Editorial: First Quarter 2023 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS

I WELCOME you to the first issue of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS in 2023. This issue includes 25 papers covering different aspects of communication networks. In particular, these articles survey and tutor various issues in "Wireless Communications", "Cyber Security", "IoT and M2M", "Internet Technologies", "Network Virtualization", "Network and Service Management and Green Communications", and "Vehicular and Sensor Communications". A brief account for each of these papers is given below.

I. WIRELESS COMMUNICATIONS

Albeit our biased Internet of Things (IoT) perception centered around radio frequency (RF) based terrestrial wireless networks, IoT has recently been extended to challenging communication mediums and extreme environments. RF systems have been regarded as the default means of connectivity even if they are not always the best option under all circumstances. At this very point, optical wireless communication (OWC) technologies can complement, replace, or co-exist with audio and radio wave wireless systems to improve overall network performance. To this aim, the survey by Celik et al. [A1] reveals the full potential of OWC-based IoT networks by providing a top-down survey of four main domains: the Internet of Terrestrial Things (IoTT), Internet of underWater Things (IoWT), the Internet of Biomedical Things (IoBT), and Internet of underGround Things (IoGT). The survey covers each domain with a dedicated and self-contained section that starts with a comparative analysis, explains how OWC can be hybridized with existing wireless technologies, points out potential applications fitting best the related domain, and discusses open communication and networking research problems. Most importantly, instead of presenting a visionary framework, the survey discloses that OWC-IoT has become a reality by listing ongoing proof-of-concept prototyping efforts and available commercial off-the-shelf products.

WiFi sensing offers a novel sensing modality for detecting physical activities without requiring cumbersome wearable sensors or privacy-invasive camera tracking. Utilizing radio-frequency signals from the ubiquitous WiFi enabled devices through our environments, WiFi sensing can enable always-on and non-obstructive sensing and tracking. However, to take full advantage of these pervasive radio-frequency signals, it is important to efficiently process the signal data in realtime at the edge in order to handle the immense volume of signal data available in our environments. Furthermore, improvements in edge hardware such as machine learning accelerators offer advanced computational capabilities which can thus be leveraged towards novel edge WiFi sensing applications. In this context, the paper by Hernandez and Bulut [A2] presents a survey which categorizes the techniques and methods required for developing an end-to-end edge WiFi sensing system. Emphasis is placed into identifying and defining signal processing, data preparation, and on-device prediction making techniques commonly used within WiFi sensing research. Towards achieving a greater understanding of the capabilities of these techniques, the work also evaluates them in the context of both prediction accuracy as well as on-device edge inference speed and energy consumption.

The advent and recent technological advancement in Artificial Intelligence (AI) has found various applications in numerous areas which include the wireless communication systems. As researchers push the frontier and advance the development of more efficient communications systems using AI, new threats and attacks that disrupt AI-enabled systems evolve rapidly. For instance, these attacks may come in the form of small perturbations to the original input of a neural network used to develop the AI-enabled system thus manipulating the operation of the AI system to cause an error in the inference process. These perturbations are not just white noise samples but are specifically crafted to produce a vector in the input feature space that can mislead the developed AI model. In this context, the paper by Adesina et al. [A3] provides a comprehensive review on Adversarial Machine Learning (AML) and its applications in the wireless communications domain as well as the unique properties of wireless adversarial attacks. The paper summarizes recent studies in AML attacks in various application areas in wireless communications such as spectrum sensing, resource allocation and signal classification to provide insightful guidelines and references for future works. Furthermore, this study presents methods for AML attack detection and mitigation in the literature and shares important ideas that can help in the safe adoption of AI-enabled solutions to emerging wireless communications applications in the presence of adversaries.

The next generation of satellite technologies is being characterized by the recent technical progress in the

Digital Object Identifier 10.1109/COMST.2023.3238202

non-geostationary orbit (NGSO) satellites, which offers intriguing novel communication opportunities for providing non-terrestrial connectivity solutions and supporting a wide range of digital technologies from diverse industries. NGSO promises a substantial boost in communication speed and energy efficiency, and thus, tackling the main inhibiting factors of commercializing the conventional geostationary orbit (GSO) satellites for broader utilization. The successful realization of NGSO communication systems is being achieved by the ongoing development efforts and investments, which have indeed pushed the satellite communication potentials towards higher bounds that need to be explored to support the rapid proliferation of various space-based applications and services. In this direction, the paper by Al-Hraishawi et al. [A4] presents a survey on the state-of-the-art NGSO research focusing on the communication prospects, including physical layer and radio access technologies along with the networking aspects and the overall system features and architectures. Beyond this, there are still many NGSO deployment challenges to be addressed to ensure seamless integration not only with GSO systems but also with terrestrial networks. These unprecedented challenges are also discussed including coexistence with GSO systems in terms of spectrum access and regulatory issues, satellite constellation and architecture designs, resource management problems, and user equipment requirements. The survey concludes with a set of innovative research directions and new opportunities for future NGSO research.

