospitals. To address this situation, a new multi-mixed area decorrelation privacy model was proposed that reduces the influence of the behavior trajectories of user private information [65]. Moreover, they considered using the method of multiple mixed regions to replace these hotspots, thereby removing the correlations; experiments have shown that this method is more effective than using traditional data.

When attackers try many times to speculate about the user trajectory, the correlation-removing methods cannot protect the user location privacy as effectively. Accordingly, researchers have proposed the method of generating false location/trajectory to mislead the attackers. Liao *et al*. [66] designed a 5G-based MFemtocell technology framework using pseudonymous technology to address the impact of users' exposure on their driving trajectories, and consequently proposed a dynamic grouping algorithm (DGD) to resolve the SIoV security and privacy issues brought about by this high-speed dynamic privacy. Users dynamically generate groups [67] of areas along their own trajectories while driving, constantly exchanging pseudonyms with other users in the group; users will then get new pseudonyms after leaving the group, which increases the difficulty of guessing and thereby protects the user movement track. When users enjoy location-based services anytime and anywhere, they constantly expose their location privacy and driving routes. For this reason, Cui *et al*. proposed a location privacy protection scheme based on real-time location data [68]. This method dynamically generates a virtual position for users according to the driving conditions, which misleads the attackers about their driving route, and uses anonymous set entropy and the success rate of track as a measure; subsequent experiments proved that this method is better able to protect the user routes.

Moreover, researchers have also found that the trajectory information can be protected by suppressing the transmission of position data. Buttyan *et al*. [69] added a silent area on the basis of the mixed space and designed a position privacy protection scheme based on the mixed area. This involved setting a concentric circular quiet area around the mixed area. After entering the silent area, the vehicles will adopt a random silence strategy to stop its own communication. After passing through the silent space and entering the mixed space again, they will resume the communication randomly according to the silent strategy. When a vehicle drives out again, attackers cannot link it to a particular vehicle that entered the area; thus, user trajectory privacy protection is realized. However, since users cannot send information during this time, this will affect the use of functions such as automatic parking and route planning. Mixed areas such as these are generally set up at large intersections or shopping malls. Li *et al*. [38] applied crowdsourcing awareness technology to SIoV and designed a two-stage privacy-preserving (TSPP) suppression algorithm to avoid the leakage of user private information. While driving vehicle, some data needs to be uploaded regularly, and there is a certain probability at a certain location that the system will suppress the uploading of certain sensor data. TSPP can reduce the correlation in time and space for the user between two consecutive locations; this will not only protect the user trajectories, but also prevents users from enjoying location-based services.

Due to users usually send out location-based information during the normal process of driving, and user behavior characteristic has certain regularity, user personal privacy information can be inferred from the user trajectory. The privacy protection technology based on driving trajectory can reduce the correlation between multiple locations, and reduce the probability that the user trajectory information will be exposed, researchers mainly achieve privacy protection by the false location positions, blurring the accurate locations and suppressing the sending of the location information.

However, real-time positioning and driving trajectory policies only start from the location data, and the purpose of protecting the location data is achieved by hiding accurate locations, fuzzing the relevant location information, but they ignore the demand content in the user request information. User published content may contain other information such as the user's target location and interests, this information can be used by attackers to indirectly infer the user location data. The location privacy protection technologies based on location and driving trajectory are not enough to protect the user location information. Therefore, researchers consider to protect location privacy from the aspect of published content.

3) Privacy protection based on published content

In addition to their own target location, the information sent by the user also includes the content of the services they require or the data they communicate with other people. An attacker who steals this type of data can conceivably sift out the key information, while users' interests can be obtained through modeling, analysis and other information. Thus, protecting the user published content information can reduce the risk of privacy.

Wang *et al*. provided a comprehensive review of the privacy protection algorithms about user disseminated content [14]. This review summarized the privacy issues and attack patterns of content dissemination, along with the challenges and problems to be solved in the future related research. Wu *et al*. [30] proposed a secure multimedia data transmission mechanism based on the pseudonym, which employs user attribute information to dynamically generate a unique key for the users. Users will encrypt the data they transmit using this key, which can prevent users from outside the communication group from attacking and stealing the communication data. While this ensures information security, it can also reduce the complexity of key generations. It can effectively protect user behavior information when combined with pseudonym technology.

Users who employ signature technology to encrypt messages can better protect their privacy; however, the system will encounter certain difficulties when verifying the user identities. The identity-based batch signature verification scheme [70] [71], while able to authenticate messages, is not resistant to replay attacks and does not possess the capacity for anti-repudiation [72]. Lu *et al*. [73] conducted research on user information security, improves on the existing methods, and proposes a certificate signature scheme based on pairing technology. The user first needs to register with an authority; subsequently, the trusted authority (TA) generates a public and private key pair for the user after verifying the user identity. Users store these keys in the vehicle's anti-tampering device and generate an anonymous certificate for message authentication before each communication. As shown in the Fig. 7, When other entities receive the messages, they first authenticate the certificates and signatures of the messages; when both have passed verification, the reliability of the message is determined.

