Guest Editorial
Introduction to the Special Section on Blockchains in Emerging Vehicular Social Networks

NOWADAYS, human factors are involved in Vehicular ad hoc networks (VANETs) and this arises to the vehicular social networks (VSNs) that promote the prosperity of VANETs and lay a solid foundation for the development of vehicular based services. With the development of fast and reliable vehicular communication techniques and various user-centric applications, VSNs are likely to pave the way for sustainable development by promoting transportation efficiency. However, the flourish of VSNs is still somehow plagued by security issues. For instance, emerging data-intensive applications such as insurance premium assessment always rely on the analysis and mining of the large-scale VSNs data. Therefore, the users' data security and privacy become one of the most concerned issues. More examples of real threats are easy to find. If the traffic related messages are not authenticated and integrity-protected in VSNs, a single bogus and/or malicious message can potentially incur a terrible traffic accident. Thus, the real deployment of VSNs acquires appropriate security and privacy protection against the holistic environment. To meet such security and privacy requirements, a just recently proposed technique named blockchain should be significantly considered.

Blockchain, widely known as one of the disruptive technologies, can provide technical support for VSNs in terms of big data management and security. Firstly, blockchain can create a ledger for VSNs, which records all data and behaviours occurring in VSNs, and coordinates all events that occurred and will happen. Once the data is uploaded to blockchain as a ledger, it is computational impossible for tampering. Secondly, blockchain can be further used to address security issues related to VSNs, such as the safety of connection and communication between intelligent vehicles. Meanwhile, the decentralized consensus mechanism will effectively strengthen the security of the system. By integrating with the smart contract, the blockchain can turn every vehicle into an independent network node, which can self-maintain and adjust. Versatile novel security properties can be offered by blockchain. Hence, it is urgent to explore the latest understanding and advances in the blockchain based techniques in VSNs.

The response to our Call for Papers on this special issue was overwhelming, with 36 articles submitted from around the world. During the review process, each paper was assigned to and reviewed by multiple experts in the relevant areas, with a rigorous two-round review process. Thanks to the courtesy of the Editor-in-Chief of IEEE Transactions on Vehicular Technology, Prof. Kato Nei, we are able to accept 10 excellent articles covering various aspects of blockchains in emerging VSNs. The overall accept ratio reaches 27.8%. In the following, let us introduce these articles and highlight their main contributions.

In "Lightweight Blockchain Consensus Protocols for Vehicular Social Networks," the authors present lightweight blockchain consensus protocols that are specifically designed for vehicular social networks, or other networks that resemble them. They are lightweight in the sense that no puzzles are required to solve and no cryptocurrency systems are required to build beforehand. Various scenarios are considered, including whether the communication is reliable and whether the vehicle grouping is static. Although they break their solution of the consensus problem into private chain and public chain, they provide a scheme to smoothly bridge between them. Theoretical analysis is provided to guarantee the algorithms to succeed with high probability, before experiments are conducted to verify the algorithms and compare their theoretical performance versus simulation performance, namely worst-case performance versus average performance.

The security and privacy of data generated by various applications in VSNs is a great challenge, which blocks the further development of VSNs. The emerging Blockchain technology seems to be a good catalyst for the development of VSN with its high security and irreversible features. However, the full duplicates of Blockchain data need to store in each node to ensure security, which is unacceptable for vehicles with limited resources. In "LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks," to address the above storage challenge, a lightweight Directed Acyclic Graph (DAG) based Blockchain (LDV) is proposed for resource-constrained VSNs. Specifically, based on the in-depth analysis of VSNs, the authors propose the social-based data reduction approach. In detail, each node only stores the interested data within the topic groups of interest and ignores the irrelevant data. To avoid the huge storage cost within large-scale groups with large amounts of data, they further present the historical data pruning method within a group, which reduces the storage requirement by reducing the number of duplicates stored in each node.

Charging EVs takes time and thus in-advance scheduling is needed. As this process is done frequently due to limited mileage of EVs, it may expose the locations and charging pattern of

Digital Object Identifier 10.1109/TVT.2020.2991623

the EV to the service providers, raising privacy concerns for their users. Nevertheless, the EV still needs to be authenticated to charging providers. In "Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," the authors tackle this problem by utilizing distributed applications enabled by blockchain and smart contracts. We adapt zero-knowledge proofs to blockchain for enabling privacy-preserving authentication while removing the need for a central authority. They introduce two approaches, one using a token based mechanism and another utilizing the Pederson Commitment scheme to realize anonymous authentication. They also describe a protocol for the whole process which includes scheduling and charging operations. The evaluation of the proposed approaches indicates that the overhead of this process is affordable to enable real-time charging operations for connected EVs.

