DATA SCIENCE AND ARTIFICIAL INTELLIGENCE FOR COMMUNICATIONS


Irena Atov


Kwang-Cheng Chen


Ahmed Kamal


Shui Yu

This is the second issue of the Data Science and Artificial Intelligence for Communications Series. The series, despite its short lifetime, is proving to be very popular, and is receiving many submissions. These submissions undergo a rigorous review process in order to ensure the high quality of the papers selected for publication.

The innovation in artificial intelligence (AI), machine learning (ML), and network data analytics provides a huge opportunity to revolutionize the world's communications systems and user experience. Through gathering, processing, learning, and controlling the vast amounts of information in an intelligent manner, these analytics tools enable the possibility to automate and optimize systems in a way that was not previously possible. This is particularly important as the communications infrastructures evolve to support increasingly more complex communications and enable, through the connectedness of meters, sensors, and things, a plethora of new services. Supporting such immensely diverse applications with equally diverse traffic characteristics will require dynamic, highly adaptive network environments, while ensuring highly reliable, secure, and ultra-low-latency service performance guarantees.

For this second issue, we accepted six articles after a thorough review process. These all feature new opportunities to develop and advance various areas of communications through the use and applications of AI/ML/deep learning technologies. Topics covered range from emotion sensing and monitoring, neural network-based robust IoT networking, channel state information estimates verification in device-to-device communications, deep reinforcement learning-based Service Function Chain allocation in IoT networks, using machine learning for channel modeling in vehicle-to-vehicle communications, and data security issues in clouds providing Machine Learning as a Service.

Emotion is a complex mental state that guides people's thoughts and behaviors. The ability to recognize one's own emotions and to understand others' emotions helps people manage their personal lives and social relations more successfully. Mobile and wearable devices have become ubiquitous, and they provide great opportunities for building emotional intelligent applications. In the first article, "Emotion Sensing for Mobile Computing," by J. Shu, M. Chiu and P. Hui, the authors introduce how mobile and wearable devices work as "emotion sensors" by leveraging their sensing, computing, and communication capabilities. This helps in monitoring people's mental health, facilitating social interactions, and improving user experience. The article introduces a general emotion sensing framework that consists of sensing, inferring, and responding steps. The article discusses how various sensing modalities enabled by mobile and wearable devices can be used, and describes the widely used inferring procedures and methods. The authors present three solutions for facial expression recognition on smartphones as a case of emotion inference. Emerging emotion sensing applications are introduced, and finally challenges and opportunities are presented.

An important application of IoT is in smart cities, and in this case many low-powered devices are widely deployed, and networked. It is important for these devices and their interconnections to be resilient to all attacks, and especially malicious ones that can cause nodes, and in particular high-degree nodes, to fail, hence causing communications disruption. There is, therefore, a strong motivation for improving the robustness of IoT topology and maintaining a high communication capacity in cases of node failure. However, existing robustness optimization algorithms have a prohibitively high computational cost that is an obstacle to efficient topology self-optimization in IoT systems. This problem is addressed in the second article, "An Intelligent Robust Networking Mechanism for the Internet of Things," by N. Chen, T. Qiu, X. Zhou, K. Li, and M. Atiquzzaman. This article proposes a solution to this problem by introducing a robust networking model based on artificial intelligence that improves IoT topology robustness protecting its communications. Using the Back-Propagation neural network learning algorithm, the model extracts topology features from a dataset by supervised training. The experimental results show that the model achieves better prediction accuracy, thereby optimizing the topology with minimal computation overhead.

Device-to-device (D2D) communications is used in various applications using wireless communications. With limited wireless resource, and in data intensive applications, data transmission requirements may not be guaranteed for all users. Some users must therefore temporarily disconnect from a network to guarantee the normal operation of the network. The user access control strategy depends on the authenticity of channel state information (CSI) estimation, as users with higher CSI values may be allocated more wireless resource and be allowed to stay in the network with higher probabilities. To solve this problem, in the third article, "Heuristic-Learning-Based Network Architecture for Device-to-Device User Access Control," by D. Lin, S. Hu, Y. Gao, and

W. Tang, the authors propose a heuristic learning method in which each user's CSI needs to be verified, and the users advocating a larger CSI may be detected to be fraud. The results indicate that a dramatic increase of network performance can be captured by the proposed algorithm.

