Lightweight Reputation Management for Multi-Role Internet of Vehicles

Chaogang Tang, *Member, IEEE,* Huaming Wu, *Senior Member, IEEE,* Shuo Xiao

***Abstract*—With the rapid development of the Internet of Vehicles (IoV), smart vehicles can fulfill multiple roles in either the information-centric IoV or the task-oriented IoV. However, malicious vehicles may undermine the trustiness of vehicles towards each other, and further damage these IoV networks. Given the multiple roles undertaken by vehicles in IoV networks, we aim to design a lightweight reputation-based mechanism for a hybrid IoV network in this article. This mechanism can realize real-time reputation updates and synchronization in the device-edge-cloud continuum. Simulation is conducted to validate the reputation management strategy in this article. We also discuss some opportunities and challenges to shed a light on the future research directions in this topic.**

***Index Terms*—Internet of vehicles, task-oriented, reputation update, synchronization.**

I. Introduction

In recent years, we are witnessing a rapid advance in the Internet of Vehicles (IoV) such as the world's first 5G-capable electric car unveiled in China [1]. Familiar scenes in science fiction movies are being reproduced in reality including environmental sensing, autonomous driving, and man-machine interaction. Such advances benefit from not only the integration of internal vehicle networks, inter-vehicle networks and mobile Internet, but also the rapid development of deep learning, natural language understanding, and text-to-speech technologies. The social interactions on the road are also undergoing major changes. For instance, smartphone-centric interaction is being replaced by smart vehicle-centric interaction when people are traveling on the road. Against this backdrop, it seems hardly surprising that there is a startling rise in vehicular applications and services.

Apart from basic service provisioning including safety guarantee and infotainment service, smart vehicles can further fulfill multiple roles depending upon different IoV application paradigms. For instance, in information-centric IoV networks (In-IoV), vehicles disseminate various real-time information and share intriguing multimedia content among themselves using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication technologies. In task-oriented IoV networks (Ta-IoV), typically exemplified by Vehicular Edge Computing (VEC) and Vehicular Fog Computing (VFC), smart vehicles can act as both task initiators and task performers.

C. Tang and S. Xiao are with the School of Computer Science and Technology, China University of Mining and Technology, 221116, Xuzhou, China (e-mail: cgtang@cumt.edu.cn, sxiao@cumt.edu.cn).

H. Wu is with the Center for Applied Mathematics, Tianjin University, 300072, Tianjin, China (e-mail: whming@tju.edu.cn)

Corresponding author: Huaming Wu

Among all the have-to-be-addressed issues, trustworthiness may be the most urgent one in either In-IoV or Ta-IoV [2], [3]. Various V2V wireless links are established among unacquainted or unauthorized vehicles for data transmission, information forwarding, and content sharing. In In-IoV, malicious vehicles could send bogus messages to uninterruptedly undermine the trustiness of vehicles towards each other. In Ta-IoV, malicious vehicles as task performers can send forged feedback to service/application requestors, which can tremendously damage VEC or VFC networks. Many reputation-based coping strategies are used for trustiness-related issues in In-IoV. These works have a wide consensus on trust crisis alleviation when reputation-based strategies are applied.

However, there are no off-the-shelf solutions to the trustiness-related issues in Ta-IoV, which is worthy of further investigation in our view, since it is significant but challenging to prevent some selfish vehicles from delivering low-quality services in Ta-IoV [4]. Given the multiple roles undertaken by vehicles in IoV networks, we make our efforts to design reputation-based mechanisms for both In-IoV and Ta-IoV which are hereafter referred to as a hybrid IoV network (Hy-IoV) in this article. The major contributions are threefold, given below:

- We provide an architectural overview of reputation-based mechanisms in Hy-IoV, where two kinds of Ta-IoV scenarios are given and the roles undertaken by vehicles are also explained in detail.
- We focus on the lightweight reputation design, i.e., real-time reputation update and global synchronization, to cater to the features of Hy-IoV.
- We highlight the opportunities and challenges in Hy-IoV, in the hope to shed a light on the future research directions in this topic.

The remainder of this article is organized as follows. We review the state-of-the-art works that apply the reputation mechanism to various IoV application scenarios. Then, we present a reputation mechanism in a hybrid IoV network and the lightweight reputation design. We also discuss malicious vehicle identification, and some challenges and open issues in this topic.

II. Related Work

Recently, plenty of studies pay attention to the security-related issues in IoV [2], [3], [5], in terms of vehicular communications and task offloading. Some apply blockchain technologies to IoV such as [6], [7], while some apply reputation-based technologies such as [8], [9].

For instance, Tian *et al.* [10] proposed a reputation framework for detecting malicious behaviors such as denial of traffic service in IoV. Road Side Unit (RSU) is responsible for event verification during interactions with vehicles. They introduce market trading-related theories to control the dissemination of false messages from malicious vehicles. Liu *et al.* [11] propose a reputation system, that enables vehicles and RSU to calculate reputation separately. Thus, both vehicles and RSUs can supervise each other. Furthermore, a reliability evaluation module is proposed to identify unreliable results and records.

In the past few years, driving violations are becoming increasingly prevalent among developing countries, which incurs numerous traffic jams and accidents. In view of this, Jabbarpour *et al.* [12] combined blockchain technology with VEC to create a new concept named self-fining vehicle. This kind of vehicle is capable of recording driving violations, issuing tickets, and paying fines in a distributed way. Various emergent technologies, such as encryption, authentication, and blockchain, are applied to the architecture for security-related issues, thus improving the quality of experience.

Instinctively, the message from an untrusted environment cannot be fully reliable. Besides, efficient reward measures are needed to encourage the honest message generator. Against this backdrop, to motivate vehicles as honest message generators, Vishwakarma *et al.* [13] put forward an incentive strategy named SmartCoin using consortium blockchain, aiming to achieve multiple goals such as transportation improvement and traffic jam reduction [14]. Ying *et al.* [15] designed a leader election approach for Opportunistic Autonomous Vehicle Platoon (OAVP) based on reputation, and it consists of a leader election and incentive mechanism. This approach is used for solving trustiness-related issues in OAVP.

