frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 03 October 2025
DOI 10.3389/fphy.2025.1624955

A localized differential privacy-based location preservation method using a hidden Markov model in vehicular networks

Jiwei Li* and Qiuju Zhang

College of Information Engineering, Henan Logistics Vocational College, Zhengzhou, China

Check for updates

OPEN ACCESS

EDITED BY
Sanbo Ding,
Hebei University of Technology, China

REVIEWED BY
Xiao-Wei Zhang,
Tiangong University, China
Yuhan Xie,
Hebei University of Technology, China

*CORRESPONDENCE
Jiwei Li,
✉ jiweili@mls.sinanet.com

RECEIVED 08 May 2025
ACCEPTED 09 September 2025
PUBLISHED 03 October 2025

CITATION
Li J and Zhang Q (2025) A localized differential privacy-based location preservation method using a hidden Markov model in vehicular networks.
Front. Phys. 13:1624955.
doi: 10.3389/fphy.2025.1624955

In the rapid development of vehicular networks, the exchange of information between vehicles and between vehicles and the infrastructure is becoming increasingly frequent. Vehicle location data have become one of the core types of information. However, location data contain a large amount of user privacy, and once leaked, they can severely threaten user safety and freedom. Therefore, there is an urgent need for a method that can balance privacy protection, data availability, and processing efficiency. In this paper, we propose a localized differential privacy location protection method based on the hidden Markov model (HMM) in vehicular networks, which addresses the problem of vehicle location privacy protection. The method consists of an HMM-based continuous location privacy protection algorithm and a localized differential privacy perturbation algorithm. The algorithm introduces the HMM into the field and utilizes its ability to accurately predict the continuous changes in vehicle location, thereby providing a scientific basis for privacy protection. At the same time, it combines the spatial correlation of location distribution to construct a privacy-preserving security area, which effectively restricts the range of the localized differential privacy perturbation, reduces the error, and improves data availability while safeguarding privacy. Second, this method incorporates a two-stage localized differential privacy perturbation algorithm to achieve dynamic differential privacy protection of vehicle location, adapting to real-time changes in vehicle location data through collaboration between the client and server. Based on the experiments and analysis using an actual trajectory dataset, the results show that the method provides strong privacy protection, high data availability, and efficient processing, thereby verifying its feasibility and effectiveness.

KEYWORDS

hidden Markov models, vehicles, localized differential privacy, privacy preservation, location security

Highlights

The main highlights of this paper are as follows:

1. This paper proposes a localized differential privacy location protection method based on the hidden Markov model in vehicular networks.
2. The method is thoroughly verified to demonstrate strong privacy protection, high data availability, and high processing efficiency through experiments and analyses on an actual trajectory dataset.

1 Introduction

In the current digital era, vehicular network technology is advancing at an unprecedented pace. The scope of its application continues to expand, which has a profound impact on society and people's lives. Vehicular networks represent a specific application of IoT technology in the field of transportation, enabling the intelligence and informatization of the transportation system. This is achieved through the exchange of information between vehicles and vehicles, vehicles and infrastructure, vehicles and people, and vehicles and networks [1]. Location information in vehicular networks serves as a fundamental basis for the realization of many applications. In terms of intelligent traffic management, the traffic department relies on the real-time uploaded location data of vehicles to accurately monitor the real-time distribution of traffic flow. Traffic-congested road sections are found in real time, and signal timing is optimized by an intelligent traffic signal control system, thus effectively easing traffic congestion and improving road traffic efficiency [2–4]. For example, during the morning and evening rush hours, the system can dynamically adjust the length of signal lights according to changes in traffic flow. This ensures that vehicles can pass through intersections in a fast and orderly manner. For travelers, location-based navigation services use vehicle location information, combined with real-time road conditions, to plan the optimal travel route for users. It avoids congested roads and saves travel time. In addition, location information in vehicular networks also plays an important role in logistics and distribution, shared mobility, and other fields, facilitating efficient resource scheduling and accurate service provision [5, 6].

However, with the extensive collection and use of location information in vehicular networks, the risk of vehicle location privacy leakage has become increasingly prominent. Vehicle location information contains a large amount of sensitive data closely related to the vehicle owner's personal details, such as daily travel patterns, home address, and workplace. Once this information is obtained by lawless elements, it may trigger a series of severe consequences. Malicious attackers can track the location of the vehicle to accurately locate the vehicle owner and commit crimes such as theft and robbery, which directly threaten the personal and property safety of the vehicle owner [7, 8]. For example, by analyzing the location of a vehicle that remains stationary for extended periods at night, an attacker may infer the owner's home address and subsequently determine n opportune time to commit a burglary. At the same time, the leakage of location information may also lead to unwarranted intrusion into the personal life of the vehicle owner, such as receiving a large number of targeted harassment advertisements and sales calls. The quality of life of the vehicle owner can be severely affected. In some extreme cases, the leakage of location information may even be exploited for more complex criminal activities, such as kidnapping and extortion, thus posing a serious threat to public security [9].

Numerous privacy protection techniques have been developed to address the problem of location privacy leakage in vehicular networks. Among these, localized differential privacy technology has attracted significant attention in the field of vehicular network privacy protection due to its unique advantages. The core feature of the localized differential privacy technique is its ability to protect location data at the point of generation, i.e., locally within the vehicle, without the need to rely on a trusted third party [10]. This characteristic makes localized differential privacy techniques well-suited to the distributed, open, and frequently changing node dynamics of a network environment such as the vehicle network. In vehicular networks, the large number of vehicles and the constantly changing driving status make it difficult to guarantee the existence of a completely trusted third party that can centrally process and protect the location data of all the vehicles. Localized differential privacy techniques protect vehicle location privacy to a certain extent by adding well-designed random noise, which makes it impossible for an attacker to infer the true location information of a vehicle accurately. Even if the data are accessed during transmission or by an untrustworthy data collector, the vehicle's location privacy can be protected to a certain extent [11].

Although localized differential privacy techniques have significant advantages in location privacy protection in vehicular networks. The dynamic nature of vehicle location change in vehicular networks raises new challenges. When a vehicle is in motion, its location is influenced by a variety of factors, such as road conditions, traffic regulations, and travel purposes, resulting in a complex and dynamically changing pattern. Traditional localized differential privacy methods often use fixed privacy-protection strategies, which cannot be flexibly adjusted according to the actual situation of vehicle location changes. For example, when the vehicle is in a busy urban traffic section, the surrounding vehicles are dense, and the location information is more likely to be correlated with analysis and inference. In such cases, fixed-strength privacy protection may be insufficient to address the increased risk of privacy leakage. When a vehicle is traveling on an empty highway, the risk of privacy leakage is relatively low, and if high-strength privacy protection measures are still used, the location data will be excessively perturbed. This will lead to a significant reduction in data usability and affect the normal operation of various applications that rely on location information in vehicular networks [12].