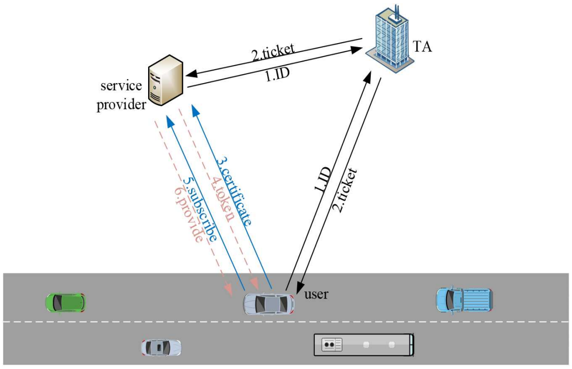

Fig. 7 Services based on pseudonym authentication

Yang [74] proposed a location privacy protection method to defend against attacks in LBS background IoV. This is mainly achieved through five steps. In the first step, the user identity, location and request content are split into two groups, then encrypted and sent to the trusted third party (TTP) and the service provider (SP) respectively. After receiving the information, the TTP and SP extract the content, check the packet loss, and then send the signature to the SP in order to query the most accurate services. The third party forwards the services to the user based on the received address. However, this method necessitates reliance on a trusted third party, which is prone to a single point of failure. For this reason, Li *et al*. introduced fog computing into the line sharing service SIoV model to preprocess user data and establish the system [75]. This new security model uses fog computing to reduce the bandwidth required by the system, and further improves anonymous authentication to protect user identity information, limits the number of participants by limiting the rate, and uses the resolution capability rate to request routing services that can protect the privacy of users and groups.

Privacy protection based on published content is mainly to reduce the probability of information disclosure through encryption and signature, and try to ensure the security of information on the basis of ensuring the integrity of published content. Compared with the location privacy protection technologies based on location and driving trajectory, privacy protection based on published content has a lower impact on the accuracy of services, but complexity and computational cost will be higher.

The three policies based on user behavior information can protect the user location privacy to some extent, but they all have imperfections, for example, they don't take into account the objects of information interaction. Unreliable social friends in the user relationship network may also leak user information for profit. Thus, the user relationship network is also a weak point from which attackers could obtain user location information. Accordingly, in order to reduce the risk of user location privacy leakage, we need to protect the user relationship network.

C. LOCATION PRIVACY PROTECTION BASED ON USER RELATIONSHIP NETWORK

The user relationship network structure in the SIoV context includes a relationship of direct or indirect connection between users. Due to the high-speed mobility of the smart vehicles, the user relationship network structure will also continue to change. The connections between nodes face many unknown attacks. For example, unreliable social partners may sell user relevant data. Attackers may also speculate on user habits and preferences by analyzing social relationships. Accordingly, researchers have proposed various research methods to protect user location privacy by analyzing social user relationship network.

The collection of real-time traffic information in the SIoV context requires data collected by users; however, this will result in user location data being exposed. Thus, Feng *et al.* [76] proposed a selective sharing scheme (S2PD). According to this method, the user will need to upload the data through encryption keys. When the data needs to be shared, the encrypted data in the cloud will be decoded into a semi-decrypted state; subsequently, the receiver downloads the semi-decrypted data and uses the sender's key to decrypt it. Because the user shared this data through the cloud services, the data will not be sent to unauthorized users, meaning that users will not reveal their information to untrusted users when sharing sensitive data. In order to ensure the real effectiveness of interactions in the process of information sharing, Chen *et al.* [77] proposed a blockchain-based data exchange framework that sends the user data to the data pool. The users on the receiving end announce the services they need and search the data pool for optimal data, while the users at the sending end send the data through the edge server after verifying the identities of the receiving users, which improves the efficiency of information interaction. This article also proposed an iterative two-way auction mechanism designed to encourage more users to participate, which can ensure that the interests both parties are maximized. This will not only ensure that both parties can obtain the information they need, but will also hide the user private information.

Because the topology of the vehicle-mounted ad hoc network is random, it is able to accommodate any connected node. The collaboration between nodes is highly important. In order to reduce the threats to privacy caused by socializing with untrusted users, users try to select some trusted users to make friends with. Referencing the method that user identification based user attribute information in across social networks [78] can help researchers to find two users whose properties are more similar.

Li *et al.* proposed a privacy protection scheme for friends matching that represents the user feature attributes in binary [79]. The elements in the attribute information set are operated with hash algorithm and run the transmission protocol which based on random inadvertent. Finally, the users are matched according to similarity. The users matched only to know whether or not there is an intersection between the characteristic attribute sets matched by both parties, but do not know any other information about the other side's intersection attributes; thus, users can share information with each other without worrying about privacy. Due to the large number of SIoV users, it takes a large amount of calculation to select users with similar characteristics and attributes. Xiao *et al.* [80] designed a privacy trusted network model based on user credibility, further used the Bayesian algorithm to represent the degree of confidence of a specific vehicle as a random variable, after which he subsequently designed a vehicle rating algorithm to evaluate the vehicle level. Communicating with highly trusted users can reduce the risks of user privacy; when the user trustworthiness is listed, the users can identify which nodes are untrustworthy and freely choose users to cooperate with.

