Security and privacy for 6G: A survey on prospective technologies and challenges

Van-Linh Nguyen, *Member, IEEE*, Po-Ching Lin, *Member, IEEE*, Bo-Chao Cheng, Ren-Hung Hwang, *Senior Member, IEEE*, Ying-Dar Lin, *Fellow, IEEE*

***Abstract*—Sixth-generation (6G) mobile networks will have to cope with diverse threats on a space-air-ground integrated network environment, novel technologies, and an accessible user information explosion. However, for now, security and privacy issues for 6G remain largely in concept. This survey provides a systematic overview of security and privacy issues based on prospective technologies for 6G in the physical, connection, and service layers, as well as through lessons learned from the failures of existing security architectures and state-of-the-art defenses. Two key lessons learned are as follows. First, other than inheriting vulnerabilities from the previous generations, 6G has new threat vectors from new radio technologies, such as the exposed location of radio stripes in ultra-massive MIMO systems at Terahertz bands and attacks against pervasive intelligence. Second, physical layer protection, deep network slicing, quantum-safe communications, artificial intelligence (AI) security, platform-agnostic security, real-time adaptive security, and novel data protection mechanisms such as distributed ledgers and differential privacy are the top promising techniques to mitigate the attack magnitude and personal data breaches substantially.**

***Index Terms*—6G, security and privacy, AI security, physical layer security, connection security, service security.**

I. Introduction

6G is the sixth generation standard for cellular communications that are currently under development to succeed 5G. 6G offers an ambitious vision of truly autonomous networks that will be commercially deployed someday in the 2030s [1]. 6G will be able to support speeds of over 1Tbps, 50 times faster than 5G, while latency is projected at 10-100μs [1]. Researchers expect that this standard will expand connectivity for both conventional coverage areas in 5G and space-air-ground-sea applications. The coverage and network capability will enable a wide range of digital services such as wearable displays, implantable devices, telepresence applications (rendering of 3D holographic representation of each participant in a meeting), mixed reality, tactile Internet [2], [3], and autonomous driving [4], [5]. With the substantial increase of coverage and network heterogeneity, there are severe concerns that 6G security and privacy can be worse than the previous generations. For example, the involvement of connected devices in every aspect of humans (e.g., implants/cyborgs) poses serious concerns of potential leaks of personal information (e.g., health records). Potential loss from security attacks could be irrecoverable, not only about finance or personal reputation as currently but also about life (e.g., fatal crash because of attacks into autonomous driving). Further, the achievements of artificial intelligence can be abused for massive online surveillance [6]. By contrast, novel technologies such as quantum-safe communications and distributed ledgers promise to significantly improve 6G security and privacy. Many believe that robust security and enhanced privacy technologies will be key provisions to the success of 6G.

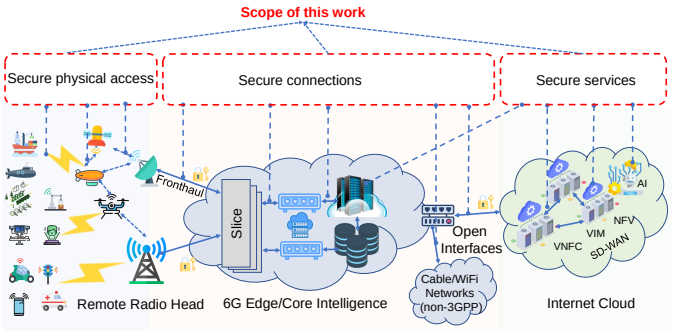

Fig. 1. A concept of generic mobile networks for 6G and the scope of this work. Security and privacy preservation technologies in the physical layer, connection layer, and service layer are pillars of 6G networks.

However, research on security and privacy issues for 6G networks is still at an early stage. Existing studies on such issues are mostly for the Internet of Things (IoT) networks [7], 5G networks [8]–[10], quick excursions into specific technologies, such as Artificial Intelligence and Machine Learning (AI/ML) [6], [11], or fragmented ideas in generic surveys about 6G concepts [12]. Lack of related work is because many fundamental components of 6G networks remain largely undefined. However, the evolution of prior networks (from 4G to 5G) indicates that every network generation tends to stay in use for years. For capital expenditure and payback

This work was supported in part by the Ministry of Science and Technology (MOST) of Taiwan under Grant No 110-2811-E-194-501-MY2, Grant No 108-2221-E-194-022-MY3, and Grant No 108-2221-E-194-019-MY3 and in part by the Advanced Institute of Manufacturing with High-Tech Innovations (AIM-HI) through the Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

Van-Linh Nguyen, Po-Ching Lin, Ren-Hung Hwang are with the Department of Computer Science and Information Engineering (*e-mail: {nvlinh, pclin, rhhwang}@cs.ccu.edu.tw*), Bo-Chao Cheng is with the Department of Communications Engineering (*e-mail: bcheng@ccu.edu.tw*), National Chung Cheng University, Chiayi, Taiwan.

Van-Linh Nguyen is also with the Department of Information Technology, Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam (*e-mail: nvlinh@ictu.edu.vn*).

Ren-Hung Hwang is also with Advanced Institute of Manufacturing with High-tech Innovations, National Chung Cheng University and a Jointly Appointed Professor of AI college, National Yang Ming Chiao Tung University, Taiwan.

Ying-Dar Lin is with the Department of Computer Science, National Yang Ming Chiao Tung University, Taiwan (*e-mail: ydlin@cs.nctu.edu.tw*).

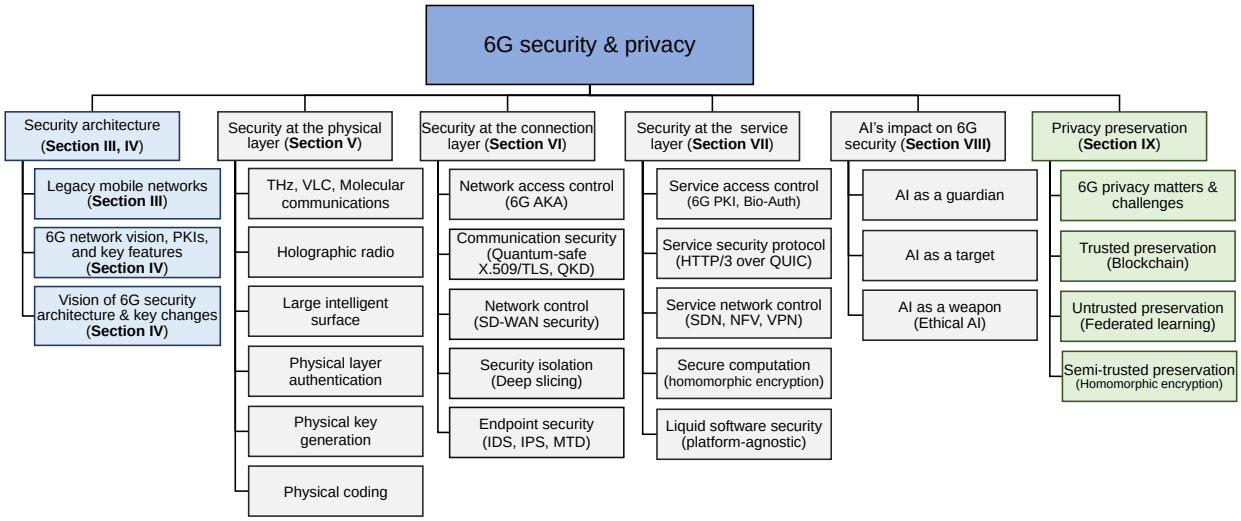

Fig. 2. A taxonomy of key points of our survey on security & privacy for 6G: security architecture, specific security technologies in the three layers, privacy enhancing models, and AI's impact on those fields.

optimization, many network providers favor rolling out a new network generation while still enhancing the technologies on existing infrastructure [13]. Moreover, backward compatibility is necessary to maintain connectivity for deployed devices. As the basis of inheritance, 6G security and privacy will presumably adopt many features from 5G.

Inspired by security evolution in prior generations, this work provides a systematic review of existing research efforts on security and privacy for 6G networks. The survey reviews the issues of 6G enabling technologies and state-of-the-art defense methods. Also, we adopt the three-layer architecture in 6G-enabled IoT networks [14], [15], including physical (perception) layer, connection (network) layer, and service (application) layer, to classify the attacks and corresponding solutions. This layer-based review approach can particularly benefit the operators and developers of interest in preventing the specific attacks on the fundamental protocols that impact many 6G applications. By conducting the problems in each technology, our goal is to provide a holistic view of the evolution of core security and privacy issues, along with the remaining challenges for further enhancements. Figure 1 illustrates the scope of this work. The lessons learned from the survey indicate that 6G networks will need significant upgrades of security protection and data privacy preservation. To this end, the study aims to answer the fundamental question: What are the major potential changes of 6G security infrastructure from the prior generations? What are new challenges and prospective approaches for privacy preservation in 6G to satisfy the requirements in laws, such as General Data Protection Regulation (GDPR)?

A. Review methodology

Rather than using all brand-new technologies, 6G security and privacy will continue the trajectory of many enabling technologies from prior generations because of costly deployment. Inspired by this inheritance, we outline potential changes of 6G security and privacy, seen through the mirrors of the lessons learned from two aspects. The first is to fix remaining security issues and enhance privacy preservation in security architecture and several legacy technologies, such as Software defined Networking (SDN). The other is to address potential security and privacy issues in futuristic technologies which will highly impact 6G, such as THz communications. As illustrated in Figure 2, this work covers discussions on every aspect, from security architecture to specific technologies in each layer, or factors that impact 6G security and privacy.

Security attacks are often the main motivations that drive how security systems in the next generation should be changed to counter the exploit of old vulnerabilities. Such attacks often reveal weaknesses of system or protocol flaws that the creators may never have thought of at the design stage. Learning from such attacks is a straightforward approach to get to know how different the security enhancements of mobile networks are – sometimes for fixing known vulnerabilities exploited by attacks in prior generations. For example, authentication protocol flaws revealed by security attacks often require upgrades of core network functions to fix. However, most vendors are opposed to such a replacement because of the high cost. These not-yet-been-fixed issues thus become potential targets for upgrades in 6G, or are a basis for future research.

B. Contributions

In summary, the main contributions of this article are as follows. First, the work provides a systematic overview of the evolution of security architecture and vulnerabilities in legacy networks. By investigating the shortcomings of the standards and technical insights of protocol flaws in such networks, required enhancements to 6G security and privacy are highlighted. Second, our survey provides a holistic view of security and privacy issues and how the existing solutions must be changed to satisfy the new demands in 6G. Since 6G will continue on the techno-economic trajectory of 5G, a systematic review on transition and possible changes of 6G security and privacy can shed light on the best plan for

the operators/developers to upgrade the security infrastructure/defense systems at the right time. Finally, our discussions about lessons learned from the shortcomings of existing security architecture and remaining technical challenges may help researchers/developers quickly identify relevant issues and starting points for further works. To the best of our knowledge, this survey is the first attempt to provide a thorough review of security and privacy for 6G from security architecture, specific technologies in the layers, to AI's impact on those fields.

C. Structure of the paper

The rest of this paper is organized as follows. Section II presents related work and point of departure of our survey. Section III reviews lessons learned from security issues and the evolution of security architecture in legacy networks (from 1G to 5G). Section IV describes 6G networks and our vision about potential changes in its security architecture. The problems and prospective technologies of 6G security in the *physical layer*, *connection layer*, and *service layer* are then discussed in Section V, Section VI, and Section VII, respectively. The impact of *artificial intelligence* on 6G security is detailed in Section VIII. Privacy concerns and potential solutions in 6G are presented in Section IX. Section X discusses several other aspects of 6G security& privacy in the coming years. Section XI concludes this paper. The key points of our survey are shown in Figure 2. The acronyms used in this work are listed as follows.

