Editorial: First Quarter 2019 IEEE Communications Surveys and Tutorials

I WELCOME you to the first issue of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS in 2019. This issue includes 35 papers covering different aspects of communication networks. In particular, these articles survey and tutor various issues in "5G Networks," "Wireless and Cellular Communications," "Software Defined Networks and NFV," "Internet Technologies and Multimedia Communications," "Network Security: Classic Networks," "Network Security: Emerging Networks" and "Miscellaneous." There are three papers in the miscellaneous category that survey the issues in Power Line Communications, Network Verification and Testing, and Quantum Computing. A brief account for each of these papers is given below.

I. 5G NETWORKS

The fifth generation (5G) communication is expected to support diverse scenarios and applications to include but, not limited to enhanced mobile broadband (eMBB), ultra-reliable low latency communication (URLLC) and massive machine type communication (mMTC). In order to meet various requirements of 5G and beyond communications, the future new radio not only considers the traditional sub-6 GHz but, also considers the millimeter-wave (mmWave) band and terahertz (THz) band to overcome spectrum scarcity and provide wide bandwidth from dozens of MHz to several GHz. Efficient transmission technologies like massive multiple-input multiple-output (MIMO) are proposed to improve system capacity. In order to effectively support the design, deployment, and evaluation of the 5G and beyond wireless communication technologies, accurate channel characterization and modeling are of great importance. In this context, the paper titled "The Design and Applications of High-Performance Ray-Tracing Simulation Platform for 5G and Beyond Wireless Communications: A Tutorial" by Danping He, Bo Ai, Ke Guan, Longhe Wang, Zhangdui Zhong, and Thomas Kuerner presents a comprehensive tutorial on the design of high-performance ray-tracing (RT) simulation platform and the applications. With the aim to fulfill the requirements of the 5G system and beyond, the paper points out that the RT should support massive simulation tasks for the moving scenarios and MIMO simulation with high performance (accuracy and efficiency), good usability, and availability. The practices in the design of high-performance RT simulation platform and the applications for 5G and beyond communications are introduced, with the publicly available high-performance cloud-based RT simulation platform – CloudRT (http://www.raytracer.cloud/) as a main reference.

With the rapid increase and explosive growth in the number of mobile-connected devices and mobile data traffic, cellular networks have become an important part of the Internet of Things (IoT) since the main part of the IoT communications are designed over wireless cellular technologies. One of the promising solutions to deal with this explosive growth is deployment of small cells (e.g., femtocells). Small cells will help mobile operators to enhance coverage and capacity of the network, and provide low cost and high quality services to mobile users. In this context, the paper titled "Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview" by Fadi Al-Turjman, Enver Ever, and Hadi Zahmatkesh presents a survey on the use of femtocells and their applications in traffic modeling and deployment issues in the 5G/IoT era. The paper also discusses various design factors which are essential while considering such applications. Finally, the paper presents some open research issues associated with IoT-femtocell based applications which are still waiting to be resolved.

With rapidly increasing quality of experience requirements, the end users are expecting the 5G communication and beyond to provide services like ultra-low latency, extremely high data rate, high reliability, large communication coverage and so on. Cooperative relaying is an effective way of enhancing the communication capability in future wireless communications, with the help of the relay node amplify, or compress/compute, or decode and then forward the original message overheard. As a new relaying strategy, lossy forwarding is developed from decode-and-forward relay and has already shown its superiority in terms of outage probability, coverage area, etc., which makes it a promising technique in future wireless communications. In this context, the paper titled "A Tutorial on Lossy Forwarding Cooperative Relaying" by Jiguang He, Valtteri Tervo, Xiaobo Zhou, Xin He, Shen Qian, Meng Cheng, Markku Juntti, and Tad Matsumoto presents a tutorial and survey on the achievable rates and outage analysis for different cooperative communication network scenarios with the lossy forwarding strategy. Moreover, this tutorial also presents comparative discussions which highlight the future research directions of applying lossy forwarding to future communication systems.

Digital Object Identifier 10.1109/COMST.2019.2896498

A wide range of existing network applications, e.g., industrial control, as well as emerging communication paradigms, such as fifth generation (5G) wireless networking and the tactile Internet, demand Ultra-Low Latency (ULL) packet transport with latencies on the order of one millisecond or less. Traditional packet networks can typically only reduce the end-to-end packet latencies to the order of tens of milliseconds. The IEEE 802.1 working group has recently launched the Time Sensitive Networking (TSN) task group to develop link layer standards for supporting ULL packet flows. In parallel, the Internet Engineering Task Force (IETF) has launched the development of Deterministic Networking (DetNet) standards to support ULL packet flows at the network layer. In this context, the article titled "Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research" by Ahmed Nasrallah, Akhilesh S. Thyagaturu, Ziyad Alharbi, Cuixiang Wang, Xing Shao, Martin Reisslein, and Hesham ElBakoury provides an up-to-date comprehensive survey of the IEEE TSN and IETF DetNet standards as well as the related research studies. The survey of these standards and research studies is organized according to the main categories of flow concept, flow synchronization, flow management, flow control, and flow integrity. ULL networking mechanisms play a critical role in the 5G network access chain from wireless devices via access, backhaul, and core networks to the Internet at large. Therefore, this survey also covers studies that specifically target the support of ULL in 5G networks, with the main categories of fronthaul, backhaul, and network management.

