Editorial: Fourth Quarter 2018 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS

I WELCOME you to the fourth issue of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS in 2018. This issue includes 35 papers covering different aspects of communication networks. In particular, these articles survey and tutor various issues in "Wireless Communications," "Optical Communications," "Vehicular and Sensor Communications," "IoT and M2M," "5G and SDN," "Network Virtualization," "Network Security," "Network and Service Management and Green Communications," and "Internet Technologies." A brief account for each of these papers is given below.

I. WIRELESS COMMUNICATIONS

Nowadays, precise prediction of systems and automatic control based on the prediction has caused extensive interests in both academic field and industrial field. The more accurate the prediction, the better control will be achieved. This desire was first achieved by machine learning. However, with the increase of the system complexity, deep learning is becoming a more powerful tool in precise prediction and system control. Compared to traditional machine learning methods, deep learning is able to handle more complex systems and to yield more accurate prediction. Meanwhile, deep learning system does not need delicate pre-processing of the input data, and it can adjust the system automatically. For these advantages, deep learning has been extensively used in many fields. In this context, the paper titled "Deep Learning for Intelligent Wireless Networks: A Comprehensive Survey" by Qian Mao, Fei Hu, and Qi Hao conducts a comprehensive survey on the deep learning applications in wireless network. These applications are categorized as physical layer applications, data link layer applications, routing layer applications, and other network functions. For each category, the application methods are summarized, analyzed, and compared. It can be seen that the deep learning approaches increase the network performance significantly. However, computation complexity and how to efficiently collect network environment parameters used for deep learning network are tricky problems. Meanwhile, some popular implementation platforms of deep learning approach for communication network are provided and compared. Finally, ten future research trends are presented, which can help researchers to identify unsolved issues in this field.

Finding a route from the source node to the destination node is of critical importance in nearly all types of communication networks. With the advent of wireless networks and its proliferation into several types like wireless sensor network, cognitive radio network, wireless ad-hoc network, wireless local area network, cellular network and device-to-device network etc., necessitate the need of routing protocols to fulfill the unique requirements of each network. Thus, numerous routing protocols had been proposed for each type of network targeting different performance criteria. The device-to-device (D2D) communication has been proposed to enable direct communication between the cellular nodes without passing data from the base station (BS). The third generation partnership project (3GPP) defines three possible network scenarios for D2D communications which are in-coverage, partial-coverage and out-of-coverage scenarios. Establishing a multi-hop D2D route is crucial in all types of these network scenarios whenever the two nodes which want to communicate, are not in the transmission range of each other. In this context, the paper titled "Routing in Multi-Hop Cellular Device-to-Device (D2D) Networks: A Survey" by Farrukh Salim Shaikh and Roland Wismüller presents a survey, where the paper classifies the routing schemes proposed for D2D networks, based on the interaction behavior of D2D nodes with the cellular network. Each class has been further divided into several categories, which help to select a routing algorithm based on varying user and network requirements. The paper concludes with the discussion of open research problems and highlights the future research directions that require further investigations.

The combination of ubiquitous Internet connectivity, availability of multi-purpose applications, and lack of instruments to control sensitive information flows pose a serious privacy threat for the users of mobile devices (e.g., smartphones and tablets). In particular, the network traffic of such devices is an invaluable source from which it is possible to infer sensible information about mobile users (e.g., social life, position, habits). More worryingly, the adoption of encryption protocols (e.g., SSL/TLS) does not seem to be enough to prevent such information leaks. In this context, the paper titled "The Dark Side(-Channel) of Mobile Devices: A Survey on Network Traffic Analysis" by Mauro Conti, QianQian Li, Alberto Maragno, and Riccardo Spolaor classifies the works that have been published in the field of network traffic analysis targeting mobile devices. Furthermore, the paper compares the techniques applied in such works, as well as validates their results. The paper also discusses countermeasures,

Digital Object Identifier 10.1109/COMST.2018.2878592

challenges, and future research trends in the considered field.

As a powerful network architecture, Space-Air-Ground Integrated Network (SAGIN) has been proposed to cope with the increasing traffic demands of various applications and services in wireless communication systems. However, compared to existing terrestrial communication systems, SAGIN is much more complex and will face many unprecedented challenges due to its specific characteristics such as heterogeneity, self-organization, and time-variability. It is difficult to use the limited network resources in SAGIN to obtain the best performances for information exchanging, especially for the inter-operating among different network segments. Therefore, the network design, system integration and protocol optimization in SAGIN are of great necessity and significance. In this context, the paper titled "Space-Air-Ground Integrated Network: A Survey" by Jiajia Liu, Yongpeng Shi, Zubair Md. Fadlullah, and Nei Kato presents a survey. First, the paper starts by introducing the architecture for SAGIN. Then, the paper provides a comprehensive overview of the research works about SAGIN, with the emphasis on resource allocation, performance analysis, mobility management, and inter-segment operation. Furthermore, the paper identifies several existing network architectures applicable for SAGIN. Finally, the paper points out some technical challenges and future directions when designing and optimizing such an integrated system.

