Blockchain-Enabled Trust Management With Location Privacy Preservation in Vehicular Ad Hoc Networks

Yibing Li, Yangjie Cao, *Member, IEEE*, Yan Zhuang, Jie Li, *Fellow, IEEE*, Gangxin Du, and Jianhuan Chen

***Abstract*—With the advancement of intelligent transportation systems, location-based services (LBSs) have been widely applied in vehicular ad hoc networks (VANETs). LBS utilizes mobile devices to gather vehicle location data, which is then processed using relevant technologies. By combining this data with additional information, LBS offers users personalized and intelligent services. However, providing LBS brings critical security issues related to the exposure of vehicle positions, as well as privacy-preserving problems during the process of collecting location information in VANETs. We propose a distributed trust-based k anonymity scheme to address the aforementioned issues. Our proposed scheme adopts a trust framework among vehicles for various types of LBS. This framework involves a multiparty evaluation and consideration of trust value fluctuations to enhance the efficiency of establishing a reliable k anonymous cloaking region. Furthermore, by leveraging the tamper-proof and decentralized nature of blockchain, we employ a lightweight consortium blockchain to maintain the security of the trustworthiness data throughout the entire model. Extensive security analysis and rigorous experiments have been conducted to demonstrate that the scheme exhibits a certain degree of resilience against attacks on various trust models. Additionally, it has the ability to construct anonymous regions with limited time delay, thereby preserving the privacy of vehicle locations. In comparison to other schemes, it exhibits lower computational complexity and enhanced security.**

***Index Terms*—Blockchain, distributed k-anonymity, location privacy security, trust mechanism, vehicular ad hoc networks (VANETs).**

Manuscript received 28 April 2023; revised 10 September 2023 and 29 October 2023; accepted 19 December 2023. Date of publication 25 January 2024; date of current version 9 July 2024. This work was supported in part by the National Key Research and Development Program of China under Grant 2020YFB1710900; in part by the National Natural Science Foundation of China under Grant 61972092 and Grant 61932014; in part by the Collaborative Innovation Major Project of Zhengzhou under Grant 20XTZX06013; and in part by the Strategic Research and Consulting Project of Chinese Academy of Engineering under Grant 2022HENYB03. *(Corresponding author: Jie Li.)*

Yibing Li is with the School of Computer and Artificial Intelligence, Zhengzhou University, Zhengzhou 450001, China.

Yangjie Cao, Yan Zhuang, Gangxin Du, and Jianhuan Chen are with the School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450003, China (e-mail: caoyj@zzu.edu.cn).

Jie Li is with the School of Cyber Science and Engineering, Zhengzhou University, Zhengzhou 450003, China, and also with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: lijiecs@sjtu.edu.cn).

Digital Object Identifier 10.1109/JIOT.2024.3350694

I. Introduction

ACCORDING to a recent report by the Foresight Industry Research Institute, the global Internet car market size is expected to exceed 1.5 trillion yuan by 2025, and the future market potential of the global Internet car market is enormous [1]. Vehicular ad hoc network (VANET) is a self-organized, open-structured traffic communication network that supports information interaction between vehicles-to-vehicles (V2V) and vehicles-to-roadside (V2R) units. It is an emerging technology that effectively addresses current traffic safety concerns in high-speed mobile environments. As an essential communication foundation for intelligent transportation systems, VANETs are the focus of attention for researchers [2], [3], [4], [5], [6].

Location-based service (LBS) technology plays an important role in the implementation of intelligent vehicle applications. Vehicles transmit their location information to location service providers (LSPs) in order to avail value-added services associated with their geographical position. In VANETs, LBS offers convenience to vehicles, but they also present the potential risk of compromising vehicle location privacy leakage [7]. Additionally, it is important to note that vehicle location information can function as a quasi-identifier, potentially enabling malicious entities to accurately identify individual users by correlating multiple occurrences of vehicle location data with publicly available external information. This situation has the potential to result in a breach of user privacy.

Currently, within the field of location-based privacy protection, the k anonymity algorithm stands as one of the most popular privacy protection algorithms. It is a compromise between the quality of service and user privacy [8], [9], [10] that is selecting at least k vehicle locations and the implementation of obfuscation techniques to ensure that these k vehicle locations are indistinguishable while guaranteeing the available quality of service. It can be seen that the k anonymity algorithm relies on cooperation between vehicles to achieve location privacy protection. Once malicious behavior occurs within vehicles, it can severely disrupt the entire system and lead to the inability to achieve the goal of protecting vehicle locations. The trustworthiness of vehicles is a necessary prerequisite for the effective implementation of the k anonymity algorithm. Therefore, when selecting the k anonymity algorithm to address location privacy issues in

VANETs, we introduce a trust mechanism to address the trust crisis among vehicles when establishing anonymous cloaking regions. While a computationally redundant and complex trust management framework can achieve node trustworthiness, it cannot adapt to the high mobility of VANETs. Vehicles' data and privacy security will be seriously threatened if an effective trust management architecture cannot be established in VANETs. Therefore, it is essential to establish a simple and effective trust management mechanism. We propose a simple and effective trust mechanism for VANETs by refining the meticulous refinement of direct vehicle information assessments and integrating the Bayesian methodology with the beta distribution, a comparatively uncomplicated computational enhancement. Consequently, we have circumvented the intricacies and redundancies of computation that arise as historical data attains a certain threshold.

Blockchain is a data structure or storage technique in the field of information technology. It is characterized by its unique combination of cryptography, peer-to-peer networking, and distributed deployment, which collectively ensure the security of the vehicle's data [11], [12], [13], [14]. Blockchain technology was first introduced by Satoshi Nakamoto in 2008 [15]. Bitcoin's underlying technology has generated significant interest among academics and has emerged as a key catalyst for the development of the Industrial Internet of Things [16], [17]. Blockchain is a tamper-evident, decentralized, consistent, and powerful tool that can effectively address privacy-related concerns and facilitate trust management [18]. Traditional consensus algorithms used in blockchain technology suffer from problems, such as slow processing speed and inefficient resource utilization, making them unsuitable for meeting the needs of VANETs. In recent years, researchers have focused their studies on consensus mechanisms in two aspects: 1) throughput and 2) computational efficiency [19], [20]. Therefore, designing a lightweight consensus algorithm is crucial for implementing blockchain technology in the vehicular networking environment. Leveraging the technical features of blockchain and combining them with lightweight consensus algorithms, we utilize blockchain to record vehicles' historical trust information, thereby ensuring the availability of blockchain in VANETs.

The contributions of this article are then summarized as follows.

1) We develop a novel trust management framework to evaluate the trustworthiness of vehicles within anonymous cloaking regions. This framework takes into account multiparty evaluation results and trust value fluctuations. In essence, our framework is based on an improved Bayesian method that quantifies trustworthiness by utilizing two parameters: a) trust value and b) confidence value. The computation of trust value involves integrating direct evaluations and secondary reputation assessments, thereby enhancing the efficiency of establishing trustworthy k-anonymous cloaking regions.
2) We propose a lightweight PBFT consensus mechanism based on the trust management framework. This mechanism aims to reduce voting time to some extent and is well suited for VANETs, assuming that the majority of roadside units (RSUs) in the network are honest. We employ RSUs to store historical trustworthiness on the blockchain, guaranteeing the trustworthiness of information, whether it is on-chain or off-chain.
3) Building upon the aforementioned, we design an anonymous cloaking region construction scheme to achieve the blurring of trusted vehicle locations within the same region. Our scheme comprises four distinct stages, including the transmission of requests by requester vehicles, among others. The primary objective of this scheme is to facilitate the provision of LBSs to vehicles while preserving location privacy.
4) We provide security analysis and conduct extensive experiments to demonstrate the effectiveness and security of the proposed scheme. This measure guarantees the protection of vehicle location privacy for a limited time frame. By comparing our scheme with other existing approaches, we have identified several advantages that it possesses.

The remainder of this article is organized as follows. In Section II, we present the related work. In Section III, we introduce the system architecture and problem definition. In Section IV, we describe the proposed trust management framework, which includes behavioral evaluation of vehicles, trust mechanism evaluation, and the k-anonymous cloaking region. In Section V, we analyze the security of the proposed model. In Section VI, we experimentally verify the performance of the proposed model in terms of effectiveness, and Section VII concludes this article.