Researchers have hoped to use the anonymous identities to complete the information exchange process by means of the group signature method; however, the joining and revocation of members remain problems. Regarding vehicle safety communication, researchers have combined the pseudonym and the group signature approaches [81] to create the ring signature [82] [83]. This approach exhibits good anonymity and spontaneity [84] [85] and can provide very good protection for communication between users. However, the problem of how a ring should be formed between users needed to be solved urgently. Accordingly, Mei *et al.* used encryption technology [86] to improve the ring signature scheme by allowing users to form a ring spontaneously while driving; to achieve this, the system distributes a public-private key pair for each user. This article designed two ring formation methods: the RSUs auxiliary rings formation method is mainly used in areas with complete technical facilities, while the autonomous collaborative ring formation method between users can be applied to areas with imperfect infrastructure and is easily able to cope with the joining and revocation of members. These methods feature non-repudiation and traceability.

Although signature schemes can hide user identities, verification is difficult, and researchers accordingly hope to establish a more secure communication environment for users. Yang *et al.* [87] proposed a social network approach to study trustworthy information sharing. The traditional SN method was used to study user credibility in the SIoV context. Trust between users was divided into direct trust and indirect trust, with strong and weak connections between users indicating the differing trust levels. The author classified the data, designed an indirect trust model and algorithm, and built a secure network capable of sharing information. Accordingly, users can share information at any time without worrying about the leakage of their private information. However, the calculation involved in this method is more complicated. Wazid *et al.* [88] proposed an authentication key management protocol (AKM-IoV) based on fog computing. In this approach, vehicles, RSUs, and cloud servers perform authentication key management between fog servers to verify their identities, then communicate with each other. The parties then establish a session key between them to ensure secure communication. As the communication between users is completely confidential under this model, malicious users cannot track the user private information through their communication. This method has superior security features.

The location privacy protection method based on the user relationship network can compensate for the gaps in location privacy information protection in terms of both user attribute information and user behavior information. Existing researches on user relationship network-based location privacy protection are mainly centered around finding reliable users. This method can be applied in combination with other types of user information to obtain better privacy protection performance.

The location privacy protection method based on user relationship network starts from the network structure of information interaction, can compensate for the gaps in location privacy information protection in terms of both user attribute information and user behavior information. Such as selecting trusted friends, unique key and signature, these methods have higher protection effect on the user relationship network, can prevent the communication objects from leaking user data information, and cannot affect the accuracy of the services. However, they are of high complexity and easy to produce certain delay, which is suitable for services with delay tolerance.

Existing researches on user relationship network-based location privacy protection are mainly centered around finding reliable users. This method can be applied in combination with other types of user information to obtain better privacy protection performance.

D. PERFORMANCE EVALUATION

Location privacy protection technologies for SIoV need to consider the availability of services and operating costs on the basis of user privacy protection. This paper measures the degree of privacy protection from the following three aspects:

(1) Availability of services: Refers to the convenience and effectiveness of SIoV in providing users with location-based services, which reflects the service quality obtained by users after using location privacy protection methods in the SIoV context. Comparing the quality of services obtained before and after using the location privacy protection algorithm, and analyzing the value of delay and service precision, can figure out the degree of influence of these technologies on service availability.

(2) Degree of privacy protection: Refers to the measurement of user location privacy protection, which is generally reflected by the risk of disclosing private location information, and which stands in contradiction with service availability. The higher the degree of privacy protection, the lower the service availability; accordingly, a balance between the two needs to be struck.

The trajectory anonymous entropy and tracking success rate are used to represent the degree of protection of user location privacy from the relevant studies. Trajectory anonymous entropy H_i is used to represent the degree of uncertainty of the correlation between trajectory T_i and trajectory T_j:

$$H_i = -\sum_{j \in AS_i} p(i,j) \times \log_2 (p(i,j)) \tag{3}$$

Here, $p(i,j)$ represents the probability that the attackers regard the false trajectory of user *j* as the true trajectory of user *i*, that is, the probability that the user *i* hides his/her true trajectory successfully.

The tracking success probability is the anonymous set size of the vehicles' trajectory $|AS_i|$. This is equal to the probability of 1, and can be written as follows:

$$Pt_i = \Pr(|AS_i| = 1) \tag{4}$$

Here, the anonymous set AS_i about user *i*, is a set of all target LBS users (including *i*). If $|AS_i| = 1$, then user *i* has no anonymity. To measure a system's overall tracking probability, one method is to compute the percentage of users with $|AS_i| = 1$. For example, if 47% of all users have $|AS_i| = 1$, then Pt = 0.47 and the system assures 53% anonymity.

(3) Calculation overhead: The computational cost of protecting the user private location information in the SIoV context includes computing cost, runtime cost and service provider cost. These costs generally require users to share. Different users have different budget expenses, so the goal is to reduce the expenses on the same degree of privacy protection.

We searched the performance indicators in the existing literatures, studied their simulation processes, and analyzed their simulation results and diagrams to find the average values of the three performance indicators in each class of methods. Finally, we conducted detailed theoretical analysis of each class of methods according to the three performance indicators. The analysis and comparison results of various user location privacy protection algorithms for different user data types are listed in Table 1.

Location privacy protection policy based on user attribute information simply operates on the user *ID*, it will not affect the service quality, so the service availability obtained is relatively high. The calculation processes of the algorithms are relatively simple because they are achieved through a simple *k*-anonymity or pseudonym, which requires less computational overhead. However, these algorithms are not enough to resist multiple attacks by attackers, so the degree of user location privacy protection is general.

