A DAG-Based Reputation Mechanism for Preventing Peer Disclosure in SIoV

Yijing Li, *Student Member, IEEE*, Xiaofeng Tao, *Senior Member, IEEE*, Xuefei Zhang, *Member, IEEE*, Jin Xu, *Member, IEEE*, Yisong Wang, and Wenbo Xia

***Abstract*—The sensitive information of vehicles which is closely related to the safety of transportation makes the privacy problems in the vehicular networks a popular concern. The development of artificial intelligence (AI) has led the Internet of Vehicles (IoV) to the next phase of intelligence, the Social IoV (SIoV). For social purposes, vehicles may upload captured images with more sensitive information. As a result, the privacy problem is even more serious in SIoV. The exited studies of privacy-preserving methods in vehicular networks mainly consider the spontaneous privacy disclosure. However, the main privacy leakage in real life comes from peer disclosure rather than spontaneous privacy disclosure, which is usually ignored. Therefore, this article innovatively presents a decentralized scheme for solving the peer disclosure issues in SIoV, which, to the best of our knowledge, is the first research in SIoV peer disclosure discussion. A directed acyclic graph (DAG)-based mutual supervision (Dmsv) algorithm is designed for mutually distrustful vehicles. It is verified that our proposed algorithm reduces at least 72% multidimentional privacy loss of image entropy leakage probability when compared with nonpeer disclosure prevention. The decentralized scheme also achieves a relatively low delay of around 24 s from the transaction generation to a network-wide consensus. This article provides a feasibility of applying DAG in a mobile system and provides guidance on how the transportation situation influences the confirmation delay and how to adjust the incentive mechanism according to the transportation situation to maintain robustness.**

***Index Terms*—Blockchain consensus, decentralized system, directed acyclic graph (DAG), peer disclosure, Social Internet of Vehicles (SIoV).**

I. Introduction

PRIVACY issues exist in all aspects of life and, therefore, have gradually become one of the hot topics in B5G and 6G investigations [1]. Since vehicle privacy contains unique vehicle information, such as vehicle location and driver's identity which are sensitive to the safety of transportation, the privacy issues are particularly prominent in the vehicular networks [2]–[5].

Moreover, with the development of vehicle technology and artificial intelligence (AI), the vehicular network steps to the next phase of intelligence, the Social Internet of Vehicles (SIoV) [6], [7]. In SIoV, vehicles are more intelligent and the vehicular networks are capable of realizing automation, scalability, autonomous supervision, and management through the social interaction between intelligent vehicles. Meanwhile, vehicles are developed more versatile and business oriented and, therefore, carry special businesses with more privacy-sensitive information [5], e.g., upload a captured image for social purposes. Consequently, the requirement of privacy protection in SIoV is more urgent than that in ordinary IoV scenarios.

At present, the privacy protection research of IoV mainly focuses on the perspective of spontaneous disclosure, which means the entity itself takes some actions to prevent the possible privacy leakage when it transmits some necessary information. For example, some studies preserve privacy through cryptography [8]–[11], such as pseudonym system and information encryption, some apply the blockchain technology [12], [13], and there are also some other methods like data processing.

However, in real life, most of the privacy leakage come from the peer disclosure perspective [14]. It could be an observation of one's action, location, or the glance capture of one's face image. The peer disclosure usually happens before the entity knows it and, therefore, it is hard to prevent. Actually, the situation is even more severe in the vehicular network especially SIoV, where the image accidentally captured by on-vehicle camera evolves great privacy information of other entities, which may further lead to severe traffic problems.

The existed literature on peer disclosure mainly lies on the online social network (OSN) [14]–[16]. Most studies on OSN peer disclosure discuss the qualitative classification of the influencing factors without enough scientific measurement formula or convincing quantitative analysis, which cannot explain how the entity actions influence the risk level of peer disclosure.

There are some studies that focus on the co-location privacy of vehicles [17]–[19], which only protect one dimension of vehicle privacy (the location privacy). To the best of our knowledge, it is the first time the peer disclosure issues are discussed in SIoV. Moreover, the privacy-preserving methods under peer disclosure proposed in these studies are basically

Manuscript received 25 October 2021; revised 22 April 2022; accepted 1 July 2022. Date of publication 7 July 2022; date of current version 21 November 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61932005 and Grant U21A20449; in part by the Beijing Natural Science Foundation under Grant L212003; and in part by the 111 Project of China under Grant B16006. *(Corresponding author: Xiaofeng Tao.)*

The authors are with the National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: liyijing@bupt.edu.cn; taoxf@bupt.edu.cn; zhangxuefei@bupt.edu.cn; jin.xu@bupt.edu.cn; wangyisong@bupt.edu.cn; 3084617577@qq.com).

Digital Object Identifier 10.1109/JIOT.2022.3189108

realized from the perspective of large systems or platforms, which requires a strong and credible center with data of all members to complete the peer behavioral assessments and take preventive actions, which is undoubtedly unrealistic in terms of implementation.

First, it is clear that a distributed system is necessary in order to solve the above-mentioned implementation difficulties associated with a centralized system. However, a fully decentralized system poses new challenges. With different owners, vehicles are naturally distrustful of each other, and a distributed system without the ability to regulate behavior would be a mess. Therefore, a mutual monitoring mechanism based on the reputation value is particularly important.

However, a reputation-based mechanism seems not reliable in some situation. For example, a malicious vehicle may dishonestly score the behavior of others or cheat vehicles with less information for higher scores, which may cause chaos. Therefore, we try to find an efficient distributed consensus method in the reputation mechanism, which can realize the authenticity, immutability, and accessibility of all vehicle reputation, and ensure a certain degree of privacy.

Recently, blockchain has shown great application potential in Internet of Things (IoT) systems, such as smart vehicles [13], energy trading [20], supply chains [21], and so on. Blockchain is decentralized, highly secure, interoperable, and trust building, and can solve the high infrastructure and maintenance costs of traditional centralized IoT systems. The consensus method of blockchain is regarded as a practical technology to achieve data consistency in a decentralized system.

However, traditional Proof-of-Work (PoW) and Proof-of-State (PoS) methods result in a long consensus time in a huge system, which conflicts with the characteristics of vehicle networks, such as a high mobility and fast-changing topology. In this way, a directed acyclic graph (DAG) seems a feasible way to solve the long latency problem [22]. As is analyzed in [23], DAG consensus method maintains the advantage of low latency even in large-scale participation. The random and finite view of each member also ensures a certain degree of privacy.

Therefore, in this article, we propose a distributed peer disclosure solution based on the reputation mechanism by referring to the idea of DAG consensus in the blockchain. Our main contributions can be concluded as follows.

1) To the best of our knowledge, this article is the first study that focuses on the privacy-preserving mechanism for preventing peer disclosure in SIoV. Different from the existed peer disclosure studies, we provide multidimensional privacy of vehicles and give a scientific measurement of the peer disclosure impacts and convincing simulations.
2) A DAG-based mutual supervision (Dmsv) algorithm is proposed for SIoV mutual supervision. Our proposed algorithm is proved to possess stability by combining the results of simulations with the inherent nature of the DAG consensus, which extends the feasibility of DAG from stable state to a mobile system.
3) Simulation results show that our proposed scheme achieves robustness under a large-scale decentralized SIoV system. Under the DAG-based mechanism, the privacy loss of image entropy leakage probability can be reduced by at least 72% when compared with non-peer disclosure preventing while keeping a relatively low delay of around 24 s from transaction generation to network-wide consensus.
4) Macroscopically speaking, this study provides the guidance of how vehicle density influences the confirmation delay and how to adjust the incentive mechanism according to the vehicle density to maintain robustness.

II. Related Work

Privacy issues are essential for the security of the IoV network. Various solutions have adopted spontaneous privacy disclosure prevention methods, for example, through cryptography or applying blockchain technology. However, most of the research ignore the peer disclosure perspective. With the development of AI, IoV comes to the next phase of intelligence, SIoV, where the peer disclosure issues are more serious. In this section, we provide an overview of the exited studies of privacy preserving in these domains, the feature of peer disclosure and SIoV, as well as the expected solution of peer disclosure in SIoV.

A. Privacy Preserving Methods in IoV

The privacy issues in IoV have gained great public concern in these years and, therefore, the privacy-preserving methods are also well investigated.

