Editorial: Second Quarter 2019 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS

I WELCOME you to the second 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 "Wireless and Cellular Communications," "Vehicular Communications," "Optical Communications," "Network Virtualization," "Internet of Things," "Network Security," and "Internet Technologies." A brief account for each of these papers is given below.

I. WIRELESS AND CELLULAR COMMUNICATIONS

The exponential growth of new wireless communication technologies and multimedia contents, together with the development of very efficient and high-performing mobile terminals, require ever more sophisticated ad-hoc strategies for the massive multicast and broadcast distribution of multimedia contents and applications. The strategies proposed on this topic in the recent literature aim to reach several ambitious goals, like the guarantee of stringent Quality of Service (QoS) requirements, the maximization of spectral efficiency and throughput, and the minimization of delay and losses, at the same time exploiting at best the capabilities of present and future mobile systems. In this framework, the paper titled "Multicast and Broadcast Services over Mobile Networks: A Survey on Standardized Approaches and Scientific Outcomes" by Domenico Striccoli, Giuseppe Piro, and Gennaro Boggia presents a survey of the baseline approaches and the novel strategies on the multicast and broadcast multimedia content distribution over last-generation mobile networks. The paper analyzes many aspects, like network architectures, analytical models, optimization strategies and algorithms, at different layers of the protocol stack. Furthermore, the paper discusses the lessons learned on the main research topics. The survey concludes with a discussion of the key challenges and open issues to be tackled by future research.

The presence of wireless communication technologies is increasing significantly, especially because of the rise of the Internet of Things (IoT). Given many of these technologies compete with one another in the same shared environment and have limited number of license-free Industrial, Scientific, and Medical (ISM) radio bands, the proper employment of wireless Medium Access Control (MAC) protocols is essential to guarantee efficient and reliable wireless communication. Over the last decade, wireless MAC protocols have been proposed as typical hardware-specific implementations, designed as a single building-block where the data-link layer is tightly coupled with the Physical Layer (PHY). Despite the wide range of wireless MAC protocols, the many heterogeneous requirements and the inability to interact with such implementations in an easy and efficient way imply that there is no one-size-fits-all solution. Given the rise of SDRs and the Software-Defined Networking (SDN) paradigm, also in the wireless domain, the popularity and usage of programmable MAC protocols are expected only to increase. In this context, the paper titled "Survey on the Programmability of Wireless MAC Protocols" by P. H. Isolani, M. Claeys, C. Donato, L. Z. Granville, and S. Latré presents a survey that investigates and highlights the challenges of the state-of-the-art on the programmability of wireless MAC protocols. In addition, the survey provides an overview of the evolution from small/limited MAC parameter configurations to the design of a complete software-defined MAC layer.

The theory of compressive sensing (CS) was initially established by Donoho, Candes, Tao, *et al.* in 2004. It is a new signal sampling theory, showing that a sparse signal can be recovered from far fewer samples than the number of samples required by the traditional Shannon-Nyquist sampling theory. CS has widespread applications in various fields, such as wireless communications, since the inherent characteristics of CS are more suitable for the sparse channel impulse response than the Shannon-Nyquist sampling theory. Specifically, CS can be regarded as a cryptosystem when a random measurement matrix is used as a key. This kind of intrinsic cipher feature makes it receive much attention in secure wireless communications. In this context, the paper titled "Secure Wireless Communications Based on Compressive Sensing: A Survey" by Yushu Zhang, Yong Xiang, Leo Yu Zhang, Yue Rong, and Song Guo, presents a detailed review on secure wireless communications based on CS. It firstly introduces different CS cryptosystems according to the types of random measurement matrices including Gaussian matrix, circulant matrix, and other special random matrices. Then, based on these CS cryptosystems, the paper reviews secure wireless communications from different communication scenarios, including wireless wiretap channel, wireless sensor network, Internet of Things, crowdsensing, smart grid, and wireless body area networks.

With a multitude of different wireless technologies being developed for IoT and broadband services, an increasing number of spectrum bands are being targeted by multiple wireless technologies, for example: the 5 GHz unlicensed band where

Digital Object Identifier 10.1109/COMST.2019.2913929

LTE was recently proposed to operate alongside Wi-Fi; the 3.5 GHz Citizens Broadband Radio Service (CBRS) band in the U.S. which is opening to more technologies; and the 2.3–2.4 GHz band under the Licensed Shared Access (LSA) framework in Europe. In such emerging heterogeneous deployments, there will be an increased level of interference and higher complexity of interactions. Spectrum sharing mechanisms have to cope with this and should thus be carefully designed, in order to efficiently utilize the spectrum. In this context, the paper titled "Survey of Spectrum Sharing for Inter-Technology Coexistence" by Andra Voicu, Ljiljana Simić, and Marina Petrova presents a survey of spectrum sharing with a focus on coexisting technologies with equal spectrum access rights. First, the technical and non-technical aspects that affect the spectrum sharing mechanism design are classified based on a technology circle, giving a system-level view. Next, this classification is used to review the literature on inter-technology coexistence within different regulatory frameworks: primary/primary, secondary/secondary, and coexistence in a spectrum commons. Finally, the survey identifies and discusses key future research challenges for inter-technology coexistence such as: network-wide aspects of PHY-layer interference management techniques, coexistence among more than two dominant technologies, robustness of optimized solutions in practice, flexible testing platforms, and network coordination.