II. Optical Communications

Evolution of radio access networks, primarily driven by end-users bandwidth demands and the underlying need for wireline transport network throughput, has brought up intensive studies and standardization efforts on the future radio base station architecture and its functional splits. Therein, the analogue connection to a simple antenna unit, the analogue Mobile Fronthaul (a-MFH), may need to be extended to several kilometers, and that would require employment of highly reliable fiber-based transport with proactive and reactive link monitoring capability. In this regard, the paper titled "A Tutorial on Fiber Monitoring for Applications in Analogue Mobile Fronthaul" by Patryk Urban Gustavo Amaral and Jean Pierre von der Weid provides overall requirements for monitoring of the analogue fiber link. The authors have shown that the a-MFH brings up opportunities for a variety of monitoring techniques and implementations based on well-known optical reflectometry techniques in time and frequency domains, which they have summarized in terms of principles of operations, proof of concept works and performance evaluations.

High Performance Computing (HPC) and Data Center (DC) communications, covering quite different scales, have increasingly higher bandwidth demands and at the same time require lower and lower power consumptions. They are already consuming megawatts of power, and a linear extrapolation of trends reveals that they may eventually lead to unrealistic power consumption scenarios in order to satisfy future requirements. Conventional complementary metal oxide semiconductor (CMOS)-based electronic interconnects are not expected to keep up with the envisioned future board-to-board and chip-to-chip (within multi-chip-modules) interconnect requirements because of bandwidth-density and power-consumption limitations. However, low-power and high-speed optics-based interconnects are emerging as alternatives for DC and HPC communications; they offer unique opportunities for continued energy-efficiency and bandwidth-density improvements, although cost is a challenge at the shortest length scales. Plasmonics-based interconnects on the other hand, due to their extremely small size, offer another interesting solution for further scaling operational speed and energy efficiency. In this context, the paper titled "Survey of Photonic and Plasmonic Interconnect Technologies for Intra-Datacenter and High-Performance Computing Communications" by Christos A. Thraskias, Eythimios N. Lallas, Niels Neumann, Laurent Schares, Bert J. Offrein, Ronny Henker, Dirk Plettemeier, Frank Ellinger, Juerg Leuthold, and Ioannis Tomkos presents a survey, where it reviews all recent advancements on photonic and plasmonic short distance interconnections and outlines the associated challenges and future perspectives of this area. This paper compares conventional electrical, photonic and plasmonic short distance interconnect technologies in terms of bandwidth density and energy efficiency, based on the latest literature data. These three technologies were also compared at the device level, including output devices, photodetectors, passive devices and electrical circuitry.

III. Vehicular and Sensor Communications

Recent advances in mobile computing, wireless communication and sensing have enabled the development of a number of interesting and desirable applications in Intelligent Transportation Systems (ITSs). In this way, Vehicular Ad Hoc Networks (VANETs) emerge as a new technology to integrate wireless networks capabilities to vehicles, providing ubiquitous connectivity as well as allowing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Thus, interconnected vehicles can collect and share information about themselves and the surrounding environments in real time. Given this scenario, there is an extensive list of potential applications for VANETs, such as safety, transport efficiency and information/entertainment applications. In all of them, a fundamental requirement is to know the localization of the different mobile entities (e.g., cars, buses, trucks, trams, etc.) in order to properly design those applications. In this context, the paper titled "Localization Prediction in Vehicular Ad Hoc Networks" by Leandro Balico, Antonio Loureiro, Eduardo Nakamura, Raimundo Barreto, Richard Pazzi, and Horacio Oliveira, presents a tutorial and survey on how to use a localization prediction approach as an extension of a data fusion localization system to provide highly accurate and reliable localization information anywhere and anytime in VANETs. First, the paper presents different proposals to perform localization prediction in a VANET discussing its potential application scenarios. Then, the paper elaborates on the problem of predicting a vehicle's future location, describing proposed approaches for localization, target

tracking and time series prediction methods highlighting their advantages and disadvantages through an analytical discussion. Furthermore, the paper presents a set of experiments showing the results of such techniques when applied to a realistic VANET scenario. Finally, the paper discusses the applicability, pros, and cons of each technique and some particularly interesting future research directions.

Unmanned aerial vehicles (UAVs) are envisioned as aerial communication platform to provide telecommunication services in a timely and economical manner due to their high maneuverability and low cost. The development of such UAV communication systems requires accurate models to characterize propagation in air-to-ground and air-to-air channels with possible non-stationarity and temporal variations. These channels have strong impact on the real-time capabilities and coverage performance of the UAV communications operating in different environments and at different altitudes. Therefore, empirical and analytical channel modeling is important to evaluate the reliability of UAV communications. In this context, the paper titled "A Survey of Channel Modeling for UAV Communications" by Aziz Altaf Khuwaja, Yunfei Chen, Nan Zhao, Mohammed-Slim Alouini, and Paul Dobbins presents a survey to overview the recent progress in UAV channel measurement methods for low altitude platforms. Moreover, the paper describes the channel modeling approaches for UAV channels and provides future research challenges for UAV measurement methods and channel modeling techniques.