ACRONYMS

AI/ML	Artificial Intelligence and Machine Learning
AMF	Access and Mobility Function
AUSF	Authentication Server Function
CSI	Channel State Information
DDoS	Distributed Denial-of-Service
GDPR	General Data Protection Regulation
GUTI	Global Unique Temporary Identifier
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IRS	Intelligent Reflecting Surfaces
KPIs	Key Performance Indicators
LDPC	Low-Density Parity-check Code
LIS	Large Intelligent Surface
LTE	Long-term Evolution
MEC	Multi-access Edge Computing
MIMO	Multiple-input and Multiple-output
MTD	Moving Target Defense
NaaS	Network as a service
NFV	Network Function Virtualization
NOMA	Non-Orthogonal Multiple Access
NSA	Non-Standalone
PET	Privacy Enhancing Technologies
RAN	Radio Access Network
SA	Standalone
SD-LAN	Software-Defined Local Area Network
SD-WAN	Software-Defined Wide Area Network
SDN	Software defined Networking
SEAF	Security Anchor Function
SN	Serving Network
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

II. RELATED WORK AND OUR SURVEY POSITION

Security and privacy for 6G are still in the infancy of their development cycle, as are related surveys. Existing studies on security and privacy issues [7], [10], [16], [17] can be categorized into three groups: (1) security and privacy preservation for IoT networks and their subsidiaries, e.g., wireless sensor networks, vehicular networks, (2) security and privacy issues for existing 4G/5G cellular networks, and (3) security and privacy in 6G by analyzing issues around specific key technologies, such as machine learning.

IoT security and privacy is not a new topic. Several technologies of IoT security and privacy may partially contribute to the 6G field. For example, the authors of [18] present security-related challenges and sources of threats in IoT, highlighting various prospective technologies for 6G, such as blockchain. A narrower approach is to address security in specific network types, which may become a reality in 6G, such as vehicular networks [19] and 6G-enabled IoT networks [15], [20]. However, discussions of specific attacks in 6G networks in the mirror of IoT security are somewhat limited. Moreover, given little vision of 6G concepts at the time of the studies of [21], [22], many predictions on the security issues for next-generation networks favor referring to conventional threats such as side-channel attacks and Distributed Denial-of-Service (DDoS) attacks. Several field surveys such as security in 6G heterogeneous vehicular networks [23], tactile Internet [20], security in edge-computing-assisted IoT networks [24] indicate that ultra-high reliability and real-time protection will be key requirements of many applications in future networks. However, 6G communication models and security architecture are not explicitly included in the discussions of the surveys.

Security and privacy topics for cellular networks have attracted much attention because of the popularity of mobile devices in our daily lives. Most current security and privacy surveys of cellular networks are for 5G. For example, the authors of [7], [10] present various aspects of 5G security architecture standards [8], [9], [38]–[40] relevant to security attacks and privacy problems in multiple layers, such as core/backhaul networks. The limitations and security challenges of specific technologies such as SDN [26], programmable networking, and Network Function Virtualization (NFV) [17], [41], particularly for Radio Access Network (RAN) [42] and Multi-access Edge Computing (MEC) [27], [43] – which promise to play the key roles in 6G – are hot topics and have been partially addressed. The open discussions and technical materials from these 5G security and privacy surveys [10], [17], [26] and specific technologies [25], [44] are important sources for our review of the legacy technologies that impact 6G security and privacy. The overview of several state-of-the-art studies in this field is listed as the top five entries in Table I.

Exploring new technologies for 6G security and privacy started to gain traction recently. The overviews of the studies

TABLE I
SEVERAL RELATED STATE-OF-THE-ART STUDIES AND OUR SURVEY POSITION

The paper	Year	Paper type	Mobile network generation	Content coverage						Contributions
				Core architecture	Physical layer security	Connection layer security	Service layer security	AI security	Privacy preservation	
Dai et al. [25]	2019	Short paper	5G/B5G					●	●	► Blockchain and deep learning for 5G networks and beyond
Ahmad et al. [10] *	2019	Comprehensive survey	5G/XG	●		●	●		●	►Security and privacy in 5G and overview of the changes of security and privacy in the next-generation network (not specify 6G)
Farris et al. [17]	2019	Comprehensive survey	5G/B5G			●	●			► SDN/NFV security survey
Chica et al. [26]	2020	Comprehensive survey	5G/B5G				●			► SDN security survey
Ranaweera et al. [27]	2021	Comprehensive survey	5G/6G				●			►Multi-Access Edge security
Wang et al. [28]	2020	Short survey	6G				●		●	►An overview of security and privacy in key applications/ technologies of 6G networks
Ylianttila et al. [29] *	2020	White paper	6G		●	●			●	►6G research challenges for trust, security and privacy
Kantola [30]	2020	Short survey	5G/6G			●			●	►Trust networking
Sheth et al. [31]	2020	Comprehensive survey	6G					●		►A taxonomy of AI techniques for 6G networks
Sun et al. [6]	2020	Comprehensive survey	6G					●	●	►Machine learning for 6G privacy
Mahmoud et al. [32]	2021	Comprehensive survey	6G		●				●	►A generic survey about 6G technologies, applications, challenges
Xie et al. [33]	2021	Comprehensive survey	5G/6G		●					►Physical layer authentication
Huang et al. [34]	2021	Short survey	5G/6G					●		►Intelligent Reflecting Surface aided pilot contamination attack & defense
Pirandola et al. [35]	2021	Comprehensive survey	6G		●	●				►Advances in quantum cryptography
Xu et al. [36]	2021	Short brief	5G/6G		●					►Pilot spoofing attack in Massive MIMO systems & countermeasures
Porambage et al. [37] *	2021	Comprehensive survey	6G				●		●	►Security and privacy briefs for 6G applications
Our survey	2021	Comprehensive survey	B5G/6G	●	●	●	●	●	●	►A comprehensive security survey on the prospective technologies and challenges for 6G on all layers and core architecture

* The studies are closely related to our work.

in this direction are listed in the last twelve entries of Table I. Closely related to our work, Wang et al. [28] sketch a quick overview of the vision of 6G security and privacy through the mirror of emerging applications, e.g., wireless brain-computer interactions and multi-sensory XR applications. However, that study lacks a relevant technical discussion on how such security architecture will evolve or any detail of AI's progress in enhancing security. Ylianttila et al. [29] highlight several key technologies of 6G security and privacy along with their challenges that remain, but no discussion on connection and service layer security. On the other hand, many authors have carried out surveys on narrower issues, such as physical layer security [33], [34], [36], quantum-safe security technologies [35], [45], AI-driven security [6], [31], trusted networks [30], which are supposed to be the top priorities in 6G. Recently, the authors in [37] highlight possible security and privacy challenges in different 6G technologies and applications. However, there is no comprehensive survey to provide a holistic view of 6G security and privacy issues in the context of overall security architecture, protection solutions in the fundamental communication technologies, or how they evolve from the legacy networks to satisfy the new demands in 6G applications. The knowledge on security transition and the feasibility of prospective technologies can shed light on the best plan for the operators/service providers/developers to upgrade their security infrastructure/defense systems at the right time.

III. SECURITY ISSUES AND THE EVOLUTION OF SECURITY ARCHITECTURE IN LEGACY MOBILE NETWORKS

A preferable way to comprehensively understand 6G security and privacy is to look at lessons learned from would-be failures of the current security architectures and legacy technologies if applied to satisfy 6G requirements. This section presents our assessment of security attacks and privacy issues for various generations of cellular networks. We then highlight lessons learned from the prior security transitions to envisage potential changes and enhancements for security and privacy preservation features in 6G.

A. 1G,2G,3G - Security issues of phased-out and phasing-out networks

There are many memorable milestones with the development of the first three generations of mobile networks, particularly in security. The first generation (1G) of mobile networks provided neither security nor privacy. Launched in the 1980s and 1990s, respectively, the second generation (2G) and the third-generation (3G) played a critical role in completely transforming the era of analog phone services (1G) to IP-based networks (3G). Although many operators around the world, particularly in developing countries, still offer 2G and 3G services, both networks are scheduled to be entirely switched off in the next five years [46]. 2G and 3G gave many valuable lessons of how security issues can be exploited by attackers. For example, the most infamous attack on 2G and 3G was International Mobile Subscriber Identity (IMSI)-catcher [47], [48], where the attacker exploited unencrypted identity information during authentication and paging procedures to track mobile subscribers. Many law enforcement and intelligence agencies in some countries still use IMSI-based tracking to follow crimes [47]. On the other hand, absence of end-to-end encryption in communications was the root cause of many eavesdropping attacks such as man-in-the-middle, phone fraud, and SMS interception [49]. Downgrade attacks [48], [50] were also a headache in the dual-network

infrastructure of 2G and 3G. In such an attack, an attacker would force a victim to connect to 2G networks which do not require mutual authentication. After downgrading successfully, the attacker could launch another man-in-the-middle (MITM) attack [51] and freely collect the IMSI of UE for further location tracking. Many security attacks, which appeared for the first time in 2G and 3G, such as signalling DoS attacks [52] and energy depletion attacks [53], have not yet been resolved.

B. 4G, 5G - Security issues and enhancement of operating networks in the next five years

Launched from 2009, the Long-term Evolution (LTE)-Advanced standard (official technology of 4G in ITU requirements [54]) has evolved strongly over the years, resulting in the most widely deployed network [55]. Compared to 3G, 4G security has been enhanced significantly. For example, 4G/LTE [56] Evolved Packet System-Authentication and Key Agreement (EPS-AKA) included a series of security enhancements for interconnection between 3GPP and non-3GPP networks. A new cipher and integrity checking mechanism [56] was also introduced to protect the signalling data between UEs and the core network. With EPS-related cryptographic key involvement, a UE can verify the Serving Network (SN)'s identity. Tunnel encryption was first proposed with the support of IPSec. Despite many upgrades of security features, the 4G/LTE security architecture has several weaknesses. First, 4G is not immune to DDoS attacks, which can be launched from malicious mobile applications to overload the Home Subscriber Server (HSS) and Mobility Management Entity (MME) servers with multiple authentication requests. Such overloading potentially blocks the access of legitimate subscribers to the network [57]. Although IMSI/Global Unique Temporary Identifier (GUTI), a temporary identifier, is used to hide a subscriber's long-term identity, researchers found that TMSI/GUTI allocation frequency is predictable [58] and can be used for tracking the location of any subscriber.

The authentication decision model of a home network to consult a serving network during UE authentication in 4G also has many security flaws. Because the decision is made solely by the serving network, a well-organized attacker can create fake serving networks to track subscribers [59], [60]. Another big vulnerability lies in the Voice over LTE (VoLTE) service [61], [62], which uses packet-based LTE networks and IP protocol to establish voice and media calls. The authors of [63] found the problem of keystream reuse in VoLTE – the packets of the first call are encrypted with the same keystream as those of the second call – being exploited to decrypt and access the contents of a recorded target call. Criminals use VoLTE to spoof a caller, launch denial-of-service attacks, subdue voice calls, and strip the victim's mobile account of money [62].

Featured upgrades in 5G security

5G has been upgraded significantly in terms of both security architecture and authentication protocols to satisfy a service-oriented network model as well as fixing many vulnerabilities in 4G. According to the latest specifications [8], other than the five security features in 4G networks, 5G adds a new domain: service-based architecture (SBA) security. 5G is also the first standard to have its authentication architecture as a unified framework. This platform supports both 3GGP and non-3GPP access networks, e.g., Wi-Fi and cable networks. With a unified platform, 5G enables *one authentication execution*, in which a UE can be authenticated in a 3GPP access network, and then move to other non-3GPP network without the need for reauthentication [39].

5G protects UE identities better than 4G. 5G specifically designs Subscription Concealed Identifier (SUCI), an encrypted form of the Subscription Permanent Identifier (SUPI), to conceal the subscriber's real information in the authentication stage [73]. With the enhancement, a UE's permanent identifier, e.g., the IMSI, will not be sent over 5G networks in plaintext. This feature is a major security update over earlier network generations. 5G also made its first attempt to support lawful interceptions. For example, in some special cases, e.g., the court issues subpoena for investigating a crime, the operators can provide lawful interception services to the authorized law enforcement agents. 5G enables two new additional authentication methods: EAP-AKA' and EAP-TLS. EAP-AKA' has the same mission and security capabilities as 5G-AKA but for the difference in the message format and the role of entities [8]. EAP-TLS, as defined in RFC 5216, is designed for subscriber authentication in IoT or private networks. Many potential non-USIM devices, such as laptop or IoT devices, now are able to subscribe and access to the 5G core by using EAP-TLS, which was impossible in earlier generations.