III. Reputation Mechanism in Hybrid IoV Network

We give a brief introduction of the two IoV application paradigms in what follows. Then, we present a lightweight reputation model for Hy-IoV that especially considers how to prevent vehicles from delivering poor-quality computing services.

A. Information-centric IoV Application Paradigm

In the In-IoV application paradigm, vehicles can not only connect to Internet, but also interact with each other. With the aid of Vehicular Ad hoc Network (VANET), internet-enabled vehicles can serve multiple purposes, including real-time information (e.g., warning signals) dissemination and content-centric infotainment sharing. Malicious vehicles probably seek sabotage when they are engaged in these behaviors. The damage activities include privacy infringement, content forgery, data revelation, etc. Against this backdrop, it is of paramount importance for IoV to guarantee the reliability of vehicles engaged in these activities.

Numerous works strive to tackle these issues with newly emergent SDN- and Blockchain-based trust models. Although these approaches have obtained satisfactory results to a great extent, they come at the expense of long response delays and the high cost of system maintenance and data storage.

B. Task-oriented IoV Application Paradigm

VFC and VEC are two similar but slightly different Ta-IoV application paradigms. It is foreseeable that, though with slow progress, VFC and VEC will become the workhorse for smart city construction. Nowadays, onboard computers have become the standard configuration for smart vehicles, thus making them capable of computing, storage, and networking. Then, idle computational resources in vehicles can be fully exploited to serve resource requestors including a variety of Internet of Things (IoT) devices. This thought has become the driving force behind the development of VFC in which smart vehicles act as mobile computing nodes for service provisioning.

However, with the explosive growth in vehicular applications/services, these "computers with wheels" are facing a dilemma in satisfying their own computational requirements, let alone service provisioning for others. Such an observation gives rise to the advent of VEC in which vehicles outsource their applications/services in the form of tasks to the edge servers that are usually deployed at RSUs.

As a whole, both VFC and VEC are devoted to response latency reduction compared to the sensor-to-cloud paradigm where IoT tasks and vehicular applications are offloaded to the cloud for execution. The difference lies in that smart vehicles act as task performers and initiators in VFC and VEC, respectively. However, driven by the interest, vehicles probably pursue more benefits by delivering poor quality computing services in VFC, which degrades the quality of service as well as the quality of experience, and is also unfair to those well-behaved vehicles. On the other hand, malicious vehicles can also send fake task offloading requests to RSU, and even pretend to be an edge server for jamming attacks in VEC.

Some blockchain-based approaches, intended for similar issues arise in Ta-IoV, are often seen in the existing literature. However, they do not perfectly suit our focus, i.e., preventing vehicles from delivering poor-quality services or maliciously sending offloading requests.

C. Architecture Overview

Whether it is In-IoV or Ta-IoV, ensuring the reliability of vehicles is vitally important, though the focus and adopted technologies are different. Then, one question naturally arises as to whether there exists one general approach that caters to the features and requirements of both IoV paradigms (i.e., Hy-IoV). To address this issue, we present a lightweight reputation model for Hy-IoV which especially considers how to prevent vehicles from delivering poor-quality computing services.

The architectural model depicted in Fig. 1 consists of one cloud center, RSUs, and smart vehicles. The cloud center is geographically located in a distant place with unfettered computing and storage capabilities. RSUs are deployed along the road in densely populated areas to cover more vehicles via V2I communication technologies. Each vehicle undertakes multiple roles in Hy-IoV. A reputation mechanism is applied for guaranteeing the trustiness of vehicles in Hy-IoV.

Each vehicle will be assigned a score to assess its performance as a participator in Hy-IoV. The score can be regarded as an overall impression within a certain time limit coming

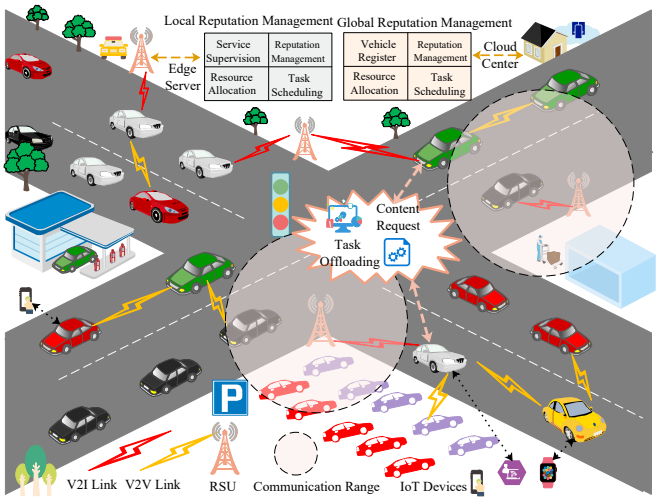


Fig. 1: An architectural overview on the reputation model in Hy-IoV

from vehicles, IoT devices, and RSUs. The reputation value for each vehicle is updated periodically based on the score. Generally, the well-behaved vehicle is rewarded while the deliberately under-performing vehicle is punished. In particular, one vehicle with a reputation value below the given threshold can be viewed as a malicious node in Hy-IoV, and is thus forbidden to participate in activities in Hy-IoV.

It shall be noted that the score comes from the evaluation of the following activities that are categorized based on the roles undertaken by vehicles in Hy-IoV.

- Information Initiator (IN): The vehicle acts as an information initiator to share information among the entities involved in Hy-IoV. Such information includes warning signals, vehicle status, multimedia content, etc. If one vehicle as the information initiator has offensive conduct and intentional sabotage, it may broadcast fake warning signals among vehicles to disturb them and further undermine Hy-IoV.
- Information Transfer (IT): The vehicle acts as an information transfer to forward information-centric data including warning signals, vehicle status, multimedia contents, etc. If the vehicle as the information transfer seeks intentional sabotage, it may illegally intrude, steal, and tamper with the forwarded data, aiming to break the trustiness of vehicles towards each other, and even cause damages to Hy-IoV.
- Task Initiator (TI): As a task initiator, the vehicle offloads vehicular tasks/applications to RSU for execution in VEC, owing to restricted computing capabilities. If a vehicle as the task initiator displays malicious behaviors, it may frequently send fake offloading requests to RSU, and interfere with legitimate offloading requests, therefore lowering the efficiency of Hy-IoV.
- Task Performer (TP): As a task performer, the vehicle executes the tasks offloaded from resource requestors such as IoT devices that have limited computing capabilities. If the vehicle as the task performer displays selfish behaviors, it may deliberately violate Service Level Agreement (SLA) and service statement, by delivering poor-quality computing services.

