Crowdsensing Intelligence by Decentralized Autonomous Vehicles Organizations and Operations

Zhengqiu Zhu, Xiao Wang, *Senior Member, IEEE,* Yong Zhao, Sihang Qiu, Zhong Liu, Bin Chen*, and Fei-Yue Wang*, *Fellow, IEEE*

***Abstract*—With the rapid growth of connected and autonomous vehicles (CAVs), vehicular crowdsensing (VCS) has emerged as an effective way in a wide range of applications, especially in intelligent transportation systems. However, centralized VCS frameworks have confronted many problems, such as privacy, security, utility, and dependability. To remedy these challenges, blockchain technology can be applied in VCS systems for effectively forming decentralized autonomous vehicles organizations and operations. This article briefly introduces blockchain-based VCS solutions addressing the current problems and presents potential directions for future research.**

***Index Terms*—Connected and autonomous vehicles, Vehicular crowdsensing, Blockchain technology**

I. Introduction

THE practice of data collection through traditional static sensor networks is not only coverage-limited but also cost-consuming. With the enrichment of social sensors and the development of connected and autonomous vehicles (CAVs), vehicular crowdsensing (VCS) has attracted increasing attention for being effective in collecting specific data and providing precise services [1]. By integrating human and machine intelligence, this promising sensing paradigm makes full use of onboard devices and participating CAVs to collect multi-domain data, further transform the data to cognitive-level information and form crowdsensing intelligence.

Though the current centralized VCS framework brings convenience to collaborative management and control, it also confronts many severe challenges, including but not limited to privacy, security, utility, efficiency, and dependability issues [2]. Taking privacy and security issues as an example, since worker selection often requires personal information and task content are often related to a range of movement, such information may result in personal location and identity information leakage. Besides, malicious participants could be a potential threat to the central mode since they send fake results to gain rewards easily. Without effective solutions to these challenges, the participation confidence of CAVs and the widespread of VCS applications cannot be guaranteed.

Fortunately, the rapid development of blockchain technology in recent years has provided an opportunity to implement a decentralized VCS framework since it spawns the emergence of the so-called Decentralized Autonomous Organization (DAO), a new vehicle organization and operation form that various rules are encoded on a blockchain with the help of smart contracts [3]. Moreover, it can not only operate with third-party intervention but also achieve a transparent, secure, and traceable transaction of data/tasks. Therefore, some blockchain-based solutions are designed and applied to VCS to enhance the performance of VCS-based services [4]. Moreover, to cope with the complexity of social demensions and optimize the decision-making process in the decentralized VCS organizations and operations, the ACP approach and blockchain technology were integrated to construct the parallel VCS system [5].

Although promising, leveraging blockchains to build decentralized autonomous VCS systems is non-trivial and it remains several issues to be addressed [6]. First, public blockchain lack support for data privacy. Second, different entities may misbehave in serving VCS applications. Further, simply putting all workload on-chain would increase the processing costs. To remedy the current literature on "crowdsensing intelligence by decentralized autonomous vehicles organizations and operations", we propose a typical system model of blockchain-based VCS based on existing literature, briefly introduce blockchain-based VCS solutions addressing centralized VCS-related challenges, and present open issues and opportunities for future research.

II. System Model of Blockchain-based VCS

Blockchain is a distributed ledger with natural properties of decentralization, trust, anonymity, and tamper-resistant and is promising to be integrated with CAV systems to address the privacy, security, and utility issues of crowdsensing. Since interactions are traceable and immutable in a blockchain, blockchain-based VCS overcomes various vulnerabilities and improves crowdsensing in various ways, such as improving reliability, introducing a fair evaluation of reward and reputation, preserving sensitive information, and reducing deployment costs. In light of the current research, a typical system model of blockchain-based VCS is proposed, as shown in Fig. 1.

Manuscript received November XX, 2022; revised November XX, 2022; accepted November XX, 2022. This study is supported by the National Natural Science Foundation of China (62173337, 21808181, 72071207), and Humanity and Social Science Youth Foundation of Ministry of Education of China (19YJCZH073). (Corresponding author: Fei-Yue Wang and Bin Chen).

Zhengqiu Zhu, Yong Zhao, Sihang Qiu, Zhong Liu, and Bin Chen are with the College of System Engineering, National University of Defense Technology, Changsha 410073, Hunan Province, China; and also with Hunan Institute of Advanced Technology, Changsha 410073, Hunan Province, China. (e-mail: zhuzhengqiu12@nudt.edu.cn; zhaoyong15@nudt.edu.cn; sihangq@acm.org; phillipliu@263.net; chenbin06@nudt.edu.cn).

Xiao Wang is with the School of artificial intelligence, Anhui University of China, Hefei 230039, Anhui Province, China. (e-mail: xiao.wang@ahu.edu.cn).

Fei-Yue Wang is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China. (e-mail: feiyue@gmail.com).

Digital Object Identifier 10.1109/TIV.2022.XXXXXXX

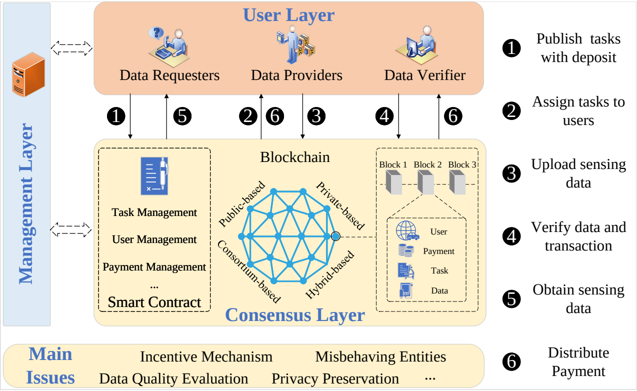


Fig. 1. An illustrative system model of blockchain-based VCS.

The system model is mainly divided into three layers: the user layer (different entities involved), the consensus layer, and the management layer [7]. The user layer is mainly responsible for handling various interactions between participating entities and the crowdsensing system. The consensus layer transmits and records various transaction information based on the blockchain network to ensure worker privacy, data security, and system efficiency. The management layer, connected by dotted arrows, is not necessarily needed in a specific blockchain-based VCS application. On-chain processing incurs a monetary cost, so simply putting all workload on-chain is highly uneconomical. Thus, it is required to realize a delicate joint on-chain and off-chain design. The management layer here is used to cope with the issues (e.g., worker reputation management) on an off-chain network to enhance execution efficiency and save execution costs.

There are mainly three kinds of entity roles in the user layer: data requester, data provider (or worker, participants), and data verifier. The requester publishes the task to the blockchain to obtain information meeting his/her needs and provide corresponding rewards. The data provider is the participating vehicle that undertakes the tasks on the blockchain. They can choose to accept tasks from a public or private blockchain according to their privacy considerations. Once the task is completed and the required data is uploaded, the data provider will be rewarded according to their contributions. While the data verifier is responsible for generating new transactions, verifying the data quality, fixing the problems, and recording them on the ledger. Since data verifiers contribute to evaluation and recording, they deserve to obtain part of the transaction costs or rewards. It is noteworthy that the identity of an entity is not fixed, that is to say, a participating user on the blockchain can be either a data provider or a data verifier.

Four categories of blockchain can be used to construct the blockchain part of the system model: public, private, consortium, or hybrid [8]. The different categories vary in their properties where the respective blockchain can be selected according to the needs of the system model. A public blockchain-based model is permissionless and open for any interested user to join, gather, allocate, and process the information through a consensus mechanism as Service Level Agreement. While a private blockchain-based model is permissioned and has certain restrictions to access the information for different entities in a VCS platform. Unlike a public blockchain, transactions are recorded by selected verifiers from the same organization. And thus, it can be designed to support some critical factors, such as privacy, security, and reliability. The consortium blockchain-based model is semi-decentralized and has a pre-selection ability to indicate the type of intelligent services in the VCS platform. A hybrid blockchain-based model integrates public and permissioned types of blockchain, in which a feature-based approach is applied to support a flexible environment for sharing secured information and easy for users to join contracts.

The functional components with respective computational mechanisms are implemented as smart contracts and hosted on blockchains. In a typical blockchain-based VCS application, a variety of smart contracts are used to transmit and record information, including user management smart contracts, task management smart contracts, compensation management smart contracts, etc. Among these, user management contract is designed to maintain and update user addresses, types, and reputation; task management contract is used to select task-worker pairs; and payment management contract is used to pay reasonable rewards to workers. The operation process of the decentralized VCS system generally includes six steps: 1) requesters release the tasks along with the data quality criteria, and advance the deposit; 2) a certain smart contract assigns tasks to appropriate workers according to the matching mechanism; 3) workers perform tasks and upload sensed data to the network; 4) verifiers evaluate the data quality and checks the legitimacy of the transaction; 5) the requester receives the data and releases subsequent rewards; 6) a certain smart contract sends rewards to workers and verifiers.