Location privacy protection policy based on user behavior information is analyzed in three categories: location, driving trajectory and published content. The whole processes of algorithm implementation require more computation, so

Table 1: Performance evaluation of location privacy protection policies

Techniques	Calculation overhead	Service availability	Degree of user location privacy protection
Location privacy protection policy based on user attribute information [28]- [45]	low	medium	medium
Location privacy protection policy based on user behavior information [46]- [75]	high	medium	high
Location privacy protection policy based on user relationship network [76]- [88]	medium	high	medium

users will be allocated more computation cost. The original data sent by users may be lost during the calculation process because the entire calculation processes have many steps and are complex calculations, which will have a certain impact on the service availability. User location data can be protected from the attackers because of so many precise calculations, so the degree of user location privacy protection is very high.

Location privacy protection policy based on user relationship network protects user social processes, it will not interfere with the factors affecting the quality of services, such as the addresses of users and published contents, so the service availability obtained by users is relatively high. However, such methods require constant user authentication and therefore incur some overhead. This type of algorithms can reduce the leakage of user location data in the processes of information transmission and achieve a relatively high degree of location privacy protection.

We analyzed the degree of user location privacy protection from the perspective of application scenarios. We can divide application scenarios into three types: social hot spots (shopping malls, intersections, hospitals and other areas with high traffic flow), roads with normal two-way traffic, and remote areas with low traffic flow. The analysis and comparison results of various user location privacy protection algorithms for application scenarios are listed in Table 2 (✓represents that the algorithms can have better performance in the application scenarios).

When a user is in a social hotspot, a large number of users can communicate with the target user. All three methods are suitable for such a scenario. The location privacy protection technology based on user behavior information can protect the location information about users from three aspects of location, driving trajectory and published content, which can achieve a higher degree of location privacy protection.

When a user is in the roads with normal two-way traffic, he/she need to obey the traffic rules, so there is not enough opportunity to change their driving route, which brings some difficulty to the protection of location privacy. The user needs to interact with other unfamiliar users to obtain LBSs, so user location privacy needs to be protected from the perspective of user relational network. Therefore, the location privacy protection policy based on the user relationship network has a higher degree of protection for the user location privacy.

When a user is in the remote areas with low traffic flow, there are not enough users here to help he/she achieve location privacy protection policy based on user relationship network and *k*-anonymity based on user attribute information. The user can only achieve location privacy protection by constructing false location/trajectory, thus, the false location method and virtual trajectory technology can achieve a higher degree of protection for user location privacy.

Table 2: Application scenarios analysis of location privacy protection policies

Techniques	social hotspot	two-way traffic roads	remote areas
Location privacy protection policy based on user attribute information [28]- [45]	✓	✓	
Location privacy protection policy based on user behavior information [46]- [75]	✓		✓
Location privacy protection policy based on user relationship network [76]- [88]	✓	✓	

The location privacy preservation technology in SIoV has great signification for the development of SIoV applications. This paper surveys recent progress in the area, summarizes existing research results, and introduces three types of location privacy protection algorithms. It can thereby be seen that each type of privacy protection algorithm has its own unique characteristics. As shown in Table 1, the scope of their application and performance can vary. Location privacy protection policy based on user relationship network has the highest service availability, in degree of user location privacy protection aspect, location privacy protection policy based on user behavior information has the best performance. Moreover, a further comparative analysis of location privacy protection policies was provided in Table 3.

V. FUTURE WORKS

We can obtain the information we need in various ways; at the same time, our private information can be leaked in many ways. The attackers, moreover, may exist on any stage in the process. As our daily life becomes increasingly intertwined with intelligent technologies, the attackers' methods of attack also become more and more diverse. In order to resist attackers' violation of user privacy, we must constantly update and improve the existing methods of defense. This section identifies three future research directions in the field of location privacy protection.

Table 3: Comparative analysis of location privacy protection policies

Techniques	Advantages	Disadvantages	Representative methods
Location privacy protection policy based on user attribute information [28]- [45]	Low overhead and simple implementation	Low user service availability	*K*-anonymous [28] Pseudonym [38]
Location privacy protection policy based on user behavior information [46]- [75]	High degree of privacy protection	High computational overhead	Mix-zone [69] Crowdsourcing policy [55]
Location privacy protection policy based on user relationship network [76]- [88]	Availability of serviceis is high and dataloss rate is low	Implementation is complex and expensive	Ring signature [82] Trust network model [87]

A. INTRODUCE BLOCKCHAIN TECHNOLOGY

The blockchain which born from Bitcoin and developed by Satoshi Nakamoto [89], has played a significant role in legal real estate medicine [90] and other fields. Therefore, we hope to introduce blockchain technology into the location privacy protection technology of SIoV. As illustrated in Fig. 8, the application of blockchain technologies to location privacy protection research in the SIoV context can compensate for the deficiencies of existing algorithms.

The most important feature of blockchain technology is decentralization: this means it does not rely on any third-party mechanism, and each node is equal. Applying this concept to research on SIoV location privacy protection can avoid over-reliance on trusted third parties, thus avoiding the problem of the single point of failure and reducing overhead to a certain extent.

