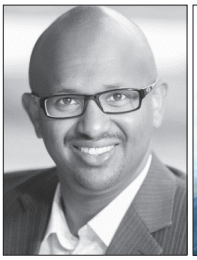
Blockchain Envisioned Drones: Realizing 5G-Enabled Flying Automation


Sahil Garg


Gagangeet Singh Aujla


Aiman Erbad


Joel J. P. C. Rodrigues


Min Chen


Xianbin Wang

Nowadays the deployment of drones/UAVs is not just limited to military and defense establishments; they are also widely deployed in geo-dispersed applications (environmental monitoring, rescue operation monitoring, road and traffic surveillance, natural disaster monitoring, soil and crop analysis, and consumer product delivery). Drones have become the instigators and enablers of global mechanization. For example, the influx of precocious drones is recognizable looking at the high angled photography of peculiar landscapes. Likewise, multiple drones coordinate and collaborate with each other to form a web of flying computing resources which can sense, analyze, and transmit data to remote cloud servers and storage spaces. Even more, the popularity of next generation communication technologies has opened a new vertical in the form of 5G-enabled flying automation using drones. This new dimension for drone communication has attracted the wide attention of the academia, research and industrial communities. 5G-enabled flying automation empowers the astronomically large numbers of connected things in a drone-enabled smart ecosystem to communicate among themselves and thereafter decisively handle the progressively intricate traffic conditions.

There is no point in arguing that if drones are used for the doorstep delivery of anything, the process will provide many benefits. Still, the idea is not endorsed. The rationale for this demeanor is the lack of trust among people to let a strange device enter into secure premises like homes, warehouses or offices. The resistance will remain until a certitude is developed in the system. A mature authentication system for a chip-level authentication of drones may serve the purpose before allowing them into the premises. Any such mechanism needs the storage of identity records, for which blockchain is the most suitable contender due to its competency in distributed environments. Some companies like Dorado are working on the integration of blockchain and drones to be used in doorstep delivery of all goods that can be carried using drones. Blockchain is expected to storm the world of information storage and retrieval, and it is interesting how the combination of the two is going to affect the entire technological ecosystem.

The application areas of drones are numerous, but the usage of drones in the area of security and surveillance differentiates it from other counterparts. Drones may serve as a replacement for the high-security areas where human security guards may not prove to be very effective as they don't feel tired, dizzy, sleepy, or bored like humans. The future of drone robotics looks safe in this field. Still, even after so many associated advantages, drones have a problem with their identity and operation management. It is evident from the Gatwick airport incident[1] when in 2018 some unidentified drones were observed. It was proactively dealt with and investigated by the authorities and the airport flight operations were temporarily shut, which incurred huge financial losses. The drones were never identified due to the absence of a proper registration and flight permission infrastructure. Blockchain can be a viable solution to overcome such problems by registering each drone on the blockchain and then permitting it to operate. Even more, wildlife and area conservancy also have drone applicability because of their environmental and geographic constraints. Poaching in national parks can be avoided with the help of drones and the associated data can be stored on the blockchain. For example, a company named Soar (https://soar.earth) is shifting the trend from the usage of static map data toward the more up-to-date information gathered with the help of drones. Once the envisioned applications of drones become reality, various challenges arise which need to be tackled at the right time and in the right manner. Drone flight, routing, flight planning, time of flight, flight restrictions, air pollution, and crowded skies, are some of the challenges which we need to address today. The right to privacy is the most important aspect which is at stake. A spy drone, if used to track something, can pose a great threat to the privacy of individuals and should be dealt with carefully as any violation can lead to severe damages. Therefore, blockchain-envisioned drones, a novel architecture for coordinating the access of drones in the controlled airspace and providing navigation services between locations referred to as nodes using a 5G-enabled flying automation, is a fascinating innovation which requires deep investigation at various levels. For this purpose, different solutions, mechanisms and architectures are required to understand and investigate the pros and cons of block drones to realize 5G flying automation.