Support vector machine (SVM) is one of the typical ML methods and widely used for its high efficiency. In some real-world scenarios, when training an SVM classifier, many entities face a same problem that they are lacking in data attributes. Multiple entities are required to share data to combine a dataset with diverse attributes and then jointly train a comprehensive classifier. However, the data privacy concerns are raised because of the data sharing. In "Secure SVM Training Over Vertically-Partitioned Datasets Using Consortium Blockchain for Vehicular Social Networks," the authors propose a privacy-preserving SVM classifier training scheme over vertically-partitioned datasets possessed by multiple data providers. They utilize consortium blockchain and threshold homomorphic cryptosystem to establish a secure SVM classifier training platform without a trusted third-party. They keep much training operations locally over original data and necessary interactions between participants are protected by threshold Paillier and consortium blockchain. Security analysis proves that the proposed scheme can preserve the privacy of original data and the training intermediate values.

In "TrustAccess: A Trustworthy and Secure Ciphertext-Policy and Attribute Hiding Access Control Scheme Based on Blockchain," the authors aim to propose a trustworthy and secure ciphertext-policy access control scheme based on blockchain, named TrustAccess, to achieve trustworthy access while guaranteeing the access policy privacy. To make exiting hidden policy CP-ABE more efficiency and scalability for blockchain, they propose an optimized hidden policy CP-ABE, named HP-CP-ABE, to ensure policy privacy while satisfying large universe access requirements. Finally, they prove the effectiveness of the TrustAccess by security analysis from the aspect of blockchain operations and HP-CP-ABE. Extensive experiments are conducted to evaluate and demonstrate the efficiency of TrustAccess through comparison with other related schemes.

The Vehicle-to-Grid (V2G) network is highly emerging where the battery powered vehicles provide energy to the power grid. A robust, scalable and cost-optimal mechanism is required that can support the increasing number of transactions in a V2G network. To achieve this requirement, the normal blockchain enabled V2G networks require high computation power and are not suitable for micro-transactions due to the mining reward being higher than the transaction value itself. In "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network," the authors propose a lightweight blockchain-based protocol called Directed Acyclic Graph based V2G network (DV2G). They make use of a tangle data structure to record the transactions in the network in a secure and scalable manner. A game theoretic approach is used to model the energy trading between the vehicles and grid in a cost-optimal manner. The proposed model is free from the need of heavy computation for adding the transactions to the data structure and does not require any fees to post the transaction. The proposed model proves to be highly scalable and supports micro-transactions required in V2G network.

With the emergence of advanced communication and computing technologies, more and more data can be fast and conveniently collected from heterogeneous devices, and VSN has to meet new security challenges such as data security and privacy protection. Searchable encryption (SE) as a promising cryptographic primitive is devoted to data confidentiality without sacrificing data searchability. In "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," to achieve secure and efficient keyword search in VSN, the authors design a new blockchain-based searchable public-key encryption scheme with forward and backward privacy (BSPEFB). BSPEFB is a decentralized searchable public-key encryption scheme since the central search cloud server is replaced by the smart contract. Meanwhile, BSPEFB supports forward and backward privacy to achieve privacy protection.

VSNs support diverse kinds of services such as traffic management, road safety, and sharing data. However, its complex, large-scale and dynamic network structure poses new security challenges. Among these challenges, secure data transmission has turned to be a spotlight. Ciphertext-policy attribute-based encryption (CP-ABE) may be adopted to realize one-to-many data sharing in VSNs. In traditional CP-ABE schemes, the access policy is stored and granted by the cloud, which lacks credibility due to centralization. In "A Secure and Verifiable Data Sharing Scheme Based on Blockchain in Vehicular Social Networks," the authors propose a secure and verifiable one-to-many data sharing scheme to solve the above problem. They use blockchain to record the access policy, realizing user self-certification and cloud non-repudiation. Considering the computing capabilities of the vehicular user, they propose an effective scheme for certificating. Meanwhile, considering the sensitive information included in the access policy, they propose a policy hiding scheme. The proposed scheme also supports data revocation when a vehicular user no longer wants to share the data in VSNs.

In "An Efficient Decentralized Key Management Mechanism for VANET With Blockchain," the authors propose an efficient decentralized key management mechanism for VANET with blockchain (DBKMM). They first define a blockchain network in which RSUs act as network nodes and are responsible for performing key management and storing public key data. Then, they design a smart contract to automatically complete the registration, update and revocation of user's public key. Furthermore, based on the bivariate polynomial, they present a lightweight mutual authentication and key agreement protocol which can mitigate DoS attacks for the wireless communication in VANET. Finally, they analyze the security and performance of the proposed scheme through experiments and simulation. The decentralized nature of blockchain solves the inefficiency and high cost of centralized structure. Experiment results show that the authentication and key agreement protocols have better performance than some traditional schemes in terms of the cost, communication, storage, computation overhead and latency.

Last but not least, in "BloCkEd: Blockchain-Based Secure Data Processing Framework in Edge Envisioned V2X Environment," the authors present the proposed blockchain-based secure data processing framework designed for the edge envisioned V2X environment (hereafter referred to as BloCkEd). Specifically, a multi-layered edge enabled V2X system model for BloCkEd is designed, which includes the formulation of a multi-objective optimization problem. In addition, the BloCkEd comprises an optimal container-based data processing scheme, and a blockchain-based data integrity management scheme, designed to minimize link breakage and reduce latency. Using Chandigarh City, India, as the scenario, they implement and evaluate the proposed approach in terms of its latency, energy consumption, and service level of agreement violation.