As an alternative transmission scheme to orthogonal frequency division multiplexing (OFDM), cyclic prefixed singlecarrier (CP-SC) transmissions have been widely adopted to reduce a high peak-to-average power ratio (PAPR), high sensitivity to inter-carrier interference (ICI) caused by carrier frequency offsets, and sensitivity to spectral nulls due to receiver processing in the frequency domain, which are inherent impairments of OFDM. Furthermore, OFDM is less adaptable to burst transmissions so that CP-SC is more appropriate in environments composed of heterogeneous sensors and devices such as static, mobile, and ad-hoc devices, which is a general system setup for 5G and beyond-5G. For various CP-SC based systems, how to exploit the achievable full diversity in the realistic frequency selective fading channels is the key question in applying CP-SC-based transmissions. In this context, the paper by Kim et al. [A5] presents a tutorial. First, the paper starts by providing the basic concept and operation of CP-SC transmissions. Then, the paper elaborates on various types of diversity that are achievable by CP-SC transmissions, and QR decomposition (QRD)-M-based data detection in the receiver to achieve the diversity. Furthermore, the paper exemplifies various CP-SC based wireless systems for relaying, spectrum sharing, physical layer security, and distributed cyclic delay diversity with accompanying link-level simulations. Finally, the paper discusses potential research directions with CP-SC transmissions in emerging systems.

In the 6G mobile network, environmental sustainability is a critical mission for the system design as the number of devices grows enormously. Besides, it is also essential to evolve the power-saving mechanisms for the user equipment (UE) to extend the battery life. In the 4G era, the 3rd Generation Partnership Project (3GPP) proposed the Discontinuous Reception (DRX) mechanism for the LTE system to solve the power consumption issue for devices with downlink packet call sessions and successfully prolonged the devices' battery life. Consequently, the DRX is regarded as one of the most efficient power-saving mechanisms. However, with the broad deployment of the 5G network, the deteriorating UE power consumption drives the researchers to improve the existing DRX mechanism so that the UEs can support more diverse applications and complicated computations with high transmission rates. In this context, the paper by Lin et al. [A6] presents a tutorial and survey for the DRX mechanism. First, the paper introduced the basic operations of the DRX mechanism and extensions in the 4G and 5G standards. Next, the paper introduced key performance metrics for analyzing the DRX mechanism and summarized the recent work from different system perspectives. Finally, the paper elaborated on new challenges of improving the DRX mechanism and the vision in the 6G network.

In the current traction, Industrial Internet of Things (IIoT) applications are dominantly catered by data or model driven solutions. While these approaches demonstrate promising results, they lack the human intuition, which comes from experience and perspective. Adding such parameters and creating personalized and customized decision pipelines is challenging. Electroencephalography-based (EEG) Brain-Computer Interfaces is a technology that has the potential to decode the intuition of the operator and integrate key inferences into process loops for enhancing conventional solutions. The integration of EEG along with the conventional statistical pipelines will facilitate intelligent model designs that can dynamically learn from the operator and offer flexible as well as accurate decisions on factory floors. In this context, the paper by Ajmeria et al. [A7] presents an exhaustive discussion on EEG, its key signal processing approaches, and its scope of application in IIoT, with detailed deployment architectures. The review highlights the existing challenges of such solutions and proposes possible off-the-shelf strategies for overcoming them. It also presents a case study on a potential deployment performed on lab-scale experiments with a single-channel EEG headset, demonstrating how a minimalistic setup overcomes complex applications like job inspection in manufacturing processes.