The former two activities are pretty common in In-IoV. The latter two activities often occur in Ta-IoV, which however has not drawn much attention yet.

IV. Lightweight Reputation Design

Before going further, we first give a formal definition of the reputation concept in this article. The description of reputation, which depends upon the concrete context, generally refers to an opinion that people have towards someone/something, according to the observed behaviors or displayed personality [4]. It is important to note that in Hy-IoV, the reputation of a vehicle is the opinion that other entities involved in Hy-IoV (e.g., IoT devices, vehicles, and RSU) have toward the vehicle, based on the direct or indirect interactions between the entities and the vehicle (e.g., the four discussed activities in Hy-IoV).

A. Reputation Management in Hy-IoV

Reputation management in this article should be efficient and time-saving, considering the features of Hy-IoV such as high mobility, variable topology, and rigorous latency requirements for tasks. Fig. 2 shows the sketch for reputation management for Hy-IoV, in which some key modules are elaborated as follows.

- Score Computation: In the score computation module, the score of one vehicle is calculated based on the impression or opinion that is derived from the evaluation of the engaged activities. For the In-IoV scenario, the impression comes from other vehicles that request or forward the information-centric data. The impression in In-IoV indicates the level of interest from other vehicles. Then, the impressions can constitute a score using linear and nonlinear functions. For the Ta-IoV scenario, the impression mainly comes from entities such as IoT devices and RSUs requesting computing resources/services. The impression in Ta-IoV indicates the level of service that can be achieved from the perspective of service consumers. Similarly, the score can also be represented by a function of these impressions.
- Reputation Aggregation: The reputation values can be propagated using a centralized/distributed way through various network paths in the device-edge-cloud continuum. Then, the reputation aggregation module integrates the collected reputation values into a single value for the vehicle. Many approaches such as simple additive weighting (SAW) technology can be adopted to achieve this goal.
- Reputation Storage: The reputation storage module is of essential importance to reputation management in Hy-IoV. In this article, the cloud center takes charge of reputation storage. Some security measures, such as reputation verification, authentication, authorization, and anti-jamming mechanisms, can be used to secure the reputation value as depicted in the figure.
- Reputation Synchronization: The reputation synchronization model works in a distributed fashion, which requires

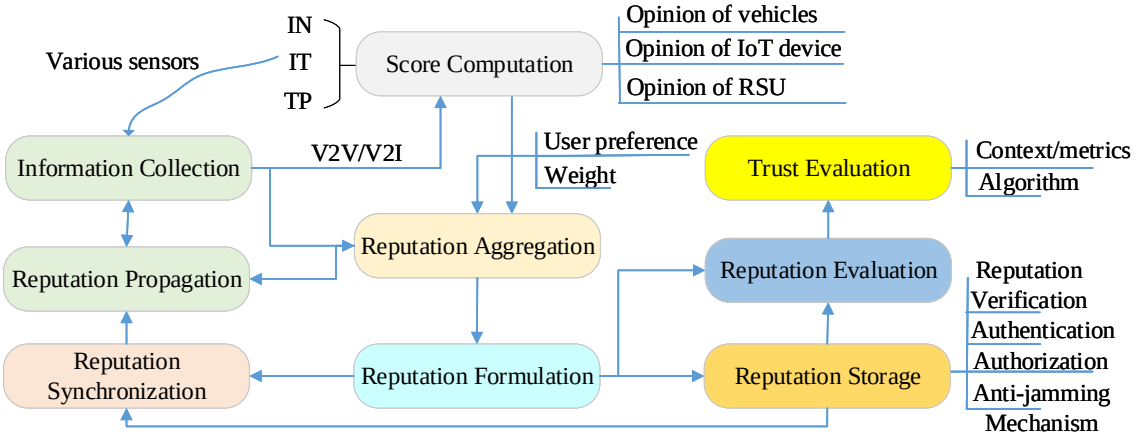


Fig. 2: Sketch for reputation management in Hy-IoV

cooperation between RSU and the cloud center to realize decentralized reputation updating and global reputation synchronization. In particular, RSU deployed with an edge server is responsible for local reputation updating, and the cloud center is responsible for reputation synchronization.

- Reputation Evaluation: The reputation evaluation module aims to construct a reputation list for all the vehicles in Hy-IoV, which is accomplished at the cloud center. To this end, the cloud center needs RSU and IoT devices to send the calculated reputation values in a timely fashion, and then incorporate them into the global reputation values that can be used for trustworthiness assessment.

Owing to the space limitation, we do not detail other modules in Fig. 2, which however does not mean these modules are not as important as the above modules.

B. Lightweight Reputation Updating and Synchronization

In this article, we skip the details of algorithm design for reputation calculation and evaluation but focus on the lightweight reputation management scheme, especially the reputation updating and synchronization in Hy-IoV. We expect that vehicles cannot deliberately manipulate their own reputation. To achieve this purpose, RSU is put in charge of the periodical update for reputation values. In this article, we assume that RSU deploying the edge server can be trustworthy, in the sense that RSUs are deployed and regulated by local government without profit-driven consideration. In the meanwhile, it is also assumed that the involved entities in Hy-IoV, including IoT devices and vehicles, are willing to accept the supervisor of RSU, so the latter can acquire their status information such as location, destination, and speed.

When a vehicle participates in the aforementioned activities, it will be given a score to assess its performance. For instance, when the vehicle as the computing node in Hy-IoV executes IoT tasks, the score can be calculated based on the response latency. Generally, the shorter the response latency, the higher the score. Then, the score is integrated into the reputation of the vehicle based on a predefined reputation aggregation scheme.