Study [8] provides a comprehensive comparison of different privacy-preserving methods in vehicular ad hoc network (VANET) and their evaluation as well. Study [9] achieves personalized content privacy for autonomous vehicles through k-anonymity. Xing *et al.* [24] proposed a double k-anonymity method in IoV to protect the location privacy and the request information. Literature [25] introduces a privacy-preserving secure framework for electric vehicles in IoT using matching market and encryption.

Different from the traditional cryptography methods, some studies apply blockchain as a possible solution. Bellini *et al.* [26] gave a comprehensive view of the blockchain-based distributed trust and reputation management systems both in IoV structure and application. Research [27] proposes a distributed blockchain-based anonymous reputation system (BARS) to break the linkability between real identities and public keys to preserve privacy for VANETs. Literature [28] introduces a joint privacy and reputation assurance and proved efficiently and synergistically support for VANETs by applying blockchain technology.

B. SIoV

With the development of vehicle technology and AI, recently, IoV has come to the next phase of intelligence, the SIoV. As a special case of the Social IoT (SIoT) system [29]–[31], SIoV regards intelligent vehicles as the interactive social objects and presents vehicular a social network platform following cyber–physical architecture with existing VANETs technologies, such as V2V and V2I communications [32], [33].

Study [6] gives a comprehensive discussion about the concept, architecture, and application of SIoV and provides some implementation details as well as experimental analysis to demonstrate the efficacy of the SIoV system in a technical way. Study [7] also provides a comprehensive review of SIoV and further clarifies that privacy issues of SIoV are the main challenge in the implementation of SIoV.

Different from the IoV system, vehicles in SIoV not only transmit sensitive information but as a social subject to transmit social information visible to the public. Therefore, it seems that blockchain is a feasible technology to solve the privacy issues in SIoV for the transparent visibility and immutability of information and there are few related studies. Arora and Yadav [34] proposed a blockchain-based approach for authentication and secure data exchange among vehicles and nodes within the SIoV environment. Research [35] introduces a secure, automated, and privacy-shielding protocol for charging of SIoV based on blockchain technology.

However, it is noticed that most of these research of privacy-preserving in IoV and SIoV have the same problem that there is still a trusted and powerful third party for reputation records in most literature, or they do not consider the threat of malicious users in a fully distributed system without a third party. Moreover, the most important thing is that almost all privacy discussed in these studies are self-disclosure rather than peer disclosure, which is a big part of privacy disclosure in real life.

C. Peer Disclosure

Peer disclosure, the disclosure of one's private information by peers, can potentially raise severe privacy challenges [14]. The idea of peer disclosure was first proposed in 2015 to describe the disclosure of one's privacy by friends in OSNs [14]. Then, some researchers followed this idea to further explore peer disclosure in OSN.

For example, Dissanayake *et al.* [36] drew on the viewpoint of communication privacy management and impression management theory and provide privacy protection for peer information disclosure in the OSN environment through simulation analysis. Pham *et al.* [15] explored the common privacy metrics and common privacy protection techniques used in peer disclosure. This research has some obvious limitations that due to the characteristics of OSN, the realization of peer disclosure prevention in these studies all counts on a trust centralized platform such as FACEBOOK to prevent peer disclosure while ignoring the potential threat of the platform with all knowledge, which is undoubtedly unrealistic.

When the situation comes to the vehicular domains, innovated by the peer disclosure concept in OSN, researchers began to pay attention to the notion of shared privacy or interdependent privacy, which is similar to peer disclosure. The most typical form of interdependent privacy in vehicular networks is co-location privacy, which means vehicles in a short distance share the same privacy of the location.

Research [37] provides a comprehensive description of interdependent privacy including the history, characteristics, and challenges. Zhang *et al.* [38] provided a comprehensive view of the shared location privacy between vehicles and analyze the effect of co-location privacy. Literature [19] proposes a game theory-based solution to preserve co-location privacy by balancing communication efficiency and privacy by adjusting the communication range.

To the best of our knowledge, there is no research investigating the peer disclosure problems in SIoV. However, the studies in interdependent privacy provide us with some new insights into the solution of peer disclosure in SIoV. We hope that not only co-location privacy is protected, but more privacy-sensitive information about the vehicles, such as drivers' identity, can be effectively protected in the way we have proposed.

D. DAG

As is discussed before, due to the distributed characteristics of vehicles and the consideration of security, a decentralized system is required in the realization of peer disclosure in SIoV. The consensus method of blockchain is regarded as a practical technology to achieve data consistency in a decentralized system and there is already some research supporting this idea [34], [35].

However, traditional PoW and PoS methods result in a long consensus time in a large-scale system, which conflicts with the characteristics of the vehicular networks, such as high mobility, a large amount of data, and fast-changing topology. In this way, DAG seems a feasible way to solve the long latency problem [22].

DAG is a distributed ledger technology different from the mainstream blockchain, upgrading synchronous bookkeeping to asynchronous bookkeeping, which is considered by many researchers to solve the high concurrency problem of the traditional blockchain and is an innovation of the blockchain from capacity to speed [23], [39]. Applying DAG as the network base addresses the limitations of the blockchain. This allows blockchain to scale infinitely at a fraction of the cost. Recently, DAG has been widely applied in blockchain consensus which allows any node to insert a new transaction into the ledger immediately, as long as they process the earlier transactions [40], [41].

DAG is considered a great solution to solve the consensus latency challenge brought by traditional consensus algorithms, such as PoW and PoS in a large-scale system both in academia and industry fields [42], [43]. In industrial applications, the most widely used and well-known is the tangle-based IOTA cryptocurrency [44], [45], which there are already some standards and white papers [46]. As for the academic field, there are already a great amount of research to prove the advantages of DAG [47]–[49]. For example, research [23] provides the performance analysis and optimal communication node deployment of DAG-base blockchain-enabled wireless IoT. Literature [42] applies a self-referencing DAG structure and a voting-based PBFT consensus algorithm to maintain the number of transactions per second (TPS) while keeping a relatively

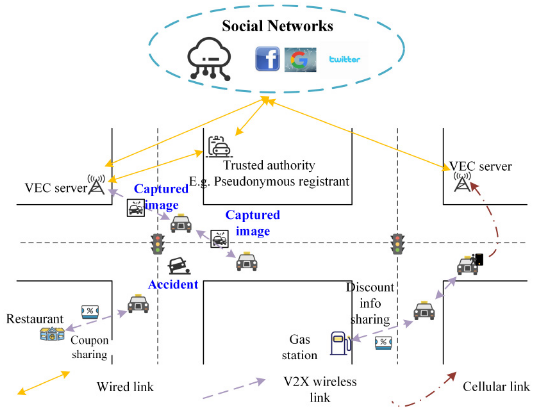


Fig. 1. Structure of the SIoV system.

low latency in wireless networks. Study [50] provides the proof that DAG has the probability to be applied on smart vehicles.

To the best of our knowledge, there are few studies about the DAG-based privacy-preserving method, especially for peer disclosure in SIoV. Therefore, we try to propose a distributed peer disclosure solution based on the reputation mechanism by referring to the idea of the DAG consensus in the blockchain.

III. System Model

In this article, we consider a vehicle-oriented SIoV system, as is shown in Fig. 1. There are mainly three layers in the SIoV system, vehicles and on-vehicle users, VEC servers and trusted authority, and the social networks.

Vehicles, as the main entities, communicate with each other about the traffic information, the entertainment information through V2X wireless links as in the IoV system. Especially, with social purposes, vehicles may communicate extra information in different formats. For example, the coupon of a restaurant, the discount information of a gas station, or the captured images of the traffic accident, which is our main focus in this article.

There are VEC servers and trusted authority as the fundamental infrastructures in SIoV. VEC servers can communicate with vehicles through V2X wireless links and with on-vehicle users through cellular links. Trusted authority, such as pseudonymous registrant, takes the responsibility of the access management of SIoV, connects the VEC servers and social networks by wired links.

The social networks, for example, Facebook, Google, and Twitter are the main embodiment of social characteristics in SIoV. Different from the traditional OSNs, the social networks in SIoV carry more vehicle applications, such as the traffic policing social platform we proposed.

Based on the SIoV system, we propose a DAG-based SIoV supervision scheme. The idea of the proposed scheme is to facilitate supervision for vehicular privacy-preserving and traffic policing among vehicles. Considering the nature of decentralization, vehicles are not willing to contribute computation resources for other vehicles' privacy-preserving efforts. Therefore, a reputation-based mutual supervision scheme is necessary.