With the increasing demand for intelligent services, the sixth-generation (6G) wireless networks will shift from a traditional architecture that focuses solely on a high transmission rate to a new architecture that is based on the intelligent connection of everything. Semantic communication (SemCom), a revolutionary architecture that integrates user as well as application requirements and the meaning of information into data processing and transmission, is predicted to become a new core paradigm in 6G. While SemCom is expected to progress beyond the classical Shannon paradigm, several obstacles need to be overcome on the way to a SemCom-enabled smart wireless Internet. In this context, the paper by Yang et al. [A8] provides a holistic review of the fundamentals of SemCom, its applications in 6G networks, and the

existing challenges and open issues with insights for further in-depth investigations. The paper starts with the motivations and compelling reasons for SemCom in 6G. Then, an overview of SemCom-related theory development is provided. After that, three types of SemCom, i.e., semantic-oriented communication, goal-oriented communication, and semantic-aware communication are introduced. Following that, the design of the communication system is organized into three dimensions, i.e., semantic information (SI) extraction, SI transmission, and SI metrics. For each dimension, the benefit and limitations of the existing techniques, as well as the remaining challenges are discussed. Then, the potential applications of SemCom in 6G and portray the vision of future SemCom-empowered network architecture are presented. Finally, future research opportunities are outlined.

Wireless communication technologies have relied on the radio frequency (RF) spectrum, mostly on the sub-6 GHz and more recently on the millimeter wave spectrum. RF-based wireless networks still face the "spectrum crunch" issue, require high transmit power and have high deployment cost and, as a result, can not support further significant enhancements of the data rate and energy efficiency needed by future generation networks. Visible light communication (VLC) has attracted significant research interest as a promising technology to complement RF networks due to its inherent advantages such as low deployment cost, low energy requirements, and the vast amount of license-free bandwidth. However, the realization of VLC systems continues to be hindered by challenges such as short transmission distance, line-of-sight blockages, and random device orientation. The emergence of reconfigurable intelligent surfaces (RISs) and their potential for optical wireless communications offer several design opportunities to overcome the limitations of VLC systems. Since the design constraints and channel properties of VLC differ from those of RF systems, the community needs to understand the critical differences between RIS-assisted RF and VLC systems. In this context, the paper by Aboagye et al. [A9] presents a tutorial and survey. First, the paper provides an overview of recent developments and standardization efforts in VLC and optical RIS. Then, the paper elaborates on the design of RIS-based VLC systems and the integration of RIS with other emerging technologies in VLC. Finally, the paper discusses a range of promising research directions for future work.

II. Cyber Security

Blockchain technology has attracted a huge attention from both industry and academia because it can be integrated with a large number of everyday applications working over features of modern information and communication technologies (ICT). Peer-to-peer (P2) architecture of blockchain enhances these applications by providing strong security and trust-oriented guarantees. Despite of these incredible features that blockchain technology brings to these ICT applications, modern research have indicated that these strong guarantees are not sufficient enough and blockchain networks may still prone to various security, privacy, and reliability related issues. To overcome these issues, it is important to identify the anomalous behaviour within time. Therefore, nowadays anomaly detection models are playing an important role in protection of modern blockchain networks. In this context, the paper by Hassan et al. [A10] presents a survey regarding integration of anomaly detection models in blockchain technology. For this, we first discuss that how anomaly detection can aid in ensuring security of blockchain based applications. Then, we demonstrate certain fundamental evaluation matrices and key requirements that can play a critical role while developing anomaly detection models for blockchain. Afterwards, we present a thorough survey of various anomaly detection models from perspective of each layer of blockchain to provide readers an in-depth overview of integration that has been carried out till date. Finally, we conclude the article by highlighting certain important challenges alongside discussing that how they can serve as a future research directions for new researchers in the field.

The metaverse is a fully immersive, hyper spatiotemporal, and self-sustaining virtual shared space for humans to play, work, and socialize, which is recognized as an evolving paradigm of the next-generation Internet after the Web and the mobile Internet revolutions. As the metaverse integrates a variety of emerging technologies as its foundation, severe security breaches and privacy invasions (inherited from underlying technologies or emerged in the new digital ecology) during the life-cycle of metaverse services can hinder its wide deployment. Besides, the intrinsic characteristics of metaverse (e.g., immersiveness, hyper spatiotemporality, sustainability, and heterogeneity) can bring about a series of fundamental challenges such as scalability and interoperability in metaverse security provision. In this context, the paper by Wang et al. [A11] presents a survey. First, the paper starts by giving an overview of the architecture, key characteristics, enabling technologies, and modern prototypes of metaverse. Then, the paper presents the taxonomy of security and privacy threats in the metaverse and discusses the critical challenges and existing/potential solutions to resolve them. Finally, the paper discusses a range of open issues to be tackled by future research.

