TCA: A Trusted Collaborative Anonymity Construction Scheme for Location Privacy Protection in VANETs

Wenbo Zhang[1], Lin Chen[1], Hengtao Su[1], Yin Wang[1], and Jingyu Feng[1*]
[1] Xi'an University of Posts & Telecommunications
Xi'an, 710121, China
[e-mail: zhangwenbo@xupt.edu.cn, abbyccc11@163.com, zippybo@126.com, 1264667841@qq.com, fengjy@xupt.edu.cn]
[*]Corresponding author: Jingyu Feng

Received January 21, 2022; revised September 18, 2022; accepted October 5, 2022; published October 31, 2022

Abstract

As location-based services (LBS) are widely used in vehicular ad-hoc networks (VANETs), location privacy has become an utmost concern. Spatial cloaking is a popular location privacy protection approach, which uses a cloaking area containing *k*-1 collaborative vehicles (CVs) to replace the real location of the requested vehicle (RV). However, all CVs are assumed as honest in *k*-anonymity, and thus giving opportunities for dishonest CVs to submit false location information during the cloaking area construction. Attackers could exploit dishonest CVs' false location information to speculate the real location of RV. To suppress this threat, an edge-assisted Trusted Collaborative Anonymity construction scheme called TCA is proposed with trust mechanism. From the design idea of trusted observations within variable radius *r*, the trust value is not only utilized to select honest CVs to construct a cloaking area by restricting *r*'s search range but also used to verify false location information from dishonest CVs. In order to obtain the variable radius *r* of searching CVs, a multiple linear regression model is established based on the privacy level and service quality of RV. By using the above approaches, the trust relationship among vehicles can be predicted, and the most suitable CVs can be selected according to RV's preference, so as to construct the trusted cloaking area. Moreover, to deal with the massive trust value calculation brought by large quantities of LBS requests, edge computing is employed during the trust evaluation. The performance analysis indicates that the malicious response of TCA is only 22% of the collaborative anonymity construction scheme without trust mechanism, and the location privacy leakage is about 32% of the traditional Enhanced Location Privacy Preserving (ELPP) scheme.

Keywords: Privacy protection, trust mechanism, VANETs.

This work was supported in part by the National Natural Science Foundation of China under Grant 61802302, in part by the Natural Science Foundation of Shaanxi Province under Grant 2019JM-442.

http://doi.org/10.3837/tiis.2022.10.013 **ISSN : 1976-7277**

1. Introduction

As a significant component of Intelligent Transportation Systems (ITS), vehicular ad-hoc networks (VANETs) can acquire traffic circumstances and vehicle conditions to reduce traffic accidents and improve traffic efficiency [1-3]. The system model of VANETs is shown in **Fig. 1**. By deploying Roadside Units (RSUs) around the road and installing an On-board Unit device (OBU) on vehicles, the vehicles in VANETs can share driving parameters and roads information with other vehicles and nearby RSUs. Due to the high-performance, scalable, and reliable data centers of the cloud, these unprecedented amounts of data can be managed and stored through the cloud server in vehicular networks [4].

Recently, the Location-based Services (LBS) of vehicular networks have developed rapidly with the progress of GPS positioning technology [5]. By sending location and service request messages, autonomous vehicles can enjoy various LBSs provided by the Location Service Provider (LSP). For instance, autonomous vehicles can get relevant location information of parking lots, gas stations, shopping centers, hotels, and restaurants within a certain range. However, the convenience of LBS also brings the risk of privacy disclosure. For example, attackers collect location information of a specific vehicle to infer its sensitive information, such as residence, workplace, and living habits [6], and even more bring potential risks to property and personal safety by destroying the automatic driving system. It is feasible that maintain an acceptable level of service degradation for autonomous vehicular networks in the presence of location privacy threats [7].

Aiming at these problems, a lot of work has been done on location privacy protection. As one of the most popular approaches for vehicles' location privacy, spatial cloaking employs a trusted third-party (named anonymizer) [8-10] which expands the real location of the Request Vehicle (RV) to a cloaking area. When requesting LBS, the RV's real location is replaced by a cloaking area that contains other k-1 Collaborative Vehicles (CVs). With a cloaking area, attackers are difficult to distinguish the RV from the other k-1 CVs. Furthermore, compared with other solutions, spatial cloaking is able to provide precise query results without any requirement for complicated cryptographic technologies.

However, most spatial cloaking schemes assume that CVs always tell the truth, and fail to consider location cheating behaviors during the construction of the cloaking area. The high mobility and volatility characteristics of VANETs make adjacent vehicles usually unknown to each other [11]. This may offer opportunities for dishonest CVs to provide false location information, which leads that the cloaking area cannot satisfy the privacy protection requirement of RV. More seriously, attackers could exploit dishonest CVs' false location information to speculate the real location of the RV. Hence, how to efficiently defend against location cheating behaviors launched by dishonest CVs has become a challenging issue to achieve better spatial cloaking.

In this paper, an edge-assisted Trusted Collaborative Anonymity construction scheme with a trust mechanism called TCA is proposed for protecting the location privacy of vehicles against location cheating behaviors launched by dishonest CVs. The main contributions are described as follows.

- Introduce the design idea of trusted observations within variable radius r to verify the location information of CVs. When a CV sends location information during the construction of the cloaking area, the trusted third-party anonymizer can broadcast verification needs to his adjacent vehicles called Observer Vehicles (OVs) to require trusted observations to check whether the distance between the CV and OVs is within a radius r.

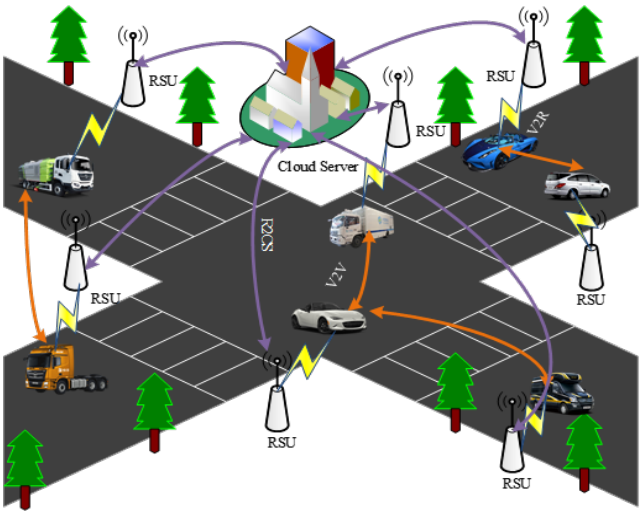


Fig. 1. The system model of VANETs.

- Design an edge-assisted trust value prediction method to support trusted observations. The Collaborative Trust (CT) value and Observer Trust (OT) value are evaluated respectively. Both CT value and OT value can be incorporated into a Synthetical Trust (ST) value. With the three types of trust value, three trust judgment strategies can be adopted to support trusted observations. To deal with the massive trust value calculation demand brought by large quantities of LBS requests, edge computing is employed during the trust evaluation.
- Establish a multiple linear regression model to calculate the variable radius *r* based on the privacy level and service quality of RV. The radius *r* can be dynamically adjusted in the light of vehicles' regional activity. The radius *r* is used to verify CVs' location verification on the basis of trusted observations. By restricting *r*'s search range, trust value can also be utilized to predict the trust relationship between RV and CVs, and construct the trusted cloaking area.

The organization of this paper is as follows. In Section 2, preliminaries related to privacy protection, trust mechanism, and edge computing are described. We propose the TCA scheme in section 3 and analyze the security in Section 4. In Section 5, the simulation analysis of the TCA scheme is performed. Finally, we conclude the paper in Section 6.

2. Related Works

2.1 Spatial Cloaking Location Privacy Protection

Since spatial cloaking was first introduced by Grunwald and Gruteser [12], many approaches had been proposed to protect location privacy. In [13], by converting trajectories into location points, a virtual trajectory generation algorithm was proposed to protect vehicles' privacy. In [14], the works related to identity and location privacy threatening factors, problems, and solutions were studied. The research indicated most of the solutions use pseudonym identity or address changing scheme to protect identity privacy. In [15], a pseudonym changing strategy based on the Vehicular Location Privacy Zone (VLPZ) was proposed to address pseudonym changing strategies issues, in which the RSUs were considered as typical places to implement a VLPZ. In [16], in order to overcome the weakening of the effectiveness of

location obfuscation when users move and recurrently request for LBS, a *k*-anonymity privacy protection scheme DUMMY-Q based on query perturbation was proposed. In DUMMY-Q, query privacy can be protected even if the user's identity is exposed. In [17], an Attribute-based *k*-Anonymous collaborative scheme (ABAKA) was proposed. To obtain the *k*-1 collaborative users, ABAKA provided *p*-sensitive as well as *k*-anonymity. In [18], based on the user's location privacy preference model, a Dynamically Adjustable *k*-anonymous (DAK) algorithm was designed to determine the privacy protection strength in different contexts. The DAK selected one anonymous group of adjacent vehicles to construct the cloaking area, and obtain the requested vehicle's dummy location. In [19], by employing a function generator used to generate the transforming parameters, an Enhanced Location Privacy-Preserving (ELPP) scheme was first proposed. Without the parameters, the anonymizer knows nothing about the user's real location. In [20], a distributed social-aware location-privacy protection (SLP) protocol which developed three strategies can conceal the original sender among the insecure vehicular networks without the help of a trusted third party. To stimulate users participating in the cloaking area construction. [21] proposed a *k*-anonymity location privacy scheme based on an auction mechanism. To achieve trajectory *k*-anonymity privacy protection, [22] proposed Location Recombination Mechanism (LRM) which could generate *k*-1 fake trajectories similar to base trajectories in terms of geographical features and probabilistic features.

However, a trust mechanism is not introduced in these existing works, which fails to consider location cheating behaviors during the cloaking area construction. The attackers may infer the true location of the RV when they are applied directly to the VANETs.

2.2 Trust Mechanism

Trust mechanism can play an important role in VANETs, which enables the vehicle to judge whether the received message is trustworthy, and provides the basis for the punishments or rewards on specific vehicles.

Considerable researches have been done on trust evaluation. In [23], based on the verification of the behavior of the vehicle on the network, the vehicle periodically contacted the certification and traffic management agency to update its trust value. In [24], a reliable reputation system was designed. If the agent vehicle completes the task honestly, a virtual check is awarded. The check can be used to encourage cooperative vehicles and punish malicious vehicles. In [25], a reputation model was proposed to verify the trustworthiness of messages sent in VANETs. In this model, each vehicle requested the vehicles within its communication range to express opinions about the sending vehicle's trustworthiness. In [26], a novel decentralized trust management scheme for vehicles was proposed, in which all RSUs can participate in the trust value updating process. The trust information of all the vehicles can also be provided to all RSUs in this scheme.

In the trust mechanism, the beta function is one of the most popular designs. In the beta function, the number of trusted and untrusted behaviors a vehicle performed is calculated first. Then, the trust value with the beta function will be denoted by $Beta(\alpha, \beta)$ [27].

$$Beta(\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} \theta^{\alpha-1} (1-\theta)^{\beta-1} \tag{1}$$

Where θ is the probability of vehicles' behaviors, $0 \leq \theta \leq 1$, $\alpha > 0$, $\beta > 0$.

Take an example for the *i*-th vehicle (V_i), and unt_i denote the number of trusted and untrusted behaviors conducted by V_i respectively. When the message is trusted, $\alpha = tru_i + 1$, otherwise $\beta = unt_i + 1$. Thus, the trust value of V_i is calculated as:

$$T_i = Beta\,(tru_i + 1, unt_i + 1) \tag{2}$$

The expectation value can be derived as $E[Beta(\alpha, \beta)] = \alpha / (\alpha + \beta)$. To make the maximum trust value of V_i tend to 1, the T_i can be further described as follows:

$$T_i = \frac{1 + tru_i}{1 + tru_i + unt_i} \tag{3}$$

where $0 \le T_i \le 1$. When $tru_i \ge 1$ and $unt_i = 0$, T_i is always equal to 1. For V_i, the more often it sends trusted messages, the higher the trust value will be.

3. Our Proposed TCA Scheme

Based on the trust mechanism, an edge-assisted trusted collaborative anonymity construction scheme (TCA) is proposed in this paper to protect the location privacy of vehicles. Specifically, the TCA scheme consists of three modules: edge-assisted trust value evaluation, trusted observation within variable radius *r*, and trusted cloaking area construction. In this section, we first describe the design architecture of the TCA scheme and then introduce the three modules. Finally, we give the execution strategies of TCA.

3.1 Architecture Overview

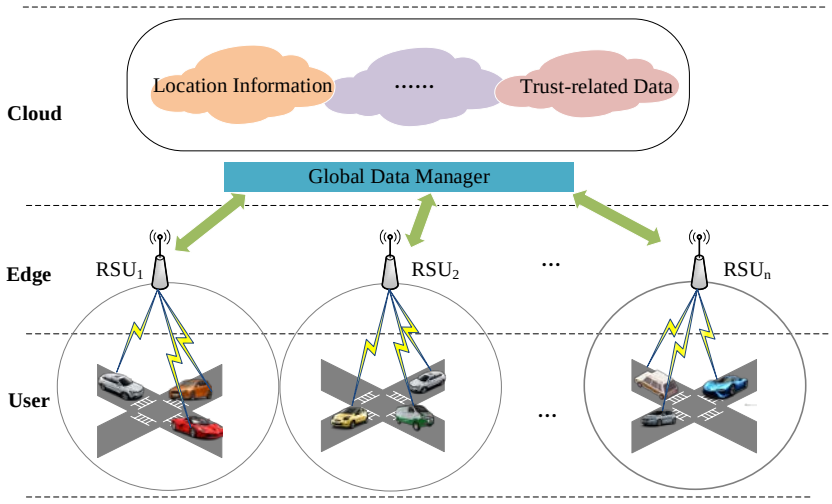


Fig. 2. Network architecture of the TCA scheme.

The architecture of the TCA scheme is present in this section, including network architecture and system architecture. As shown in **Fig. 2**, the network architecture defines the components and functions contained in the TCA scheme and consists of three layers.

- Cloud Layer — Due to the features of the power storage capacity and wide coverage, the cloud layer is responsible for managing trust-related data, such as historical location information, collaborator behaviors, observer behaviors, and so on.
- Edge Layer — With rich communication, calculation, and storage capabilities, RSUs are good candidates for "edge nodes". They can be deployed as the intermediate nodes between the cloud and vehicles to assist the data aggregation and trust value evaluation.
- User Layer — This layer consists of RV, CV, and OV. A vehicle can request LBS as a RV, help other vehicles as a CV during cloaking area construction, or play the role of OV to verify the location information from CVs.

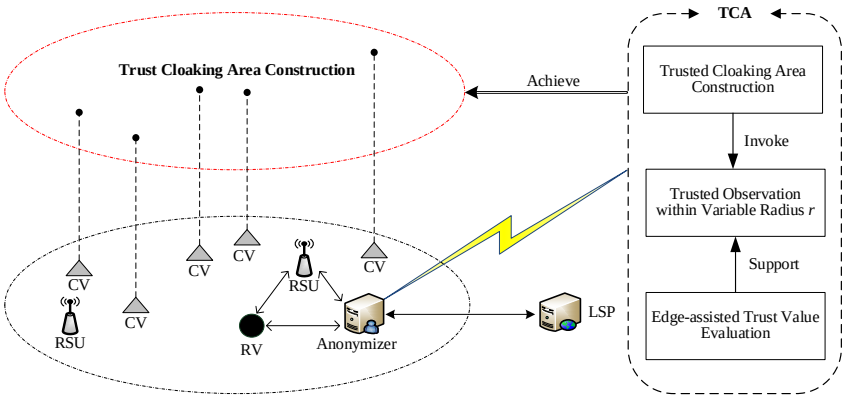


Fig. 3. System architecture of the TCA scheme.

Specifically, the TCA scheme consists of three successive modules as shown in **Fig. 3**:

1) Edge-assisted trust value evaluation. In this module, the trust values of vehicles are predicted rapidly with the assistance of RSUs. The trust value is predicted according to the historical behavior of vehicles. If vehicles always submit a true location, they will reward a higher trust value; otherwise, if vehicles always submit a false location, their trust value will be lower than the former.

2) Trusted observation within variable radius *r*. The radius *r* will be dynamically changed through the established multivariate linear model based on the privacy level and service quality of RV.

3) Trusted cloaking area construction. Combining trust value and radius *r* of vehicles, the appropriate CVs for RV are selected within this module which is used to replace RV's real location information during sending LBS requests to LSP.

3.2 Edge-assisted Trust Value Evaluation

In the process of cloaking area construction, trust value evaluation occurs in the following two cases.

- Trust value evaluation is employed to differentiate dishonest CVs and honest CVs. The trust value is evaluated according to the historical behavior of vehicles. Dishonest CVs can be predicted using the trust value; for example, when compared to honest CVs, dishonest CVs usually report false location and reward a lower trust value.
- After receiving the location information from CVs, the anonymizer should broadcast verification requirements to the adjacent vehicles called OVs. Then, the OVs check whether the distance between a CV and OVs is within variable radius *r*. To ensure the verification credibility and improve the verification efficiency, the trust value evaluation related to OVs should also be involved.

However, with the growing number of LBS requests, a massive trust evaluation may be required. Hence, edge computing is potentially a good approach to assist the evaluation of trust values, in which RSUs can be deployed as the edge nodes.

The detailed trust value evaluation process is as follows. Take the *i*-th vehicle (V_i) for example. The two-tuple (f_i, t_i) represent the amount of false and true location reported by V_i. The trust value with a role of CV is evaluated as:

$$CT_i = \begin{cases} \dfrac{1+t_i}{f_i+t_i+1} - \delta \cdot \dfrac{f_i}{t_i+1}, & f_i < t_i, \\ 0, & f_i \geq t_i. \end{cases} \tag{4}$$

where $0<\delta<1$ is the threshold of trust value. If $f_i=0$, CT_i is equal to 1, denoting V_i behaves honestly. If $f_i > 0$, CT_i will decrease sharply as f_i increases.

Likewise, the two-tuple (w_i, c_i) denote the amount of wrong and correct observations submitted by V_i. The trust value with a role of OV is evaluated as:

$$OT_i = \begin{cases} \dfrac{1+c_i}{w_i+c_i+1} - \delta \cdot \dfrac{w_i}{c_i+1}, & w_i < c_i \\ 0, & w_i \geq c_i \end{cases} \quad (5)$$

If $OT_i \geq \delta$, V_i's observation will be adopted by the anonymizer when V_i plays the role of OV.

Synthesizing CT_i and OT_i, the comprehensive trust value is evaluated as:

$$ST_i = \begin{cases} \dfrac{1+t_i+c_i}{f_i+t_i+w_i+c_i+1} - \delta \cdot \dfrac{f_i+w_i}{t_i+c_i+1}, & f_i+w_i < t_i+c_i \\ 0, & f_i+w_i \geq t_i+c_i \end{cases} \quad (6)$$

To help the anonymizer to make a rapid verification decision, three trust judgements can be adopted.

-***J1***: V_i's location information will be accepted directly when $CT_i = 1$.

-***J2***: V_i's location information will be accepted by the anonymizer, and invoke the process of trusted observations within radius r when $CT_i \geq \delta$.

-***J3***: V_i's location information will be rejected when $CT_i < \delta$ or $ST_i < \delta$.

According to the predicted trust value, the trusted CVs can be selected to participate in LBS request.

3.3 Trusted Observation within Variable Radius r

In this paper, the variable radius r can be used to meet the personalized requirements of RV during the cloaking area construction. The privacy protection level (l_p) and service quality level (l_q) should be taken into account. Generally, the larger r is, the more dispersed the distribution of the vehicle in the constructed cloaking area will be, and the higher l_p will be. But, the l_q of RV cannot be guaranteed. On the contrary, the smaller r is, the lower l_p will be. But RV can get a higher l_q.

Since r changes along with l_p and l_q, there is a certain mapping relationship among them. We can build the multiple linear regression function to predict r from l_p and l_q, which is calculated as follows:

$$r = f\left(l_p, l_q\right) = \alpha_0 + \alpha_1 l_p + \frac{\alpha_2}{l_q} + \varepsilon \quad (7)$$

where α_0 is the regression constant, α_1, α_2 is the regression coefficient, ε is a random error term.

With the least square method, the influence of l_p and l_q on r is calculated as follows:

$$y = \alpha_0 + \alpha_1 l_p + \frac{\alpha_2}{l_q} + \varepsilon - r \quad (8)$$

When $\alpha_0 = \hat{\alpha}_0, \alpha_1 = \hat{\alpha}_1, \alpha_2 = \hat{\alpha}_2, \alpha_0, \alpha_1, \alpha_2$ can be obtained if the (9) reaches the minimum.

$$G = \sum_{o=1}^{2} \left(y_o - \alpha_0 - \alpha_1 l_{po} - \frac{\alpha_2}{l_{qo}} \right)^2 \quad (9)$$

By taking the partial derivative of the above equation and setting it equal to 0, the normal equations can be obtained as follows:

$$\begin{cases} \dfrac{\partial G}{\partial \alpha_0} = -2\sum_{o=1}^{2}\left(y_o - \alpha_0 - \alpha_1 l_{po} - \dfrac{\alpha_2}{l_{qo}} \right) = 0, \\ \dfrac{\partial G}{\partial \alpha_1} = -2\sum_{o=1}^{2}\left(y_o - \alpha_0 - \alpha_1 l_{po} - \dfrac{\alpha_2}{l_{qo}} \right) l_{po} = 0, \\ \dfrac{\partial G}{\partial \alpha_2} = -2\sum_{o=1}^{2}\left(y_o - \alpha_0 - \alpha_1 l_{po} - \dfrac{\alpha_2}{l_{qo}} \right) \dfrac{1}{l_{qo}} = 0. \end{cases} \tag{10}$$

The above equation can be simplified as the matrix form, where

$$\boldsymbol{L} = \begin{bmatrix} 1 & l_{p1} & l_{p2} \\ 1 & l_{q1} & l_{q2} \end{bmatrix} \quad \boldsymbol{\alpha} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \end{bmatrix} \quad \boldsymbol{Y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \tag{11}$$

when $\left(\boldsymbol{L}^T \boldsymbol{L}\right)^{-1}$ exists, $\boldsymbol{\alpha} = \left(\boldsymbol{L}^T \boldsymbol{L}\right)^{-1} \boldsymbol{L}^T \boldsymbol{R}$ can be obtained. Finally, RV can define the error in (7) according to practical experience and get the optimal range of r.

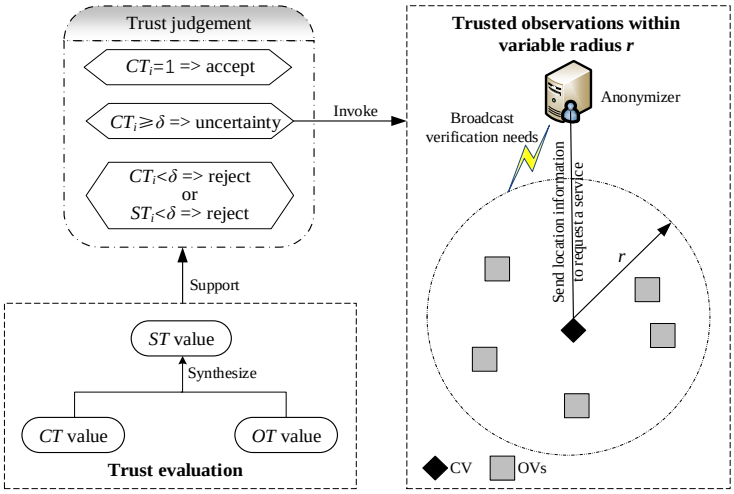


Fig. 4. Architecture of trusted observation within variable radius r.

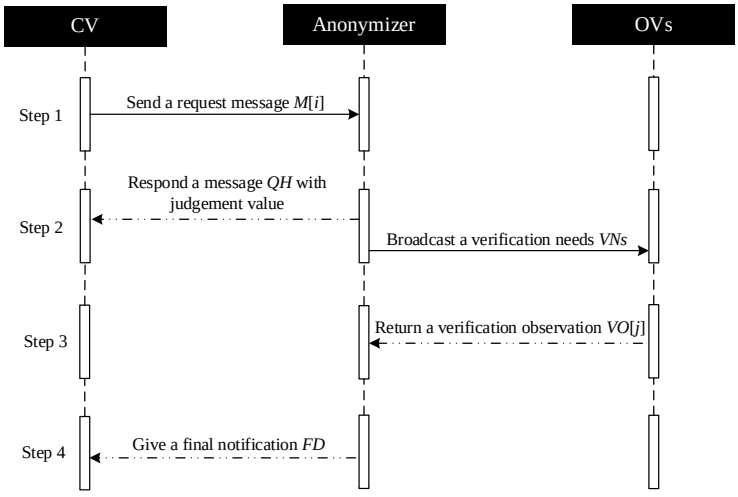


Fig. 5. Execution strategies of trusted observation within variable radius r.

Algorithm 1 Detect false location information

Input： $l_{i,}$, Θ, r, v_{ij}, and d
Output： *result*
1: Initialize *result* = 0.
2: **for** each $V_i \in \Theta$ **do**
3: **if** $CT_i \geq \delta$ **then**
4: **if** $d > r$ and $v_{ij} = 0$ **then**
5: *result* = 0. It means location information l_i is false.
6: **end if**
7: **if** $d \leq r$ and $v_{ij} = 1$ **then**
8: *result* = 1 which means l_i is true.
9: **end if**
10: **end if**
11: **if** $CT_i < \delta$ **then**
12: *result* = 0 which means l_i is false.
13: **end if**
14: **end for**

The architecture of trusted observation within variable radius r is shown as **Fig. 4**, and the process will be invoked under the condition $CT_i \geq \delta$. As shown in **Fig. 5**, this process can be executed with four steps.

Step 1. CV→AN: $M[i] = E_{pk}(PID_i \| l_i \| Sig_{s_i}(l_i))$

A CV (e.g. V_i) sends anonymizer (abbreviated as AN) a message $M[i]$ to obtain judgement value, where l_i is V_i's location information, pk is anonymizer's public key, s_i is V_i's private key, PID_i indicates the pseudonym of V_i.

Step 2. AN→CV: $QH = E_{pi}(j_i \| r)$

AN→OVs: $VNs = E_{pj}(PID_i \| l_i \| Sig_{sk}(l_i) \| ttl_i \| r)$

The anonymizer decrypts $M[i]$ with its private key sk and verifies with V_i's public key.If the verification is valid, the anonymizer sends the judgement value j_i to V_i.

- For $CT_i < \delta$ or $ST_i < \delta$, $j_i = 0$. In this case, the anonymizer rejects V_i's location information.
- For $CT_i \geq \delta$, $j_i = 1$. In this case, the anonymizer broadcasts verification requirements VNs to the adjacent vehicles (OVs) centered on V_i within the variable radius r, where ttl_i is the valid time. All OVs must return observations within the valid time. r can be dynamically adjusted in the light of vehicular regional activity. If there are more vehicles in a vehicular region, the radius r is assigned a smaller value and vice versa.

Step 3. OVs→AN: $VO[j] = E_{pk}(PID_j \| ttl_i \| r)$

The OV (e.g. V_j), assumed as one of OVs, returns an observation result $VO[j] = E_{pk}(PID_j \| ttl_i \| r)$ to the anonymizer. The anonymizer receives the observation $VO[j]$ and measures the distance by the strength of the received signal. The distance remark is denoted as d. If $d \leq r$, it means that OV is within the range, and $d > r$ means not. The verification result of the anonymizer is denoted as v_{ij}. For $d > r$, $v_{ij} = 0$, it means l_i is false location information. For $d \leq r$, $v_{ij} = 1$, it means l_i is real location information.

Step 4. AN→CV: $FD = E_{si}(u_i)$

If $v_{ij} = 1$, the anonymizer gives the final notification FD. Here, u_i is the final decision of the anonymizer and can be given under the (12).

If $u_i = 1$, V_i can get permission from the anonymizer to participate in the cloaking area construction, and vice versa. It is noticed that u_i is based on the majority rule. Let n denote the number of OVs and e_j is the trusted weight of V_j. If $OT_j \geq \delta$, $e_j = 1$, otherwise, if $OT_j < \delta$, $e_j = 0$.

$$u_i = \begin{cases} 1, \ \sum_{j=1}^{n} e_j \cdot v_{ij} > \frac{n}{2}, \\ 0, \ \sum_{j=1}^{n} e_j \cdot v_{ij} \leq \frac{n}{2}. \end{cases} \tag{12}$$

Depending on the tuples (r, d, v_{ij}), Algorithm 1 is designed to detect whether l_i is false or not, where d is the estimated distance between V_i and V_j, v_{ij} is the verification result of V_j, and Θ denotes all the vehicles within the variable radius r.

3.4 Trusted Cloaking Area Construction

To protect RV's real location, the goal is to construct a trusted cloaking area with CVs. Firstly, a candidate set of CVs should be selected through the trust relationship between RV and CVs. We estimate the trust relationship by combining the trust evaluation mechanism and trusted observation with variable radius r method. If the CV's trust value is higher than δ and meets the RV's privacy requirements, it means that the trust relationship between CV and RV is good and the CV could be selected for constructing a cloaking area. The process of trusted cloaking area construction is shown in **Fig. 6**.

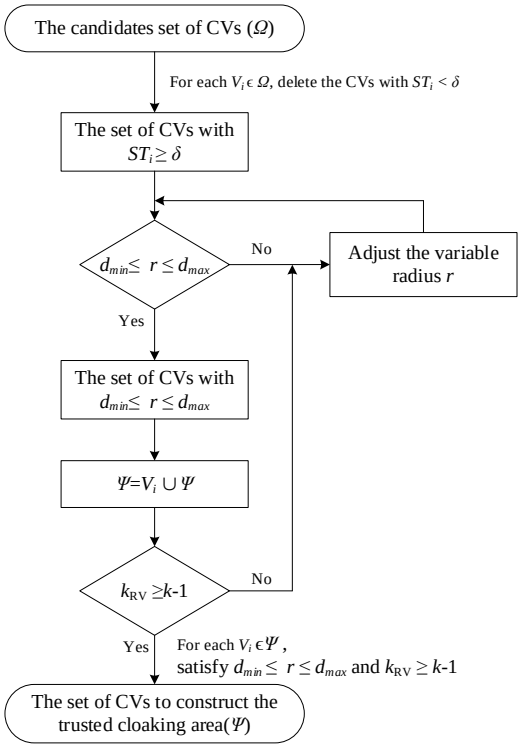


Fig. 6. Process of the trusted cloaking area construction.

