Editorial: First Quarter 2020 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS

I WELCOME you to the first issue of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS in 2020. This issue includes 25 papers covering different aspects of communication networks. In particular, these articles survey and tutor various issues in "Wireless and Cellular Communications," "5G Communications," "Vehicular and Sensor Communications," "IoT and M2M," "SDN and NFV," "Internet Technologies," and "Network Security." A brief account for each of these papers is given below.

I. WIRELESS AND CELLULAR COMMUNICATIONS

Traditionally, the unlicensed spectrum has been widely dominated by Wi-Fi (IEEE 802.11-based) technologies. Recently, cellular (3GPP-based) technologies have expanded their operation to the unlicensed spectrum as well. Such extension started with LTE-based 4G systems and continues with a native feature in NR-based 5G systems, through the so-called NR-based access to Unlicensed spectrum (NR-U). NR-U will support, among others, standalone operation in the millimeter-wave (mmWave) spectrum region, by adhering to Listen-Before-Talk (LBT) requirements for accessing the channel. In the case of beam-based transmissions, the NR-U coexistence framework is significantly different to that of LTE in unlicensed spectrum due to the use of directional antennas, which enhances the spatial reuse but also complicates the interference management. Consequently, some major design principles need to be revisited for beam-based NR-U. In this context, the paper titled "New Radio Beam-based Access to Unlicensed Spectrum: Design Challenges and Solutions" by Sandra Lagen, Lorenza Giupponi, Sanjay Goyal, Natale Patriciello, Biljana Bojovic, Alpaslan Demir, and Mihaela Beluri presents a tutorial and overview of beam-based NR-U. First, it reviews the standardization landscape of NR-U. Then, it elaborates on the major design principles for NR-U, by considering the beam-based transmissions and the worldwide regulatory requirements. Different problems and the potential solutions related to channel access procedures, frame structure, initial access procedures, retransmission procedures, and scheduling schemes are discussed. Finally, a simulation evaluation of different LBT-based channel access procedures for NR-U/Wi-Fi indoor mmWave coexistence scenarios is provided and future perspectives are highlighted.

Cloud systems are very important for current and future technologies to allow user devices to execute applications that necessitate more resources than what can be provided locally. However, in conventional cloud service, the cloud servers are located far away from the users, leading to a prohibitive access delay that makes the execution of real-time applications impossible in this service model. To circumvent this problem, mobile edge cloud systems were created where the servers are located near the user. This edge service model has very complex problems to be solved to configure its system, such as deciding resource allocation or where to execute the applications of each user. These problems are too complex for conventional solutions. For this, machine learning algorithms are applied due to their aptitude in analyzing big amounts of data and finding near-optimal solutions in quick execution times. In this context, the paper titled "Machine Learning Meets Computation and Communication Control in Evolving Edge and Cloud: Challenges and Future Perspective" by Tiago Koketsu Rodrigues, Katsuya Suto, Hiroki Nishiyama, Jiajia Liu, and Nei Kato present a survey, where the paper overviews existing solutions that utilize learning mechanisms to configure mobile edge computing systems. Besides that, the survey offers categories of mobile edge computing problems, promising machine learning algorithms and open issues in this research area to guide future research in the machine learning-based mobile edge computing field.

The current Internet architecture is TCP/IP based in which communication is based on the locations of the devices. On the other hand, Named Data Networks (NDN) is a new proposed future Internet architecture, in which content name is used as a driving parameter of communication instead of location. NDN is suitable especially in wireless environment due to built-in caching and mobility support. The packet forwarding mechanism in NDN is quite simple and uses two types of packets named, Interest and Data. Moreover, the packet forwarding mechanism is broadcast based and many approaches are proposed to provide efficient forwarding. In this context, the paper titled "Forwarding Strategies in NDN-Based Wireless Networks: A Survey" by Asadullah Tariq, Rana Asif Rehman, and Byung-Seo Kim presents a detailed survey regarding various packet forwarding mechanisms proposed for NDN-based wireless networks such as MANETs, VANETs, WSNs, and WMNs. Firstly, the paper starts by providing an overview of NDN, its architecture as well as differences between NDN and TCP/IP. Then, the paper elaborates in detail various kinds of forwarding strategies in each of wireless networks, i.e.,

Digital Object Identifier 10.1109/COMST.2020.2976449

MANETs, VANETs, WSNs, and WMNs. Finally, the paper provides the key issues and open research challenges of forwarding in NDN based wireless networks which can be tackled in future research.