The reputation of one vehicle is updated by the covering RSU. In particular, well-behaved vehicles will be rewarded by raising their reputation value, while deliberately underperforming vehicles will be punished by lowering their reputation value. Owing to the limited coverage of RSU and the high mobility of vehicles, RSU is only responsible for covering vehicles. When one vehicle leaves the coverage of its serving RSU, this RSU will stop supervising it, and also stop updating its reputation value. This reputation value is then sent back to the cloud center which is responsible for global reputation synchronization. For instance, when a vehicle gets access to a new area, the serving RSU will download the up-to-date reputation list from the cloud center. Considering the multiple roles undertaken by vehicles in Hy-IoV, the reputation updating and synchronization can be described as follows:

1) Entities such as vehicles and IoT devices in Hy-IoV need to register with the cloud center. The cloud center assigns each entity a unique identification (ID). A default reputation is generated for each vehicle after registration, and the cloud center stores and manages the reputation list for all the vehicles in Hy-IoV.
2) RSU acquires the up-to-date reputation list from the cloud and stores it locally for a period of time. When nearby vehicles participate in the activities, they need to obtain the reputation values of their own and others, with the aim to evaluate the trustiness of the vehicular nodes in Hy-IoV. Vehicles with higher reputation values are more likely to be trusted. IoT tasks tend to be executed by vehicles with high reputation value, and information-centric data from vehicles with high reputation value is more attractive to other vehicles in Hy-IoV.
3) RSU maintains the reputation values for nearby vehicles. On one hand, for the vehicle as IN and IT, RSU gathers the reputation values from other vehicles. On the other hand, for vehicles such as TI and TP, RSU directly calculates the reputation based on the performance of the vehicle. These multi-role reputation values are further aggregated at RSU to form a single value, considering multiple factors such as preferences and importance.
4) When one vehicle leaves the serving area, RSU sends back the reputation value immediately to the cloud cen-

TABLE I: Parameter Settings

Parameter Descriptions	Default Values
The number of vehicles	[10, 30]
Transmit power of vehicles (mW)	80
Transmit power of RSU (mW)	120
The processing capability of RSU (MHz)	1000
Initial reputation	[0,1]
Information-centric data size (KB)	[10, 30]
Task-input data size (KB)	[20,50]
The number of CPU cycles required for tasks	[10,30]
Latency requirement	[0,1]

ter for global synchronization. The vehicle can request its own reputation value from RSU before leaving and from the cloud center at any time.

V. Malicious Vehicle identification

In the beginning, vehicles only have the initial reputation values in Hy-IoV, and it is difficult for our reputation system to identify which vehicles are malicious and which are not. In this case, we assume that there are no malicious vehicles in Hy-IoV. When the number of engaged activities increases, the reputation is gradually accumulated and begins to show a large difference. Then, we use a threshold to distinguish malicious vehicles from normal vehicles in Hy-IoV, given the reputation list. Note that the threshold can change adaptively to cater to the dynamics of Hy-IoV.

To secure vehicular communications and task offloading, malicious vehicles should be punished. As mentioned earlier, some malicious vehicles can be forbidden to participate in activities in Hy-IoV. However, the punishment mechanism should be designed depending upon the malicious extent. By doing so, we can guarantee fairness for those vehicles which only deliver poor-quality computing services and tend to change their selfish behaviors after punishment. For instance, for the vehicles delivering poor-quality computing services, RSU may reallocate IoT tasks that are supposed to be allocated to them, thus reducing their profits in Hy-IoV. Task reallocation occurs with a certain probability that can be set empirically.

VI. Hy-IoV Application Simulation

A simulation is carried out on the reputation management framework for multi-role vehicles proposed in this article. Although four kinds of roles vehicles can undertake, the engaged activities actually fall into two categories, that is, In-IoV scenario and Ta-IoV scenario, respectively. For the sake of simplicity, we randomly generate a set of vehicles that only serve as the information initiators and task performers that belong to the above two categories, respectively. On the one hand, these vehicles disseminate information-centric data through wireless V2V links; On the other hand, they also perform IoT tasks under the supervision of RSUs in Hy-IoV. In addition, some involved parameters in the simulation are depicted in Table I.

Note that the cloud center assigns each vehicle with an initial reputation. As mentioned earlier, the reputation calculation for vehicles in In-IoV is based on the level of interest from other vehicles, while the reputation calculation for vehicles in Ta-IoV is based on the response latency. To cater to the two scenarios, the interest degree follows the uniform distribution. In addition, the reputation calculation for vehicles as the task performers can refer to the previous work [4] and we do not detail it anymore in this article.

The simulation results are depicted in Fig. 3. In particular, Fig. 3(a) shows the reputation variation for the vehicle that always has malicious behaviors along the time slots. We adopt SAW technology to incorporate the two kinds of reputation values, and we pay more attention to the malicious behaviors emerging in Ta-IoV. It is obvious, observed from this figure, that the reputation is decreasing along the time slots. When the reputation value is lower than the predefined threshold, the activities that the vehicle can get involved in are restricted and even forbidden.

On the other hand, Fig. 3(b) shows the reputation variation for the malicious vehicle which displays malicious behaviors with certain probability along the time slots. Specifically, the vehicle has normal behaviors with a probability of 100%, 80%, and 60%, respectively. Obviously, the accumulated reputation values for the vehicle displaying different malicious behaviors are increasing along the time slots. Similar to the conclusion drawn from Fig. 3 (a), the vehicle is punished by increasingly lowering its reputation value, when it has malicious behaviors, in spite of different probabilities.