Mobile networks have started moving into the era of 5G. The first standardizations have already been released and deployment will soon begin. Cloud-RAN is recognized as one of the main 5G enablers. In Cloud-RAN the base station equipment is offloaded by moving processing into datacenters. The traditional Cloud-RAN architecture requires a high capacity network connection, which can be difficult and expensive to deploy. Hence, researchers are looking into new possibilities to deploy the so-called crosshaul network proposed for 5G. The newest trends in this area point towards including more functionalities on site, lowering the capacity requirements to the crosshaul network. The exact separation between the on site functionalities and the functionalities processed in a datacenter is referred to as the functional split. In this context, the paper entitled "A Survey of the Functional Splits Proposed for 5G Mobile Crosshaul Networks" by Line Larsen, Aleksandra Checko, and Henrik Christiansen surveys a range of functional splits. The functional split options under study in this paper are those proposed by 3GPP in TR 38.801. The paper provides an overview of where the most research has been directed in terms of functional splits, and maps the standardization currently taking place into the research directions.

II. Wireless and Cellular Communications

The millimeter wave (mmWave) bands offer orders of magnitude more spectrum than conventional wireless frequencies to provide unprecedented bitrates to next-generation cellular mobile terminals. On the other hand, mmWave links suffer from increased free-space pathloss, atmospheric absorption, and severe channel intermittency. To overcome these issues, future networks must operate through highly directional antennas to provide an additional beamforming gain to the link budget in dense scenarios. The consequence is the need for accurate alignment of the transmitter and the receiver beams, an operation which is particularly challenging for control layer procedures, such as initial access, handover and beam tracking, and which might introduce additional latency to access the network. In this perspective, the paper titled "A Tutorial on Beam Management for 3GPP NR at mmWave Frequencies" by Marco Giordani, Michele Polese, Arnab Roy, Douglas Castor, and Michele Zorzi overviews recently proposed measurement strategies for beam management in future cellular networks operating at mmWaves, and provides guidelines for the design of accurate, cost-effective, robust, and energy-efficient control schemes based on the 3GPP NR standard. The tutorial demonstrates that the best approach depends on the specific scenario in which the nodes are deployed, and suggests the optimal choice as a function of the system parameters.

During the last decade, we witnessed the Bing Bang of mobile gadgets such as smartphones, tablets, laptops, and others. The continuously growing number of client devices involved in wireless communications, as well as the plurality of wireless networks operating in the same area, poses many challenges, most of which are caused by huge interference. Being the most popular and widespread wireless technology, Wi-Fi needs to address such challenges. For that, IEEE 802 is developing a new amendment to the Wi-Fi standard, namely 802.11ax, which will soon replace the current flagship 802.11ac version. In this context, the paper titled "A Tutorial on IEEE 802.11ax High Efficiency WLANs" by Evgeny Khorov, Anton Kiryanov, Andrey Lyakhov, and Giuseppe Bianchi figures out the main problems inherent to dense Wi-Fi networks and highlights the latest achievements of the 802.11 community in solving them. Apart from providing a comprehensive overview of the main revolutionary features introduced in the Wi-Fi technology with a rather detailed explanation of why such features were designed and how to use them, the paper provides a solid survey of the existing studies and open issues. The latter should be especially exciting for academia since it gives the ideas of possible new problem statements and opens new research directions.

Constructive Interference (CI) is a technique that allows two concurrent transmissions to the same receiver. Instead of colliding with each other, the receiver can demodulate the incoming signal correctly. The highly synchronized network and simple flooding routing feature makes CI an interesting solution for low-latency low-power wireless communication. In this context, the paper titled "Constructive Interference in 802.15.4: A Tutorial" by Tengfei Change, Thomas Watteyne, Xavier Vilajosana, and Pedro Gomes provides a comprehensive study about the advantages and drawbacks of CI, and discusses future work in that field. This paper consists of three parts. First, a comprehensive study about CI research in the last decade. This study lists the advantages of CI for ultra low-latency and low-power applications, but also clearly highlights its drawbacks, including limited throughput and security challenges. Second, the paper contains a hands-on tutorial about how to implement CI, and comes with all the source code needed for implementing CI, under a BSD open-source license. Third, the paper discusses future research directions for CI, including how it could be integrated in industrial standards such as the IETF 6TiSCH industrial IoT standards.

Emerging wireless communication technologies such as IoT and multimedia significantly increased the demand for large bandwidth and high frequency usage which consequently led to frequency shortage, especially, with the remarkable increase of the users of those technologies. Cognitive radio (CR) technology appeared as a promising solution for this shortage by allowing unlicensed users, i.e., secondary users (SU), to dynamically access vacant bands of the licensed user, i.e., primary user (PU) in non-interfering basis. Spectrum sensing is the foremost functional component in CR, since it determines vacant spectrum bands of the PU, therefore, those bands can be exploited by the SU without license. Blind spectrum sensing approaches have an advantage of determining the vacant bands without requiring a prior knowledge of the PU signal characteristics. In this context, the paper titled "Blind Spectrum Sensing Approaches for Interweaved Cognitive Radio System: A Tutorial and Short Course" by Faroq Awin, Esam Abdel-Raheem, and Kemal Tepe presents a tutorial and survey on the topic. The paper overviews the principle of operation and implementation algorithms of different blind spectrum sensing approaches. Moreover, it presents a comprehensive discussion about their performances and applications and finally concludes with highlighting the open issues and challenges.