Facilitated by the substantial advances in wireless communications supported by sophisticated signal processing and nano-electronics solutions, affordable 'always-on' connectivity has become a commercial reality. As these techniques have developed in unison over the past four decades, four generations of global wireless standards have been developed and ratified, spanning from 2G to 5G. In the 2G systems conventional convolution and block codes were used, while in the 3G systems both convolutional and turbo codes found application. However, turbo codes were patented, hence its users had to pay royalty, which has led to the renaissance of LDPC codes during the 4G era of the 2000s. Since their inception in 2008, polar codes have been shown to offer near-capacity error correction performance across a wide range of block lengths and coding rates. Hence, they have been selected to provide error protection in the control channels of the Third Generation Partnership Project's (3GPP) New Radio (NR) standard. Against this background, the paper entitled as "The Development, Operation and Performance of the 5G Polar Codes" by Zeynep B. Kaykac Egilmez, Luping Xiang, Robert G. Maunder, and Lajos Hanzo describes the operation of the 3GPP NR polar codes specified in the 3GPP standard TS 38.212. They also elaborate on the associated schemes, such as the code block segmentation, Cyclic Redundancy Check (CRC) attachment, CRC scrambling, CRC interleaving, frozen and parity check bit insertion, sub-block interleaving, bit selection, channel interleaving and code block concatenation. The configuration of these components is different for the uplink, as well as for the broadcast and downlink control channels. However, the lack of visualizations and diagrammatic explanations in the TS 38.212 standard limits its reader-appeal. This motivates the conception of this paper, which provides detailed tutorials on the operation and motivation of the components of the 3GPP NR polar codes, as well as surveys of the 3GPP discussions that led to their specification. Furthermore, the authors comprehensively characterize the error correction and error detection performance of the 3GPP NR polar codes in the uplink, as well as in the broadcast and downlink control channels.

The paper mentioned in the paragraph above provides the entire history and operation of the 3GPP NR polar codes and sets the background for further in-depth discussions on polar codes and quantum-domain polar codes. The family of quantum-domain polar codes are capable of mitigating the deleterious effects of quantum decoherence in quantum circuits. The quantum polar codes may be designed by exploiting the so-called classical-quantum isomorphism, which is a scientific way of expressing that under certain conditions there is a quantum-domain counterpart for a classical-domain polar code. To elaborate a little further in conceptually simple plausible terms, in the quantum-domain classical bits can be mapped to the spin or charge of an electron. However, the above-mentioned decoherence may inflict not only bit-flips, but also phase-flips on the quantum-bits. Hence upon exploiting the above-mentioned classical-quantum isomorphism, two codes are needed for mitigating the bit-flips and phase-flips. Hence instead of a half-rate classical code, a quarter-rate quantum code has to be used. In the treatise "Polar Codes and Their Quantum-Domain Counterparts", Zunaira Babar, Zeynep B. Kaykac Egilmez, Luping Xiang, Daryus Chandra, Robert G. Maunder, Soon Xin Ng, and Lajos Hanzo commence their discussions with the polar-coding basics and then demonstrate that Arikan's classical-domain polar codes are capable of approaching Shannon's capacity at a low encoding and decoding complexity, while conveniently supporting rate adaptation. By virtue of these attractive features, polar codes have found their way into the 5G New Radio (NR) standard. Hence in this paper the authors provide a comprehensive survey of polar codes, highlighting the major milestones since its conception. Furthermore, they provide detailed tutorial insights into the operation of the polar encoder, the multiplicity of decoders as well as into their code construction methods. Finally, they extend their discussions to quantum-domain polar codes with an emphasis on syndrome-based quantum polar decoders.