Blockchain is an emerging technology that is considered the key to building trust without a trusted third party due to its decentralization and security features. It is also regarded as an enabler of 6G networks and the Internet of Things to improve network performance and user experience. To have a systematic view of the blockchain running process and explore its intrinsic nature, it is necessary to reveal the relations of the blockchain system with communication, networking, and computing. In this context, the paper by Cao et al. [A12] presents a survey, where the paper revealing the intrinsic nature of blockchain from a methodological perspective. First, it introduces how blockchain works, the research activities and challenges, illustrating the typical blockchain use cases and topics. Then, the article specifies how to adopt the stochastic process, game theory, optimization theory, and machine learning to study the blockchain running processes and protocols/algorithms design. Finally, the paper summarizes the advantages and limitations of this analysis method and points out the remaining problems for future research.

Medical research helps save millions of human lives. Both clinical and epidemiological research requires access to health data to develop and improve treatment methods. To facilitate such research, health data needs to be collected, stored, and shared among different healthcare actors. The employed mechanisms have to overcome several challenges related to, e.g., data security, patient privacy, and interoperability. The industry and research community turned its focus to the possible use of blockchain technology to solve some of these challenges in the healthcare domain. In this context, the paper by Arbabi et al. [A13] presents a survey. The paper identifies the interactions between healthcare actors and considers the functional components of health data storage systems. Then, the paper analyzes the implications of each non-functional requirement for each functional component and describes resulting challenges, grouping them into three categories: security, privacy, and interoperability. Nine potential benefits for health data storage systems are derived from the fundamental features of the blockchain technology. The authors review the existing solutions in the state-of-the-art and map them to the taxonomies of interactions, functional components, challenges, and benefits. Moreover, an extensive discussion of compliance with privacy-related regulations of GDPR and HIPAA is presented in the survey. Finally, the authors discuss unresolved challenges in the integration of blockchain and smart contracts in the healthcare sector and outline gaps and future directions for research.

Due to the large-scale heterogeneous network topology and booming real-time applications with more restricted quality of service requirements, 6G systems can apply the communication techniques such as non-orthogonal multiple access, mobile edge computing, millimeter-wave, massive multiple-input and multiple-output, visible light communication, terahertz, and intelligent reflecting surface to improve the communication performance. However, the 6G security and privacy protection performance will be degraded by physical (PHY)-layer attacks (such as jamming and spoofing) and higher-layer attacks including denial-of-service attacks and selfish attacks. Most existing PHY and cross-layer security schemes rely on the full knowledge of the attack model and channel varying model, thus having severe performance degradation in 6G systems with a larger number of users, shorter communication latency, and higher spectrum than 5G. In this context, the paper by Lu et al. [A14] presents a survey. Firstly, this paper investigates the potential PHY and network attacks in 6G systems and discusses the physical cross-layer security solutions and privacy protection. Then, this paper provides an overview of reinforcement learning (RL) algorithms and discusses how to apply RL in 6G PHY cross-layer security and privacy protection. Next, the RL based security schemes for unmanned aerial vehicles and cross-layer scenarios are reviewed. Finally, this paper points out four future directions and provides potential solutions for 6G systems.

Malware attacks pose severe threats to cyber security. The number of new malware examples has increased significantly in these years. To this end, researchers have proposed various malware classification methods to detect and analyze malware examples. We observe that Machine Learning (ML) models, especially Deep Learning (DL) models, are widely used as malware classifiers. However, ML models also introduce additional security risks, i.e., adversarial attacks. Attackers exploit vulnerabilities in ML models and generate adversarial malware examples to bypass them. To improve the adversarial robustness of ML-based malware classifiers, defenders further propose several methods to mitigate adversarial attacks. The abilities of both attackers and defenders evolve in the continuous game. In this context, the paper by Yan et al. [A15] presents a survey. First, the paper summarizes the attack and defense methods for ML-based malware classification into a "Defense-Attack-Enhanced-Defense" process. It also proposes a unified malware classification framework. Then, the paper provides a comprehensive review of recent research works according to the process, which helps readers understand the related field. Finally, the paper also summarizes the critical challenges faced by researchers and proposes some promising future work directions.

Over the past decade, the world has witnessed the success of blockchain as a novel technology that builds systems with decentralization, transparency, and immutability. As an essential market process, auctions have been well studied and applied in many business fields due to their efficiency and contributions to fair trade. Complementary features between blockchain and auction models trigger the great potential for research and innovation. On the one hand, the decentralized nature of blockchain can provide a trustworthy, secure, and cost-effective mechanism for managing the auction process. On the other hand, auction models can be leveraged to provide incentives to stakeholders (including regular blockchain users, miners, token holders, and external resource providers) and maintain the blockchain's economic stability and operation. In this context, the paper by Shi et al. [A16] presents a detailed survey. This paper attempts to explore how blockchain technology and auction models work and when they should be fused together to tackle corresponding challenges. The paper first reviews the existing solutions for integrating blockchain and auction models, with application-oriented taxonomies generated. Moreover, the survey highlights a range of open research challenges and future directions in this field.