This Special Issue of the IEEE Network is intended to present and highlight the advances, latest technologies, implementations and applications related to the potential integration of blockchain with drone-enabled smart ecosystems. The Special Issue focuses on several topics that are recent concerns in the community, including data integrity and privacy preservation, cloud/edge/fog analysis for big data evaluations, energy harvesting, inter-drone communications, secure content dissemination, software defined drone networks, IoT architectures and protocols, and other enabling technologies to realize the vision of block drones through 5G-enabled flying automation. It is interesting to note that the call for papers received an especially strong response from the community, further attesting to the rapid development of this scientific area. We hope these articles will show their value over time, while being immediately helpful for our current readership. We summarize the accepted articles in this editorial as follows.

In the article "Blockchain-based UAVs Path Planning for Healthcare 4.0: Current Challenges and Way Ahead", S. Aggarwal *et al.* focus on designing a distributed P2P platform for UAVs that ensures confidentiality, integrity, identity management, and

[1]https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the.gatwick-drone

privacy-preservation in healthcare 4.0. In particular, a three-layered architecture for real-time collection, processing, and transmission of medical data is designed. The proposed architecture provides a distributed platform for the UAVs that ensures security and privacy of medical data with a consensus mechanism. The simulation results show that the proposed system provides an effective solution for reliable data transmission via UAVs while preserving sensitive healthcare information against potential threats. Based on the merits, it is believed that the proposed blockchain-enabled UAV path planning method is a step toward effective and efficient management for shared medical data.

The article "Exploiting 5G and Blockchain for Medical Applications of Drones" by J. Chen *et al*. comprehensively exploits the potential of 5G and blockchain for promoting medical applications of drones. They first categorize the key challenges in the drones' medical applications. Then the intrinsic characteristics of 5G is explored to provide a reliable communication link with satisfactory data rate, low latency, high scalability and low energy cost, while blockchain is found to be able to meet the security requirements in terms of confidentiality, integrity, availability and authentication. In the scenario of disaster relief, an illustrative example of using 5G and blockchain to promote medical applications of drones is given.

In the article "Emerging Drone Trends for Blockchain-Based 5G Networks: Open Issues and Future Perspectives", T. Han *et al*. discuss 5G communication networks and Mobile Edge Computing as promising technologies that can provide several benefits to drone-enabled environments and solve some of the presented issues. They introduced new security concerns of drone communication networks, given their recent popularity. These concerns are related to the possibility of malicious users taking advantage of this brand new technology, which caused many governments to ban drones due to public safety. Next, blockchain technology is discussed as a novel solution to the security issues, which raised its decentralized nature, making it inherently safe.

In the article "Analysis of Using Blockchain to Protect the Privacy of Drone Big Data" by Z. Lv *et al*., blockchain technology is adopted to solve the privacy protection problem of UAVs big data. In particular, the proposed privacy protection scheme uses a number theory research unit (NTRU) cryptosystem for encryption of blockchain data. Privacy analysis is provided to validate the security requirements. The performance evaluation results show that the proposed UAV big data privacy protection scheme based on blockchain technology has a low computing cost in terms of key production, encryption, and decryption. It also outperforms the conventional approaches. This work aims to provide a guideline for future research in the privacy protection of UAV data.

In the article, "Blockchain-based Privacy Preservation for 5G-enabled Drone Communications", Y. Wu *et al*. explain the potential of leveraging blockchain to facilitate privacy preservation in a broad range of real-world applications, including the monitoring and tracking of individuals in demonstrations and enforcing social/physical distancing during pandemics such as COVID-19. Specifically, they introduce the architecture for 5G-enabled drone communications and blockchain, review existing blockchain-based solutions, and study existing legislation and data privacy regulations that need to be considered in the design of blockchain-based solutions. They conclude with a number of thought-provoking future research challenges, which will most certainly advance the conversation on this topic.