Security vulnerabilities of 5G

Because of its complexity, 5G has security weaknesses. First, the 5G-AKA protocol fails to meet several goals that it is expected to have. For example, the agreement between subscribers and serving networks is weak [74] because of the lack of a binding assumption on the channel between the serving network and the home network. This vulnerability could allow an attacker to transfer the network bill to someone else for his access on a serving network. Although 5G-AKA can defeat IMSI-catcher attacks [47], [72], researchers of [74] found that user tracking is still possible in 5G by observing synchronization failure messages over time. In another work [60], the authors propose that a seemly harmless service, like paging, can be exploited to locate a user with fewer than 10 calls. Finally, the issue of using a rogue base station to fool a UE into disclosing its SUPI, e.g., by leveraging a spoofed pre-authentication message, has not yet been fixed in 5G [75].

C. Network deployment strategies' impact on security architecture and security transition

Because of cost, operators may select either of two deployment strategies: Standalone (SA) vs. Non-Standalone (NSA). NSA provides control signalling of a new standard to the base stations of older standards, whereas in SA, the base stations of a new standard are directly connected to the core network without an intermediate carry of the old infrastructure. Deployment in an NSA strategy has two benefits: (1) much lower cost than SA and (2) reusing existing facilities. By contrast, deployment of the SA strategy requires high CAPEX but can provide services with the full capacity of the new

TABLE II
SECURITY ISSUES OF THE NETWORKS FROM 1G TO 6G

Target	Attack name	Time exposed /authors	Method to uncover	Affected Networks 1G	2G	3G	4G	5G	6G	Protocol flaws, bugs	Risk level	Consequence	Status of attack fix *
Availability	Signalling DoS attacks	► 2007: [64] 2012: [57] 2016: [52]	Signalling storm		●	●	●	●	●	Limited radio resources	High	Block user access	No
	Paging DoS attacks	► 2013: [65]	Hijack paging procedure		●					Paging procedure bugs	High	Block user access	Partially fixed
	DDoS Authentication server	► 2009: [66]	Use phone botnets		●	●			●	Core networks connect IP services	High	Block user access	No
	SMS saturation attacks	► 2009: [67]	Send massive SMS to block voice calls		●	●				Text messages use the same control channels as voice calls	High	Block voice communications	Partially fixed
	Energy depletion attacks	► 2019: [53]	Send random false authentication messages,			●	●	●	●	Weak authentication	High	Disable IoT devices, shutdown low-power sensor networks	No
Integrity	Cloning attacks	► 1995: [68]	Clone the victim's ESN, MDN	●						No protection for identity	High	Phone fraud	Yes
	SIM card rooting	► 2013: [69]	Exploit sloppy encryption		●	●	●			Implementation flaws	High	Clone SIM card	Partially fixed
	Partitioning attacks	► 2002: [70]	Use side-channel attacks		●	●				Insecure wireless channels	High	Clone SIM card	Yes
	Impersonation attacks	► 2020: [71]	Exploit no integrity protection of the user plane			●	●	●	●	Authentication protocol bugs	High	Impersonate a user	No
	Voice IP attacks	► 2015: [62] 2020: [63]	Exploit SIP leaked session info, hidden data channels, keystream reuse in subsequent calls				●	●	●	IP-based service vulnerability	High	Caller spoofing, service interruption, subdue voice calls, over-billing	Partially fixed
Confidentiality	SMS interception	► 2013: [49]	Reverse engineering		●					Authentication protocol bugs	Medium	User tracking	Yes
	IMSI-catcher	2013: [49] 2014: [48] 2015: [72]	Use downgrade attacks, unencrypted paging information		●	●			-	Authentication protocol bugs	High	User tracking	Partially fixed
	Traceability attack	►2015: [52], [72] 2018: [59] 2019: [60]	Exploit information from failure messages, paging errors			●	●	●	●	Authentication protocol bugs	High	User tracking	No

*If the status of attack fix is *yes*, it means the attacker cannot use that approach to launch a similar attack on the latest standard.

standard. Most operators may prioritize the deployment of NSA to rapidly bring new technology to the market and monetize their investment gradually rather than move all at once.

From a security perspective, the selection of either deployment strategy has particular impacts. Unlike SA-deployed networks with the full benefits of native security in a new standard, operators have to support a transition procedure which can be a potential security risk. To support NSA in 5G, operators must deploy EUTRA-NR Dual Connectivity, where 4G-LTE is the master radio access technology and 5G-NR serves as secondary radio access technology with UEs connected to both radios [9]. However, the use of confidentiality protection is optional [8] in the dual authentication and may open the door for potential exploitation if not set up correctly.

D. Lessons learned from the security issues and enhancement from 1G to 5G for 6G security

Every network generation has its shortcomings. Although many methods have been developed to mitigate exploitation, several vulnerabilities remain as a result of the complexity of replacing core protocols. Table II summarizes several *known* security attacks and privacy violations against the security architectures and core authentication protocols across the prior generations, in conjunction with their statuses of being fixed. The attacks are categorized by the security principles (confidentiality, integrity, availability). Following the summary, signalling DoS, DDoS against authentication servers, energy depletion attacks, and user tracking are four of the many attacks that will continue to be a headache with 6G security architecture and applications. This stems from the fact that the flaws in the underlying protocol designs (e.g., weak authentication) and the limitations of radio resources are generic issues of all network generations, and to fix them perfectly is a challenge. In summary, four key lessons learned from the security issues and enhancement of legacy networks are as follows.

1) *New applications are often sources of security threats which in turn call for security enhancement*. New applications offer brand features that highlight the enhancements of new network standards compared to those of earlier generations. However, they potentially result in new vulnerabilities. For example, the VoLTE protocol contains a security problem of keystream reuse in two subsequent calls. Exploiting this vulnerability, an attacker can decrypt the contents of an encrypted VoLTE call and eavesdrop on phone calls [61], [63]. Many studies [2], [3], [29], [76] forecast that 6G will host a wave of new applications such as mixed reality and autonomous driving, which will probably also be susceptible to impersonation and DoS attacks. Enhancing the security capabilities of the technologies, before they go into operation, is thus an important issue.
2) *Supporting a legacy protocol in a new protocol deployment could expose old vulnerabilities*. The root causes are the challenge of protecting devices on old network parts with weak security capabilities and the incompatibility of core security functions of two different network standards. To address the incompatibility, the new standard must often switch to ask the old

architecture to authenticate old devices. This access control model potentially exposes old vulnerabilities in an earlier standard. For example, an attacker can launch a downgrade attack [48], [50] to force 4G-LTE devices to connect to 2G/3G networks. Then, by exploiting the vulnerabilities of no mutual verification between the UE and authentication servers in the 2G/3G standards, the attacker can freely collect the IMSI of UE and track UE location. If 6G supports legacy 4G/5G devices, security issues to guarantee the compatibility for dual network access authentication and identity management should be considered seriously.

3) *Fewer changes on protocol designs but more changes on protocol implementations are good to introduce fewer new vulnerabilities, but fixing more existing vulnerabilities faster*. This starts from the fact that fixing security architecture and protocol flaws, such as in AKA and subscriber identity management, often requires large-scale core equipment upgrades, even to end-user devices. The change can lead to a burden in finance, which many operators and subscribers may not be ready to accept. A new architecture and protocol design also needs substantial time to have its security capabilities verified, so as to avoid new vulnerabilities introduced in a real environment. A workable schedule is to prioritize security patches for protocol implementation or updates for intrusion prevention systems at the endpoints that can mitigate the impact of existing vulnerabilities. However, in the long term, a design upgrade that thoroughly eliminates the flaws and weaknesses of the old architecture is still critical.
4) *Mutual authentication and end-to-end encryption are still a challenge and the subject to demand a breakthrough*. Absence of these two features is a major source of many notorious attacks such as fake operators, eavesdropping, and traceability attacks. Even 5G is likely to fail to meet these security goals, since implementing these two features faces challenges of high computation and communication overload. Without a breakthrough in processing capacity and management models, a mandate of strong end-to-end encryption and mutual authentication in 6G can impact on many latency-sensitive services. Any delay to have such features in 6G can practically sink the hope of thoroughly fixing the existing security issues.

IV. 6G NETWORK VISION AND POTENTIAL CHANGES OF ITS SECURITY ARCHITECTURE

Each new generation of cellular networks always attempts to define or upgrade at least one of the security architecture components, such as new authentication and key management, to address challenges from new applications and business models. This section gives an overview of 6G roadmap and new changes of 6G enabling technologies in three layers (physical layer, connection/network layer, service/application layer) based on current studies and recent 6G white papers [77]–[80]. Through changes of those components, we outline security requirements and potential solutions, particularly in security architecture.

A. 6G applications, network vision, and potential security threats that impact on 6G security and privacy

6G starts the wheel of its typical 10-year evolution cycle. Based on the studies in the literature (e.g., [1], [2], [11], [81]), we summarize a roadmap of envisioned 6G development, Key Performance Indicators (KPIs), and spectrum usage in comparison to those of prior generations in Figure 3. Notably, 6G will enable network speeds over 1Tbps, latency under 1ms, and energy efficiency 10-100 times better than 5G. 6G is also set with the long-term goals in mind for a sustainable and carbon-neutral world in United Nations Sustainable Development Goals (UN SDGs) at 2030s or the Internet of Senses [82]. To achieve the requirements of KPIs, 6G is targeted at three significant changes in the air-interface level: (1) pushing communications to higher frequency bands, (2) creating smart radio environments through reconfigurable surfaces, and (3) removing the conventional cell structures, such as cell-free Multiple-input and Multiple-output (MIMO) [83]). Given the spectrum at lower frequencies in earlier generations of networks no longer applied/used, besides using compatible frequencies (6G mmWave), 6G will explore new high-frequency spectrum and photonic signals (300GHz-3THz) [2], [11], [81] for native 6G communications (6G THz). Also, multi-user MIMO, holographic radio beamforming, orbital angular momentum, and VLC are important technologies to enhance 6G communications [79], [80]. A brief selection of key enabling technologies for 6G physical layer is listed in the first row of Table III.

At the connection (network) level, 6G network architecture will have several significant changes from 5G. First, 6G may achieve the concept of Network as a service (NaaS) and network automation. NaaS allows users/enterprises to personalize networks based on their needs. This per-user basis model requires a new network design. Intent-based networking, end-to-end softwarization, cloudization, and deep slicing/function virtualization are key technologies to achieve the target. Second, the rapid shift of 5G infrastructure deployments towards cloud-based networks and open source, particularly for core/RAN network components, signals the "full openness" era of 6G. The development model can unlock the potential of 6G [84], as features and improvement can be contributed at scale. This trend is primarily driven by top vendors (e.g., AT&T) to avoid depending entirely on specific equipment makers. 6G can be the first truly AI-empowered wireless cellular network. This vision will transfer the concept of "*connected things*" in 5G to "*connected intelligence*" in 6G, where most network functions and nodes will likely be controlled by AI [85]. According to [80], Deterministic networking (DetNet) or Time-Sensitive Networking (TSN), which aims to provide guaranteed latency and zero data loss, can be an important upgrade in 6G to satisfy the requirement of 6G ultra-reliable and low-latency communications (uRLLC).