Secondly, data stored in the blockchain cannot be tampered with. Storing a user personal information in the blockchain can thus prevent other malicious users or attackers from tampering with it. The data communicated between users can also be stored in the blockchain. Blockchain technology can protect the process of effective information exchange between both users and user relationship network structures.

In addition, blockchain also has the feature of transparency, meaning that the information communicated between the relevant users can be viewed by the users themselves, while other irrelevant users cannot view the data and relationships of exchange.

Blockchain technology is an emerging technology with great development potential. We want to apply it to the research on location privacy protection in the SIoV context can improve the degree of location privacy protection. In addition to storing user attribute information and communication processes, blockchain can also be treated as third party institutions to isolate the users from semi-trusted service providers. When attackers steal a single block, it will not affect the whole system and avoid a single point of failure. Blockchain not only reduces dependence on other third-party institutions, but also improves performance while also reducing overhead. Therefore, how to maximize the use of blockchain technology is an important direction of our future research.

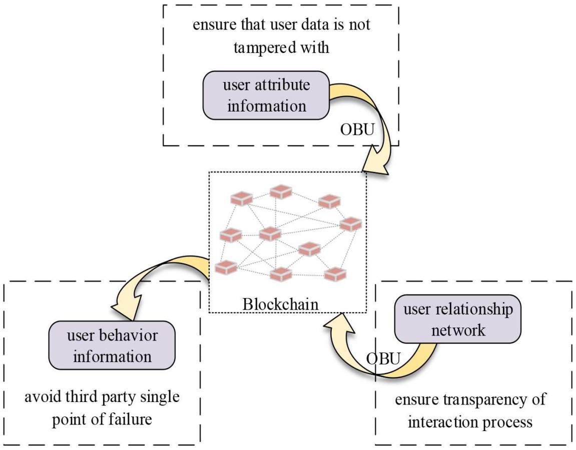
ensure that user data is not tampered with
user attribute information
OBU
Blockchain
user behavior information
avoid third party single point of failure
user relationship network
OBU
ensure transparency of interaction process

Fig. 8 Protection of location privacy of SIoV based on the blockchain

B. THE BALANCE BETWEEN THE LEVEL OF PRIVACY PROTECTION AND SERVICE REQUIREMENTS

As consumers of services, users should pay their private information to service providers or other users in order to obtain better service experience. As a matter of fact, this behavior that users provide their private information to data collectors in SIoV can be regarded as investing with expected benefits. This "profit" effect is to get a better service experience. The protection of the user location data will reduce the accuracy of the location data information paid by the user or extend the payment time. Therefore, the "profit" will also be affected by the investment behavior, the accuracy of the services will be reduced or the time cost will be increased.

Existing algorithms have striven to minimize the impact of factors (such as service precision and delay) on service availability on the basis of protecting user location privacy. However, the current privacy protection mechanism cannot well balance the interests between user privacy information and network services in SIoV.

Therefore, we will conduct and analysis from a game theory perspective in future research work, model the relationship between user private information and service needs in the SIoV context, and identify the equilibrium point of incentive cooperation between privacy protection behavior and expected benefits of users. It would be possible to improve the service quality of SIoV if the Nash equilibrium is obtained between the degree of user location privacy protection and service requirements.

C. WEIGHT ALLOCATION OF USER RELATIONSHIP NETWORK

Location privacy protection methods based on user relationship networks are targeted at friends who can interact and share information together. Users have direct or indirect relationships between other users on the road; moreover, untrusted users may leak relevant information about the target users, even if the friends are trusted. Nor can it be guaranteed that friends' information will not be stolen. Therefore, while protecting the user relationship network can reduce the risk of the user private location information being leaked, the existing location privacy protection algorithms based on user relationship network treat all users equally, meaning that their protection cannot calibrated according to the proximity of friends.

In the previous literature [91], we analyze user social behavior through adapting the posterior probability-based information entropy weight allocation method in order to identity users. In SIoV, such weighted methods are worth applying to the location privacy protection technology. Targeted protection based on the closeness and distance of users' friends would not only improve the protection of user private location data, but would also save on resources. We hope to weight the undirected graph of user relationship network according to the degree of intimacy between users could protect user location privacy through the undirected graph. In addition, the intimacy function that could be used to judge the degree of intimacy of the relationship between users is also the focus of our future research, and the matching algorithm could be used to unify the direct and indirect relationship between users, these methods solve the resource wastage caused by the different degrees of closeness of the between user relationships.

VI. CONCLUSION

Adopting the SIoV perspective, this paper summarizes the research status of user location privacy protection technology in the SIoV context in recent years. At present, user location privacy protection methods play an important role in SIoV systems, as they can improve the system and increase customers' viscosity. Firstly, the underlying concepts and location privacy of SIoV are expounded upon. In addition, the state of the current research is analyzed in detail from three perspectives, namely user attribute information, user behavior information and user relationship network, after which the performance is also evaluated with reference to these three aspects. Finally, the future research directions related to location privacy protection technology are discussed in combination with existing researches. The location privacy protection technology of the SIoV is the product of the era of big data, and there are still many key issues that need to be investigated.

REFERENCES

[1] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492-6499, 2019.

[2] L. Hua, M. H. Anisi, P. L. Yee, and M. Alam, "Social networking-based cooperation mechanisms in vehicular ad-hoc network-a survey," *Vehicular Communications*, 2017, pp. 57-73.