II. 5G Communications

Applications such as wireless industrial automation or vehicular communications require communication systems that provide low latency combined with high reliability. As existing communication systems are not able to fulfill all of these requirements, using multiple communication paths, i.e., Multi-Connectivity (MC), is a promising approach to decrease latency and increase reliability. Traditionally, MC approaches like Multipath-TCP (MP-TCP) or Dual-Connectivity (DC) make use of multiple links to achieve higher data rates. Due to strict latency and reliability requirements of emerging applications, recently more focus is drawn to how MC can be used to enhance these parameters. In this context, the paper titled "Multi-Connectivity as an Enabler for Reliable Low Latency Communications - An Overview" by Marie-Theres Suer, Christoph Thein, Hugues Tchouankem, and Lars Wolf provides an overview of MC techniques for achieving lower latency and higher reliability with focus on wireless one-hop networks. The authors provide a definition for MC, identify main scheduling categories, network architectures and concepts on different layers for implementing MC. MC approaches established in standardization and relevant approaches in the literature are discussed on a layer-by-layer basis. Finally, the authors identify and discuss further research challenges such as a comparison of MC approaches on different layers, dynamic scheduling techniques for MC and influence of path characteristics on MC performance.

With the rapid development of mobile communication network, the existing 4G network cannot meet the needs of users, and 5G network came into being. Compared with the existing 3G and 4G networks, the 5G network will present the features such as diversified terminals and huge number of nodes, ultra-high density deployment of nodes, coexistence of multiple wireless network technologies and security mechanisms, end-to-end direct communication, and new techniques including Vehicle to Everything (V2X), Software Defined

Network (SDN) and Network Function Virtualization (NFV). The introduction of the new features and techniques brings about the huge challenges for the security aspects in 3GPP 5G networks. In this context, the paper titled "A Survey on Security Aspects for 3GPP 5G Networks" by Jin Cao, Maode Ma, Hui Li, Ruhui Ma, Yunqing Sun, Pu Yu, and Lihui Xiong presents a survey of security aspects in 3GPP 5G networks. Firstly, the paper overviews the security architectures and functionalities in the 3GPP 5G networks. Subsequently, the paper analyzes in detail the security requirements or vulnerabilities and discusses the existing solutions for these new features and techniques in the 3GPP 5G networks. Finally, the paper gives some potential areas and research directions for these new features and techniques.

The growth of mobile networks offered to gratify the upcoming demands of novel network services for portability, enhanced performance, elasticity, and energy efficiency. 5G mobile networks adopt new networking concepts to further improve these features that has led to the new security issues in the system. Security risks can have high consequences, hence it becomes the primary concern in many telecommunications industries today. Consequently, the complication and strength of security attacks have enlarged recently, making the detection or prevention of sabotage a global challenge. The fast growth of 5G network is leading to the high level of security issues at different levels. The new technology certainly provides the new threats and other security issues. In this domain, the paper titled "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions" by Rabia Khan, Madhusanka Liyanage, Dushantha Nalin K. Jayakody, and Pardeep Kumar has explored existing and probably upcoming 5G security issues in the available literatures and its relevant understanding. The authors have explored the inclusive exploration on 5G security model, next generation threat landscape for 5G, IoT threat landscapes, and threat analysis in 5G networks. The survey covers complete research on security challenges in key 5G security domains, including authentication, access control, communication security, and encryption. The survey also highlights the identified security issues associated with 5G key technologies, i.e., Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, Multi-access Edge Computing (MEC), and Network Slicing (NS) concepts. Then, the survey includes a horizontal analysis of security monitoring and privacy aspects on 5G network. Finally, a comprehensive list of future directions and open challenges is included to encourage future research on 5G security domain.