With the new network capabilities, 6G extends the capacity of the three key services of 5G (uRRLC, eMBB

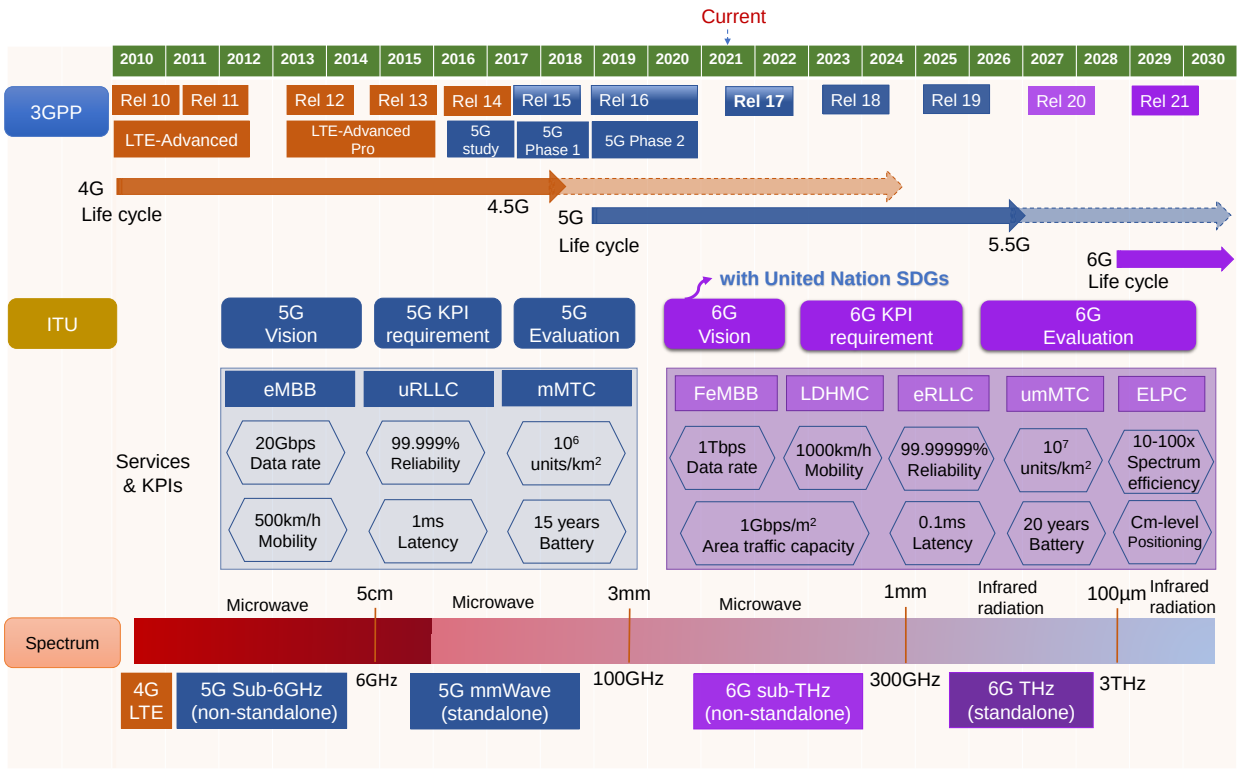

Fig. 3. The roadmap of 6G in comparison with 5G life cycle. KPI: Key Performance Indicator; eMBB: enhanced mobile broadband; uRLLC: ultra-reliable and low-latency communications; mMTC: ultra-massive machine-type communications; FeMBB: further-enhanced mobile broadband; ERLLC: extremely reliable and low-latency communications; LDHMC: long-distance and high-mobility communications; ELPC: extremely low-power communications; umMTC: ultra-massive machine-type communications; THz: Terahertz.

and mMTC) while also enables new features such as long-distance and high-mobility communications (LDHMC) and extremely-low power communications (ELPC) – as illustrated in Figure 3. Notably, new applications are supposed to appear in 6G, including extended reality/digital twin, tactile/haptic Internet, smart medical nano-robot, fully automated driving, and holographic telepresence [2], [3]. Extended reality (XR) refers to the combination of Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) to enable real-and-virtual combined environments and human-machine interactions in real-time. In 6G, XR will be a key technology for many futuristic industries such as manufacturing, education, and training, including practicing for hazardous environments that are too risky or expensive to carry out on the field. Similarly, the digital twin extends the combination of virtual reality technologies (VR/AR/MR) to simulate the real-world counterpart (copy of physical objects and their behavior in real-time), such as modeling urban environments for planning practice. Tactile/haptic Internet denotes an internet network of ultra-low latency, extremely high availability, reliability, and security that can enable humans and machines to interact with each other in real-time. Finally, autonomous driving and holographic telepresence are the prospective technologies in 6G that also require ultra-low latency and extremely high reliability. To support these time-sensitive applications, more computing power will not only be placed at the edge but at every hop of 6G communications. AI technologies are expected to play a key role in boosting intelligence and autonomous capability in such computing nodes. Following [3], [86], other enabling technologies for 6G service layer and AI are summarized in the third and fourth rows of Table III.

B. Space-air-ground-sea integrated networks in 6G: the premise for convergence of heterogeneous networks

3GPP has initiated the first discussions on the integration of non-terrestrial networks with mobile terrestrial systems that will be likely ready to use in the early 2030s [87], the era of 6G. In essence, the space-air-ground-sea integrated networks model can enable high-rate, reliable transmission and extremely broader coverage than four separate network segments. Figure 4 illustrates the shape of 6G space-air-ground-sea integrated networks. The networks will use high-altitude platforms (e.g., floating stations), low-earth-orbit satellites, terrestrial base stations, and on-board ships to relay signals among the end-devices in coverage. With the expansion of coverage, 6G will bring up broadband transmission for maritime communications that will significantly benefit users in offshore ships and islands [88], [89]. The benefits may be beyond civil applications of infotainment or remote learning, e.g., enhancing efforts to rescue persons and ships in distress. However, many challenges still should be overcome, such as protocol optimization designs to reduce the propagation delay, operate different RAN capabilities, and keep service continuity (between mobile terrestrial systems and non-terrestrial

TABLE III
COMPARISON OF KEY ENABLING TECHNOLOGIES FOR 5G AND 6G

Layer		5G	6G	Challenges
Physical layer	Spectrum & communication	● Sub-6GHz ● mmWave communication	● mmWave communications ● Terahertz communications ● Visible Light Communication (VLC) ● Molecular communication	► High-frequency processing in THz consumes much energy, no commercial THz chip ► Molecular communications are still under development
	Antenna modulation	● Massive MIMO, NOMA ● Beamforming ● Intelligent Reflecting Surfaces	● Ultra-massive MIMO, Cell-free MIMO ● NOMA ● Holographic radio ● Large intelligent surfaces (LIS)	► Most technologies are still at the early stage of research and development ► Heterogeneity of 6G devices and services
	Coding	● LDPC, Polar code	● Multiuser LDPC, space-time coding	► High energy consumption, challenge to process terabits per second
Connection layer (Network layer)	Networking & features	● SDN ● NFV ● Network slicing ● Blockchain ● UAV networks ● Low-power networks	● SD-WAN ● NFV ● Deep slicing ● Blockchain, distributed ledgers ● Deterministic networking ● Quantum communications ● Space-air-ground-sea integrated networks	► Challenge to transform the current Internet into the fully software-defined networks ► High cost to deploy deep slicing ► Quantum computers have not yet been realized ► The complexity to manage space-air-ground-sea networks over the worldwide area ► Few commercial blockchains/distributed ledgers
Service layer	Edge/Cloud features	● Cloud services ● Container-based virtualization ● Edge computing ● Massive IoT services	● Services everywhere ● Container-based virtualization ● Zero-touch service orchestration ● Distributed/autonomous computing ● Quantum computing	► Quantum computers have not yet been realized ► Edge servers have not yet fully deployed ► High energy consumption
AI in use	AI model & capability	● Machine learning ● Deep learning	● Trustable AI ● Explainable AI ● Superintelligent AI	► Current AI has no creativity ► Design of low-complexity AI solutions

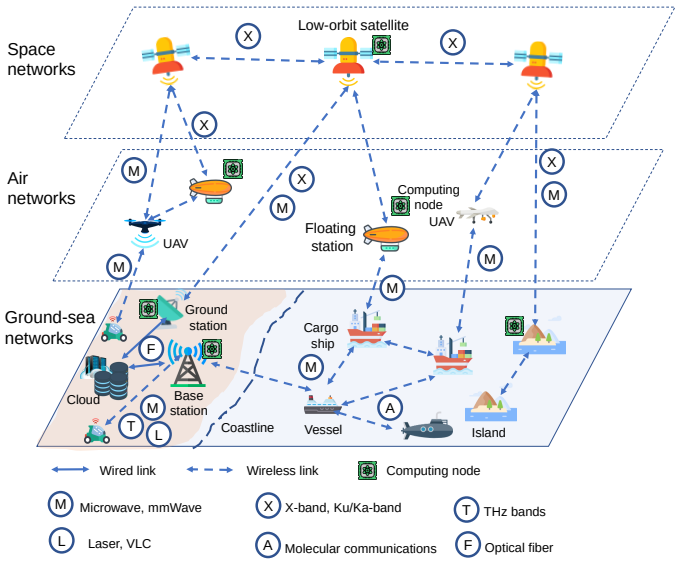

Fig. 4. An overview of 6G networks with the integration of non-terrestrial networks and mobile terrestrial systems, including the communication technologies for the typical links (e.g., satellite-ground link, satellite-aerial link, inter-satellite link, aerial-sea link, aerial-ground link, point-to-point link (ground), ground-sea link, ship-to-ship link).

networks) [87]. Cooperation for infrastructure sharing among different operators is also critical since the satellite-based access systems and ground stations may be located in different regions.

From security perspective, non-terrestrial networks are also vulnerable to wireless-targeted security attacks such as jamming and signalling DoS attacks [37]. Degradation of signals because of such attacks can interrupt communications and delay delivery of messages in critical applications. Moreover, with the important role of high-altitude platforms, masquerading base stations becomes a real threat in hostile areas. With the high heterogeneity of network structure, the appearance of new 6G applications and enabling technologies creates new challenges for security and privacy preservation. Figure 5 highlights six typical applications and six key security requirements for 5G and 6G networks, summarized from the literature [20], [28], [37], [88], [90]–[92]. Notably, besides enhancing most 5G security principles, real-time security protection and full security automation will be the two key features to appear in 6G, given the rise of many time-sensitive applications and the complexity of integrated networks. Many believe that advanced AI and high-performance computing will be key factors to realize the goals. In this vision, 6G will continue the trajectory of migrating enterprise security services into the edge nodes and clouds in 5G while advancing pervasive data intelligence usage to enhance the protection capability. Finally, Zero Trust and Zero Touch architecture, where the protection system is supposed not to trust anything and keep verifying every entity before granting them access or the hassles of passwords are expected to be eliminated, is likely the mainstream of 6G security systems to stop data breaches.

C. Overview of several security and privacy issues on typical 6G applications: finding the origin of the issues

Table IV summarizes security and privacy issues on the applications, security requirements, potential solutions, and remaining challenges. In general, different applications have different requirements in terms of security. Similarly, the attacks vary by application. However, several attacks can impact multiple applications. For example, an attacker can launch signalling DoS attacks to overload and degrade the performance of nearly all the services (e.g., XR, tactile Internet, autonomous driving). On the other hand, eavesdropping, jamming, or API vulnerabilities are common in autonomous driving and space-air-sea networks. Because of the impact of an attack on multiple applications, in the next sections, we adopt the three-layer architecture to classify attacks and corresponding defense solutions for 6G enabling technologies instead of focusing on several applications only. This layer-based review approach can significantly benefit the operators

TABLE IV
SECURITY AND PRIVACY ISSUES OF SEVERAL 6G APPLICATIONS

6G applications	Reference	Potential security issues	Potential privacy issues	Security requirement: High confidentiality & integrity	Zero Touch	Subscriber privacy	Ultra-lightweight security	Real-time security	Energy efficiency	Key solutions	Open challenges
Extended Reality Digital Twin	[90]	Embed malicious content into XR applications to attract click, deepfake XR services, malware injection, DoS against XR services, physical damage	Expose biometric data such as iris or retina scans, fingerprints and handprints, face geometry, and voiceprints	M	H	H	H	M	M	Security edge protection, differential privacy, IDS/MTD	Practical implementation of real-time security
Tactile interaction	[20], [92]	DoS against tactile services, Man-in-the-middle attacks	Expose biometric data such as fingerprints	M	H	H	M	H	L	Physical layer security quantum-safe communications IDS/MTD	Practical implementation of real-time security
Space-air-sea communications	[28], [88]	Jamming, DoS attacks, eavesdropping, API vulnerabilities	Signalling-based location tracking, expose identity	H	H	H	M	M	M	End-to-end security, non-ID, blockchain, distributed ledgers, quantum communications, firewall/IDS/MTD	Practical implementation of blockchain/distributed ledgers, quantum communications, end-to end security
Smart medical Nano-Robot	[93]	Inject malware to create malfunction device cycles and cause physical damage	Expose body health information such as heat rate, blood pressure, pathological behavior..	H	H	H	H	L	H	Physical layer security, IDS/MTD	High-performance edge security, efficient lightweight security, energy efficiency
Autonomous driving	[91]	Jamming V2X DoS attacks, eavesdropping, Fake beacon messages to create virtual traffic jam, sudden crash...	Location tracking, compromised credentials (pseudonyms)	H	H	H	L	H	M	Blockchain, distributed ledgers, misbehavior detection, physical security isolation, IDS/MTD	Practical implementation of blockchain/distributed ledgers, real-time edge security
Holographic telepresence	[20], [94]	DoS attacks, eavesdropping, deepfake agent	Expose personal behavior, social habits, biometric data	M	H	H	M	H	L	Physical layer security, IDS/MTD	Ultra-lightweight security, energy efficiency