In the article "Building Agile and Resilient UAV Networks Based on SDN and Blockchain", N. Hu *et al*. propose a novel software-defined unmanned aerial vehicle (UAV) network with a decentralized control plane by integrating SDN and blockchain technology. The proposed architecture decouples the control plane and data plane of a UAV network and utilizes a decentralized control plane to manage all the UAVs. This design concentrates the management and control functions on the ground base station and simplifies the complexity of unmanned aerial vehicles, which helps improve the survivability of the UAV network. The paper creatively applies blockchain technology to the design of the UAV network control plane, which improves the robustness, trustworthiness and ubiquitous access capability of the control plane. The networking of large-scale UAV groups has always been a key issue that plagued the development of UAV technology. The architecture proposed in this paper has important reference value for UAV networking design.

In the article "Design Guidelines for Blockchain-Assisted 5g-UAV Networks", M. Aloqaily *et al*. propose a decentralized drone service delivery (DaS: Drones as a Service) architecture that combines emerging features such as 5g networks, blockchain and fog/cloud computing to provide security and reliability of services. This architecture allows a swarm of UAVs to communicate between each other to collaborate in order to fulfill a common task using 5G infrastructure. Both public and private blockchains are deployed within the UAVs, supported by fog and cloud computing devices and data centers, to provide a wide range of complex authenticated service and data availability. This paper provides the guidelines to combine the features provided by each of these paradigms to enable optimal resource management and better security, reliability, and delivery success rates compared to traditional UAV-supported cellular networks. Also, it discusses the various challenges and future research, highlighting emerging technologies such as Federated Learning. This work will have a significant impact on the design of reliable and secure DaS platforms, enabling new innovative services that represent an important pillar of modern smart cities.

In the article "Block-Chain Empowered Trusted Networking for Unmanned Aerial Vehicles within B5G Era", X. Jian *et al*. propose a blockchain-empowered trusted networking framework for an unmanned aerial vehicle ad hoc network (UAANET), as well as the corresponding network architecture, protocol stack, key control signaling, and algorithms. This article makes a breakthrough in solving the problems of network security and stability: introducing the security of blockchain into ad hoc networks does not previously exist. Beyond that, it proposes a new metric for selecting links, and uses blockchain related technologies to eliminate untrusted nodes in the UAANET, as far as possible to ensure the safety and credibility of the UAANET. This work will have a huge impact on the safety and stability of future UAANET.

In the article "Securing Data Sharing from the Sky: Integrating Blockchains into Drones in 5G and Beyond", J. Kang *et al*. utilize permissioned blockchain to design a decentralized data management system for 5G and Beyond (B5G) drone networks. The authors introduce credit as a metric and propose a secure and universal credit-based scheme for reliable miner selection for permissioned blockchain-based B5G drone networks. The proposed blockchain and credit-based mechanism is a well-motivated solution that provides a promising way to enable data sharing in a secure manner. The work will have a huge impact on decentralized and secure data sharing in the future 5G and Beyond drone networks.

In the article "Blockchain-Empowered Drone Network: Architecture, Features, and Future", Z. Chang *et al*. propose to utilize the concept of blockchain in the development of drone networks. The authors studied the architecture of blockchain-enabled drone networks with edge computing and investigated the interaction between the edge service provider (ESP) and drones. Here, incentive mechanism is explored via a single-leader multiple-follower game model, where the ESP is the leader and drones are the followers. Accordingly, a two-stage Stackelberg game is introduced to investigate the relations and interactions between the ESP and drones. In the initial stage, the ESP pres-

ents its price strategy for the computing resources and in the next stage the drones which are deployed for service provisioning compete for these resources in a non-cooperative fashion to carry on the blockchain process. Performance evaluations are conducted to illustrate the benefits of the proposed architecture on developing blockchain envisioned drones.