Wireless sensor and actuator networks (WSANs) are a natural extension of wireless sensor networks (WSNs) and integrate a small number of resource-rich sinks and actuators into their topology. The latter are able to change the state of the environment with their actions, hence closing the control loop on the underlying monitoring system. This allows for greater potential for computations in the network. While today's WSANs are limited in their actuation, reasoning, and sensing abilities, the WSANs of the future will likely have even more heterogeneous nodes and be deployed on a massive scale. In order to achieve this, several challenges must be tackled and resolved. Computational Intelligence (CI) techniques encompass a wide range of intelligent techniques that are able to process imprecise information and see approximate yet good-enough solutions to these problems. In this context, the paper entitled "A Review of Computational Intelligence Techniques in Wireless Sensor and Actuator Networks" by Nicolas Primeau, Rafael Falcon, Rami Abielmona, and Emil Petriu presents a survey of CI techniques within this emerging field. First, the paper starts by justifying the need for such a survey by comparing it with other relevant surveys. The problem is then contextualized within the CI and WSAN worlds with the problems plaguing WSANs specifically elaborated upon. Subsequently, the surveyed works are categorized along the five major axes corresponding to the WSAN problem they tackle. Finally, the paper concludes by shedding some light on future trends and opportunities under each problem category.

Although significant advancements have been made in underwater wireless sensor networks (UWSNs) to explore the ocean realm, currently, most of the networks are hardware-based and application-oriented with inflexible closed-form architectures which are difficult to reconfigure, reprogram and evolve. They also lack the capability of network resource sharing, and are far from serviced-oriented networks. To further propel the development of UWSNs, the emerging software-defined technologies are envisioned as driving forces to reprogram and softwarize the network resources in order to improve resource utilization efficiency and facilitate network management. Therefore, more active research on software-defined UWSNs are required as they are critical building blocks to transform conventional UWSNs towards programmable networks with high network flexibility and adaptability to satisfy a wide range of underwater application requirements. In this context, the paper entitled "Software-Defined Architecture and Technologies for Underwater Wireless Sensor Networks: A Survey" by Hanjiang Luo, Kaishun Wu, Rukhsana Ruby, Yongquan Liang, Zhongwen Guo, and Lionel M. Ni presents a comprehensive review on underwater software-defined architectures and technologies, and hope to inspire and promote more research activities in this area. The programmable software-defined technologies are surveyed at all layers of UWSNs, which include SDR, UCR, SDM, NFV, IoUTs and Sensor-cloud, towards the realization of a software-based, programmable, user-customizable and service-oriented next-generation UWSNs. Furthermore, the paper summarizes these complementary technologies and highlights key issues for the directions of future research.

Ambient backscatter is a breakthrough communication technology which enables two IoT devices to communicate without using battery or any other energy sources. Because ambient backscatter avoids the maintenance-heavy batteries and dedicated power infrastructure, it provides a bunch of new IoT applications and enables ubiquitous communications (with no restrictions except the existence of ambient RF signals) among pervasive devices which are cheap and have near-zero maintenance. In 2016, MIT Technology Review listed ambient backscatter communication as one of the 10 breakthrough technologies, and this technology is expected to bring us closer to the IoT era. In this context, the paper titled "Ambient Backscatter Communications: A Contemporary Survey" by Nguyen Van Huynh, Dinh Thai Hoang, Xiao Lu, Dusit Niyato, Ping Wang, and Dong In Kim, provides a comprehensive overview of the state-of-the-art research and technological developments on the architectures, protocols, and applications of emerging ambient backscatter communications systems (ABCSs). In particular, this paper first provides a fundamental background for general readers to understand basic concepts, operation methods and mechanisms, and applications of ABCSs. This paper then summarizes advanced design techniques related to architectures, hardware designs, network protocols, standards, and solutions of the ABCSs. Finally, challenges, open issues, and potential future research directions are highlighted and discussed.

IV. IoT AND M2M

Internet of Things (IoT) is spreading in almost every industry, business, and aspects of our lives where an enormous

amount of sensing devices participates in generating big or streaming data. Applying analytic algorithms and techniques over such data to discover new information, predict future insights, and make control decisions is a crucial process that makes IoT a worthy paradigm for businesses and a quality-of-life improving technology. In recent years, deep learning (DL) techniques have drawn the attention of researchers in many areas of IoT to get best out of IoT data. In this context, the paper titled "Deep Learning for IoT Big Data and Streaming Analytics: A Survey" by Mehdi Mohammadi, Ala Al-Fuqaha, Sameh Sorour, and Mohsen Guizani presents a tutorial and survey. First, the authors review the characteristics of IoT data and its challenges for DL methods. In specific, they highlight IoT fast and streaming data as well as IoT big data as the two main categories of IoT data generation and their requirements for analytics. The paper then presents several main architectures of DL that are used in the context of IoT applications followed by several open source frameworks for the development of DL techniques and algorithms. Reviewing different applications in various sectors of IoT that have utilized DL is another part of this study in which the authors identify five foundational services along with twelve application domains. Then, the new paradigm of implementing DL on IoT devices is surveyed and several approaches to achieve it are introduced. Reviewing DL based on fog and cloud infrastructures to support IoT applications is another part of this survey. Finally, the paper also presents the challenges and future research direction in the path of DL for IoT applications.