Recent technological advances have made Multi-Access Edge Computing (MEC) much more feasible. The major goal of MEC is to offer data and services with low latency and at a high rate. To accomplish these, MEC offers cloud services to final consumers at the network periphery. MEC will have a profound impact on wireless sensor networks, cognitive small cells, micro grids, and on networks formed by autonomous vehicles as communication relays. In this context, the paper titled "Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends" by José Moura and David Hutchison presents a tutorial and survey of MEC. First, the paper provides an overview of theoretical games, namely the Repeated Prisoner's Dilemma, Coalitional, Stackelberg, Evolutionary, and Bayesian. It then reviews the relevant literature, focusing on the various mechanisms for model enhancement in terms of cooperation incentives and automatic learning. The work provides useful guidelines for researchers to design models and algorithms that address the technical challenges imposed by new MEC cases on a heterogeneous network infrastructure. Finally, considering the outcomes as well as the gaps and limitations of literature, the paper discusses open problems for applying Game Theory to a broad range of MEC scenarios, notably: low access latency for data and services; distributed offloading/computing; proactive data edge caching managed by means of data popularity, social connections, and available node battery energy; low-power wireless communications for remote sensors; indoor location-based services; RAN (Radio Access Network) for pervasive applications/data; and security/privacy issues in upcoming cyber physical systems.

Wireless Sensor Networks, Mobile Ad hoc Networks, Delay-Tolerant Networks, and Vehicular Ad Hoc Networks are the paradigms which appeared as a result of wireless capabilities of mobile devices. These mobile devices can either be mobile by design or mobile by nature. These networks of mobile devices have an advantage over the conventional data networks in terms of limitation, when equipped with storage capabilities. In this context, the paper titled "Mobility as an Alternative Communication Channel: A Survey" by Benjamin Baron, Promethee Spathis, Marcelo Dias de Amorim, Yannis Viniotis, and Mostafa H. Ammar presents a survey of direct data delivery approaches where the data between a source and a destination is carried through one or more entities that are independent. The paper differentiates these direct data delivery approaches on the basis of purpose of the entity movement. In the latter part, this paper surveys the indirect data delivery approaches where multiple mobile entities are involved in delivering the data between the source and destination and take turns in doing so. The paper also presents a classification of these approaches.

Because it is capable of significantly enhancing both system's spectral efficiency and energy efficiency, index modulation (IM) has emerged as a promising technology to meet the escalating mobile data traffic and energy consumption demands of wireless communication systems. As IM can be implemented in the frequency domain, spatial domain, time domain and channel domain, various IM techniques were typically developed separately in their respective implementation domains. In this context, the paper titled "Novel Index Modulation Techniques: A Survey" by Tianqi Mao, Qi Wang, Zhaocheng Wang, and Sheng Chen offers a comprehensive survey of IM-aided systems. Fundamental principles common to different IM techniques are highlighted, and advantages and drawbacks of various IM-aided systems are detailed. Better designs for frequency-domain IM systems are also provided for the first time. By addressing a range of challenges and open issues on IM, it is demonstrated that this attractive technology will play an important role in future communication systems.

III. Software Defined Networks And NFV

Software-defined networking (SDN) is an emerging network paradigm that offers to ameliorate the constraints of traditional environments by giving programmability control of the networking devices. In SDN, the network architecture is split into a programmable data plane and a logically centralized control plane. The data plane of SDN becomes a set of simple forwarding devices and the control plane implements the control logic desired by network operators. With the separation of the control and data planes, SDN simplifies policy enforcement and network (re)configuration and evolution. The network innovations it provides, position SDN as the future of networking for many information technology areas, e.g., cloud computing, network function virtualization (NFV), and Internet of Things. In this context, the paper titled "Fault

Management in Software-Defined Networking: A Survey" by Yinbo Yu, Xing Li, Xue Leng, Libin Song, Kai Bu, Yan Chen, Jianfeng Yang, Liang Zhang, Kang Cheng, and Xin Xiao presents a survey. First, the paper starts by providing an overview of the main fault problems in SDN. Then, the paper elaborates on fault management in SDN for improving network reliability and security from several aspects, including system monitoring, fault diagnosis, fault recovery and repair, and fault tolerance. Next, the paper analyzes the gap between solutions developed in an academic research context and practical deployments for SDN fault management. Finally, the paper discusses a range of open challenges and potential directions for future research.