In the article "Deep Learning and Blockchain with Edge Computing for 5G-Enabled Drone Identification and Flight Modes Detection", A. Gumaei *et al*. propose a secure and intelligent 5G-enabled Unmanned Aerial Vehicle (UAV) or drone identification and flight modes detection framework by integrating blockchain with a deep recurrent neural network (DRNN) and edge computing. The proposed framework enables remote monitoring, collection and storing of raw radio frequency (RF) signals of different drones under several flight modes on a cloud server to train a DRNN model and then distribute the trained model on edge devices for detecting drones and their flight modes. The framework utilizes blockchain for data integrity and securing data transmission. The performance improvement achieved by the proposed framework will have a great impact on the future UAV industry for accurate detection of drone and their flight modes in a secure manner.

In the article "Sharding-Enabled Blockchain for Software-Defined Internet of Unmanned Vehicles in the Battlefield", B. Ghimire *et al*. propose a secure, robust, and intelligent architecture for automated battlefield scenarios leveraging private blockchain enriched by smart contracts and sharding and 5G enabled software defined IoUV. This paper envisions a novel and remarkable approach where each type of activity on the battlefield is recorded in a specific tamper-proof ledger and the actions of UVs are automated through smart contracts. The proposed approach is fully secure by allowing communication with only trusted peers and robust against any kind of resource-related issues. Further, it is the first and striking work to employ two forms of sharding to make the IoUV efficient and robust against any resource-related issues.

In this article "A Blockchain-Based Secure Crowd Monitoring System Using UAV Swarm", W. Xiao *et al*. propose a drone-swarm-aided distributed monitoring system in a blockchain-powered network that supports high mobility and security enhancement. In order to meet the high-efficiency identity authentication, secure drone swarm communication and distributed data management requirements of the monitoring system, this article considers the data collection, data transmission, data access, and other aspects of the monitoring system, and designs a complete blockchain-enabled and UAV-swarm-aided secure crowd monitoring scheme. It uses trusted computing and data decryption/encryption technology to realize identity authentication, drone sub-swarm key distribution, and secure data transmission. The blockchain technology is used to ensure the authenticity of the identity of UAV nodes, the reliability of UAV cooperation in monitoring tasks, the confidentiality of information in the process of data transmission, and the availability of public group decision making.

In the article, "Blockchain-Powered Policy Enforcement for Ensuring Flight Compliance in Drone-Based Service Systems", M. S. Rahman *et al*. propose a drone flight compliance mechanism in a drone-based commercial delivery service system by utilizing blockchain technology. The authors mainly address the issues of drone collision and citizen privacy during drone flights. The proposed system uses smart contracts to set policies and establishes pre-allocated flight paths for different drones to avoid collisions and ensure citizen privacy by restricting their access to unauthorized areas. The blockchain enforces the policies to monitor compliance of the drone flights and identify non-compliant drone services to penalize the corresponding service providers. This article is a pioneering work in employing blockchain in drone flight automation, which will have a significant impact on drone flight automation and commercialization of drone-based commercial services.

In the article "Blockchain based Task Offloading in Drone-aided Mobile Edge Computing", S. Luo *et al*. propose a secure and intelligent framework for task offloading in edge computing by integrating blockchain and drone. The proposed framework utilizes blockchain to increase the accountability of executing the offloaded tasks in the mobile edge computing servers. At the same time, the authors use drones to extend the coverage of Mobile Edge Computing. This paper is a groundbreaking work in developing a set of offloading policies in smart contracts, which does not previously exist. The proposed framework is an elegant breakthrough that provides a promising way to enhance edge computing accountability. The work provides a solution for infrastructure providers to build user trust, encouraging more people to use their services. This work will have a huge impact on the intelligent and optimal control and operation of future-generation wireless communication networks and edge computing.