The Internet of Things (IoT) has recently advanced from an experimental technology to what will become the backbone of future customer value for both product and service sector businesses. This underscores the cardinal role of IoT on the journey towards the fifth generation (5G) of wireless communication systems. IoT technologies augmented with intelligent and big data analytics are expected to rapidly change the landscape of myriads of application domains ranging from health care to smart cities and industrial automations. The emergence of Multi-Access Edge Computing (MEC) technology aims at extending cloud computing capabilities to the edge of the radio access network, hence providing real-time, high-bandwidth, low-latency access to radio network resources. IoT is identified as a key use case of MEC, given MEC's ability to provide cloud platform and gateway services at the network edge. MEC will inspire the development of myriads of applications and services with demand for ultra-low latency and high Quality of Service (QoS) due to its dense geographical distribution and wide support for mobility. MEC is therefore an important enabler of IoT applications and services which require real-time operations. In this paper entitled "Survey on Multi-Access Edge Computing for Internet of Things Realization," Pawani Porambage, Jude Okwuibe, Madhusanka Liyanage, Mika Ylianttila, and Tarik Taleb provide a holistic overview on the exploitation of MEC technology for the realization of IoT applications and their synergies. We further discuss the technical aspects of enabling MEC in IoT and provide some insight into various other integration technologies therein.

The Smart Grid is one of the most compelling Cyber Physical Systems that has been developed in recent years. Its capabilities to improve the energy usage integrate Renewable Energy Sources or create prosumers show promise in terms of offering more energy and democratizing access to electricity. However, there are multiple technical challenges that must be solved in order to have a full-fledged system like this that makes possible covering all these features. One of them is guaranteeing interoperability and interconnectivity at the data level among the different devices and appliances present in a deployment based Smart Grid, so that they will be able to interchange information seamlessly. In this context, the paper titled "Middleware Architectures for the Smart Grid: A Survey on the State-of-the-Art, Taxonomy and Main Open Issues" authored by Jesús Rodríguez-Molina and Daniel Kammen presents a survey containing the most prominent middleware architectures for the Smart Grid, along with an assessment of their advantages and disadvantages. In addition to the several key features (service availability, computational capabilities, message coupling and middleware distribution), conclusions and open issues have also been included in the paper.

V. 5G AND SDN

The constant evolution of mobile networks allows the creation of new use cases and applications. With the upcoming fifth generation of mobile networks (5G), the Tactile Internet and the ultra-reliable and low-latency communication infrastructure which it will offer, the realization of haptic communication over mobile networks will be possible. This type of immersive communication requires the joint consideration of mobile network infrastructure, bilateral teleoperation control and haptic data processing as well as determining the Key Performance Indicators (KPIs). In this way, 5G networks will be able to provide the appropriate Quality of Service (QoS) for an optimum Quality of Experience (QoE) for the user. In this context, the paper titled "Towards Haptic Communications over the 5G Tactile Internet" by Konstantinos Antonakoglou, Xiao Xu, Eckehard Steinbach, Toktam Mahmoodi, and Mischa Dohler presents a survey which reviews all the aspects of the multidisciplinary topic of haptic communication. Furthermore, it presents the requirements and KPIs of Tactile Internet use cases. Finally, the survey highlights the main challenges and also discusses the potential of current technologies and methodologies.

The increasing demand of wireless and mobile data set the objective of 5G wireless networks. The promising 1000x throughput, low latency network access, and more energy efficient implementation require exploration of higher frequencies beyond 6 GHz. The millimeter wave frequency band provides larger bands but suffers from the higher signal power loss through vapors and gases absorption. This path loss can be compensated with the directional beamforming provided by the massive MIMO implementations. The traditional MIMO architecture that requires one transceiver per antenna becomes infeasible with the massive MIMO implementation due to the cost, space, and power consumption. Hybrid beamforming divides the beamforming into digital and RF domains such that

all or subset of antennas are connected to one transceiver (RF chain). It renders the trade-off between flexibility and the cost for application specific implementation. In this context, the paper entitled "A Survey on Hybrid Beamforming Techniques in 5G: Architecture and System Model Perspectives" by Irfan Ahmed, Hedi Khammari, Adnan Shahid, Ahmed Musa, Kwang Soon Kim, Eli De Poorter, and Ingrid Moerman provides a comprehensive review of the hybrid beamforming architectures; signal processing techniques with all possible combinations of antennas; resource management including resource block allocation, beam management, and medium access management; finally, beamforming in HetNet is reviewed as an application aspect of the hybrid beamforming. We identify the limitations of the current work and the possible future research directions in each of the aforementioned areas of hybrid beamforming.

The focus of the fifth generation (5G) wireless communication is to provide seamless communication for machines and user devices building the Internet-of-Things (IoT). In addition to large capacity, massive connection density, and ultra-high reliability, 5G networks also need to support latency critical applications, such as automated manufacturing, smart transportation, telemedicine and telesurgery, real-time control and robotics, and smart grid. In particular, several emerging technologies including wearable devices and virtual/augmented reality are shaping the demeanor of human end users, and they have special requirements for user satisfaction. Some of these use cases have a strict latency requirement on the order of 1 ms. Current fourth generation networks are not capable of fulfilling all the technical requirements for achieving such low latency with these services. In this context, the paper titled "A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions" by Imtiaz Parvez, Ali Rahmati, Ismail Guvenc, Arif I Sarwat, and Huaiyu Dai presents a survey on low latency wireless systems for 5G networks and beyond. The emerging technologies for achieving low latency are summarized covering three domains: (1) radio access network, (2) core network, and (3) caching. Following this, a general overview of 5G cellular network composed of software defined networks, network function virtualization, caching, and mobile edge computing is presented, which can support latency critical services along with massive connectivity and high throughput. The authors also overview recent results from the field tests, trials, and experiments, followed by a discussion of open issues, challenges, and future research directions.