III. Vehicular and Sensor Communications

In the last few decades, Global Navigation Satellite Systems (GNSS) have become indispensable elements in our society. Currently, GNSS are not only used for position, velocity, and time solution, but they also find their applicability in a wide variety of situations, such as energy distribution and power grid monitoring, automated stock trading systems, transportation and automated vehicles, telecommunications, etc. Due to the increase in GNSS popularity, intentional interference in GNSS is becoming an increasing threat. Critical application areas such as aviation can be severely affected by un-detected and un-mitigated interference, and therefore interference management solutions are crucial. Methods to cope with such intentional interference enclose interference detection, interference mitigation, interference classification, and interference localization. In this context, the paper titled "A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft" by Ruben Morales-Ferre, Philipp Richter, Emanuela Falletti, Alberto de la Fuente, and Elena Simona Lohan presents a survey in interference management methods developed in the last four decades by the research community. Mathematical models, comparative tables for various interference management solutions, as well as comparative numerical results are presented. Some of the main findings are that, the most promising jammer mitigation approaches in GNSS-based aviation application are the pre-correlation approaches, while spoofing mitigation is effective only in the post-correlation/navigation domain. Also, cost-effective on-board navigation solution should rely on maximum three GNSS antennas and it is found in the paper that one antenna suffices for jamming detection and only two antennas are required for efficient spoofing detection.

During the past few years, there has been a tremendous amount of interest in the utilizing civilian unmanned aircraft vehicles (UAVs) for a wide range of applications. UAVs' popularity is due to the fact that they have proved their applicability and efficiency. However, lack of standardization in this domain has set back their utilization to the fullest. It is anticipated that the total growth in the commercial UAV sales and applications would increase significantly if their communication and network technology is standardized. Regarding this matter, the paper titled "Potential Data Link Candidates for Civilian Unmanned Aircraft Systems: A Survey" by Maede Zolanvari, Raj Jain, and Tara Salman presents a survey, where potential candidates with proper adaptions as standard UAV datalinks are studied in detail. The strengths and weaknesses of these available technologies and their capability to satisfy the basic requirements are highlighted. On the other hand, to standardize suitable datalink technologies for UAVs, authors have studied several promising aerial standards and how they can be modified and specified for UAVs. At the end, the authors bring up some future challenges in this area with several potential solutions to motivate further research work in this domain.

Vehicular Ad-hoc networks have become very popular during last 2 decades. They have received attention from both the academia and industry for improvement in traffic conditions and driving safety. The vehicles need to communicate with each other and exchange the data within themselves and with the existing infrastructure. Named Data Networking (NDN) which is a recent implementation of the Information-Centric Networking (ICN) is very suitable for the communication among the entities in the vehicular networks. In order to improve the driver's experience, safety and reliability of traffic, many researches have yielded excellent results in the past but there are still some issues in the domain of vehicular networks that need attention. These issues and challenges

are mostly related to the content delivery, data dissemination, and the experience of user as they are adversely affected by the ephemeral nature of the vehicular networks. To overcome these challenges, NDN has been used for communication in the vehicular networks in recent past. In this context, the paper titled "Named Data Networking in Vehicular Ad hoc Networks: State-of-the-Art and Challenges" by Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, Yasir Faheem, Rasheed Hussain, and Adlen Ksentini presents a systematic and detailed review of NDN in vehicular ad-hoc networks. The authors discuss the role and feasibility of NDN in the vehicular ad-hoc networks and shed light on the naming, routing, forwarding, mobility and security mechanisms for vehicular ad-hoc networks. Lastly, the authors discuss the simulation tools for NDN-based vehicular ad-hoc networks and conclude the paper with open challenges and future research directions.

As the number of elderly population is significantly increasing, aging brings various health related issues such as hearing impairment, cognitive decline, and memory loss. The older adults also tend to fall frequently. Therefore, it is important to provide home-based assisted living for elderly people. The assisting system would monitor daily human activities especially anomalous behavior to ensure safer and independent living of elderly. Advances in the field of communication technologies and availability of various small and cheap sensors, smartphones and cameras have made it easier to monitor daily human activities. Human activity recognition (HAR) is one such technology that analyses human activities automatically and facilitates anomalous behavior detection. In this context, the paper titled "A Survey on Anomalous Behavior Detection for Elderly Care Using Dense-sensing Networks" by Samundra Deep, Xi Zheng, Chandan Karmakar, Dongjin Yu, Len Hamey, and Jiong Jin presents a survey that thoroughly reviews dense-sensing networks based human activity and anomalous behavior detection. The survey provides an overview of the key challenges in current activity and anomaly detection technologies. Meanwhile, it discusses the importance of sensor fusion while deploying a dense-sensing network based human anomalous behavior detection. The survey highlights that employing sensor fusion techniques could significantly increase the efficiency of dense-sensing network. It also examines research challenges and open issues that guide the readers for future research directions.