II. Related Work

A. K-Anonymity Algorithms

Samarati first proposed the k-anonymity algorithm, as mentioned by Sweeney [21]. In simple terms, the k-anonymity algorithm requires that a certain number (at least $k-1$) of quasi-indistinguishable records exist in the published data in order to protect the privacy of the data. The k-anonymity algorithm can be divided into two categories: 1) centralized and 2) distributed. The centralized algorithm involves the inclusion of a trusted third party between the mobile user and the LBS. This third party is responsible for processing and querying the private data. Spatiotemporal is a typically centralized algorithm [22], [23]. The core idea is that the precise spatiotemporal information is no longer present in the query request uploaded by the user to the application server. Instead, it is replaced by a coarse-grained anonymous region formed by combining k spatiotemporally user locations. However, in practice, it is difficult to find a trusted third party. If an attacker manages to capture the third party, the privacy of all users will be compromised. Unlike the centralized algorithm, the distributed algorithm does not rely on a trusted third party but instead relies on the collaboration between users to form k-anonymity sets. In this approach, distributed servers work together to build anonymous cloaking regions. Gedik and Liu [24] proposed the first distributed k-anonymity algorithm in 2007, which addressed the limitation

of centralized algorithms. Sun et al. [25] distinguished between sensitive and common locations of users by defining location labels to reduce computation. At the same time, Ghinita et al. [26] proposed a peer-to-peer privacy-preserving query service algorithm called P^4QS. It addresses the issue that in specific areas with low user activity, the system has to wait passively until it receives at least $k-1$ collaborators to construct anonymous cloaking regions. This is achieved by enabling the generation of false locations. Luo et al. [27] and Li et al. [28] used the Dirichlet distribution to construct a trust management mechanism in the *k*-anonymity algorithm. However, as the historical trust data accumulates, the computational cost will increase.

B. Trust Management Models in VANETs

Mahmoud and Shen [29] developed a trust-based navigation scheme for trust management by integrating a trust mechanism with a system of rewards and punishments. However, the central server of a centralized trust management system cannot handle single points of failure and the massive amounts of data in intelligent transportation systems [30], [31], [32], [33]. Next, a significant amount of research [34] on distributed trust management models began on VANETs. In [35], Sybil attackers who simulated "ghost vehicles" on the road were effectively suppressed through cooperation among neighboring vehicles. Minhas et al. [36] developed a framework that integrates different dimensions of role-based, experience-based, and majority-based trust. Raya et al. [37] argued that previous studies have primarily concentrated on an entity-oriented framework for trust values, overlooking the importance of assessing the reliability of these values. They proposed the establishment of a data-oriented distributed trust management system. It combines multiple related but conflicting evaluation metrics that are highly resistant to attackers and steadily converge to the correct decision. Yang et al. [38] proposed the first blockchain-based distributed trust management system. However, there are problems, such as the adoption of proof-of-work and proof-of-stake consensus mechanisms, which will consume a significant amount of computational time. The network structure of the vehicular network is complex. Luo et al. [27] maintained two blockchains: one for storing query requests and the other for storing vehicle certificates. This approach sacrifices some computation time but ensures vehicle location privacy to a certain extent. Liu et al. [39], [40] proposed the reputation update scheme PPRU for privacy protection in cloud-assisted vehicular networks and introduced the trust management and privacy protection scheme BTMPP for emergency message dissemination in vehicular networks.

C. Beta Distribution

In common approaches, mutual trust among vehicles is calculated using a modified Bayesian method. Here, we initially introduce the standard Bayesian approach. According to the Bayesian method, the comprehension of a phenomenon is partially derived from prior knowledge. At the same time, an additional facet is contingent upon the present assimilation of novel data, thereby resulting in a renewed comprehension. By engaging in a continuous process of acquiring new information, our comprehension and knowledge steadily enhance over time

$$P(\text{Belief}|\text{Observation}) = \frac{P(\text{Observation}|\text{Belief}) * P(\text{Belief})}{\text{NormalizingConstant}} \tag{1}$$

where $p(Belief)$ is the prior probability, $p(Observation|Belief)$ is the likelihood function, and $p(Belief|Observation)$ is the posterior probability.

We use the Beta distribution to represent the belief probability, denoted as $p(Belief)$. Therefore, θ can be assumed to follow a beta distribution, which is provided as follows:

$$\text{Beta}(\theta, \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \tag{2}$$

here, $\alpha \geq 0$ denotes the magnitude of benign behaviors and $\beta \geq 0$ the magnitude of malicious behaviors. Initially, θ is uniformly distributed between 0 and 1, which can be described as Beta(q, 1, 1). Then, if there are s observations with normal behaviors and f observations with misbehavior, the posterior distribution is updated by $\alpha = \alpha + s$ and $\beta = \beta + f$. As a standard Bayesian inference method, the Beta distribution has the characteristic that its prior and posterior distributions are conjugate. We incorporate it into the trust-level calculation process to predict vehicle behavior.

TABLE I
PARAMETERS USED IN THE PROGRAM

Notation	Definition
f	The maximum number of malicious vehicles in the system
p_s	The rationality of query frequency space in the area s_m
$\triangle f$	The default maximum tolerance difference
p_f	The reasonability of query frequency
p_r	Evaluation of the cooperator vehicle behavior
η_r	Balance parameter
l_r	The rationality of the location information
d_c	The relative distance between the cooperative vehicle and the RSU
l_a	authenticity of location information
$t_r - t_q$	The current propagation delay
$trans(\triangle t_r)$	The expected propagation delay
p_r	Evaluation the requester vehicle behavior
η_c	Balance parameter
w_1,w_2	Adjusting parameter
CT	The current time
t_{last}	The time point at which the most recent update was executed
t_{ij}	True value
s_{ij}	Confidence value
θ	Uniformly distributed
T_{ij}	Trustworthiness

III. SYSTEM ARCHITECTURE

Before discussing the details of the proposed system, we present in Table I the main abbreviations and variable names that we use throughout this article.

In VANETs, we employ an approach that involves constructing anonymous cloaking regions to protect the privacy of vehicle locations while still providing LBSs for vehicles. Additionally, establishing trusted relationships among vehicles is a crucial prerequisite for creating effective anonymous cloaking regions. Throughout this process, a lightweight blockchain and its consensus mechanism play a pivotal role

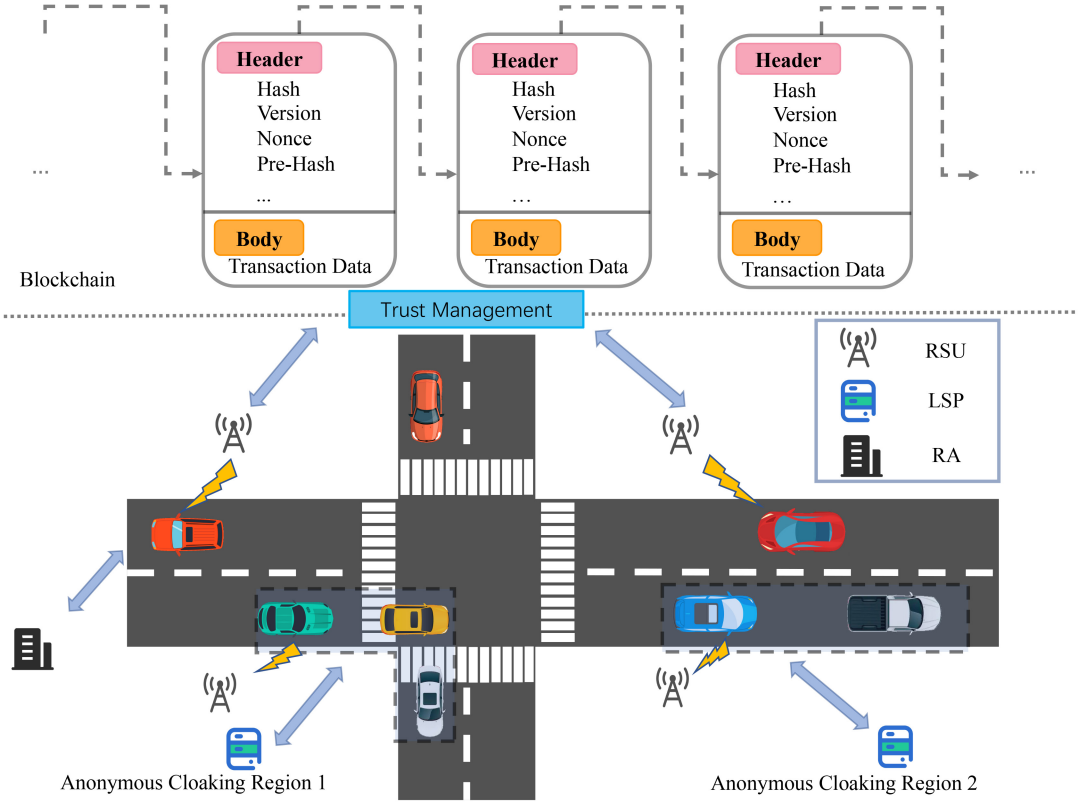

Fig. 1. System architecture.

in ensuring data security. Therefore, as shown in Fig. 1, our system architecture consists of the lightweight blockchain, the trust mechanism, and the LBS.