In recent years, many countries in Asia, Europe and North America have developed high-speed railways (HSR) to connect major cities. HSR has become an important way of transportation. With the widespread development of HSR and the rising speed of trains, timely and reliable wireless transmission of train control signals and passengers' mobile data become more and more important. To this end, this survey paper entitled "Development Trend of Mobile Communication Systems for Railways" by Rui Chen, Wen-Xuan Long, Guoqiang Mao, and Changle Li provides an overview of the current mobile communication systems for railways and analyzes its future development trends and technical challenges. It is envisaged that the future development of mobile communication systems for railways be divided into three stages. In the first stage, LTE-R will be gradually deployed, working with GSM-R. GSM-R will be responsible for the transmission of security data related to train dispatching and control, while LTE-R will be responsible for transmission of other non-security data. In the second stage, LTE-R will completely replace GSM-R. Meanwhile, 5G-R will be gradually phased in to provide emergency communication among trains, as well as Internet access inside carriages. In the third stage, a complete 5G-based heterogeneous mobile communication systems for railways will be deployed, which can meet the communication requirements of various railway scenarios. However, the current GSM-R system may also likely evolve directly to 5G-R, depending on the maturity of 5G networks and other commercial and government policy factors. It is expected that future mobile communication systems for railways, including T2I, T2T, intra-carriage and intra-station communications, will be finally deployed with 5G-R based heterogeneous networks.

The revolutionary technologies employed in the fifth generation (5G) wireless communication systems, including massive multiple-input multiple-output (MIMO), vehicle-to-vehicle (V2V), high-speed train (HST), and millimeter wave (mmWave) communications, introduce new propagation properties. These in turn demand higher requirements for 5G channel modeling, e.g., smooth time evolution, spatial consistency, frequency dependency, etc. Wireless propagation channels at various frequency bands, e.g., 450 MHz to 100 GHz, and in diverse propagation scenarios should be sufficiently measured and parameterized. The existing channel models covering various 5G scenarios, especially standard 5G channel models, should be thoroughly investigated. Besides, researches on beyond 5G (B5G) channel modeling, e.g., terahertz (THz) channel modeling, visible light communication (VLC) channel modeling, and channel modeling based on big data theories are still at their very early stages. In this context, the paper titled "A Survey of 5G Channel Measurements and Models" by Cheng-Xiang Wang, Ji Bian, Jian Sun, Wensheng Zhang, and Minggao Zhang presents a tutorial and survey. First, the paper starts by stating the requirements of the 5G channel modeling. Then, the paper extensively elaborates recent channel measurements and models, including scenario-specific 5G channel models and general 5G channel models covering more scenarios. Finally, the paper discusses a range of future research directions for 5G and B5G channel measurements and models.

In order to address the energy shortage of miniature communication devices in the future 5G and IoT era, engineers initially seek additional energy from renewable source. However, harvesting renewable energy heavily depends on the ambient environment, which results in its uncontrollability, unpredictability and unreliability. Therefore, we may opt for radio-frequency (RF) signal based wireless energy transfer (WET) as an alternative technique for supplying controllable and reliable energy to communication devices. However, operating in the same spectral band may result in contradiction between RF based WET and conventional wireless information transfer (WIT). Understanding the inherent relationship between WET and WIT and efficiently coordinating them in the RF spectral band results in the

promising research topic of Integrated Data and Energy Communication Networks (IDENs). In this context, the treatise titled "Integrated Data and Energy Communication Network: A Comprehensive Survey" by Jie Hu, Kun Yang, Guangjun Wen, and Lajos Hanzo provides the first detailed survey on the key techniques of IDENs from its bottom to top layers, including the information theoretical foundations of integrated WET and WIT in the same spectrum, the hardware implementation of the WET chain, the transceiver design of the physical layer, resource allocation and protocol design for MAC and networking techniques for connecting heterogeneous users in IDENs. This treatise aims for providing insights into the emerging topic of IDENs, which may be used as guidance for both engineers and researchers, who are willing to contribute to making this promising vision a reality.

Recent years have seen unprecedented growth in the literature related to the introduction of Software Defined Networking (SDN) paradigm in mobile communications. The publications cover broad range of topics, from overall architecture to design of specific network services within the new context. However, the big question is to know how far we are from practical realization of the concept. While 5G standardization is already in the final phase, it is more plausible that we could only see point solutions incorporating SDN idea in a 5G mobile network instead of a fully programmable network. In this context, the paper titled "Will SDN Be Part of 5G?" by Zainab Zaidi, Vasilis Friderikos, Zarrar Yousaf, Simon Fletcher, Mischa Dohler, and Hamid Aghvami identifies six major obstacles in realization of a SDN-based mobile network, i.e., fronthaul, latency of GPP (General Purpose Platforms), backward compatibility, disruptive deployment, SDN specific security vulnerabilities, and clear and compelling business case. The paper summarizes the work under each theme and highlights the gaps. 5G NR standard tried to address the backward compatibility issue through the non-standalone scenario, advocating an evolutionary approach of network deployment. Fronthaul is still an open issue especially for the areas where optical fiber is not available and too expensive to install. Latency of GPPs is improved over time but the best reported implementation is still not suitable for 5G data speeds. The work under security area is much mature and many new issues have been identified and respective solutions are designed.