When a vehicle is in motion, spatial and temporal data need to be shared with the location-based application servers to maintain access to the services they provide. Users participating in tasks on the mobile crowdsourcing platform must also share location data to complete the collective intelligence-sensing tasks. In scenarios involving location information sharing, servers or service platforms maintain extensive records of users' historical movement trajectories. Once an attacker obtains these records and analyzes the spatial and temporal correlation of the user's mobile trajectory through modeling, it is possible to infer the user's next mobile behavior, which may lead to the leakage of the user's real location and related personal privacy. Therefore, the spatio-temporal correlation in the process of dynamic location change should be further considered when protecting vehicle location privacy. It is necessary not only to protect the real location information of the vehicle in real-time but also to ensure that the service provider can obtain aggregated analysis results with strong usability. Some of the existing dynamic location privacy protection methods have paid attention to the spatio-temporal correlation of vehicle location changes. However, there are still problems, such as high algorithmic complexity and poor usability of location data after privacy processing. To address the above problems, this study proposes a localized differential privacy location protection method based on the hidden Markov model (HMM). The main contributions of this paper are as follows.

1. This paper proposes a localization differential privacy location-protection method based on the HMM in vehicle networks. This method introduces the HMM into the domain of vehicle location privacy-protection, leveraging its ability to accurately predict the continuous changes in vehicle locations. This model can construct a continuous privacy-protection algorithm for location data, effectively addressing the temporal continuity characteristics of vehicle location data. It provides a more scientific and reasonable basis for subsequent privacy-protection operations. Additionally, when combined with the designed two-stage local differential privacy-perturbation algorithm, this model can achieve more precise and dynamic local differential privacy protection for vehicle locations. This enhances the security and privacy of location data in vehicle networks.
2. This method combines the spatial correlation of location distribution to construct the privacy-protection security area, which effectively restricts the scope of localized differential privacy perturbation. It significantly reduces the error caused by the privacy-protection operation. The method guarantees privacy while preserving data usability to the greatest extent. The method in this paper designs a two-stage localized differential privacy-perturbation algorithm, which achieves dynamic localized differential privacy protection of vehicle location through the collaborative work between the client and server. It meets the needs of real-time changes in vehicle location data in practical applications.
3. The method in this paper is thoroughly verified to demonstrate strong privacy-protection strength, high data availability, and high processing efficiency through experiments and analyses on the actual trajectory dataset. Therefore, the method proposed in this paper demonstrates both feasibility and effectiveness.

The remainder of this paper is organized as follows: Section 2 presents the related work. Section 3 contains the related definitions. Section 4 presents the system architecture. Section 5 presents the design process of the method proposed in this paper. Section 6 contains the theoretical analysis of the algorithm. Section 7 contains the experimental analysis. Section 8 provides the summary of this study.

2 Related works

Vehicle location information constitutes the basis for the normal operation of vehicular networks. The vehicle track is essentially a spatial and temporal sequence formed by the location over a period of time, which can effectively reflect the behavioral patterns and driving preferences of vehicle users. In the process of providing users with high-quality location services, location service providers may cause users' sensitive information to be leaked. Therefore, at the present stage, many experts, at home and abroad, have carried out extensive research on the privacy protection of vehicle trajectory.

Li et al. [13] proposed an energy-efficient location privacy-protection strategy. This strategy integrates closely related users into an intimate fog group. Users send their location-based service requests to this fog group, thereby avoiding direct interaction between users and service providers and, thus, successfully masking the users' precise location information. Ying et al. [14] proposed an improved E-SLP scheme that simultaneously protects the user's behavioral information and ensures the quality of the service they receive. However, this approach overly relies on trusted friends, which leads to some limitations in its application scope. Qian et al. [15] proposed a method that reduces the frequency of user requests to the server using caching technology when the user initiates a service request. This method reduces the possibility of privacy information leakage, but the time complexity of this method is high. Hakeem et al. [16] proposed a certificate-signing scheme using pairing technology. The scheme requires authentication of message certificates and signatures during vehicle interactions to ensure message integrity and user identity authenticity, but its space complexity is high. Azad and others [17] proposed a scheme that uses a crowdsourcing server to assign user requests to multiple "workers," who carry out the message forwarding operation on behalf of the user, and designed a cooperative crowdsourcing system to protect the privacy of vehicle location. The system ensures the reliability of the "workers" to collect the messages, but the time efficiency is low. Ren et al. [18] designed a vehicle location privacy-preserving framework called EGeoIndis. The framework guarantees the indistinguishability of geolocation information by abstracting maps into bitmaps. Moreover, it applies a linear programming approach to minimize quality loss, and at the same time, it guarantees the indistinguishability of geolocation information. Yang et al. [19] used a differential privacy-based group sensing technique to optimize the process of distributing data from the vehicle network. They used the distribution density of in-vehicle units as a measure to add noise to the user's true location, thereby generating an interfering location and achieving the goal of protecting vehicle location privacy. Takagi et al. [20] proposed a graph exponential mechanism that ensures the indistinguishability of geographic locations. They evaluated the effectiveness of privacy preservation and the loss of data utility of the location-based services. Compared to the traditional planar Laplace mechanism, the mechanism demonstrates superior data utility while maintaining the same level of privacy protection. Mehta et al. [21] studied the improved L-diversity trajectory data publishing mechanism. They designed a trajectory privacy protection scheme based on L-diversity, but this scheme is less efficient in computation time and lacks usability. Qiu et al. [22] focused on the trajectory-generating model. The method of generating and publishing false trajectories based on the original trajectory is used to protect trajectory data privacy, but this scheme overlooks sensitive semantic locations, which can easily lead to the leakage of sensitive location information. Arif et al. [23] studied the privacy protection problem in vehicle trajectory data publishing mechanisms, using differential privacy to mitigate vulnerabilities of connected vehicle data to denial-of-service attacks, central system failures, and privacy leakage. Shang et al. [24] proposed a blockchain-based data-sharing scheme for privacy-preserving authentication in connected vehicles. This scheme performs authenticated communication between vehicle nodes and roadside units, which is performed using authentication and access control schemes. Cheng et al. [25] proposed a personalized optimal trajectory data distribution algorithm based on differential privacy theory, which allocates the privacy budget according to the user's actual privacy needs, but this scheme has a high communication overhead. Li et al. [26] ensure that any sub-trajectory of length W in the published trajectory meets the differential privacy requirements by generating false trajectories. This, in turn, avoids the leakage of sensitive information of individual users due to the publication of vehicle trajectory data. Al-Hussaeni et al. [27] proposed a SafePath trajectory data publishing algorithm for transportation system scenarios by constructing a prefix tree to achieve privacy protection of personalized trajectory data. However, the prefix tree construction of this scheme is more complicated, and the algorithm takes a longer time. Ding et al. [28] proposed a streaming trajectory data-publishing mechanism. They also provided three different counting query functions that satisfy differential privacy with a wide range of applicability.

3 Relevant definitions

3.1 Localized differential privacy

Definition 1: (ε, local differential privacy; ϵ, LDP) [29]

A randomization algorithm F satisfies ε-local differential privacy, if and only if, for any input x, x', and any possible output y, it satisfies Equation 1.

$$\frac{Pr[F(x) = y]}{Pr[F(x') = y]} \le e^{\varepsilon}. \tag{1}$$

From Definition 1, it can be observed that localized differential privacy places a constraint on the similarity of the outputs of any two different input values. This restriction makes it very difficult for an attacker with arbitrary background knowledge to infer the original data from the outputs. As a result, the user's privacy is highly secured. Here, ε is the privacy budget, and this value specifically indicates the strength of privacy protection. The smaller the value of ε, the stronger the privacy protection. The larger the value of ε, the weaker the privacy protection.