The advancement in deep neural networks has made them more favourable for Network Intrusion Detection Systems (NIDS). While deep learning models exhibit a highly accurate detection engine for NIDS, they are known to be vulnerable to adversarial attacks that introduce an imperceivable modification to input features and cause the deep learning model to misclassify. Much progress has been made in generating adversarial attacks and constructing adversarial defences to mitigate the impact of adversarial attacks. However, most research on adversarial learning is targeted at supervised classification tasks in Computer Vision, which differs from unsupervised anomaly detection tasks in NIDS. In this context, the paper by He et al. [A17] presents a survey. First, the paper reviews existing NIDS structures and discusses their impact on adversarial learning. Then, the paper summarises typical formulations and strategies of adversarial attacks and defences in general and how they have been applied in the NIDS domain. Finally, the paper provides unique challenges

and open problems facing adversarial learning in NIDS and proposes guidelines and possible future directions for research.

III. IoT and M2M

There is an unprecedented growth of modern day IoT applications which collect data, analyze and extract insightful information to make decisions and actuations without human intervention, which we term autonomic IoT applications. The rapid increase of such applications necessitates the end-to-end measurement and evaluation of application quality. However, the existing approaches for evaluating quality of IoT applications is mostly focussed on end-user perspective which is unsuitable for autonomic IoT applications which involve machine-to-machine interactions and no human intervention. Thus, the existing literature on evaluating application quality lacks to cover the requirements put forward by autonomic IoT applications. In this context, the paper by Fizza et al. [A18] presents a tutorial and survey. First, the paper presents an in-depth survey of current state-of-the-art techniques and approaches for evaluating quality of IoT applications. Particularly, the paper surveys various definitions to identify the factors that contribute to understanding and evaluating quality in IoT, followed by open issues and future research directions towards realizing fine-grained quality evaluation of modern day IoT applications. The authors envision that the identified research direction will, in turn, enable real-time diagnostics of IoT applications, make them more informed and quality-aware.

IV. Internet Technologies

As the number of mobile devices are growing exponentially, and intelligent services, such as real-time video analytics, online gaming, autonomous driving, are penetrating in devices, traditional cloud-centric artificial intelligence (AI) technologies are facing significant challenges in terms of unexpected delay, data privacy leakage, etc. These urgent concerns call for distributed AI and distributed computing paradigms, where data processing and resource-intensive computing can be performed near data sources. Distributed AI empowered by end-edge-cloud computing (DAI-EECC) is a promising technology that has attracted extensive attentions in recent years, which can enable low-latency and privacy-preserved intelligent services across mobile devices, edge devices, and cloud servers. In this context, the paper by Duan et al. [A19] presents a tutorial and survey. The paper first comprehensively introduces some fundamental technologies in supporting distributed AI. Then, it discusses the state-of-the-art distributed AI optimization technologies empowered by the end-edge-cloud computing paradigm. Further, the paper summarizes security and privacy threats in the DAI-EECC architecture, as well as defense technologies in accordance with each threat. Finally, the paper presents several emerging applications and highlights some open issues to be tackled by future research efforts.

As the network infrastructure grows to accommodate new and more complex applications that have been introduced by recent trends and technologies, such as Internet of Things and 5G, network operators and administrators have ended up with a cumbersome network configuration process to manage the network. At the same time, end-users regardless of their knowledge are expected to interact and use the network infrastructures. Thus, it is of utmost important to create autonomous configuration processes of the network, while creating an intelligent interface that will allow the end-users to express what they want from the network in an abstract way, without specifying complex technical information. Intent Based Networking (IBN) is a new paradigm that tries to achieve that by allowing users to declaratively express what they want from the network, while an underlying network management system will automatically configure the network with minimal human intervention. In this context, the paper by Leivadeas and Falkner [A20] present and survey the main components needed to build an autonomous IBN system. Specifically, the paper summarizes efforts made to build IBN components of intent expression, intent translation and resolution, and intent activation and assurance. Finally, the paper introduces a number of open challenges to be tackled and possible solutions to be followed.