Take the sample in Fig. 2 as the explanation of the DAG-based SIoV supervision scheme. In this scheme, vehicles upload the captured images of accidents or illegal behaviors to the DAG-based SIoV platform for mutual supervision. This scheme involves a pseudonymous registrant, a DAG-based SIoV platform, observer vehicles, and under-observation vehicles.

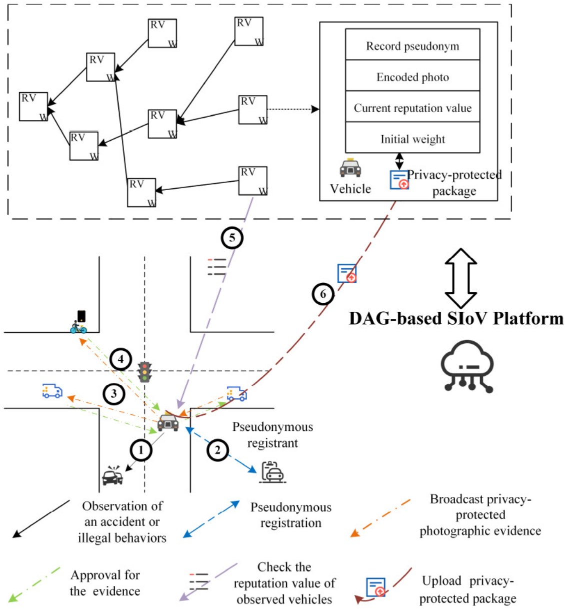

RV
W
Record pseudonym
Encoded photo
Current reputation value
Initial weight
Vehicle
Privacy-protected package
5
6
DAG-based SIoV Platform
4
3
1
2
Pseudonymous registrant
Observation of an accident or illegal behaviors
Pseudonymous registration
Broadcast privacy-protected photographic evidence
Approval for the evidence
Check the reputation value of observed vehicles
Upload privacy-protected package

Fig. 2. Sample of the DAG-based SIoV supervision algorithm.

1) *Pseudonymous Registrant:* A pseudonymous registrant is a centralized third party who takes responsibility for allocating pseudonyms for vehicles in this scheme. The pseudonym mechanism is to prevent co-location privacy leakage when uploading packages.
2) *DAG-Based SIoV Platform:* A DAG-based SIoV platform is a platform maintained by all vehicles. Blocks on the platform consist of the recording pseudonym, encoded photograph, current reputation value of the upload vehicle, and the initial weight of this block. The weight of blocks is cumulative and the confirmation of a graph path is based on the cumulative weight of the chain.
3) *Observer Vehicles:* A vehicle captures an accident or illegal behavior and uploads the encoded images to the SIoV platform.
4) *Under-Observation Vehicles:* A vehicle that breaks traffic rules and is captured by another vehicle is called under-observation vehicle.

IV. DAG-Based SIoV Supervision Scheme

In this section, we provide the details of the DAG-based SIoV supervision scheme, the problem formulation and workflows. First, to better understand the proposed scheme, some basic information about DAG are summarized in Section IV-A.

A. Basic Information About DAG

According to the IOTA white paper and some authoritative related research [45], [46], we organize and summarize the basic information about DAG in the following.

1) Descriptions: Nodes are entities that issue and validate *transactions*. The network is composed of nodes. *Sites* are transactions represented on the graph. For example, in Fig. 2, vehicles are considered as nodes, and the encoded photograph consisting of recorded illegal events is considered as the transaction (site) that needs to approve.

The main idea of DAG is as follows: to post a transaction, the node must make an effort to approve other transactions. *Tips* are defined as the unapproved transactions in the graph. In order to issue a transaction, a node follows some rules.

1) The node chooses two transactions in the graph to approve according to the Markov chain Monte Carlo (MCMC) algorithm [51], [52].
2) The node checks the two transactions and gives up the conflicting transactions.
3) For a node to publish a valid transaction, it must solve a cryptographic puzzle similar to the one in the Bitcoin blockchain.

The *weight* of a transaction is a positive integer proportional to the amount of work that the issuing node invested into it, which in our system, is defined as the significance of the recorded event. In general, a transaction with a larger weight is more important than the one with a smaller weight. The own weight of a particular transaction plus the sum of weights of all transactions that directly or indirectly approve this transaction is called the *cumulativeweight* of a transaction. The *height* of a transaction site means the length of the longest oriented path to the genesis, while the *depth* means the length of the longest reverse-oriented path to some tip.

2) Stability of the System: According to the analysis in the existed research, the stability of the DAG-based system is reflected in the stability of the total number of tips in the graph. However, there are some assumptions under the conclusion, which are described in the following.

First, the process of incoming transactions can be modeled by a Poisson point process [53]. Meanwhile, the process has to be time homogeneous [54]. Then, assume that all devices (vehicles in our system) have approximately the same computing power. With the three assumptions, when time tends to infinity, the total number of tips in the graph will fluctuate around a constant value and not escape to infinity. Therefore, the DAG-based system remains stable. The comprehensive proof can be found in the IOTA white paper [46] under low and high loads.

3) Possible Attacks and MCMC Algorithm: For DAG networks, the main means of attack is the $double-spending$ attack [51]. In the double-spending attack, attackers issue a big double-spending transaction using all of their computing power. This transaction would have a very large own weight and would approve transactions prior to the legitimate transaction used to pay the merchant.

In order to prevent such an attack, the DAG network sets the main TANGLE not to expand infinitely but selects the sub tangle with the heaviest cumulative weight as the main part of the DAG, and those with larger cumulative weight differences from the main body will be discarded [23], [46], [51]. At this point, another situation can be avoided as a bonus, that is, *lazynodes*, who do not want to consume the arithmetic power to approve new transactions, but spend a very small amount of arithmetic power to approve transactions that are older. Then, the chain of these nodes has a big gap in cumulative weight when compared with the main body of DAG and will be eliminated. Due to the little contribution to the main body, they will be labeled as *lazynodes* and the transactions they issued will not be approved.

At the same time, the DAG consensus method is set up so that when each transaction chooses the tips it wants to approve, instead of choosing them randomly, the MCMC algorithm performs random wandering to prevent attacks [52], [55]–[57]: select the tip at the end of a random walk beginning at the first transaction in the DAG network.

We have to clarify one important issue that, due to the asynchronous nature of propagation, it takes a while for a transaction to be acknowledged by the whole network, so the DAG architecture seen by each node at the same moment may not be the same [46]. So, the DAG network is not strictly a delay-sensitive network [58], then it is widely considered reasonable to apply the MCMC algorithm in the real-time selection of tips [46].

It is easy to see why the MCMC selection algorithm will not select one of the attacker's tips with high probability. The reasoning is identical to the lazy tip scenario: the sites on the parasite chain will have a cumulative weight that is much smaller than the sites that they reference on the main tangle. Therefore, it is not probable that the random walker will ever jump to the parasite chain unless it begins there, and this event is not very probable either because the main tangle contains more sites [55].

B. Workflow and Algorithms of the DAG-Based SIoV Supervision Scheme

The whole procedure of the scheme is shown in Fig. 3, and it is easier to understand in conjunction with Fig. 2.

Information of the SIoV social platform is mainly in the form of images. Vehicles upload the captured images of emergencies or violations to the SIoV platform for social and supervision purposes. For peer disclosure privacy reasons, the entities that are necessary to record the event will be remained, while unrelated vehicles and pedestrians in the images will be encoded by the observer (Fig. 4). As in the sample of reputation-based peer disclosure preventing—the encoded process, vehicles in this event with high reputation will be well protected and those with lower reputation will not be protected as a punishment (Fig. 4). The coded images are bound to the observer's pseudonym, location, and reputation, packaged into a block, and uploaded to the DAG architecture. The specific scoring method, upload conditions, and the process will be introduced as follows.