The article "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach" by C. Feng *et al*. proposes a blockchain-enabled efficient and secure data-sharing model for 5G flying drones which aims to address the security issue for authentication and data sharing in a drone's open and untrusted environment. Specifically, blockchain and attribute-based encryption (ABE) are applied to ensure the security of instruction issues and data sharing. The authentication mechanism in the model employs a smart contract for authentication and access control, public-key cryptography for providing accounts and ensuring accounts' security, and a distributed ledger for security audit. In addition, to speed up outsourced computations and reduce electricity consumption, an ABE model with parallel outsourced computation is constructed, and a generic parallel computation method for ABE is proposed. The analysis of the experimental results shows that parallel computation significantly improves the speed of outsourced encryption and decryption compared to serial computation.

We would like to express our sincere gratitude to all the authors who submitted their valuable findings, as well as to the highly qualified reviewers who voluntarily participated in the review process and provided constructive feedback on a very tight schedule. The Guest Editors are also immensely grateful to the former Editor-In-Chief, Professor Mohsen Guizani, for the opportunity to organize this special issue, and the current Editor-In-Chief, Professor Chonggang Wang, for his unwavering support and guidance in preparing and finalizing this editorial. Special thanks goes to the administrative staff of the journal for their tireless support throughout the journey leading to publication. We sincerely hope that this special issue will contribute to the body of knowledge.

Biographies

Sahil Garg received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018. He is currently working as a post-doctoral research fellow at École de Technologie Supérieure, Université du Québec, Montréal, Canada; and a MITACS researcher at the Global AI Accelerator, Ericsson, Montreal. He is also a visiting researcher with the School of Computer Science and Engineering (SCSE) at Nanyang Technological University (NTU) Singapore. He has many research contributions in the area of machine learning, big data analytics, security and privacy, Internet of Things, and cloud computing. He has a total of 80+ publications in highly ranked journals and conferences, including 30+ IEEE transactions/journal papers. Some of his research findings have been published in top-cited journals such as IEEE TII, IEEE TCC, IEEE TMM, IEEE TETC, IEEE TVT, IEEE TNSM, IEEE TSUSC, IEEE TNSE, *IEEE IoT Journal*, *IEEE Systems Journal*, *IEEE Communications Magazine*, *IEEE Network Magazine*, *IEEE Wireless Communications*, *IEEE Consumer Electronics Magazine*, FGCS, JPDC, *Applied Soft Computing*, *Computer Networks*, and *Information Sciences*, including various respected international conferences such as-IEEE Globecom, IEEE ICC, IEEE WCNC, IEEE CCNC, IEEE VTC, IEEE Infocom Workshops, ACM MobiCom Workshops, ACM MobiHoc Workshops, etc. He was the recipient of the prestigious Visvesvaraya Ph.D. fellowship from the Ministry of Electronics & Information Technology under the Government of India (2016-2018). He was awarded the 2020 IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher) and the IEEE ICC Best Paper Award in 2018 at Kansas City, Missouri. Dr. Garg serves as the managing editor

of *Human-centric Computing and Information Sciences* (HCIS) and an associate editor of *IEEE Network*, *IEEE Transactions on Intelligent Transportation Systems*, *Applied Soft Computing* (Elsevier), and the *International Journal of Communication Systems* (Wiley). He has been a lead guest editor for a number of special issues in prestigious journals and magazines such as IEEE TII, IEEE T-ITS, *IEEE IoT Journal*, *IEEE Network*, Elsevier's COMNET, and Elsevier's FGCS. In addition, he also serves as a Workshops and Symposia Officer of the IEEE ComSoc Emerging Technology Initiative on Aerial Communications. He serves/has served as the Workshop Chair/TPC Co-Chair/Publicity Co-Chair for several International workshops organized in conjuction with the prestigious IEEE/ACM conferences, including IEEE Infocom, IEEE Globecom, IEEE ICC, and ACM Mobicom. He is a member of IEEE, the IEEE Communications Society, IEEE Computer Society, IEEE Industrial Electronics Society, IEEE Software Defined Networks Community, IEEE Smart Grid Community, ACM, and IAENG.