The concept of the Metaverse first appeared in the science fiction novel Snow Crash written by Neal Stephenson in 1992. Twenty years later, the Metaverse is once again a buzzword. In short, the Metaverse is commonly described as an embodied version of the Internet. Using augmented reality (AR), virtual reality (VR), and the tactile Internet, users will explore the virtual worlds in the Metaverse in much the same way we navigate website pages today. Dubbed “the successor to the mobile Internet”, the concept of the Metaverse has grown in popularity. Even though the Metaverse exists today as a lite version, it has far yet to realize the full vision of an immersive, embodied, and interoperable environment. In order to succeed the Internet, particularly in terms of its accessibility to billions of users today, the Metaverse must address implementation issues from communication, networking, and computation perspectives. In this context, the paper by Xu et al. [A21] present a full dive into realizing the edge-enabled Metaverse by focusing on the edge-enabled Metaverse to realize its ultimate vision. An introduction to the architecture, as well as current developments, are presented by way of a succinct tutorial of the Metaverse. As part of our approach to enabling ubiquitous, seamless, and embodied access to the Metaverse, we examine communication and networking challenges, as well as cutting-edge concepts and solutions to enabling embodied avatars to be immersed and interacted with in the Metaverse through next-generation communication systems. Furthermore, due to the high computational costs that are associated with rendering 3D virtual worlds and running data-hungry avatars driven by artificial intelligence, we discuss how the Metaverse can be realized on edge devices with limited resources by using cloud-edge-end computation frameworks. After exploring blockchain technologies, we explore how they can contribute to the interoperability of the Metaverse, not just enabling the economic circulation of virtual user-generated content but also allowing physical edge resources to be managed in a way that is transparent, immutable, and decentralized. The final part of our presentation discusses future research directions toward

realizing the true vision of a metaverse that is enabled by the edge.

V. Network Virtualization

Cloud computing brings advantages for application and service deployment in terms of scalability, on-demand resource provisioning, and pay-as-you-go pricing model. A variety of new emerging 5G and beyond era applications demand high data rate and low latency. To deal with these ongoing requirements, edge computing with various paradigms of cloudlet, mobile edge computing and fog computing, provides resources at the edge of the network and closer to the end devices. However, edge computing can not sustain the ongoing traffic explosion and the latency is still high for ultra-low-latency applications. The concept of Software Defined Networking (SDN) decouples the forwarding devices from the control plane, in order to facilitate network management. SDN enables programmable data plane technology with the capability of programming packet processing through some high-level languages; thus, ending to faster adoption of new data plane functions and facilitating development of prototyping. Network elements, e.g., switches and routers connect end-devices to the edge infrastructure, as well as edge computing resources to the cloud infrastructure. The new paradigm of In-Network Computing (INC) exploits programmable network elements, not only for the purpose of connectivity, but also for the purpose of computation. Programmable switches can process in the scale of billion packets per second, while experiencing sub-microsecond packet processing delays. Leveraging in-network computing, the packets can be processed at line-rate, and prior to the edge/cloud servers. The survey by Kianpisheh and Taleb [A22] provides a comprehensive survey on INC. INC studies has been categorized in groups of in-network analytics, in-network caching, in-network security, in-network coordination, and technology specific applications in the scopes of cloud/edge computing, 5G/6G, and NFV. The related studies are compared considering proposed methodology/implementation/performance-related criteria as well as application specific criteria. In comparison with server/SDN-controller based schemes, INC-based schemes will gain benefits for the application specific criteria. In-network analytics can gain higher inference speed, with less bandwidth consumption required for data transmission. In-network caching schemes reduce content access delay, and bandwidth consumption by offering storage at the edge. In-network security schemes can have lower mitigation latency and bandwidth consumption required for traffic analysis. In-network implementation of functionalities of new generations of mobile communications, virtual network functions, functionalities of edge intelligence, will reduce computational cost and power consumption, with a lower experience of latency and higher throughput achievement. However, there exist possible compromised application specific criteria due to hardware limitation of the network elements, which have been discussed in the survey. Co-design approaches can enrich INC with general purpose computation. The benefit gains and the compromised application specific criteria in comparison with fully-in-network implemented schemes, have been discussed in the survey. The resource allocation schemes for technology-specific applications to deal with hybrid computational environment have been investigated. Finally, the research directions in this newly emerging topic have been given.

The existing packet forwarding technology cannot meet the increasing needs of Internet development, such as low delay, high throughput, high security and high reliability. By integrating artificial intelligence (AI) technology into the programmable data plane (PDP), AI-driven packet forwarding has changed the traditional packet forwarding pattern. On the one hand, the PDP can provide more network state information for precise AI models. Correspondingly, the AI models can produce the more effective and flexible forwarding logic. This new pattern is expected to provide a promising and smart data plane to support the future network, which is equipped with high intelligence and high computing power. In this context, the paper by Quan et al. [A23] presents a survey. This paper summarizes the different packet forwarding frameworks assisted by the AI and PDP. The authors also analyze and discuss the main researches on AI-driven packet forwarding in four branches: delay, throughput, reliability and security. Besides, the paper highlights the development trend and challenges of future packet forwarding research.