As is shown in Fig. 2, the information is in the form of blocks on the graph, and the whole graph is expanded in the form of DAG. Each block contains several important pieces of information, one is the reputation value of the uploaded vehicle and the other is the weight of this block. When a new block is uploaded, *k* block tips are selected based on the

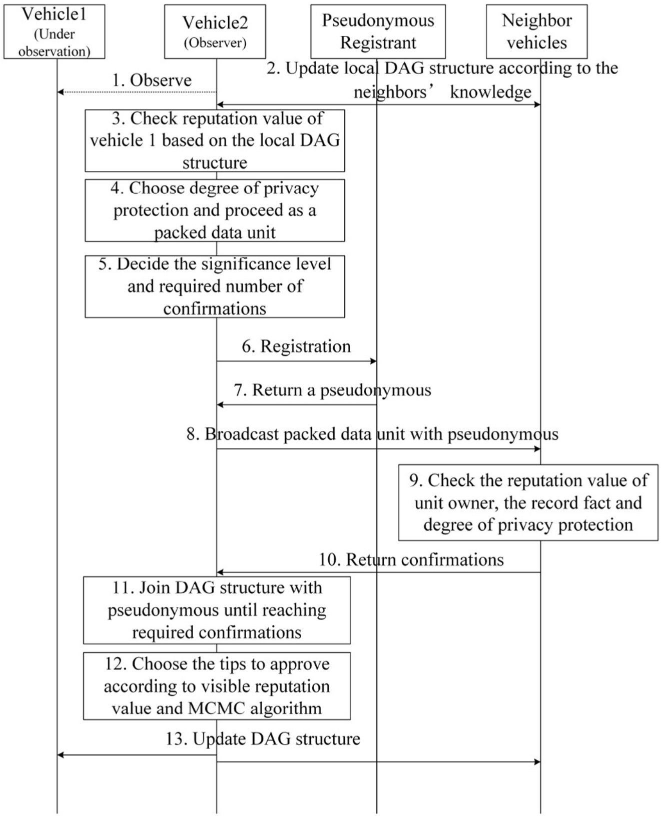

Vehicle1 (Under observation)
Vehicle2 (Observer)
Pseudonymous Registrant
Neighbor vehicles
1. Observe
2. Update local DAG structure according to the neighbors' knowledge
3. Check reputation value of vehicle 1 based on the local DAG structure
4. Choose degree of privacy protection and proceed as a packed data unit
5. Decide the significance level and required number of confirmations
6. Registration
7. Return a pseudonymous
8. Broadcast packed data unit with pseudonymous
9. Check the reputation value of unit owner, the record fact and degree of privacy protection
10. Return confirmations
11. Join DAG structure with pseudonymous until reaching required confirmations
12. Choose the tips to approve according to visible reputation value and MCMC algorithm
13. Update DAG structure

Fig. 3. Detailed workflow of the DAG-based mutual supervision under the SIoV scheme.

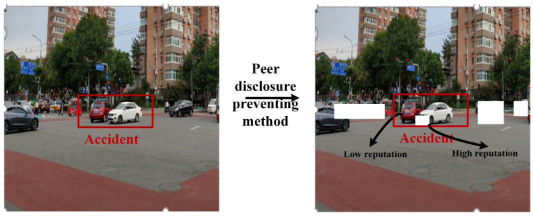


Fig. 4. Sample of reputation-based peer disclosure preventing—the encoded process.

threshold value of the credibility value and the randomness of the MCMC algorithm to be used in the diagram.

If and only if the cumulative weight of a chain reaches a certain threshold, the information on this chain will be acknowledged. Chains with no block selection for a certain period of time will be eliminated. According to the IOTA white paper [46], the DAG network will remain stable under a constant transaction arrival rate. The stable symbol is the stability of the tip number.

For an upload vehicle, the chain in which it uploads blocks being acknowledged fast or getting more weight is the primary goal. The former depends on the choice of the dominant chain and the time it takes to upload, while the latter is not only related to the choice of the chain in which it is located but also to the initial weight of the upload transaction. The initial weight of each block is related to the significance of transactions and also the number of confirmations it gets. Detailed settings and descriptions can be found in the next section.

C. Problem Formulation

First, we assume that the SIoV system consists of a traffic environment with multiple connected intersections and n vehicles as the supervision entities and DAG consensus nodes with an average density ρ. There are violations, traffic accidents, and other events that require uploading and consensus supervision, which we call "transactions" in the scheme. The process of incoming transactions follows a Poisson point process with a rate λ. We assume the rate $\lambda = \rho u$ is linearly related to the density ρ, u is a constant, which is easy to understand that the event happens with higher probability when the vehicle density is high. Vehicles drive along the road with a stable speed v and choose a random direction when arriving at an intersection.

Consider a case that at time t, there is a transaction i, $i \in \{1, 2, \dots, |E^t(n)|\}$ ($|E^t(n)|$ is the total number of transactions at time t) happening and being observed by a vehicle j as a captured image, $j \in \{1, 2, \dots, n\}$. As is shown in Fig. 3, steps 3 and 4, vehicle j checks the significance of the transaction and the reputation value of entities in the captured image to decide the degree of privacy protection. Entities with high reputation will be well protected while low reputation with less protection. This is the motivation of vehicles to mutually protect privacy for other entities.

Here, we measure the privacy information by information entropy. Referring to study [59], the encoding image has quantitative coding metasurfaces of geometrical information and physical information. Here, we consider the physical information entropy since privacy is a physical mapping. On the basis of the image with an assumed far-field pattern, the physical entropy of a coding metasurface is expressed as

$$H = -\sum_{x=1}^{X}\sum_{y=1}^{Y} P_{xy}\log_2 P_{xy}, H \geq 0 \tag{1}$$

where P_{xy} represents the joint probability of an adjacent pixel group, in which contains the gray level x of the current pixel and the gray level y of its adjacent pixel.

Based on the analysis of the level of transaction significance, the weight of transactions is different. We assume that the transaction with high weight is more important, for example, an accident. The transaction with low weight is less important, such as a red light jumping behavior. With this consideration, high weight calls for more confirmations. According to the IOTA white paper [46], the weight of the transaction should be the index of 3. Therefore, we use different confirmation number 3^{α} to reflect in different level of initial weight $IW_{i,j} = 3^{\alpha}$, $\alpha = \{0, 1\}$. Note that if a transaction does not reach the required confirmation number in a limited time, the transaction may lose timeliness and will be discarded. For example, a vehicle observes a red light jumping and misclassifies it as a high significance event, if the vehicle density ρ is too low to reach the high confirmation number, no one could prove the fleeting act after a while. The confirmation probability can be described as

$$P_{i,j}^{\text{confirmation}} = \frac{\varepsilon(\rho)}{3^{\alpha}} \tag{2}$$

where ε is the adjustment factor that indicates $\varepsilon(\cdot) = \arctan(\cdot)$.

A accidentally captured vehicle $j^{'}$ has a privacy leakage probability as

$$H^{\text{leakage}} = HP_{i,j}^{\text{confirmation}} \tag{3}$$

which highly ensures the privacy of accidentally captured vehicle in this scheme.

When reaching the required confirmations, the vehicle will pack the transaction as a new block

$$\text{Block}_{i,j,t} = \left\{i, j, t_i, IW_{i,j}\right\} \tag{4}$$

which indicates that transaction i is observed and uploaded by vehicle j at time t.

Since the DAG graph seen by each node at the same moment is different, we define a new local view of the graph according to the specificity of the vehicle. We define the global graph of DAG at time slot t as $G(t)$ with totally $L(t)$ tips. The local graph of vehicle j at time slot t as $G_j(t)$, where there are totally $N[G_j(t)]$ tips in the view of vehicle j. As for the tip selection process in the DAG network, once a node wants to issue a transaction, it needs to approve k transactions in the former network. Rather than simply random select tips, nodes are required to use the MCMC algorithm to prevent the double-spending attacks from malicious vehicles, which we have introduced in Section IV-A and detailed in [46], [51], and [52].

The update of the local view of the DAG graph is based on the encounters brought by the vehicle movement, which follows gossip [23] principles; therefore, it can be described as:

$$G_j(t) = \bigcup_{\forall \mathrm{Z}_j^t} G_{\mathrm{Z}_j^t}(t) \tag{5}$$

where Z_j^t is the neighbor vehicle set of vehicle j which encounters vehicle j at time slot t.