Here, Ω denotes the candidate set of CVs. According to the trust value, the anonymizer selects k-1 honest CVs from Ω within the variable radius r. k_{RV} denotes the anonymity of RV.

Ψ indicates the set of CVs that can be used to construct the cloaking area. d_{min} and d_{max} respectively denote the minimum and maximum range that needs to be reached in the cloaking area construction. To meet personalized requirements, RV sets d_{min} and d_{max} based on practical experience. If the variable radius r is out of this range, r should be adjusted according to the following rules.

Rule 1: For $r \leq d_{min}$, the distance between CVs and RV is small. It may lead to privacy leakage. Therefore, r should be recalculated as $r = r + (d_{max}\text{-}d_{min}) / 2$.

Rule 2: For $r > d_{max}$, the distance between CVs and RV is large. It may result in inaccurate service, so r should be set as $r = d_{max}$.

Finally, the anonymous determines whether the cloaking area is successfully constructed by judging the following constraints condition.

$$k_{\mathrm{RV}} \geq k-1 \,\&\&\, d_{\min} \leq r \leq d_{\max} \tag{13}$$

If (13) holds, the anonymizer constructs the trusted cloaking area successfully. Otherwise, the anonymizer adds new CVs according to the rule $r = r + (k - 1 - g)$ min ($|\Delta_1|$, $|\Delta_2|$), where g denotes the number of new CVs, $\Delta_1 = r - d_{max}$ and $\Delta_2 = r - d_{min}$. The construction of a trusted cloaking area is successful until $k_{\mathrm{RV}} + g \geq k - 1$ is satisfied.

3.5 Execution Strategies

By introducing the TCA scheme, we can protect the location privacy of vehicles against location cheating behaviors launched by dishonest CVs with six execution strategies, as shown in **Fig. 7**. The execution strategies can be performed as follows.

Step 1. RV→AN: $R1 = E_{pk}\,(ID_{RSU} \,||\, PID \,||\, l \,||\, Sig_{sv}(l) \,||\, k\}$

The RV sends a request to the trusted third-party anonymizer (abbreviated as AN), where pk is the anonymizer's public key, ID_{RSU} is the RSU closest to RV, sv, l, and k are V's private key, location, and anonymity degree, respectively. To ensure the security of LBS acquisition, a vehicle V needs to register first and apply the irreversible hash function to convert its identity ID into a pseudonym $PID = H(ID)$.

Step 2. AN→RSU: $R2 = E_{PK_{RSU}}(PID \,||\, l \,||\, Sig_{sv}(l) \,||\, k)$

The anonymizer uses its private key sk to decrypt the request message and verify whether $Sig_{sv}(l)$ is a legal signature on l. If not, the anonymizer rejects the request message. Otherwise, the anonymizer sends the trust value request message $R2$ to RSU, where PK_{RSU} is the public key of RSU.

Step 3. RSU→AN: $Q1 = E_{pk}\,(PID \,||\, TD \,||\, \Omega \,||\, per \,||\, k)$

RSU sends trust-related data aggregation to the anonymizer. Here, Ω is the set of candidates of CVs, and TD represents the trust value of RV estimated by RSU. $TD \geq \delta$ means that the permission is gained, and $TD < \delta$ or $per = 0$ means that the permission is rejected, where $0<\delta<1$ is the threshold of trust value.

Step 4.AN→RV: $Q2 = E_{pv}\,(PID \,||\, per)$

RV→AN: $R3 = \{PID, E_{pk}\,(E_{pl}(rc))\}$

If per=1, anonymizer sends response message to RV, where pv is the public key of RV. Then RV sends message $R3$ to the anonymizer. Here, rc is the requested content to LSP, p_l is LSP's public key.

Step 5. AN→LSP: $R4 = \{PID, E_{pl}(rc), \Psi\}$

The anonymizer sends message $R4$ to LSP, where Ψ is the set of CVs for constructing the cloaking area. The CVs in Ψ can take place of RV during LBS requests.

Step 6. LSP→AN: $Q3 = \{PID, E_{pk}(sr, Sig_{sl}(sr))\}$

AN→RV: $Q4 = \{PID, E_{pv}(sr, Sig_{sk}(sr))\}$

LSP obtains *rc* by decrypting *R*4 with private key *sl*, and sends the service result *sr* to the anonymizer. Then, the anonymizer returns *Q*4 to RV. Finally, RV gets *sr* with its private key.

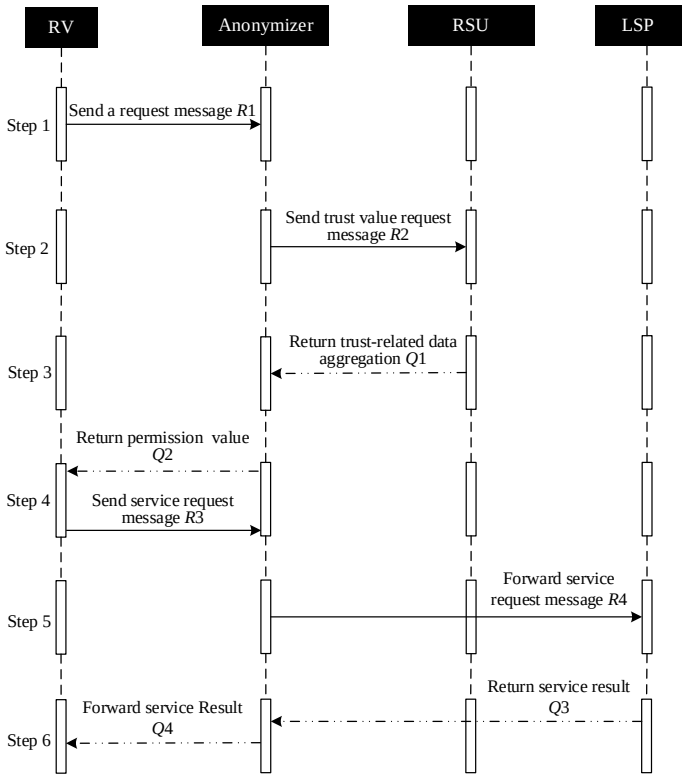


Fig. 7. Execution strategies of the TCA scheme.

4. Security Analysis

The security analysis focuses on how the TCA scheme protects RV's location privacy against dishonest CVs, malicious LSP, and transmission leakage.

4.1 Privacy against Dishonest CVs

Challenge 1: Dishonest CVs may enable the real location of the RV to be guessed by sending fake location information during the process of cloaking area construction.

Lemma 1: TCA is resistant to threats from dishonest CVs.

Proof: In the TCA scheme, only the CVs with higher trust values can be selected to construct the cloaking area, whereas dishonest CVs will be filtered out. So, the TCA scheme can avoid the real location of the RV being guessed.

4.2 Privacy against Malicious LSP

Challenge 2: Malicious LSP may reveal RV's real location by inferring sensitive contents from the request information.

Lemma 2: TCA is resistant to attacks from malicious LSP.

Proof: In the TCA scheme, the anonymizer transfers the trusted cloaking area containing at least *k*-1 CVs to LSP, instead of RV's real location. Hence, LSP could guess RV's true location

with a probability of 1/*k*. LSP can obtain and decrypt the request content *rc* during LBS request. However, due to the policy of dynamic changing pseudonyms of RV, *rc* cannot be relevant to a specific vehicle. To solve a length of *l* hash function inversely, the time complexity is $O(2^{l-1})$. Therefore, there is a computing challenge that LSP should calculate $ID=H^{-1}(PID)$ to get the identity information of the vehicle. That is, LSP is hard to obtain the correct identity information.

4.3 Privacy against Transmission Leakage

Challenge 3: An attacker may obtain RV's request content and LSP's results in the process of transmission.

Lemma 3: TCA is resistant to transmission leakage.

Proof: When the LBS request is sent by RV, the requested content of RV is encrypted by LSP. No one except LSP can decrypt the requested content. When the service result *sr* is provided by LSP, it is signed with the private key of LSP and encrypted with the public key of the anonymizer. Therefore, attackers cannot get any useful information from RV during the transmission.

5. Performance Analysis

5.1 Simulation Setup

To evaluate the effectiveness of the TCA scheme, a performance simulation was conducted. The simulation experiments were implemented with the PyCharm platform and Python language and performed on machines with Intel Core-i5 3.4-GHz, 8 GB RAM, and Windows 10 OS. The simulation elements are shown in **Table 1**.

Table 1. Simulation elements

Parameters	Description	Default
n_v	Number of vehicles	100
k	Degree of anonymity	10~80
cycle	Cycle simulation rounds	200
per	Dishonest CVs (%)	10%~50%
δ	Trust value threshold	(0.2, 0.5, 0.8)
r	The variable radius	200-1000(m)

The simulation was performed in a cycle-based manner. In each cycle simulation round, one vehicle would be selected randomly as the RV, and then *k*-1 CVs were selected to participate in the location privacy protection. The behavior rule followed by honest CVs is to always report real location, while dishonest CVs submit fake location.

5.2 Simulation Result

In this section, we analyze the experimental results of the TCA scheme in terms of malicious responses, detection and false alarm rate, location privacy leakage, and overload. In order to analyze the effectiveness, we make a comparison between TCA scheme and the traditional collaborative *k*-anonymity (C-*k*) construction scheme without a trust mechanism.

5.2.1 Malicious Response

Dishonest CVs forge location information during the cloaking area construction in every cycle. This may result in a significant number of malicious responses that waste network resources. Thus, it is necessary to analyze whether the TCA scheme has an inhibitory effect on malicious responses. The comparison between TCA and C-*k* scheme without trust mechanism is shown in **Fig. 8**. In this simulation, the trust value threshold δ is set as 0.2, 0.5, and 0.8, respectively.

It is obvious that the malicious response of TCA and C-*k* both increase linearly. With the increase of δ, the malicious response decreases sharply. Even when δ = 0.2, the malicious response of the TCA scheme is almost one-fourth of that of the C-*k* scheme. And when δ = 0.5, the malicious response of the TCA scheme is only 22% of the C-*k* scheme. Especially at δ = 0.8, the performance of TCA is the best, and the effect of malicious response is negligible. However, with the growth of δ, the requirement for vehicle honesty is higher, and the construction of a cloaking area is relatively more difficult. Even so, as shown in **Fig. 8**, the TCA has better performance in suppressing malicious responses than the C-*k* scheme, which indicates that the trust mechanism is feasible and important for constructing a cloaking area.

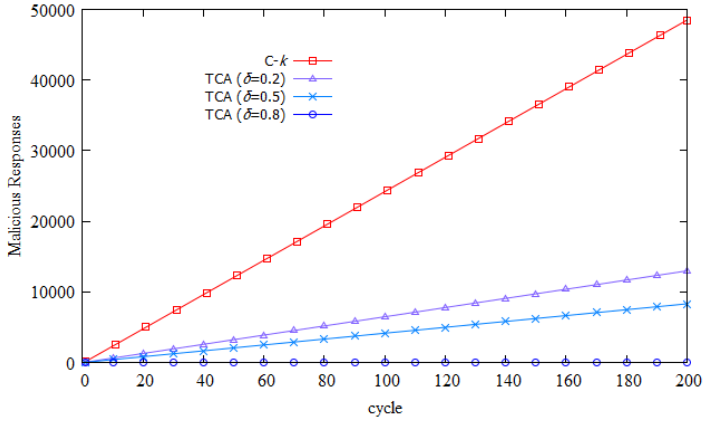
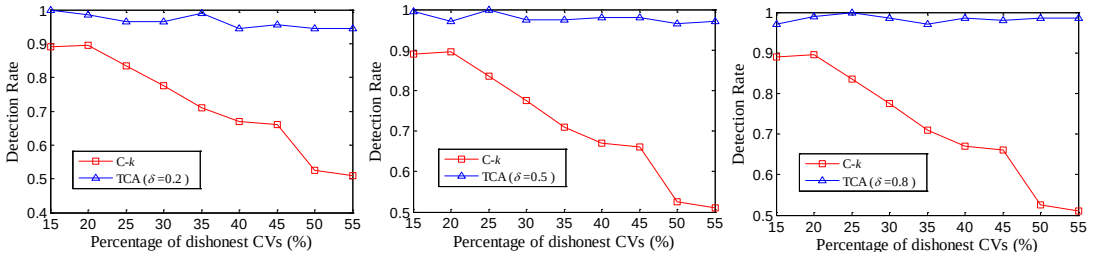


Fig. 8. Comparison of suppressing malicious responses between TCA scheme and C-*k* scheme.

5.2.2 Detection and False Alarm Rate

Generally speaking, less than 10% of dishonest CVs poses a limited threat and over 50% would collapse the entire network. Therefore, the parameter *per* is set between 10% and 50% in the simulations.

As shown in **Fig. 9**, with the percentage of dishonest CVs increasing, the detection rate and false alarm rate of C-*k* increased and decreased linearly, respectively. However, the TCA scheme maintains a high detection rate and a low false alarm rate, and the growth and decline speed is relatively small. Thus, the trust mechanism plays a huge role in improving the performance of the TCA scheme.



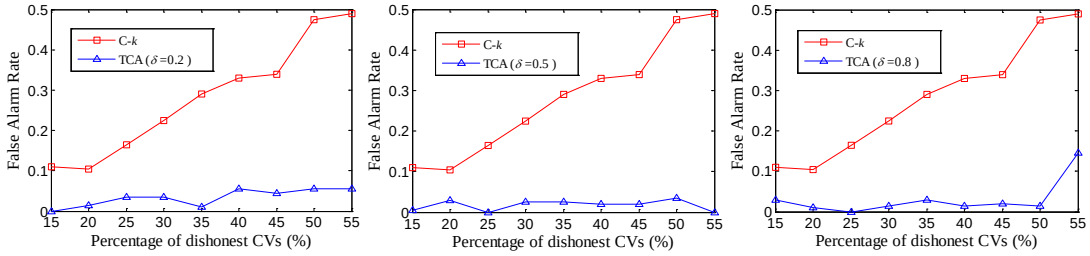


Fig. 9. Comparison of detection and false alarm rate between TCA and traditional C-*k* scheme under the percentage of dishonest CVs. (a), (b) and (c) are the detection rate with δ= 0.2, 0.5, and 0.8, (d), (e) and (f) are the false alarm rate with δ = 0.2, 0.5, and 0.8.