L: Low; M: Medium; H: High; DoS: Denial-of-Service, V2X: Vehicle-to-Everything; XR: eXtended Reality
IDS: Intrusion Detection System; MTD: Moving Target Defense

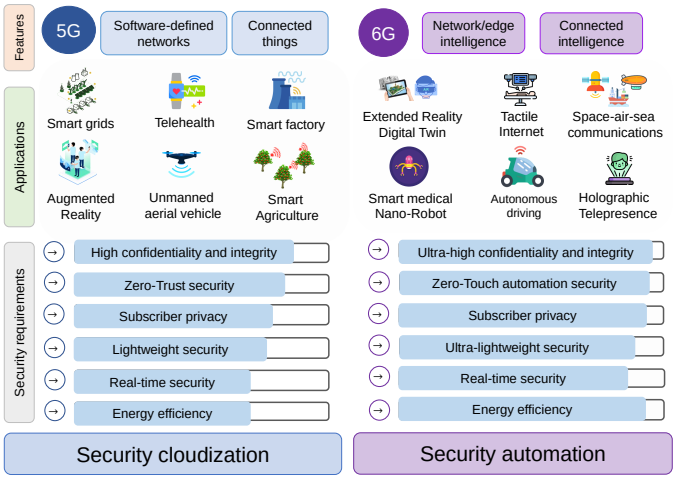

Fig. 5. An overview of typical 6G vs 5G applications and security requirements in comparison. 6G security will upgrade 5G security with new capability in terms of intelligence, automation, and energy efficiency.

and developers of interest in preventing specific attacks that cause high risk to many applications while not limited to the six typical ones listed in this subsection. The flaws of related protocols and the remaining challenges of the technologies are then the starting points for further enhancements.

D. 6G for the expectation of the Internet of Everything and security evolution

6G is expected to be the mobile generation network for heterogeneous technologies. According to [2], [95], the human-to-machine and machine-to-machine interaction promise to become more common to support wireless brain-computer applications, smart implants, textile integrated fabrics, and autonomous health in upcoming decades. In this vision, 6G will enlarge the interconnectivity beyond the things for a world of the Internet of Everything (IoE) where many wireless technologies coexist. 6G IoE will expand the common uses of IoT applications and offer them for every industry. Due to the significant expansion of the network coverage, many self-organizing networks (SON) will be proposed and operated in practice, where AI-empowered automation control systems can assist in simplifying the planning, configuration, management, optimization, and healing of mobile radio access networks and beyond. In 6G, SON can be enhanced to self-sustainable networks (SSNs) [2] to eliminate the need for separate charging of heterogeneous devices, e.g., by combining energy-efficient communication, energy harvesting/power transfer techniques, and offloading of energy-intensive processing from the devices to the computing nodes (servers located at the edge or floating stations as the illustration in Figure 4).

With the transformation of the network technologies and applications towards autonomous functions and heterogeneous connectivity, 6G security and privacy issues will significantly differ from conventional IoT and computer security. First, contemporary IT security is not designed for serving a massive number of connected and high-mobility heterogeneous devices. These large-scale IoT devices, which are not equipped with strong cryptography schemes or mutual authentication as a result of their resource/energy constraints, could introduce enormous concerns of the weak links for intrusion. Second, security aspects of the new protocols in 6G IoE communications such as brain-computer interactions and molecular communications will require specific security protection requirements (e.g., trustable communications or real-time response), due to the direct risks to human life. However, 6G may still inherit several security threats from legacy networks and IoT/IT environments due to using the same fundamental protocols, e.g., TCP/IP. Some example attacks are DoS, eavesdropping, vulnerabilities exploitation, and spoofing, as shown in Table IV. With heterogeneous networks' high complexity, 6G needs new security and privacy preservation approaches, e.g., more automation and interoperability support. In the following

subsection, we envisage 6G overall security architecture and sketch out the potential changes, which are then detailed in the next sections.

E. Vision of 6G security architecture and potential changes

6G will certainly require adjustment in its security architecture to satisfy new applications and the expansion of the space-air-ground-sea integrated network model (as presented above). Figure 6 envisions an abstract 6G security architecture with several key potential changes in core components of current 3GPP security architecture. Figure 7 illustrates six new changes for core components of 6G security architecture and their potential impact on related stakeholders: network operators (①—④), subscribers (②,⑤), and service providers/developers (⑤,⑥, ⑦). In the chain, network operators provide network connectivity for subscribers and probably the dedicated Internet infrastructure for service providers, tenants, and developers. Therefore, network operators will be the main stakeholders to upgrade the network access and network domain security infrastructure. The service providers offer value-added services for subscribers (infotainment, web) and probably platforms for developers/tenants (cloud storage, data analytic). At this aspect, the service providers will take into account the upgrade on the application domain and service-based architecture security. Since developers develop and maintain cloud/edge applications (XR/AR game), the potential upgrades of enhancing security for application development or supporting new security API (following the services provided by the third-party providers) will be their task. In 6G, network operators can play the role of a service provider, e.g., mobile storage. As a result, they may also involve in many parts of enhancing service security. Finally, subscribers may see little impact from the upgrades, e.g., by changing a new device or the SIM card registration.

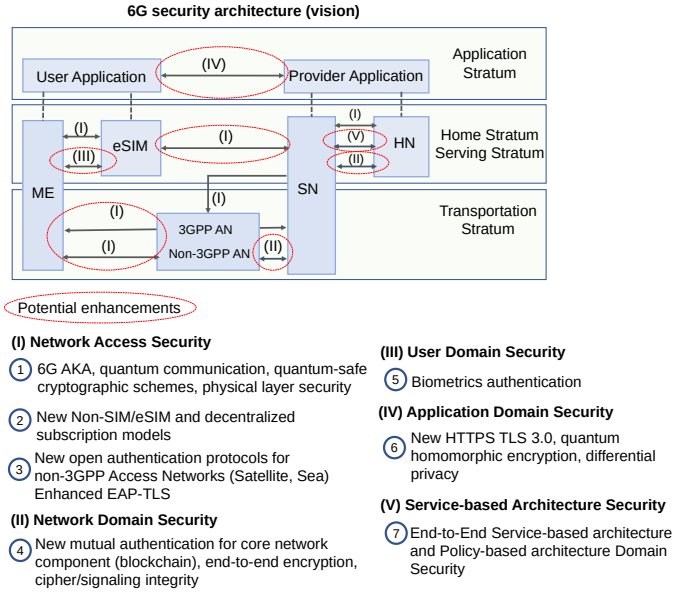

Fig. 6. Abstract 6G security architecture and potential changes for core components in 6G security architecture (marked by red circles). ME: Mobile Equipment, SN: Serving Network, HN: Home network, AN: Access network.

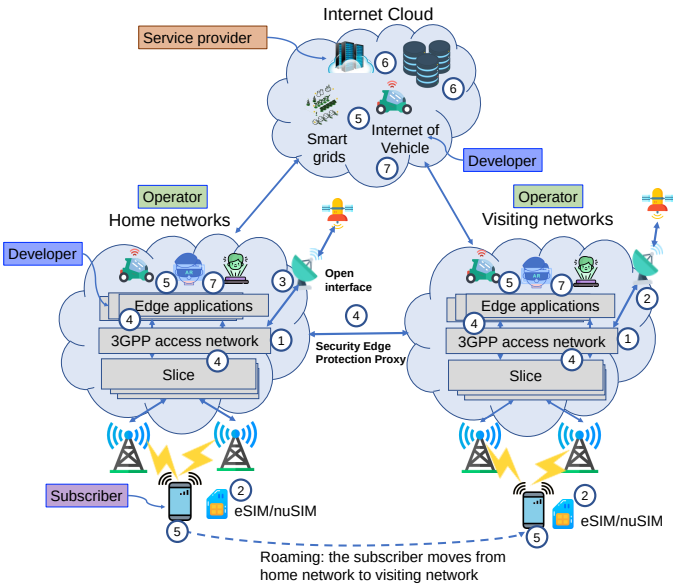

Fig. 7. The illustration of seven changes of 6G security components (①—⑦ in Figure 6) and the potential impact on the related stakeholders: operator, subscriber, and service provider/developer.

① *6G requires new authentication model and cryptographic schemes for communication security. 6G-AKA, quantum-safe cryptographic schemes, and physical layer security are the top candidates*. The changes in 6G network design towards cloud-based and open programmable networking platforms urge reform of authentication architecture. 6G will likely inherit some security models from 5G, such as a unified authentication platform for both open and access network agnostic. However, many new functions need to be added to complement these. For example, a 6G-AKA protocol needs to certify the clear roles of which component, Authentication Server Function (AUSF) or Security Anchor Function (SEAF), will decide authentication in cross-slice communications. 6G-AKA needs to be able to verify the claimed identity of an endpoint in a deep-sliced and open programmable networking platform. Other than improving network access control, physical layer security can be a game changer to protect 6G IoT networks against conventional threats such as impersonation attacks. Details about physical layer security for 6G are presented in Section V. Quantum-safe cryptographic schemes [96] are prospective technologies for secure communications in 6G, particularly for highly sensitive and strategic sectors such as banking or defense. These technologies are a remarkable upgrade in 6G. In turn, crypto-systems such as elliptic curve cryptography (ECC) may not disappear soon, at least not until their replacement by quantum technology is technically practicable. Details of quantum-safe cryptographic schemes communication security are presented in Section VI-B.

② *New user identity management model will be the major change of 6G subscriber management, compared with 5G*. Despite many enhancements in security and convenience, SIM cards and the identity management model have seen no significant change since 2G. The requirement of plugging it into devices practically limits many IoT applications. Using an

TABLE V
SECURITY DOMAINS, STAKEHOLDERS, AND STANDARDIZATION BODIES.