A. Lightweight Blockchain

Generally, there are three types of blockchains: 1) public blockchain; 2) consortium blockchain; and 3) private blockchain. In this article, there is a significant amount of public data circulation closely related to the driving safety of vehicles in the VANET environment. Compared to the public blockchain, the consortium blockchain requires the "permission" of the coalition members in terms of joining mechanisms and consensus rules. The participating parties can negotiate to reach a consensus and modify the consensus rules, selectively applying them. Consortium blockchain is more suitable for supporting scenarios with relatively complex business processes based on the consensus rules reached through multiparty cooperation. Therefore, we use the consortium blockchain. In this article, we assume that the majority of RSUs are honest. The lightweight blockchain comprises connected blocks, where the block header encapsulates the current version number, the address of the previous block, a timestamp, and other information. The block body mainly records event information. We treat the construction of an anonymous cloaking region as a transaction and have the RSU record its historical trust information on the blockchain to encourage honest behavior by requester and cooperator vehicles. The complete life cycle of a transaction includes transaction generation, transaction propagation, block creation, block validation, and blockchain updates. All transactions must be stored on the blockchain.

Given the aforementioned premise, the lightweight practical Byzantine fault tolerance (LPBFT) consensus algorithm (Algorithm 1) is utilized to ensure the suitability of the model for the high liquidity of VANETs. Compared to the traditional PBFT consensus algorithm, which necessitates the reception of $2f+1$ ready and commit messages from distinct nodes in order to proceed to the reply phase. The LPBFT consensus algorithm requires a minimum of $f+1$ votes, where f represents the maximum number of malicious vehicles within the system. The LPBFT consensus algorithm employs a random selection process to determine the primary node. To optimize the operational efficiency of the LPBFT consensus algorithm, the designated miner has been bestowed with triple accounting privileges. In the subsequent execution of the consensus algorithm, the phase involving the selection of miners is omitted.

B. Trust Management Mechanism

In previous research, many scholars have primarily focused on developing more precise and complex trust mechanisms, without adequately considering their suitability for the VANET environment. In a real-time demanding VANET environment, we typically expect the computation to be simple and efficient. Therefore, we propose a new trust management framework.

C. Location-Based Services

LBSs include the registration authority (RA), RSUs, LSPs, and vehicles. As shown in Fig. 1, we have delineated two

Algorithm 1 LPBFT Consensus Algorithm

Miner Selection
for *each RSU* **do**
  miner ← select an RSU at random
end for
Transaction Generation
transaction ← constructing an anonymous cloaking region
transaction ← update the trust value
Transaction Propagation
RSU ← get transaction from vehicles
Block Generation
block ← miner packs transactions into a block
Block Verification
for *each RSU* **do**
  result ← RSU verifies the block
  if *result* == *true* **then**
    count ++
  end if
end for
if *count* >= $f + 1$ **then**
  blockchain ← miner adds the block to the blockchain
else
  return block generation
end if

distinct anonymous cloaking regions, each offering different services to cater to varying LBS requirements. Here, we categorize LBSs into two types: 1) direction-specific services, such as obtaining information about conditions ahead and 2) nondirectional services, such as searching for nearby gas stations. The purpose of differentiating anonymous cloaking regions is to address the varying methods used to calculate trust values for vehicles in various scenarios. The specific variations in calculation methods are extensively elaborated upon in Section IV.

1) Registration Authority: The RA is responsible for managing vehicle certificates, which includes registration, updating, and revocation of certificates. The RA also provides proof of the existence of certificates. When it is impossible to determine whether a vehicle's behavior is malicious, the RA can initiate dispute arbitration and track the malicious vehicles.

2) Roadside Units: We assume that RSUs are extensively deployed on both sides of the roads. This not only ensures that vehicles can access the required data at any time, but also allows them to promptly record new trust information in the blockchain. Through the use of RSUs in the vehicular network, a blockchain core network is formed, with multiple encoded blocks stored in the RSUs. These collectively establish an extensive, decentralized database. Even if a vehicle departs from the communication range of the RSU from which it sent a query request due to high-speed movement, the vehicle can still communicate with any other RSU to obtain the query results. RSUs receive query requests from vehicles, construct anonymous cloaking regions, and send them to the LSP. Finally, they return the query results to the requester vehicles. Additionally, they are also responsible for maintaining the corresponding blockchain.

3) Location-Based Service Provider: After receiving the anonymous cloaking region and the query content, the LSP proceeds to retrieve the pertinent information from the database and subsequently returns the obtained results.

IV. Proposed Trust Management Framework

A. Evaluation of Vehicle's Behaviors

In order to prevent the leakage of vehicle location privacy during the construction of the anonymous cloaking region, after verifying the vehicle identity, we need to assess the trust of the vehicle based on its current behavior. The requester vehicle requests the RSU to obtain information about the cooperator vehicle that meets the conditions based on its own requirements. The cooperator vehicle provides its geographic location to the RSU in response to the request from the requester vehicle that meets the specified conditions. Due to the different behavior patterns of requester vehicles and cooperator vehicles, the malicious behavior is also different. The malicious requester vehicle sends numerous invalid queries to overwhelm the computational resources of RSU and LSP, resulting in system crashes. Furthermore, the malicious cooperator vehicle incorrectly reports location information, resulting in the mixing of the anonymous cloaking region with the malicious vehicle. This, in turn, causes the failure of the correct construction of the anonymous cloaking region.

Thus, we evaluate the current trust value of the requester vehicle in terms of querying reasonability from space and frequency. Additionally, we evaluate the current trust value of the cooperator vehicle based on the rationality and authenticity of its location information.

1) Querying Reasonability From Space: The existing literature has indicated that the likelihood of users initiating LBS queries varies depending on their locations. In their scheme, they divided the entire location map into $n \times n$ cells with equal size $\{s_1, s_2, \ldots, s_m, \ldots, s_{n*n}\}$, corresponding to query frequencies $\{f_1, f_2, \ldots, f_m, \ldots, f_{n*n}\}$. According to the previous query history, each cell is defined to have a query probability that is accessible to all users. Then define the rationality of the query frequency space p_s

$$p_s = 1 - \frac{|f_m - f_{mh}|}{\Delta f} \tag{3}$$

where $|f_m - f_{mh}|$ represents the difference between the current query frequency of the vehicle and the historical query frequency in the area s_m, and Δf represents the default maximum tolerance difference.

2) Querying Reasonability From Frequency: The researchers indicated that the query behaviors of users in LBS exhibit certain regularity. To prevent malicious vehicles from sending a large number of query requests in a short period and conducting differential attacks on the system, we use P_t to represent the reasonableness of P_r's querying frequency. In real life, the frequency of queries varies throughout the day. To account for this, we divide the day into n time periods, denoted as $\{t_1, t_2, \ldots, t_n\}$. Each time period corresponds to different

query times in the corresponding period $\{\mu_1, \mu_2, \ldots, \mu_n\}$, the reasonability of query frequency is

$$p_f = \begin{cases} e^{-|q_k - \mu_k|}, & q_k > \mu_k \\ 1, & q_k \leq \mu_k \end{cases} \tag{4}$$

where $|q_k - \mu_k|$ indicates the difference between the number of query times and the number of historical query times in the t_k period.