III. The Current Focus of Blockchain-based VCS

DAO paves the way for the design of decentralized autonomous VCS systems. Regarding blockchain-based VCS systems, existing studies focus on coping with the issues of location privacy preservation of participants, misbehaving entities, data quality control, incentive mechanism design, reputation management, sensitive data privacy-protection, etc [9]. This section follows a short introduction to these issues.

A. Blockchain-based location privacy and identity preservation

Current studies typically integrate blockchain, location obfuscation, and smart contract design to address the privacy issue. When a VCS application is deployed on a public blockchain, a specified mechanism is required to ensure privacy preservation, such as differential and distortion location privacy technology. Besides, instead of novel location obfuscation mechanisms, the features of private blockchain can be used to provide a secure environment. The study in [7] proposed a blockchain-enabled conditional decentralized VCS by exploring the characteristics of participating entities. Specifically, a strict privacy preservation scheme where the zk-SNARK proof is integrated with a mixed task smart contract was designed to ensure that the transaction content in the blockchain would not reveal any private information of participants. With the designed scheme, both privacy disclosure can be prevented and data confidentiality can be guaranteed. To tackle location and re-identity attacks, Yang et al. [10] proposed a MCS platform comprising several private blockchain networks and a public blockchain network. The operational process of this platform can be mainly divided into four steps: (1) requesters initiate and submit tasks to the public blockchain; (2) agents (associate miners between public blockchains and private blockchains) upload a copy of tasks to a private blockchain; (3) a smart contract allocates rewards to participants who complete tasks and contribute to blockchains (e.g., both private and public); (4) agents submit the sensed data to a public blockchain. The innovative task allocation mechanism proposed in this work ensures that the location and identity information of participants are invisible to the MCS platform.

B. Blockchain-based solutions to misbehaving entities

In a typical VCS system, the entities include requesters, participants, and a centralized platform. The different entities may misbehave, for instance, the recruited workers submit false sensing data; the requesters upload a number of tasks during a short time interval to clog the centralized server providing service for other requesters; a misbehaving platform intentionally modifies the reputation scores of participants or adjusts evaluation results of submitted data [11]. Relying on smart contracts, DAO's operational rules, participants' responsibility and authority, and the rewards and penalties terms are open and transparent. To address these security threats, the study in [12] presented a consortium blockchain-based VCS system (namely VeSenChain), which is transparent and traceable for miners accessing all interactions. The decentralized VeSenChain system tackles the security threat using a tamper-proof feature and ensures authenticity by registration on the chain. Moreover, intelligent organizations and operations among different entities (i.e., requesters, workers, and roadside units) are supported by an interactive protocol based on smart contracts. All VCS activities transactions and service requests generated by requesters are recorded in a smart contract and thus enable a secure and transparent interactive environment. Before participating in sensing tasks or acquiring services, CAVs are required to register into VeSenChain first.

C. Consensus-driven quality control

It is a significant issue to ensure data quality in crowdsensing activities since it could be impacted by many factors, such as CAVs' movements, the precision of the embedded sensors, and the quality of communication channels. Different from traditional solutions, the study in [13] proposed a blockchain consensus-driven quality control model for crowdsensing. In the system model, a verifier selection mechanism and a two-times consistency policy are devised to build system credibility and integrity. The whole operation process of the proposed system is organized within 11 steps and two consensuses. Before sending the sensed data to the requester, the verifier is responsible for evaluation through a novel approach, which integrates fuzzy logic theory and circuit-breaking technology for protecting evaluation criteria. After the workers upload sensed data, the verifier produces a Merkle tree published to the whole network and the system achieves the first consensus. Besides, the verifier also generates the grades for the data quality assessment in order to determine the rewards of workers. After that, the verifier generates another Merkle tree based on previous Merkle trees and other factors (e.g., worker's identity and reward). The second consensus is achieved after the new Merkle tree is generated and published.