Finally, we would like to express our thanks to all the authors for their supports and excellent contributions. We also would like to thank all the reviewers for their volunteered efforts in reviewing the papers, and for their insightful comments and constructive suggestions for improving the quality of the articles. Respectfully, we appreciate the advice and support of the Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Prof. Kato Nei, for his help in the whole publication process.

HONGWEI LI, *Lead Guest Editor*
University of Electronic Science and Technology of China
Chengdu 611731, China

CHAO ZHANG, *Guest Editor*
Tsinghua University
Beijing 100091, China

MOHAMED MAHMOUD, *Guest Editor*
Tennessee Tech University
Cookeville TN 38505, USA

RONGXING LU, *Guest Editor*
University of New Brunswick
Fredericton E3B 5A3, Canada

Hongwei Li received the Ph.D. degree from the University of Electronic Science and Technology of China, in 2008. He is currently the Head and a Professor with the Department of Information Security, School of Computer Science and Engineering, University of Electronic Science and Technology of China. He worked as a Postdoctoral Fellow with the University of Waterloo from October 2011 to October 2012 under the supervision of Prof. Sherman Shen. His research interests include network security and applied cryptography. He has published more than 100 technical papers. He is the author of a book, *Enabling Secure and Privacy Preserving Communications in Smart Grids* (Springer, 2014). He serves as an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL and *Peer-to-Peer Networking and Applications*, a Guest Editor of IEEE NETWORK, IEEE INTERNET OF THINGS JOURNAL and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He also serves/served the Technical Symposium Co-chairs of ACM TUR-C 2019, IEEE ICCC 2016, IEEE GLOBECOM 2015 and IEEE BigDataService 2015, and Technical Program Committees for many international conferences, such as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE SmartGridComm, BODYNETS and IEEE DASC. He won Best Paper Awards from IEEE MASS 2018 and IEEE HEALTHCOM 2015. Dr. Li currently serves as the Secretary of IEEE ComSoc CIS-TC. He is the Distinguished Lecturer of IEEE Vehicular Technology Society.

Chao Zhang has been an Associate Professor with the Institute of Network Sciences and Cyberspace, Tsinghua University, China, since Nov 2016. Before that, he worked as a Postdoc Researcher with UC Berkeley from September 2013 to September 2016. His research interest lies in system and software security. He has published several papers in top-tier security conferences, including a paper ranked as the top ten most-cited paper in top four security conferences in 2013. His defense solution FPGate won the Special Recognition Award in Microsoft's BlueHat Prize Contest in 2012. He co-led a team CodeJitsu from UC Berkeley and designed a system Glactica able to automatically assess vulnerabilities and fix them. This system competed with other 104 systems of its kind in Cyber Grand Challenge launched by DARPA, and won the First Place in defense in 2015 and the Second Place in offense in 2016. His vulnerability discovery solutions have found hundreds of 0 day vulnerabilities, including dozens of vulnerabilities in IoT devices and blockchain. He is on the editorial boards of the *Cybersecurity* journal, and served/serves the technical program committees of IEEE and others international conferences, including IEEE S&P 2016 (student PC), ACM CCS'2019, RAID 2019, ASIACCS 2019.

Mohamed M. E. A. Mahmoud received the Ph.D. degree from the University of Waterloo in April 2011. From May 2011 to May 2012, he worked as a Postdoctoral Fellow in the Broadband Communications Research Group — University of Waterloo. From August 2012 to July 2013, he worked as a Visiting Scholar with the University of Waterloo, and a Postdoctoral Fellow with Ryerson University. Currently, Dr. Mahmoud is an Associate Professor with the Department Electrical and Computer Engineering, Tennessee Tech University, USA. His research interests include security and privacy preserving schemes for smart grid communication network, mobile ad hoc network, sensor network, and delay tolerant network. Dr. Mahmoud has received NSERC-PDF Award. He won the Best Paper Award from IEEE International Conference on Communications (ICC'09), Dresden, Germany, 2009. He is the author for more than 23 papers published in major IEEE conferences and journals, such as INFOCOM conference and IEEE Transactions on Vehicular Technology, Mobile Computing, and Parallel and Distributed Systems. He serves as an Associate Editor in the Springer *Journal of Peer-to-Peer Networking and Applications*. He has served as a Technical Program Committee Member for several IEEE conferences and as a reviewer for several journals and conferences such as IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the *Journal of Peer-to-Peer Networking*.

Rongxing Lu is currently an Associate Professor with the Faculty of Computer Science, University of New Brunswick (UNB), Canada. Before that, he worked as an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow with the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal," when he received his Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He is presently a Senior Member of IEEE Communications Society. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He was/is on the editorial boards of several international referred journals, e.g., IEEE NETWORK, and served/serves the Technical Symposium Co-Chair of IEEE GLOBECOM'16, IEEE ICC'21, and many technical program committees of IEEE and others international conferences, including IEEE INFOCOM and ICC. He currently serves as the Vice Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee).