Editorial: Third Quarter 2020 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS

I WELCOME you to the third issue of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS in 2020. This issue includes 20 papers covering different aspects of communication networks. In particular, these articles survey and tutor various issues in "Wireless, Optical, and Sensor Communications," "IoT and M2M," "Network Security," and "Internet Technologies." A brief account for each of these papers is given below.

I. WIRELESS, OPTICAL, AND SENSOR COMMUNICATIONS

Future wireless networks have a substantial potential in terms of supporting a broad range of complex compelling applications both in military and civilian fields, where the users are able to enjoy high-rate, low-latency, low-cost and reliable information services. Achieving this ambitious goal requires new radio techniques both for adaptive learning and for intelligent decision making because of the complex and dynamically fluctuating nature of the heterogeneous network topology supporting sophisticated wireless services. Machine learning (ML) algorithms have been widely employed for supporting big data analytics, efficient parameter estimation and interactive decision making, for example. Hence in the article entitled "Thirty Years of Machine Learning: The Road to Pareto-Optimal Wireless Networks" by Jingjing Wang, Chunxiao Jiang, Haijun Zhang, Yong Ren, Kwang-Cheng Chen, and Lajos Hanzo reviews the three-decade historic evolution of ML by elaborating on supervised learning, unsupervised learning, reinforcement learning, and deep learning. Furthermore, they investigate a suite of compelling applications in the context of wireless networks, including heterogeneous networks (HetNets), cognitive radios (CR), Internet of Things (IoT), machine to machine networks (M2M), and so on. The article aims for assisting the readers in clarifying the motivation, methodology as well as the pros and cons of the various ML algorithms in the context of hitherto unexplored services as well as scenarios of future wireless networks. More explicitly, the authors recommend these powerful learning and optimization techniques for solving challenging multi-component optimization problems and for exploring the entire Pareto front of optimal solutions.

As we head toward future mobile networks (5G and beyond), the coverage map of certain promising paradigms to the Radio Access Networks is increasing considerably. These paradigms include technologies from the computing world such as Software Defined Networks and Network Function Virtualization, as well as technologies from autonomous management such as Self-Organizing Networks. With this progressive shift, the nature of resources and the approaches for resource management in Cloud Radio Access Networks (C-RAN) have been evolving to pave the way toward more efficiency, and new business opportunities, where the RAN infrastructure and the spectrum can be shared between multiple operators, including virtual ones who do not even own any infrastructure. Within this context, the paper titled "On Energy Efficient Resource Allocation in Shared RANs: Survey and Qualitative Analysis" by Fatma Marzouk, João Paulo Baracca, and Ayman Radwan presents the opportunities and synergies arising from the combination of these paradigms in the RAN. It also lists the relevant standardization activities, research projects, and state of the art schemes that leverage some (or all) of these paradigms for C-RAN efficient resource management. Particularly, it offers a tutorial on how to leverage the arising synergy of their application to bring more energy efficiency to future mobile networks. Moreover, the paper summarizes a range of recent resource allocation schemes with respect to the aforementioned metric and highlights the current gaps in the literature. The paper then concludes by elaborating on the open challenges that need to be tackled by future research, which makes the paper a very important read and guide for young researchers, looking to start their research in such promising area.

Researchers use data and signals to measure physical quantities and convey information between different communication nodes, respectively. Studying and analyzing associated systems requires appropriate modeling to understand the theoretical performance and helps to implement and design suitable practical systems. Theoretical statistical studies adopt the symmetric Gaussian distribution as a convenient model for analysis and design. Then, practical systems can be implemented using the closest symmetrical signal to the theoretical one. An important step to move close to actual data and signals is to deal with asymmetric (improper) Gaussian signals, which include the symmetric one as a special case. Then, it is important to realize and approximate it by some asymmetric discrete signals to suit the practical system constraints. This study benefits several fields that uses data and signals, such as signal processing, communication systems, power systems, optics, acoustics, etc. In this context, the paper titled "A Journey From Improper Gaussian Signaling to Asymmetric Signaling," by Sidrah Javed, Osama Amin, Basem Shihada and Mohamed-Slim Alouini presents a tutorial and survey. First, the paper introduces a comprehensive mathematical stochastic background about the complex proper and improper Gaussian signals. Then, the paper focuses on communication system

Digital Object Identifier 10.1109/COMST.2020.3013455

theoretical system performance followed by the design guidelines in addition to impropriety detection, estimation, filtering and separation procedures. After that, the paper moves to the practical implementation journey part via asymmetric discrete signals. Finally, the paper discusses several applications followed by useful learned lessons and challenges that are suitable for future research.