Security domain	Features	Main stakeholders	Standardization bodies	Potential upgrades in 6G
Network access security	Enable a UE to authenticate and access to access network securely (3GPP access and Non-3GPP access), prevent attacks on the radio interfaces	● Network operator	● 3GPP, ETSI, ITU-T, NGMN ● 5G PPP, IETF, NIST	► Physical layer security (Section∼V) ► 6G authentication and key management, endpoint security (Section∼VI) ► Trust networks (blockchain) (Section∼VI)
Network domain security	Enable network nodes to securely exchange signalling data and user plane data (e.g., serving networks and home networks)	● Network operator	● 3GPP, ETSI, ITU-T, NGMN ● 5G PPP, IETF, NIST	► Enhanced IPSec/TLS (Section∼VI)
User domain security	Secure the user access to mobile equipment	● Subscriber ● Network operator ● Device vendors	● 3GPP, ETSI	► Distributed subscription (Section∼VI)
Application domain security	Enable user applications and provider applications to exchange data securely	● Developer ● Service provider	● 5G PPP, IETF	► Biometric authentication (Section∼VII) ► Enhanced HTTPS (Section∼VII) ► AI-empowered security (Section∼VIII) ► Enhanced privacy (Section∼IX)
Service-based architecture security	Enable network functions to securely communicate within the serving network domain and the other domains, e.g., network function registration, discovery,	● Service provider ● Developer	● 5G PPP, IETF	► End-to-end SECSaaS (Section∼VII)

◇ 3rd Generation Partnership Project (3GPP)'s major security fields: Security architecture, authentication, RAN security, subscriber privacy, network slicing
◇ European Telecommunications Standards Institute (ETSI) 's major security fields: NFV, MEC security, security architecture, privacy
◇ Union International Telecommunications Standardization Sector (ITU-T)'s major security fields: Cybersecurity, trust networks, authentication
◇ Next Generation Mobile Networks (NGMN)'s major security fields: Subscriber privacy, MEC security, network slicing
◇ 5G Infrastructure Public Private Partnership (5G PPP)'s major security fields: Subscriber privacy, security architecture, authentication
◇ Internet Engineering Task Force (IETF)'s major security fields: Security protocol draft standards in RFC, public-key infrastructure
◇ National Institute of Standards and Technology (NIST)'s major security fields: Information security standards (ISO 27001, NIST SP 800-53,...)

eSIM (a SIM card embedded in a mobile device) or non-SIM model can remove the barriers to 6G implant devices. This shift will require a fundamental change in identity storage or release, e.g., a SIM could be part of a system-on-chip (nuSIM) [29]. A decentralized subscription model can be another significant upgrade from the centralized authentication and authorization paradigm of 5G. Currently, a visited network can neither authenticate the UE in 5G nor sell any service (e.g., VR/AR content) to subscribers [97]. A roaming agreement must be made to connect with the UE's home network, which charges all the services. Such a model will protect the revenue for home operators, which at least comes with a revenue-sharing agreement with the visited networks. Because of the hostility of operators, this roaming model has not as yet been changed from 2G. From a user's perspective, such roaming is quite inconvenient, particularly if the user leaves the home network's coverage. It will be a significant upgrade in 6G if the visited network can authenticate the UE for the services it provides to the UE, and as does the home network. However, it is unclear how one would balance the right of operators if using a decentralized subscription. Until there is a new business model to satisfy operators (e.g., monetizing from extra application services), or a mutual trust protocol among operators, a centralized subscription model and authentication for roaming connections between the home network and a serving network will need improvements in the coming years. Given the inevitable transition from traditional telephone services to VoIP and Internet services, the revenue drop of the roaming division may motivate operators to accept the sell-access-as-service model. In that way, the current authentication model may have more space to be simplified in 6G.

③ *New open authentication protocols are necessary because of the expansion of 6G to non-terrestrial networks, such as satellite and maritime communications, new open authentication protocols are necessary*. 6G can open more interfaces for heterogeneous applications such as space-air-ground-sea networks. Other than EAP-AKA and EAP-TLS, this means that more standards may be rolled out to support authentication in maritime communications. However, compared to traditional ground or satellite networks, the integrated network will be affected by limited and unbalanced network resources [98]. Supporting open authentication protocols for the integrated network is highly recommended and a subject of many ongoing efforts, e.g., in [99].

④ *Mutual authentication is critical for the goal of 6G trust networks*. In 5G, mutual authentication is still based on a conventional symmetric key model. However, Blockchain and Distributed Ledger Technologies (DLT) can be prospective solutions to change the way of protecting confidentiality and integrity in 6G [100], [101]. Blockchain and DLT guarantee mutual trust, high privacy preservation, and single-failure disruption prevention. They can also enhance the communication reliability of 6G key entities, such as authentication servers or between a Serving Network and a Home Network. However, blockchain and DLT are at a very early stage due to many of their fundamental components still under active development. Storing and processing large-scale records/blocks at the nodes in time need further breakthroughs in the coming years since operations of the state-of-the-art blockchain solutions require huge memory and resources (for mining power-of-work). Such a computation burden can significantly impact network performance and device energy, limiting many potential applications.

⑤ *Biometric authentication or a passwordless service access control model is a long-awaited feature for security in 6G applications*. Password-based protection models have been essential for protecting many applications for decades. However, they have many shortcomings. Some are easy to be compromised, costly in storage, and hard to memorize. Future technology like brainwave/heartbeat-based authentication can provide more theft-resistant and enhance user experience:

citizens can use their bio-identity to access the network and services anywhere without tracking many passwords. This *passwordless* authentication will be a massive leap forward for a 6G security posture. More details about such authentication schemes are given in Section VII-C.

⑥ *Enhanced HTTPS TLS and homomorphic encryptions are the future technologies to enhance service and data security in 6G applications*. Notably, both enhanced HTTPS TLS and homomorphic encryption will be equipped with quantum-resistant algorithms to resist quantum attacks (e.g., AES-256 or ECC P-384). Besides, homomorphic encryption allows performing operations, such as search and query, on encrypted data directly without decryption. Therefore, subscribers can send their data to third parties (e.g., operators, cloud providers) for storage or processing. More details about enhanced HTTPS TLS and homomorphic encryption are given in Section VII-F.

⑦ *Service-based Security Architecture in 5G is upgraded into End-to-End service-based and Policy-based security architecture in 6G*. A Service-based Architecture Domain security is the pillar of 5G security architecture. 6G will take this feature to a new level, End-to-End Service-based Architecture or even Policy-based architecture domain security, to satisfy the personalization and micro-deployment flexibility. Furthermore, applications such as mixed reality may move closer to a UE, i.e., on edge nodes. For optimization purposes, the protection model for communication between a UE and such applications may work based on flows or flexible control by policies from the control plane unit of the serving network.

Table V summarizes 6G security components, the related main stakeholders, corresponding standardization bodies and mentioned potential upgrades for each of them. More details of the changes are subsequently presented in the next sections.

F. Summary of lessons learned from key possible changes of 6G security

This section reviews the key changes of 6G in terms of enabling technologies, security requirements, and security architecture. In summary, three lessons learned from these potential changes for 6G security architecture are as follows.

1) *Many 5G features will not fade away but be fully supported with further security enhancement for 6G usage*. United authentication framework and security isolation in 5G technologies will continue to play a central role in 6G to converge the authentication features for multi-access networks. However, given the expansion of network coverage to the space-air-ground-sea integrated environment, security capabilities of the 5G-AKA framework will be the target of further enhancements.
2) *Deploying non-SIM-based identity management will be a huge step for 6G security*. This ambitious goal is to reform the current SIM-based identity management to using a non-SIM card and decentralized subscription model. Pursuing this goal will be an important step towards removing the barriers to implant devices and user experience in 6G. However, it is unclear whether operators will support such bold changes. Enhancing eSIM technologies can be a reasonable approach to prepare for a future leap of the transition.
3) *A unified authentication framework, passwordless authentication, and open security model are the future of 6G security, but in relevant context*. A unified authentication framework and open interface model can enable access control and security architecture simplification for space-air-ground integrated networks – a key goal of 6G. Meanwhile, by decreasing the complexity of memorizing and storing login information as in conventional password-based models, *passwordless* authentication is a long-awaited feature that will enhance user experience and convergence of access control that many 6G services expect. However, building a comprehensive architecture to support the features for all 6G applications will require long-term effort. Implementing the features for the applications that need them first and then expanding the implementation to the whole network – when the infrastructure is ready – is likely the best approach.

The following sections cover security attacks and prospective defense technologies, which will powerfully dominate 6G physical layer, connection layer, and service layer, based on the summary in Table V.

V. Security in the physical layer

Since the physical layer is the cornerstone of wireless communications, protecting physical-layer information can prevent many conventional attacks on radio signals such as eavesdropping and jamming that nearly impact on every 6G application. The premise of physical layer security is to exploit the characteristics of wireless channels (e.g., fading, noise) to enhance confidentiality and perform lightweight authentication. Low complexity of physical layer security will particularly benefit 6G low-cost IoT devices, which often lack energy and computation capacity to run advanced authentication mechanisms. Besides, relying on physical laws, physical layer security is robust against cryptanalysis, which has been the top concern of conventional cryptographic algorithms. Physical layer security can be implemented at the base stations/IoT gateways of the operators or in the signal modulation algorithms. The following subsections look at key security concerns and several prominent defense approaches for enabling technologies in 6G.

A. Security in 6G mmWave communications

As we noted in the previous section, when 6G networks start to roll out, a substantial number of 5G devices will still be on. Therefore, mmWave and massive MIMO are still crucial physical layer technologies in 6G compatible (non-standalone) networks. Figure 8 illustrates three common attacks in mmWave MIMO networks: eavesdropping, jamming, pilot contamination attacks (PCA). Eavesdropping is carried out through inferring and wiretapping (sniffing) open (unsecured) wireless communications. In 6G mmWave MIMO networks, beamforming technology can benefit security. As illustrated in Fig. 8, an eavesdropper (Eve) must locate in the beam scope (Figure 8.a) or use a reflector (Figure 8.a) to wiretap the channel. The eavesdropper can be a legitimate person (internal) of the network (e.g., employee) or someone

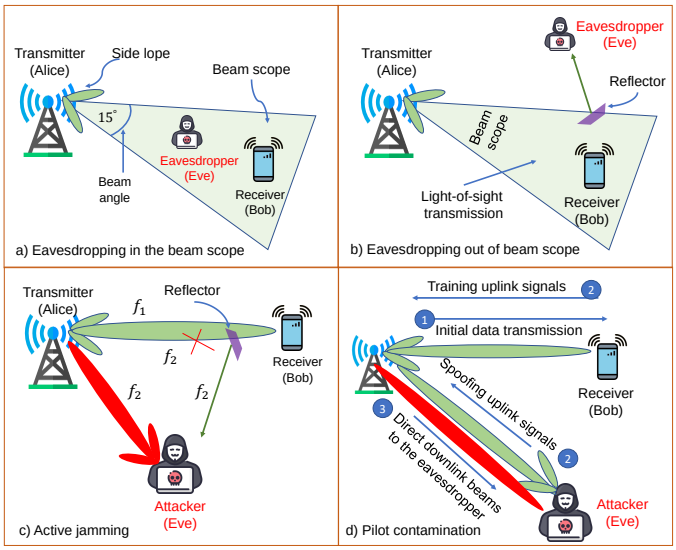

Fig. 8. Illustration of three common attacks against 5G physical layer technologies that can occur in future 6G compatible networks: a) Eavesdropper wiretaps beamforming signals in the beam scope of the transmitter (Alice); b) Eavesdropper wiretaps beamforming signals from the transmitter by placing a reflector in the beam scope of the transmitter (Alice); c) A jammer generates signals at the frequency f_2 (based on the information obtained from eavesdropping attack) that can partially degrade transmission between the Alice and Bob; d) Pilot contamination attacks.

outside (external). Based on the information about the transmission signals (e.g., the frequency f_2) between the transmitter (Alice) and the receiver (Bob), the eavesdropper can carry out two other attacks. One is jamming attack (Figure 8.c), where the jammer can inject radio signals (same frequency as Bob's f_2), so as to occupy a shared wireless channel. Such aggressive injection prevents legitimate users (e.g., Bob) from using a wireless channel to communicate, a kind of DoS. The other one is PCA, where the attacker intentionally transmits identical pilot signals (spoofing uplink signals in step 2 of Figure 8.d) to contaminate user detection and channel estimation phase of the transmitter (Alice). In the worst case, the transmitter will steer the partial beam towards the attacker in the manipulated downlink direction (step 3 of Figure 8.d), which practically degrades a legitimate user's transmission or causes signal leakage. Ultra-massive MIMO and Multi-User MIMO are susceptible to PCA [102]. Besides, a cell-free massive MIMO system can risk itself by exposed location of radio stripes [29], i.e., dense antennas are easier to reach by physical attacks.

Preventing the three aforementioned attack types has attracted much attention recently. In essence, enlarging signal strength between legitimate UEs over an eavesdropper's channels, i.e., maximizing the secrecy rate, is a fundamental approach to preventing eavesdropping and PCA. Key techniques of signal strength-based approaches are to equip secrecy capacity maximization in the precoding process [103], where the transmitter will spread information signals to the receivers to gain pre-knowledge about the communication channel (i.e., channel state information). The most common idea is to introduce extra randomness into the modulation, which aims to prevent an eavesdropper from predicting the next signal sequence/frequency that the transmitter will use. Many recent studies [102], [104] rely on this method. For example, Zhang et al. [105] proposes a method where the sender will create multiple random frequency shifts (as illustrated in Figure 9.a) in the publicly known pilot sequence or frequency hopping to evade eavesdropping. Another emerging technique is to use covert communication with artificial noise or friendly jamming (as shown in Figure 9.b), where artificial interference signals will be added in the null-space of a legitimate user channel to confuse the eavesdropper on the real transmission channel [106], [107]. Another approach is to use physical key generation (Figure 9.d), i.e., to exploit the entropy of randomness in the transmit-receive channels such as Channel State Information (CSI) to generate secrecy keys for communications. The authors of [108] propose a physical key exchange between the transmitter and the legitimate users to verify the transmission against untrusted partners. However, integrating the encryption/decryption process into the precoding can impact the performance of the crowded transmission, let alone the threats of internal attacks (i.e., the eavesdropper is one of the legitimate users). An emerging approach is to use AI/ML techniques (e.g., reinforcement learning [109]) to enhance CSI knowledge and apply proper defense strategies such as channel hopping, although most methods still suffer a setback of high energy consumption. Note that maximizing the secrecy rate can also significantly mitigate jamming attacks. Without obtaining information about particular communication signals between the transmitter and the legitimate receiver (through eavesdropping), it is a challenge for an attacker to jam a communication channel effectively, given the extremely high cost of overwhelming all frequencies in modern times broadband wireless channels. Because of the frequent changes of transmission frequency (frequency hopping), attacking at a fixed frequency also has little impact on the overall performance of the receiver/transmitter. More details on jamming attacks and corresponding anti-jamming methods can be found in the surveys [110], [111].