Intra-Body Networks promise new possibilities for advanced medical procedures and commercial applications by establishing Intra-Body Communication (IBC) links between embedded/on-body sensors and external relays/data aggregators. Traditional implementations rely on RF-based approaches. However, the use of non-RF techniques has gained traction as viable alternatives for leveraging the body as a medium. The most commonly studied methods include: Ultrasound (acoustic-based), Capacitive Coupling, the propagation of near electric fields around and through the body, Magnetic Resonant Coupling, transmission and reception of magnetic energy via loosely coupled coils wrapped around parts of the body and Galvanic Coupling (waveguide-based), the coupling of low-level current into the body via electrodes. In this context, the paper titled, "Comprehensive Survey of Galvanic Coupling and Alterative Intra-Body Communication Technologies", by William Tomlinson, Stella Banou, Christopher Yu, Milica Stojanovic, and Kaushik Chowdhury, presents a survey where various physical layer properties of the aforementioned IBC solutions are analyzed. Metrics include operating frequency, attenuation, channel characteristics, power consumption, data rate, communication distance, and safety limitations in the body. No specific IBC is superior for all performance metrics, but each offers its own set of trade-offs that influence application choices. Furthermore, potential use cases and open research challenges are presented for Galvanic Coupling.

The stringent requirements of Public Protection and Disaster Relief (PPDR) voice services are met by the legacy public Safety Networks (PSNs) which are based on Land Mobile Radio (LMR) technologies. However, due to their limitations in supporting broadband services, the need for migration toward new technologies has emerged. Due to the current massive advancement in LTE technologies, it is considered as a very promising candidate to serve the striving, tightly-constrained needs of PSNs. LTE-based PSNs may replace LMR technologies due to their capability of running broadband emergency services, scalability, interoperability, availability of huge LTE market, for infrastructure and spectrum sharing, among others. However, there are a few barriers facing the deployment of LTE-based PSNs. PSNs have to be designed to carry both mission-critical (during emergencies) and non-mission-critical (during relief) communications. The commercial LTE originally is not designed for high reliability which is the essence of mission-critical operations. Also, earlier LTE releases are not optimized for voice communications as compared to LMR systems. In this regard, 3GPP (the 3rd Generation Partnership Project) has been working to converge LTE services to PSNs. Starting from LTE release 14, many enhancements have been made such as the provision of proximity services and group communication. In this context, the paper titled "LTE-Based Public Safety Networks: A Survey" by Abdallah Jarwan, Ayman Sabbah, Mohamed Ibnkahla, and Omneya Issa presents a survey of recent research efforts and advancements of LTE-based PSNs. Future research areas such as rapid emergency deployment, spectrum management, priority management, and radio resource management are discussed. Also, a simulation environment is developed using NS-3 to facilitate and enable realistic evaluation of future LTE-based PSNs.

Energy unavailability is one of the limitations of Wireless Sensor Networks (WSNs). Traditionally, batteries have been used to provide power to the sensor nodes and having a limited lifetime affecting the operation time of the network. Different solutions have been proposed to solve this problem by focusing on the maximization of the available energy in a WSNs. The proposed solutions are oriented to the development of techniques that act at the physical and data-link layers; such is the case of the Medium Access Control protocols (MAC). The MAC protocols are one of the widely studied and implemented solutions due to their capability to balance between energy conservation and critical network parameters such as throughput, latency, collision reduction, and control messages. In this context, the paper titled "Improvements of Energy-Efficient Techniques in WSNs: A MAC-Protocol Approach" by Vanessa Quintero, Claudio Estevez, Marcos Orchard, and Aramis Pérez presents a survey where the authors study the ability of MAC protocols to adapt to new working conditions while incorporating new technologies such as Energy Harvesting Devices (EHD), the addition of information that can be obtained from the battery and how the Duty Cycling (DuC) mechanism can be adjusted with the purpose of increasing energy efficiency and extending the network lifetime.

It is no longer science fiction to harness the benefits of quantum computing and signal processing - the global quantum-race is on, given its huge potential and economic and scientific impact. Scientists from the University of Science and Technology China in Hefei have established satellite-based quantum entanglement distribution over a record-distance of

1200 km. The Canadian company D-Wave has sold its quantum annealing computer to several major stake-holders and both IBM as well as Google are also testing their own quantum computers. One of IBM's quantum platform has also been made available for collaborative research in the cloud upon application. The University of New South Wales in Sydney has received a 75 Million Australian Dollar government grant and an even higher momentum has been built up at the University of Waterloo in Canada. In Europe, Gunther H. Oettinger, Commissioner for the Digital Economy and Society outlined the plan to launch a 1 Billion Euro flagship initiative on quantum technology. As part of this momentum, the EU's QUANTERA project coordinates the quantum research of 26 countries. The British Government has also invested 300 Million GBP into the so-called quantum hubs. Given this global momentum, this survey entitled "Quantum Algorithms for Wireless Communications" by Botsinis, Alanis, Babar, Nguyen, Chandra, Ng and Hanzo investigates the employment of quantum computing for solving large-scale search problems in wireless communication systems. By exploiting the inherent parallelism of quantum computing, quantum algorithms may be invoked for approaching the optimal performance of classical wireless processes, despite their reduced number of cost-function evaluations. In this contribution, authors discuss the basics of quantum computing using linear algebra, before presenting the operation of the major quantum algorithms, which have been proposed in the literature for improving wireless communications systems. Furthermore, they investigate a number of optimization problems encountered both in the physical and network layer of wireless communications, while comparing their classical and quantum-assisted solutions. Finally, they state a number of open problems in wireless communications that may benefit from quantum computing.

II. Vehicular Communications

The development of advanced sensor technologies such as LIDAR, Radar, and camera inaugurated a new era in autonomous driving. However, various advanced sensors equipped on autonomous vehicles have intrinsic limitations, such as unreliability of decision making by sensors' alone, infeasibility of sensors' restricted perception capacities and operating conditions, as well as inefficiency of the persistent pursuit of high precision and expensive sensors. At this point, networking and communication technologies can greatly make up for sensor deficiencies, and are more reliable, feasible and efficient to promote the information interaction, ultimately greatly improve the perception and planning capabilities of autonomous vehicles. In this context, the paper titled "Networking and Communications in Autonomous Driving: A Survey" by Jiadai Wang, Jiajia Liu, and Nei Kato presents an overview of the networking and communication technologies in autonomous driving from two aspects: intra- and inter-vehicle. The paper also elaborates on the new trends of communication technologies in autonomous driving. Finally, the paper investigates the verification methods as well as the challenges and open issues, which are convenient for researchers to refer to and carry out further studies.

Autonomous car technology has gained a lot of interest from both academia and industry. As a result, many prototype versions of this technology are pervading our roads for test drives. The commercialization of this technology is still speculative. However, in the past few years, we have witnessed significant investments into research and development and commercialization of this technology. The autonomous car technology leverages research results from multiple disciplines such as computer science, electrical engineering, and mechanical engineering, and it includes different core components such as detection, prediction, vision, perception, planning, and actuation. All these features must work together seamlessly to enable the operations of the autonomous car. Additionally, complex algorithms that see, perceive, and decide on different functions of the car such as moving, accelerating, decelerating, stopping, and so on are also used. This complex mechanism of the autonomous car technology requires an in-depth study of all the components of the autonomous car. Furthermore, it is also necessary to review the recent advances of this technology. In this context, the paper titled "Autonomous Cars: Research Results, Issues, and Future Challenges" by Rasheed Hussain and Sherali Zeadally presents a comprehensive survey that covers almost every aspect of the autonomous cars. This work surveys the current state-of-the-art solutions for different components of the autonomous car. The paper starts with the advantages of autonomous car technologies and then describes in detail the components that together constitute an autonomous car. Then it discusses current solutions that have been proposed to date for the autonomous car covering a wide range of fields such as computer vision, machine and deep learning, communication, and control. The paper also discusses the future technical, non-technical, social, and economical research challenges.

The advent of next generation intelligent vehicles has enabled the vehicles to communicate with each other and passengers that are travelling through these vehicles are able to communicate with each other and can also obtain information by querying the vehicles which are in the near proximity. This gives rise to the vehicular social networks and also gives rise to the issues that are related to the security and privacy. The topology of these networks is highly dynamic and this can cause threats to the individual privacy. In this context, the paper titled "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions" by Xiaojie Wang, Zhaolong Ning, MengChu Zhou, Xiping Hu, Lei Wang, Yan Zhang, Fei Richard Yu, and Bin Hu presents a comprehensive survey on the dissemination of the content in the vehicular social networks. The paper also documents the security and privacy issues that are faced in these networks and also surveys the solutions to these problems. The paper distinguishes between the mobile social networks and the vehicular social networks and classifies the security and privacy issues on the basis of features. The paper concludes with the open research issues and challenges in this domain.

III. Optical Communications

Free Space Optical (FSO) communication technology, also known as Optical Wireless Communications (OWC) is a

technology that is sometimes seen as an alternative to existing technologies, such as radio frequency. In other cases, FSO is considered as a strong candidate to complement and integrate with next-generation technologies, such as 5G wireless networks. Accordingly, FSO technology is being widely deployed in various indoor (e.g., data centers), terrestrial (e.g., mobile networks), space (e.g., inter-satellite and deep space communication), and underwater systems (e.g., underwater sensing). As the application portfolio of FSO technology grows, so does the need for a clear classification for FSO link configurations. In this context, the paper titled "Classification Framework for Free Space Optical Communication Links and Systems" by Abdelbaset Hamza, Jitender Deogun, and Dennis Alexander presents a survey that aims to give researchers a jump-start to tap into the growing and expanding realm of the FSO technology in different environments. The paper proposes a multi-level classification framework to classify existing and future indoor, terrestrial, space, underwater, and heterogenous FSO links and systems using common and simple unified notation. The proposed classification is then used to summarize major experimental work, systems, and standards in the area. It is also envisioned that the proposed classification can be used as a unified framework to define different FSO channel models for future standards and simulation tools.

The increasing complexity of modern optical communication networks has motivated researchers and practitioners to investigate new and enhanced techniques for system automation and optimization. Such increase in complexity is required to support the new services envisioned for 5G and beyond, which are highly dynamic and require unprecedented performance in terms of throughput, latency and reliability. At the networking and physical layers, this translates into the need to make dynamic adjustments to a high number of parameters (e.g., routing configurations, modulation format, symbol rate, coding schemes, etc.), which often need to be carried out live, while the network is operational. Considering the high volumes of data available in current optical networks, advanced mathematical approaches such as those derived from the Machine Learning discipline are the enablers for extracting meaningful information from data and allowing operators to perform complex network tasks automatically. Among these, we envision failure management, traffic prediction, network performance monitoring and estimation of the quality of transmission as major tasks to be addressed. In this context, the paper titled "An Overview on Application of Machine Learning Techniques in Optical Networks" by Francesco Musumeci *et al.* provides an overview and classification of the different use cases for Machine Learning in optical networking. The paper also contains an introductory tutorial on Machine Learning for researchers and practitioners interested in this field and identify some possible new research directions to stimulate further investigations.

IV. Network Virtualization

Technologies such as cloud computing, network function virtualization, and software defined networking will accelerate the upbringing of 5G. It will allow to accommodate the wide range of use-cases targeted by 5G and beyond generation networks, and meet the diverse and sometimes conflicting requirements. In particular, under the network softwarization paradigm, isolated, programmable, and service-customized networks known as network slices can be deployed on top of a common physical infrastructure. This is referred to as network slicing, and it requires the implementation of efficient virtual resource planning mechanisms. In this vein, the paper titled "A Survey on the Placement of Virtual Resources and Virtual Network Functions" by Abdelquoddouss Laghrissi and Tarik Taleb, presents a survey that provides an overview on the main concepts, use cases, and technologies of network virtualization with a focus on virtual network functions (VNFs) and virtual machines (VMs). It also elaborates on the most relevant and recent approaches conceived for the placement of VNFs and VMs. Finally, it draws a broader view on the key challenges, lessons learned, and open research venues to be tackled by the research community.

Computer networks, such as datacenter networks, enterprise networks, and Internet Service Providers' networks, have become a critical infrastructure of the information society. In order to cope with and to optimize for network dynamics (e.g., policy changes, evolving traffic patterns, and failures), networks have to embrace changes. By offering programmability, Software-Defined Networking (SDN) facilitates updating networks' behavior. SDN however does not imply that networks keep meeting their strict requirements (i.e., in terms of correctness, availability, and performance) during their updates. In this context, the manuscript "Survey of Consistent Software-Defined Network Updates" by Klaus-Tycho Foerster, Stefan Schmid, and Stefano Vissicchio presents a survey of mechanisms and protocols to provide consistent and efficient network updates. Their paper identifies and discusses different consistency properties, as well as the corresponding algorithmic techniques to meet them. Moreover, the relationship to classic optimization problems is investigated, as well as tradeoffs between update speed and cost. Even though the survey is motivated by Software-Defined Networks, the underlying issues are not new, and the authors provide a historical perspective on the network update problem.

Broadband access network technologies have been consistently evolving over the last few years, with a considerable increase in upstream and downstream speeds, as well as substantial improvements in terms of latency reduction. For telecom service providers, this evolution has led to the development of new services for residential networks (such as N-Play services). However, this service delivery model is still largely supported by the use of physical Residential Gateways, which often constitute an obstacle, due to reliability or cost issues, sometimes to the point of hampering the introduction of new services. In the meantime, the current trend towards the introduction of service and network virtualization technologies has pushed operators to consider virtualizing the devices in the customer network, including the residential gateway and the services it provides. In this context, the paper titled "Virtualization of Residential Gateways: A Comprehensive Survey" by Jorge Proença, Tiago Cruz, Paulo Simões, and Edmundo Monteiro presents a survey covering past and current

developments concerning the implementation of the virtualized Residential Gateway (vRGW) concept. This survey covers several different aspects, such as the strategies documented by industry players, research work, and initiatives from standardization bodies. The paper also details some of the developments that may ease the introduction of the vRGW, such as network or node virtualization performance enhancements, and hardware acceleration mechanisms. Finally, the authors also propose a taxonomy to classify and organize the surveyed proposals.

Software Defined Network (SDN) facilitates network management and enables efficient programming by improving network performance and monitoring capabilities, which has been proven successful in many scenarios. Attracted by these advantages, enterprises and governments have strong motivations to deploy SDN. However, the significant deployment costs, the difficulties in hiring professional SDN programmers and the complexity of OpenFlow protocol slow down the SDN deployment step, which promotes the birth of the hybrid SDN network. Hybrid SDN network combines the robustness of traditional protocols with the flexibility of SDN while avoiding their limitations and incompatibility. In this context, the paper titled "A Survey of Deployment Solutions and Optimization Strategies for Hybrid SDN Networks" by Xinli Huang, Shang Cheng, Kun Cao, Peijin Cong, Tongquan Wei, and Shiyan Hu presents a tutorial and survey. First, the paper gives an overview of the model and background of hybrid SDN networks. Then, the paper describes how to seamlessly unify a traditional network with an SDN network from perspectives of the control plane and the data plane, respectively. Furthermore, the paper compares some typical optimization strategies and traffic engineering algorithms in hybrid SDN networks. Finally. the paper summarizes some application scenarios and discusses the future research and development trend.

Both as the decentralization paradigm, blockchain guarantees the immutability and security via the consensus among the validating peer nodes, and the edge computing enables mobility support, location awareness and low latency by pushing resources and services to the distributed edge of networks. These different advantages of blockchain and edge computing directly lead to their complementary roles to each other. The incorporation of blockchain into edge computing enhances security, privacy and the automatic resource usage by adapting to the coordination, heterogeneity and mobility at the edges but avoiding the excessive encryption overheads, while edge computing brings the powerful decentralized network, rich computation and storage resources to the scalability enhancement of blockchain. In this context, the paper titled "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges" by Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang presents a tutorial and survey. First, the paper gives an overview of blockchain and edge computing, and then presents the motivations and requirements of the integration of blockchain and edge computing. Furthermore, the paper discusses the frameworks of the integrated system and its realization of the network security, data integrity and computation verification. Finally, the paper discusses the significant research challenges of the integrated system, and explores the broader perspectives.

V. Internet of Things

The growth of new sensing and wireless communication technologies has led to various smart sensing systems that are becoming an important part of smart cities. These smart sensing systems can provide different monitoring applications in a city with timely information to support the decision making and the assets management to meet the demand of high living quality of the citizens. The monitoring performance depends on where and how the smart sensing devices make the measurements. It turns out that the deployment of the smart monitoring systems during the configuration phase and the management of the systems during the running phase are important to the sensing in smart cities. In this context, the paper titled "The Sensable City: A Survey on the Deployment and Management for Smart City Monitoring" by Rong Du, Paolo Santi, Ming Xiao, Athanasios V. Vasilakos, and Carlo Fischione presents a survey on smart city sensing. First, the paper overviews the supporting infrastructures and technologies for smart city monitoring systems. Then, the paper elaborates on various approaches for the deployment and the sensing management of the monitoring systems, and presents and analyzes the current real-world systems for different smart city monitoring applications. Finally, the paper discusses the challenges and open problems to be tackled by future studies.

Low-power wide-area networks (LPWANs) are a kind of network that are used to connect things to the Internet from a wide variety of sectors. These technologies provide Internet of Things (IoT) devices with the ability to transmit short messages over long distances, while considering the minimum energy consumption. IoT applications will cover a wide range of human and life needs, from intelligent environments (cities, homes, transportation, etc.) to health and quality of life. LPWAN technologies can be divided into two classes: the unlicensed frequency band (LoRa, DASH7, SigFox, Wi-SUN, etc.) and the licensed frequency band standards (NB-IoT, LTE Cat-M, EC- GSM-IoT, etc.). In general, both types of standards only consider fixed interconnected things, and less attention has been given to the mobility of the devices. In this context, the document entitled "Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility" by Wael Ayoub presents a proof that addresses the mobility of things and connectivity in each of the three LPWAN standards: LoRaWAN, DASH7, and NB-IoT. In particular, the paper shows how the mobility of things can be achieved while transmitting and receiving data. Then, it provides a general and technical comparison for the three standards. Finally, it illustrates several application scenarios where mobility is required and shows how to select the most appropriate standard. Finally, it addresses the challenges and perspectives of research.

As the Internet of Things (IoT) has become an integral part of our lives, with applications ranging from smart homes and healthcare to industrial automations and smart cities, the security of IoT networks has become more and more crucial. One

of the major concerns for many researchers is the security of the routing process in IoT networks. The Routing Protocol for Low Power and Lossy Networks (RPL) is the most investigated routing protocol as it became the standard for routing in many IoT environments and applications. The Internet connectivity of IoT networks exposes them to traditional routing attacks, and the design of RPL to meet the resource-constraint nature of IoT devices has introduced its own set of attacks. In this context, the paper titled "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things", by Ahmed Raoof, Ashraf Matrawy, and Chung-Horng Lung presents a survey on the most current routing attacks on RPL and their mitigation methods. It starts with a detailed review of RPL standard, then moves to discuss recently published attacks on RPL-based networks and their mitigation methods. In addition, the paper introduces a first-of-its-kind classification scheme for the mitigation methods of RPL's attacks based on the techniques used for the mitigation. Furthermore, a thorough discussion of RPL-based Intrusion Detection Systems (IDSs) and a classification of those recent IDSs is presented.

Despite numerous attempts to optimize routing in IoT, RPL has been found by numerous studies to suffer from several issues regarding efficiency and deployment. Hence, several enhancements/extensions for RPL have been made. However, the extent to which such enhancements have succeeded in addressing the reported limitations of RPL has not been thoroughly assessed before. In this context, the paper titled "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations" by Baraq Ghaleb, Ahmed Al-Dubai, Elias Ekonomou, Ayoub Alsarhan, Youssef Nasser, Lewis Mackenzie, and Azzedine Boukerche comprehensively reviews research proposals aiming at augmenting RPL investigating where such proposals still fall short, the challenges and pitfalls to avoid in the development of further successful extensions. The survey found that research attempts in this context have mostly fallen short in tackling RPL's limitations and, thus many issues that were supposed to be solved by such proposals remain open for research. The survey shows that the memory limitations in the storing mode of RPL, and the long source headers in non-storing mode have not been efficiently addressed. Besides, the extensions targeting the load-balancing issue of RPL suffer from the instability problem. Finally, the survey has found that a high percentage of reviewed articles have serious pitfalls that undermine achieving the sought objectives, and thus, need to be avoided in the development of further extensions including the unrealistic operation conditions, the absence of real large-scale testbeds evaluations, the under-specification of metric-composition, and the greater complexity induced by some proposed solutions.

The ubiquitous use of IoT technologies for ease in control and monitoring can be observed today in every walk of human life ranging from eHealth to industrial control systems. Such a dependence on IoT is no doubt beneficial, but at the same time being connected to the Internet, the IoT devices are vulnerable to numerous threats at various layers of IoT architecture. Any such successful attack can cause significant security and privacy issues. Correspondingly, the successful launch of some sophisticated cyber-attacks such as NotPetya, Mirai, DuQu2, and Stuxnet on Industrial Control Systems have rendered existing IoT security protocols ineffective. Similarly, the lack of attention to IoT device security by the manufacturers is also one of the contributing factors towards IoT vulnerabilities. In this context, the paper titled "Anatomy of Threats to the Internet of Things" by Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, and Wei Ni presents a tutorial and survey on a range of vulnerabilities and threats at various layers of IoT architecture. The paper also carries out a diligent analysis on the methodology of various IoT threats especially malware attacks, and also presents a defense in depth approach to protect IoT systems. The survey concludes with a summary of IoT security issues; lessons learned and the gist of open research challenges.

Blockchains, the distributed ledger technology, are a great contribution to the vision of decentralized networking environments where no central trusted authority is required to govern and authorize communications between two participating peers. Having proved its mettle in the domain of digital finance, blockchains are now attracting research attention for decentralizing and securing the Internet of Things (IoT). By eliminating the need for central intermediaries for providing IoT services, blockchains have the potential to enhance the security and privacy of IoT edge communications, as well as to introduce new business models for IoT service provisioning. Currently, however, there are significant challenges to integrating blockchains with the IoT, which researchers are endeavoring to address. In this context, the paper titled "Applications of Blockchains in the Internet of Things: A Comprehensive Survey", by Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Rehmani, presents a survey which aims to paint a coherent and comprehensive picture of the state-of-the-art in integrating blockchains with the IoT. First, the paper starts with discussing the working principles of blockchains and how their inherent properties of immutability, decentralization, security, and auditability can benefit the IoT. From there, the paper delves into the challenges faced by researchers in this area, along with discussions on the recent research efforts made to meet these challenges. Additionally, the paper outlines future research directions towards developing a decentralized, secure medium for the IoT.

VI. Network Security

Smart cities have emerged due to advancements in the Internet of Things and communication technologies. They provide new grounds for the optimization of the available resources in the cities and are capable of improving the lifestyle and quality of living for the citizens. Smart cities can improve the transportation system of a city as well as its energy consumption, education, and decision making. With all these advantages, the smart cities also pose a considerable threat to the security and privacy of citizens and there are many issues that arise due to this. In this context the paper titled "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges" by Mehdi Sookhak, F. Richard Yu,

and Helen Tang categorizes the developments that are being carried out currently and that will be carried out in the future. The paper also presents a survey all the issues related to the security and privacy of a smart city. The paper also provides requirements that are needed for the design of a secure city and concludes with the open research issues in this area.

The impacts of a cybersecurity incident, such as data breach, financial loss, and reputation damage have been a long-lasting threat to organizations, governments, enterprises and individual users, which motivates the crowd to understand and defend against cybersecurity incidents. The increasing number and high-quality incidents related data provides the opportunity to proactively predict cybersecurity incidents before damage occurs. Both the security community and industrial circles are pursuing and proposing cybersecurity incident prediction schemes with the help of aggregating various data sources. Hence, we are witnessing the shift from primarily reactive detection to proactive prediction. In this context, the paper titled "Data-Driven Cybersecurity Incident Prediction: A Survey" by Nan Sun, Jun Zhang, Paul Rimba, Shang Gao, Leo Yu Zhang, and Yang Xiang presents a survey, where the paper overviews the outlook of cybersecurity incident prediction with a focus on utilized data and presents the methodology commonly adopted in this emerging field. Furthermore, the survey discusses a range of challenges and future directions in cybersecurity incident prediction.

Physical layer security (PLS) has arisen as a novel concept that can integrate and may even substitute encryption-based schemes, which suffer from many drawbacks and practical issues in future wireless systems. The essential idea of PLS is to utilize the characteristics of the wireless channel including randomness, spatial decorrelation, diversity, etc. along with its impairments including noise, fading, interference, dispersion, etc. to guarantee confidential data transmission to the legitimate users only against unintended receivers (eavesdroppers). In this context, the paper titled "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey" by Jehad Hamamreh, Haji Furqan, and Huseyin Arslan presents an inclusive tutorial and survey that can help solidify and deepen the understanding of the big picture of physical layer security. Particularly, the paper comprehensively classifies the existing physical layer security techniques against wireless passive eavesdropping into fundamental domains. For each domain, several examples are given and illustrated along with reviewing the most recent security advances. Moreover, the lessons learned, advantages, and disadvantages of each technique are discussed to give an insight on the trade-off among security and the other communication requirements. The paper then reviews and discusses the recent applications of PLS techniques into emerging technologies such as VLC, BAN, IoT, PLC, smart grid, mm-Wave, cognitive radio, VANET, UAV, UWB, D2D, RFID, index modulation, and 5G-NOMA systems. The paper finally concludes with recommendations and future research directions for designing robust, strong security methods for current and future wireless systems.

With the ever-growing number of connected devices, wireless communication technologies have become an indispensable part of our everyday lives. Meanwhile, due to their open nature, wireless networks are prone to eavesdropping attacks. Traditionally, protecting confidentiality of data transmission is addressed via computational security (e.g., public key cryptography). However, the proliferation of wireless ad-hoc networks without a centralized infrastructure has spurred the demand for development of device-centric solutions for security. In this context, physical layer security has emerged as a promising alternative or complement to the conventional cryptographic solutions. The paper titled "An Overview of Physical Layer Security with Finite-Alphabet Signaling" by Sina Rezaei Aghdam, Alireza Nooraiepour, and Tolga M. Duman reviews recent developments on physical layer security with an emphasis on the results with practical assumptions such as finite-alphabet signaling and finite-length codes. First, the paper provides a description of the fundamental concepts in physical layer security including the wiretap channel model and different secrecy metrics. Then, a review of the recent results on secure transmission with discrete signaling and practical coding schemes are presented, and finally, the paper is concluded by providing a summary of the lessons learned and an overview of some directions for future research.

Attacks such as Advanced Persistent Threats (APT) have been one of the major threats that industrial and governmental sectors are facing. The exponential growth of attacks and skillful APT actors make this type of threats difficult to detect and mitigate at early stages. The rate at which the attack tools and techniques are evolving is making any existing security measures inadequate. As defenders strive to secure every endpoint and every link within their networks, attackers are finding new ways to penetrate into their target systems. With each day bringing new forms of malware, having new signatures and behavior that is close to normal, a single threat detection system would not suffice. While it requires time and patience to perform APT, solutions that adapt to the changing behavior of APT attacker(s) are required. In this context, the paper titled "A Survey of Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities" by Adel Alshamrani, Sowmya Myneni, Ankur Chaudhary, and Dijiang Huang presents a survey of the current methods that are used to prepare and launch APT attacks. The paper covers the novel strategies attackers use to perform APT attacks. The paper brings all methods and techniques that could be used to detect different stages of APT attacks, learning methods that need to be applied and where to make your threat detection framework smart and undecipherable for those adapting APT attackers. It also presents different case studies of APT attacks, different monitoring and mitigation methods to be employed for fine-grained control of security of a networked system. The survey concludes with different challenges in defending against APT and opportunities for further research.

With the fast development of information and communication technologies, along with the rapid evolution of heterogeneous wireless access networks, the security issues in wireless information transmission have attracted increasing concerns from both academia and industry. Physical

layer security presents distinctive advantages and promising prospects to cope with the emerging security challenges due to its characteristics of achieving perfect secrecy, low computational complexity and resource consumption, and good adaptation for channel changes. In this context, the paper titled "A Survey of Optimization Approaches for Wireless Physical Layer Security" by Dong Wang, Bo Bai, Wenbo Zhao, and Zhu Han presents a survey on the optimization and design of physical layer security. First, the survey summarizes the research topics on physical layer security designs and discusses the fundamental performance metrics and optimization problems. Furthermore, the survey reviews the state of the art of optimization approaches on each research topic. Then, the survey discusses the impacts of channel state information on the physical layer security designs. Finally, the survey concludes with the observations on potential future directions and open challenges.

Bloom filter (BF) consists of an array of bits and relies on the values of these bits to identify the absence and existence of any queried element. Due to their space efficiency, BF and its variants have been widely employed as a content summarization to support constant-time approximate membership query in the communities of both communications and computer science. In the field of networking, BFs are employed to enable routing and forwarding, Web caching, security enhancement, content delivering, etc. In databases, BFs is a proper option to support query and search, privacy preservation, key-value store, content synchronization, duplicate detection and beyond. In this context, the paper titled "Optimizing Bloom Filter: Challenges, Solutions, and Comparisons" by Lailong Luo, Deke Guo, Richard T. B. Ma, Ori Rottenstreich, and Xueshan Luo presents a tutorial and survey. First, the paper reviews the existing BF variants from the performance and generalization dimensions. To improve performance, BF variants try to reduce false positives and implementation cost. For generalization, the BFs are redesigned with diverse input sets and output functionalities. Furthermore, the paper conducts a comprehensive analysis and qualitative comparison among the existing 60+ BF variants. Finally, the paper highlights the future trends of designing and using BFs.

VII. Internet Technologies

Named Data Networking (NDN) is a promising paradigm conceived for future Internet architectures. Rather than forwarding packets based on their destination addresses in IP, NDN forwards packets based on named data, in which the name is hierarchically structured like URL to facilitate traffic demultiplexing and provides context for data consumption. Therefore, NDN has to imply a substantial re-engineering of forwarding plane in the content router to provide fast name lookup, intelligent forwarding strategy, and effective caching policies. In this context, the paper titled "Packet Forwarding in Named Data Networking Requirements and Survey of Solutions" by Zhuo Li, Yaping Xu, Beichuan Zhang, Liu Yan, and Kaihua Liu presents a tutorial and survey, where it starts by providing more accurate requirements of NDN forwarding plane. Then, the paper elaborates on various prevalent approaches and compares all the schemes proposed for NDN forwarding plane based on the data structure utilized. Moreover, the survey concludes with a comparative discussion that highlights a range of open problems to be tackled by future research.

Internet classification is known as a challenging and attractive topic by practitioners from different fields. On one hand, it is challenging due to the growing of new technologies; that are constantly changing the rules of the game disabling classical approaches. Classical approaches utilize port and payload matching to identify the type of traffic. On the other hand, its interest can be found varied over improving Quality of Service (QoS) and detecting cyber-attacks, among others. Given these arguments more sophisticated techniques and methods are required for Internet traffic classification. Thus, Machine Learning (ML) emerges on this field showing signs of future success becoming a key tool to build traffic classification solutions in real network traffic scenarios. As a result, this paper titled "Towards the Deployment of Machine Learning Solutions in Network Traffic Classification: A Systematic Survey" by Fannia Pacheco, Ernesto Exposito, Mathieu Gineste, Cedric Baudoin, and Jose Aguilar explores the elements that allow ML to work in the traffic classification field. A systematic review is introduced based on the steps to achieve traffic classification by using Machine Learning techniques. The main aim is to understand and to identify the procedures followed by the existing works to achieve their goals. The result of this study is a set of trends that outlines common, challenging and future directions for Machine Learning based traffic classification.

Deep Packet Inspection (DPI) is a network traffic analysis method that is used for various purposes such as traffic classification, intrusion detection, virus and spam filtering, protocol misbehavior detection, or resource management. Within a DPI system (from an architectural viewpoint), the analysis process can be divided up to three phases, which are evolved into substantive research areas in the recent years: packet parsing, packet classification, and payload inspection, respectively. Since on-line DPI requires large amount of processing power in order to analyze high volume network traffic in real time, network bandwidth beyond 10 Gbit/s brings novel challenges for software-based packet inspection solutions. The requirement for hardware assistance of any DPI phase is therefore emerging with the evolution of the core networks. In this context, the paper titled "FPGA-Assisted DPI Systems: 100 Gbit/s and Beyond" by Péter Orosz, Tamás Tóthfalusi and Pál Varga presents a survey that investigates the FPGA acceleration of the DPI phases and presents the state-of-the-art considering 100 Gbit/s networking and beyond. The paper demonstrates the benefits and the drawbacks of stepping towards FPGA-based acceleration for each DPI phase. Authors argue that the hybrid hardware- and software-based architecture can eliminate the capacity bottleneck of the entirely software-based DPI solutions. Besides the detailed presentation of related proposals and scientific results, the best practices are highlighted and explained for each DPI phase.

Science and engineering applications are generating data at an unprecedented rate. From large facilities such as the Large

Hadron Collider to portable DNA sequencing devices, these instruments can produce hundreds of terabytes in short periods of time. While general-purpose networks can transport basic data such as emails and Web content, they face numerous challenges when transferring terabyte- and petabyte-scale data. In response to this challenge, the Science Demilitarized Zone (Science DMZ) has been proposed. The Science DMZ is a network or a portion of a network designed to facilitate the transfer of big science data. The main elements of the Science DMZ include: i) specialized end devices, referred to as data transfer nodes (DTNs), built for sending/receiving data at a high speed over wide area networks; ii) high-throughput, friction-free paths connecting computing systems; iii) performance measurement devices to monitor end-to-end paths; and iv) security policies and enforcement mechanisms tailored for high-performance environments. The article, titled "A Comprehensive Tutorial on Science DMZ" by Jorge Crichigno, Elias Bou-Harb, and Nasir Ghani, reviews fundamental network concepts that have a large impact on Science DMZs, such as router architecture, TCP attributes, and operational security. Then, the tutorial delves into protocols and devices at different layers, from the physical cyberinfrastructure to application-layer tools and security appliances, that must be carefully considered for the optimal operation of Science DMZs. The article also contrasts Science DMZs with general-purpose networks and presents empirical results and use cases.

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