Assume that in an SIoV system, a block $\text{Block}_{i^{'},j,t}$ is set to be acknowledged for the whole network in T time slots

$$\sum_{b=1,2,\ldots,T} \left(p_g\right)^b = 1. \tag{6}$$

Therefore, the probability of an event $i^{'}$ is acknowledged by vehicle j is

$$P_{i^{'},j,t}{}^{\text{acknowledge}} = \left\{ \begin{matrix} \sum_{b=1,2,\ldots,t-t_{i^{'}}} \left(p_g\right)^b, t - t_{i^{'}} < T \\ 1, t - t_{i^{'}} \geq T \end{matrix} \right\} \tag{7}$$

where p_g is the propagation probability obtained in (6).

To prevent the double-spending attacks and maintain the stability of the DAG network, it has been a standard to use the MCMC algorithm, and the heaviest body of the sub-DAG remained principle. However, the heaviest sub-DAG remained principle is too abstract to guide the SIoV system. Therefore, we try to use some numerical formulas to describe the sub-DAG remained process, where a reputation baseline rv_{base}^t is introduced as a screening of cumulative weight.

Under this assumption, there is a selection principle that only the tips with the uploading entity reaching reputation baseline rv_{base}^t at the moment has the possibility to be chosen

$$rv_{\text{base}}^t = \sigma\beta^{\left[\frac{t}{S}\right]} \tag{8}$$

where σ is the initial baseline of reputation value when $t = 0$, and S the slot number setting in the incentive scheme, where every S slots, the reputation value baseline expands. In this way, sub-DAG with little cumulative weight, which are those transactions with little approvals, will be discarded.

For a chain M in the DAG network, the cumulative weight of the chain is

$$CW_M^t = \sum IW_{i,j}, \text{ for } \forall \text{ Block}_{i,j,t} \in M. \tag{9}$$

Once the cumulative weight has over weighted the weight baseline cw_{base}, each upload entity of the blocks on the chain has a reputation reward

$$CW_M^t \geq cw_{\text{base}}, RV_j^{t+1} = RV_j^t + 1, \text{for } \forall \text{ Block}_{i,j,t} \in M. \tag{10}$$

It has to be noticed that the reputation reward of a specific part on the chain that has reached the cumulative weight baseline and been confirmed only counts one time.

On the other hand, the traditional sub-DAG remain selection process does not clarify how to define the heaviest sub-DAG, how many tips should be contained, and how big the gap between different sub-DAG should be. Therefore, it is hard to conclude what is the best strategy to maintain the performance of DAG. Therefore, we try to find the reputation mechanism settings that maximize the DAG network size under different vehicle densities. The comparison is all held under the stable state of the DAG network, where the tip number $L(t)$ is stable

$$\begin{aligned} \max_{\rho,\beta,S} \quad & \text{Size}[L(t), C(t)] \\ \text{s.t.} \quad & \lim_{t\to\infty} |L(t+1) - L(t)| = h. \end{aligned} \tag{11}$$

Here, the size of DAG is define *BREADTH* as the tip number $L(t)$ and *HEIGHT* as the length of longest chain remained $C(t)$. h is a little threshold that indicates the stability of $L(t)$.

Based on the purposes and the above analysis, we provide a Dmsv algorithm in the next section.

D. DAG-Based Mutual Supervision Algorithm

According to the detailed working flow of the DAG-based SIoV supervision scheme, we propose a Dmsv algorithm in this section. There are mainly six parts in this algorithm: 1) *SYSTEMINITIALIZATION*; 2) *PREPROCESSING*; 3) *REGISTRATION*; 4) *GAINCONFIRMATIONS*; 5) *UPDATE*; and 6) *STABILIZATION*. For each step of the former four parts, the description can be found in the same serial number. The aim of this algorithm is to find the reputation mechanism settings that maximize the DAG network size under different vehicle densities.

V. Performance Analysis

In this section, we simulate the scheme to prove the stability of the DAG-based SIoV network and show the performance of the Dmsv algorithm. We set the vehicle velocity at a constant 15 m/s [60]. The initial reputation baseline σ is fixed as 5. The constant u is defined as 0.3.

TABLE I
COMPARISON IN PRIVACY LOSS AND THE COMPARISON WITH [17]

	vehicle location privacy loss		vehicle identity privacy loss	pedestrian privacy loss
	low vehicle density	high vehicle density		
Proposed Dmsv Scheme	26.82%	27.71%	$\leq$28%	$\leq$28%
Solution for co-location attack in [17]	25%	30%	–	–

```
Algorithm 1 Dmsv Algorithm
Input: Observer vehicle(OV) $j$, under-observation vehicle(UOV) $i$, $\sigma$, $\rho$
Output: $\alpha$, $Pseudonymous$, $Size[L(t), C(t)]$, $\beta$, $S$
    /*SYSTEM INITIALIZATION*/
    Initialize DAG settings $\beta$ and $S$;
    /*PREPROCESSING*/
    1. Observer vehicle $j$ observes an ellegal event and checks the reputation value of an under-observation vehicle $rv_i^t$;
    2. Observer vehicle $j$ update the local DAG structure according to the neighbors' knowledge;
    3. Observer vehicle $j$ determines the significance of the event and the degree of privacy protection $dp_i^t$ for UOV $i$ and compute the required confirmations $\alpha$;
    4. Observer vehicle $j$ proceeds the captured image of $i$;
    5. Observer vehicle $j$ computes own reputation value $rv_j^t$;
    /*REGISTRATION*/
    6. Observer vehicle $j$ sends the ID to pseudonymous registrant;
    7. Pseudonymous registrant returns observer vehicle $j$ a $Pse_j^t$;
    /*GAIN CONFIRMATIONS*/
    8. Observer vehicle $j$ broadcasts the packed data unit of $\left(Pse_j^t, dp_i^t, rv_i^t, encoded\_image\right)$ to its neighbors;
    9. Neighbors check the packed data unit and return confirmations;
    if gains enough confirmation $\alpha$ then
        turns to Step 10;
    else
        turns to Step 1;
    end if
    /*UPDATE*/
    10. Observer vehicle $j$ chooses $k$ tips on DAG structure and issue the new transaction;
    11. Observer vehicle $j$ and neighbors update the local DAG structure;
    /*STABILIZATION*/
    12. repeat Step 2 to 11 for $T$ time slots;
    until reach a stable $L(t)$
    the stable size as $Temp\_Size[L(t), C(t)]$;
    13. repeat $\beta = \beta + \Delta\beta$ and Step 2 to 12 for $R$ times;
    until find the maximum $Temp\_Size[L(t), C(t)]$
    14. repeat $S = S + \Delta S$ and Step 2 to 13 for $R$ times;
    until find the maximum $Temp\_Size[L(t), C(t)]$
    return the maximum $Size[L(t), C(t)]$ and the $\beta$, $S$ under maximum size;
```

A. Analysis on Privacy Loss

First, on the basis of (1), we consider a 256 × 256 traffic image with maximum entropy, that is, the gray level of each pixel is different. The way of image coding is regarded as adjusting the information entropy of the protection area to 0 (as is in Fig. 4). It is easy to understand that with different vehicle and pedestrian densities, the coding processing area is different [see the relation in (2)].

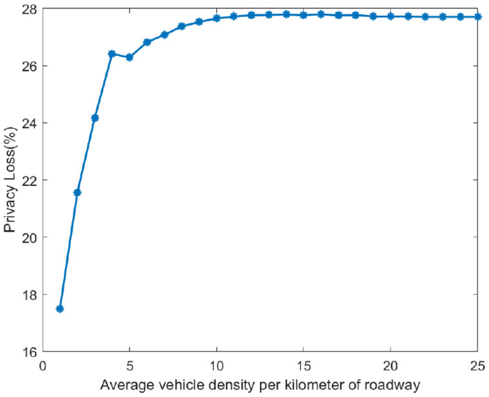


Fig. 5. Influence of average vehicle density in privacy loss.

The fuzz area in the captured image is determined by the relative location (distance) between the observe vehicle and other vehicles. Also, the angle of observation influences the image and the fuzz area a lot. Therefore, we choose an average area (16 pixels per vehicle) of the fuzz process for each entity that needs the peer disclosure prevention process.

Due to the existence of confirmation probability, our scheme can reduce the privacy loss of image entropy leakage probability by at least 72% compared with the upload without any privacy protection (Fig. 5).