Software defined networking (SDN) has recently emerged as an important networking paradigm that is increasingly adopted in operational networks. SDN is fundamentally different from the conventional (legacy) Internet Protocol (IP) networking in that SDN decouples the control plane from the data plane and controls the network operations through a central SDN controller. This central SDN control together with the separation of data plane and control plane as well as emerging well-defined application programming interfaces for SDN networks make SDN very attractive for network operators. However, many organizations are hesitant to completely switch over to SDN due to a variety of reasons, such as budget constraints for new SDN equipment. Hybrid SDN networks can ease the transition from conventional IP networking to SDN network operation by deploying a limited number of SDN switches among the legacy networking equipment. Hybrid SDN networks strive to reap some of the benefits of SDN network operation, e.g., simplified flexible network control, with only a limited investment. This survey paper entitled "Hybrid SDN Networks: A Survey of Existing Approaches" by Rashid Amin, Martin Reisslein, and Nadir Shah comprehensively covers the existing literature on hybrid SDN networks. The main survey sections cover hybrid SDN network deployment strategies, i.e., where to place the few SDN switches, controllers for hybrid SDN networks, protocols for hybrid SDN network management, traffic engineering mechanisms for hybrid SDN networks, as well as testing, verification, and security mechanisms for hybrid SDN networks. Based on the outcomes as well as the gaps and limitations of the existing research studies, this survey derives guidelines for future research on hybrid SDN networks.

VI. Network Virtualization

Network Functions Virtualization (NFV) is a revolutionary technology that has become a key component for the realization of 5G networks. NFV is expected to yield significant benefits that can be fully achieved if its main open issues are addressed. The NFV Orchestrator (NFVO) and its dependability implications represent one of the most important to be considered. The NFVO maintains a global view of the network state, manages available resources and it can be used to enhance the efficiency on providing service dependability. On the other hand, since the NFVO is logically-centralized, it may affect the entire network as a result of a misoperation, and its temporal absence can make the network very vulnerable. Dependability is fundamental for making NFV a reality; however, the NFVO is a potential dependability bottleneck if it is not well planned and designed. Based on the need of having a structured vision that allows identifying the current status, needs and challenges in this regard, the paper titled "Dependability of the NFV Orchestrator: State of the Art and Research Challenges" by Andres J. Gonzalez, Gianfranco Nencioni, Andrzej Kamisinski, Bjarne E. Helvik, and Poul E. Heegaard presents a tutorial on the dependability challenges of the NFVO, by providing background information, reviews on the available literature and the current architectural solutions, in order to identify relevant design and research problems that must be addressed, and in this way provide a structured insight into the required future research.

Network Functions Virtualization (NFV) is widely recognized as a novel approach to significantly reducing hardware cost and improving operational efficiency. The clear separation between modular software based network functions and the standard server platforms makes the management of orchestration of network functions and services much more adaptive, scalable, and flexible. However, in the virtualization environment, the attack surface becomes very unclear and the defense line turns to be extremely blurred, making security as one of the vital concerns in the development and deployment of NFV. In this context, the paper titled "NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures" by Montida Pattaranantakul, Ruan He,

Qipeng Song, Zonghua Zhang, and Ahmed Meddahi presents a comprehensive survey to holistically address the security issues in NFV. First, layer-specific threat taxonomy is established based on the threat analysis of five well-defined NFV use cases. Then the security mechanisms deployed in traditional networks and NFV environments are comparatively studied, together with an analysis on the existing security countermeasures, resulting in a set of security requirements and recommendations for designing secure NFV based services. The open issues and future research topics in this emerging domain are finally summarized.

VII. Network Security

In recent years cyber-attacks have been on the rise. Targeted attacks and Advanced Persistent Threats (APTs) pose some of the biggest challenges of the security community and some of the most significant threats for organizations. In this new era of cybercrime, attackers are highly motivated, organized and have both the time and resources necessary to achieve their goals. Therefore, the technologies that have been used in the past for both detection and forensic analysis must evolve and adapt to this new threat landscape. In this context, the paper titled "From Intrusion Detection to Attacker Attribution: A Comprehensive Survey of Unsupervised Methods" by Antonia Nikiti, Alexis Myelomas, Paul D. You, and Vasilios Kato presents a survey. In specific, the paper first presents a comprehensive overview of unsupervised and hybrid methods for intrusion detection, as well as on feature engineering techniques and publicly available datasets. Furthermore, the paper presents a discussion on the evolution of the current detection techniques towards correlation and attribution. Finally, the paper discusses how the current IDS attack classes need to be extended in order to properly reflect the current threat landscape.

The domain name system (DNS), which was initially created to facilitate the translation of human readable domain names to IP addresses, has turned into a fundamental infrastructure in sustaining the operations of various Internet services (e.g., email and Web). Despite its ubiquitous role, DNS has been abused/ misused to perform large-scale attacks that affected millions of Internet users. To detect and prevent threats associated to DNS, researchers introduced passive DNS replication and analysis as an effective alternative approach for analyzing live DNS traffic. As a result, researchers have implemented several systems that may vary in terms of their objective and scope, threat detection approach, data collection and enrichment, evaluation methods and detection outcomes. In this context, the paper titled "Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Literature Survey" by Sadegh Torabi, Amine Boukhtouta, Chadi Assi, and Mourad Debbabi presents a survey, where the paper overviews the implemented systems that utilize passive DNS traffic for the purpose of detecting malicious behaviors on the Internet. In addition to the in-depth comparative discussion of the implemented systems and their key strengths/weaknesses, the survey concludes with presenting an implemented system prototype, which leverage a big data analytics framework to present a feasible approach for near-real time threat detection using passive DNS traffic in future research.