IV. IOT AND M2M

Large-scale sensor networks have always been one of the major challenges for ubiquitous deployment of Internet-of-Things (IoT) systems. Previous studies on sensor networks utilize ad-hoc networking techniques to establish large scale IoT systems. Such ad-hoc networking, however, often suffers from the limited communication range, unreliable wireless links, and the time-varying network topology. To address these limitations, LoRa communication technology arises as a promising solution. Unlike traditional communications, LoRa enables long-range communications over tens of kilometers in rural areas. LoRa significantly simplifies the network deployment and management for large scale IoT systems as one LoRa gateway is able to cover large areas. In this context, the paper titled "A Survey on LoRa Networking: Research Problems, Current Solutions and Open Issues" by Wan Du and Jothi Prasanna Shanmuga Sundaram reviews the research problems, existing efforts and the remaining open issues in LoRa networking. The deployment challenges of LoRa technology are unveiled and recent solutions are discussed in detail. Moreover, the comparative discussions on existing works may inspire further works and optimization in LoRa networking and support wide deployment of the LoRa networks.

To achieve the parallel interactions between the human world and the computer network, Internet-of-Things along with wireless mobile communication and computing open up some future opportunities as well as challenges for constructing a novel intelligent system. In this context, the cyber-physical-social system (CPSS) emerged as the association system that integrates computing, physics and human resources and enables the coordination among the cyber, physical and social worlds. It supports self-synchronization, parallel execution and supervisory control in physical, information, cognitive and social domains so that it can provide an ideal paradigm to achieve the design and construction of a smart environment with command and control organizations. In this context, the paper titled "Cyber-Physical-Social Systems: A State-of-the-Art Survey, Challenges and Opportunities" by Yuchen Zhou, Fei Richar Yu, Jian Chen, and Yonghong Kuo presents a survey, which overviews the background, architecture design, applications, standards, real-world case studies, and some enabling techniques and networks of CPSSs. Moreover, to enable the pervasive computation services and the frequent content retrieval and delivery in CPSSs, the authors further propose a virtualization architecture and an integrated framework of caching, computing and networking for CPSSs. The survey concludes with a discussion of some research issues, where challenges and possible solutions are unearthed for researchers in the related research areas.

The massive Machine Type Communication (mMTC) is one of the categories of the emerging diversified telecommunication services. As their number is increasing, it is becoming difficult and challenging to fulfil their diverse communication requirements in ultra-dense and dynamic wireless networks. Some of the other challenges in this regard are handling of sporadic and dynamic MTC traffic, quality of service, radio access network congestion, and huge signaling overhead. In this context, the paper titled "Towards Massive Machine Type Communications in Ultra-Dense Cellular IoT Networks: Current Issues and Machine Learning-Assisted Solutions" by Shree Krishna Sharma and Xianbin Wang identifies and analyzes technical issues, recent advances and potential solutions, and proposes new research directions. First, the authors provide key enablers for mMTC in cellular networks along with the quality of service provisioning issues and mMTC features. Then, they shed light on the channel access mechanisms and key features of emerging IoT standards like NB-IoT and LTE-M. The authors also describe the existing and emerging solutions to the problem of congestion in the radio access

network. Lastly, they list down the challenges, advantages and use cases for machine learning techniques applications in ultra-dense cellular networks and focus on the low-complexity Q-learning approach in mMTC and conclude the paper with open research challenges and future research directions.