Moreover, to prove the feasibility of our proposed scheme, we compare our simulation results with a similar research [17] in privacy loss (see Table I). Considering the fairness of the comparison scheme, we choose the values in [17] that are similar to our parameter settings for comparison. Referring to the quantifying results of co-location prevention solution without obfuscation, where the co-location proportion is 50% (which is close to the upload probability settings in our scheme), we convert the location hiding probability in [17] to the vehicle density for further comparison. It can be seen in Table I that the solution in [17] shows its advantages in vehicle location privacy loss under low vehicle density (around six vehicles per kilometer of roadway) while our proposed Dmsv scheme is superior in high vehicle density (around 25 vehicles per kilometer of roadway). Moreover, our proposed Dmsv scheme protects multidimensional privacy by at least 72%, such as the vehicle identity privacy and pedestrian privacy, which are not considered in [17].

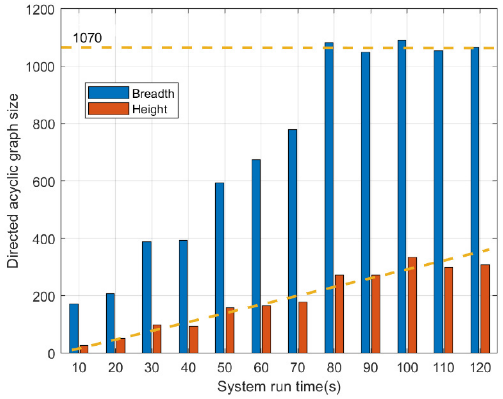


Fig. 6. Influence of time in graph size.

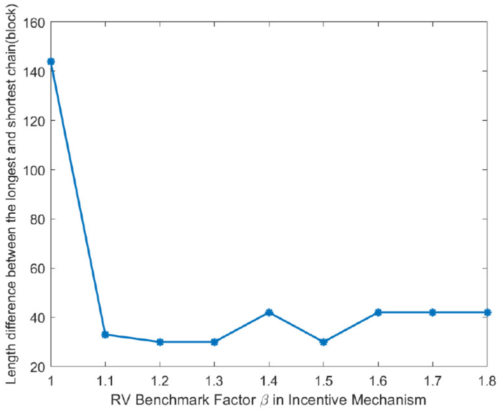


Fig. 7. Influence of RV benchmark β in scheme stability.

B. Analysis on the Stability of DAG-Based SIoV Network

In the DAG network analysis, first and the most important, we demonstrate the stability of our DAG-based SIoV network by the change in the size of the DAG over time. According to the IOTA white paper [46], the stability of the DAG network lies on the stability of tip numbers $L(t)$ in the DAG network, which in our definition, is the *BREADTH* of the DAG network. Here, we define the transaction incoming rate λ as a Poisson point process with an average value of 3. We simulate many times and find the network always trends to a stable state. Therefore, we only present one of the cases that $S = 10$, $\beta = 2$.

As is shown in Fig. 6, the tip number $L(t)$ (*BREADTH*) remains stable around 1070 after 80 s. The length of the longest chain remained in DAG network $C(t)$ (*HEIGHT*) always grow at a linear speed around $\lambda = 3$. This performance of DAG size is fully consistent with the definition of stability and cumulative weight growth in studies [23], [46].

Fig. 7 shows how does the RV benchmark β influences the length gap between the longest and shortest chain, which we think, is another aspect of stability of the DAG-based SIoV network. First, we have to clarify, a double-spending attack is that a malicious node prepares a great number of lightweight transactions with its full computation power, and tries to issue those transactions in a short time to achieve double spending. From this perspective, if the length gap between the longest and shortest chain is very unstable. For example, if the length gap is very close, attackers who issue many transactions at once are more likely to change the cumulative weight of distribution and complete the double-spending attack. Therefore, we believe that a stable length gap with a relatively high value is also one of the conditions for the stability of DAG networks.

Therefore, we adjust the reputation value benchmark β in the incentive mechanism from 1 to 1.8, to analyze the length gap between the longest and the shortest chain in the system where the unit is a transaction. It can be seen that with the increase of β, the length gap fluctuates continuously and finally leveled off, which can provide a prerequisite reference for the subsequent reputation mechanism simulation. The only different case happens when $\beta = 1$ because the reputation value will not change under such settings and, therefore, no vehicles or no transactions will be discarded no matter how they perform. This is very detrimental to the stability of the scheme.

C. Analysis on the Graph Size of DAG-Based SIoV Network

Fig. 8 gives a comprehensive result of how the reputation value benchmark β and S influence the size of the DAG and provides scientific guidance of how the settings should be in the following simulations. We simulate the result all in 100 second, where the DAG networks all reaches a stable state.

First, it is easy to understand that with a transaction incoming rate $\lambda = 3$ in 100 s, the *HEIGHT*, which is also the length of the longest chain is always around 300. The *BREADTH* of DAG shows fluctuations with peaks in both S and beta change simulations. For an already smooth DAG network, larger size means that the system has more possibilities to withstand a higher transaction arrival rate. Therefore, we naturally want to make the graph network larger under smooth conditions by setting the reputation value mechanism. In summary, we conclude that $\beta = 2.2$ and $S = 13$ are the most favorable settings for the graph size under the current setup of such a system. The favorable settings may differ under different traffic conditions, such as the different vehicle density. In the following, we will further explain the fluctuations of these two values physically.

As is shown in Fig. 8(a), $\beta = 1$ is the special case since the reputation value will not change in this case and, therefore, no vehicles will be eliminated no matter how it performs, then, the graph will expand without any limitation. As β increases, the reputation value limit becomes rigorous, the candidate tips are less than before, leading to the possibility of a tip being selected by more than one transaction, then, the breadth will increase. However, when β is greater than 2.2, due to the strict reputation value limitation, the chain elimination rate is greater than the growth rate, which is unfavorable to the size of the graph.

Fig. 8(b) shows how S influences the size of the DAG. When S is too small, the reputation value baseline rises quickly, there will be a lot of chains are eliminated which is unfavorable to the size of the graph. As S increases, the problem slows down, and graph breadth increases. But after S continues to increase, the reputation value baseline rises too slowly, almost

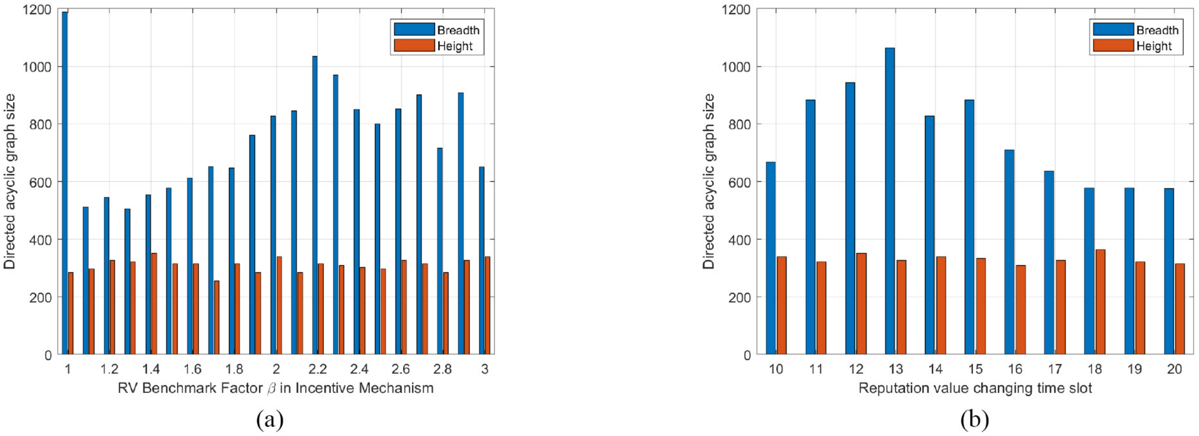


Fig. 8. How the reputation value benchmark β and S influence the size of the DAG. (a) Influence of RV benchmark β in graph size. (b) Influence of RV benchmark S in graph size.

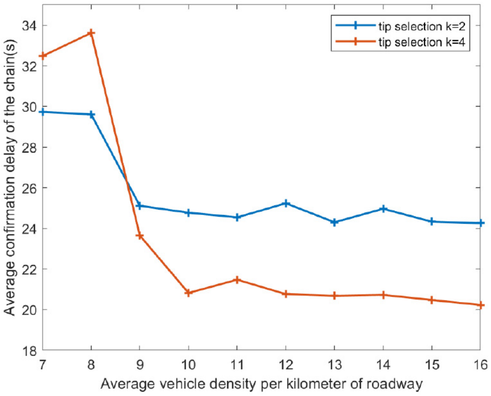


Fig. 9. Influence of vehicle density in chain confirmation delay.

no tips will be eliminated, every vehicle's reputation value status is relatively equal, the upload situation is more average. The possibility of a tip being selected by more than one block is smaller than before, so the breadth will decline.