The primary technologies such as blockchain and consensus protocols that make the Bitcoin a vast success will now also being envisioned in various next-generation applications. It includes smart trading in smart grids, Internet of Things (IoT), vehicular networks, health-care data management, and smart cities, to name a few. As the length of popularity largely depends on the amount of security built on the system which surpasses all its other benefits. The exponential growth in the market value of bitcoins motivate adversaries to exploit weaknesses for profit, and researchers to discover new vulnerabilities in the system, propose countermeasures, and predict upcoming trends. In this context, the paper titled "A Survey on Security and Privacy Issues of Bitcoin" by Mauro Conti, Sandeep, Chhagan Lal, and Sushmita Ruj presents a survey, which includes the state-of-the-art on security threats and solutions for Bitcoin and its underlying technologies such as BlockChain, consensus algorithms, and peer-to-peer networks. The paper reviews all the security threats till date starting from packet sniffing to the double spending. Moreover, the survey includes the privacy and anonymity related challenges in Bitcoin and similar cryptocurrencies. Finally, the authors summarize the lessons learned, and present the possible future problems and research directions concerning the security and privacy issues in Bitcoin.

Modern IoT technologies are being deployed in a wide range of application domains including large-scale critical infrastructures like smart grids, industrial control, intelligent transportation, health monitoring and control systems, as well as in non-critical environments like smart homes. Unfortunately, the provision of such systems with remote control and connectivity capabilities creates new attack opportunities, for remote or nearby hackers. In the case of IoT devices being part of critical systems and services, the attack paths are usually easy to identify, since they will directly affect the interconnected critical system. On the other hand, in the case of attacks against IoT devices that are not directly connected to critical systems, their underlying security risks are usually underestimated. In this context, the paper titled "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," by Ioannis Stellios, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez, presents a survey of recent IoT-enabled attacks. First the paper presents a generic risk-based methodology that models IoT-enabled attacks. Then, the paper applies this methodology to assess, in a high level, various real or proof-of-concept IoT-enabled attacks, which have affected various application domains. Finally, based on the analysis of these attacks, the paper presents a taxonomy of existing security controls for mitigating the relevant risks, as well as of the current research gaps in IoT security.

The adoption of the Internet of Things (IoT) based networks is inevitable, with similar systems already seen for monitoring and control of industrial systems (energy, water etc.). It is essential that correct security solutions be found before wide-scale adoption of insecure processes which widely assist

modern society. As interest in the IoT grows, its application will involve more data sensitive projects. As such, ensuring its security is a priority. With preventative measures difficult to implement due to inherent architectural constraints, solutions must turn to second line methods of defense. In this context, the paper titled "A Critical Review of Practices and Challenges in Intrusion Detection for IoT: Towards Universal and Resilient Systems" by Elhadj Benkhelifa, Thomas Welsh, and Walaa Hamouda, examines Intrusion Detection System (IDS) for IoT as one such defense and determines that despite the variety of existing systems available; none are able to defend against all types of attacks (from the physical layer up) due to their architectural implementation. Therefore, the paper discusses the case that these methods are outdated whilst not holistically covering the whole IoT model. The papers concludes that in order to comprehensively secure IoT based networks built of heterogeneous device types, a new approach must be taken. This involves the application of more physical hardware, using network probes to collect data and securely transport it to a remote server (likely cloud-based) so as to perform detection types as resource intensive as required.

The requirement for much higher data rates and lower latencies in 5G cellular communications calls for novel approaches, such as device-to-device (D2D) communication which does not require data packets to flow through a base station. This naturally leads to the adoption of a multi-hop architecture which allows intermediate nodes to relay packets from an originating node to the destination. Multi-hop Cellular Networks (MCNs) are expected to play an important role in 5G cellular communications. However, MCNs are vulnerable to attacks on their routing protocols, such as eavesdropping, man-in-the-middle and denial of service. Countermeasures against such attacks are needed. In this context, the paper titled "A Survey of Secure Routing Protocols in Multi-Hop Cellular Networks" by Gholamreza Ramezan, Cyril Leung, and Z. Jane Wang is timely. The paper includes an overview of the main security objectives for MCN routing protocols which are classified as D2D or Internet-of-Things (IoT) oriented. Common approaches for securing routing protocols are discussed. The paper summarizes a number of routing protocols in the context of MCN and Internet-of-Things (IoT) networks as well as Software-Defined Networking (SDN) architectures and provides a useful guide for researchers to navigate the referenced literature. Finally, the paper describes several open problems deserving of further investigation.

Software defined networking implements the network control plane in an external entity, rather than in each individual device as in conventional networks. The external entity has complete knowledge of the topology of a network under its control, and programs the forwarding tables of each individual device in the network. In contrast, conventional networks have the control plane, i.e., network control functions such as routing protocol implementations, running inside each network device to learn forwarding tables in a distributed fashion. The paper titled "Comparative Analysis of Control Plane Security of SDN and Conventional Networks" by AbdelRahman Abdou, Paul C. van Oorschot, and Tao Wan provides a survey, complemented by a framework allowing for an objective security comparison between SDNs and conventional networks. This enables analysis of how network functions are delivered by the control planes of SDN and conventional networks, and to compare security threats and mitigations. The framework consists of five network properties and two threat models. Such properties are critical for successful operation of networks in practice, as they enable networks to function efficiently, scale, and ensure the networks' high availability. Despite the architectural difference between SDNs and conventional networks, comparable security exposures were found in the control plane security as both network paradigms provide similar network properties and are analyzed under the same threat models. However, defenses vary; SDN cannot depend on edge based filtering to protect its control plane, while this is arguably the primary defense in conventional networks.