VII. Challenges

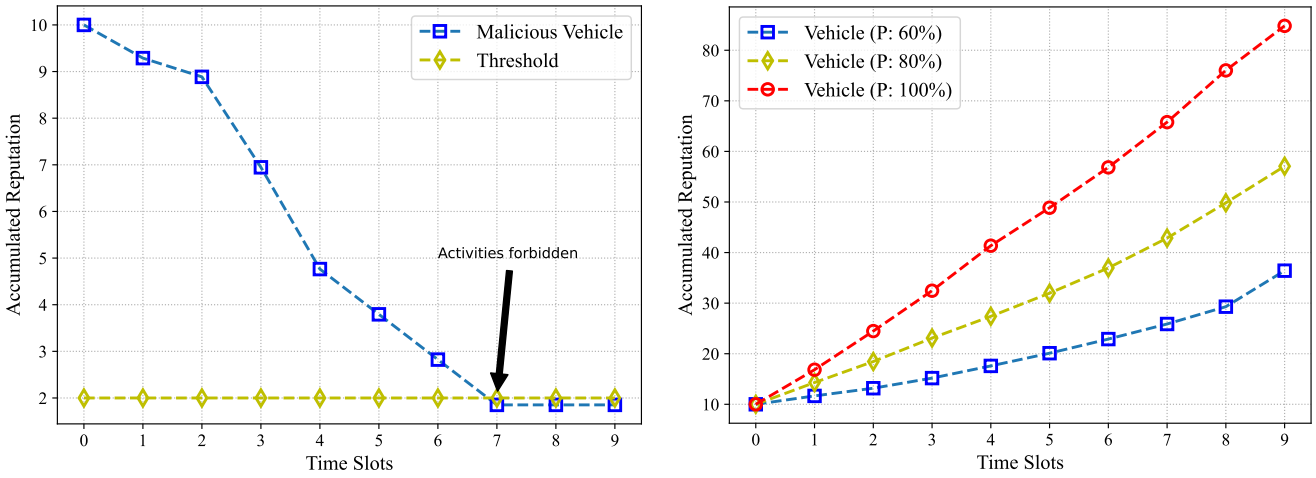
Lightweight reputation management is one of the key enablers for vehicles playing multiple roles in Hy-IoV. However, there are still challenges that urgently need to be solved. Herein, we will explore some of them, in the hope of offering guidance for future directions in this field.

A. Reputation Construction for IoT Device and RSU

In this article, we focus on lightweight reputation management for vehicles in Hy-IoV, under the premise that IoT devices and RSUs are trustworthy in Hy-IoV. However, IoT devices and RSUs may also have malicious behaviors, e.g., they could distort the truth on purpose by rating highly the selfish vehicles delivering poor-quality computing services. In addition, these entities could collude with each other to damage Hy-IoV, and it makes no sense to only investigate the reputation of vehicles in Hy-IoV against this backdrop. As a result, more comprehensive reputation management strategies are required for trustiness-related issues arising in the future.

B. Privacy Protection in Hy-IoV

Although reputation-based schemes for vehicles are investigated in this article, security issues still arise in Hy-IoV. On the one hand, tasks from IoT and vehicles usually implicitly contain task-related purposes, and identity-related information such as personalities and preferences. Such information may be deduced after a vast amount of data is collected by malicious nodes in Hy-IoV. Thus, it is important to avoid



(a) Vehicle with malicious behaviors

(b) Vehicle displaying malicious behaviors with probabilities

Fig. 3: Reputation management in Hy-IoV for vehicles having malicious behaviors including IN and TP

privacy disclosure of user data. Considering the rigorous latency requirements in task offloading and the high mobility of vehicles, lightweight security frameworks and data encryption approaches are still required in Hy-IoV. On the other hand, an extreme case exists, despite the low probability, that is, all the vehicles in Hy-IoV are malicious nodes within a period of time. They can collude together to cause a tremendous burden on front-haul wireless and back-haul links, and further damage the network. Accordingly, algorithms for anomaly detection and attack recognition are required in Hy-IoV.

C. Testbed Construction

To realize practical reputation management for multi-role vehicles in Hy-IoV, we need to consider the costs of deployment, operation and maintenance of the public infrastructure such as RSUs and various reputation strategies. Furthermore, more incentives are required to engage drivers in the aforementioned four activities. Accordingly, there is actually a long way to go before practical deployment, operation, and wide application. As an alternative, it is more cost-effective to design a testbed, in order to flexibly and quickly deploy and investigate various algorithms and reputation management schemes.

VIII. Conclusion

In this article, we presented an efficient reputation management scheme for Hy-IoV, where vehicles can fulfill multiple roles. We made our efforts to give an architectural overview of the reputation-based mechanism in Hy-IoV. In addition, we designed a lightweight reputation management scheme that can realize real-time reputation updates and global synchronization. For future work, we will focus on the fairness issue, especially for newly joined vehicles. They have initial reputation values which may be lower than other well-behaved vehicles. Based on the reputation values, they may not frequently obtain offloading requests, although they have rich computing resources. Thus, it is unfair to these vehicles to some extent. Accordingly, we plan to design a more fair allocation strategy for task offloading requests, aiming to seek a tradeoff between newly joined vehicles rich in computing resources and well-behaved vehicles with high reputation values.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62071327 and Tianjin Science and Technology Planning Project under Grant 22ZYYYJC00020.

References

[1] C. Tang, W. Chen, C. Zhu, Q. Li, and H. Chen, “When Cache Meets Vehicular Edge Computing: Architecture, Key Issues, and Challenges”, *IEEE Wirel. Commun.*, vol. 29, no. 4, pp. 56–62, 2022.

[2] S. Su, *et al.*, “A Reputation Management Scheme for Efficient Malicious Vehicle Identification over 5G Networks, ” *IEEE Wirel. Commun.*, vol. 27, no. 3, pp. 46–52, 2020.

[3] E. Zavvos, *et al.*, “Privacy and Trust in the Internet of Vehicles”, *IEEE Trans. Intell. Transp. Syst.* , vol. 23, no. 8, pp. 10126-10141, 2022. 2019

[4] C. Tang and H. Wu, “Reputation-Based Service Provisioning for Vehicular Fog Computing, ” *J. Syst. Archit.* , vol. 131, pp. 102735, 2022.

[5] A. Hbaieb, S. Ayed, and L. Chaari, “A survey of trust management in the Internet of Vehicles,” *Comput. Networks*, vol. 203, pp. 108558, 2022.

[6] S. Singh, J. Park, P. Sharma, and Y. Pan, “BIIoVT: Blockchain-Based Secure Storage Architecture for Intelligent Internet of Vehicular Things”, *IEEE Consumer Electron. Mag.*, vol. 11, no. 6, pp. 75-82, 2022.