Software Defined Networking (SDN) decouples the control plane and the data plane. The network resources in SDN are managed by a logically centralized controller. The centralized SDN controller has a global network view, which makes the network easy to control and manage. Machine learning techniques can bring intelligence to the SDN controller by performing data analysis, network optimization, and automated provision of network services. The programmability of SDN enables that the optimal network solutions made by machine learning algorithms can be executed on the network in real time. In this context, the paper titled "A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges" by Junfeng Xie, F. Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, Chenmeng Wang, and Yunjie Liu presents a tutorial and survey. First, the paper starts by providing an overview of SDN and widely-used machine learning algorithms. Then, the paper summarizes a range of recent studies on the application of machine learning algorithms in the realm of SDN, which are intended to provide useful guidelines for researchers to understand the referenced literature. Furthermore, the paper discusses a range of open problems to be tackled by future research. Finally, the paper explores some broader perspectives.

Facilitating a convenient mode of Internet access to end-user devices, Wireless Local Area Networks (WLANs) have been ubiquitous in various environments. However, the management of these networks requires the adoption of novel techniques, especially in dense and dynamic environments. Software-Defined Networking (SDN) revolutionizes the network management aspects of such massive infrastructures by separating the data plane and control plane and offering interfaces to abstract the monitoring and control of underlying network components. The convergence of SDN and WLAN referred to as Software-Defined WLANs (SDWLAN), has been realized as a diverse set of architectures and enables the adoption of novel centralized control mechanisms such as association control and channel assignment. In this context, the paper titled "A Review of Software-Defined WLANs: Architectures and Central Control Mechanisms" by Behnam Dezfouli, Vahid Esmaeelzadeh, Jaykumar Sheth, and Marjan Radi presents a comprehensive survey of SDWLANs. First, the paper introduces standard network management protocols utilized in traditional and software-defined networks. Next, the paper reviews SDWLAN architectures and reveals their primary objective, components, interconnection protocols, and APIs provided. Concerning observability and configurability, programmability, virtualization, scalability, and traffic shaping, the paper compares these architectures and highlights research directions to address the current and upcoming requirements of SDWLANs. Then, the paper categorizes and studies the centralized association control and channel assignment mechanisms, highlights the research challenges, and identifies how the potential features of SDWLAN architectures can be employed to design more efficient central control mechanisms.

The phenomenal growth of Internet traffic and emerging cloud-based applications demand high capacity and high performance networks, which poses new challenges regarding network manageability and scalability. To cope with these challenges, a highly flexible Segment Routing (SR) paradigm was introduced by the Internet Engineering Task Force as a source routing methodology to replace the current inefficient destination based routing schemes. SR solved the network challenges by steering along performance engineered paths represented as an ordered list of instructions called segment list and encoded as a MPLS label stack or an IPv6 address list in the packet header. Due to its rich set of capabilities such as flexibility and scalability, SR has been extensively studied in the industry for a broad set of applications, including traffic engineering techniques, restoration from failures, traffic protection, service function chaining, network monitoring, data centers and service provider networks. In this context, the paper titled "Segment Routing in Software Defined Networks: A Survey" by Zahraa N. Abdullah, Imtiaz Ahmad, and Iftekhar Hussain presents a tutorial and survey. First, the paper starts by providing an overview of the basic concepts and unique features of SR architecture. Then, the paper examines the techniques to effectively construct the label stacks that represent the explicit paths in SR and describes a broad set of SR applications in networks, especially in software defined networks. Finally, the paper addresses some open issues in the SR, which can be rich areas for future work.

Service Function Chaining (SFC) is a networking concept that refers to the traversal of network traffic through a set of network services (service functions). Mainly for security reasons, a network operator may deploy firewalls and proxies, stitched together in the edges of the network, to prevent attacks. Today, large-scale data-centers and Internet Service Providers, among others, express the need for a dynamic operation to achieve SFC, to reduce configuration and management complexities. Dynamic SFC is now a hot topic and while different research problems have been studied so far, in our article, we focus on the problem of Traffic Steering for SFC which refers to the forwarding and routing logic of traffic among SFs. The Traffic Steering inherits several functionalities from traffic engineering protocols and can be enhanced with SDN. In this context, the paper titled "Traffic Steering for Service Function Chaining" by Hajar Hantouti, Nabil Benamar, Tarik Taleb, and Abdelquoddous Laghrissi presents a comprehensive survey on Traffic Steering methods for SFC and identifies relevant challenges and new research issues. The survey concludes that a vast research area in SDN-NFV-Cloud-based traffic steering for SFC still has open issues related to reliability, scalability, flexibility limits and QoS in SFC solutions.

IV. Internet Technologies And Multimedia Communications

In the 21st century, various mobile devices such as smartphones, tablets and smart watches have been disseminated rapidly and widely, and people spend more than 80% of their lives indoors, which has led to the development of various services and applications based on the users' indoor location, as determined by the mobile devices. The fingerprinting technology is considered to the very accurate indoor positioning technology, but it requires the preliminary step of the offline fingerprinting map construction, which consumes a considerable amount of time and efforts. Moreover, the fingerprinting map must be entirely reconstructed whenever the access points are added, modified or removed, or the interior features, such as walls or even furniture, are changed. Many researchers have realized the problems in the fingerprinting technology and actively conducted studies to address them. In this context, the paper titled "Indoor Positioning Technologies Without Offline Fingerprinting Map: A Survey" by Beakcheol Jang and Hyunjung Kim presents a survey of indoor positioning technologies that do not require the construction of offline fingerprint maps. First, the paper starts by providing overviews and problems of localization and fingerprinting technologies. Then, the paper categorizes indoor positioning technologies without offline fingerprinting map into simultaneous localization and mapping, inter/extrapolation and crowdsourcing-based technologies, and describes their algorithms and characteristics, including advantages and disadvantages. The paper compares them in terms of its own parameters: accuracy, calculation time, versatility, robustness, security and participation. Finally, the paper presents the future research direction of the indoor positioning techniques.

In a world full of communicating devices, it is crucial to understand how the exchange of information is realized. Working with a legacy or proprietary protocol for which no documentation is available requires reverse engineering of the communication protocol. To date, a lot of critical communication still is unencrypted; therefore in many cases assessing the security properties of unknown protocols requires the analysis of network traces. In recent years, automating this kind of analysis has received a lot of attention. However, most of these approaches were developed independently of each other; likewise, existing categorizations of this area of research also have discussed them in an isolated manner. The paper titled "Survey of Protocol Reverse Engineering Algorithms: Decomposition of Tools for Static Traffic Analysis" by Stephan Kleber, Lisa Maile, and Frank Kargl presents a survey regarding methods of automation for static traffic analysis. It structures the efforts of protocol reverse engineering on the conceptional level and identifies and compares the applied methods and algorithms across all approaches directly. This new point of view highlights the utility of each algorithm for particular protocol reverse engineering situations. While on the one hand, the paper maps which compatible methods can be combined into more efficient new approaches, it also identifies open questions that have not been addressed sufficiently. This especially concerns the requirement to analyze binary protocols efficiently.

Video streaming services are widely deployed and recognized as the Internet killer application. With the dramatic growth of video streaming traffic, there has been a practical challenge for service providers in satisfying the demands of their customers while maintaining a high profit. On one hand, this is challenged by the users' request for high-quality video content without stalls. On the other hand, the best-effort network infrastructure is suffering from sudden and high fluctuating bandwidth due to uncertain characteristics of bandwidth and the congestion on the paths. Instead of the traditional video streaming solutions, the new worldwide video delivery system HTTP Adaptive Streaming (HAS) is rapidly being deployed and is becoming the de-facto solution for Over-The-Top (OTT) adaptive video streaming services over the Internet. In HAS, the bitrate selection is performed by the client via bitrate adaptation logic (ABR) scheme which is not specified in the standard. In this context, the paper titled "A Survey on Bitrate Adaptation Schemes for Streaming Media Over HTTP" by Abdelhak Bentaleb, Bayan Taani, Ali C. Begen, Christian Timmerer, and Roger Zimmermann presents an overview of state-of-the-art ABR schemes for HAS delivery system. First, the paper surveys various ABR schemes that are proposed over the last several years. Then, the paper classifies the ABR schemes based on the entity of the system where the ABR logic is implemented. Next, the paper presents comparisons between different ABR schemes. Finally, the paper describes a discussion on emerging trends within HAS.

V. Network Security: Classic Networks

Security-related data (in short security data), used to detect abnormal network events, are worth studying for the purpose of network security measurement. Different categories of security data provide different perspective on network status. Various network attacks can be detected by collecting and analyzing specific types of security data in order to capture sufficient information on malicious activities of the attacks. Thus, it is significant to conduct a deep-insight survey on the categories of security data and data analytics for network attack detection. In this context, the paper titled "Security Data Collection and Data Analytics in the Internet: A Survey" by Xuyang Jing, Zheng Yan, and Witold Pedrycz gives a comprehensive tutorial and survey. It provides a detailed classification and discussion on the security data towards network security measurement. Based on the usage of data categories and the types of data analytic methods, the paper thoroughly reviews current detection methods for Distributed Denial of Service (DDoS) flooding and worm attacks by applying a proposed set of requirements to evaluate their performance. It builds the relationship between the collected categories of data, the applied analytic methods and attack types. Finally, the paper outlines a number of open issues and highlights future research directions.

In recent years, attacks on critical infrastructure control networks have constantly been on the rise, which is mainly due to several circumstances. For once, the need to take fast and cost effective decisions in a global market pressures service providers to upgrade their previously isolated control systems to remotely accessible control networks. The downside of this combination manifests as a persistent security challenge on the control system side due to the vastly different development speeds of control systems and ICT technologies, leading to legacy control systems interacting with highly modern ICT networking technologies. This leaves control systems and their vendor-specific communication protocols largely exposed to threats from outside networks. The paper titled "Security Challenges in Control Network Protocols: A Survey" by Anna Volkova, Michael Niedermeier, Robert Basmadjian, and Hermann de Meer presents a comprehensive security survey of the most important control system communication protocols (Modbus, OPC UA, TASE.2, DNP3, IEC 60870-5-101, IEC 60870-5-104, and IEC 61850). Therefore a uniform methodology is introduced to perform the security analysis. Its first step is the generation of an adversary model and the definition of relevant attack scenarios; secondly, vulnerable protocols are identified before and after applying the IEC 62351 security standard. Subsequently, possible improvements are discussed which include general protection measures, enhancements to IEC 62351 as well as improvements targeting specific control system protocols. Most notably, despite the fact that all analyzed protocols lack certain security features, it is shown that currently some recent Modbus derivate as well as OPC UA perform best.