As a fifth generation of wireless technologies, 5G turns the communication networks to service-oriented, on-demand, and highly heterogeneous. Therefore, it is of utmost importance to approach the design and the optimization of 5G network from an end-to-end perspective. Since the concept of sharing resources is well-known for its considerable benefits in any realm to which it is applied, shifting from the exclusive ownership of network resources to sharing enables all participants to cope with stringent service requirements in 5G networks, thereby gaining significant performance improvements and cost savings at the same time. In this context, the paper entitled "Sharing Distributed and Heterogeneous Resources toward End-to-End 5G Networks: A Comprehensive Survey and a Taxonomy" by Nina Slamnik-Kriještorac, Haris Kremo, Marco Ruffini, and Johann Marquez-Barja surveys the literature on network resource sharing, providing an in-depth, and comprehensive perspective of sharing by recognizing evolution of the main trends, the techniques which enable sharing, and the challenges that remain to be addressed from an end-to-end network perspective. Such perspective spans heterogeneous resource sharing that crosses both wireless and optical network domains, and extends to IoT, edge, and cloud, which altogether coexist in 5G network. By identifying up to what extent and how can resources be shared, and recognizing the challenges that have arisen from highly dynamic, and strongly diverse 5G environment, this paper focuses on the relevant features of a comprehensive sharing model, paving the way toward bringing more efficiency and flexibility to network architectures, which is a seminal point for future research directions.

With the rapid advancement of wireless sensing methodologies, many studies have shown the success of re-using wireless signals (e.g., WiFi) to sense human activities and thereby realize a set of emerging applications, ranging from intrusion detection, daily activity recognition, gesture recognition to vital signs monitoring and user identification involving even finer-grained motion sensing. These applications arguably can brace various domains for smart home and office environments, including safety protection, well-being monitoring/management, smart healthcare and smart-appliance interaction. The movements of the human body impact the wireless signal propagation (e.g., reflection, diffraction and scattering), which provide great opportunities to capture human motions by analyzing the received wireless signals. In this context, the paper titled "Wireless Sensing for Human Activity: A Survey" by Jian Liu, Hongbo Liu, Yingying Chen, Yan Wang, and Chen Wang presents a survey of existing wireless sensing systems in terms of their basic principles, techniques, and system structures. Particularly, the survey describes how the wireless signals could be utilized to facilitate an array of applications including intrusion detection, room occupancy monitoring, daily activity recognition, gesture recognition, vital signs monitoring, user identification, and indoor localization. The future research directions and limitations of using wireless signals for human activity sensing are also discussed.

II. IoT and M2M

IoT systems are accessible worldwide, consist mainly of constrained resources and constructed by lossy links. Therefore, crucial modifications of existing security concepts for information and wireless networks should be implemented to provide effective IoT security methods. Applying existing defense mechanisms, such as encryption, authentication, access control, network security and application security, is challenging and insufficient for mega systems with many connected devices, with each part of the system having inherent vulnerabilities. In this context, the paper titled "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security" by Al-Garadi, Mohammed Ali, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani reviews various IoT security threats and discusses IoT attack surfaces. A comprehensive review of the potential uses of ML and DL methods in IoT security is provided by the paper. These methods are then compared at the end of each subsection in terms of their advantages, disadvantages, and applications in IoT security. Afterward, the uses of the ML and DL methods for securing the main IoT layers (i.e., perception, network, and application layers) are reviewed. Finally, an extensive list of issues, challenges, and future directions related to the use of ML and DL in effectively securing IoT systems are presented and classified according to data; learning strategies; ML and DL for IoT security in the interdependent, interconnected, and interactive environments of IoT systems; diverse security tradeoffs in IoT applications and synergic integration of ML and DL with blockchain for IoT security.