We balance querying reasonability from space and reasonability from frequency by η_r, and then we can get the following results for v_r behavior evaluation:

$$p_r = \eta_r p_s + (1 - \eta_r) p_f. \tag{5}$$

3) Rationality of Location Information: Here, we categorize LBSs into two types: 1) services that differentiate between directions, such as the service that provides information about the status of the car ahead and 2) services that do not differentiate between directions, such as the service that allows you to check for nearby gas stations. For the former, if the requester vehicle travels in a direction different from the specified direction, we consider it malicious since it is required to travel in the same direction. We use $l_r \in \{-1, 0, 1\}$ to indicate the rationality of the location information. When the value of l_r is 1, 0, and -1, it represents reasonable, uncertain, and unreasonable, respectively. The vehicle must be located near the RSU in the corresponding area. The vehicle is considered malicious if the distance between the vehicle and the RSU in the specified area exceeds a certain threshold. We use l_r to denote the rationality of the location information under the service type that does not distinguish the direction

$$l_r = \begin{cases} 1 - \frac{\text{DistanceMax} - d_c}{\text{DistanceMax}}, & \text{d}_c \leq \text{DistanceMax} \\ 0, & \text{d}_c > \text{DistanceMax} \end{cases} \tag{6}$$

where d_c represents the relative distance between the cooperative vehicle and the RSU. Additionally, DistanceMax denotes the maximum allowable value for the relative distance between the vehicle and the RSU that can be tolerated.

4) Authenticity of Location Information: After receiving a request from the requester, if the vehicle is deemed malicious and intentionally provides a false location to RSU, it will require additional time for the malicious vehicle to generate a suitable false location. Subsequently, the response time of the cooperative vehicle is utilized to assess the authenticity of the location information. In this case, the rationality value of the location information l_a is

$$\begin{aligned} l_a = &-\left|\left(t_r - t_q\right) - \text{trans}(\Delta t_r)\right| \\ &+ \cos\left|\left(t_r - t_q\right) - \text{trans}(\Delta t_r)\right| \end{aligned} \tag{7}$$

where $t_r - t_q$ denotes the current propagation delay, and $\text{trans}(\Delta t_r)$ denotes the expected propagation delay.

In summary, the parameter η_c is used to achieve a balanced equilibrium between the rationality of location information and the authenticity of location information. This allows us to calculate the current evaluation result for η_c, which is limited to the range of [0, 1] for the requester vehicle

$$p_r = \eta_c l_r + (1 - \eta_c) l_a. \tag{8}$$

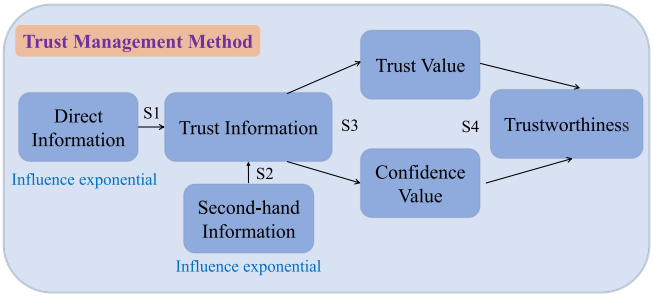

Fig. 2. Proposed trust management framework.

B. Proposed Trust Management Model

Inspired by Li et al. [41], we propose a new trust management model. In the proposed scheme, we evaluate the trustworthiness of vehicles in order to identify malicious vehicles while efficiently creating the anonymous cloaking region. In the standard Bayesian scheme, each new observation is given equal weight in the update, regardless of its occurrence or provider. Two types of information can influence a node's opinion about observations: 1) direct information and 2) indirect information. In our scheme, two types of observations affect vehicle assessment: direct and indirect information. In this process, we should follow two principles. First, the longer the past vehicle behavior, the less influence it should have on the current trust evaluation. Second, information from second-hand sources should have less impact than information from direct sources. Based on the above assumptions, we propose an improved Bayes-based trust mechanism.

Here, we provide the framework of the proposed framework as shown in Fig. 2, which consists of four steps, S1, S2, S3, and S4, as described below. From this framework, we can see that the proposed framework meets the requirements mentioned above.

1) Step 1: Update initial trust through direct information. Historical information serves as the initial trust, and the initial trust is updated through direct information. In this step, the old observations are terminated using the exponential decline method of influence. The use of bias tests to control the true value of direct trust implies that there is a veto against some malicious behavior. Let $s \in \{1, 0\}$ be the set of symbols for observations. That is, if the observation is normal behavior, $s = 1$; otherwise, $s = 0$. Therefore, using the evaluation of vehicle i on vehicle j as an example, the posterior distribution is updated as follows:

$$\begin{aligned} \alpha_{ij}{}' &= w_1^{CT - t_{\text{last}}} * \left(\alpha_{ij}\right) + s_{ij}{}' \\ \beta_{ij}{}' &= w_1^{CT - t_{\text{last}}} * \left(\beta_{ij}\right) + 1 - s_{ij}{}' \end{aligned} \tag{9}$$

where $w_1 \in (0, 1)$ is the adjusting parameter, CT represents the current time, while t_{last} refers to the time point at which the most recent update was executed. The variable $w_1^{CT - t_{\text{last}}}$ denotes the exponential decay factor utilized to expire previous observations partly.

2) Step 2: Distribution and adoption of second-hand information. Assuming that neighboring vehicles are defined as vehicles that have jointly constructed an anonymous cloaking region, second-hand information distribution involves

the network-wide distribution of direct information from all neighboring vehicles participating in bidding after the construction of an anonymous cloaking region. Second-hand information adoption involves randomly selecting n previously neighboring vehicles, summarizing their average results as new information, and using it to update existing knowledge. In this step, we follow the principle of exponential decay, which states that the impact of second-hand information on current results diminishes over time

$$\alpha_{kj} = w_1^{CT-t_{\text{last}}} * \left(\alpha_{kj}\right) + s_{kj}$$
$$\beta_{kj} = w_1^{CT-t_{\text{last}}} * \left(\beta_{kj}\right) + 1 - s_{kj}. \tag{10}$$

Assuming vehicle i takes into account the viewpoints of n neighboring vehicles of vehicle j, the resulting distribution can be expressed as

$$\alpha_{ij} = \alpha_{ij}{}' + \frac{w_2}{n}\left(\sum_{i=1}^{n} \alpha_{k_n j}\right)$$
$$\beta_{ij} = \beta_{ij}{}' + \frac{w_2}{n}\left(\sum_{i=1}^{n} \beta_{k_n j}\right) \tag{11}$$

where $w_2 \in (0, 1)$ is the adjusting parameter.

3) Step 3: Evaluate the trust value and confidence value. We update the direct and second-hand information of this evaluation based on the first two steps. In this step, to achieve objectivity, we quantify the evaluation into two parameters: trust value and confidence value. The behavior of a vehicle follows the Beta probability density function distribution. The trust value t_{ij} represents the trust estimation of vehicle i toward vehicle j. It is calculated based on the expectation of the Beta probability density function distribution. The confidence value s_{ij} is used to evaluate the accuracy of the trust value and is expressed by its standard deviation

$$t_{ij} = E\big(\text{Beta}(\theta, \alpha_{ij}, \beta_{ij})\big) = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}. \tag{12}$$

High trust indicates that the vehicle's performance meets the requirements for this round. The high confidence value represents the accuracy of the calculated trust value, which can be described as the quality of the trust opinion

$$s_{ij} = \sqrt{\frac{\alpha_{ij}\beta_{ij}}{\left(\alpha_{ij} + \beta_{ij}\right)^2\left(\alpha_{ij} + \beta_{ij} + 1\right)}}. \tag{13}$$

4) Step 4: Evaluate trustworthiness. We will assign weights to the trust and confidence values in step 3 based on different situations, and then combine them to create the final evaluation index, trustworthiness T_{ij}

$$T_{ij} = 1 - \frac{\sqrt{\frac{(t_{ij}-1)^2}{x^2} + \frac{(c_{ij}-1)^2}{y^2}}}{\sqrt{\frac{1}{x^2} + \frac{1}{y^2}}} \tag{14}$$

the values of x and y are constants. The research in [15] shows that the most appropriate values for the trustworthiness parameters are $x = \sqrt{2}$, $y = \sqrt{9}$. Therefore, in this article, we also set x to be $\sqrt{2}$ and y to be $\sqrt{9}$.