D. Blockchain-based incentive model

As a distributed ledger, blockchain is applied in crowdsensing to resist security risks in the incentive process. The existing blockchain-based crowdsensing incentive models can be roughly classified into two categories: main incentive goal and rewards form [14]. The main incentive goal refers to the abovementioned issues, such as service quality-oriented, privacy security-oriented, trusted transaction-oriented, and hybrid target oriented. While incentive models based on rewards form can be divided into social service, game playing, and monetary reward. Among these models, the study in [15] proposed a decentralized architecture built on the consortium, taking both economic incentives and data quality into account. Blockchain technology eliminates the need for a trusted third party. In this work, the authors proposed a hybrid incentive approach considering data quality, reputation, and monetary awards to boost worker willingness to participate in sensing tasks and submit sensed data. The proposed reward model achieves a remarkable improvement of the task initiator's utility compared to the state-of-the-art incentive models. Another incentive model using zero-knowledge proof methods [16] can achieve information privacy protection, but contract execution costs are relatively high. In summary, the existing blockchain-based crowdsensing incentive models have their merits and limitations.

IV. Open Issues in Blockchain-based VCS

Through the introduction and discussion in previous sections, we have understood the existing studies of crowdsensing intelligence by decentralized autonomous vehicles organizations and operations. However, a number of related open issues have not been deeply investigated and remain addressed. First, it is promising to address threat modeling in VCS using blockchain techniques. Since DoS attacks, malware attacks, and eavesdropping attacks in VCS systems are not fully addressed by blockchain-based approaches and blockchain is capable of mitigating these attacks due to its natural properties. Besides, to achieve accurate evaluation and verification, most of the entities in the blockchain would participate in the process. As the number of sub-tasks and participants increases, the multi-point verification feature may cause a decrease in the execution efficiency and further magnify the execution costs. Therefore, it is promising to study the design of on-chain and off-chain scheme to save costs as well as a reasonable verification mechanism to improve efficiency. Moreover, with the increase of entities' privacy preservation requirements and the increasingly complex and changeable sensing scenarios, the single-chain structure can no longer meet the sensing requirements. Therefore, it is necessary to study practical multi-chain structures to cope with the multi-domain complex environment. For instance, the incentive model can be integrated with a cross-chain consensus mechanism to realize multi-domain crowdsensing. Last but not the least, we also need to break through the technical limitations and security issues of DAO itself to further improve the decentralized self-organization of VCS, so as to achieve extensive applications.

References

[1] Z. Zhu, Y. Zhao, B. Chen, S. Qiu, Z. Liu, K. Xie, and L. Ma, “A crowd-aided vehicular hybrid sensing framework for intelligent transportation systems,” *IEEE Trans. intell. vehicl.*, p. early access, Oct. 2022, doi: 10.1109/TIV.2022.3216318.

[2] Z. Chen, C. Fiandrino, and B. Kantarci, “On blockchain integration into mobile crowdsensing via smart embedded devices: A comprehensive survey,” *J syst architect*, vol. 115, p. 102011, Jan. 2021, doi: 10.1016/j.sysarc.2021.102011.

[3] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang, and F.-Y. Wang, “Decentralized autonomous organizations: Concept, model, and applications,” *IEEE Trans. comput. soc. sy.*, vol. 6, no. 5, pp. 870–878, Sept. 2019, doi: 10.1109/TCSS.2019.2938190.

[4] P. Lang, D. Tian, X. Duan, J. Zhou, Z. Sheng, and V. C. Leung, “Cooperative computation offloading in blockchain-based vehicular edge computing networks,” *IEEE Trans. intell. vehicl.*, vol. 7, no. 3, pp. 783–798, Jul. 2022, doi: 10.1109/TIV.2022.3190308.

[5] Y. Ren, H. Jiang, X. Feng, Y. Zhao, R. Liu, and H. Yu, “Acp-based modeling of the parallel vehicular crowd sensing system: Framework, components and an application example,” *IEEE Trans. intell. vehicl.*, vol. early access, pp. 1–13, Nov. 2022, doi: 10.1109/TIV.2022.3221927.

[6] D. Cao, X. Wang, L. Li, C. Lv, X. Na, Y. Xing, X. Li, Y. Li, Y. Chen, and F.-Y. Wang, “Future directions of intelligent vehicles: Potentials, possibilities, and perspectives,” *IEEE Trans. intell. vehicl.*, vol. 7, no. 1, pp. 7–10, Mar. 2022, doi: 10.1109/TIV.2022.3157049.