Internet of Things (IoT) is one of the disruptive technologies that is poised to revolutionize many sectors of our lives that include, but not limited to, lifestyle, health, comfort, industry, trade, agriculture, and so on. The future of IoT will have a deep economical, commercial, and social impact on our lives. However, the resource-constrained nodes in IoT networks are luring targets for cyber-attacks. Despite extensive research on security in IoT, the unique characteristics of IoT nodes render the existing security inefficient to encompass the entire security spectrum of IoT networks. Therefore, Machine Learning (ML) and Deep Learning (DL) techniques are employed to provide embedded intelligence and are leveraged to cope with different security problems such as attack detection and mitigation, authentication, access control, trust management, and security at different layers of communication. In this context, the paper titled, "Machine Learning in IoT Security: Current Solutions and Future Challenges" by Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain presents a comprehensive survey on the role of machine and deep learning in the security of IoT networks. The paper starts with the motivation of using machine and deep learning in IoT security by discussing the characteristics

of and security challenges in IoT networks. The paper dives deeper into security attacks at different layers of IoT communication and then discusses the machine and deep learning models that are leveraged for IoT security. The paper then discusses in detail, the current ML- and DL-based security solutions in IoT networks. The paper also covers emerging ML techniques such as Adversarial Machine Learning (AML) in IoT security. In the end, the paper also identifies future research directions in using machine and deep learning for security in IoT networks.

The Internet of Things (IoT) extends the Internet connectivity into billions of IoT devices around the world, creating massive amount of distributed data and unlimited opportunities in the future "smart world". To achieve its full potential and benefits in diverse applications, the huge amount of sensory data collected by the IoT systems needs to be effectively analyzed by leveraging machine learning (ML) techniques. By integrating IoT, ML and autonomous control, the concept of autonomous IoT (AIoT) was proposed as the next wave of IoT that can explore its future potential. In order to achieve autonomy, a promising method is for the intelligent agents to leverage the techniques in the field of reinforcement learning (RL) and deep reinforcement learning (DRL) for decision making. This development brings both numerous technical challenges and rich research, development, and commercialization opportunities. In this context, the paper titled "Deep Reinforcement Learning for Autonomous Internet of Things: Model, Applications and Challenges" by Lei Lei, Yue Tan, Kan Zheng, Shiwen Liu, Kuan Zhang, and Xuemin Shen presents a tutorial and survey. First, the paper starts by providing a tutorial of DRL. Then, the paper proposes a general model for the applications of RL/DRL in AIoT. Furthermore, the paper presents a comprehensive survey of the state-of-art research on DRL for AIoT, where the existing works are classified and summarized under the umbrella of the proposed general DRL model. Finally, the paper identifies the challenges and open issues for future.

IoT has become imminent in all the fields of life by interconnecting low-cost sensors with the Internet, which collect physical world data and assist in autonomously controlling real-world infrastructures. However, these sensors produce and transmit an immense amount of data, which is challenging to manage by resource-limited IoT devices having low computational power, limited storage, and constrained communication resources. Software defined networking provides centralized network management, which could be exploited to manage complexity issues in seamless IoT service orchestration. Moreover, edge computing offers an effective solution for the resource-limitation challenge in IoT by providing resources near the edge of IoT to execute latency-sensitive and compute-intensive tasks. In this context, the paper titled, "Complementing IoT Services through Software Defined Networking and Edge Computing: A Comprehensive Survey" by Wajid Rafique, Lianyong Qi, Ibrar Yaqoob, Muhammad Imran, Raihan ur Rasool, and Wanchun Dou presents a comprehensive survey on end-to-end IoT services orchestration. This survey discusses state-of-the-art research on IoT service orchestration using SDN and edge computing and presents key requirements, use cases, standardization, and security challenges in this paradigm. It comprehensively outlines the current challenges, open problems, and future research directions in complementing IoT services through SDN and edge computing.

The Internet of Things (IoT) is swiftly turning into a reality, transforming every physical object into an information source. This has brought a significant increase in the number of devices entering the telecommunication framework, and is expected to demonstrate an exponential growth in the coming years. Besides supporting this massive number of predominantly autonomous IoT devices, a prime concern is to accommodate their sporadic-natured short packet data transmissions and lower power constraints. This has driven researchers away from classical grant-based access schemes notorious for their large signaling overhead and power-consuming retransmissions. To this end, grant-free access has been identified as a key medium access control technique for providing connectivity to such sporadically transmitting IoT devices. However, due to the limited number of available channel resources, grant-free access must be carefully designed to minimize collisions. In this context, the paper titled "Grant-Free Non-orthogonal Multiple Access for IoT: A Survey" by Muhammad Basit Shahab, Rana Abbas, Mahyar Shirvanimoghaddam, and Sarah J. Johnson provides a comprehensive review of non-orthogonal multiple access (NOMA), a technique capable of serving multiple devices over the same channel resource, in grant-free communications. Besides a detailed review of the various grant-free NOMA schemes proposed by academia and industry, an information theoretic perspective is also provided, which highlights the gaps between theory and practice. Finally, the paper presents some open research challenges, possible solutions, and comprehensively discusses the future directions of grant-free NOMA in IoT.