Remaining challenges

The core issue for MIMO channels is the assumption of the effective precoding process. However, precoding is heavily impacted by fading influence and partial/imperfect CSI in practice. Most existing defense approaches, which have heavily relied on the assumption of perfect knowledge of full or partial CSI information of the eavesdroppers [112], likely fail at their task in the harsh environment. Utilizing secrecy channels with poor knowledge on the CSI of the eavesdropper is then the center of many ongoing efforts. An early study [113] on the issue suggests a potential solution is to transform the uncertain CSI constraints into deterministic ones through decoupling the legitimate transmission outage probability and the secrecy outage probability. The other open challenge is to detect cooperative eavesdroppers, where several eavesdroppers cooperate to wiretap a wireless channel or perform active attacks (PCA) against the base stations [114], [115]. Finally, besides helping to evade the attacks, the attacker can use covert channels to create a backdoor for leaking data or intrude the system. The common defense methods are detecting dangerous

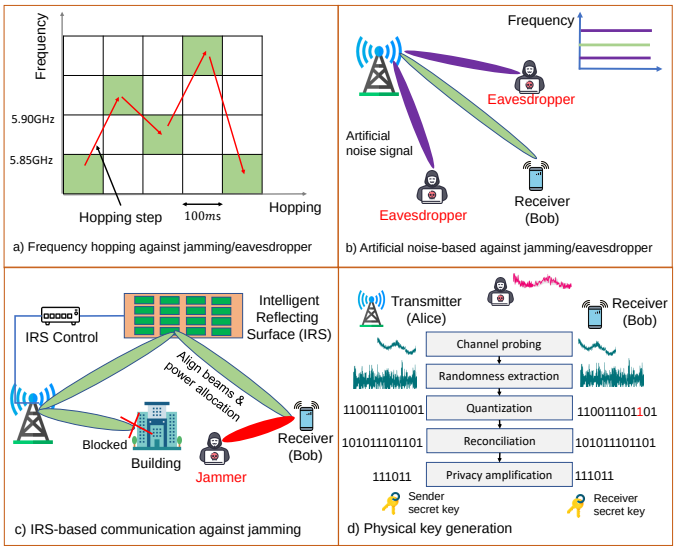

Fig. 9. Illustration of several methods to mitigate eavesdropping/jamming attacks for 6G physical technologies: (a) Frequency hopping; (b) Artificial noise generation; (c) Large Intelligent Surface/Intelligent Reflecting Surface-aided; (d) Physical key generation.

open ports, anomaly signals, or blocking traffic of vulnerable protocols at the upper layers (e.g., ICMP). More detail of covert channel countermeasures can be found at [116].

B. Security in 6G Large Intelligent Surface

Large Intelligent Surface (LIS), the other name of Intelligent Reflecting Surface (IRS), is a revolutionary technology for 5G beyond and 6G that uses a planar array of low-cost reflecting elements to dynamically tune the transmission signal phase shift for enhancing communication performance [117]. LIS supports a programmable space through a LIS controller, which is referred to as intelligent control. Many believe that LIS/IRS will be a critical technology for 6G dense THz networks since deploying so many 6G radio units to overcome the limited coverage of THz communications (presented below) is extremely expensive. By contrast, expanding the use of low-cost LIS/IRS devices (made of metallic or dielectric patches with low-power and low-complexity electronic circuits) to replace several 6G radio units can accomplish the same performance with much lower expenditure. LIS/IRS model benefits security significantly. As illustrated in Figure 9.c, LIS/IRS can be used to reflect the signals between a base station (Alice) and receivers (e.g., Bob), effectively making propagation channel more favorable. This reflecting model is extremely helpful if the direct link quality (between Alice and Bob) is degraded due to far distance or obstacles. The authors of [118] indicate that optimizing the transmit powers and the phase shift at each element of the LIS/IRS can maximize the sum-secrecy rate, e.g., by destructing the reflected signal power to the eavesdropper or providing different communication links to the receivers. Technically, the idea of using IRS as a data transmitting source to enhance security is similar to that of using multi-path propagation channels to provide different secure communication links to legitimate users [119].

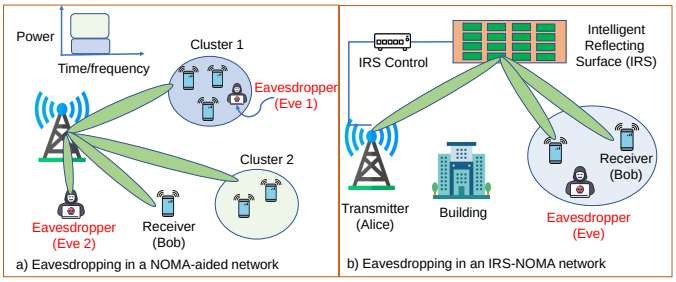

Fig. 10. Illustration of two eavesdropping attack cases in NOMA-aided networks: a) in NOMA-cluster networks and (b) IRS-NOMA networks.

C. Security in NOMA for 6G massive connectivity

Besides MIMO, IRS, and beamforming, Non-Orthogonal Multiple Access (NOMA) is another important technology of 5G that can also be used to support 6G massive connectivity. By allocating channel resources for the receivers fairly via assigning more power for "weak signal" users and subtracting power of strong signal users [120], the NOMA-aided transmitters allow more users to gain the channel, which practically increases the number of simultaneously served users. NOMA supports both multicast transmission (to cluster users) and unicast transmission (to specific user). However, NOMA still suffers multiple security threats. For example, as illustrated in Figure 10, an internal eavesdropper can wiretap or launch jamming attacks on the legitimate users in the beam scope of NOMA clusters (Figure 10.a) or reflecting the scope of Intelligent Reflecting Surfaces (IRS) (Figure 10.b). The mentioned techniques on maximizing the transmission secrecy rate in mmWave can be applied for NOMA-aided networks to mitigate the attacks. Moreover, the assessments from channel condition (weak/strong) of legitimate users from NOMA's successive interference cancellation (SIC) process can benefit the CSI knowledge-based defense strategies [121]. However, in an extreme case, several eavesdroppers may cooperate in interfering with the normal operations of a NOMA, e.g., by sending a large number of identical pilot signals to the NOMA-aided transmitter in the "superimposed messages" broadcasting stage. As a result, the transmitter may waste much power to allocate for these malicious users. In this case, the cooperation of NOMA systems or NOMA systems with the other partners (e.g., IRS) can enhance the security of the systems, i.e., using multi-path channels to provide different communication links to legitimate users. Indeed, enhancing physical layer security for the NOMA-aided networks (i.e., where NOMA is integrated with other technologies such as visible light communication [122] and THz) has been a hot topic recently. A short survey on the relevant matters can be seen at [115].

D. 6G Holographic radio technology with Large Intelligent Surface

Holographic radio, or holographic beamforming and MIMO, is a new paradigm and disruptive radio technology for 6G indoor/outdoor communications that uses software-defined antenna or photonics-defined antenna arrays than conventional

phased arrays or MIMO systems [94], i.e., uses no phase shifter or active amplification in the beam-steering process. With the assist of LIS panels, holographic radio can generate the directional beams perfectly through holographic recording and reconstruction. At this point, holographic radio can enable intelligent and reconfigurable wireless environments [86] while maintaining low cost, spectrum efficiency, and energy efficiency of network devices greatly. From security, similar to LIS technology, holographic radio will benefit the secrecy rate optimization through canceling out reflections of the base station signals to eavesdroppers [94]. On the bad side, the electromagnetic waves scatter uncontrollably in the holographic spatial space can cause more concerns of being interfered with or wiretapped [123].

Remaining challenges

Holographic radio is heavily under development with many remaining challenges, e.g., few available implementations for hardware design. Similarly, the specific researches on the security aspect of holographic radio technology are still in its infancy.

E. Security in 6G Terahertz communications

Terahertz is expected to be the central communication technology in 6G. Technically, THz can enable ultra-high data rate (up to terabits per second [124]) for many 6G applications such as tactile Internet and XR/AR services, which 5G technologies such as mmWave will not be able to support [2], [81]. However, THz technology is strongly impacted by the surrounding atmospheric conditions, i.e., the spectrum is absorbed by water molecules and spreading loss. THz also has low penetration power against specific obstacles (e.g., thick wall). Because of the high absorption resonance, THz's communication coverage is relatively small, within dozens of meters.

With the low coverage area and high absorption resonance, 6G likely includes dense networks of THz-enabled devices for effective communications. To enhance transmission performance, THz antennas will need to perfectly align signal beams to reduce the angular divergence of transmitted signals. The limited transmission coverage and the high directionality characteristic theoretically make THz much more secure and resilient against attacks, e.g., jamming and eavesdropping [125]. To be successful, an eavesdropper's antenna must be located in the beam scope of transmitting signals, which is even smaller than that of mmWave MIMO antenna, to wiretap a THz link. As a result, it will be much more difficult for an eavesdropper to place a receiver and intercept signals without blocking the receiver's transmission and thereby potentially reveal his attack intention. Performing successful jamming in THz networks to disrupt transmission is not also easy. According to [125], given the large bandwidths, THz can enable frequency hopping over a large number of sub-channels. The frequency hopping in a wide range can reduce the probability of an adversary detecting and interfering with a particular signal. Moreover, to jam the link successfully, the attacker must generate high power bandwidth to overwhelm the receiver while keeping a short distance, e.g., several meters away from the receiver.

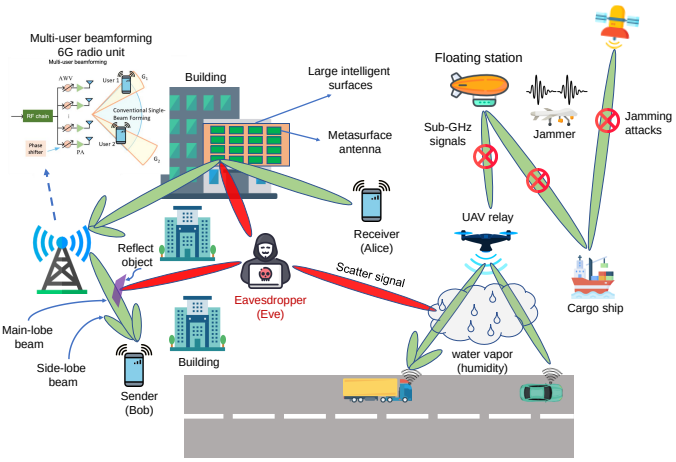

Fig. 11. Illustration of eavesdropping and jamming attacks in 6G heterogeneous networks. The eavesdropper (Eve) can sit behind a building to collect scatter signals from reflectors or the self-creating gaseous cloud.

The high cost and probably the awareness of users make eavesdropping and jamming less attractive.