Algorithm 2 K-Anonymous Cloaking Region Construction

$Req = < p_{r_{id}}, t_r, Cer_{p_{r_{id}}}, I_r, Num(\text{ trans }),$
$sig_{SK-p_{r_{id}}}\left(t_r \left\| Cer_{p_{r_{id}}} \right\| I_r\right) >$
V_r send Req to nearby RSU
if *RSU check sig* ! = *true or RSU check cer* ! = *legal* **then**
  Return Req identity information error warning
else
  RSU send Req to V_c
  if V_c check V_r identity != legal and trustworthiness of V_r < *Threshold* **then**
    return error warning
  else
    $Res =< p_{c_{id}}, p_{r_{id}}, t_c, I_c, sigg_{SK-p_{r_{id}}}(t_c \| I_c) >$
    V_c send Res to V_r
    if V_r check V_c identity != legal **then**
      return error
    else
      add V_c to cloaking region
      $count \leftarrow get\ k-1\ V_c$
      if $count < k-1$ **then**
        generate virtual vehicles
      end if
    end if
  end if
end if
RSU $\leftarrow V_c, V_r$ issue result
LSP $\leftarrow$ get query request from RSU
LSP return query content
RSU issue the result to V_r

C. Anonymous Cloaking Region Construction

As shown in Fig. 3, establishing a k-anonymous cloaking region (Algorithm 2) is an important measure for protecting the location privacy of vehicles. The process is as follows.

1) Step 1: Requester vehicles to send requests. When a requester vehicle initiates an LBS query, it first broadcasts the request to the RSU

$$\text{Req} = \langle p_{r_{id}}, t_r, \text{Cer}_{r_{id}}, \text{Num(trans)}$$
$$\text{sig}_{SK-p_{r_{id}}}\left(t_r || p_{r_{id}} || I_r\right)\rangle \tag{15}$$

where $p_{r_{id}}$ represents the pseudonym of the requester vehicle, t_r denotes the timestamp when the requester initiates the request, $\text{Cer}_{r_{id}}$ signifies the public-key certificate of the requester vehicle, and Num(trans) indicates the transaction number. According to the historical trust information of the vehicle, the content of the query initiated by the requester vehicle can be retrieved on the RSU. I_r contains information such as the type of LBSs to be requested by the vehicle. The type of LBS to be requested by the vehicle and other information, $\text{sig}_{SK-p_{r_{id}}}(t_r||p_{r_{id}}||I_r)$ is the content signed using the private key of the requester vehicle, and "||" indicates the union operation.

2) Step 2: Validate the request and assess the trustworthiness of the requester. First, the signature is verified by

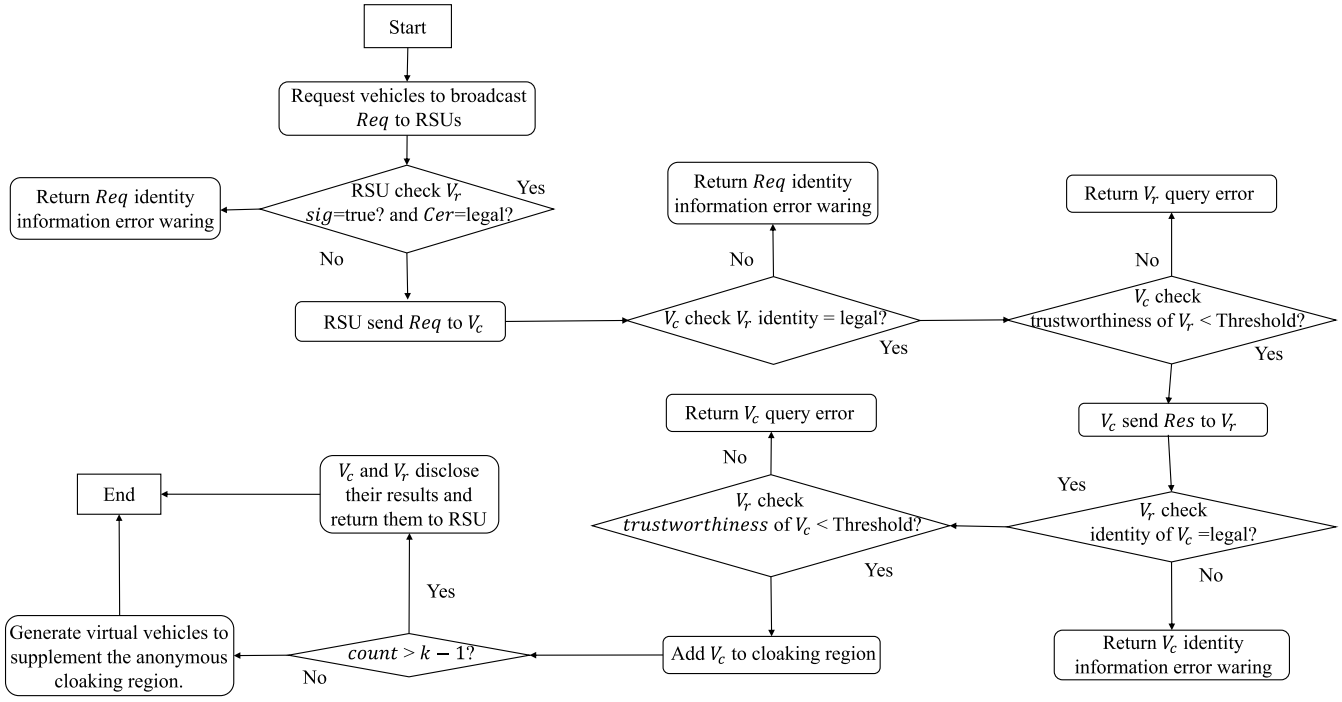

Fig. 3. Anonymous cloaking region construction process diagram.

the nearest RSU, followed by the validation of the requester vehicle's certificate. If the validation fails, a warning is sent to the requester vehicle indicating an error in the identity information. If the validation succeeds, the RSU sends the request to the cooperator vehicles, which will then validate the identity of the requester vehicle and calculate its trustworthiness. If the trustworthiness is below the set threshold, the vehicle is not considered, and a warning is sent to the requester vehicle indicating a query error. Otherwise, proceed to the next step.

3) Step 3: Cooperator vehicles send cooperative responses, and the requester vehicle verifies the identity of the cooperator vehicles and computes their trustworthiness. In this step, the cooperator vehicles submit their cooperative responses to the requester vehicle, which then validates the identity of the cooperator vehicles and computes their trustworthiness

$$\text{Res} = \langle p_{c_{id}}, t_c, \text{sig}_{SK-p_{c_{id}}}(t_c||I_c)\rangle \tag{16}$$

where $p_{c_{id}}$ represents the pseudonym of the partner vehicle, t_c denotes the timestamp when the requester initiates the response, I_c indicates the response content, and $\text{sig}_{SK-p_{c_{id}}}(t_c||I_c)$ represents the content that is signed using the private key of the partner vehicle. Next, similar to the second step, the requester vehicle verifies the identity of the cooperator vehicles and computes their trustworthiness. If the cooperator vehicle are not met, a response error is returned. Otherwise, the cooperator is selected as one of the candidate vehicles for the k-anonymity cloaking region and proceeds to the next step. Then, $k-1$ cooperator vehicles are randomly selected from the eligible candidate vehicles. If the number of eligible cooperator vehicles is less than $k-1$, virtual vehicles will be generated to supplement the k-anonymity cloaking region.

4) Step 4: The requester vehicle and the cooperator vehicles share their results and send them back to the RSU. The RSU then sends the final query request to the LSP. Once the LSP returns the query results, the RSU distributes them to the requester vehicle and the selected cooperator vehicles.

It should be noted that once a vehicle's trustworthiness is calculated, it will be sent back returned to the RSU and updated on the blockchain, regardless of whether it successfully forms a k-anonymity cloaking region. Furthermore, there is no direct communication between vehicles, which to some extent ensures the privacy of vehicles. During the trust evaluation process, we validate biases in the vehicle's trust assessment. If a biased evaluation that exceeds cognitive limitations, we will disregard that evaluation.

Regarding the calculation cost and complexity of proposing a solution, will primarily focus on discuss the computational complexity of vehicles. The construction process involves signing, verifying, encrypting, and decrypting. The corresponding complexities are defined as $O(Sig)$, $O(Ver)$, $O(Enc)$, and $O(Dec)$. If there are z collaborative vehicles in the network, the time complexity for requesting vehicles is $(z+1)*O(Sig)+z*O(Ver)+z*O(Dec)+z*O(1)=O(Sig)+O(Ver)+O(Dec)$. For collaborative vehicles that do not provide a response, the calculation complexity is $O(Sig)+O(Ver)+O(1)=O(Sig)+O(Ver)$. For collaborative vehicles that require cooperation, the calculation complexity is $2*O(Sig)+O(Ver)+O(Enc)+O(1)=O(Sig)+O(Ver)+O(Enc)$.

