IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 14, 2021, accepted March 28, 2021, date of publication April 6, 2021, date of current version April 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3071407

Semantic and Trade-Off Aware Location Privacy Protection in Road Networks via Improved Multi-Objective Particle Swarm Optimization

CENXI TIAN, HONGYUN XU, TAO LU, (Member, IEEE), RUI JIANG, AND YONG KUANG
School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China

Corresponding author: Hongyun Xu (hongyun@scut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61272403 and in part by the National Natural Funds for Major Scientific Instruments and Equipment Development under Grant 41627803.

ABSTRACT Location privacy protection is an essential but challenging topic in the field of network security. Although the existing research methods, such as k-anonymity, mix zone, and differential privacy, show significant success, they usually neglect the location semantic and the proper trade-off between privacy and utility, which may allow attackers to obtain user privacy information by revealing the semantic correlation between the anonymous region and user's real location, thus causing privacy leakage. To solve this problem, we propose a location privacy protection scheme based on the k-anonymity technique, which provides practical location privacy-preserving through generating an anonymous set. This paper proposes a new location privacy attack strategy termed semantic relativity attack (SRA), which considers the location semantic problem. Correspondingly, a semantic and trade-off aware location privacy protection mechanism (STA-LPPM) is presented to achieve privacy protection with both high-level privacy and utility. To be specific, we model the location privacy protection as a multi-objective optimization problem and propose the Improved Multi-Objective Particle Swarm Optimization (IMOPSO) to generate the optimal anonymous set calculating the well-design fitness functions of the multi-objective optimization problem. In this way, the privacy scheme can provide mobile users with the right balance of privacy protection and service quality. Experiments reveal that our privacy scheme can effectively resist the semantic relativity attack while preventing significant utility degrading.

INDEX TERMS K-anonymity, location privacy, location semantic, multi-objective optimization problem, particle swarm optimization algorithm, road networks.

I. INTRODUCTION

In recent years, location-based service has become a crucial part of our daily activities. With the rise of mobile technologies, people can enjoy various location-based services using high-precision positioning devices, including searching for the nearest hotel, restaurant, hospital. Despite the benefits of Location-Based Services (LBS), it may also yield a high risk of privacy leakage when users send their position information to the server, leading to severe security issues. Many related works propose Location Privacy Protection Mechanisms (LPPMs) to protect users' position information from being leaked to the attackers to tackle the above problem. Most of these mechanisms are formulated based on k-anonymity [1], which is practically applied against re-identification attacks by generating an anonymous group. When using k-anonymity to enhance the user location privacy [2]–[6], the improved algorithms usually consist of k-anonymity and some other optimization aspects. In this way, the anonymous process is implemented more effectively, e.g., [2] utilizes the Markov model to predict query location first before selecting anonymous cells, which reduces the interaction between users and location service provider (LSP) and improves user privacy. Besides, to provide mobile users with more effective privacy protection, many related works also focus on achieving the right trade-off between privacy and utility [7]–[12]. Such mechanisms generally apply the Weighted Sum Method (WSM) to balance the privacy and utility, i.e., the trade-off between privacy and utility can be achieved through parameter adjusting.

Notwithstanding the demonstrated success, the above methods rarely consider the location semantic, making them

The associate editor coordinating the review of this manuscript and approving it for publication was Yan Huo.

quite vulnerable to semantic-related attacks. The attackers can infer users' positions with high confidence by considering prior knowledge of the road network's location semantics. Therefore, involving the location semantics in the location privacy protection scheme's design is essential for enhancing the method's privacy protection capability to resist semantic-related attacks. Besides, how to achieve a good balance of privacy protection and service utility is also an unresolved problem. The existing methods usually make a trade-off between privacy and service utility by adopting a weighted sum strategy. However, the general optimization of privacy or utility will inevitably compromise the other, making it difficult to reach an optimal trade-off between privacy and utility.

On the other hand, the weighted sum strategy requires the users to adjust proper privacy parameters by assigning different weights to a privacy scheme and a utility scheme. It is unpractical when the server receives massive user requests quickly since different users may have different privacy and utility requirements. It is difficult for users to choose the optimal parameters that can best match their privacy utility requirements under various circumstances. Thus, it is necessary to automatically obtain the optimal trade-off between the privacy and the utility for each user instead of the cumbersome manual setting of weights.

Based on the above observation, we aim to fill the gap in semantic-relativity location privacy protection and achieve an automatic optimal trade-off between the privacy and the utility of the location privacy protection method. To this end, we first propose a new attack called semantic-relativity attack (SRA), with which an attacker can infer the user's position by considering prior knowledge of location semantics of the road network. Correspondingly, an improved semantic and trade-off aware location privacy protection mechanism (STA-LPPM) is designed to simultaneously resist semantic-relativity attacks while achieving an optimal trade-off between privacy and utility. In particular, to reach a good balance of privacy and utility, we model the privacy protection scheme as a multi-objective optimization problem, and Particle Swarm Optimization (PSO) is adopted to solve the optimization problem. We model searching for anonymous edges as a Multiple Traveling Salesman Problem (MTSP) to adapt the vanilla Particle Swarm Optimization to the road network scenario. Firstly, Breadth-First Search (BFS) is adopted to generate the candidate edge sets with predefined sizes. Then, the candidate edge sets are numbered in sequence to constitute the particle space. Finally, Particle Swarm Optimization is used with the candidate edge sets to produce the final anonymous edge set. To reach a good balance of privacy and utility, we propose two types of fitness functions (i.e., privacy metrics and utility metrics) to enable PSO to find the optimal trade-off solution. The main contributions of this paper can be summarized as follows:

1. We propose a semantic and trade-off aware location privacy protection mechanism, which can resist the semantic-relativity attack while maintaining a good balance of privacy and utility. To the best of our knowledge, this is the first work taking both semantic relativity and adaptive trade-off problems into consideration in road networks for location privacy protection.

2. We propose a new attack called semantic-relativity attack (SRA), with which an attacker can infer the user's position by considering prior knowledge of location semantics of the road network.

3. To find the optimal solution with a balanced trade-off between privacy and utility, we adapt multi-objective Particle Swarm Optimization to the road network scenario for generating the final anonymous edge set. Besides, we also design two novel fitness functions for dual-objective optimization.

4. Experimental results on real-world data show that the final anonymous edge set generated by our method can effectively resist the semantic relativity attack and achieve good utility at the same time.

The rest of this paper is organized as below. Section II expounds on the recent research on location privacy. In Section III, we illustrate the system architecture of the proposed privacy scheme STA-LPPM, and the related definitions and description of semantic relativity attack are also involved. Additionally, we elaborate the concrete implementation of STA-LPPM in detail in Section IV, followed by the demonstration of the Improved Multi-Objective Particle Swarm Optimization (IMOPSO) algorithm in Section V. In Section VI, the experiment results and comparisons with the other two anonymous algorithms are fully interpreted, and our conclusion and future plan will be further described in Section VII.

II. RELATED WORK

Location privacy protection is a trending topic in network security, attracting much attention [13]–[19]. Among which, Privacy attack and LPPM are two crucial issues in location privacy protection of road networks.

Prior research works studying privacy attacks on location privacy suggest that most adversaries obtain user information from having access to any entities in the LBS system. For instance, under the premise that the attacker can directly obtain distance information of users from the LBS server, Argyros *et al.* [20] present the user discovery attacks in location proximity services, which can effectively infer user information by bounding the user within a specific area. Relevantly, works in [21] show that the malicious friends in location proximity services can narrow down the search space with users' background information. Also, to protect user privacy information from being inferred by learning user mobility, specifically for the real-world road network scenario, many research works have been carried out. For example, Montjoye *et al.* [22] put forward that an attacker can reproduce user identity information depending on a small quantity of user location information. Worse still, the location trajectories can be de-anonymized even with sufficient privacy protection, including the noise-fuzzy technology or the anonymity technology [23]–[25]. Specifically, in the

presence of prior knowledge of user mobility, an optimal inference attack is available [26], e.g., generating the Markov transition matrix of each user. Based on the prior knowledge of user mobility and the geographical distribution of user locations, Bayesian inference can be characterized with a hidden Markov process [25]. However, most of these attack models neglect the semantic relativity for the real scenario, which is likely to be exploited for inferring the user's real location by attackers. For this reason, semantic relativity between the anonymous road edge and user's real location is revealed, leading to user privacy leakage.