Connecting the unconnected and monitoring the unmonitored have become essential requirements for industry and modern life to overcome the world digital divide problem. One effective technology to achieve these targets is through emerging space communications. Technologies with low design and deployment costs are the new frontiers for the space industry, such as CubeSats. In fact, CubeSats are envisioned to provide low-cost alternatives that enable several applications, including remote sensing, space exploration, and rural connectivity for the Internet of Things (IoT) networks and ubiquitous coverage. In this regard, the paper titled "CubeSat Communications: Recent Advances and Future Challenges" by Nasir Saeed, Ahmed Elzanaty, Heba Almorad, Hayssam Dahrouj, Tareq Y. Al-Naffouri, and Mohamed-Slim Alouini presents a holistic view on CubeSats from the communications engineering perspective. In particular, the paper thoroughly investigates the various communications aspects of CubeSats, including channel modeling, modulation and coding, global coverage, and networking. Then, it concludes with future research challenges such as the integration with next-generation cellular systems and the realization of the Internet of Space Things.

Device to Device (D2D) communication allows devices to communicate with each other without the access points. Devices are able to do the data forwarding and data sharing

through opportunistic encounters which is affected by the mobility of the users. This makes the modelling of realistic mobility patterns a difficult task because of inherent complexity of human mobility patterns. In this context, the paper titled "A Comprehensive Survey on Mobility-Aware D2D Communications: Principles, Practice and Challenges" by Muhammad Waqas, Yong Niu, Yong Li, Depeng Jin, Sheng Chen, and Zhu Han presents a detailed survey of the mobile D2D communication. The paper studies the nature of mobility in order to improve the system wide level performance and achieve the real-life observation. The paper reviews the state-of-the-art problems and solutions for encouraging mobility in D2D communications. The paper also provides a summary of mobility advantages by identifying the mobility models, problems, and requirements of different proposals. The paper also discusses the mobility aware D2D communication to provide a deeper understanding of the related problems and potential solutions. Lastly, it concludes with providing the future research directions and open problems related to the real-life people and vehicles interaction scenarios in a dynamic environment.

III. Network Security

Visible light communication (VLC) is an emerging technology that has been introduced as a promising solution for 5G and beyond, owing to the large unexploited spectrum, which translates to significantly high data rates. VLC technology operates in the visible light frequency spectrum and uses light for both illumination and data communication purposes simultaneously. Some of the noted advantages of VLC systems over traditional radio frequency (RF) systems is the higher security that VLC systems provide. This is basically inherited from the fact that light does not penetrate through walls. However, security issues arise naturally in VLC systems due to their open and broadcast nature. Specifically, VLC systems could be as vulnerable as their RF counterparts when their nodes are deployed in public areas and/or when there are large windows in the coverage areas. Thus, security for VLC systems is as important as it is for RF systems. Due to this, security should be deeply investigated in the VLC context. On the other hand, security in wireless communication systems, including 5G and beyond wireless networks, may be enhanced by introducing physical layer security (PLS) techniques. In fact, PLS techniques have been applied to a wide range of RF applications in an effort to improve the overall system security by complementing existing cryptography-based security techniques. The potential of PLS stems from its ability to leverage features of the surrounding environments via sophisticated encoding techniques at the physical layer. Indeed, PLS schemes can be applied in the same spirit to VLC systems. In this context, the paper entitled "Physical Layer Security for Visible Light Communication Systems: A Survey" by Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Majid Safari, Chadi Assi, and Harald Haas provides a comparative and unified survey on PLS for VLC from information theoretic and signal processing point of views. Specifically, it covers almost all aspects of PLS for VLC, including different channel models, input distributions, network configurations, precoding/signaling strategies, secrecy capacity, and information rates. In addition, it proposes a number of timely and open research directions for PLS-VLC systems, including the application of measurement-based indoor and outdoor channel models, incorporating user mobility and device orientation into the channel model, and combining VLC and RF systems to realize the potential of such technologies.