V. Security Analysis

A. Slandered Attack

Malicious vehicles can interfere with the system by providing unsuitable recommendations, which contain wrong

accusations and false praises. In our model, a bias check is applied to the direct and second-hand information of vehicles, based on the historical information stored in the blockchain. If certain incorrect evaluations are imperceptible, they will be disregarded. Such a practice will somewhat exclude wrong recommendations and prevent situations where accurate evaluations are overlooked.

B. On–Off Attack

Malicious vehicles will utilize the dynamic nature of information updates to switch between normal and malicious behaviors in order to hide their malicious behaviors. For this attack, our trust mechanism monitors the standard deviation of historical trustworthiness. It will be monitored once the trustworthiness shows abnormal fluctuations, effectively suppressing on–off attacks.

C. Selective Behavior Attack

The purpose of a selective misbehavior [41] attack is to exclude the victim node from the network while enabling the attacker to access standard services. In other words, the attacker behaves maliciously toward the vehicle it intends to attack and behaves honestly toward the important vehicles that play a crucial role in providing network services. In the model, there are direct evaluations of vehicles as well as evaluations from neighboring vehicles that have cooperated, which helps to mitigate such attacks to some extent.

D. Sybil Attack

A single malicious vehicle fakes multiple identities in the vehicle network to extend its reach. For this case, we propose the model in which a legitimate identity is set to have only one certificate simultaneously. The trustworthiness is retained when the vehicle enters the network again.

VI. Experiments

A. Experiment Environment

We validate the proposed model on the open-source platform md_blockchain. The elliptic curve cipher (ECC) algorithm and Rivest–Shamir–Adleman (RSA) are the most popular encryption algorithms. The elliptic curve digital signature algorithm (ECDSA) combines the ECC and RSA algorithms.To minimize overhead, ensure security, and maintain consistency in our experiments, we utilize the ECDSA-secp256k1 algorithm for encrypting/decrypting and signing/verifying the messages used in the model. All of our programming is done in Java. The experiment environment is: Intel Core i7 CPU @ 16 GB 2400 MHz, and the Operating System is macOS 11.6.1.

B. Validity

The validity of the model is first verified. We assume two common patterns of malicious vehicle behavior.

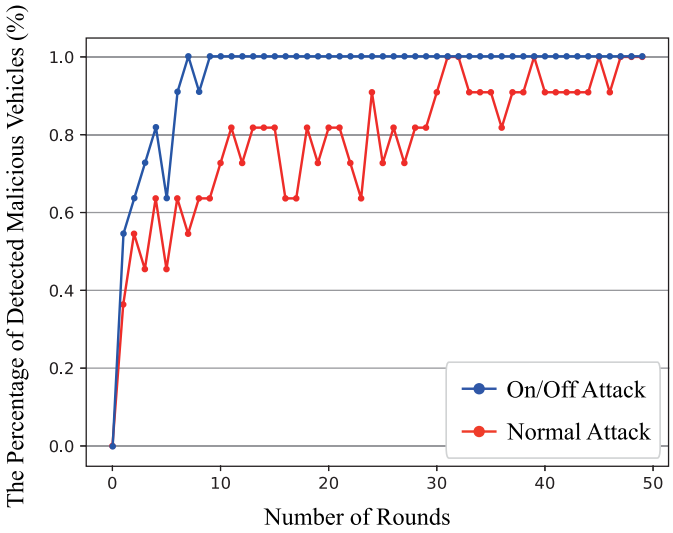

Fig. 4. Percentage of detected malicious vehicles.

1) Simple Malicious Behavior Pattern: Malicious vehicles always exhibit malicious behavior. In this case, it is usually easy for the system to identify and remove them from the candidate list of anonymous cloaking regions.

2) Malicious Behavior Using On–Off Attacks Pattern: The malicious vehicles exhibit alternating malicious behavior, meaning that they display honest behavior in one round and malicious behavior in the next round. This is done in an attempt to conceal their malicious intentions and evade detection by the system's monitoring.

As shown in Fig. 4, the horizontal coordinate represents the number of rounds, while the vertical axis represents the percentage of detected malicious vehicles. As shown in the solid blue line in Fig. 4, the system's ability to identify malicious vehicles improves as the rounds advance. In the experiment, we selected 30% of them to exhibit malicious behavior. We define a complete request–response process as one round, and there can be multiple request–response processes in a single round. It can be seen that the percentage of identified malicious vehicles continues to increase in the first five rounds, with some fluctuations in the eighth round. However, in the 11th round, all the malicious vehicles in the system are fully identified. The solid red line in Fig. 4 shows the percentage of malicious vehicles identified by the system as the vehicle progresses through the rounds in the on–off attack behavior mode. Compared to the first scenario, the malicious vehicle manages to evade detection by the system in certain rounds. Despite some fluctuations, the vehicle also exhibits a correct recognition rate of over 90% after 38 rounds.

C. Trustworthiness

Next, we discuss the trend of trustworthiness changes under different behaviors. In our model, a vehicle can play different roles in different rounds, where it may act as a requester vehicle in one round and as a cooperator vehicle in the next round. During the process of constructing the k-anonymity region, vehicles cooperate with each other,

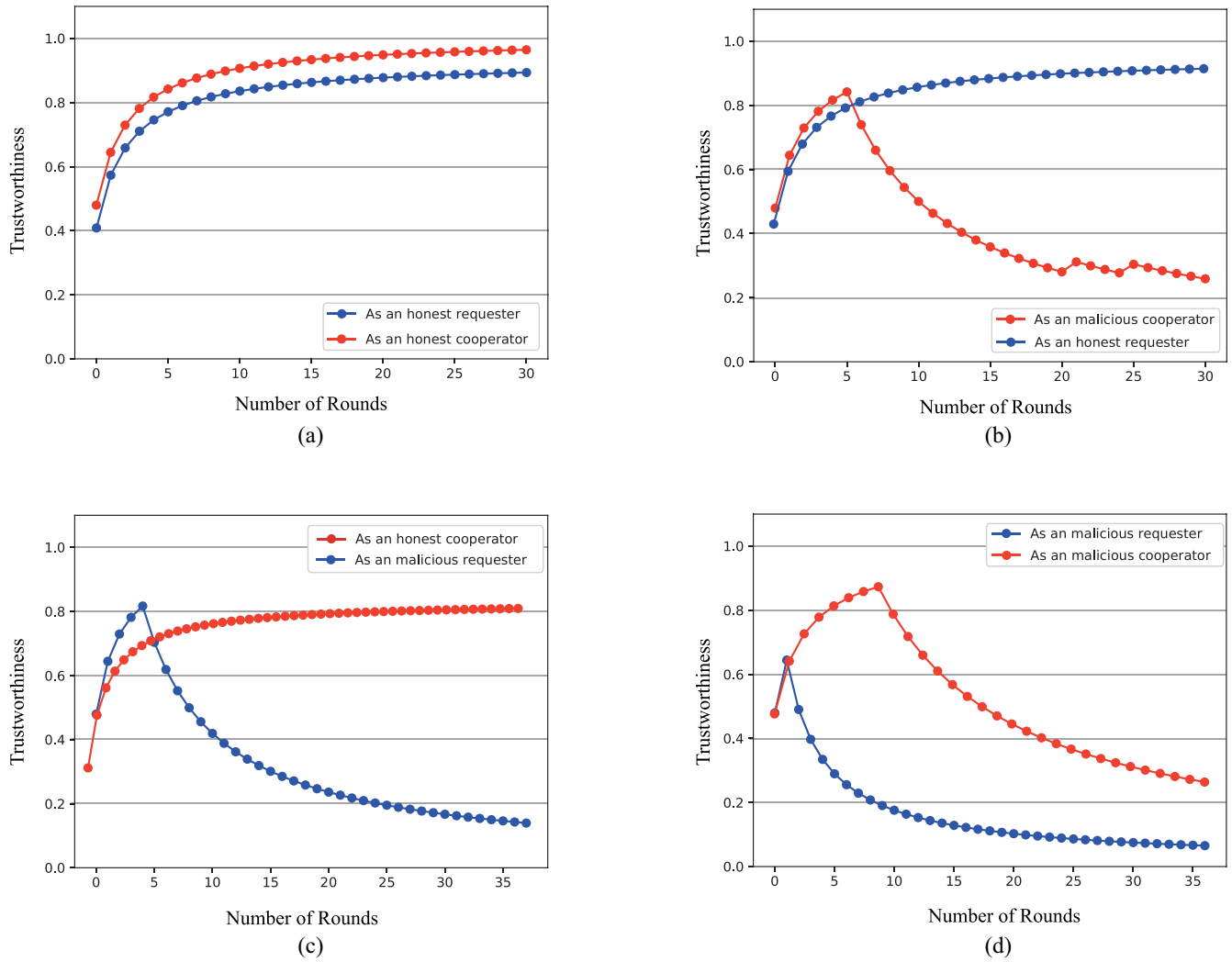

Fig. 5. Trustworthiness under different behaviors. (a) Honest requester and honest cooperator. (b) Honest requester and malicious cooperator. (c) Malicious requester and honest cooperator. (d) Malicious requester and malicious cooperator.