Various LPPMs have been implemented for different LBS systems [27]–[37]. For instance, Argyros *et al.* [20] leverage spatial cloaking to maintain a level of privacy in proximity services. Using the resembling cloaking strategy, the proposed spatial and temporal transformations in [31] enforce privacy by hiding mutual proximity. Concerning other realistic scenarios with sparse data and missing location problems, *Murakami* uses multiple learning methods to resist location privacy attacks based on a Markov chain model [23]. Besides, some LPPMs improve location privacy protection via considering locations semantic. Earlier work in [38] achieves anonymous protection comparing the multiplication of semantic similarities and Euclidean distance with the real location on user devices, leading to the extra overhead of running the privacy algorithm. To realize the personalized location privacy protection based on location semantics, Kuang *et al.* [39] propose a personalized sensitivity weight assignment algorithm to allow users to divide multiple location semantics by themselves, ignoring the semantic relationship between them multiple location semantics. In this way, the malicious attacker may infer user privacy information by revealing the semantic relationship between the cloaking region and user's actual location. The above two methods generally ignore the fine-grained classification of location semantics, leading to the inaccurate evaluation of semantic relativity., thus the privacy methods cannot prevent attackers from inferring user privacy information via revealing the semantic relativity of the anonymous edge set and the real location.

The general LPPMs usually solve privacy problems without retaining data utility. Thus coordinating privacy with utility remains one of the heated issues for location privacy protection [40]. Several works have been developed to tackle this problem for obtaining the proper trade-off between privacy and utility. Both [7] and [40] engage in relevant research of dynamically tweaking the related parameters of LPPM, which turned out to be not appropriate for a complex real-world scenario. Kuang *et al.* [41] propose the Location Privacy Requirements, and represented it with a triplet <K, L, H>, where H denotes the privacy coefficient, the smaller it is, the narrower the scope of the candidate grid area will be, resulting in the enhancement of the utility and the decline of privacy, unfortunately, due to its tendentious implementing way, the trade-off problem is still unresolved. Combining k-anonymity and clustering techniques, Wu *et al.* [12] propose the anonymizer coordination strategy to ensures that the anonymizers always provide strong privacy protection and good service for the recommendation service. To further provide personalized privacy service, Casper's novel privacy framework in [8] is divided into two parts: the location anonymizer and the privacy-aware query processor; the former generates the cloaking regions to protect exact user location, the other is designed to deal with anonymous queries. Also, these techniques generally implement trade-offs through adjusting the weighting parameter customized by mobile users. Since most mobile users learn less about background knowledge of location privacy, optimization results can be far from meeting users' anticipated needs. Unlike these techniques, we simultaneously optimize the privacy and utility, i.e., we use IMOPSO to designate the final anonymous edge set with the optimal fitness value obtained by calculating multiple fitness functions containing privacy metrics and utility metrics.

Previously, PSO is commonly used for searching optimal solutions for general functions, owing to its fast convergence rate and operability. Also, it is widely applied to improve privacy-preserving method efficiency [21], [42], [43]. For example, in [43], a PSO anonymization is utilized for accelerating the process of finding similar attributes, and the anonymous users are chosen with similar attributes. Relevantly, [21] realizes the privacy protection via the multi-objective optimization algorithm, i.e., it uses the hybrid elite selection strategy to process user privacy information. However, location privacy protection for the real-world road network scenario is a complicated problem equipped with semantic attributes. The general PSO-based privacy schemes fail to protect location privacy adequately. This paper defines privacy metrics and utility metrics based on the real-world road network dataset. Our privacy scheme thus has more practical significance in improving privacy protection and retaining decent utility.

III. PRELIMINARIES

In this section, we first demonstrate the system architecture of STA-LPPM and the privacy-preserving process, after which we introduce some related definitions and the semantic relativity attack in detail.

A. SYSTEM ARCHITECTURE

The privacy protection system's main framework involving STA-LPPM consists of three parts: the mobile user, the anonymous server, and the LBS server, as shown in Fig. 1. The detailed process of implementing the privacy protection system is described below. Firstly, the trusted third-party anonymous server preloads the original version of a road network, while mobile users send their privacy information (i.e., real locations, query requests) to the LBS server via various mobile devices. The trusted third party then generates an anonymous edge set by running IMOPSO iteratively, then sends it to the LBS server for further user query processing. Finally, the LBS server processes the user query requests and returns the query results to the third-party anonymous

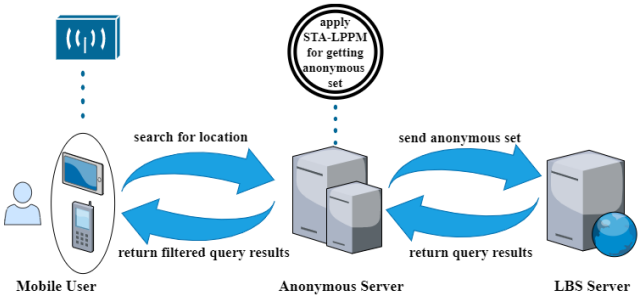


FIGURE 1. The framework of the privacy protection system.

server, in which these results are first filtered and then offered to the mobile users. In this paper, we define the location semantic as a one-to-one matching between each location and each semantic type, and the location semantic road network is described as $G = (V, E, L)$, where $V = \{V_1, \cdots, V_n\}$ represents the set of all road intersections in the road network, where n denotes the total number of road intersections. $E = \{e_1, \cdots, e_p\}$ represents the set of all road edges in the road network, with each road edge containing different location semantics, where p denotes the total number of road edges. Significantly, Mobile users can customize the sensitive location semantics $L = \{l_1, \cdots, l_b\}$ according to different privacy requirements, where b denotes the total number of types of sensitive location semantics, and each location semantic corresponds to a particular value of semantic sensitivity.

Meanwhile, we define the set of location popularity $pop = \{pop_1, \cdots, pop_b\}$, each element representing the value of location popularity of multiple location semantics preset by the privacy protection system. Furthermore, $sen = \{sen_1, \cdots, sen_b\}$ is defined to represent semantic sensitivity values, with each element ranging from 0 to 1, according to the users' privacy requirements. The semantic sensitivity can be used for evaluating the relativity between user privacy and location semantic, i.e., a bigger value of the semantic sensitivity indicates a stronger privacy demand of the user. The location popularity demonstrates the intrinsic privacy attributes of location semantics in a road network. For instance, the value of a hospital's location popularity is naturally higher than that of a park.

B. RELATED DEFINITION

Definition 1 (Semantic Sensitivity): Semantic sensitivity means the sensitivity values of different types of location semantics preset by mobile users, which can be formulated as $W = \{w_i \,|\, 1 \le i \le b, 0 \le w_i \le 1\}$, where b denotes the total number of types of the location semantics and w_i denotes the sensitivity value of the i-th location semantics. The higher the value of semantic sensitivity is set, the stronger the correlation between the location semantic and the user privacy information is, e.g., the patients assign a higher value to the hospital.

Definition 2 (Semantic Attribute Set): A semantic attribute set consists of all the semantic attributes of a location. For instance, a hospital's semantic attribute set can be described as $sem_{hospital} = \{service, health, patient\}$, where $service, health, patient$ represent three different semantic attributes.