[7] P. Zhao, C. Li, Y. Fu, Y. Hui, Y. Zhang, and N. Cheng, “Blockchain-enabled conditional decentralized vehicular crowdsensing system,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18 937 – 18 950, Apr. 2022, doi: 10.1109/TITS.2022.3166216.

[8] Z. Sisi and A. Souri, “Blockchain technology for energy-aware mobile crowd sensing approaches in internet of things,” *T emerg telecommun t*, p. early access, Jan. 2021, doi: 10.1002/ett.4217.

[9] C. Xu, H. Wu, H. Liu, W. Gu, Y. Li, and D. Cao, “Blockchain-oriented privacy protection of sensitive data in the internet of vehicles,” *IEEE Trans. intell. vehicl.*, p. early access, Apr. 2022, doi: 10.1109/TIV.2022.3164657.

[10] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, “A blockchain-based location privacy-preserving crowdsensing system,” *Future gener comp sy*, vol. 94, pp. 408–418, May. 2019, doi: 10.1016/j.future.2018.11.046.

[11] M. Kadadha, H. Otrok, R. Mizouni, S. Singh, and A. Ouali, “Sensechain: A blockchain-based crowdsensing framework for multiple requesters and multiple workers,” *Future gener comp sy*, vol. 105, pp. 650–664, Apr. 2020, doi: 10.1016/j.future.2019.12.007.

[12] J. Zhang, X. Huang, W. Ni, M. Wu, and R. Yu, “Vesenchain: Leveraging consortium blockchain for secure and efficient vehicular crowdsensing,” in *2019 Chinese Control Conference (CCC)*. IEEE, Guangzhou, China, 2019, pp. 6339–6344.

[13] D. Liang, J. An, J. Cheng, H. Yang, and R. Gui, “The quality control in crowdsensing based on twice consensuses of blockchain,” in *UbiComp 2018*. ACM, New York, NY, United States, 2018, pp. 630–635.

[14] X. Xu, J. Cheng, J. Liu, Y. Yuan, H. Li, and V. S. Sheng, “A survey of blockchain-based crowd sensing incentive mechanism,” in *International Conference on Artificial Intelligence and Security*. Springer, Qinghai, China, 2022, pp. 245–259.

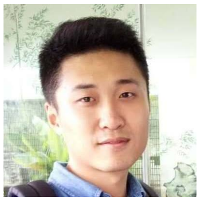
[15] L. Wei, J. Wu, and C. Long, “A blockchain-based hybrid incentive model for crowdsensing,” *Electronics*, vol. 9, no. 2, p. 215, Jan. 2020, doi: 10.3390/electronics9020215.

[16] L. Wang, Z. Cao, P. Zhou, and X. Zhao, “Towards a smart privacy-preserving incentive mechanism for vehicular crowd sensing,” *Security and Communication Networks*, vol. 2021, May. 2021, doi: 10.1155/2021/5580089.

Zhengqiu Zhu received the B.E. and M.E. degree in Simulation Engineering from National University of Defense Technology, Changsha, China, in 2016 and 2018, where he is currently pursuing the Ph.D. degree in the College of Systems Engineering. He was also a visiting Ph.D. student in the research group of Multi-scale Networked Systems at University of Amsterdam (UvA). He has authored or coauthored more than 30 publications in international refereed journals and conferences. His research interests include mobile crowdsensing, ubiquitous computing, and social computing.

Xiao Wang (Senior Member, IEEE) received the B.E. degree in network engineering from the Dalian University of Technology, Dalian, China, in 2011, and the M.E. and Ph.D. degrees in social computing from the University of Chinese Academy of Sciences, Beijing, China, in 2013 and 2016, respectively. She is currently the President of Qingdao Academy of Intelligent Industries and an Associate Professor with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. She has authored or coauthored more than 60 publications in international refereed journals and conferences. Her research interests are cyber-physical-social systems, social computing, social transportation, cognitive intelligence, especially in aspects of social network analysis, data fusion, multiagent modeling, and computational experiments. She served the IEEE Transactions on Intelligent Transportation Systems, the IEEE/CAA Journal of Automatica Sinica, and ACM Transactions on Intelligent Systems and Technology as a Peer Reviewer with a good reputation. As a Member of IEEE Intelligent Transportation Systems Society (ITSS) BoG, she always cooperates with the other BoG members to advance important initiatives of the society, give full play to the role of female researchers in ITSS activities, and spread the worthy ideas to the society.