V. SDN AND NFV

Software defined networking (SDN) has proved to be a promising new networking paradigm, with ongoing efforts to integrate it with several next generation networking architectures such as IoT, VANET, 5G, etc. Several topics in SDN such as security, energy efficiency, fault management, resource allocation, scalability, etc. have been surveyed so far. However, controller placement in SDN – despite being an important topic on the verge of maturity – has not yet been comprehensively reviewed and consolidated. The controller placement problem (CPP) in SDN was first proposed in 2012, and has since evoked significant interest in the community. Being a key design choice of the SDN control plane, the controller placement impacts a wide range of network issues such as latency, resiliency, energy efficiency, load balancing, etc. In this context, the paper titled, "A Survey on Controller Placement in SDN" by Tamal Das, Vignesh Sridharan, and Mohan Gurusamy consolidate the state-of-the-art on this topic with respect to the diverse objectives for which the CPP has been optimized, the variety of methodologies adopted to solve the CPP, and the various networking domains in which the CPP has been employed. They also compare and contrast the design choices in modeling the CPP in SDN, as well as wide range of metrics that have been used in the literature to measure the effectiveness of the CPP in SDN.

Despite the anticipated benefits of Network Functions Virtualization (NFV), its adoption is hampered by the limited performance that can be achieved on commodity servers, as these still struggle to achieve line-rate processing, especially for compute-intensive Virtualized Network Functions (VNFs). Hardware acceleration can be used to improve the performance of VNFs, but simply adopting dedicated hardware would neglect the flexibility envisioned for NFV. Thus, programmable accelerators such as Field-Programmable Gate Arrays (FPGAs) can be used to provide high performance while maintaining flexibility. Although promising, the adoption of FPGAs in NFV still presents a number of challenges regarding efficient implementation of VNFs on the FPGA fabric, the seamless integration of these devices in a heterogeneous NFV Infrastructure (NFVI) and the programming of VNFs for FPGAs, which still typically requires expertise in hardware design and description. In this context, the paper titled "A Survey on FPGA Support for the Feasible Execution of Virtualized Network Functions", by Gabriel Niemiec, Luis Batista, Alberto Schaeffer-Filho, and Gabriel Nazar presents a survey covering the main research efforts that contribute to the adoption of FPGAs in NFV. The paper covers the implementation of FPGA-based VNFs, FPGA-enabled NFVI platforms and high-level synthesis tools to ease the programmability of VNFs for FPGAs. The survey concludes with a discussion on the main open challenges identified for the efficient and seamless adoption of FPGAs in NFV.

Future networks such as 5G will connect new industries and empower new user experiences for multimedia streaming services especially when downloading high definition videos such as 4K/8K irrespective of the user's location. However, the main challenge for telecom operators and service providers is the QoE management aspect due to the exponential growth of emerging services (e.g., video streaming, video gaming etc.) on smart devices that have different capabilities such as screen size and computational power/resources. The Software Defined Networks (SDN), Network Function Virtualization (NFV) and Multi-Access Edge/Cloud Computing have merged as cutting-edge technologies to provide service customization during multimedia streaming service delivery. In this context, the paper titled "QoE Management of Multimedia Streaming Services in Future Networks: A Tutorial and Survey" by Alcardo Alex Barakabitze, Nabajeet Barman, Arslan Ahmad, Saman Zadtootaghaj, Lingfen Sun, Maria G. Martini, and Luigi Atzori presents a tutorial and comprehensive survey of QoE control and management solutions for multimedia services in future softwarized and virtualized networks. The paper starts with a description of QoE modelling, monitoring, and optimization at different points in the network as important elements for end-to-end QoE management. This is followed by a description of network softwarization and virtualization technologies leveraging SDN, NFV, MEC, Fog/Cloud Computing as important elements for managing multimedia streaming services in future networks such as 5G. The paper further provides QoE control and management techniques using softwarized and virtualized network. Finally, the paper presents the end-user's QoE management challenges and research directions/recommendations regarding multimedia streaming services in future networks.

VI. INTERNET TECHNOLOGIES

Demands for indoor positioning-based services (IPS) in commercial and military fields have spurred various positioning systems and techniques. The main factors affecting indoor positioning accuracy are complex multipath propagation and changing electromagnetic environments. With the rapid development of sensors and wireless networks, almost all indoor targets are covered by multiple sensors and wireless networks, and thus integrating measurement information of multiple sensors and wireless networks to improve the accuracy of indoor positioning has become the promising means for indoor positioning. In this context, the paper titled "A Survey on Fusion-Based Indoor Positioning" by Xiansheng Guo, Nirwan Ansari, Fangzi Hu, Yuan Shao, Raphael Nkrow, and Lin Li overviews the fusion-based indoor positioning from a unified positioning framework, which consists of three fusion characteristics: source, algorithm, and weight spaces. The survey is invaluable for researchers to acquire a crisp grasp of the concept of indoor fusion-based positioning systems and techniques. Moreover, the readers can gain insights from this survey to further advance the state of the arts of indoor positioning.