VIII. Network and Service Management and Green Communications

Big data applications in data centers often involve scheduling of data-parallel jobs, including queries and Web services. Optimizations for job scheduling and resource allocation in data center networks (DCNs) have gained pervasive attention in both industry and academia. To deploy an efficient cluster framework, many previous efforts have been paid to design algorithms and implement approaches with different objectives to meet various job demands, including the desirable properties of fault tolerance, work conservation, consistency control, scalability and computation efficiency. As cluster frameworks can be classified into different categories according to scheduling objective, controller management and prior knowledge requirements, a great number of solutions have been elaborated for conquering crucial challenges in data centers, such as providing low latency and minimizing job completion time. By understanding these inherent patterns and situation in-depth, developers can upgrade existing frameworks using state-of-the-art technologies. In this context, the paper titled "Cluster Frameworks for Efficient Scheduling and Resource Allocation in Data Center Networks: A Survey" by Kun Wang, Qihua Zhou, Song Guo, and Jiangtao Luo presents a survey, where the paper provides a solid starting ground and comprehensive overview of cluster frameworks in DCNs. Moreover, the survey points out a number of promising areas deserved for further researches and sheds light on forthcoming audience in this area.

Community Networks provide the infrastructure with the concept of defending the Internet access right of every human being. These community networks have evolved over the years and have been diversified according to their offered services and underlying technologies. They also face lots of challenges but, sustainability is one such challenge that is common across all these diverse variations of community networks. In this context, the paper titled "Community Networks and Sustainability: A Survey of Perceptions, Practices, and Proposed Solutions" by Panagiota Micholia, Merkourios Karaliopoulos, Iordanis Koutsopoulos, Leandro Navaroo, Roger Baig,

Dimitris Boucas, Maria Michalis, and Panayiotis Antoniadis presents a survey of how sustainability is perceived in different research communities and how the managers of these community networks try to achieve the goals of sustainability. The paper also surveys the extent of individual, business and community needs fulfilment from the community networks. Moreover, the paper also surveys the sustainability of community networks with the context of politics, culture and economy. The survey also highlights a number of key research directions that pave the path of the future researches in this area.

IX. Internet Technologies

Location information for events, assets, and individuals enables a wide range of applications across different verticals, such as consumer, networking, industrial, health care, public safety, and emergency response use cases. These applications spanning from customer-centric location-based services, to resource allocation in wireless networks, to emergency call positioning have diverse location accuracy requirements. To fully exploit the potential of location awareness and enable new advanced location-oriented services, localization systems should leverage on modern sensor-rich mobile devices and the ubiquity of wireless communication networks. Moreover, traditional localization algorithms need to be combined with complementary technologies including accurate vertical position, i.e., height estimation, reliable user mobility classification, and efficient indoor mapping solutions. In this context, the paper titled "A Survey of Enabling Technologies for Network Localization, Tracking, and Navigation" by Christos Laoudias, Adriano Moreira, Sunwoo Kim, Sangwoo Lee, Lauri Wirola, and Carlo Fischione starts with fundamental localization techniques, overviews the most typical architectures, and presents the 4G LTE positioning architecture as a case study. Then, the paper surveys localization systems in cellular networks including recent results on 5G, WLAN-based systems, and range-free schemes for WSN. Subsequently, fusion techniques for combining multi-source sensory data are described, followed by techniques for delivering reliable vertical information towards accurate 3D location, which are applicable in cellular and WLAN systems. Then, the paper discusses mobility state estimation in cellular networks and recent advances in mapping physical indoor spaces for supporting tracking and navigation applications. Finally, the paper discusses architectural considerations related to service availability, system scalability, security, and privacy, followed by an outline of future research directions, and the authors' outlook on the technology roadmap.

The throughputs supported by network interfaces in data centers are in the range of 40Gbps and higher. However, the packet processing speeds on server-class network hosts are limited due to the overheads imposed by the architecture of the network stack. Nevertheless, there is a great need for a speedup in the forwarding engine, which is the most important part of a high-speed router. As a result, numerous software-based and hardware-based solutions have appeared recently with a goal of increasing packet processing speeds. An operating system's networking stack is conceived for general purpose communications rather than high-speed networking applications. In this context, the paper titled "Fast Packet Processing: A Survey" by Danilo Ceroviæ, Valentin Del Piccolo, Ahmed Amamou, Kamel Haddadou, and Guy Pujolle presents a survey. First, the paper provides an overview of the existing solutions that are based on software and of the solutions that are based on hardware like GPUs and FPGAs. Moreover, the survey provides a comparative analysis of these solutions and it discusses their integration possibilities in virtualized environments. Finally, the paper discusses the latest approaches and future directions in the packet processing field.

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, ONF Research Associate
Editor-in-Chief
IEEE Communications Surveys and Tutorials
Distinguished Professor, National Chiao Tung University
Director, Network Benchmarking Lab
Web: www.cs.nctu.edu.tw/∼ydlin