[3] A. Siddiqa, M. A. Shah, H. A. Khattak, A. Akhunzada, I. Ali, Z. Razak, and A. Gani, "Social Internet of Vehicles: complexity, adaptivity, issues and beyond," *IEEE Access*, 2018, pp. 62089-62106.

[4] S. An, B. H. Lee, and D. R. Shin, "A survey of intelligent transportation systems," *Computational Intelligence Communication Systems and Networks*, 2011, pp. 332-337.

[5] A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, and S. K. Das, "Vehicular Social Networks: a survey," *Pervasive and Mobile Computing*, 2018, pp. 96-113.

[6] L. Wang, and X. Meng, "Location privacy preservation in big data era: a survey," *Journal of Software*, 2014.

[7] V. Milanes, J. Villagra, J. Godoy, J. Simo, J. Perez, and E. Onieva, "An intelligent V2I-based traffic management system," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 49-58, 2012.

[8] L. Xing, Q. Ma, and L. Jiang, "Microblog user recommendation based on particle swarm optimization," *China Communications*, vol. 14, no. 5, pp. 134-144, 2017.

[9] L. Xing, Q. Ma, and S. Chen, "A novel personalized recommendation model based on location computing," *Chinese Automation Congress*, 2017, pp. 3355-3359.

[10] B. Liu, H. Xiong, S. Papadimitriou, Y. Fu, and Z. Yao, "A general geographical probabilistic factor model for point of interest recommendation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 5, pp. 1167-1179, 2015.

[11] G. Sun, L. Song, D. Liao, H. Yu, and V. Chang, "Towards privacy preservation for "check-in" services in location-based social networks," *Information Sciences*, 2019, pp. 616-634.

[12] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 3015-3045, 2017.

[13] B. Mi, X. Liang, and S. Zhang, "A survey on social Internet of Things," *Chinese Journal of Computers*, 2018.

[14] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. Yu, and B. Hu, "Privacy-preserving content dissemination for Vehicular Social Networks: challenges and solutions," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1314-1345, 2018.

[15] Y. Liu, Y. Shi, and H. Feng, "Intrusion detection scheme based on neural network in Vehicle Network." *J. Commun*, vol. 35, no. 2, pp. 232-239, 2014.

[16] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in Vehicular Network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760-776, 2018.

[17] R. G. Engoulou, M. Bellaieche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, no. 15, pp. 1-13, 2014.

[18] C. Caballerogil, J. Molinagil, J. Hernandezserrano, O. Leon, and M. Sorianoibanez, "Providing k-anonymity and revocation in ubiquitous VANETs," *Ad Hoc Networks*, 2016, pp. 482-494.

[19] S. Ferdous, F. Chowdhury, M. O. Alassafi, A. A. Alshdadi, and V. Chang, "Social Anchor: Privacy-friendly Attribute Aggregation from Social Networks," *IEEE Access*, 2020, pp. 1-1.

[20] X. Li, J. Niu, Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599-3609, 2018.

[21] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 5 , no. 3, pp. 1606-1615, 2018.

[22] D. A. Rivas, J. M. Barceloordinas, M. G. Zapata, and J. Morillopozo, "Security on VANETs: privacy, misbehaving nodes, false information and secure data aggregation," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942-1955, 2011.

[23] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 8-15, 2006.

[24] B. Hoh, and M. Gruteser, "Protecting location privacy through path confusion," *International Workshop on Security*, 2005, pp. 194-205.

[25] N. Haddadou, A. Rachedi, and Y. Ghamridoudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks,"

IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3657-3674, 2015.

[26] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, no. 2, pp. 107-118, 2017.

[27] A. K. Malhi, and S. Batra, "Fuzzy-based trust prediction for effective coordination in vehicular ad hoc networks," *International Journal of Communication Systems*, vol. 30, no. 6, 2017.

[28] S. Dietzel, J. Petit, F. Kargl, and B. Scheuermann, "In-network aggregation for vehicular ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1909-1932, 2014.

[29] L. Sweeney, "K-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557-570, 2002.

[30] D. Wu, L. Deng, H. Wang, K. Liu, and R. Wang, "Similarity aware safety multimedia data transmission mechanism for Internet of Vehicles," *Future Generation Computer Systems*, 2019, pp. 609-623.

[31] L. Nkenyereye, C. Liu, and J. Song, "Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles," *Future Generation Computer Systems*, 2019, pp. 488-499.

[32] D. Belli, S. Chessa, B. Kantarci, and L. Foschini, "Toward fog-based mobile crowdsensing systems: state of the art and opportunities," *IEEE Communications Magazine*, vol. 57, no. 12, pp. 78-83, 2019.

[33] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: a blockchain-based anonymous reputation system for trust management in VANETs," *Trust Security and Privacy in Computing and Communications*, 2018, pp. 98-103.

[34] Y. Mei, Y. Cui, and G. Jiang, "A privacy preserving communication scheme for VANETs," *Applied Mechanics and Materials*, 2014, pp. 5133-5138.

[35] A. R. Beresford, and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46-55, 2003.

[36] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," *Wireless Network Security*, 2013, pp. 107-112.

[37] G. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 9, pp. 2658-2667, 2016.