The never ending struggle between attackers and defenders in cyber security incites research on novel approaches to defending information systems and computer networks. One of such approaches is being proactive in the sense that the defender estimates when and where the cyber attacks are going to happen. Maintaining situational awareness in the computer networks, keeping track of attack history, and understanding attacker's behavior can be used to estimate the attacker's intention and predict the attacker's next move. Numerous approaches were proposed, varying in goals and methods, although often complementing each other. For example, discrete models, such as attack graphs and Bayesian networks, were used to model the attacks and attacker‘s progress, while time series were used to predict numbers and intensity of attacks. In this context, the paper titled "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security" by Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Èeleda presents a survey that overviews the methods of predicting the cyber attacks and changes in the security situation. A recent shift towards methods based on machine learning or supported by data mining and utilization of real-time data analytics and collaborative intrusion detection system may facilitate the predictions even further. However, there is still a deficit in the proper evaluation of such methods.

Distributed Denial of Service (DDoS) attacks are some of the most devastating attacks in existence. Their continued dominance is largely due to the fact that they continue to evolve and grow with time. Initially a staple at the Network Layer, recently these attacks have demonstrated a tendency to percolate the Application Layer as well, giving rise to more sophisticated attack vectors. Application Layer DDoS attacks can be executed using comparatively fewer resources and at much lower attack volumes, making existing defense mechanisms obsolete. The variety of ways in which these attacks can be executed also lends to their potency. Defense mechanisms that aim to tackle these newly rising challenges must be mindful of their myriad varieties, how these different classes of attacks are executed and how they can be detected. In this context, the paper titled "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications" by Amit Praseed and P. Santhi Thilagam presents a survey highlighting the current research landscape and future research directions pertaining to Application Layer DDoS attacks. First, the paper presents a detailed taxonomy of existing Application Layer DDoS attacks and how they can be executed. Second, the paper presents a detailed discussion about how the different classes of Application Layer DDoS can be detected. The paper also presents a brief discussion of the different datasets, tools and measures of accuracy that can help new researchers in the area.

Intrusion detection is the process of monitoring the events occurring in computer systems and/or networks for detecting a wide range of security attacks ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders. It is becoming more challenging to detect the attacks with the increase in the complexity of the current systems and networks. Hence, there is considerable interest in making use of machine learning techniques for detecting attacks in such complex systems and networks. Although several machine learning based intrusion detection techniques have been proposed over the years, there is a knowledge gap in choosing the machine learning techniques and identifying the best features for efficiently detecting different types of attacks. In this context, the paper titled "A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection" by Preeti Mishra, Vijay Varadharajan, Udaya Tupakula, and Emmanuel S. Pilli provides detailed insights and critical analysis of different machine learning based intrusion detection techniques for detecting different types of attacks. In particular, it will help the readers in making a selection of particular machine learning technique for detecting a specific attack, identifying the best features for efficient attack detection, awareness on the limitations of the machine techniques and comparison with other approaches. We also make suggestions for improvement in each category of technique and present the future directions of machine learning for intrusion detection applications.

VI. Network Security: Emerging Networks

Underwater wireless networking has been becoming a hot research topic since human underwater activities in oceans are growing fast in recent years with a huge number of sensors, actuators and various types of vehicles deployed underwater. Since radio signal cannot propagate well in underwater environments, currently acoustic communication is widely used. However, peculiar features of underwater acoustic networks (UWANs) such as very constrained resources pose big challenges in defending UWANs against security threats. In this context, the paper titled "On Securing Underwater Acoustic Networks: A Survey" by Shengming Jiang presents an extensive survey and significant tutorial content on UWAN security protocols and algorithms. First, it discusses the fundamentals of network security in general and the main UWAN security threats faced by the physical layer to the transport layer. Then it reviews countermeasure schemes against the typical UWAN security threats, securing protocols for communication and networking as well as cryptographic primitives designed for UWANs and UWAN security structures that address several security issues systematically. Finally, the paper closes with a comprehensive discussion on the reviewed schemes and highlighting remaining issues for further research.

The advancement of data communication technologies promotes widespread data collection and transmission in various application domains, thereby expanding big data significantly. Such data is essentially people-centric, which have changed the IT industry and people's way of life and the services they avail. At the same time, privacy violations frequently occur during the communication and aggregation of data. Accordingly, privacy preservation is now prevalent in census data products, social networks, location-based services and smart power grids. These privacy issues have initiated a trend in research in which the goal is to allow individuals to use services by communicating strictly necessary information while preserving the privacy of individuals and preventing sensitive information from being inferred during data communication and data mining. With the continuous improvement of the public's privacy awareness, many industrial and research bodies are actively developing solutions to fulfill the ever-increasing requirements for privacy. In this content, the paper titled "Privacy Preservation in Big Data From the Communication Perspective—A Survey" by Tao Wang, Zhigao Zheng, Mubashir Husain Rehmani, Shihong Yao, and Zheng Huo presents a survey. First, the paper provides an overview of the privacy-preserving framework, which is intended to provide useful guidelines for researchers to understand the referenced literature. Then, the paper elaborates on differential privacy and its generalization and challenges in emerging applications. Finally, the paper discusses a range of open problems to be tackled by future research.

Cooperative Intelligent Transportation Systems (cITS) represent the culmination of vehicular ad-hoc networks (VANETs) and autonomous driving, in which vehicles on the road cooperatively work to improve safety and efficiency of transportation, with minimal driver intervention. Due to the inherent networked nature of these systems, security has long been a priority for researchers in VANETs, and thus also for cITS. Public key infrastructures (PKIs) for real-world deployment have recently been proposed to protect the integrity of these networked systems. However, such cryptographic means do not protect against attackers that possess key material: misbehavior detection refers to means by which such attackers can be detected. The "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems" by Rens W. van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl provides an overview, classification, and taxonomy of misbehavior detection mechanisms. In particular, the survey focuses on the commonalities between existing detection approaches and the new context posed by the (partially) autonomous driving, where data exchanged between vehicles may be applied immediately by control algorithms. Finally, the paper discusses a number of solved and open challenges, as well as a discussion of how misbehavior detection may apply to other Cyber-Physical Systems (CPS).

The adoption of the Internet of Things (IoT) paradigm is expected to revolutionize each domain of human life, by introducing billions of smart devices able to interconnect and to jointly provide sensing and actuation services. On the other hand, distributed IoT systems can introduce new potential attack surfaces to be exploited by malicious cybercriminals. If not appropriately considered, IoT security threats can bring tremendous economical and reputation damages, thus undermining the widespread adoption of IoT. Therefore, the analysis of security for IoT systems requires a systematic approach accounting for the manifold attack surfaces and potential countermeasures. In this context, the paper "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems" by Ivan Farris, Tarik Taleb, Yacine Khettab, and JaeSeung Song presents a comprehensive survey of SDN/NFV-based security solutions to increase the protection of IoT systems. To this aim, the paper first provides a detailed study of security threats for IoT domains, especially highlighting the additional requirements introduced by IoT environments. By identifying the main security features of SDN and NFV security mechanisms, the proposed analysis includes comparison with conventional security approaches, allowing to point out the advantages as well as the complementarity in manifold IoT environments, and to derive the lessons learned so far. Another key contribution of this survey is represented by an extensive discussion on future research directions towards the broad deployment of SDN/NFV-based security solutions for IoT systems.

Since the invention of Bitcoin in 2008, Permissionless Blockchains have received widespread attention not only from the scientific community. Bitcoin's main innovation is the ability to achieve consensus on a set of financial transactions in the permissionless setting, i.e., without prior identification or registration of the participants. In order to defeat Sybil attacks, Bitcoin limits the ability to participate in the consensus process to the computational resources using Proof-of-Work. While most attention has been targeted at these aspects, all Permissionless Blockchains employ Peer-to-Peer networks as a basis for the communication between participants of the system. In this context, the paper titled "Network Layer Aspects of Permissionless Blockchains" by Till Neudecker and Hannes Hartenstein provides a tutorial and survey. First, the paper provides a systematization of all known attacks on the network layer of Permissionless Blockchains. Based on this systematization, the requirements performance, low cost of participation, anonymity, Denial-of-Service resistance, and topology hiding can be derived. Then, the paper gives an overview of design options and inherent tradeoffs. This overview enables the design of optimized network layers. Finally, the paper demonstrates possible directions of future research and applicable methods by analyzing two aspects of the network layer.

The Blockchain technology formed the basis of secure transactions in Bitcoins. It consists of a distributed ledger consisting of blocks of verified transactions. After the success of bitcoins, the technology has found applications in many areas such as banking, logistics, and smart transactions. In this context, the paper entitled “Security Services Using Blockchains: A State of the Art Survey” by Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka surveys Blockchain-based approaches to provide security services. These services include authentication, confidentiality, access control list (ACL), data and resource provenance, and integrity assurance. The aim is to provide insights into the technology usefulness in providing adequate security guarantees. First, the paper provides a brief background of the technology. Following that, the authors discuss each service’s traditional approaches, their challenges, how Blockchains can be used to resolve these challenges, and explore several Blockchain-based approaches for the service along with their comparison. Furthermore, they discuss the challenges associated with the Blockchain-based services to spur of further research in this area.

Communications security has never been more vital in the history of mankind than at the time of writing in the interest of preventing eavesdropping and other malicious tempering with confidential information. Public key based secure communications techniques are widely used, but in the face of the ever-increasing computing power becoming available at a low cost, they gradually become less secure. Hence more secure theoretically non-decypherable alternatives are sought by the research community. As a design option, physical-layer security has come a long way, where for example the unique, hardware-specific imperfections of the communications equipment are exploited for identifying the legitimate parties. Another commercially available solution is to use the diverse variants of quantum key distribution (QKD). Against this background, the paper titled “Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook” by Nedasadat Hosseinidehaj, Robert Malaney, Soon-Xin Ng, and Lajos Hanzo, surveys the recent advances in this alluring field. They argue that the recent launch of the Chinese quantum-enabled Micius satellite heralds a major step forward for long-range quantum communication. Using single-photon discrete-variable quantum states, this exciting new development proves beyond any doubt that all of the quantum protocols previously deployed over limited ranges in terrestrial experiments can in fact be translated to global distances via the use of low-orbit satellites. Hence, they survey the imminent extension of space-based quantum communication to the continuous-variable regime - the quantum regime that is deemed to be most closely related to classical wireless communications. The continuous variable (CV) regime offers the potential for increased communication performance, and represents the next major step forward for quantum communications and the development of the global quantum Internet.