Gagangeet Singh Aujla is an assistant professor of computer science at Durham University, United Kingdom. Before this, he worked as a post-doctoral research associate at Newcastle University, UK, a research associate at Thapar University (India), a visiting researcher at the University of Klagenfurt (Austria), and in various academic positions for more than a decade. He received his Ph.D. in computer science and engineering from Thapar Institute of Engineering and Technology, Patiala, Punjab, India in 2018. He received the B.Tech and M.Tech. degrees in computer science and engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2003 and 2013, respectively. For his contributions in the area of scalable and sustainable computing, he was awarded the 2018 IEEE TCSC Outstanding Ph.D. Dissertation Award of Excellence. The main themes of his research are energy-efficient, reconfigurable, resilient and intelligent surfaces (smart city, smart grid, IoT-edge-cloud systems, healthcare systems, transportation systems). Some of his research findings are published in top cited journals such as IEEE TKDE, IEEE TDSC, IEEE TVT, IEEE TITS, IEEE TSC, IEEE TCC, IEEE TII, IEEESuSC, IEEE JSAC, *IEEE IoT Journal*, *IEEE System Journal*, *IEEE Communications Magazine*, *IEEE Network*, *IEEE Internet Computing*, *IEEE Consumer Electronics Magazine*, *Future Generation Computer Systems*, *Information Sciences*, *Computer Networks*, *Computer and Security*, the *Journal of Network and Computer Applications*, the *Journal of Parallel and Distributed Computing*, *Sustainable Computing: Informatics and Systems*, *Neural Computing and Applications* and top-tier conferences such as ACM Mobicom Wkps, ACM MobiHoc Wkps, IEEE Infocom Wksps, IEEE Globecom, IEEE ICC, IEEE WiMob, IEEE IC2E, etc. To develop himself as a researcher, he worked on various research projects awarded by EPSRC, the Department of Science and Technology (India), and the Austrian Federal Ministry of Education, Science and Research. He is leading several workshop series (SecSDN and BlockSecSDN) in conjunction with different IEEE Communication Society conferences including IEEE Infocom, IEEE Globecom, IEEE ICC, and many more. Contributing to the research community, he is an associate editor for *Adhoc Networks* (Elsevier), a topic editor for *Sensors*, a guest editor for *IEEE Transaction on Industrial Informatics*, *IEEE Network*, *Neural Computing and Applications* (Springer), *Computer Communications* (Elsevier), *Software: Practice and Engineering* (Wiley), and *Transactions on Emerging Telecommunications* (Wiley). He is Senior Member of the IEEE, Member of the ACM and Life Member of ISTE.

Aiman Erbad is currently an associate professor with the College of Science and Engineering, Hamad Bin Khalifa University (HBKU). Prior to this, he was an associate professor at the Computer Science and Engineering (CSE) Department and the Director of Research Planning and Development at Qatar University. He also served as the Director of Research Support responsible for all grants and contracts from September 2016. Dr. Erbad obtained a Ph.D. in computer science from the University of British Columbia (Canada), a Master of computer science in embedded systems and robotics from the University of Essex (UK), and a BSc in computer engineering from the University of Washington, Seattle. He received the Platinum award from H.H. The Emir Sheikh Tamim bin Hamad Al Thani at the Education Excellence Day 2013 (Ph.D. category). He also received the 2020 Best Research Paper Award from Computer Communications, the IWCMC 2019 Best Paper Award, and the IEEE CCWC 2017 Best Paper Award. His research received funding from the Qatar National Research Fund, and his research was published in respected international conferences and journals. He is an editor for *KSII Transactions on Internet and Information Systems*, an editor for the *International Journal of Sensor Networks* (IJSNet), and a guest editor for *IEEE Network*. He also serves as a Program Chair of the International Wireless Communications Mobile Computing Conference (IWCMC 2019), as a Publicity chair of the ACM MoVid Workshop 2015, as a Local Arrangement Chair of NOSSDAV 2011, and as a Technical Program Committee (TPC) member in various IEEE and ACM international conferences (NOSSDAV, MMSys, ACMMM, IC2E, and ICNC). His research interests span cloud/fog computing, multimedia systems and networking, Internet of Things, and cyber security. He is a senior member of IEEE and ACM.