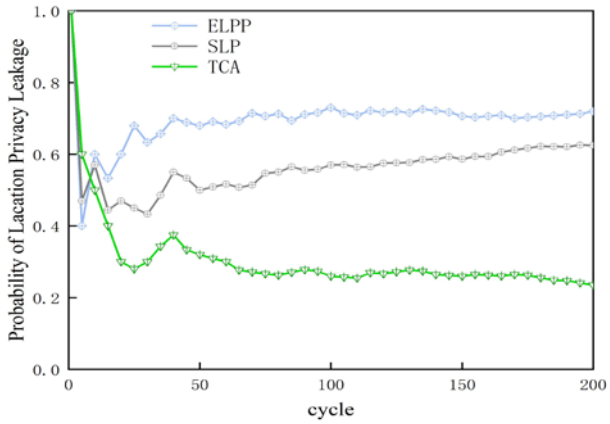


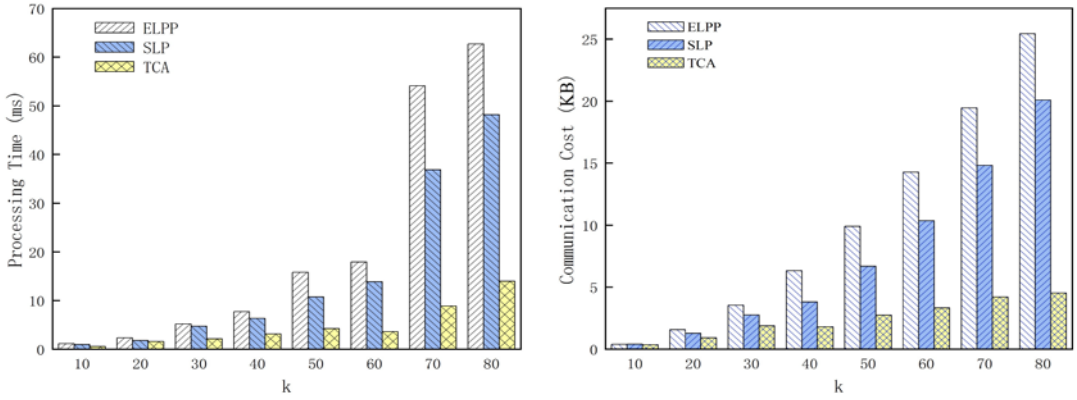
Fig. 10. Comparison of location privacy leakage among the TCA scheme, ELPP scheme and SLP scheme.

5.2.3 Location Privacy Leakage

We also analyze the effect of the TCA scheme on privacy preservation from the perspective of location privacy leakage probability. In the simulation, the percentage of dishonesty is set at 30%. The ELPP scheme [19] is the first to provide enhanced location privacy for the LBS environment, which employs an entity-named function generator to protect location privacy. The SLP scheme [20] selects a trustworthy candidate of the next-hop to assist in constructing the cloaking area without the trusted third party. The comparison among our TCA scheme, the ELPP scheme and the SLP scheme is shown in Fig. 10. With trust mechanism, our TCAC scheme can get the lowest probability of location privacy leakage. It can be found that with the increase of the number of simulations, the leakage probability of the ELPP scheme is stable and always around 0.75, SLP scheme is stable and always around 0.62; and the TCA scheme is stable at around 0.24.

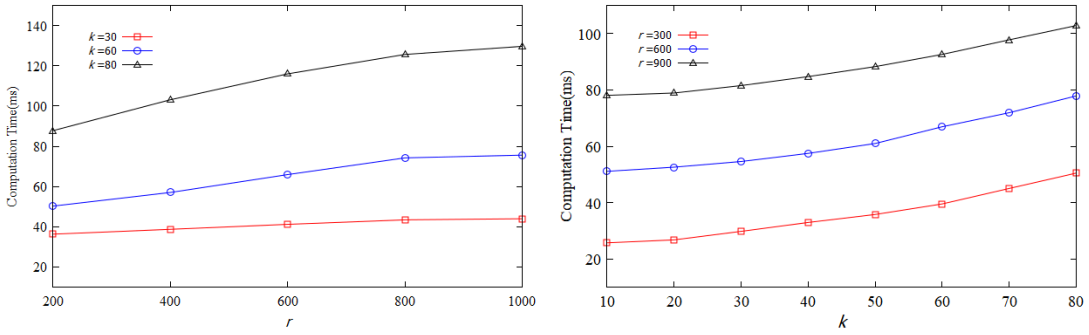
5.2.4 Overload Analysis

As we know, an anonymizer is an important component of the trusted third-party structure. Once the anonymizer is unable to handle a large amount of data, the system will be blocked. Therefore, we analyze the overload that the anonymizer executes TCA scheme in terms of communication and processing time costs. The anonymity degree *k* will be varied from 10 to 80 during the comparison among TCA, SLP and ELPP schemes.



(a) (b)

Fig. 11. Comparison of overload among the TCA scheme, SLP scheme and ELPP scheme.



(a) (b)

Fig. 12. Influence of r and k on computation cost. (a) shows the effect of r on the consumption time when three k values are taken respectively, and (b) shows the effect of k when three r values are taken.

As shown in **Fig. 11**, the processing time and communication cost of the ELPP scheme and SLP scheme increase sharply with k, while both of them increase more smoothly in the TCA scheme. When k = 70, the processing time of ELPP and SLP scheme is about 5 times and 4 times that of TCA scheme, respectively, and the communication cost of ELPP and SLP scheme is about 4 times and 3 times that of TCA scheme, respectively. The reason for this result is that the anonymizer in the ELPP scheme is not only used to build the cloaking area but also to filter query results. In the TCA scheme, the anonymizer only needs to perform several matching and comparison operations during the cloaking area construction.

In addition, the analysis that how the variable radius r and anonymity degree k affect the computation time in the TCA scheme is shown in **Fig. 12**. The computation time increases with the increase of r. This is because the larger the variable radius r is, the larger the search range and the higher processing time will be required. However, it can also be seen from **Fig. 12** that when anonymity degree k is determined, the influence of the variable radius r on the computation time is very limited, while the influence of the change of k value is very large. When k is set as a larger value, such as 80, more CVs will be searched within the same r. In this case, the processing time will be higher.

6. Discussion

Noting that how to efficiently defend against location cheating behaviors launched by dishonest CVs has become a challenging issue to achieve better spatial cloaking, we propose

an edge-assisted Trusted Collaborative Anonymity construction scheme called TCA to protect the location privacy of vehicles by introducing trust mechanism. From the design idea of trusted observations within variable radius *r*, the trust value is not only used to verify false location information from dishonest CVs, but also utilized to select honest CVs to construct the trusted cloaking area by restricting *r*'s search range. To make our major contribution clear, we take the online car hailing as an instance to discuss the possible application of our TCA scheme.

In recent years, online car hailing is a new trend in the field of transportation system, which is the combination of new concepts and traditional industries. It combines information technology and digital taxi, and has changed people's traditional way of taking taxi. Users can book vehicles online anytime and anywhere, which brings great convenience to people's travel.

In order to guarantee the safe and normal operation of online car hailing system, it is assumed that the system should meet the following two conditions:

a) The service provider is reliable and will not disclose the existing information about users and drivers.

b) Drivers are always honest and provide accurate location information for users.

Fig. 13. User fakes a location, leading to the car driving to false location.

Obviously, the operation of online car hailing service is based on reliable location information, which requires users to provide real location information. However, as shown in **Fig. 13**, for some purpose, the user may submit his location beyond the actual location. When the user forges the location without verification, it can disturb the normal operation of online car hailing, resulting in a waste of resources. At present, it is very simple for users to forge the current location by using smart phone applications Locaholic or FakeLocation. Since the online car hailing system can't find out whether the user is using applications such as "fake location", it's difficult to detect the false location.

Fortunately, the TCA scheme can be used to identify the false location of online car hailing system. Each user can play the role of a requester who sends location information to request a specific service, or an observer who returns observations related to verification results. In order to distinguish malicious from honest users, trust mechanism can be used to evaluate the trust value of users. If malicious users always report false location information or wrong observations, they will get lower trust value than honest users. On this basis, the requester trust value (CT) and the observer trust value (OT) can be computed respectively. The comprehensive trust value (ST) is obtained by CT and OT value. Then, the real location can

be verified according to three trust judgments: *J1*, *J2* and *J3*.