VI. Network and Service Management and Green Communications

With the rapid development of networks, a large amount of sensitive information of users is transmitted on the Internet, such as bank accounts and payment records. To this end, encryption technologies, e.g., Secure Socket Layer/Transport Layer Security (SSL/TLS), are widely used to ensure security and privacy, so that the network packets can only be decrypted by legitimate receivers. Traffic analysis is a significant tool for network management and anomaly detection. However, the developing encrypted traffic brings new challenges, as the analysis methods based on plaintext payload are almost invalid. Faced with this challenge, machine learning has been employed to extract useful information from encrypted traffic. In this context, the paper by Shen et al. [A24] presents a survey. Firstly, the paper starts by providing an overview on the application scenarios of encrypted traffic analysis. Then, the paper introduces machine learning techniques that are commonly used in encrypted traffic analysis. Furthermore, the general framework including traffic collection, traffic representation, traffic analysis and performance evaluation is summarized. Moreover, recent studies on encrypted traffic analysis are summarized and reviewed according to the application scenarios. Finally, the paper elaborates on challenges and future research directions.

VII. Vehicular and Sensor Communications

The Internet of Things (IoT) networking paradigm encompasses the Internet connectivity of energy and computing resources constrained devices. At the edge of the connectivity infrastructure, gateways carry the information that flows

between IoT devices and servers. Many standardization efforts, either from official standards development organizations or from newly-formed alliances and consortia, deal with IoT networks. Great attention is given to standards that will offer connectivity to low-power devices that are at long range from the gateways, forming the so-called Low Power Wide Area Network (LPWAN). Already, several research proposals have focused on the LPWAN, with most of them combining the Long Range (LoRa) and the LoRa Wide Area Network (LoRaWAN) technologies. In this context, the paper by Milarokostas et al. [A25] presents a survey of the major available technologies that are part of the LPWAN research field. The paper focuses on LPWAN technologies for the access-side of these networks and discusses cloud-based solutions for the server-side. Several IoT key performance indicators are used to provide a comprehensive comparison of LPWAN technologies. As a standout LPWAN solution, the combination of LoRa PHY and LoRaWAN MAC is studied in detail. The survey is meant to serve as a reference point for researchers in the field; hence, an extensive overview of existing research work in the domain of LoRa/LoRaWAN systems is provided, complemented by a well-compiled list of available simulators.

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.

APPENDIX: RELATED ARTICLES

[A1] A. Celik, I. Romdhane, G. Kaddoum, and A. M. Eltawil, "A top-down survey on optical wireless communications for the Internet of Things," *IEEE Commun. Surveys Tuts.*, early access, Nov. 8, 2022, doi: 10.1109/COMST.2022.3220504.

[A2] S. M. Hernandez and E. Bulut, "WiFi sensing on the edge: Signal processing techniques and challenges for real-world systems," *IEEE Commun. Surveys Tuts.*, early access, Sep. 23, 2022, doi: 10.1109/COMST.2022.3209144.

[A3] D. Adesina, C.-C. Hsieh, Y. E. Sagduyu, and L. Qian, "Adversarial machine learning in wireless communications using RF data: A review," *IEEE Commun. Surveys Tuts.*, early access, Sep. 12, 2022, doi: 10.1109/COMST.2022.3205184.

[A4] H. Al-Hraishawi, H. Chougrani, S. Kisseleff, E. Lagunas, and S. Chatzinotas, "A survey on non-geostationary satellite systems: The communication perspective," *IEEE Commun. Surveys Tuts.*, early access, Aug. 9, 2022, doi: 10.1109/COMST.2022.3197695.

[A5] K. J. Kim, H. Liu, M. Wen, T. A. Tsiftsis, P. V. Orlik, and H. V. Poor, "QR decomposition-based cyclic prefixed single-carrier transmissions for cooperative communications: Concepts and research landscape," *IEEE Commun. Surveys Tuts.*, early access, Jul. 29, 2022, doi: 10.1109/COMST.2022.3194997.

[A6] K.-H. Lin, H.-H. Liu, K.-H. Hu, A. Huang, and H.-Y. Wei, "A survey on DRX mechanism: Device power saving from LTE and 5G new radio to 6G communication systems," *IEEE Commun. Surveys Tuts.*, early access, Oct. 28, 2022, doi: 10.1109/COMST.2022.3217854.