D. Analysis on the Confirmation Delay

In Fig. 9, we provide how the vehicle density affects the average chain confirmation delay on the graph as well as the comparison between different tip selection k. According to the existed simulation in Fig. 8, here, we set the reputation value mechanism as $\beta = 2.2$ and $S = 13$.

For each curve in this figure, the overall trend shows similar, i.e., a gradual decrease and stabilization. The reason for this trend is that as the vehicle density increases, the rate at which transaction gets enough approvals is faster and the average delay to reach transactional network-wide consensuses decreases. As the vehicle density continues to increase, the competition for tip selection becomes intense, which is detrimental to the latency but will eventually reach a balance and form a stable latency. Such results are also consistent with previous studies [23], [46] and prove the correctness of our algorithm.

As for the comparison between different tip selection k, high tip selection number k leads to lower confirmation delay in the stable state. It is easy to understand that under the same vehicle density, a node choosing four tips is much easier for the former transactions to reach the consensus reputation value. Since the current research all consider $k = 2$, here, we indicate that in our current simulation, the average confirmation delay of the final scheme is about 24 s.

Due to the asynchrony of DAG distributed nodes [23], the algorithm proposed in this article is nondelay sensitive and allows errors caused by delay. Combined with the computing power advantage of the powerful vehicles in the SIoV phase, we think that the delay of 24 s is completely acceptable in our scenario.

VI. Conclusion

This study is designed to solve the peer disclosure problems in the next phase of vehicle intelligence, SIoV. The presented study tries to establish a decentralized blockchain-based scheme for vehicular networks and an incentive-based scheme for mutually distrustful vehicles. Innovatively, a new fast consensus method, DAG, is used in this system to solve the great challenges of vehicle mobility. The simulation is to discuss the effect of vehicle density and incentive mechanism settings. These simulation results confirm the robustness and feasibility of the scheme. Also, some guidance on how to adjust the incentive mechanism according to the vehicular environment is provided. In the next step of our research, more realistic factors in SIoV will be studied, such as the impact and guidance of vehicle performance and road conditions on the implementation of the scheme.

References

[1] X. You *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, Jan. 2021, Art. no. 110301. [Online]. Available: https://doi.org/10.1007/s11432-020-2955-6

[2] X. Hou *et al.*, "Reliable computation offloading for edge-computing-enabled software-defined IoV," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7097–7111, Aug. 2020, doi: 10.1109/JIOT.2020.2982292.

[3] H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks," in *Proc. IEEE 1st Int. Workshop Veh. Commun. Sens. Comput. (VCSC)*, 2012, pp. 12–17, doi: 10.1109/VCSC.2012.6281235.

[4] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, "Privacy-preserved federated learning for autonomous driving," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 16, 2021, doi: 10.1109/TITS.2021.3081560.

[5] J. Wang, C. Jiang, K. Zhang, T. Q. S. Quek, Y. Ren, and L. Hanzo, "Vehicular sensing networks in a smart city: Principles, technologies and applications," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 122–132, Feb. 2018, doi: 10.1109/MWC.2017.1600275.

[6] K. M. Alam, M. Saini, and A. E. Saddik, "Toward Social Internet of Vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.

[7] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in Social Internet of Vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019, doi: 10.1109/ACCESS.2019.2922236.

[8] K. Emara, "Safety-aware location privacy in VANET: Evaluation and comparison," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10718–10731, Dec. 2017, doi: 10.1109/TVT.2017.2736885.

[9] J. Wang, Z. Cai, and J. Yu, "Achieving personalized *k*-anonymity-based content privacy for autonomous vehicles in CPS," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4242–4251, Jun. 2020, doi: 10.1109/TII.2019.2950057.

[10] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A Privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018, doi: 10.1109/TVT.2018.2870167.

[11] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019, doi: 10.1109/TVT.2019.2894720.

[12] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive Internet of Vehicles," *IEEE Netw.*, vol. 34, no. 2, pp. 46–51, Mar./Apr. 2020, doi: 10.1109/MNET.001.1900161.

[13] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018, doi: 10.1109/TITS.2017.2777990.

[14] J. Chen, J. W. Ping, Y. Xu, and B. C. Y. Tan, "Information privacy concern about peer disclosure in online social networks," *IEEE Trans. Eng. Manage.*, vol. 62, no. 3, pp. 311–324, Aug. 2015, doi: 10.1109/TEM.2015.2432117.

[15] V. Pham, S. Yu, K. Sood, and L. Cui, "Privacy issues in social networks and analysis: A comprehensive survey," *IET Netw.*, vol. 7, no. 2, pp. 74–84, Mar. 2018, doi: 10.1049/iet-net.2017.0137.

[16] C. Valliyammai and A. Bhuvaneswari, "Semantics-based sensitive topic diffusion detection framework towards privacy aware online social networks," *Clust. Comput.*, vol. 22, pp. 407–422, Jan. 2019. [Online]. Available: https://doi.org/10.1007/s10586-018-2142-y

[17] A. Olteanu, K. Huguenin, R. Shokri, M. Humbert, and J. Hubaux, "Quantifying interdependent privacy risks with location data," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 829–842, Mar. 2017, doi: 10.1109/TMC.2016.2561281.

[18] N. Vratonjic, K. Huguenin, V. Bindschaedler, and J. Hubaux, "A location-privacy threat stemming from the use of shared public IP addresses," *IEEE Trans. Mobile Comput.*, vol. 13, no. 11, pp. 2445–2457, Nov. 2014, doi: 10.1109/TMC.2014.2309953.

[19] A. Olteanu, M. Humbert, K. Huguenin, and J. Hubaux, "The (co-)location sharing game," *Proc. Privacy Enhanc. Technol.*, vol. 2, pp. 5–25, May 2019, [Online]. Available: https://doi.org/10.2478/popets-2019-0017

[20] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020, doi: 10.1109/TSMC.2019.2896323.

[21] T. Feng, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, 2016, pp. 1–6, doi: 10.1109/ICSSSM.2016.7538424.

[22] W. Yang, X. Dai, J. Xiao, and H. Jin, "LDV: A lightweight DAG-based blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5749–5759, Jun. 2020, doi: 10.1109/TVT.2020.2963906.

[23] Y. Li *et al.*, "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, Aug. 2020, doi: 10.1109/TNET.2020.2991994.

[24] L. Xing, X. Jia, J. Gao, and H. Wu, "A location privacy protection algorithm based on double k-anonymity in the Social Internet of Vehicles," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3199–3203, Oct. 2021, doi: 10.1109/LCOMM.2021.3072671.

[25] G. Kumar *et al.*, "A privacy-preserving secure framework for electric vehicles in IoT using matching market and signcryption," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7707–7722, Jul. 2020, doi: 10.1109/TVT.2020.2989817.

[26] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020, doi: 10.1109/ACCESS.2020.2969820.

[27] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Security Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, New York, NY, USA, 2018, pp. 98–103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.

[28] Z. Li and C. T. Chigan, "On joint privacy and reputation assurance for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 10, pp. 2334–2344, Oct. 2014, doi: 10.1109/TMC.2013.2296513.

[29] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a social structure to the Internet of Things," *IEEE Commun. Lett.*, vol. 15, no. 11, pp. 1193–1195, Nov. 2011.

[30] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[31] A. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, "The cluster between Internet of Things and social networks: Review and research challenges," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 206–215, Jun. 2014.

[32] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.

[33] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th ACM/IEEE Design Autom. Conf. (DAC)*, Jun. 2010, pp. 731–736.

[34] A. Arora and S. K. Yadav, "Block chain based security mechanism for Internet of Vehicles (IoV)," in *Proc. 3rd Int. Conf. Internet Things Connected Technol. (ICIoTCT)*, May 2018, p. 6, doi: 10.2139/ssrn.3166721.

[35] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchainbased electric vehicle charging with dynamic tariff decisions," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, 2017.