Network Function Virtualization (NFS) is now being used in many communications networks, including IoT networks, due to its prospect of achieving efficient resource management. In an NFV-enabled IoT infrastructure, a Service Function Chain (SFC) consists of an ordered set of Virtualized Network Functions (VNFs) that are connected based on the business logic of service providers. However, due to the dynamic nature of IoT networks, and the large number of IoT devices, the SFC embedding process for IoT networks can become inefficient. Motivated by this problem, and by the fact that VNF nodes and physical network devices are usually heterogeneous, the fourth article, "Service Function Chain Embedding for NFV-Enabled IoT Based on Deep Reinforcement Learning," by X. Fu, F. R. Yu, J. Wang, Q. Qi, and J. Liao, introduces a solution to this problem in which the complex VNFs are decomposed into smaller VNF components (VNFCs) in order to make more effective decisions. A deep reinforcement learning (DRL)-based scheme with experience replay and target network is also proposed as a solution that can efficiently handle complex and dynamic SFC embedding scenarios. Simulation results present the efficient performance of the proposed DRL-based dynamic SFC embedding scheme.

Vehicle-to-vehicle (V2V) communications have become a major research topic in the last decade because of their many potential applications and opportunities, including being part of the intelligent transportation system. However, the performance of V2V communications fundamentally depends on the propagation channels in which they are operating. The development and analysis of V2V systems thus requires suitable channel models. The fifth article in this month's series, "Machine-Learning-Based Data Processing Techniques for Vehicle-to-Vehicle Channel Modeling," by C. Huang, A. F. Molisch, R. He, R. Wang, P. Tang, and Z. Zhong, deals with channel modeling for V2V communications, and in particular machine-learning based techniques. The article reviews some state-of-the-art applications including identification of channel line-of-sight situations, tracking of Multipath Components (MPCs), and MPC clustering. The data obtained with these methods form the basis for accurate channel models. Some challenges of machine-learning-based data processing for V2V channel research are discussed as the basis for future studies.

Machine Learning as a Service (MLaaS) is provided by several cloud service providers, such as Google, Amazon and Microsoft. MLaaS acts as cloud-assisted machine learning services. MLaaS provides a range of customized training and prediction services that only require users to upload local data. However, outsourced deep learning also brings about various privacy and security concerns. The sixth article, "Data Security Issues in Deep Learning: Attacks, Countermeasures, and Opportunities," by G. Xu, H. Li , H. Ren, K. Yang, and R. H. Deng, addresses data security issues in deep learning, and investigates the potential threats of deep learning. The article then presents the latest countermeasures based on various underlying technologies, where the challenges and research opportunities on offense and defense are also discussed. Then they propose the SecureNet protocol, which is presented as the first verifiable and privacy-preserving prediction protocol to protect model integrity and user privacy in deep neural networks.

We thank all the authors and reviewers for contributing to this Series. We also thank the Editor-in-Chief of *IEEE Communications Magazine*, Dr. Tarek El-Bawab, for his support and guidance, as well as the *IEEE Communications Magazine* staff for their efficient processing of the papers.

BIOGRAPHIES

IRENA ATOV [SM] (i.atov@ieee.org) received her Ph.D. in electrical engineering from RMIT University, Australia in 2003. She is currently Principal Architect at Microsoft, USA, in their Intelligent Conversation and Communications Cloud (IC3) Group, O365 Services. Previously, she has worked in academia, consulted for industry through her own company and worked for Telstra in Melbourne, Australia as Program Director of Network Analytics and Resilience. Her research in network architecture design and performance optimization led to the development of several commercial IT software products.

KWANG-CHENG CHEN [M'89, SM'94, F'07] (kwangcheng@usf.edu) is a professor of electrical engineering at the University of South Florida, Tampa. He has widely served in IEEE conference organization and journal editorship. He has contributed essential technology to IEEE 802, Bluetooth, LTE and LTE-A, and 5G-NR wireless standards. He has received a number of IEEE awards. His recent research interests include wireless networks, artificial intelligence and machine learning, IoT and CPS, social networks, and cybersecurity.

AHMED E. KAMAL [SM'82, M'87, SM'91, F'12] (kamal@iastate.edu) is a professor of electrical and computer engineering at Iowa State University in the USA. He served the IEEE Communications Society as a Distinguished Lecturer, as the chair of the technical committee on Transmission, Access and Optical Systems (TAOS), and as a chair or co-chair of a number of conferences and symposia. He is currently serving as the lead editor of the *IEEE Communications Magazine* Data Science and Artificial Intelligence for Communications Series. Kamal's current research interests include wireless networks, cloud computing, and machine learning applications in communications and networking.

SHUI YU [SM] (Shui.Yu@uts.edu.au) is a professor in the School of Computer Science, University of Technology Sydney, Australia. His research interests include security and privacy, networking, big data, and mathematical modelling. He is a Series Editor of *IEEE Communications Magazine*, a member of AAAS and ACM, and a Distinguished Lecturer of the IEEE Communication Society.