7. Conclusion

In this paper, we propose an edge-assisted trusted collaborative anonymity scheme called TCA to protect location privacy in VANETs by introducing the trust mechanism. The TCA scheme is designed in three successive modules: edge-assisted trust value evaluation trusted observation within variable radius r and trusted cloaking area construction. In the TCA scheme, the trust value is not only used to select honest CVs to construct a cloaking area by restricting *r*'s search range but also utilized to verify false location information from dishonest CVs. Assisted by edge computing, RSUs that play the role of edge nodes can rapidly evaluate trust value by means of aggregated trust-related data. The performance analysis indicates that our TCA scheme is resilient to restrain dishonest CVs, and merely requires limited processing time and communication cost. Meanwhile, the simulation results show that our TCA scheme can effectively reduce the location privacy leakage better than the traditional ELPP and SLP scheme. For future works, we are planning to investigate artificial intelligence in driverless vehicles and study privacy protection from the perspective of driverless vehicles. In addition, as the combination of edge computing and artificial intelligence, edge intelligence is also one of the topics that need to be concerned in the future.

References

[1] B. Ghosh, M. T. Asif, J. Dauwels, U. Fastenrath, and H. Guo, "Dynamic prediction of the incident duration using adaptive feature set," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 11, pp. 4019-4031, 2019. Article (CrossRef Link)

[2] C. Tan, S. Bei, Z. Jing, and N. Xiong, "An Atomic Cross-Chain Swap-Based Management System in Vehicular Ad Hoc Networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-14, 2021. Article (CrossRef Link)

[3] S. Chen, A. Fu, J. Shen, S. Yu, H. Wang, and H. Sun, "RNN-DP: A new differential privacy scheme base on Recurrent Neural Network for Dynamic trajectory privacy protection," *Journal of Network and Computer Applications*, vol. 168, pp. 102736, 2020. Article (CrossRef Link)

[4] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: a survey," *IEEE Access*, vol. 8, pp. 131723-131740, 2020. Article (CrossRef Link)

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

[6] X. Zhang, X. Gui, and Z. Wu, "Privacy preservation for location-based services: a Survey," *Journal of Software*, vol. 9, no. 26, pp. 2373-2395, 2015. Article (CrossRef Link)

[7] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, "Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols," *IEEE Trans. Veh. Technol*, vol. 62, no. 4, pp. 1505-1518, 2013. Article (CrossRef Link)

[8] X. Li, M. Mao, H. Liu, J. Ma, and K. Li, "An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism," *Soft Computing*, vol. 21, no. 1, pp. 3907-3917, 2017. Article (CrossRef Link)

[9] S. Zhang, G. Wang, M. Z. A. Bhuiyan, and Q. Liu, "A dual privacy preserving scheme in continuous location-based services," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4191-4200, Oct. 2018. Article (CrossRef Link)

[10] Y. Long, Y. Chen, W. Ren, H. Dou, and N. Xiong, "DePET: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and K-anonymity," *IEEE Access*, vol. 8, pp. 192587-192596, 2020. Article (CrossRef Link)
[11] J. Feng, N. Liu, J. Cao, Y. Zhang, and G. Lu, "Securing traffic-related messages exchange against inside-and-outside collusive attack in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9979-9992, 2019. Article (CrossRef Link)
[12] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of ACM Mobisys*, San Francisco, CA, USA, pp. 31-42, May. 5-8, 2003. Article (CrossRef Link)
[13] H. Yu, G. Li, and J. Wu, "A location-based path privacy protection scheme in Internet of Vehicles," in *Proc. of INFOCOM 2020*, Toronto, ON, Canada, pp. 665-670, 2020. Article (CrossRef Link)
[14] H. Lim and T. Chung, "A Survey on Privacy Problems and Solutions for VANET Based on Network Model," in *Proc. of International Conference on Algorithms and Architectures for Parallel Processing*, pp. 74-88, 2011. Article (CrossRef Link)
[15] B. Abdelwahab, S. Sidi-Mohammed, and M. Samira, "VLPZ: The Vehicular Location Privacy Zone," *Procedia Computer Science*, vol. 83, pp. 369-376, 2016. Article (CrossRef Link)
[16] A. Pingley, N. Zhang, X. Fu, H. Choi, S. Subramaniam, and W. Zhao, "Protection of query privacy for continuous location-based services," in *Proc. of 2011 Proc. INFOCOM*, Shanghai, China, pp. 1710-1718, Apr. 10-15 2011. Article (CrossRef Link)
[17] T. Dargahi, M. Ambrosin, M. Conti, and N. Asokan. "ABAKA: A novel attribute-based k-anonymous collaborative solution for LBSs," *Computer Communications*, vol. 85, pp. 1-13, 2016. Article (CrossRef Link)
[18] Y. Zheng, J. Luo, and T. Zhong, "Service recommendation middleware based on location privacy protection in VANET," *IEEE Access*, vol. 8, pp. 12768-12783, 2020. Article (CrossRef Link)
[19] T. Peng, Q. Liu, and G. Wang, "Enhanced location privacy preserving scheme in location-based services," *IEEE Systems Journal*, vol. 11, no. 1, pp. 219-230, 2017. Article (CrossRef Link)
[20] B. Ying and A. Nayak, "A distributed social-aware location protection method in untrusted vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 6114-6124, 2019. Article (CrossRef Link)
[21] Y. Zhang, W. Tong, and S. Zhong, "On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2528-2541, 2016. Article (CrossRef Link)
[22] Y. Wang, M. Li, S. Luo, Y. Xin, and Y. Yang, "LRM: A Location Recombination Mechanism for Achieving Trajectory k-Anonymity Privacy Protection," *IEEE Access*, vol.7, pp. 182886-182905, 2019. Article (CrossRef Link)
[23] R. Mühlbauer and J. H. Kleinschmidt, "Bring your own reputation: a feasible trust system for vehicular ad hoc networks," *Journal of Sensor Actuator Networks*, vol. 7, no. 3, pp.1-23, Sept. 2018. Article (CrossRef Link)
[24] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559-1574, 2017. Article (CrossRef Link)
[25] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs)," in *Proc. of CogSIMA 2016*, San Diego, CA, USA, Mar.21-25, pp. 1-5, 2016. Article (CrossRef Link)
[26] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495-1505, 2019. Article (CrossRef Link)
[27] A. Jϕsang and R. Ismail, "The beta reputation system," in *Proc. of the 15th Bled Electronic Commence Conference*, pp.1-14, Jun. 17-19 2002.

Wenbo Zhang received the B.S. degree and M.S. degree in Electronic Science and Technology from the Zhengzhou Information Science and Technology Institute, China, in 2005 and 2009, respectively, and the Ph.D. degree in Computer Application Technology from Xi'an High-tech Institute, China, in 2013. He is currently an instructor of the Xi'an University of Posts and Telecommunications, Xi'an. His research interests include wireless communication security and privacy protection.

Lin Chen received her B.S. degree from Chongqing University of Posts and Telecommunications, China, in 2018. She is currently a postgraduate Student at Xi'an University of Posts and Telecommunications. Her main research interests include IoT security, blockchain, and privacy protection.

Hengtao Su is currently pursuing the undergraduation degree with the Xi'an University of Posts and Telecommunications, Xi'an, China. His current research interest includes wireless communication security.

Yin Wang received her B.S. degree from Xi'an University of Posts and Telecommunications, China, in 2018. She is currently a postgraduate Student in Xi'an University of Posts and Telecommunications. Her main research interests include IoT security and privacy protection.

Jingyu Feng is an associate professor and supervisor of M.S. students of Xi'an University of Posts & Telecommunications, China. He received his B.S. degree in Electrical Information Science and Technology from Lanzhou University of Technology, China, in 2006. He received his Ph.D. degree in Information Security from Xidian University, China, in 2011. His research interests include IOT security, privacy protection and trust management.