Joel J. P. C. Rodrigues [S'01, M'06, SM'06, F'20] is a professor at the Federal University of Piauí, Brazil; senior researcher at the Instituto de Telecomunicações, Portugal; and collaborator of the Post-Graduation Program on Teleinformatics Engineering at the Federal University of Ceará (UFC), Brazil. He is the leader of the Next Generation Networks and Applications (NetGNA) research group (CNPq), an IEEE Distinguished Lecturer, Member Representative of the IEEE Communications Society on the IEEE Biometrics Council, and the President of the Scientific Council at ParkUrbis – Covilhã Science and Technology Park. He was Director for Conference Development - IEEE ComSoc Board of Governors, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee member of the IEEE Life Sciences Technical Community and Publications co-Chair. He is the editor-in-chief of the *International Journal of E-Health and Medical Communications* and editorial board member of several highly respected journals. He has been general chair and TPC Chair of many international conferences, including IEEE ICC, IEEE Globecom, IEEE Healthcom, and IEEE LatinCom. He has authored or coauthored over 950 papers in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He had been awarded several Outstanding Leadership and Outstanding Service Awards by the IEEE Communications Society and several best papers awards. He is a member of the Internet Society, a senior member ACM, and a Fellow of IEEE.

Min Chen has been a full professor in the School of Computer Science and Technology at Huazhong University of Science and Technology (HUST) since Feb. 2012. He has 300+ publications, including 200+ SCI papers, 100+ IEEE tranactions/journal papers, 34 ESI highly cited papers, and 12 ESI hot papers. He has published 12 books. His Google Scholar Citations reached 26,080+ with an h-index of 81 and i10-index of 240. His top paper was cited 3080+ times. He was selected as a Highly Cited Researcher in 2018, 2019 and 2020. He received the IEEE Communications Society Fred W. Ellersick Prize in 2017, and the IEEE Jack Neubauer Memorial Award in 2019. His research focuses on cognitive computing, 5G networks, wearable computing, big data analytics, robotics, machine learning, deep learning, emotion detection, and mobile edge computing, among other topics. He is a Fellow of IEEE.

Xianbin Wang (S'98-M'99-SM'06-F'17) is a professor and Tier-1 Canada Research Chair at Western University, Canada. He received his Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001. Prior to joining Western, he was with Communications Research Centre Canada (CRC) as a research scientist/senior research scientist between July 2002 and December 2007. From January 2001 to July 2002 he was a system designer at STMicroelectronics. His current research interests include 5G/6G technologies, Internet-of-Things, communications security, machine learning and intelligent communications. He has over 400 highly cited journal and conference papers, in addition to 30 granted and pending patents and several standards contributions. He is a Fellow of the Canadian Academy of Engineering, a Fellow of the Engineering Institute of Canada, a Fellow of IEEE, and an IEEE Distinguished Lecturer. He has received many awards and recognitions, including Canada Research Chair, CRC President's Excellence Award, Canadian Federal Government Public Service Award, Ontario Early Researcher Award, and six IEEE Best Paper Awards. He currently serves/has served as an Editor-in-Chief, Associate Editor-in-Chief, editor/associate editor for over 10 journals. He has been involved in many IEEE conferences, including Globecom, ICC, VTC, PIMRC, WCNC and CWIT, in different roles such as symposium chair, tutorial instructor, track chair, session chair, TPC co-chair and keynote speaker. He has been nominated as an IEEE Distinguished Lecturer several times during the last 10 years. He is currently serving as the Chair of the IEEE London Section and the Chair of the ComSoc Signal Processing and Computing for Communications Technical Committee.