and therefore the trustworthiness will also change with the behavior of the vehicles within the group. We observed how the trustworthiness changed under four behaviors: 1) honest requester vehicles and honest cooperator vehicles; 2) honest requesters and malicious cooperators; 3) malicious requesters and honest cooperators; and 4) malicious requesters and malicious cooperators. As shown in Fig. 5, if the vehicle exhibits consistent, honest behavior, the trustworthiness must continue to rise. As shown in Fig. 5(a), the trustworthiness of the requester vehicle grows less rapidly than that of the cooperator vehicle. In the model, the evaluation of the requester is stricter than that of the cooperator. Also, the requester node should have a greater degree than the cooperator node in a realistic vehicle network structure, and the experimental results are as expected. Also, as shown in Fig. 5(b) and (c), when one party actor behaves maliciously, the system can distinguish their behavior and reduce the trustworthiness of the malicious vehicle within five rounds. As shown in Fig. 5(d), the system can also reduce the trustworthiness of all vehicles starting in round 7 when they exhibit malicious behavior. It can be seen that the trustworthiness of malicious requester vehicles decreases faster than that of malicious cooperator vehicles.

D. Robustness

Moving on to verify the robustness of the model. In the previous section, we analyzed the security of various attacks that the model may encounter. In this section, we select the two most prevalent types of attacks for experimental validation and compare them with the approaches proposed by Luo et al. [27] and Li et al. [28].

1) Change in Plausibility Under On–Off Attack: In our experiments, we set the vehicle to suffer an on–off attack from rounds 5 to 10 and conducted 50 experiments. As shown in Fig. 6, the horizontal coordinates represent the number of experimental rounds, and the vertical coordinates represent the change in the trustworthiness of the vehicle. The solid red line is Luo et al.'s solution, where the trustworthiness of the vehicle continues to rise even after the on–off attack and rises very quickly. The penalty that the vehicle should suffer is not expressed in its trustworthiness. The blue realization is Li's

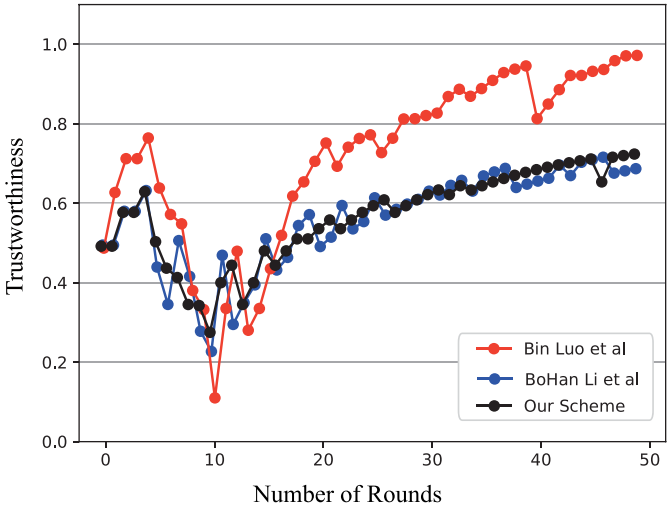

Fig. 6. Trustworthiness tendency under on–off attack.

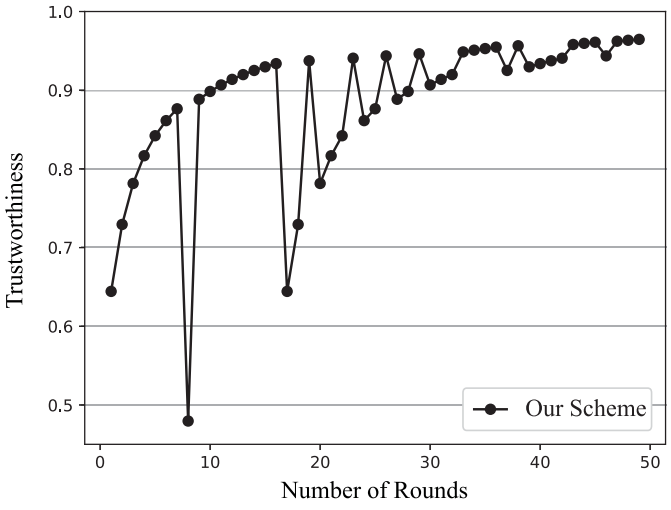

Fig. 7. Trustworthiness tendency under bad-mouthing attack.

scenario, and the black line is our scenario. Fig. 6 shows that in both cases, the increase in trustworthiness became small after round 10, which resisted the on–off attack to some extent.

2) Change in Trustworthiness for the Bad-Mouthing Attack: As depicted in Fig. 7, our model assumes that relying on second-hand information may result in an inaccurate evaluation of the trustworthiness of honest vehicles. Additionally, the honest vehicles were targeted by malicious bad-mouthing attacks in the 5th and 8th rounds. The security analysis also mentions that our model applies bias tests to both direct and second-hand information about vehicles, using historical information stored in the blockchain. If there are any inaccurate assessments beyond perception, they will be disregarded. It can be seen from the curve that the accusation of bad-mouthing is invalid as long as the vehicle continues to behave honestly. Although there are jitters in the early stages, they will gradually be overcome and recognized. It should be noted that we did not compare the schemes proposed by Bin Luo and Bohan Li because their approaches do not involve second-hand information. Therefore, we will not include them in the comparison.

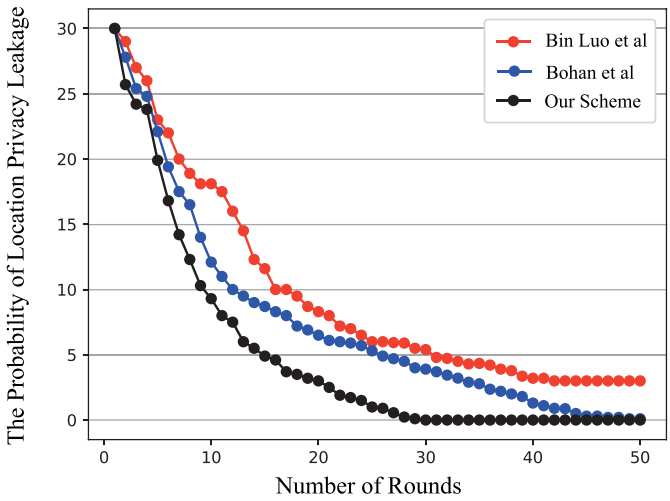

Fig. 8. Probability of location privacy leakage.

E. Location Privacy Protection

In this section, we verify the probability of location privacy leakage by setting up an experiment in which 30% of the malicious vehicles exhibit malicious behavior, either as a simple malicious behavior pattern or a malicious behavior using on–off attacks. Once a vehicle exhibits malicious behavior in the anonymous cloaking region, the location privacy of the vehicles in that region is at risk of being exposed. We found, through comparison, that all three schemes somewhat protect vehicle privacy. After 50 rounds, the desired outcome can generally be achieved. However, as shown in Fig. 8, our scheme can ensure location privacy after 30 rounds and converges slightly faster than the other two schemes.