Definition 2: Serial combinatoriality [30]. Suppose that there exist b different randomized algorithms $F_{1,}F_2, \cdots, F_b$, all acting on the same dataset D, i.e., $F_i(D)$. For any of these randomized algorithms, F_i satisfies $\varepsilon_i - LDP$; then, the serial combination of $\{F_1, F_2, \cdots, F_b\}$ satisfies $\sum_{i=1}^{m} \varepsilon_i - LDP$. The privacy budget $\varepsilon = \varepsilon_i \cdot b$. So, when a certain stochastic algorithm acts on the same dataset several times, the privacy budget increases exponentially. The corresponding level of privacy protection decreases exponentially.

Definition 3: Parallel combinatoriality [31]. Suppose that there exist b different randomized algorithms $F_{1,}F_2, \cdots, F_b$. There exists a dataset D, and it is divided into d disjoint sets $D_1, D_2, \ldots, D_d$. Each randomized algorithm acts on one dataset, i.e., $F_i(D_i)$, and satisfies $\varepsilon_i - LDP$. Then, the parallel combination of $\{F_1, F_2, \cdots, F_b\}$ satisfies $max(\varepsilon_i) - LDP$. When $F_1 = F_2 = \ldots F_d$, $\varepsilon = \varepsilon_i$; i.e., when a randomized algorithm acts on independent non-intersecting sets of data, the level of privacy protection remains constant.

3.2 Perturbation mechanism

Definition 4: Generalized random response [32]. A randomized response is applied to a candidate set D of a variable, such that the variable retains its true value with probability P and is perturbed with probability q to another value within the candidate set. The result of this perturbation is R under the perturbation process.

$$Pr[R(x) = y] = \begin{cases} \dfrac{e^{\varepsilon}}{e^{\varepsilon} + |D| - 1} & if\ y = x \\ \dfrac{1}{e^{\varepsilon} + |D| - 1} & if\ y \ne x \end{cases}. \tag{2}$$

3.3 Hidden Markov model

Definition 5: An HMM [33], as a type of Markov chain, is a dynamic Bayesian net with the simplest structure and a classical directed graph model. The variables in an HMM are divided into two groups. One group of variables is the set of state variables $\{J_1, J_2, \ldots, J_n\}$, where $J_i \in J$ represents the state of the system at the ith moment. It is assumed that the state variables are hidden and not directly observable, so the state variables are also called hidden variables. The second set of variables is the set of observed variables $\{Q_1, Q_2, \ldots, Q_n\}$, where $Q_i \in Q$ denotes the value observed at the ith moment. The observed variables can be either discrete or continuous. In an HMM, the system tends to transfer between multiple states, indicating that the range of values of the state variables is a discrete set containing multiple possible values. The basic model is shown in Figure 1.

The arrows plotted in Figure 1 are used to represent the dependencies between the variables. At any given moment T, the values of the observed variables depend only on the state variables; i.e., the value of the observed variable O_T is determined by the state variable S_T. It has no correlation with the other state variables or with the values of the observed variables. Moreover, the state S_T at moment T depends only on the state S_{T-1} at moment $T-1$, and it is not correlated with any of the earlier $T-2$ and more historical states. In summary, the state of the system at the next moment is determined only by the state at the current moment. It has no dependency on any of the past states.

The three parameters defined by the HMM are as follows:

Definition 6: State transfer probability. The probability that the model transitions between states is usually represented by the state transfer matrix $H = \left[h_{ij}\right]_{N \times N}$. Here, $h_{ij} = P(S_{T+1} = W|S_T = Z)$ denotes

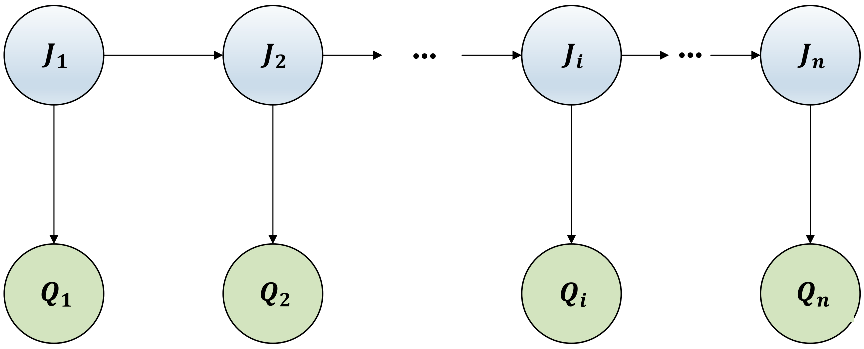

FIGURE 1
Hidden Markov model.

the probability that at moment T, if the model state is Z, then the model's state is W at the next moment.

Definition 7: Output observation probabilities. The probability that the model obtains each observation based on the current state is usually expressed as a matrix $U = \left[u_{ij}\right]_{N\times N}$. Here, $u_{ij} = P(O_T = a|S_T = b)$ denotes the probability that observation a will be obtained if the model state is b at the moment T.

Definition 8: Initial state probability. The probability of occurrence of each state of the model at the initial moment is denoted as $P_T = (p_1, p_2, \ldots, p_N)$.

3.4 Privacy-protecting security area

Definition 9: For a given time T, the set of location points is defined as those whose cumulative prior probabilities exceed the threshold θ. These location points constitute the privacy-protection safe zone at the current time T. This safe zone is denoted as S.

$$S = min\left\{L_{(i,T)}|\sum\nolimits_{L_{(i,T)}} P^{-}_{i,T} \geq 1-\theta\right\}.$$

Here, $L_{(i,T)}$ denotes the location point at time T, and $P^{-}_{i,T}$ represents the prior probability. The threshold θ is determined based on the characteristics of the prior probability distribution. By setting θ [34], the location points with higher probability at the current moment can be filtered out. These points form the secure region. When θ is small, the sum of the prior probabilities of a larger number of location points must exceed this threshold to constitute a secure region, resulting in a relatively larger secure region. An excessively large safe region expands the scope of differential privacy perturbations in localization, introducing more errors and reducing data usability. Conversely, a larger θ value shrinks the safe region, limiting the scope of differential privacy perturbations and improving data usability. However, this may weaken the privacy-protection strength as the vehicle's actual location becomes relatively easier to infer. Therefore, the setting of θ serves as a critical parameter in balancing the privacy-protection strength and data usability. By reasonably configuring θ based on the actual number of vehicles and vehicle trajectories, it is possible to maximize data usability while ensuring a certain level of privacy protection.

4 System architecture

The system architecture of the methodology in this paper mainly consists of two types of entities, client side and server side, and the function of each entity is described as follows.

4.1 Client

The client mainly contains vehicles. In the *HMM*-based location privacy protection algorithm, the client is primarily responsible for location information setting and *a priori* probability calculation, secure region determination, localized differential privacy perturbation, and *a posteriori* probability updating. Specifically, it includes setting the vehicle location information and state transfer matrix, calculating the *a priori* probability distribution at the current moment, determining the privacy-protecting security area, and judging whether the vehicle location is within the security area. The client receives the server-side random projection matrix for the first perturbation, returns the perturbation result, and calculates the updated *a posteriori* probability based on the user's perturbation location and grid division.

4.2 Server

The server side mainly includes the location service provider. On the server side, the primary tasks in the HMM-based location privacy protection algorithm include area division and parameter setting, parameter calculation and random projection matrix generation, initialization and perturbation result aggregation, and receiving data and performing a second perturbation. Specifically, it includes dividing and numbering the vehicle distribution area into grids, setting relevant parameters, calculating and generating the random projection matrix, and initializing the perturbation result statistics vector. The server receives the first perturbation result from the client and performs the second perturbation to obtain the final perturbation position. At the same time, it adds the result to the statistics vector and also indirectly supports the computation and

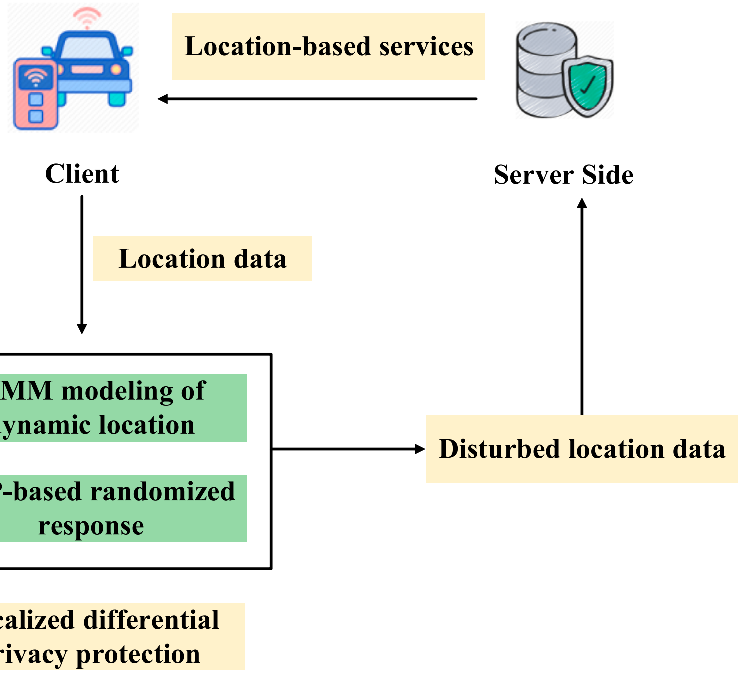
Location-based services
Client
Server Side
Location data
HMM modeling of dynamic location
LDP-based randomized response
Disturbed location data
Localized differential privacy protection

FIGURE 2
System architecture.

updating of the *a posteriori* probability by receiving information from the client.

The system architecture of the method proposed in this paper is shown in Figure 2, and the specific processes are as follows.

1. First, the real-time generated position data of the vehicle are modeled and analyzed using the HMM.
2. Subsequently, the vehicle makes use of the random response mechanism based on the localized differential privacy (LDP) model to perturb its real-time location data. Thus, the goal of localized differential privacy protection of the vehicle's location data is achieved.
3. Finally, the perturbed real-time location data are transmitted from the vehicle to the location service provider, and the vehicle sends a query request at the same time. The location service provider further optimizes the location-based service quality based on the results of the query.

5 Methodological design

The method in this paper consists of two main parts, which are mainly divided into two parts: the location privacy-preserving algorithm based on HMM and the localized differential privacy perturbation algorithm. The method design flow is shown in Figure 3.

5.1 HMM-based location privacy-preserving algorithm

Algorithm 1 takes into account the temporal correlation of the client's vehicle position over time. It then constructs a time series of position information based on the HMM. The actual location information of the client's vehicle is only held by the client, which is in a hidden state that cannot be directly observed by the outside world. The time-series formed by the real location of the vehicle in the process of continuous change constitutes the Markov model in this hidden state. The algorithm process is as follows.

1. First, the server-side grid is uniformly divided in the vehicle distribution area. After the division, the area grid is numbered $(1, 2, \ldots, c)$. The server-side parameters are set, where c is the number of regional grid G_c divisions, a is the number of vehicles, the confidence parameter η takes the value of 0.3, and the privacy budget is $\frac{\varepsilon}{4}$.
2. The server-side calculates the parameter $\gamma = \sqrt{\frac{\log \frac{2c}{\eta}}{\left(\frac{\varepsilon}{4}\right)^2 a}}$. The parameter d of the random projection matrix is calculated as $= \frac{\log(c+1)\log\frac{2}{\beta}}{\gamma^2}$. Finally, the random projection matrix $\Omega \in \left\{\frac{-1}{\sqrt{d}}, \frac{1}{\sqrt{d}}\right\}^{d\times c}$ is generated.
3. At moment T, the client-side sets the location information $L_{(i,T)}$ of vehicle i, and the state transfer matrix is set to W_i. The posterior probability distribution $P^{+}_{i,T-1}$ of the vehicle at

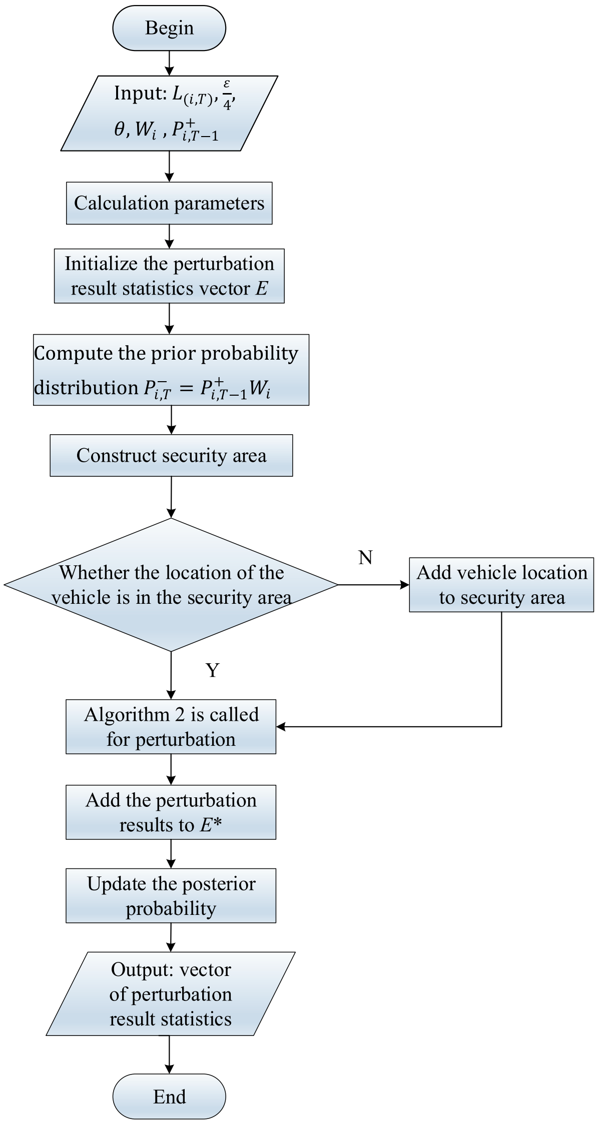
Begin
Input: $L_{(i,T)}, \frac{\varepsilon}{4}, \theta, W_i, P^{+}_{i,T-1}$
Calculation parameters
Initialize the perturbation result statistics vector E
Compute the prior probability distribution $P^{-}_{i,T} = P^{+}_{i,T-1} W_i$
Construct security area
Whether the location of the vehicle is in the security area
N
Add vehicle location to security area
Y
Algorithm 2 is called for perturbation
Add the perturbation results to E^*
Update the posterior probability
Output: vector of perturbation result statistics
End

FIGURE 3
Methodology design process.

the previous moment $T-1$ is used. The server-side initializes the disturbance result statistics vector E for the current moment.

4. The client-side first calculates the prior probability distribution $P^{-}_{i,T} = P^{+}_{i,T-1} W_i$ for vehicle i at the current moment T.
5. The client calculates the security area S. For a given moment T, a threshold θ is set. The set of location points that satisfy the sum of the prior probabilities of the locations, which exceeds the set threshold, constitutes the privacy-protecting security area at the current moment T. The client calculates the privacy-protecting security area. The formula is $S = min\left\{L_{(i,T)} | \sum_{L_{(i,T)}} P^{-}_{i,T} \geq 1-\theta\right\}$.
6. The client further determines whether the vehicle location $L_{(i,T)}$ is in the security area. If not, it needs to be added to the security area.

```
Input: Number of area grid divisions $G_c$, $a$ the number of vehicles ($a$), the confidence parameter $\eta$ = 0.3, client $i$'s location $L_{(i,T)}$ at time $T$, privacy budget $\frac{\varepsilon}{4}$, threshold $\theta$, state transfer matrix $W_i$, and the posterior probability $P^{+}_{i,T-1}$ at time $T-1$
Output: Random projection matrix $\Omega$
$\gamma = \sqrt{\frac{log\frac{2c}{\eta}}{(\frac{\varepsilon}{4})^2 a}}$, $d = \frac{\log(c+1)\log\frac{2}{\beta}}{\gamma^2}$
$\Omega \in \left\{\frac{-1}{\sqrt{d}}, \frac{1}{\sqrt{d}}\right\}^{d \times c}$ ← Generate the random projection matrix $\Omega$
for each location update moment $T$ do
  $L_{(i,T)}$ ← The client side sets the location information of vehicle $i$
  $W_i$ ← The state transfer matrix
  $P^{+}_{i,T-1}$ ← The posterior probability distribution of the vehicle at the previous moment $T-1$
  The server-side initializes the disturbance outcome statistics vector $E$ at the current moment.
  $S = min\left\{L_{(i,T)} | \sum_{L_{(i,T)}} P^{-}_{i,T} \geq 1-\theta\right\}$ ← Calculation of the security area
  if $L_{(i,T)} \notin S$ then
    Add $L_{(i,T)}$ to the security area
  end if
end for
```

Algorithm 1. HMM-based location privacy preservation algorithm.

5.2 Localized differential privacy perturbation algorithm

Algorithm 2 implements a localized differential privacy perturbation of the vehicle's true position for each moment in time through the designed two random response processes. The client sends the perturbed location to the server side.

1. The client receives the randomized projection matrix Ω, which is sent by the server side, and performs the first perturbation to the vehicle location $L_{(i,T)}$.
2. The client obeys the Bernoulli distribution and returns the true location of the vehicle $L_i{}'$ according to the probabilistic perturbation of $\frac{e^{\frac{\varepsilon}{4}}}{e^{\frac{\varepsilon}{4}}+|S|-1}$. According to the probabilistic perturbation of $\frac{1}{e^{\frac{\varepsilon}{4}}+|S|-1}$, the client returns the other locations in the security area S, except the vehicle's true location $L_i{}'$.
3. Finally, the client returns the vehicle perturbation location. It adds the perturbation result to the statistic vector. The client finally sends the perturbation result E' to the server.
4. After receiving the first perturbation result E' at the server side, the second perturbation is carried out. The perturbation location of the vehicle is $L_i{}^*$, $L_i{}^* = r_{\frac{\varepsilon}{4}} \cdot d \cdot \Omega \cdot \frac{e^{\frac{\varepsilon}{2}}}{e^{\frac{\varepsilon}{2}}+1} \cdot L_i{}'$, where $r_{\frac{\varepsilon}{4}} = \frac{e^{\frac{\varepsilon}{2}}-1}{e^{\frac{\varepsilon}{2}}+1}$. Finally, the perturbation result is added to E^*, and the client sends the perturbation result E^* to the server side.

```
Input: Client's real location $L_i$, privacy budget $\frac{\varepsilon}{4}$, and privacy-protected security area $S$
Output: Client perturbation location result
 The client receives the random projection matrix
  $\Omega$ sent by the server
 Client b~Bern($\frac{e^{\frac{\varepsilon}{4}}}{e^{\frac{\varepsilon}{4}}+|S|-1}$)
 if $b = 1$
     $E' \leftarrow L_i = L_i{}'$
 else
   b~Bern($\frac{1}{e^{\frac{\varepsilon}{4}}+|S|-1}$)
   return the location of the vehicle other than
   the true location of the vehicle $L_i{}'$
 end if
 return $E' \rightarrow$ Server side
 $r_{\frac{\varepsilon}{4}} = \frac{e^{\frac{\varepsilon}{2}}-1}{e^{\frac{\varepsilon}{2}}+1}$
   $L_i{}^* = r_{\frac{\varepsilon}{4}} \cdot d \cdot \Omega \cdot \frac{e^{\frac{\varepsilon}{2}}}{e^{\frac{\varepsilon}{2}}+1} \cdot L_i{}'$
 Return $E^* \leftarrow L_i{}^*$
 Send the perturbation result $E^*$ to the
  server side
 Update the posterior probability
   $P^+_{i,T}[c] = \Pr\left(L_{(i,T)} = G_c \mid L_i{}^*\right) = \frac{\Pr\left(E_T|L_{(i,T)}=G_c\right)\mathbf{p}^-_T[c]}{\sum_i \Pr\left(E_T|L_{(i,T)}=G_c\right)\mathbf{p}^-_T[i]}$
 end
```

Algorithm 2. Localized differential privacy perturbation algorithm.

5. Knowing the vehicle perturbation location L_i^* and the vehicle location $L_{(i,T)}$, the updated posterior probability $p^+_{i,T}$ is computed according to the partitioned grid G_c. $P^+_{i,T}[c] = \Pr\left(L_{(i,T)} = G_c \mid L_i^*\right) = \frac{\Pr\left(E_T|L_{(i,T)}=G_c\right)\mathbf{p}^-_T[c]}{\sum_i \Pr\left(E_T|L_{(i,T)}=G_c\right)\mathbf{p}^-_T[i]}$.

6 Theoretical analysis of algorithms

6.1 Privacy and security

The method proposed in this paper is based on the HMM and the localized differential privacy technique. It provides dynamic localized differential privacy protection for vehicle locations by constructing privacy-protecting security areas and designing a two-stage localized differential privacy perturbation algorithm. The setting of the security area restricts the area of localized differential privacy perturbation. It only processes the set of location points that satisfy the sum of location *a priori* probabilities exceeding a set threshold, which reduces the risk of privacy leakage. The client performs the first perturbation according to a Bernoulli distribution, and the server-side performs the second perturbation. The two perturbations cooperate so that the perturbed location information has a high degree of randomness and unpredictability, which effectively protects the vehicle's location privacy.

Second, it is assumed that L_i and L_j are any two locations within the privacy-preserving security area S at moment T, $\left(l_i, l_j \in S = \{L_1, L_2, ..., L_n\}\right)$. The location-randomized response algorithm proposed in this study achieves a randomized response with a privacy budget of $\frac{\varepsilon}{4}$ using Algorithm 1. Therefore, the final perturbed output M_{GRR} is satisfied: $\frac{Pr[M_{GRR}(L_i)=E]}{Pr[M_{GRR}(L_j)=E]} \leq \frac{\frac{e^{\frac{\varepsilon}{4}}}{e^{\frac{\varepsilon}{4}}+|S|-l}}{\frac{1}{e^{\frac{\varepsilon}{4}}+|S|-l}} = e^{\frac{\varepsilon}{4}} \leq e^{\varepsilon}$. So, it can be deduced that $\frac{Pr[M_{GRR}(L_i,\varepsilon)=E]}{Pr[M_{GRR}(L_j,\varepsilon)=E]} \leq max\{1, e^{\varepsilon}\}$. Thus, the algorithm proposed in this paper can provide ε-localized differential privacy for vehicle location.

6.2 Data availability

The method proposed in this paper establishes a privacy-preserving security area, which preserves the spatial characteristics of the location information as much as possible. Although limiting the perturbed area, the method proposed in this paper establishes a privacy-preserving security area by incorporating the spatial correlation of the location distribution. The set of location points in the security area has a high prior probability. This allows the perturbed location information to reflect the underlying distribution of vehicle locations a certain extent, thereby ensuring data usability. In Algorithm 2, the updated *a posteriori* probability is calculated based on the vehicle's perturbed location and the divided grid. This process enables the server-side to infer the vehicle's location to a certain extent based on the perturbed location information, which provides valuable data support for subsequent applications such as location service providers and improves data availability.

6.3 Time complexity

The proposed localized differential privacy location protection method in vehicular networks based on the HMM is jointly implemented using Algorithm 1 and Algorithm 2. In this paper, as shown in Algorithm 1, the computation of the prior probability for the client vehicle's location requires $O(|\tau|)$ time. It takes $O(n|\tau|\, log(S))$ time to compute the privacy-preserving security region of the vehicle. Therefore, the time complexity of Algorithm 1 is $O(|\tau|) + O(n|\tau|\, log(S))$. In Algorithm 2, the first stage of localized differential privacy perturbation takes $O(1)$ time. The second stage of localized differential privacy perturbation takes $O(n|\tau|)$ time. In addition, computing the posterior probability of the vehicle location distribution takes $O(|\tau|)$ time. Therefore, the time complexity of Algorithm 2 is $O(1) + O(n|\tau|) + O(|\tau|)$. Therefore, the overall time complexity of the method proposed in this paper is $O(|\tau| + |\tau|\, log(S) + 1 + n|\tau| + |\tau|) = O(|\tau|\, log(S) + n|\tau|)$.

6.4 Practicality

The method proposed in this paper is applicable to various scenarios requiring vehicle location privacy protection, such as intelligent transportation systems and location-based service applications. In these scenarios, vehicle location information often has important commercial value and social significance, but it also faces the risk of privacy leakage. The method proposed in this study can provide location data with a certain level of usability for related applications, demonstrating high practicaity while ensuring the privacy of vehicle locations. On the other hand, the method proposed in this paper is based on the HMM and localized differential privacy techniques, both of which have good scalability. The HMM can be easily extended to more complex location change scenarios, and the localized differential privacy technique can be adapted to different privacy requirements.

7 Experimental analysis

7.1 Experimental setup

The GeoLife dataset [35] is selected for the experimental data in this paper. This dataset collects trajectory data generated by 182 users over a period of 3 years. A large number of tuples containing timestamps and latitude/longitude information of the user's location are used to represent the user's mobile trajectory. The experimental environment is based on the Windows 10 Professional operating system, developed using PyCharm and Jupyter Notebook based on Python 3.8. The hardware environment includes an Intel(R) Core (TM) i5-10500 CPU, NVIDIA GeForce RTX 2060 GPU, and 16 GB RAM.

The default value of the privacy budget is set to 0.3, and the number of track entries is 18,320. The number of area grid G_c divisions is 26,810; the number of vehicles is a = 36,210; and the confidence parameter η takes the value of 0.3. The experimental parameters are shown in Table 1. The algorithms in [36] and [37] were selected for experimental comparison, with evaluation primarily based on three aspects: privacy-protection strength, data availability, and processing efficiency, to verify the effectiveness of the method proposed in this paper.

TABLE 1 Experimental parameters.

Parameter	Initial value
ε	0.3
Number of tracks	18,320
G_c	26,810
a	36,210
η	0.3

7.2 Measurement indicators

7.2.1 Privacy disclosure risk

Privacy protection intensity is usually measured using the privacy disclosure risk (PDR) [38]. It indicates the probability of location privacy disclosure under certain circumstances. We assume that the attacker can obtain all information except the actual query vehicle. G_i indicates whether an attacker can infer the vehicle's actual location. If the attacker can infer the real vehicle location, then G_i = *true*; otherwise, G_i = *false*. The statistic of the query result is denoted as K_i, and the number of sample groups is N. The number of the actual query vehicles in each group of samples is n. PDR is calculated using the following Equation 3.

$$PDR = \frac{\sum_{i=1}^{N} \frac{\sum_{j=1}^{n} R_i}{n}}{N},\ K_i = \begin{cases} 0, G_i = \text{false} \\ 1, G_i = \text{trun} \end{cases} \tag{3}$$

The privacy disclosure risk is related to the degree of background knowledge possessed by the privacy protection algorithm and the attacker. The smaller the value of the privacy disclosure risk, the lower the probability of privacy leakage and the higher the privacy-protection strength. The higher the value of the privacy disclosure risk, the higher the probability of privacy leakage and the weaker the privacy-protection strength.

7.2.2 Average maximum absolute error

In this section, the average maximum absolute error [39] is used to evaluate the deviation of the dynamic location data perturbation results of the client vehicles, which is defined as shown in the following Equation 4. The smaller average maximum absolute error indicates the difference between the statistical values of the vehicles located in the grid area and the real statistical values of the vehicles in the grid area after perturbation. The smaller the difference, the better the utility of the perturbation method and the higher the data availability.

$$MMAE = \frac{1}{T}\sum_{t} \max_{\varphi} \left|\hat{X}_{T,V} - \mathrm{X}_{T,V}\right|. \tag{4}$$

Here, φ denotes the whole two-dimensional region. $\mathrm{X}_{T,V}$ denotes the statistical value of the vehicle whose real location is at the grid region V at time T. $\hat{X}_{T,V}$ denotes the statistical value of the vehicle, which is located in the grid region V after the perturbation at time T.

7.2.3 Algorithm runtime

This section measures the processing efficiency of an algorithm by its running time, which is also an important criterion for assessing the algorithm's performance.

7.3 Analysis of the experimental results

7.3.1 Privacy-protection strength

In this experiment, the Bayesian mechanism with a typical background knowledge attack model [40] is chosen, the privacy disclosure of the three algorithms is compared under this attack model, and the comparison results are shown in Figure 4.

From the experimental results, it can be observed that the cumulative length of the client increases. On the whole, the privacy disclosure risk of the algorithm used in this paper is the smallest, which is approximately 24.22% on average. So, the probability of privacy disclosure of the algorithm used in this paper is the smallest, the privacy-protection strength is the largest, and the security is the highest. Through experimental comparison, it can be observed that when the cumulative length of the client is within

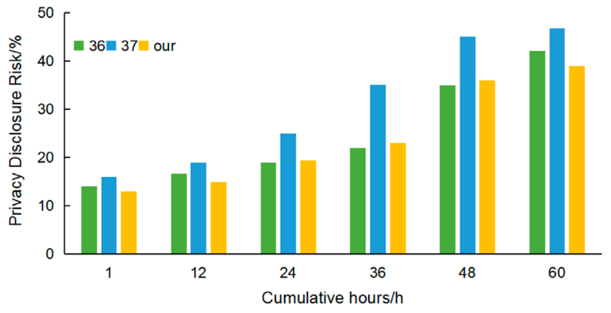

FIGURE 4
Privacy disclosure.

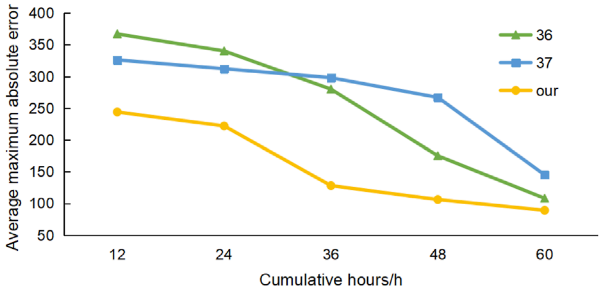

FIGURE 5
Maximum absolute error.

48 h, the privacy disclosure of this paper's algorithm and that of the algorithm in [36] are similar. Therefore, the probability of privacy disclosure is similar for both methods, and both demonstrate strong privacy protection. However, after 48 h, because the algorithm in [36] ignores the processing of spatio-temporal correlation, as time progresses, the more background knowledge the attacker obtains, the greater the probability of privacy disclosure of the algorithm in [36]. The increase in the risk of disclosure is larger, and the privacy strength is weakened. For the algorithm in [37], the privacy protection effect is poorer because it ignores the consideration of the security area. Thus, as the cumulative length increases, the growth trend of privacy disclosure risk becomes more pronounced, with the maximum disclosure risk reaching 46.8%, indicating a significant increase in the likelihood of privacy leakage.

7.3.2 Data availability

Figure 5 presents the maximum absolute error values of the algorithms at each position update moment. It can be observed that the maximum absolute error value of the proposed method in this study is lower than that of the algorithms in [36, 37] in the overall trend after perturbing the client vehicle location. In addition, the fluctuation of the maximum absolute error determined in this study is small. At the same time, the average maximum absolute error of this paper's method is less affected by the cumulative duration. The method proposed in this paper can better maintain the statistical accuracy of the perturbed position. Comparing with the algorithms in [36, 37], as the cumulative length decreases, their average maximum absolute errors keep increasing, and the statistical accuracy of the perturbed position decreases sharply. Therefore, the deviation of the perturbation results of the method proposed in this paper is smaller than that of the algorithms in [36, 37]. The statistical accuracy of the location after perturbation is higher, and the data availability is higher.

7.3.3 Processing efficiency

As observed from the experimental results in Figure 6, the running time of all three algorithms increases with an increase in the privacy budget. However, the overall running time of this paper's algorithm is relatively shorter, with an average running time of approximately 39.17 s, which has a higher processing efficiency. The average running time of the algorithm in [36] is approximately 50 s, and the processing efficiency of the algorithm used in this paper is approximately 27.6% higher. The average running time of the algorithm in [37] is approximately 55.8 s, and the processing efficiency of the algorithm used in this paper is approximately 42.46%, so the processing efficiency of the method proposed in this paper is higher.

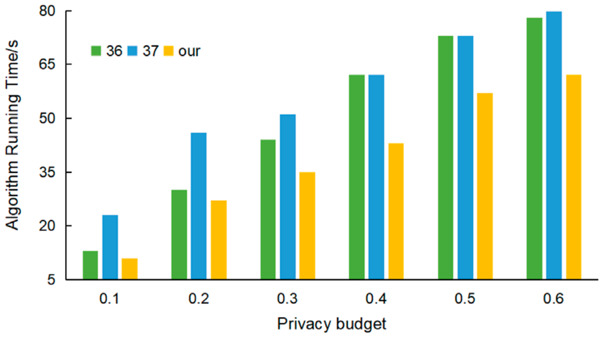

FIGURE 6
Running time.

8 Conclusion

In this paper, a localized differential privacy location protection method based on the HMM in vehicular networks is proposed to achieve vehicle location privacy protection. The method first uses the HMM to predict continuous changes in vehicle location and then combines the spatial correlation of location distribution to construct a privacy-protecting security area, which restricts the range of localized differential privacy perturbation and reduces errors. Meanwhile, a two-stage localized differential privacy perturbation algorithm is designed to reach dynamic local differential privacy protection of vehicle locations. Finally, the feasibility and effectiveness of the method are verified through experiments and analysis of actual trajectory datasets. Future research can be further promoted from various aspects. At the algorithmic level, the algorithm can be optimized to improve efficiency, such as by exploring methods to reduce the complexity of steps, such as random projection matrix generation, and considering parallelization of the algorithm to cope with large-scale data scenarios. In terms of balancing privacy protection and data availability, research can focus on a dynamic privacy budget allocation strategy, flexible adjustment based on factors such as location sensitivity, exploration of multi-granularity privacy protection, and differentiated protection for location information of different importance.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

JL: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Supervision, Writing – original draft. QZ: Conceptualization, Investigation, Methodology, Resources, Software, Visualization, Writing – review and editing.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Wen J. Distributed reinforcement learning-based optimization of resource scheduling for telematics. *Comput Electr Eng* (2024) 118:109464. doi:10.1016/j.compeleceng.2024.109464

2. Christie N, O'Toole S, Holcombe A, Bull N, Helman S. Managing the road safety risks of last mile deliveries with telematics: views among drivers and managers in the UK. *J Transport and Health* (2025) 40:101954. doi:10.1016/j.jth.2024.101954

3. Semenov I, Świderski A, Borucka A, Guzanek P. Concept of early prediction and identification of truck vehicle failures supported by In-Vehicle telematics platform based on abnormality detection algorithm. *Appl Sci* (2024) 14(16):7191. doi:10.3390/app14167191

4. von Glehn FR, Gonçalves BHP, Neto MGF, da Silva Fonseca JP. Telematics and machine learning system for estimating the load condition of a heavy-duty vehicle. *Proced Comp Sci* (2024) 232:2616–25. doi:10.1016/j.procs.2024.02.080

5. Bai Z, Miao H, Miao J, Xiao N, Sun X. Artificial intelligence-driven cybersecurity applications and challenges. *Innovative Appl AI* (2025) 2(2):26–33. doi:10.70695/AA1202502A09

6. Gambino AM, Stazi A. *Contract automation from telematic agreements to smart contracts[M]//The transformation of private law–principles of contract and tort as European and international law: a liber amicorum for mads andenas*. Cham: Springer International Publishing (2024). p. 621–41.

7. Truby J, Brown RD, Antoine Ibrahim I. Regulatory options for vehicle telematics devices: balancing driver safety, data privacy and data security. *Int Rev L Comput and Technology* (2024) 38(1):86–110. doi:10.1080/13600869.2023.2242671

8. Miao J, Wang Z, Ning X, Shankar A, Maple C, Rodrigues JJ. A UAV-assisted authentication protocol for internet of vehicles. *IEEE Trans Intell Transportation Syst* (2024) 25(8):10286–97. doi:10.1109/tits.2024.3360251

9. Marshall ET. Behavioural surveillance and risk segmentation: insights from telematics-based insurance monitoring. *The Pinnacle Res J Scientific Management Sci* (2025) 2(05):1–4. doi:10.55640/tprjsms-v02i05-01

10. Wang H, Li X, Shen Z, Liu P. Collaborative privacy-preserving based on LP and orp-drl mechanism for task offloading in mec. Available online at: https://SSRN 5153819.