Definition 3 (Semantic Relativity): Semantic relativity refers to the relationship between two different location semantics. We assume the school's semantic attribute set as: $sem_{school} = \{service, education, student\}$, and the semantic relativity between a school and a hospital can be described as: $\frac{1}{sem_{dist}+1}$, where sem_{dist} denotes the relative semantic distance between two different location semantics. sem_{dist} can be calculated as,

$$sem_{dist} = \frac{\left[sem_{type1} \cup sem_{type2}\right] - \left[sem_{type1} \cap sem_{type2}\right]}{\left[sem_{type1} \cup sem_{type2}\right]}, \tag{1}$$

where sem_{type1}, sem_{type2} indicate two different location semantics. The higher the value of sem_{dist}, the stronger the semantic relationship between two types of location semantics.

The notions used in this paper are described in Table 1.

TABLE 1. Notion list.

Name	Description
G	Semantic Road Network Model
V	The Set of the Points of Road Networks
E	The Set of the Edges of Road Networks
L	The Set of the Location Types of Road Networks
pop	The Set of Semantic Popularity Value
W	The Set of Customized Semantic Sensitivity Value
$sem_{location\_type}$	The Set of Semantic Attribute
sem_{rel}	Semantic Relativity
sem_{dist}	Semantic Relative Distance
$candidate_u$	The Set of Candidate Anonymity Edges
$REQUEST$	The Set of User Query
V_{i+1}	Updated Velocity of each particle
X_{i+1}	Updated Location of each particle
ω	Inertia Weight of PSO
c_1, c_2	Acceleration Constants of PSO
k	The K Value of K-Anonymity
X^{i+1}_{Break}	Updated breaking point of advanced PSO
X^{i+1}_{Route}	Updated Permutation of Anonymous Edges
$fit\_expression$	Fitness Function
sum_{dist}	The Sum of Semantic Relative Distance

C. SEMANTIC RELATIVITY ATTACK

By computing the value of semantic relativity between the anonymous edges and the user's edge, an attacker with intense background knowledge, including the map of the

location semantic road network, the distribution of location semantics, and the calculation of the semantic relativity value, can figure out the real user location, which is defined as a localization attack [25]. For a particular user query request, the attacker first acquires the user query information and anonymous edge set via the LBS server and then generates a new anonymous edge set $attack_{anony}$, with at least k anonymous edges, by computing the value of semantic relativity among the candidate anonymous edges, this allows the attacker to infer the user's real location efficiently.

Formally, we assume the user's edge as e_{user} containing multiple sensitive location semantics, which is described as $L_{user} = \{l_1, \cdots, l_m\}$, where m denotes the total number of types of sensitive location semantics of e_{user}. Multiple location semantics are randomly distributed on each anonymous edge of the user's anonymous edge set $S_{anony} = \{e_1, \cdots, e_k\}$, where e_1 is defined as $e_1 = \{l_a, l_b, \cdots, l_f\}$ and f denotes the total number of sensitive location semantics of e_1. According to *definition 3*, we can easily get the semantic relativity between e_{user} and any anonymous edge, i.e., the bigger the sum of the semantic relative distance of S_{anony}, the lower the degree of semantic relevance between S_{anony} and e_{user}, thus the similarity between $attack_{anony}$ and S_{anony} becomes lower, and the probability of success for semantic relativity attack is reduced. In this way, The attacker fails to find out the user's actual location, and we can then significantly improve the level of location privacy-preserving.

IV. SEMANTIC AND TRADE-OFF AWARE LOCATION PRIVACY PROTECTION

This paper proposes the Semantic and Trade-off Aware Location Privacy Protection (STA-LPPM) based on the semantic relativity attack and implementing trade-off adaptively.

This paper roughly separates the executing process of STA-LPPM into two steps: (1) We adopt BFS to search for adjacent road edges on the road network and generate a candidate anonymous edge set, depending on user information, such as the real user location. (2) We introduce Improved Multi-Objective Particle Swarm Optimization (IMOPSO) for optimizing the anonymous edge set searching in location semantic road network, and run that algorithm on the candidate anonymous edge set iteratively until the threshold value of iterations is met, after which the final anonymous edge set is designated by calculating the fitness function. The privacy metrics are being optimized constantly. In this way, we can realize the location privacy location by generating the final anonymous edge set. As shown in Fig. 2 (a), the real-world road network appears to be transformed into the location semantic road network in STA-LPPM, i.e., STA-LPPM is constructed in a real-world scenario. As demonstrated in Fig. 2, the user's sensitive location semantics are categorized into six types: the bank, community, hotel, hospital, shopping mall, and school, and all the deep orange lines in Fig. 2 (b) denote the selected candidate anonymous edges. To demonstrate the output of IMOPSO intuitively, we illustrate the final filtered anonymous edge set in Fig. 2 (c) as four areas rounded by azure dotted lines.

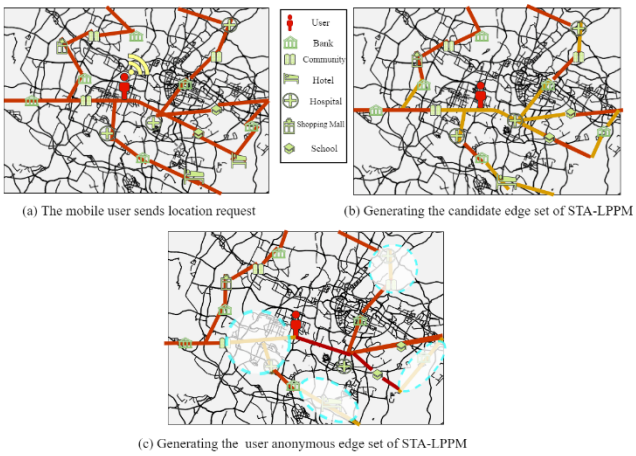


FIGURE 2. The executing process of STA-LPPM.

The flow chart of STA-LPPM is as shown in Fig. 3.

V. PSO ANONYMIZATION

A. A BRIEF INTRODUCTION OF PSO

The particle swarm optimization (PSO) is first proposed to optimize nonlinear problems [44] and is frequently applied to solve optimization model problems in different science engineering domains due to its quick convergence speed. Considering that the vanilla PSO algorithm cannot deal with the labeled location semantic information, non-serial location semantic cannot be directly used to model a particle space. Hence, the vanilla PSO algorithm is not the applicable privacy protection optimization method for the real-world road network scenario. To cope with the above problem, we propose the Improved Multi-Objective Particle Swarm Optimization (IMOPSO). The vanilla PSO algorithm usually initializes a group of particles in a feasible solution space, where each particle represents a potential optimal solution and is characterized by location, velocity, and the value of fitness. By running the PSO algorithm iteratively, an optimal solution can be obtained from the random solutions by evaluating the preset fitness functions. The updated location of a particle depends on its updated velocity and the current location. The calculations of the updated velocity and location are respectively shown as,

$$V_{i+1} = \omega \times V_i + c_1 \times r_1 \times (pbest - X_i) + c_2 \times r_2 \times (gbest - X_i), \quad (2)$$

$$X_{i+1} = X_i + V_{i+1}, \quad (3)$$

where V_{i+1} and V_i denote the updated velocity of a particle, the current velocity of a particle, respectively. Similarly, X_{i+1} and X_i stand for the updated location of a particle, the current particle location, respectively. Besides, ω, $pbest$, and $gbest$ represent the inertia parameter, the local optimum and the global optimum, respectively. Here, the local optimum and

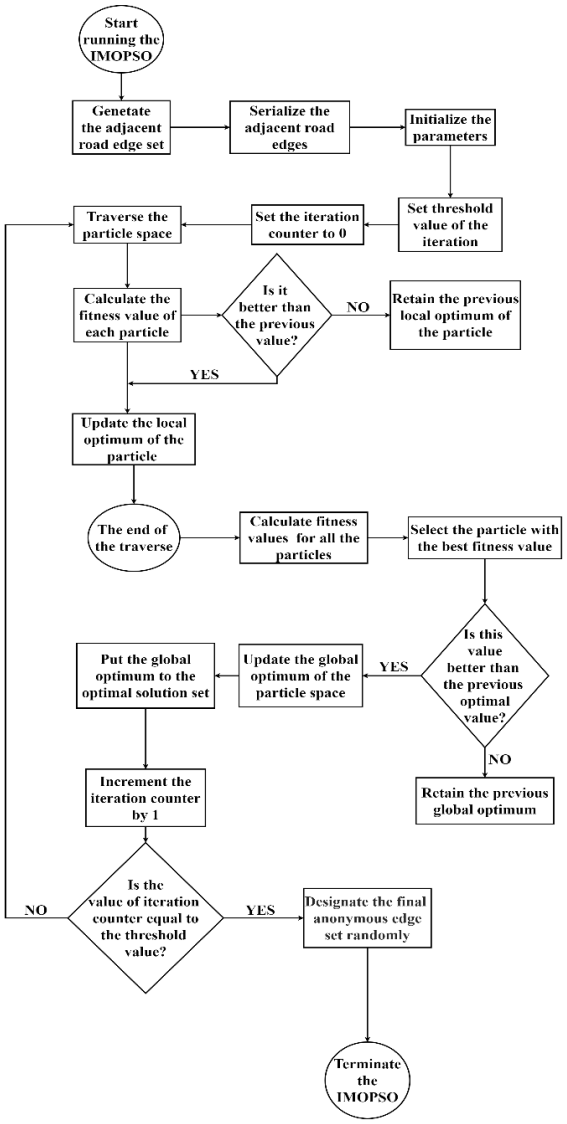


FIGURE 3. The flow chart of STA-LPPM.

the global optimum represent the best solution an individual particle has ever gone through, the best solution a particle swarm has ever met, respectively. c_1 and c_2 denote the acceleration constants, while r_1 and r_2 both stand for the random parameters ranging from 0 to 1. The flow property of the PSO algorithm's information-sharing mechanism is unidirectional, which results in the transformation of the particle swarm being influenced by both the local optimum and the global optimum. Thus, the PSO algorithm is characterized by rapid convergence.

B. PRIVACY PROTECTION ALGORITHM BASED ON PSO

Although PSO has been verified to improve the efficiency of the privacy-preserving method in recent studies, most of them fail to combine privacy protection enhancement and decent utility, leading to the unexpected loss of utility while implementing the PSO-based privacy policies. To solve this problem, we aim to introduce an improved PSO anonymization method termed IMOPSO, which calculates the fitness values of both privacy metrics and utility metrics synchronously during the optimization procedure. The objective function of IMOPSO is formulated as (4) below,

$$\begin{aligned} &optimize\ F\ (privacy, utility) \\ &\quad = [privacy\ (m_1, m_2)\ , utility\ (m_3, m_4)]^T \\ &s.t.\ optimize\ privacy\ (m_1, m_2)\ , \\ &\quad optimize\ utility\ (m_3, m_4)\ , \qquad (4) \\ &\quad optimize\ privacy\ (sem_{dist}, PRM)\ , \qquad (5) \\ &\quad optimize\ utility\ \left(sum_{\Delta e}, avg_{time\_cost}\right), \qquad (6) \end{aligned}$$

where m_1 and m_2 denote the two different privacy metrics, m_3 and m_4 denote the two different utility metrics. Equations (5) and (6) are the expanding descriptions of the objective function for privacy, the expanding descriptions of the objective function for utility, respectively. The calculations of the above metrics are elaborated in the following content.

In IMOPSO, all the candidate road edges are first numbered in sequence to carry out a brute force method, which is used to demonstrate every possible permutation of these edges. To achieve multiple anonymous edge sets that satisfy anonymity requirements, we adopt the particle breakpoint position [45] to represent various permutations of the candidate anonymous edges. For example, with the particle breakpoint set $S_{breakpoint}$ {3, 7, 11, 15}, we can separate the particle S {1, 2, $\cdots$, 15} into four non-overlapped subsets, i.e., S_1 {1, 2, 3}, S_2 {4, 5, 6, 7}, S_3 {8, 9, 10, 11}, S_4 {12, 13, 14, 15}. In this paper, the permutation of the candidate anonymous edges X^i_{Route}, is updated by itself and the permutation of particle breakpoint positions X^{i+1}_{Break}, both X^i_{Route} and X^{i+1}_{Break} are in the representation of serialization, in this way, the search for the best solution of the anonymous set in the particle space also works in the real road network scenario. Furthermore, to achieve the best trade-off between privacy protection and utility, we also propose two novel fitness functions by introducing several well-designed privacy and utility metrics.

The IMOPSO can be formulated as,

$$\begin{aligned} X^{i+1}_{Break} &= \omega \times X^i_{Break} \cdot \left[c_1 \times r_1 \times \left(pbest \otimes X^i_{Route}\right)\right] \\ &\quad \cdot \left[c_2 \times r_2 \times \left(gbest \otimes X^i_{Route}\right)\right], \qquad (7) \\ X^{i+1}_{Route} &= X^i_{Route} \oplus X^{i+1}_{Break}, \qquad (8) \end{aligned}$$

where X^i_{Route} and X^i_{Break} denote the permutation of the candidate anonymous edges of a particle after the i-th iteration, the permutation of a particle's particle breakpoint positions after the i-th iteration, respectively. Similarly, X^{i+1}_{Route} and X^{i+1}_{Break} represent the updated permutation of the candidate anonymous edges of a particle, the updated permutation of a particle's particle breakpoint positions, respectively. *pbest* denotes the current local optimal permutation of anonymous edges, while *gbest* represents the current global optimal permutation of anonymous edges. Remarkably, the parameters

with the same names (i.e., ω, c_1, r_1, c_2, r_2) are identical to those included in (2).

The operations are defined as follows:

$\otimes$: The calculation of A $\otimes$ B aims to get the better solution with the best fitness value between A and B, and both A and B denote the sequence sets with the same quantity of elements.

$\cdot$: $A \cdot B$ can be acquired by: $A \cdot B = A + \frac{B-A}{2}$. Both A and B denote the sequence sets, and the result is composed of all the intermediate values between A and B.

$\oplus$: The calculation can be performed by rearranging the permutation of the candidate anonymous edges of the sequence set A, according to the permutation of the particle breakpoint positions of sequence set B. A new sequence set is then generated as the result of the calculation.

The running process of IMOPSO can be summarized as follows:

Step 1. Initialize an n-dimension particle space as the original particle swarm. Specifically, X^1_{Route} it is assigned as an original permutation of the candidate anonymous edges for each particle, whereas.is assigned as the original permutation of particle breakpoint positions to satisfy anonymity requirements.

Step 2. Initialize *pbest* for individual particles of the original particle swarm as X^1_{Break} Then initialize *gbest* with the best fitness value calculated by the predefined fitness functions in the original particle swarm.

Step 3. Set the threshold value of iterations, and then start to run the algorithm iteratively.

Step 4. X^i_{Route} of each particle and X^i_{Break} are iteratively updated using (7) and (8), respectively. Both *pbest* and *gbest* are iteratively updated accordingly.

Step 5. After each iteration, IMOPSO increments the iteration counter by 1, and the updated *gbest* is added to the optimal solution set. If the number of iterations exceeds a certain threshold value, the operation turns to step 6. Otherwise, it turns to step 4.

Step 6. Randomly select an element from the optimal solution set as the final global solution, from which the final anonymous edge set is randomly selected.