VII. Miscellaneous

Power line communication (PLC) has been attracting worldwide interests because of demands related to emergent and heavily dependable data communication applications, such as Smart Things, multimedia, in-home and in-vehicle networks. The use of PLC technology allows data communication over preexistent and ubiquitous electrical wiring infrastructure. In the literature, the majority of research efforts in PLC has been focused on the physical layer in order to deal with issues related to the communication medium. On the other hand, although there are interesting works regarding the PLC Medium access control (MAC) sublayer, appealing research topics are still available in order to meet the demands associated with cyber physical systems that need to mitigate unfairness in resource sharing, collisions and starvation, among other issues which may degrade data communication quality. In this sense, the paper titled “Medium Access Control Protocols for Power Line Communication: A Survey” by Roberto Oliveira, Alex Vieira, Haniph Latchman, and Moises Ribeiro provides a comprehensive survey regarding the state of the art of MAC protocols for PLC systems, including an overview of existing PLC MAC research results and an organization of current PLC MAC protocols in terms of type of protocols, applications, and main research focus. Moreover, the survey presents modern PLC technologies and standards, highlighting their MAC sublayer characteristics and providing a detailed comparative analysis of PLC MAC protocols in the context of current and emerging PLC applications. Finally, future trends are identified within the scope of the MAC sublayer for PLC systems with a view to stimulating additional research efforts on PLC MAC design.

Modern networks have grown increasingly complicated. Hundreds of devices perform complex network functions to realize a variety of user customized policies (e.g., “Traffic from A to B always traverse a waypoint”). Configuring and deploying such a network are quite challenging and hence error-prone. Violations of intended policies can compromise network availability and reliability. Network operators need to ensure that their policies are correctly implemented by systematically reasoning their network. This has inspired a research field, network verification and testing. In addition, techniques ranging from formal modeling to verification have been applied in this field to help build theoretical foundation. Inspired by the success, network verification and testing have recently attracted increased attention in academic and industrial communities. In this context, the paper titled “A Survey on Network Verification and Testing With Formal Methods: Approaches and Challenges” by Yahui Li, Xia Yin, Zhiliang Wang, Jiangyuan Yao, Xingang Shi, Jianping Wu, Han Zhang, and Qing Wang presents a survey. First, the paper starts by providing an overall landscape of network verification and testing. Then, it provides a brief introduction of formal methods and an overview of techniques in the area to give guidelines for researchers to understand the literature. Following that, it provides detailed introduction of the progress in data plane verification, control plane verification, data plane testing, and control plane testing. Furthermore, the paper provides a comprehensive comparison of network verification and network testing. Finally, it discusses the challenges and a range of potential research directions in this area.

Following a tremendous pace of development, semiconductor technology is approaching atomic-scale integration. This facilitates the implementation of ever more sophisticated multi-media signal processing algorithms without unduly increasing the size of a single chip, but the downside is that quantum-effects begin to prevail. Hence, dealing with the quantum-effects becomes inevitable. Inspired by this, as well as by the promising benefits of the emerging quantum computing paradigm, a substantial multidisciplinary momentum has been gathered by the research community across the fields of quantum physics, electronics, computer science, material science etc. The main challenge is however that the fragile quantum states are prone to the deleterious effects of de-coherence, which results both bit-flips and phase-flips of the quantum-bits representing the quantum-domain operands of both quantum computing and quantum communications. Hence in duality to the classical error correction codes of almost all classical communication and storage systems, the employment of quantum codes is vital for mitigating the effects of quantum flips. Against this background, the paper titled "Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples" by Zunaira Babar, Hung Viet Nguyen, Panagiotis Botsinis, Dimitrios Alanis, Daryus Chandra, Soon-Xin Ng, and Lajos Hanzo surveys the recent advances in quantum coding. The authors demonstrate that Quantum Error Correction Codes (QECCs) can be constructed from the known classical coding paradigm by exploiting the inherent isomorphism between the classical and quantum regimes'. They also address the challenges imposed by the strange laws of quantum physics. In this spirit, this paper provides deep insights into the duality of quantum and classical coding theory, hence aiming for bridging the gap between them. Explicitly, they survey the rich history of both classical as well as quantum codes. Then they provide a comprehensive low-paced tutorial for constructing stabilizer-based QECCs from arbitrary binary as well as quaternary codes, as exemplified by the family of dual-containing and non-dual-containing Calderbank-Shor-Steane (CSS) codes, non-CSS codes and entanglement-assisted codes. Finally, they extend their discussions to a pair of popular code families, namely to the family of Bose-Chaudhuri-Hocquenghem (BCH) as well as to convolutional codes and provide detailed design examples for both their classical as well as their quantum versions.

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