The progressive adoption of Information and Communication Technologies (ICT) in the industry has triggered the development of novel wireless communication standard technologies to meet industrial requirements. The IETF IPv6 over the TSCH mode of IEEE802.15.4e (6TiSCH) working group has standardized a low power industrial-grade IPv6 wireless technology to address industrial automation and reliable monitoring. 6TiSCH is built on the Time Slotted Channel Hopping (TSCH) mode of the IEEE802.15.4-2015 standard, supporting multi-hop topologies with the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) routing protocol, and is IPv6-ready through 6LoWPAN. The 6TiSCH WG has been focused on the definition of the control plane protocols to match the TSCH synchronous link-layer operation to the routing topology and application communication needs. In this definition numerous challenges have been addressed, such as the development of secure light-weight join procedures and the definition of a simple, yet powerful scheduling function. In this context, the tutorial titled "IETF 6TiSCH: A tutorial" by Xavier Vilajosana, Thomas Watteyne, Tengfei Chang, Malisa Vucinic, Simon Duquennoy, and Pascal Thubert provides a very deep but comprehensive description of the 6TiSCH architecture and protocol suite, as well as goes through the ecosystem of hardware platforms, tools, implementations and simulators that constitute the 6TiSCH ecosystem. This paper is meant to be used both as a primer, and as a reference for researchers and engineers implementing and building upon IETF 6TiSCH specifications.

VII. Network Security

Wireless Sensor Networks (WSNs) constitute one of the most promising third-millennium technologies and have a wide range of applications due to their tremendously appealing features, e.g., low production cost, low installation cost, together with unattended, autonomous and longtime operation. WSNs have started to merge with the Internet of Things (IoT) through the introduction of Internet access capability in sensor nodes and sensing ability in Internet-connected devices. Thereby, the IoT is providing access to a huge amount of data, collected by the WSNs, over the Internet. Hence, the security of IoT should start with foremost securing WSNs ahead of the other components. However, owing to the absence of a physical line-of-defense, i.e., there is no dedicated infrastructure such as gateways to monitor and observe the information flowing in the network, the security of WSNs along with IoT is of a big concern to the scientific community. Within this context, paper titled "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures" by Ismail Butun, Patrik Österberg, and Houbing Song, categorized and treated the currently known security attacks towards WSNs and IoT, along with the techniques for prevention, detection, and mitigation of those attacks. Understanding these attacks and their associated defense mechanisms will help in paving a secure path towards the proliferation and public acceptance of IoT technology. In the paper, the authors conclude that security must be a key component when designing protocols for WSNs as well as for IoT. Without a proper assessment of possible threats and inclusion of related preventive measures, these networks will be vulnerable to attacks. Eventually, future researchers working on WSNs and IoT are strongly recommended by the authors to consider security to a higher extent while designing their routing, key distribution, trust management, and data aggregation schemes over the MAC, networking, transport, and application layers.

With the proliferation of embedded systems in consumer and industrial products, sensors converting physical properties into electrical features play a part in most people's daily lives. They are found everywhere from accelerometers in smartphones microphones in digital voice assistants to drip sensors in medical infusion pumps and temperature sensors in infant incubators. Sensors are thus often used in safety- and security-critical situations, and the integrity of their measurements can be crucial in protecting the people who depend on them. However, recent research has shown that attackers can exploit imperfections in the underlying hardware to remotely change sensor measurements, causing systems to act upon the adversarial data. In this context, "Taxonomy and Challenges of Out-of-Band Signal Injection Attacks and Defenses" by Ilias Giechaskiel and Kasper Rasmussen systematizes the space of such adversarial manipulations that enable sensor spoofing. Specifically, through a comprehensive survey of the state-of-the-art research, the article presents a chronological and thematic evolution of out-of-band signal injections, and creates a classification of sources of vulnerability and countermeasures. It further highlights cross-influences between electromagnetic, conducted, acoustic, and optical attacks, and reveals challenges that future research should address.