[7] K. Shah, S. Chadotra, S. Tanwar, R. Gupta, and N. Kumar, “Blockchain for IoV in 6G environment: review solutions and challenges”, *Clust. Comput.*, vol. 25, no. 3, pp. 1927-1955, 2022.

[8] X. Bai, S. Chen, Y. Shi, C. Liang, and X. Lv, “Blockchain-based Authentication and Proof-of-Reputation Mechanism for Trust Data Sharing in Internet of Vehicles”, *Ad Hoc Sens. Wirel. Networks*, vol. 53, no. 1, pp. 85-113, 2022.

[9] D. Kianersi, S. Uppalapati, A. Bansal, and J. Straub, “Evaluation of a Reputation Management Technique for Autonomous Vehicles”, *Future Internet*, vol. 14, no. 2, pp.31, 2022.

[10] Z. Tian, X. Gao, S. Su, and J. Qiu, “Vcash: A Novel Reputation Framework for Identifying Denial of Traffic Service in Internet of Connected Vehicles,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3901-3909, 2020.

[11] X. Liu, O. Ma, W. Chen, Y. Xia, and Y. Zhou, “HDRS: A Hybrid Reputation System With Dynamic Update Interval for Detecting Malicious Vehicles in VANETs, ” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 12766-12777, 2022.

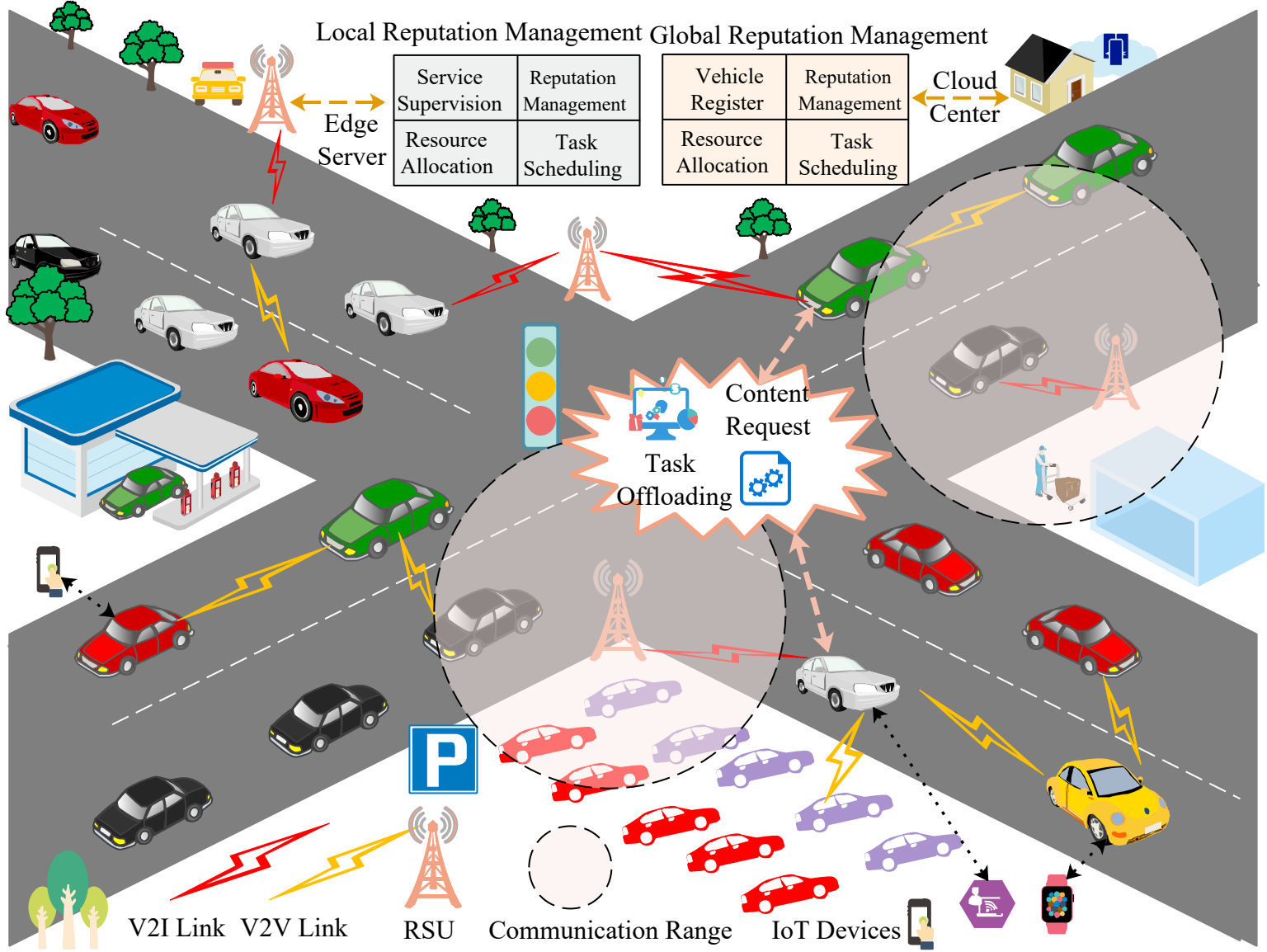
[12] M. Jabbarpour, S. SeyedFarshi, M. Sookhak, and A. Y. Zomaya, "Proposing a Secure Self-Fining Vehicle Using Blockchain and Vehicular Edge Computing", *IEEE Consumer Electron. Mag.*, vol. 11, no. 2, pp. 28-35, 2022.
[13] L. Vishwakarma, and D. Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain," *Veh. Commun.* vol. 33, pp. 100429, 2022.
[14] J. Kang, *et al*, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory, " *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906-2920, 2019.
[15] Z. Ying, *et al*, "A Reputation-Based Leader Election Scheme for Opportunistic Autonomous Vehicle Platoon," *IEEE Trans. Veh. Technol.* vol. 71, no. 4, pp. 3519-3532, 2022.