[A7] R. Ajmeria et al., "A critical survey of EEG-based BCI systems for applications in industrial Internet of Things," *IEEE Commun. Surveys Tuts.*, early access, Dec. 28, 2022, doi: 10.1109/COMST.2022.3232576.

[A8] W. Yang et al., "Semantic communications for future Internet: Fundamentals, applications, and challenges," *IEEE Commun. Surveys Tuts.*, early access, Nov. 18, 2022, doi: 10.1109/COMST.2022.3223224.

[A9] S. Aboagye, A. R. Ndjiongue, T. M. N. Ngatched, O. A. Dobre, and H. V. Poor, "RIS-assisted visible light communication systems: A tutorial," *IEEE Commun. Surveys Tuts.*, early access, Dec. 1, 2022, doi: 10.1109/COMST.2022.3225859.

[A10] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, Sep. 12, 2022, doi: 10.1109/COMST.2022.3205643.

[A11] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, early access, Sep. 7, 2022, doi: 10.1109/COMST.2022.3202047.

[A12] B. Cao et al., "Blockchain systems, technologies and applications: A methodology perspective," *IEEE Commun. Surveys Tuts.*, early access, Sep. 6, 2022, doi: 10.1109/COMST.2022.3204702.

[A13] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," *IEEE Commun. Surveys Tuts.*, early access, Nov. 24, 2022, doi: 10.1109/COMST.2022.3224644.

[A14] X. Lu et al., "Reinforcement learning based physical cross-layer security and privacy in 6G," *IEEE Commun. Surveys Tuts.*, early access, Nov. 23, 2022, doi: 10.1109/COMST.2022.3224279.

[A15] S. Yan, J. Ren, W. Wang, L. Sun, W. Zhang, and Q. Yu, "A survey of adversarial attack and defense methods for malware classification in cyber security," *IEEE Commun. Surveys Tuts.*, early access, Nov. 28, 2022, doi: 10.1109/COMST.2022.3225137.

[A16] Z. Shi, C. de Laat, P. Grosso, and Z. Zhao, "Integration of blockchain and auction models: A survey, some applications, and challenges," *IEEE Commun. Surveys Tuts.*, early access, Nov. 16, 2022, doi: 10.1109/COMST.2022.3222403.

[A17] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, Jan. 3, 2023, doi: 10.1109/COMST.2022.3233793.

[A18] K. Fizza et al., "A survey on evaluating the quality of autonomic Internet of Things applications," *IEEE Commun. Surveys Tuts.*, early access, Sep. 13, 2022, doi: 10.1109/COMST.2022.3205377.

[A19] S. Duan et al., "Distributed artificial intelligence empowered by end-edge-cloud computing: A survey," *IEEE Commun. Surveys Tuts.*, early access, Nov. 1, 2022, doi: 10.1109/COMST.2022.3218527.

[A20] A. Leivadeas and M. Falkner, "A survey on intent based networking," *IEEE Commun. Surveys Tuts.*, early access, Oct. 20, 2022, doi: 10.1109/COMST.2022.3215919.

[A21] M. Xu et al., "A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges," *IEEE Commun. Surveys Tuts.*, early access, Nov. 10, 2022, doi: 10.1109/COMST.2022.3221119.

[A22] S. Kianpisheh and T. Taleb, "A survey on in-network computing: programmable data plane and technology specific applications," *IEEE Commun. Surveys Tuts.*, early access, Oct. 14, 2022, doi: 10.1109/COMST.2022.3213237.

[A23] W. Quan et al., "AI-driven packet forwarding with programmable data plane: A survey," *IEEE Commun. Surveys Tuts.*, early access, Oct. 27, 2022, doi: 10.1109/COMST.2022.3217613.

[A24] M. Shen et al., "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, early access, Sep. 20, 2022, doi: 10.1109/COMST.2022.3208196.

[A25] C. Milarokostas, D. Tsolkas, N. Passas, and L. Merakos, "A comprehensive study on LPWANs with a focus on the potential of LoRa/LoRaWAN systems," *IEEE Commun. Surveys Tuts.*, early access, Dec. 16, 2022, doi: 10.1109/COMST.2022.3229846.

DUSIT NIYATO, *Fellow, IEEE*
Editor-in-Chief
IEEE COMMUNICATIONS SURVEYS AND TUTORIALS
Professor
School of Computer Science and Engineering
Nanyang Technological University
Singapore
Web: https://personal.ntu.edu.sg/dniyato/