C. PRIVACY METRIC

To thoroughly analyze the resilience of our proposed privacy scheme, we introduce two privacy metrics based on the semantic relativity attack defined in Section III Part C, one of which is the sum of semantic relative distances denoted by sum_{dist}, for summing up the values of the semantic distances between pairs of anonymous edges in the final anonymous edge set. According to *definition 3*, the higher the sum of sem_{dist} is, the less the final anonymous edge set and user's real location are semantically related. Thus the attacker may fail to infer user privacy information via semantic relativity attack. The other privacy metric is the semantic privacy denoted by PRM_{CR} (which also appears as PRM) applied to measure the degree of semantic privacy of an anonymous edge set, where the index *CR* stands for an anonymous edge set. PRM_{CR} can be calculated as,

$$PRM_{CR} = \frac{POP_{CR}}{SEN_{CR}}, \tag{9}$$

where POP_{CR} and SEN_{CR} denote the accumulated value of location popularity of the sensitive location semantics in the final anonymous edge set, the accumulated value of semantic sensitivity of the sensitive location semantics in the final

Algorithm 1 Improved Multi-Objective Particle Swarm Optimization

Input: (1) The map of location semantic road network Map_{sem};
(2) the set of candidate anonymous edges S_{candi};
(3) the Maximum Number Of Iterations $It_{\max}$;
(4) the size of S_{candi}, $size_{candi}$.

Output: the final anonymous edge set S_{anony}

1. **Encode** each edge of S_{candi} in sequence
2. **Generate** the matrix M_{par}
3. the set of the rows of M_{par}, which is denoted as X_{Route}, **represents** different permutation ways of the edges of S_{candi}
4. **Generate** X_{Route} as the set of various ways for separating X_{Route} into several subsets
5. **Initialize** *pbest* as $\left\{\left\{X^1_{Route}, X^1_{Break}\right\}, \cdots, \left\{X^{size_{candi}}_{Route}, X^{size_{candi}}_{Break}\right\}\right\}$ with original values
6. **Initialize** *gbest* $\left\{X^{best}_{Route}, X^{best}_{Break}\right\}$ with original values
7. $S_{anony} = \{\}$, $S_{gbest} = \{\}$
8. **for** $i < It_{\max}$
9. **for** each particle $\left[X^j_{Route}, X^j_{Break}\right]$ **in** M_{par}
10. **Calculate**

$$X^{i+1}_{Break} = \omega \times X^i_{Break} \cdot \left[c_1 \times r_1 \times \left(pbest \otimes X^i_{Route}\right)\right] \cdot \left[c_2 \times r_2 \times \left(gbest \otimes X^i_{Route}\right)\right]$$

$$X^{i+1}_{Route} = X^i_{Route} \oplus X^{i+1}_{Break}$$

11. **if** $fit\_best_{j+1}\left\{X^{j+1}_{Route}, X^{j+1}_{Break}\right\}$ *is sup erior to* $fit\_best_j\left\{X^j_{Route}, X^j_{Break}\right\}$
12. then $pbest_j\left\{X^j_{Route}, X^j_{Break}\right\} \leftarrow pbest_{j+1}\left\{X^{j+1}_{Route}, X^{j+1}_{Break}\right\}$
13. **if** $fit\_pbest_{j+1}\left\{X^j_{Route}, X^j_{Break}\right\}$ *is superior to* $fit\_gbest_j\left\{X^{best}_{Route}, X^{best}_{Break}\right\}$
14. **then** $gbest_j\left\{X^{best}_{Route}, X^{best}_{Break}\right\} \leftarrow pbest_j\left\{X^j_{Route}, X^j_{Break}\right\}$
15. $S_{gbest} \leftarrow gbest$, $i = i + 1$
16. **Randomly pick** one set out of the S_{gbest} as S_{best}
17. **Randomly pick** one subset of S_{best} as S_{anony}
18. **Return** S_{anony}

anonymous edge set, respectively. According to (9), the bigger the PRM_{CR}, the less the leakage of the privacy information of mobile users, in this way, a higher level of semantic privacy of an anonymous edge set can be obtained for achieving location privacy protection.

D. UTILITY METRIC

According to practical experience, the LBS server of a centralized system is supposed to process user query requests, including the final anonymous edge set and other public information, and return the query results to mobile users. In this process, the query efficiency is strongly related to the utility. In this paper, we propose the sum of edge distance difference denoted as $sum_{\Delta e}$ to evaluate the utility. $sum_{\Delta e}$ can be computed as,

$$sum_{\Delta e} = \sum_{i}^{n} \left(e_{anony} - e_{user}\right), \tag{10}$$

where e_{anony} denotes an anonymous edge and e_{user} denotes the road edge where the user locates. The edge distance is calculated by counting the steps between pairs of edges. Based on the query process mentioned earlier, the more e_{anony} is relatively close to e_{user}, in other words, the smaller the edge distance between e_{anony} and e_{user} is, the less the LBS server may pay for searching on the road network. Thus, the LBS server can provide mobile users with quick query feedback, and the utility is accordingly improved. Furthermore, we also introduce the average time as the other utility metric, which is denoted as avg_{time_cost} and can be calculated as below,

$$avg_{time\_cost} = \frac{sum_{time}}{sum_{count}}, \tag{11}$$

where sum_{time} and sum_{count} denote the total time consumption of running the algorithm iteratively, algorithm's iterations, respectively. The more the average time, the less the processing ability of location privacy protection scheme, i.e., the privacy system needs to spend much time to provide location privacy protection, leading to the degradation of the level of utility.

E. SECURITY ANALYSIS

In this paper, we propose a privacy scheme STA-LPPM for achieving location privacy protection via the Improved Multi-Objective Particle Swarm Optimization (IMOPSO), which ensures security for three main steps as below.

In the process of constructing the final anonymous edge set, IMOPSO uses serialization to generate multiple candidate anonymous subsets, each of which meets the privacy requirement for k-anonymity containing at least k anonymous edges. Under adequate anonymous protection, IMOPSO can prevent malicious attackers from inferring user privacy information by revealing the semantic relativity between anonymous set and user's real location. Besides, we can enumerate the candidate anonymous edge set as much as possible by assigning the particle space dimensions. Thus, the range of the best solutions is reasonably expanded, leading to optimizing the final anonymous edge set.

After generating multiple candidate anonymous edge subsets, IMOPSO searches for optimal solutions by iteratively calculating the fitness functions. Since the fitness functions consist of privacy metrics and utility metrics, IMOPSO can simultaneously optimize privacy metrics and utility, i.e., IMOPSO can generate the final anonymous edge set to resist semantic relativity attack while preventing significant utility degrading.

Finally, IMOPSO randomly selects an anonymous edge set from the optimal solution set as the final anonymous edge set, leading to the randomness of the privacy-preserving algorithm. The attackers are thus less likely to reconstruct the similar anonymous edge set for inferring user privacy information. In this way, IMOPSO can prevent information leakage effectively. According to the above technical steps, our scheme is secure and can effectively resist semantic relativity attacks while preventing significant utility degrading.

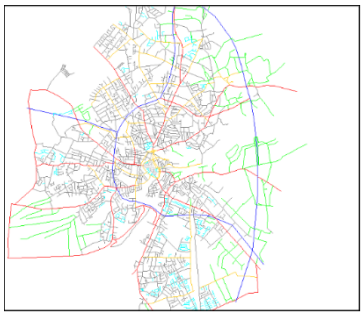
VI. EXPERIMENT AND EVALUATION

A. EXPERIMENTAL ENVIRONMENT AND SETTING

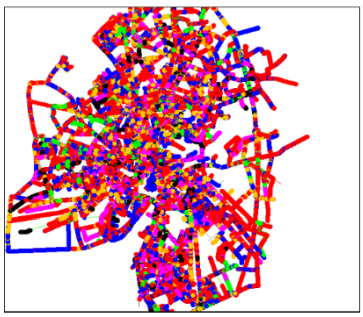
To evaluate the proposed STA-LPPM, we conduct experiments over a road network dataset generated by the Network-based Generator of Moving Objects (NGMO) [46] based on the city's road map Oldenburg, where 6,105 road intersections and 7,035 road edges are included. All the experiments are performed with a PC equipped with Intel(R) Core(TM) i5-6300U CPU and 8GB RAM. We introduce multiple location semantics into the real-world road network by randomly distributing the preset sensitive location semantics to Oldenburg's original road network. The map of the location semantic road network is as depicted in Fig. 4 (b). To verify the advantages of our method against the existing works in terms of semantic privacy protection and trade-off improvement, we conduct experiments to compare the proposed STA-LPPM with Dummy-Location Generation (DLG) [38] and BL k-disturbance [39]. All the experimental parameters are explained in detail in Table 2.

B. PRIVACY ANALYSIS

Here we compare our method to the other two methods by evaluating how privacy metrics vary with the parameter k. As observed in Fig. 5 and Fig. 6, the performances of both privacy metrics of IMOPSO are always the best amongst these three algorithms, which demonstrates that IMOPSO is superior to both DLG and BL k-disturbance in enhancing the degree of semantic privacy of the final anonymous edge set. As shown in Fig. 5, the sum of semantic relative distance of IMOSPO is twice as that of DLG and BL k-disturbance. This phenomenon results from the fact that IMOPSO uses sem_{dist} to evaluate the semantic relativity by comparing two different semantic attribute sets, which can calculate the semantic relative distance more accurately. Additionally, the scale of the anonymous set based on DLG increases with the increase



(a) The original road network of Oldenburg



(b) The semantic road network of Oldenburg

FIGURE 4. The two road networks for algorithm experiment.

TABLE 2. Experimental parameter list.

Parameter	Amount Distribution
Sum of road vertices	6105
Sum of road edges	7035
k	[2,10]
Average query time	[0.005,0.09]
Sum of edge distance differenc	[35,70]
Frequency of experiments	5000
Maximum number of iterations	20

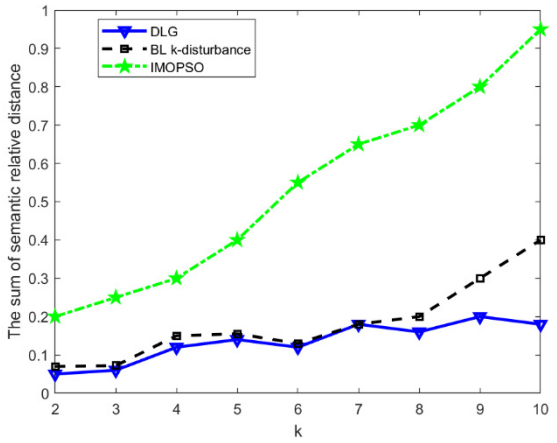


FIGURE 5. Effect of k on the sum of semantic relative distance.

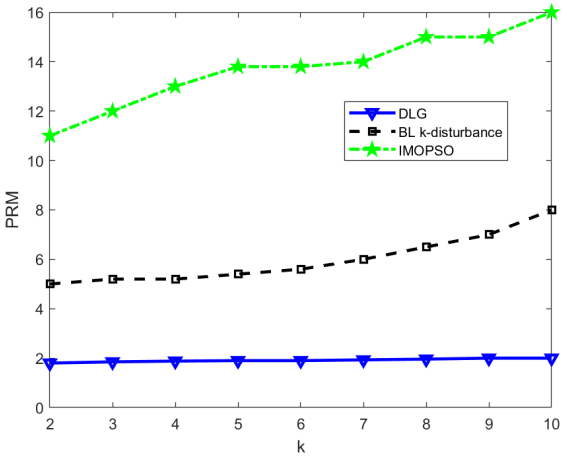


FIGURE 6. Effect of k on semantic privacy.

of k in Fig. 5 but the growth trend is nonlinear (i.e., its performance cannot satisfy the user privacy requirements as k increases). BL k-disturbance ensures the privacy protection of location semantic and sensitive location semantic, but it is limited in a specific context. Since the value of sem_{dist} of IMOPSO is well above the other two algorithms, the spatial distribution of the anonymous set of IMOPSO is more reasonable, and the resistance of semantic relativity attack of IMOPSO remains the best according to Eq. (1). As shown in Fig. 6, by comparing these three algorithms in terms of the anonymous edge selection strategy, the level of semantic privacy of IMOPSO is more than twice that of DLG and BL k-disturbance. This phenomenon results from the fact that IMOPSO uses semantic attribute sets to implement fine-grained definitions of multiple location semantics. In this way, mobile users can assign semantic sensitivity values to different location semantics more precisely. Hence the final anonymous edge set obtained by IMOPSO can evaluate the semantic privacy more accurately. Particularly, DLG consistently holds the low spot as k increases, which may attribute to its greedy strategy for filtering the final $k-1$ anonymous edge out of the $4k$ candidate anonymous edges. Hence, the degree of semantic privacy of the final anonymous edge set is lower than expected. BL k-disturbance applies the self-learning algorithm to generate an anonymous set, which improves the degree of semantic privacy of the anonymous set to a large extent, but the privacy rating of location semantic is roughly carried out by users themselves at the same time. On the contrary, IMOPSO continuously updates the anonymous sets with better privacy metrics within the threshold number of iterations. In that case, IMOPSO has practical significance in improving the degree of semantic privacy compared to the other two algorithms.

C. UTILITY ANALYSIS

To prove that our method can retain good utility while ensuring decent privacy, we adopt $sum_{\Delta e}$ and the average time described in Part D of Section IV as the utility metrics to evaluate the performance of our method. As shown in Fig. 7, the average time grows correspondingly with the increase of

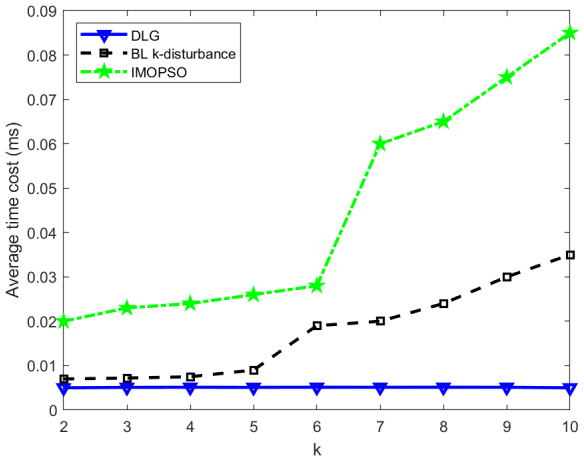


FIGURE 7. Effect of k on average time cost.

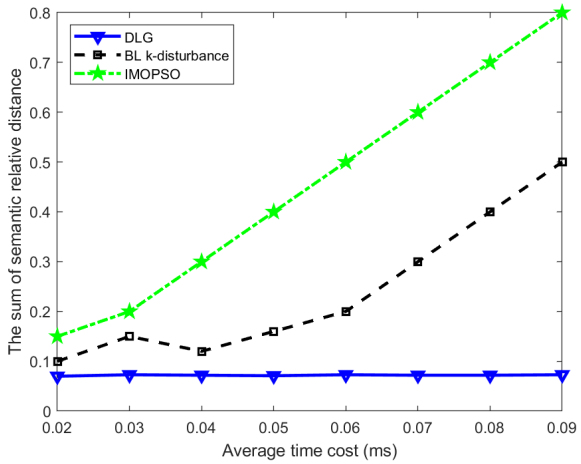


FIGURE 9. Effect comparison of three algorithms based on the sum of semantic relative distance.

the k value. Note that the calculation of semantic correlation between e_{anony} and e_{user} of BL k-disturbance occupies a large proportion in total time costs, and the final $k-1$ anonymous edges of DLG are filtered out of the original $4k$ candidate anonymous edges through three rounds. At the same time, the improved PSO anonymization algorithm of STA-LPPM involves the application of evolutionary computation. In this paper, the query time of IMOPSO is kept within tolerable limits by setting a certain iterative threshold. As shown in Fig. 8, the growing tendency of $sum_{\Delta e}$ for these three algorithms is nonlinear as the k value increases, and the sum of edge distance difference of IMOSPSO is more than twice that of DLG and BL k-disturbance. This phenomenon results from the fact that IMOPSO evaluates the sum of edge distance difference in terms of multiple candidate anonymous edge sets, guaranteeing the overall accuracy of the calculation. Notably, the distribution scope of $sum_{\Delta e}$ of DLG is broader than those of the other two algorithms due to the lack of the privacy rating for sensitive location semantics. The privacy

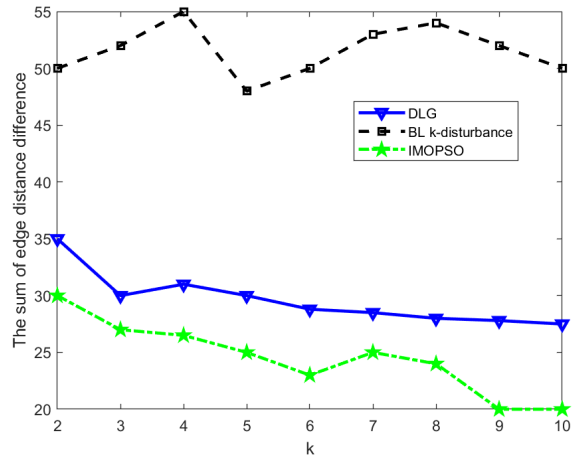


FIGURE 8. Effect of k on the sum of edge distance difference.

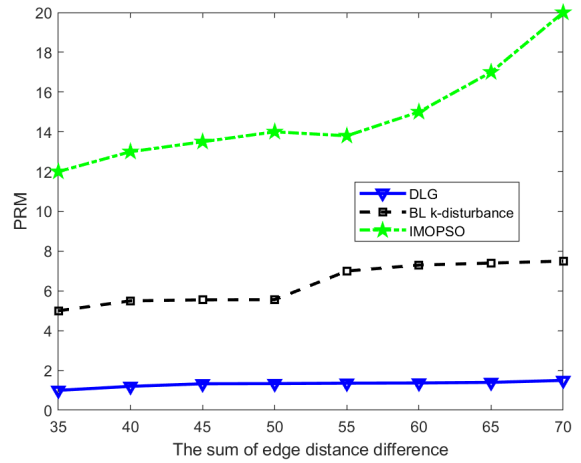


FIGURE 10. Effect comparison of three algorithms based on PRM.

rating of the location semantics of BL k-disturbance roughly includes three levels, leading to a coarse-grained LBS. and semantic relativities amongst anonymous edges are then easy to be inferred by attackers. IMOPSO thus taking advantage of maintaining the utility via the non-discrete distribution of anonymous edges of the final anonymous edge set.

D. TRADE-OFF ANALYSIS

Since the trade-off between privacy and utility in the existing methods remains being implemented in a compensatory way, we remind that our method is good in realizing optimal trade-off between privacy and utility simultaneously. To prove that IMOPSO indeed works in the compromise between privacy and utility, we conduct experiments to compare the performance of the trade-off of IMOPSO with that of the other two algorithms. As the results are shown in Fig. 9 and Fig. 10, IMOPSO implements trade-off more than twice as effectively as DLG and BL k-disturbance. As demonstrated in Fig. 9, IMOPSO maintains a high degree in resisting the semantic relativity attack as the average time

increases, indicating that IMOPSO is highly capable of providing better semantic privacy protection in a road network to DLG and BL k-disturbance. What can be concluded from Fig. 10 is that as the scope of the final anonymous edge set extends, IMOPSO has a great advantage in reconciling privacy and utility over the other two k-anonymity-based privacy-preserving approaches. Following the comparison and analysis mentioned above, it is evident that IMOPSO is more sensible in meeting user privacy requirements and a real-world road network scenario.

VII. CONCLUSION

This paper proposes an improved privacy protection strategy STA-LPPM, which is applied to improve the trade-off between privacy and utility in a location semantic road network. To analyze the effectiveness of privacy protection and utility maintaining, we first propose a new attack called semantic-relativity attack, and then propose two privacy metrics to evaluate the semantic privacy and the resistance to semantic relativity attack. Two utility metrics are used to measure the computation cost and query efficiency. STA-LPPM first employs BFS to generate a candidate edge set. After that, an optimal solution set is generated by running IMOPSO iteratively, from which the final anonymous edge set is randomly selected. As a result, the search time is minimized, and the accuracy rate is increased when forming the final anonymous edge set. The simulation results show that our privacy scheme performs better in user location protection and is practically applicable to a real-world road network scenario. STA-LPPM is thus not just a verified optimization method for enhancing the search effect of k-anonymity, but also an advanced problem-solving strategy for location privacy-preserving. For future work, we will focus on improving the trade-off problem of location trajectory privacy protection.

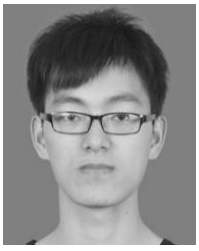
REFERENCES

[1] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.
[2] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, May 2019.
[3] S. Rajabzadeh, P. Shahsafi, and M. Khoramnejadi, "A graph modification approach for K-anonymity in social networks using the genetic algorithm," *Social Netw. Anal. Mining*, vol. 10, no. 1, pp. 1–17, Dec. 2020.
[4] P. Jain, M. Gyanchandani, and N. Khare, "Improved K-anonymity privacy-preserving algorithm using Madhya Pradesh state election commission big data," in *Integrated Intelligent Computing, Communication and Security*. Singapore: Springer, 2019, pp. 1–10.
[5] A. Razaque, M. B. H. Frej, H. Yiming, and Y. Shilin, "Analytical evaluation of K—Anonymity algorithm and epsilon-differential privacy mechanism in cloud computing environment," in *Proc. IEEE Cloud Summit*, Aug. 2019, pp. 103–109.
[6] Y. Wang, M. Li, S. Luo, Y. Xin, H. Zhu, Y. Chen, G. Yang, and Y. Yang, "LRM: A location recombination mechanism for achieving trajectory K-anonymity privacy protection," *IEEE Access*, vol. 7, pp. 182886–182905, 2019.
[7] S. Cerf, V. Primault, A. Boutet, S. B. Mokhtar, R. Birke, S. Bouchenak, L. Y. Chen, N. Marchand, and B. Robu, "PULP: Achieving privacy and utility trade-off in user mobility data," in *Proc. IEEE 36th Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2017, pp. 164–173.
[8] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," *ACM Trans. Database Syst.*, vol. 34, no. 4, pp. 1–48, Dec. 2009.
[9] M. Murshed, A. Iqbal, T. Sabrina, and K. M. Alam, "A subset coding based K-anonymization technique to trade-off location privacy and data integrity in participatory sensing systems," in *Proc. IEEE 10th Int. Symp. Netw. Comput. Appl.*, Aug. 2011, pp. 107–114.
[10] L. Hu, Y. Qian, M. Chen, M. S. Hossain, and G. Muhammad, "Proactive cache-based location privacy preserving for vehicle networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 77–83, Dec. 2018.
[11] P. Antiopi and B. Basilis, "Improvement of similarity-diversity trade-off in recommender systems based on a facility location model," in *Proc. 10th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, Patras, Greece, 2019, pp. 1–7.
[12] H. Wu, M. Li, and H. Zhang, "Enabling smart anonymity scheme for security collaborative enhancement in location-based services," *IEEE Access*, vol. 7, pp. 50031–50040, 2019.
[13] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst., Appl. Services*, May 2003, pp. 31–42.
[14] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. L. Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Oct. 2012, pp. 617–627.
[15] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 251–262.
[16] Z. Ma, F. Kargl, and M. Weber, "A location privacy metric for V2X communication systems," in *Proc. IEEE Sarnoff Symp.*, Mar. 2009, pp. 1–6.
[17] R. Shokri, G. Theodorakopoulos, J.-Y. L. Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 247–262.
[18] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in GPS traces via uncertainty-aware path cloaking," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, 2007, pp. 161–171.
[19] F. Julien, M. Raya, M. Felegyhazi, and P. Papadimitratos, "Mix-zones for location privacy in vehicular networks," in *Proc. Assoc. Comput. Mach. (ACM) Workshop Wireless Netw. Intell. Transp. Syst. (WiN-ITS)*, 2007, pp. 1–7.
[20] G. Argyros, T. Petsios, S. Sivakorn, A. D. Keromytis, and J. Polakis, "Evaluating the privacy guarantees of location proximity services," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, pp. 1–31, Feb. 2017.
[21] J. Zhang, F. Xue, X. Cai, Z. Cui, Y. Chang, W. Zhang, and W. Li, "Privacy protection based on many-objective optimization algorithm," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 20, p. e5342, Oct. 2019.
[22] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Sci. Rep.*, vol. 3, no. 1, pp. 1–5, Dec. 2013.
[23] T. Murakami, "Expectation-maximization tensor factorization for practical location privacy attacks," *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 4, pp. 138–155, Oct. 2017.
[24] A. Pyrgelis, C. Troncoso, and E. De Cristofaro, "What does the crowd say about you? Evaluating aggregation-based location privacy," *Proc. Privacy Enhancing Technol.*, vol. 2017, no. 4, pp. 156–176, Oct. 2017.
[25] R. Shokri, G. Theodorakopoulos, G. Danezis, J.-P. Hubaux, and J.-Y. L. Boudec, "Quantifying location privacy: The case of sporadic location exposure," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.* Berlin, Germany: Springer, 2011, pp. 57–76.
[26] M. Li, H. Zhu, Z. Gao, S. Chen, L. Yu, S. Hu, and K. Ren, "All your location are belong to us: Breaking mobile social networks for automated user location tracking," in *Proc. 15th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, Aug. 2014, pp. 43–52.
[27] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proc. NDSS*, vol. 11, Feb. 2011, pp. 1–17.
[28] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, lester and pierre: Three protocols for location privacy," in *Proc. Int. Workshop Privacy Enhancing Technol.* Berlin, Germany: Springer, 2007, pp. 62–76.
[29] B. Wang, M. Li, and H. Wang, "Geometric range search on encrypted spatial data," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 704–719, Apr. 2016.

[30] B. Wang, M. Li, H. Wang, and H. Li, "Circular range search on encrypted spatial data," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, Jun. 2015, pp. 182–190.
[31] G. Ghinita, M. L. Damiani, C. Silvestri, and E. Bertino, "Protecting against velocity-based, proximity-based, and external event attacks in location-centric social networks," *ACM Trans. Spatial Algorithms Syst.*, vol. 2, no. 2, pp. 1–36, Jul. 2016.
[32] H. Wu and Y.-C. Hu, "Location privacy with randomness consistency," *Proc. Privacy Enhancing Technol.*, vol. 2016, no. 4, pp. 62–82, Oct. 2016.
[33] L. Zhang, M. Chen, D. Liu, L. He, C. Wang, Y. Sun, and B. Wang, "A ε-sensitive indistinguishable scheme for privacy preserving," *Wireless Netw.*, vol. 26, no. 7, pp. 5013–5033, Oct. 2020.
[34] L. Zhang, D. Liu, M. Chen, H. Li, C. Wang, Y. Zhang, and Y. Du, "A user collaboration privacy protection scheme with threshold scheme and smart contract," *Inf. Sci.*, vol. 560, pp. 183–201, Jun. 2021.
[35] L. Zhang, J. Li, S. Yang, and B. Wang, "Privacy preserving in cloud environment for obstructed shortest path query," *Wireless Pers. Commun.*, vol. 96, no. 2, pp. 2305–2322, Sep. 2017.
[36] Q. Chen, X. Gan, W. Huang, J. Feng, and H. Shim, "Road damage detection and classification using mask R-CNN with DenseNet backbone," *Comput., Mater. Continua*, vol. 65, no. 3, pp. 2201–2215, 2020.
[37] Y. Wang, Y. Sun, S. Su, Z. Tian, M. Li, J. Qiu, and X. Wang, "Location privacy in device-dependent location-based services: Challenges and solution," *Comput., Mater. Continua*, vol. 59, no. 3, pp. 983–994, 2019.
[38] M. Zhao, X. Zhu, J. Niu, and J. Ma, "A semantic-based dummy generation strategy for location privacy," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 21–26.
[39] L. Kuang, Y. Wang, X. Zheng, L. Huang, and Y. Sheng, "Using location semantics to realize personalized road network location privacy protection," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–16, Dec. 2020.
[40] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie, "The long road to computational location privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2772–2793, 3rd Quart., 2019.
[41] L. Kuang, S. He, Y. Fan, H. Zhang, and R. Shi, "T-SR: A location privacy protection algorithm based on POI query," *IEEE Access*, vol. 7, pp. 59491–59503, 2019.
[42] P. Cortés, J. Muñuzuri, L. Onieva, and J. Guadix, "A discrete particle swarm optimization algorithm to operate distributed energy generation networks efficiently," *Int. J. Bio-Inspired Comput.*, vol. 12, no. 4, pp. 226–235, 2018.
[43] L. Zhang, S. Yang, J. Li, and L. Yu, "A particle swarm optimization clustering-based attribute generalization privacy protection scheme," *J. Circuits, Syst. Comput.*, vol. 27, no. 11, Oct. 2018, Art. no. 1850179.
[44] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proc. Int. Conf. Neural Netw. (ICNN)*, vol. 4, Nov. 1995, pp. 1942–1948.
[45] H. Zhou, M. Song, and W. Pedrycz, "A comparative study of improved GA and PSO in solving multiple traveling salesmen problem," *Appl. Soft Comput.*, vol. 64, pp. 564–580, Mar. 2018.
[46] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, no. 2, pp. 153–180, 2002.

CENXI TIAN received the B.S. degree in computer science and technology from Southwest Minzu University, in 2018. She is currently pursuing the M.S. degree with the School of Computer Science and Engineering, South China University of Technology. Her research interests include network security and location privacy.

HONGYUN XU received the B.S., M.S., and Ph.D. degrees from Central South University, in 1989, 1992, and 2005, respectively. She is currently a Professor with the School of Computer Science and Engineering, South China University of Technology. Her research interests include machine learning, network security, privacy protection, and cloud security.



TAO LU (Member, IEEE) received the B.S. degree in polymer materials and engineering from the South China University of Technology, in 2016. He is currently pursuing the M.S. degree with the School of Computer Science and Engineering, South China University of Technology. His research interests include location privacy, trajectory privacy, and machine learning.

RUI JIANG received the B.S. degree in network engineering from the Nanjing University of Information Science and Technology, in 2019. He is currently pursuing the M.S. degree with the School of Computer Science and Engineering, South China University of Technology. His research interests include location privacy and machine learning.

YONG KUANG received the B.S. degree in physics from the Officers College of PAP, in 2017. He is currently pursuing the M.S. degree with the School of Computer Science and Engineering, South China University of Technology. His research interests include Internet of vehicle, location privacy, and machine learning.