[36] I. Dissanayake, J. Zhang, F. Yuan, and J. Wang, "Peer-recognition and performance in online crowdsourcing communities," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, 2015, pp. 4262–4265, doi: 10.1109/HICSS.2015.646.

[37] M. Humbert, B. Trubert, and K. Huguenin, "A survey on interdependent privacy," *ACM Comput. Surveys*, vol. 52, no. 6, p. 122, 2020. [Online]. Available: https://doi.org/10.1145/3360498

[38] X. Zhang *et al.*, "The block propagation in blockchain-based vehicular networks," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8001–8011, Jun. 2022, doi: 10.1109/JIOT.2021.3074924.

[39] J. Herrmann, J. Kho, B. Uçar, K. Kaya, and Ü. V. Çatalyürek, "Acyclic partitioning of large directed acyclic graphs," in *Proc. 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (CCGRID)*, 2017, pp. 371–380, doi: 10.1109/CCGRID.2017.101.

[40] J. Bahri and H. R. S. Borojeni, "Electronic voting through DE-PBFT consensus and DAG data structure," in *Proc. 9th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, 2019, pp. 391–396, doi: 10.1109/ICCKE48569.2019.8965093.

[41] T. Zhou, X. Li, and H. Zhao, "DLattice: A permission-less blockchain based on DPoS-BA-DAG consensus for data tokenization," *IEEE Access*, vol. 7, pp. 39273–39287, 2019, doi: 10.1109/ACCESS.2019.2906637.

[42] K. Cao, F. Lin, C. Qian, and K. Li, "A high efficiency network using DAG and consensus in blockchain," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl. Big Data Cloud Comput. Sustain. Comput. Commun. Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, 2019, pp. 279–285, doi: 10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00049.

[43] T. F. Chiang, S. Y. Chen, and C. F. Lai, "A tangle-based high performance architecture for large scale IoT solutions," in *Proc. 1st Int. Cogn. Cities Conf. (IC3)*, 2018, pp. 12–15, doi: 10.1109/IC3.2018.00012.

[44] N. Živi, E. Kadušic, and K. Kadušic, "Directed acyclic graph as tangle: an IoT alternative to blockchains," in *Proc. 27th Telecommun. Forum (TELFOR)*, 2019, pp. 1–3, doi: 10.1109/TELFOR48224.2019.8971190.

[45] M. Bhandary, M. Parmar, and D. Ambawade, "A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle," in *Proc. 5th Int. Conf. Commun. Electron. Syst. (ICCES)*, 2020, pp. 827–832, doi: 10.1109/ICCES48766.2020.9137858.

[46] S. Popov, "The tangle," Blockchain Lab, London, U.K., White paper, 2018.

[47] S. K. Desai, A. Dua, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, "Cache poisoning prevention scheme in 5G-enabled vehicular networks: A tangle-based theoretical perspective," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2020, pp. 1–6, doi: 10.1109/CCNC46108.2020.9045200.

[48] M. Bhandary, M. Parmar, and D. Ambawade, "Securing logs of a system—An IoTA tangle use case," in *Proc. Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, 2020, pp. 697–702, doi: 10.1109/ICESC48915.2020.9155563.

[49] W. F. Silvano, D. De Michele, D. Trauth, and R. Marcelino, "IoT sensors integrated with the distributed protocol IOTA/Tangle: Bosch XDK110 use case," in *Proc. X Brazilian Symp. Comput. Syst. Eng. (SBESC)*, 2020, pp. 1–8, doi: 10.1109/SBESC51047.2020.9277865.

[50] B. Shabandri and P. Maheshwari, "Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, 2019, pp. 1069–1075, doi: 10.1109/SPIN.2019.8711591.

[51] G. Bu, W. Hana, and M. Potop-Butucaru, "E-IOTA: An efficient and fast metamorphism for IOTA," in *Proc. 2nd Conf. Blockchain Res. Appl. Innovat. Netw. Services (BRAINS)*, 2020, pp. 9–16, doi: 10.1109/BRAINS49436.2020.9223294.

[52] B. Kusmierz, W. Sanders, A. Penzkofer, A. Capossele, and A. Gal, "Properties of the tangle for uniform random and random walk tip selection," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, 2019, pp. 228–236, doi: 10.1109/Blockchain.2019.00037.

[53] M. Ross, *Introduction to Probability Models*, 10th ed. San Diego, CA, USA: Academic Press, 2014.

[54] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 2015.

[55] F. Chen, H. Jia, K. Liu, W. Tang, J. Zhu, and W. Guo, "A new attack method for malicious nodes in tangle network," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, 2020, pp. 84–87, doi: 10.1109/SmartCloud49737.2020.00024.

[56] M. A. Brady, I. Ullah, and P. J. M. Havinga, "DOSing distributed ledger technology: IOTA," in *Proc. IEEE 5th Int. Conf. Cryptogr. Security Privacy (CSP)*, 2021, pp. 55–61, doi: 10.1109/CSP51677.2021.9357600.

[57] G. Bu, Ö. Gürcan, and M. Potop-Butucaru, "G-IOTA: Fair and confidence aware tangle," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2019, pp. 644–649, doi: 10.1109/INFCOMW.2019.8845163.

[58] Q. Wang, T. Wang, Z. Shen, Z. Jia, M. Zhao, and Z. Shao, "Re-Tangle: A ReRAM-based processing-in-memory architecture for transaction-based blockchain," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, 2019, pp. 1–8, doi: 10.1109/ICCAD45719.2019.8942056.

[59] T. Cui, S. Liu, and L. Li, "Information entropy of coding metasurface," *Light Sci. Appl.*, vol. 5, Jun. 2016, Art. no. e16172. [Online]. Available: https://doi.org/10.1038/lsa.2016.172

[60] X. Zhang, J. Zhang, Z. Liu, Q. Cui, X. Tao, and S. Wang, "MDP-based task offloading for vehicular edge computing under certain and uncertain transition probabilities," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3296–3309, Mar. 2020, doi: 10.1109/TVT.2020.2965159.

Yijing Li (Student Member, IEEE) received the B.S. degree from the Mathematics School, Shandong University, Beijing, China, in 2017. She is currently pursuing the Ph.D. degree in communications and information systems with Beijing University of Posts and Telecommunications, Beijing.

Her research interests are in the area of mobile-edge computing network, blockchain, machine learning techniques, and intelligent transportation system.

Xiaofeng Tao (Senior Member, IEEE) received the bachelor's degree in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 1993, and the master's and Ph.D. degrees in telecommunication engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 1999 and 2002, respectively.

He is a Professor with BUPT. He has authored or coauthored over 200 papers and three books in wireless communication areas. He focuses on B5G/6G research.

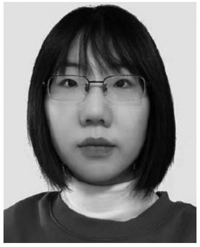
Prof. Tao is the Chair of the IEEE ComSoc Beijing Chapter and a Fellow of the Institution of Engineering and Technology.

Xuefei Zhang (Member, IEEE) received the B.S. and Ph.D. degrees in telecommunications engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2010 and 2015, respectively.

She was visiting the School of Electrical and Information Engineering, University of Sydney, Camperdown, NSW, Australia, from September 2013 to August 2014. She is currently with the National Engineering Laboratory, BUPT. Her research areas include mobile-edge computing, blockchain, reinforcement learning, and intelligent transportation system.

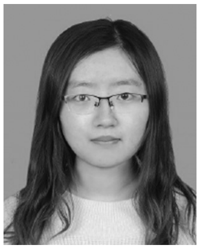
Jin Xu (Member, IEEE) received the B.S. degree in communication engineering from Shandong University, Jinan, China, in 2003, and the Ph.D. degree in circuits and systems from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2008.

She was a Senior Engineer with the Wireless Technology Department, China Mobile Research Institute, Beijing. She is currently an Associate Professor with BUPT. She has authored or coauthored over 40 papers, more than 20 patents, and one book in wireless communications. She focuses on wireless networks and signal processing.



Yisong Wang received the B.S. degree in communication engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2020, where she is currently pursuing the M.S. degree in electrical and information engineering.

Her current research interests mainly focus on blockchain and privacy protection in vehicular networks.



Wenbo Xia received the B.S. degree in communication engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2020, where she is currently pursuing the M.S. degree in electrical and information engineering.

Her current research interests mainly focus on blockchain in vehicular networks.