Moving Target Defenses (MTD) are cyber defense tools, techniques and practices proposed to address asymmetric advantages inherent in the static nature of current systems. In the context of Moving Target Defenses, the paper titled "A Survey of Moving Target Defenses for Network Security" by Sailik Sengupta, Ankur Chowdhary, Adel Alshamrani, Abdulhakim Sabur, and Subbarao Kambhampati considers categorization, implementation, and evaluation of current MTD research. The paper proposes a unified terminology that characterizes existing works and can be used to define novel MTDs. The authors then highlight how surveyed works strengthen these dynamic defenses with the use of Artificial Intelligent (AI) techniques for decision making, showcasing opportunities for improvement. Given various MTDs have been developed in the literature, the authors seek to characterize the maturity of their implementations, ranging from simulation environments to industrial settings, highlighting popular test-beds that can be leveraged by new defenses. The survey enumerates a variety of proposed qualitative and quantitative metrics that can be leveraged to measure the effectiveness of an MTD. Finally, the paper concludes by providing an overview of the state-of-the-art and highlighting the directions for future work.

Supervisory Control And Data Acquisition (SCADA) systems are crucial to a wide range of applications, such as power generation and distribution, telecommunications infrastructures, transportation, and manufacturing industries. The continuous and reliable operation of SCADA systems may have a crucial effect on public safety and health. As SCADA systems are being connected to the Internet, they are exposed to a wide range of security threats that can disrupt their normal operation. Consequently, a potential cyberattack against a SCADA system can have devastating consequences. In this context, the paper titled "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics" by Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thomas Lagkas, and Antonios G. Sarigiannidis presents a survey that overviews the landscape of SCADA security. In this work, the general SCADA architecture is provided, along with a detailed overview of widely-used communication protocols. Several high-impact security incidents and threats are presented to highlight the importance of SCADA security considerations. Furthermore, the paper provides a thorough review of SCADA security proposals and discusses the state of SCADA security. Finally, the paper compiles a list of research trends and advancements in the area of SCADA security.

The use of blockchains is expanding beyond digital currencies to audit applications, Internet of Things, supply chains, and distributed provenance, among others. In parallel, new

attacks are launched on blockchain systems by exploiting weaknesses in their cryptographic constructs, their peer-to-peer network deployments, and their application-specific use cases. It is therefore pertinent to comprehensively analyze the blockchain attack surface as a prerequisite to counter those attacks in the future. In this context, the paper titled "Exploring the Attack Surface of Blockchain: A Comprehensive Survey" by Muhammad Saad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and David Mohaisen surveys the blockchain attack surface by contextualizing various attack vectors associated with the cryptographic underpinnings of blockchain data structure, the peer-to-peer communication model of blockchain systems, and the application-specific usage of blockchain technology. Additionally, by outlining commonalities between various attack vectors, the paper helps in devising a common cure. Finally, by surveying the existing countermeasures and their limitations, the paper provides open challenges and future directions to strengthen the blockchain security.

Both blockchain and cloud computing are deemed advance technologies that are facilitating current Web-based applications and innovations. Integrating these two technologies has a high potential in strengthening functionality, performance, security, and privacy protections. Even though the voice of fusing blockchain with cloud computing is high, the challenging issue is to accurately locate the place in which the integration can successfully reengineer cloud datacenter with additional values. In this context, the paper titled "Blockchain Meets Cloud Computing: A survey" by Keke Gai, Jinnan Guo, Liehuang Zhu, and Shui Yu accomplishes a comprehensive investigation on technical fusions of blockchain and cloud computing in a variety of dimensions. Comparisons and analyses on each technical dimension also contribute to facilitating knowledge scaffold in guiding future studies in this field. Specifically, technical dimensions covered by this survey include blockchain-as-a-Service (BaaS), blockchain-based data governance/ provenance in clouds, blockchain-based access control in clouds, blockchain-enabled searchable encryptions, blockchain-based data deduplication, smart contract implementations in cloud allocations, hardware-based blockchain enhancement, and blockchain-based storage. The findings of this paper include both challenges (e.g., multi-chain technical bottleneck, user identity verification, and security) and future research opportunities (e.g., network-based blockchain technique and customized blockchain services).