[38] H. Li, D. Liao, G. Sun, M. Zhang, D. Xu, and Z. Han, "Two-stage privacy-preserving mechanism for a crowdsensing-based VSN," *IEEE Access*, 2018, pp. 40682-40695.

[39] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: accumulative pseudonym exchanging for location privacy enhancement in Vehicular Social Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93-105, 2016.

[40] R. Lu, X. Li, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86-96, 2012.

[41] N. Guo, L. Ma, and T. Gao, "Independent mix zone for location privacy in Vehicular Networks," *IEEE Access*, 2018, pp. 16842-16850.

[42] B. Palanisamy, and L. Liu, "Attack-resilient mix-zones over road networks: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495-508, 2015.

[43] F. Xia, and L. Yawei, "Dynamic mix-zone scheme with joint-entropy based metric for privacy-perserving in IoV," *Journal on Communications*, 2018.

[44] Y. Zhang, P. Chen, and L. Hao, "Research on privacy protection with weak security network coding for mobile computing," *International Conference on Advanced Cloud and Big Data*, 2019, pp. 174-179.

[45] X. Wang, L. Bai, B. Mausler, and P. Singh, "A novel conditional anonymity scheme for vehicular communication networks," *International Journal of Communication Systems*, 2019.

[46] B. Liu, W. Zhou, T. Zhu, L. Gao, T. Luan, and H. Zhou, "Silence is golden: enhancing privacy of location-based services by content broadcasting and active caching in wireless Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9942-9953, 2016.

[47] L. Hu, Y. Qian, M. Chen, M. S. Hossain, and G. Muhammad, "Proactive cache-based location privacy preserving for Vehicle Networks," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 77-83, 2018.

[48] G. Li, Q. Zhang, J. Li, J. Wu, and P. Zhang, "Energy-efficient location privacy preserving in Vehicular Networks using social intimate fogs," *IEEE Access*, 2018, pp. 49801-49810.

[49] S. Liu, A. Liu, Z. Yan, and W. Feng, "Efficient LBS queries with mutual privacy preservation in IoV," *Vehicular Communications*, 2019, pp. 62-71.

[50] B. Ying, and A. Nayak, "Social location privacy protection method in Vehicular Social Networks," *International Conference on Communications*, 2017, pp. 1288-1292.

[51] M. Zhang, M. Yang, Q. Wu, R. Zheng, and J. Zhu, "Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs," *Future Generations Computer Systems Fgcs*, vol. 4, no. 81, pp. 505-513, 2018.

[52] B. Ying, and A. Nayak, "A distributed social-aware location protection method in un-trusted Vehicular Social Networks," *IEEE Transactions on Vehicular Technology*, 2019, pp. 1-1.

[53] H. To, G. Ghinita, and C. Shahabi, "A framework for protecting worker location privacy in spatial crowdsourcing," *Very Large Data Bases*, vol. 7, no. 10, pp. 919-930, 2014.

[54] Y. Qian, M. Chen, J. Chen, M. S. Hossain, and A. Alamri, "Secure enforcement in cognitive Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1242-1250, 2018.

[55] M. A. Azad, S. Bag, S. Parkinson, and F. Hao, "TrustVote: privacy-preserving node ranking in Vehicular Networks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5878-5891, 2019.

[56] Y. Yahiatene, and A. Rachedi, "Towards a blockchain and software-defined Vehicular Networks approaches to secure Vehicular Social Network," *IEEE Conference on Standards for Communications and Networking*, 2018, pp. 1-7.

[57] Y. Yahiatene, A. Rachedi, M. A. Riahla, D. E. Menacer, and F. Naitabdesselam, "A blockchain-based framework to secure Vehicular Social Networks," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 8, 2019.

[58] J. Ni, X. Lin, and X. Shen, "Privacy-preserving data forwarding in VANETs: a personal-social behavior based approach," *Global Communications Conference*, 2017, pp. 1-6.

[59] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628-3636, 2017.

[60] J. Dai, and K. Qiao, "A privacy preserving framework for worker's location in spatial crowdsourcing based on local differential privacy," *Future Internet*, vol. 10, no. 6, 2018.

[61] S. Vodopivec, J. Bester, and A. Kos, "A survey on clustering algorithms for vehicular ad-hoc networks," *International Conference On Telecommunications*, 2012, pp. 52-56.

[62] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, "MixZone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4565-4575, 2013.

[63] I. Basaran, and H. Bulut, "Performance comparison of non delay tolerant VANET routing protocols," *International Symposium on Computers and Communications*, 2016, pp. 238-243.

[64] G. Sun, S. Cai, H. Yu, S. Maharjan, V. Chang, X. Du, and M. Guizani, "Location Privacy Preservation for Mobile Users in Location-Based Services," *IEEE Access*, 2019, pp. 87425-87438.

[65] I. Memon, H. T. Mirza, Q. A. Arain, and H. Memon, "Multiple mix zones de-correlation trajectory privacy model for road network," *Telecommunication Systems*, vol. 70, no. 4, pp. 557-582, 2019.

[66] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, "Location and trajectory privacy preservation in 5G-Enabled vehicle social network services," *Journal of Network and Computer Applications*, pp. 108-118, 2018.

[67] Y. Zhang, F. Tian, B. Song, and X. Du, "Social vehicle swarms: a novel perspective on socially aware vehicular communication architecture," *IEEE Wireless Communications*, vol. 23, no. 4, pp. 82-89, 2016.

[68] J. Cui, J. Wen, S. Han, and H. Zhong, "Efficient privacy-preserving scheme for real-time location data in vehicular ad-hoc network," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3491-3498, 2018.

[69] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: a practical pseudonym changing scheme for location privacy in VANETs," *Vehicular Networking Conference*, 2009, pp. 1-8.

[70] C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368, 2008.

[71] C. Lee, and Y. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441-1449, 2013.

[72] C. Zhang, P. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks*, vol. 17, no. 8, pp. 1851-1865, 2011.

[73] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 127-139, 2012.

[74] Y. Yang, "Perceived k-value location privacy protection method based on LBS in augmented reality," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 25-32, 2015.

[75] M. Li, L. Zhu, Z. Zhang, X. Du, and M. Guizani, "PROS: a privacy-preserving route-sharing service via vehicular fog computing," *IEEE Access*, 2018, pp. 66188-66197.

[76] X. Feng, and L. Wang, "S2PD: a selective sharing scheme for privacy data in vehicular social networks," *IEEE Access*, 2018, pp. 55139-55148.

[77] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110-9121, 2019.

[78] L. Xing, K. Deng, H. Wu, P. Xie, H. Zhao, and F. Gao, "A survey of across social networks user identification," *IEEE Access*, 2019, pp. 137472-137488.

[79] M. Li, N. Cao, S. Yu, and W. Lou, "FindU: privacy-preserving personal profile matching in mobile social networks," *International Conference on Computer Communications*, 2011, pp. 2435-2443.

[80] Y. Xiao, and Y. Liu, "Bayestrust and vehiclerank: constructing an implicit Web of trust in VANET," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2850-2864, 2019.

[81] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *International Cryptology Conference*, 2004, pp. 41-55.

[82] F. Zhang, and K. Kim, "ID-based blind signature and ring signature from pairings," *International Conference on The Theory and Application of Cryptology and Information Security*, 2002, pp. 533-547.

[83] L. Delgrossi, and T. Zhang, "Vehicle safety communications: protocols, security, and privacy," *John Wiley and Sons*, vol. 103, pp. 44-51, 2012.

[84] H. Xiong, Z. Chen, and F. Li, "Efficient and multi-level privacy-preserving communication protocol for VANET," *Computers and Electrical Engineering*, vol. 38, no. 3, pp. 573-581, 2012.

[85] B. K. Chaurasia, and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," *IEEE Transactions on Computational Science*, 2011, pp. 147-156.

[86] Y. Mei, G. Jiang, W. Zhang, and Y. Cui, "A collaboratively hidden location privacy scheme for VANETs," *International Journal of Distributed Sensor Networks*, vol. 10, no. 3, 2014.

[87] Q. Yang, and H. Wang, "Toward trustworthy Vehicular Social Networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 42-47, 2015.

[88] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. P. C. Rodrigues, and Y. Park, "AKM-IoV: authenticated key management protocol in fog computing-based Internet of Vehicles deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8804-8817, 2019.

[89] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Manubot*, 2019.

[90] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," *Journal of Medical Systems*, vol. 42, no. 88, pp. 1-11, 2018.

[91] K. Deng, L. Xing, L. Zheng, H. Wu, P. Xie, and F. Gao, "A user identification algorithm based on user behavior analysis in social networks," *IEEE Access*, 2019, pp. 47114-47123.

XIAOFAN JIA received the B.S. degree in information engineering at Henan University of Science and Technology, China, in 2018. Now she is currently working towards her M.S. degree in information and communication engineering at Henan University of Science and Technology, China. Her research interests include data mining, Social Internet of Vehicle, location privacy protection.

LING XING received the B.S. degree in electronic engineering from Southwest University of Science and Technology, China, in 2002, the M.S. degree in electronic engineering from University of Science and Technology of China, in 2005 and the Ph.D. degree in communication and information system from Beijing Institute of Technology in 2008. In 2007, she worked at Illinois Institute of Technology as a visiting scholar, Chicago, USA.

She is a professor in School of Information Engineering, Henan University of Science and Technology, China. Her research interests include multimedia semantic mining, private preserving and social computing.

JIANPING GAO received the B.S. degree in vehicle engineering from Luoyang Institute of Technology, in 2000, the M.S. degree in mechanical engineering from Southwest Forestry University, in 2003 and the Ph.D. degree in vehicle engineering from Beijing Institute of Technology in 2009. In 2007, he worked at Michigan State University as a visiting scholar, Michigan, USA.

He is a professor in School of Vehicle and Traffic Engineering, Henan University of Science and Technology, China. His research interests are new energy vehicles and intelligent connected vehicles.

HONGHAI WU received his Ph.D. degree and M.S. degree from Beijing University of Posts and Telecommunications, China, in 2015 and 2007, respectively, and his B.S. degree from Zhengzhou University, China, in 2001. He worked at China United Telecommunications Co. Ltd during 2007-2011.

He is an associate professor in School of Information Engineering, Henan University of Science and Technology, Luoyang, China. His research interests include delay/disrupted tolerant networks, opportunistic networks. and video delivery.