11. Chen X. Transforming auto insurance: the impact of telematics and real-time data on pricing and risk assessment.

12. Fang Y, Chen SX, Wan AK, Ying Z. Preserving traveller privacy in location-based social media: a local differential privacy approach. *Inf Technology and People* (2025). doi:10.1108/itp-03-2024-0396

13. Li G, Zhang Q, Li J, Wu J, Zhang P. Energy-efficient location privacy preserving in vehicular networks using social intimate fogs. *IEEE Access* (2018) 6:49801–10. doi:10.1109/access.2018.2859344

14. Ying B, Nayak A. A distributed social-aware location protection method in untrusted vehicular social networks. *IEEE Trans Vehicular Technology* (2019) 68(6):6114–24. doi:10.1109/tvt.2019.2906819

15. Qian Y, Jiang Y, Hu L, Hossain MS, Alrashoud M, Al-Hammadi M. Blockchain-based privacy-aware content caching in cognitive internet of vehicles. *IEEE Netw* (2020) 34(2):46–51. doi:10.1109/mnet.001.1900161

16. Hakeem SAA, Kim HW. Multi-zone authentication and privacy-preserving protocol (MAPP) based on the bilinear pairing cryptography for 5G-V2X. *Sensors* (2021) 21(2):665. doi:10.3390/s21020665

17. Azad MA, Bag S, Parkinson S, Hao F. TrustVote: privacy-Preserving node ranking in vehicular networks. *IEEE Internet Things J* (2018) 6(4):5878–91. doi:10.1109/jiot.2018.2880839

18. Ren W, Tang S. EGeoIndis: an effective and efficient location privacy protection framework in traffic density detection. *Vehicular Commun* (2020) 21:100187. doi:10.1016/j.vehcom.2019.100187

19. Yang M, Zhu T, Xiang Y, Zhou W. Density-based location preservation for Mobile crowdsensing with differential privacy. *Ieee Access* (2018) 6:14779–89. doi:10.1109/access.2018.2816918

20. Takagi S, Cao Y, Asano Y, Yoshikawa M. Geo-graph-indistinguishability: protecting location privacy for LBS over road networks[C]//Data and applications security and privacy XXXIII. In: *33rd annual IFIP WG 11.3 conference, DBSec 2019, Charleston, SC, USA, July 15–17, 2019, proceedings 33*. Springer International Publishing (2019). p. 143–63.

21. Mehta BB, Rao UP. Improved l-diversity: scalable anonymization approach for privacy preserving big data publishing. *J King Saud University-Computer Inf Sci* (2022) 34(4):1423–30. doi:10.1016/j.jksuci.2019.08.006

22. Qiu S, Pi D, Wang Y, Xu T. SGTP: a spatiotemporal generalized trajectory publishing method with differential privacy. *J Ambient Intelligence Humanized Comput* (2023) 14(3):2233–47. doi:10.1007/s12652-022-04481-w

23. Arif M, Chen J, Wang G, Geman O, Balas VE. Privacy preserving and data publication for vehicular trajectories with differential privacy. *Measurement* (2021) 173:108675. doi:10.1016/j.measurement.2020.108675

24. Shang F, Deng X. A data sharing scheme based on blockchain for privacy protection certification of internet of vehicles. *Vehicular Commun* (2025) 51:100864. doi:10.1016/j.vehcom.2024.100864

25. Cheng W, Wen R, Huang H, Miao W, Wang C. OPTDP: towards optimal personalized trajectory differential privacy for trajectory data publishing. *Neurocomputing* (2022) 472:201–11. doi:10.1016/j.neucom.2021.04.137

26. Li S, Qi Z, Li Q. *Vehicle trajectory data publishing mechanism based on differential Privacy[C]//2021 china automation congress (CAC)*. IEEE (2021). p. 5373–8.

27. Al-Hussaeni K, Fung BCM, Iqbal F, Dagher GG, Park EG. SafePath: differentially-Private publishing of passenger trajectories in transportation systems. *Computer Networks* (2018) 143:126–39. doi:10.1016/j.comnet.2018.07.007

28. Ding X, Zhou W, Sheng S, Bao Z, Choo KKR, Jin H. Differentially private publication of streaming trajectory data. *Inf Sci* (2020) 538:159–75. doi:10.1016/j.ins.2020.05.058

29. Liu X, Wang J, Xiong X, Sun H. Federated learning data protection scheme based on personalized differential privacy in psychological evaluation. *Neurocomputing* (2025) 611:128653. doi:10.1016/j.neucom.2024.128653

30. Batool H, Anjum A, Khan A, Izzo S, Mazzocca C, Jeon G. A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. *Inf Sci* (2024) 652:119717. doi:10.1016/j.ins.2023.119717

31. Yuan Y, Tang X, Huang Y, Wu Y, Wang J. Local differential privacy for tensors in distributed computing systems. *arXiv preprint arXiv:2502.18227* (2025). doi:10.48550/arXiv.2502.18227

32. Wang L, Liu L, Zhan P, Tang P, Wei P, Guo S. Interactive verifiable local differential privacy protocols for mean estimation[C]. In: *2024 IEEE 23rd international conference on trust, security and privacy in computing and communications (TrustCom)*. IEEE (2024). p. 1448–57.

33. Wardhana I, Gouiaa-Mtibaa A, Vrignat P, Kratz F. Contribution to estimating the level of bearing degradation using a multi-branch hidden markov model approach. *Comput Industry* (2025) 167:104254. doi:10.1016/j.compind.2025.104254

34. Yin X, Liu H, Ding J, Guo J, Wu Z, Yang L, et al. Differential privacy based multiuser multivariate multiorder markov trajectory prediction in edge-cloud environment.

35. Xie G, Hou G, Pei Q, Huang H. Lightweight privacy protection *via* adversarial sample. *Electronics* (2024) 13(7):1230. doi:10.3390/electronics13071230

36. Wang Y, Nedić A. Robust constrained consensus and inequality-constrained distributed optimization with guaranteed differential privacy and accurate convergence. *IEEE Trans Automatic Control* (2024) 69:7463–78. doi:10.1109/tac.2024.3385546

37. Yang C, Jia K, Kong D, Qi J, Zhou A. DP-GSGLD: a Bayesian optimizer inspired by differential privacy defending against privacy leakage in federated learning. *Comput and Security* (2024) 142:103839. doi:10.1016/j.cose.2024.103839

38. Nawshin F, Unal D, Hammoudeh M, Suganthan PN. AI-powered malware detection with differential privacy for zero trust security in internet of things networks. *Ad Hoc Networks* (2024) 161:103523. doi:10.1016/j.adhoc.2024.103523

39. Zhang S, Lan P, Duan B, Chen Z, Zhong H, Xiong NN. DPIVE: a regionalized location obfuscation scheme with personalized privacy levels. *ACM Trans Sensor Networks* (2024) 20(2):1–26. doi:10.1145/3572029

40. Shen Z, Zhang Y, Wang H, Liu P, Liu K, Shen Y. BiGRU-DP: improved differential privacy protection method for trajectory data publishing. *Expert Syst Appl* (2024) 252:124264. doi:10.1016/j.eswa.2024.124264