IV. Internet Technologies

In recent years, Mobile Edge Computing (MEC) has been proposed to bring intelligence closer to the edge, where data is produced. However, conventional enabling technologies for Machine Learning (ML) at mobile edge networks still require personal data to be shared with external parties, e.g., edge servers. Recently, Federated Learning (FL) has been introduced as an enabling technology in mobile edge networks since it enables the collaborative training of an ML model and also enables DL for mobile edge network optimization. However, in a large-scale and complex mobile edge network, heterogeneous devices with varying constraints are involved. This raises challenges of communication costs, resource allocation, and privacy and security in the implementation of FL at scale. In this context, the paper titled "Federated Learning in Mobile Edge Networks: A Comprehensive Survey" by Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao presents a tutorial of FL and a comprehensive survey on the issues regarding FL implementation. First, the paper begins with the motivations of MEC and describes the fundamentals of DNN model training, FL, and system design towards FL at scale. Afterwards, the paper provides detailed reviews, analyses, and comparisons of approaches for emerging implementation challenges in FL. The issues including communication cost, resource allocation, data privacy and data security, implementation of FL for privacy-preserving mobile edge network optimization, together with challenges and future research directions are also discussed.

The scaling of today's network to accommodate the ever-increasing network traffic puts new demands on accurate network data analysis for tasks like configuration, monitoring, maintenance, intrusion detection, and quality assurance. Moreover, the emphasis on network security and privacy shifts the current research focus to areas like anomaly detection, attack detection, and traffic classification. All of these tasks rely on availability of accurate network data, which can be either raw network packets, network device counters, or network flows. Network flows establish an optimum compromise between the accurate but highly resource-demanding storing and analysis of network packets and the lightweight device counters that suffer from a possibly too limited view of the network. Software or hardware utilities that convert streams of network packets into network flows are termed flow exporters. Many existing standards and research efforts define related network flow formats, flow acquisition and flow analysis methods. However, the paper "Why Are My Flows Different? A Tutorial on Flow Exporters" by Gernot Vormayr, Joachim Fabini, and Tanja Zseby, identifies substantial shortcomings of existing flow exporters that threaten reproducible data analysis and research. Deficiencies of existing flow exporters include non-deterministic results due to differing interpretation of flow definitions, missing general-purpose usability, and even implementation errors. Advancing state of the art in flow exporting, this publication features a detailed tutorial and guidelines on safeguarding accurate, reproducible flow aggregation and export. The open-source released flow-exporter go-flows is presented as a flexible and extensible reference implementation to support the community in progressing reproducible data analysis.

The Internet has been an unprecedented and lasting success story, fueled by the simplicity of its architectural design grounded on the Internet Protocol (IP). Nonetheless, several limitations of IP have been emerging in recent years, due to the shift in the Internet usage mainly caused by increased mobility, number of connected devices, network-based services, and distributed content production. The Information-Centric Networking (ICN) paradigm, pivoted on content distribution, rather than hosts "connection," has been proposed as

a possible replacement for the current IP-based Internet. A significant effort has been already put by Governments, Industry, and Academia to assess the feasibility and effectiveness of ICN. While results are promising, there is a widely underestimated aspect: how the transition from the current IP-world to the "future" ICN-world can happen in a smooth and secure way. So far, researchers have addressed the coexistence by designing their own architectures, without, however, providing the final one to move towards the future Internet. In this context, the paper titled "The Road Ahead for Networking: A Survey on ICN-IP Coexistence Solutions" by Mauro Conti, Ankit Gangwal, Muhammad Hassan, Chhagan Lal, and Eleonora Losiouk presents a survey and a classification of the coexistence architectures according to their features (i.e., deployment approach, deployment scenarios, addressed coexistence requirements and additional architecture or technology used) and evaluation parameters (i.e., challenges emerging during the deployment and the runtime behavior of an architecture).

I hope that you enjoy reading this issue and find the articles useful. Last but not the least, I highly encourage you to submit your work which fit within the scope of ComST. For detailed instructions on the preparation and submissions of manuscripts to ComST, please check the URL below: http://dl.comsoc.org/livepubs/surveys/. I will be happy to receive your comment and feedback on our journal.

YING-DAR LIN, ***Fellow, IEEE***
IEEE Distinguished Lecturer
Editor-in-Chief
IEEE COMMUNICATIONS SURVEYS AND TUTORIALS
Distinguished Professor, Department of Computer Science, National Chiao Tung University
Hsinchu 300, Taiwan
Director, Network Benchmarking Lab
Web: www.cs.nctu.edu.tw/∼ydlin