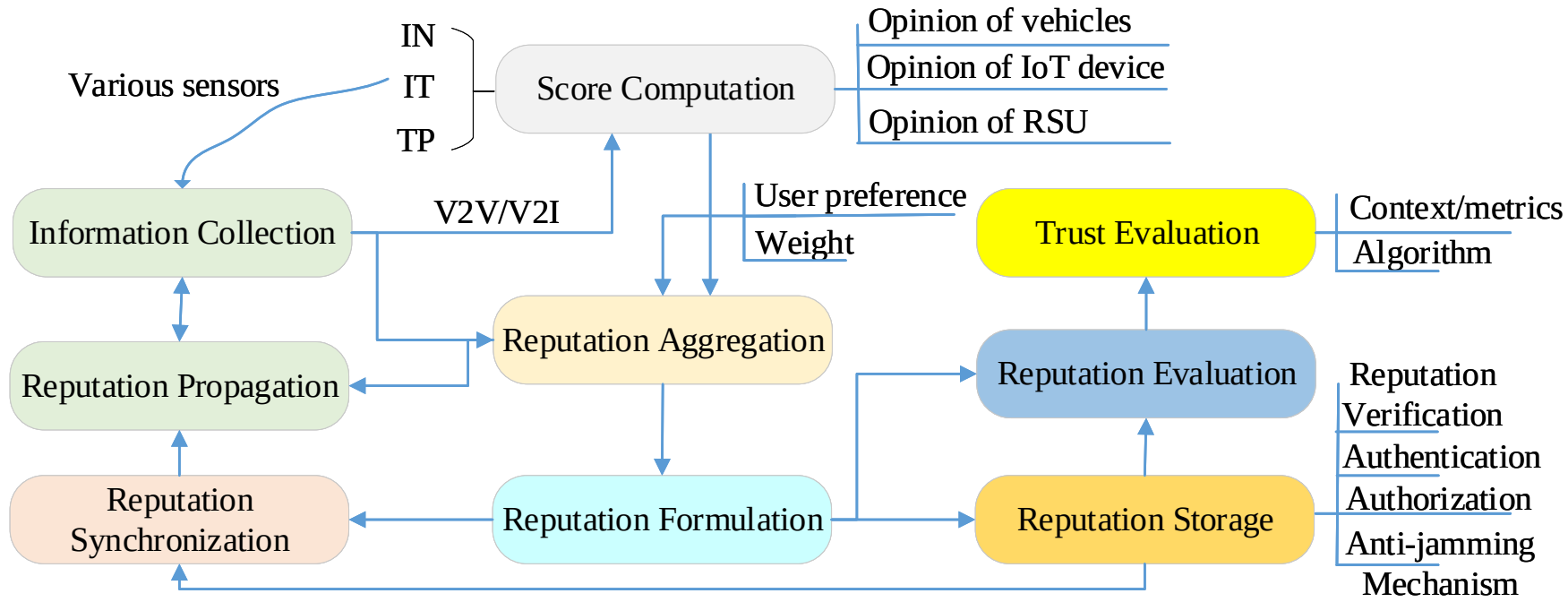
BIOGRAPHY

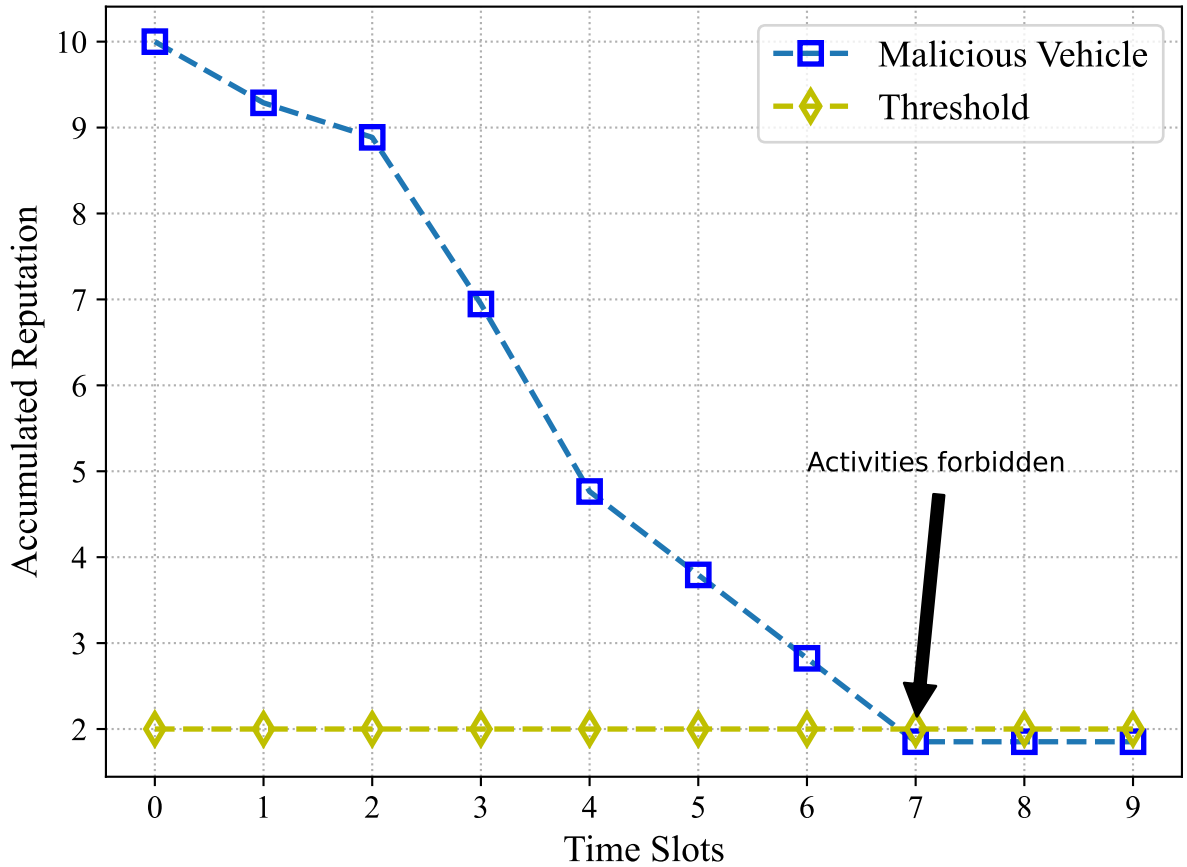
Chaogang Tang received the B.S. degree from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, and Ph.D. degree from the School of Information Science and Technology, University of Science and Technology of China, Hefei, China, and the Department of Computer Science, City University of Hong Kong, under a joint Ph.D. Program, in 2012. He is now with the China University of Mining and Technology. His research interests include mobile cloud computing, fog computing, Internet of Things, big data.