With the rise in Internet connectivity, deceptive attacks like phishing and spear phishing have become a serious threat to companies and ordinary users, with estimates of financial losses ranging from 100s of millions of dollars to couple of billion dollars each year. In addition, damages include loss of time, productivity, and reputational damage for corporations. Despite continuing attempts by researchers to detect such attack vectors, perpetrators still succeed in finding innovative techniques to bypass such security filters and detection methods. While there exist multiple challenges that need to be considered in security research, the question arises whether researchers have taken these into consideration. These challenges include: the active attacker, the base-rate fallacy, the time scale of attacks, and the lack of large, sufficiently diverse datasets. In this context, the paper titled "SOK: A Comprehensive Reexamination of Phishing Research from the Security Perspective" by Avisha Das, Shahryar Baki, Ayman El Aassal, Rakesh Verma, and Arthur Dunbar presents a systematic survey of the literature on phishing and spear phishing detection techniques. The paper also provides the first comprehensive review of user studies involving phishing attacks to determine vulnerable populations and susceptibility to phishing. Moreover, the survey identifies gaps in the literature on phishing and spear phishing detection research and in the user studies. Key observations from the analysis of research on each attack vector are discussed.

Reactive defense mechanisms (e.g., intrusion detection systems) have made significant efforts to secure a system or network for the last several decades. However, the nature of reactive security mechanisms have been limited in preventing attackers in advance. As more and more persistent, advanced, and intelligent attacks have been exhibited, defenders are often behind to deal with them. Moving target defense (MTD) is a proactive defense concept aiming to thwart potential attackers by dynamically changing attack surfaces (e.g., system/network configurations). The actions by the MTD can increase uncertainty and complexity for any attacker of the system while decreasing the opportunities for the attacker to identify targets (e.g., vulnerable system components) and introducing higher cost in launching attacks or scans (e.g., reconnaissance attacks). The desired result is that the attacker will waste time and effort without gaining useful intelligence about the system. In this context, the paper entitled "Towards Proactive Defense: A Survey on Moving Target Defense," authored by Jin-Hee Cho, Dilli P. Sharma, Hooman Alavizadeh, Seunghyun Yoon, Noam Ben-Asher, Terrence J. Moore, Dongseong S. Kim, Hyuk Lim, and Frederica F. Nelson presents a comprehensive survey on the various aspects of MTD techniques, including its key roles, design principles, classifications, common attacks, key methodologies, important algorithms, metrics, evaluation methods, and application domains, along with the pros and cons of all aspects of MTD techniques. In addition, the authors suggest highly promising future research directions and provide overall trends of proactive, adaptive MTD techniques to the readers.

The integration of information and computational technology with traditional embedded systems lead the formation of new modern cyber physical system (CPS). These CPSs gathered a considerable attention since past decade because they are part of several domains of our life. Formally, CPSs are categorized into four major types named as smart grid, intelligent transportation system, Industrial Internet of Things (IIoT), and healthcare. Modern-day CPSs are efficient enough to carry out plenty of tasks autonomously, however, these CPSs are also prone to certain passive attacks that can cause serious harm to privacy of these systems. In order to protect the privacy of such CPSs, researchers proposed the use of a state-of-the-art notion of privacy called as differential privacy. Differential privacy works over the phenomenon of obfuscation and effectively protects privacy of both data types; real-time and statistical database storage. In this context, paper titled "Differential Privacy Techniques for Cyber Physical Systems: A Survey" by Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen presents a survey in which first a comprehensive survey of techniques of differential privacy is carried out in various CPSs scenarios. Furthermore, an extensive literature about integration of differential privacy in all four CPSs domains is provided by carrying out an in-depth technical analysis regarding the implementation and functioning. Afterwards, challenges, open issues, and future research directions have been highlighted for integration of differential privacy in CPSs.

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, National Chiao Tung University
Director, Network Benchmarking Lab
Web: www.cs.nctu.edu.tw/∼ydlin