F. Construction of Anonymous Cloaking Regions

The number of members, k, within the anonymous cloaking region is an essential parameter in the model. At the same time, in real life, the value of k is adjusted as needed. This allows us to observe the effect of the parameter k on the latency in constructing the anonymous cloaking region. When vehicles enter areas with lower vehicle density, where the number of vehicles is less than the minimum value k required to meet the conditions for creating a k anonymous cloaking region, we introduce virtual vehicles to assist in forming the k anonymous cloaking region. Again, we compared the experimental results, as shown in Fig. 9, and observed that the three curves converge in their orientation, with more time spent as the value of k increases. Also, because both Luo's and Li's schemes incorporate the Dirichlet distribution into the calculation of the vehicle's trustworthiness assessment, they are more influenced by the value of k in terms of time delay than the Beta distribution used in this article. However, the error is within 200 ms, and there is no significant difference in the time delay between this model and the previous one.

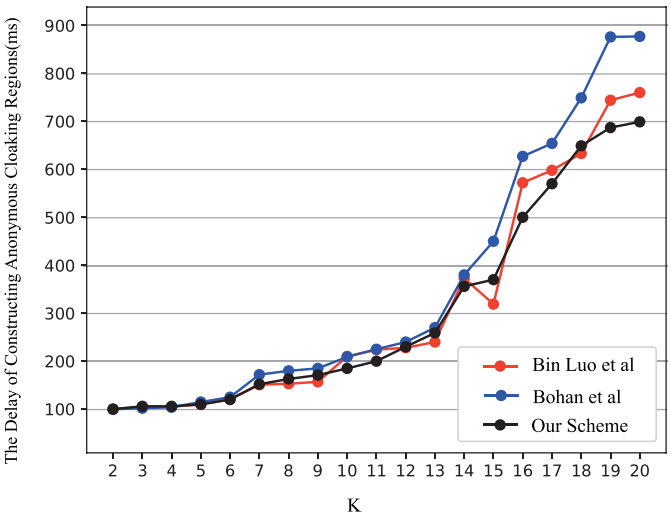

Fig. 9. Delay of constructing anonymous cloaking regions.

VII. Conclusion

In this study, we propose an improved Bayesian method that utilizes the Beta distribution to update historical trust values. This method combines direct and second-hand reputation evaluation and incorporates a trust mechanism that considers both credibility and a limited time delay when evaluating trustworthiness. A trusted k-anonymous cloaking region is constructed to protect the location privacy of vehicles. The proposed model also uploads trustworthiness to the blockchain, utilizing an LPBFT consensus algorithm. Experimental and security analyses demonstrate that our proposed solution is resilient to various attacks on trust models. Our model is simple and effective compared to existing work, providing ideas for establishing a reliable VANET.

In our model, we did not consider the adoption of federated learning technology on edge computing nodes in the VANETs. Federated learning, as a distributed machine learning paradigm, allows participants to collaboratively model without sharing their data. For future work, we will integrate federated learning technology and consider privacy-preserving solutions within a blockchain architecture in the high-concurrency context of VANETs. We will integrate these solutions with the findings of this article to establish a reliable blockchain framework that can address high-concurrency issues. Our focus will be on achieving a better balance between vehicle privacy and computational efficiency.

References

[1] "Analysis of the market status and development prospects of the global Internet of Vehicles industry in 2021." Accessed: Apr. 28, 2018. [Online]. Available: https://bg.qianzhan.com/trends/detail/506/220325-8ce5fa14.html

[2] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-defined vehicular networks with trust management: A deep reinforcement learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1400–1414, Feb. 2022.

[3] H. Khelifi et al., "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 320–351, 1st Quart., 2020.

[4] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, "A blockchain-based reputation system for trusted VANET nodes," *Ad Hoc Netw.*, vol. 140, Mar. 2023, Art. no. 103071.

[5] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao, and K. Cai, "LBS meets blockchain: An efficient method with security preserving trust in SAGIN," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5932–5942, Apr. 2022.

[6] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8078–8090, Jun. 2022.

[7] J. W. Kim, K. Edemacu, and B. Jang, "Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey," *J. Netw. Comput. Appl.*, vol. 200, Apr. 2022, Art. no. 103315.

[8] L. Zhu, Y. U. Li-Ping, Z. Y. Cai, X. W. Liu, and J. W. Zhang, "K-anonymous based anti-positioning security strategy in mobile networks," *J. Inf. Sci. Eng.*, vol. 38, no. 1, pp. 121–138, 2022.

[9] J. Liu and S. Wang, "All-dummy k-anonymous privacy protection a1gorithm based on 1ocation offset," *Computing*, vol. 104, pp. 739–1751, Mar. 2022.

[10] D. Yang, B. Ye, W. Zhang, H. Zhou, and X. Qian, "KLPPS: A k-anonymous location privacy protection scheme via dummies and stackelberg game," *Secur. Commun. Netw.*, vol. 2021, no. 5, 2021, Art. no. 9635411.

[11] X. Li, J. Liu, M. S. Obaidat, P. Vijayakumar, Q. Jiang, and R. Amin, "An unlinkable authenticated key agreement with collusion resistant for VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7992–8006, Aug. 2021.

[12] G. Du et al., "A blockchain-based trust-value management approach for secure information sharing in Internet of Vehicles," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 333–344, Jan. 2024.

[13] M. Biswas et al., "Blockchain-enabled communication framework for secure and trustworthy Internet of Vehicles," *Sustainability*, vol. 15, no. 12, p. 9399, 2023.

[14] B. Hildebrand et al., "A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions," *Comput. Sci. Rev.*, vol. 48, May 2023, Art. no. 100547.

[15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *Proc. Decent. Bus. Rev.*, 2008, Art. no. 21260.

[16] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[17] J. Huang et al., "Blockchain-based mobile crowd sensing in industrial systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6553–6563, Oct. 2020.

[18] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[19] N. Gao, R. Huo, S. Wang, and T. Huang, "FIBFT: An improved Byzantine consensus mechanism for edge computing," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2023, pp. 1–6.

[20] D. Huang, L. Li, B. Chen, and B. Wang, "RBFT: A new Byzantine fault-tolerant consensus mechanism based on raft cluster," *J. Commun.*, vol. 42, no. 3, pp. 209–219, 2021.

[21] P. Samarati and L. Sweeney, *Protecting Privacy When Disclosing Information: k-Anonymity and its Enforcement Through Generalization and Suppression*, SRI Int., Menlo Park, CA, USA, 1998.

[22] L. Hai, X. Li, L. Hui, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2017, pp. 1–9.

[23] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. 1st Int. Conf. Mobile Syst., Appl. Services*, 2003, pp. 31–42.

[24] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, pp. 1–18, Jan. 2008.

[25] G. Sun, D. Liao, H. Li, H. Yu, and V. Chang, "L2P2: A location-label based approach for privacy preserving in LBS," *Future Gener. Comput. Syst.*, vol. 74, pp. 375–384, Sep. 2017.

[26] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "MOBIHIDE: A mobilea peer-to-peer system for anonymous location-based queries," in *Proc. Int. Symp. Spatial Temporal Databases*, 2007, pp. 221–238.

[27] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2034–2048, Feb. 2020.

[28] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021.

[29] M. E. Mahmoud and X. Shen., "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3947–3962, Oct. 2011.

[30] N. Alexopoulos, J. Daubert, M. Mühlhuser, and S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, 2017, pp. 546–553.

[31] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the Internet of Vehicles," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108558.

[32] A. V. Rivera, A. Refaey, and E. Hossain, "A blockchain framework for secure task sharing in multi-access edge computing," *IEEE Netw.*, vol. 35, no. 3, pp. 176–183, May/Jun. 2021.

[33] Y. Zhang, J. Misic, and Z. Zheng, "Guest editorial introduction to the special section on blockchain for vehicles and intelligent communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 3998–4000, May 2021.

[34] W. Ruan, J. Liu, Y. Chen, S. M. N. Islam, and M. Alam, "A double-layer blockchain based trust management model for secure Internet of Vehicles," *Sensors*, vol. 23, p. 4699, May 2023.

[35] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proc. 9th ACM Int. Workshop Veh. Inter-Netw., Syst., Appl.*, 2012, pp. 73–82.

[36] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *Int. J. Comput. Intell. Theory Pract.*, vol. 9, no. 1, pp. 45–57, 2014.

[37] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE 27th Conf. Comput. Commun.*, 2008, pp. 1238–1246.

[38] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[39] Z. Liu et al., "BTMPP: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5386–5407, Apr. 2021.

[40] Z. Liu et al., "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, early access, Dec. 8, 2023, doi: 10.1109/TVT.2023.3340723.

[41] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 108–114, Apr. 2008.