Yong Zhao received the B.E. degree in Simulation from National University of Defense Technology, China, in 2019, where he is currently pursuing the master degree with Control Science and Engineering. His research interests include Reinforcement Learning, autonomous searching and crowd sensing. He is now working on localization the odor source using mobile sensors.



Sihang Qiu received his Ph.D. from the Web Information Systems group of TU Delft in 2021 and is an assistant professor at College of Systems Engineering of National University of Defense Technology. He is interested in developing novel human-AI interaction techniques. He has authored or coauthored more than 30 publications in international refereed journals and conferences. His research also focuses on human-centered AI, crowd computing, and conversational agents.

Zhong Liu obtained his Ph.D. in System Engineering and Mathematics from National University of Defense Technology and and also a professor of Science and Technology on Information Systems Engineering Laboratory. He is also the member of the National Artificial Intelligence Strategy Advisory Committee. His main research interests include artificial general intelligence, deep reinforcement learning, and multi-agent systems.

Bin Chen the corresponding author, received his B.E., M.E. and Ph.D. degree in Control Science and Engineering from National University of Defense Technology (NUDT) in 2003, 2005 and 2010. He is currently an associate research fellow in the College of Systems Engineering at National University of Defense Technology. He has authored or coauthored more than 100 publications in international refereed journals and conferences. His current research focuses on ACP-based simulation running support, parallel experimental method, data mining, mobile crowdsensing and micro-task crowdsourcing.

Fei-Yue Wang (Fellow, IEEE) received the Ph.D. degree in computer and systems engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1990. He joined The University of Arizona, Tucson, AZ, USA, in 1990, and became a Professor and the Director of the Robotics and Automation Laboratory and the Program in Advanced Research for Complex Systems. In 1999, he founded the Intelligent Control and Systems Engineering Center, Institute of Automation, Chinese Academy of Sciences (CAS), Beijing, China, under the support of the Outstanding Chinese Talents Program from the State Planning Council, and in 2002, was appointed as the Director of the Key Laboratory of Complex Systems and Intelligence Science, CAS, and the Vice President of the Institute of Automation, CAS, in 2006. In 2011, he became the State Specially Appointed Expert and the Founding Director of the State Key Laboratory for Management and Control of Complex Systems. He has been the Chief Judge of Intelligent Vehicles Future Challenge since 2009 and the Director of China Intelligent Vehicles Proving Center, Changshu since 2015. He is currently the Director of Intel's International Collaborative Research Institute on Parallel Driving with CAS and Tsinghua University, Beijing, China. His research interests include methods and applications for parallel intelligence, social computing, and knowledge automation. He is a Fellow of INCOSE, IFAC, ASME, and AAAS. In 2007, he was the recipient of the National Prize in Natural Sciences of China, numerous best papers awards from IEEE Transactions, and became an Outstanding Scientist of ACM for his work in intelligent control and social computing. He was the recipient of the IEEE ITS Outstanding Application and Research Awards in 2009, 2011, and 2015, respectively, IEEE SMC Norbert Wiener Award in 2014. He became the IFAC Pavel J. Nowacki Distinguished Lecturer in 2021. Since 1997, he has been the General or Program Chair of more than 30 IEEE, INFORMS, IFAC, ACM, and ASME conferences. He was the President of the IEEE ITS Society from 2005 to 2007, IEEE Council of RFID from 2019 to 2021, Chinese Association for Science and Technology, USA, in 2005, American Zhu Kezhen Education Foundation from 2007 to 2008, Vice President of the ACM China Council from 2010 to 2011, Vice President and the Secretary General of the Chinese Association of Automation from 2008 to 2018, Vice President of IEEE Systems, Man, and Cybernetics Society from 2019 to 2021. He was the Founding Editor-in-Chief (EiC) of the International Journal of Intelligent Control and Systems from 1995 to 2000, IEEE ITS Magazine from 2006 to 2007, IEEE/CAA JOURNAL OF AUTOMATICA SINICA from 2014 to 2017, China's Journal of Command and Control from 2015 to 2021, and China's Journal of Intelligent Science and Technology from 2019 to 2021. He was the EiC of the IEEE Intelligent Systems from 2009 to 2012, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS from 2009 to 2016, IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS from 2017 to 2020. He is currently the President of CAA's Supervision Council and new EiC of the IEEE TRANSACTIONS ON INTELLIGENT VEHICLES.