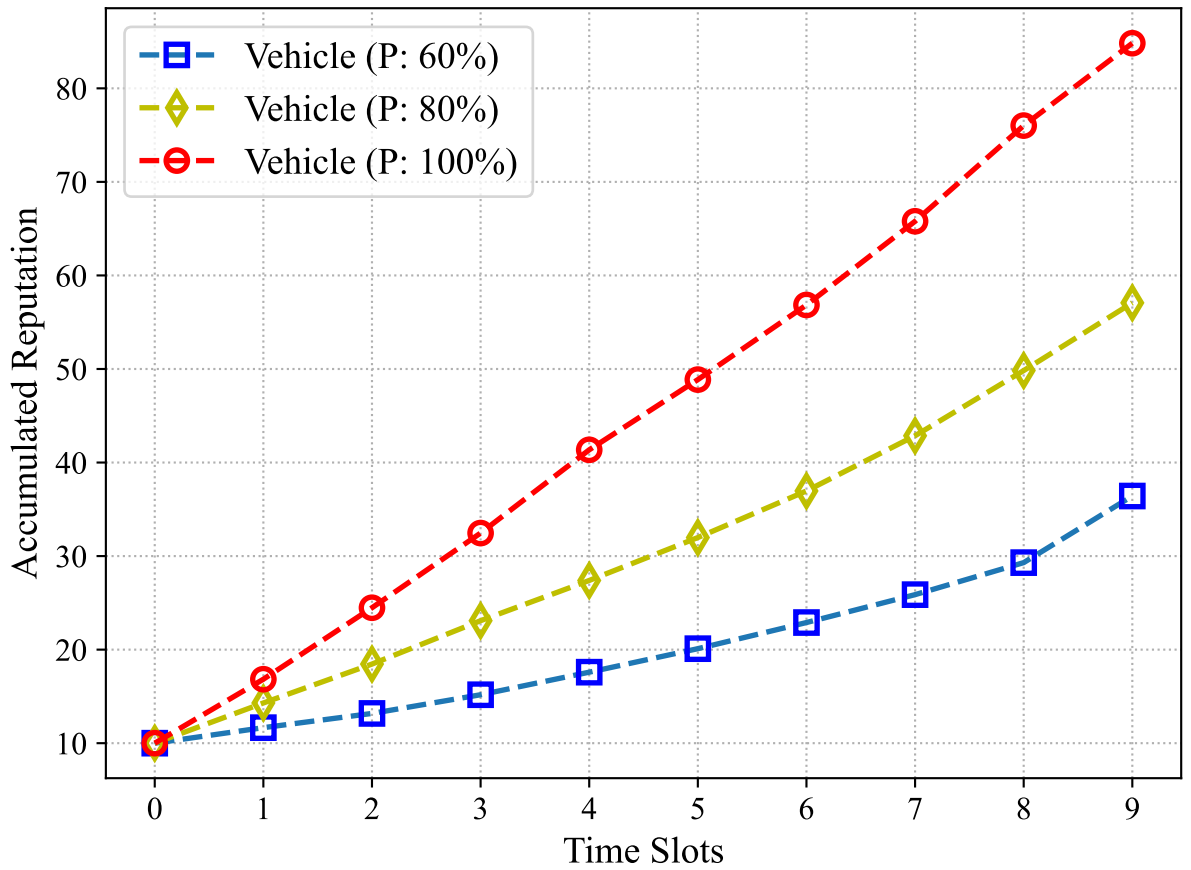
Huaming Wu received the B.E. and M.S. degrees from Harbin Institute of Technology, China in 2009 and 2011, respectively, both in electrical engineering. He received the Ph.D. degree with the highest honor in computer science at Freie Universität Berlin, Germany in 2015. He is currently an ¨ associate professor at the Center for Applied Mathematics, Tianjin University. He is a senior member of IEEE and Associate Editor of IEEE Transactions on Intelligent Transportation Systems. His research interests include wireless networks, mobile edge computing, internet of things and complex networks.

Shuo Xiao received Ph.D. degree in traffic information engineering and control from Beijing Jiaotong University in 2010. He works in China University of Mining and Technology since 2010, where he is now an Associate Professor. His research interests include the Internet of things and measure systems.


Local Reputation Management
Service Supervision
Reputation Management
Resource Allocation
Task Scheduling
Edge Server
Global Reputation Management
Vehicle Register
Reputation Management
Resource Allocation
Task Scheduling
Cloud Center
Content Request
Task Offloading
V2I Link
V2V Link
RSU
Communication Range
IoT Devices


Various sensors
IN
IT
TP
Score Computation
Opinion of vehicles
Opinion of IoT device
Opinion of RSU
Information Collection
V2V/V2I
User preference
Weight
Trust Evaluation
Context/metrics
Algorithm
Reputation Aggregation
Reputation Propagation
Reputation Evaluation
Reputation
Verification
Authentication
Authorization
Anti-jamming
Mechanism
Reputation
Synchronization
Reputation Formulation
Reputation Storage


Malicious Vehicle
Threshold
Activities forbidden
Accumulated Reputation
Time Slots
10
9
8
7
6
5
4
3
2
0
1
2
3
4
5
6
7
8
9


Vehicle (P: 60%)
Vehicle (P: 80%)
Vehicle (P: 100%)
Accumulated Reputation
Time Slots
10
20
30
40
50
60
70
80
0
1
2
3
4
5
6
7
8
9