Despite the high resistance capability against jamming and eavesdropping, THz links can still be attacked in special conditions. The authors of [126] found that wiretapping THz links is still possible in line-of-sight (LOS) transmissions. As illustrated in Figure 11, the eavesdropper (Eve) can place a reflector in the LOS beam scope of the sender (Bob) to scatter the radiation towards the attacker's (Eve's) receiver antennas located behind a building. On the other hand, the attacker can exploit the conditions of high humidity by rain/snow or self-creating gaseous cloud to collect the scatter signals of the THz links in an area (e.g., the link between a UAV and the vehicles in Figure 11). To prevent this attack type, the authors of [125] suggest that several conventional techniques, such as randomly varying power limits, frequency hopping, and strategic access point placement, can make the communication covert and much more difficult for the attacks to be successful. Ma et al. [126] proposed to share data transmission over multiple paths to enhance covert communication. Porambage et al. [37] also hint that the multi-path approach can work with the physical key exchange to support sensitive data transmission. Qiao et al. [127] indicate that LIS/IRS can also assist in steering signal power to desired user in multiple paths and reduce information leakage in Terahertz Systems. If a multi-path propagation link is not possible, lightweight encryption, beam encryption, and spatial modeling can be used [125].

Remaining challenges

Despite many defense techniques, jamming and eavesdropping are still open issues. In an extreme case, [125], cooperation of multiple adversaries to collect scatter signals is still much more challenging to prevent with the mentioned methods, given the complexity of attack re-verification during hand-off of devices. Privacy issues are also particularly concerns in 6G. In essence, the THz spectrum can be used for centimeter-level localization applications. The idea of THz Access Points (APs) following a user's motion to centimeter-level precision for improving link connectivity could expose

user locations that can be abused for inappropriate or harmful purposes. In dense networks like 6G, many THz devices can make the problem much more concerned. If the APs are compromised, they likely become potential surveillance devices for adversaries and unauthorized users. Even with potential data anonymization (detailed in Section IX), sensitive or behavioral information about users can still be assembled from mining information of multiple sources [125]. In this vision, maintaining the privacy principles (as GDPR requires) becomes critical but particularly challenging for devices with limited memory, computation power, and energy. Besides, the location exposure of APs can attract physical attacks to shut down the networks. In conclusion, there is a trade-off between high privacy and optimization for THz communications. A potential solution is to accept conditional anonymity and secure access points with hardware security modules to prevent compromise attacks.

F. Security in 6G VLC communications

Visible light communication (VLC) is a high-speed communication technique to transmit data by using visible light between 400 and 800 THz. According to [128], in an in-lab experiment, a free-space VLC system can integrate with a 50-cent off-the-shelf Light Emitting Diode (LED) to provide peak data rate up to 15.73Gbps over a distance of 1m. Similarly, the study reports the peak data rate for an underwater VLC system can reach 16.6Gbps over 5m and 6.6Gbps over 55-m in water. With a promising future of higher transmission rates and cheap deployment, VLC will be an economical alternative approach to complement 6G THz systems in indoor buildings (hospitals, personal rooms), underwater applications, or electromagnetic sensitive areas (nuclear plants). Another variant of VLC is Light Fidelity (LiFi), which is considered as the incorporation of WiFi and VLC to support bidirectional wireless networking with access points. Besides supporting super-high bandwidth, the big advantage of VLC/Li-Fi over other wireless technologies is almost no limitations on capacity [129] because of the large visible light spectrum. However, VLC/LiFi cannot penetrate a wall.

Like THz, VLC/LiFi is more secure than prior wireless communication techniques, e.g., WiFi. VLC/LiFi's coverage is small and cannot penetrate opaque objects like walls. Similar to THz technology, an eavesdropper has to move into the LOS area of the sender-transmitter VLC/LiFi link to intercept signals. There are several methods to mitigate the risk of such attacks in the literature. The goal is to maximize the secrecy rate under the constraints of the open channel. In an early study, Mostafa et al. [130] proposed to utilize beamforming signals of the transmitters (e.g., main lobe beams focus on the legitimate users) for gaining a certain secrecy rate. For multiple transmit models, the idea of using spatial modulation aided VLC systems with optical jamming has got much attention recently [131], [132]. In this technique, friendly jamming signals will be inserted into the null space of the legitimate user's channel matrix. As a result, the attacker may need to span interference signals to follow and suffer high costs while secrecy channels are protected. Recent studies [132] indicate that the combination of spatial modulation with the zero-forcing precoding strategy to utilize beamforming also gives promising results in MIMO-VLC systems. In essence, friendly jamming and beamforming aid are still mainstream techniques for protecting VLC/LiFi communications.

Remaining challenges

Most recent studies assume a VLC environment with a single eavesdropper only. However, a large-scale VLC network with the presence of multiple eavesdroppers scattered randomly (conference rooms) can be more common in the future. Proposing innovative methods for protecting VLC systems against the collusion of these collusion attackers can be an important topic in the coming years.

G. Security in 6G Molecular communications

According to [133], molecular communication is defined as a communication technique that uses chemical signals or molecules (instead of electronic and optical signals in traditional communications) as an information carrier for nano/cell-scale entities to communicate with each other. At the end of this decade, advanced nanotechnologies may be able to enable the industry-level manufacture of nanodevices to be used for many fields, e.g., drug delivery in blood vessels [86] in healthcare and water/fuel distribution monitoring in industry. The target of molecular communications is to provide connectivity for such nanodevices. 6G specifies the term of the Internet of Nano-Things and extremely low-power communications (ELPC) to indicate the vision of supporting communication among the nanodevices [86]. Besides civil applications, molecular communications are useful to provide alternative communication methods or extra covert channels in harsh environments such as water or adversarial networks (high jamming and interception), where wave-based communications often fail or suffer heavy absorption. In short, because of high promising applications, molecular communications can be in the 6G physical layer [134].

Security and privacy are particular concerns when many nanodevices may be embedded into a human body, e.g., to deliver drugs. A major threat is the potential leak of healthcare information. On the other hand, bio-machines can be remotely attacked if the communication systems are also connected to the Internet. An attacker can exploit classic vulnerabilities of IoT devices to compromise the molecular control system remotely. The authors in [135] envisaged a case where, by manipulating the configuration in bio-machines, an attacker can force to accelerate/delay the absorption process. In another attack, an attacker floods the environment with particles or kills the molecules to disrupt medical application functions in order to harm or kill the host. The side effects will be severe if a large number of bio-machines are in malfunction. In extreme cases, the immune system may react strongly to the malicious stimulate from the malfunctioned bio-machines and harm the body. The study [93] also showed a situation in which nano-robots can be manipulated to damage the patient blood vessels instead of repairing them. However, there have been no such real attacks to be recorded to date. Given the vision of implantable devices and nano-robots to be common in 6G,

protecting molecular communications against the mentioned threats is still critical.

With different network structures and interactions, protecting security and privacy for molecular communications are different from conventional approaches, i.e., existing solutions to wireless communications cannot be applied to molecular systems. Several preliminary studies [93] envisage that biochemical cryptography, which uses biological molecules like DNA/RNA information or protein structure to encode information, can protect information integrity in molecular communications. Suppose molecular communications are connected to the Internet. In that case, we believe that a strict access control system or strong firewall at the gateway portal may need to distinguish unauthorized users and filter out malicious traffic.

Remaining challenges

The research on preventing security attacks and potential data breaches in molecular communications is still at the early stage. Given the ethics, carrying out a real attack to a host or human body is somewhat less attractive.

H. Other prospective technologies for 6G physical layer security

The following three key physical-layer-based technologies will benefit many 6G applications in terms of mitigating special attacks, such as spoofing messages and tampering physical data bits, which can occur on the network and application layers.

1) Physical layer authentication: Physical layer authentication is an emerging technology to crack down spoofing or impersonation attacks. Figure 12 illustrates several cases in which attackers intentionally send falsification messages in vehicular networks to fool nearby vehicles. This attack type can cause high risks to users when connected and autonomous vehicles become popular in 6G [28]. The essence of physical layer authentication is to recognize the identities of subscribers by exploiting location-specific or device-specific properties of wireless channels. For example, it is traditionally difficult to detect Sybil attacks at the application layer, where an attacker uses a large number of pseudonymous identities to send spoofing messages (in vehicular networks) or disproportionately influence reputation-based verification systems (misbehavior detection). Using physical attributes (e.g., angle-of-arrival, Received Signal Strength Indicator) in this case has significant advantages to detect the attack successfully since all the spoofing messages, regardless of using many pseudonyms, come from a single signal source and direction [136]. The authors of [137] proposed to learn unchanging, hardware-based characteristics of the transmitter, such as its instantaneous amplitudes, phases, and frequencies, with the reference templates of all known devices to find out the attacker. The authors of [138] indicate that a deep learning-aided physical layer authentication model can soon outperform conventional statistical methods in terms of detection accuracy, particularly in heavily corrupted channels by noise.

Remaining challenges

CSI estimation errors are the major challenges of physical layer authentication. Since physical layer authentication relies

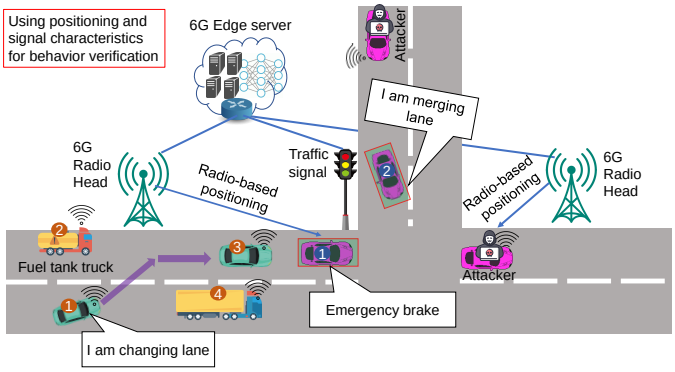

Fig. 12. An illustration of spoofing attacks to disseminate falsification beacon messages to the vehicles behind or approaching ones to an intersection in vehicular networks, which can be very common in 6G.

on the uniqueness of physical characteristics over any transmit-receive channels, it is sensitive to incorrect CSI estimation. Theoretically, a correct reference of CSIs for comparison is a must. However, that assumption is not always correct in all contexts. The authors of [139] found that low SNR (e.g., noise, user movements, distance, etc.) and overlapping CSIs from crowded nearby sources can significantly degrade the performance of the hypothesis testing process. Training data in particular can be compromised with signal patterns from untrusted sources, such as some users colluding with an adversary [140]. Thus, protecting data integrity for hypothesis testing is critical to the success of physical layer authentication. A potential solution is to fuse data from multiple sources or track multiple physical layer attributes, i.e., multi-attribute multi-observation techniques [141], to mitigate the bias of each and enhance the overall detection performance.

2) Physical key generation: Physical key generation is to protect confidentiality for communications between UEs and stations from eavesdropping. The fundamental idea is to exploit the entropy of randomness in transmit-receive channels such as CSI and Received-Signal-Strength (RSS) to generate secrecy keys for communications. Figure 9d) illustrates generic physical key generation on a TDD-based wireless channel. In the randomness extraction process, the sender and the receiver measure both CSI and RSS. Theoretically, the measured information is identical when two terminals are connected by the same wireless channel but can be different if the responder (e.g., attacker) is located one-half wavelength away from the sender. The quantization is to generate the extracted randomness into bits encoded to ensure perfect secrecy in the encoding process. To ensure the keys generated on both sides are the same, reconciliation is performed synchronously between the sender and the receiver. Such synchronous privacy amplification then creates the final encryption keys from the generated bit sequences and practically eliminates the threats from an eavesdropper's partial information, e.g., obtained from any previous processes. Existing physical key generation techniques can be CSI-based [142], RSS-based [143], phase-based [144], or code-based [145].

Remaining challenges

Securing wireless communications based on physical key

TABLE VI
PROSPECTIVE SOLUTIONS TO ENHANCE 6G PHYSICAL LAYER SECURITY

6G PHY technologies	Reference	Security & privacy issues	Key solutions	Key points	Open problems
mmWave MIMO beamforming	[103], [108], [146]	Eavesdropping Jamming Pilot contamination Location exposure	● Frequency hopping ● Injecting artificial noise or friendly jamming ● Utilize beam alignment ● Physical key generation ● Physical coding	Secrecy rate maximization	● Optimal beam alignment ● AI-based low-complexity anti-jamming ● High-performance coding ● Energy efficient solutions
Large Intelligent Surface	[119], [118]	Eavesdropping Location exposure	● Frequency hopping ● Injecting artificial noise or friendly jamming, ● Physical key generation ● Physical coding	Secrecy rate maximization	● Optimal LIS deployment ● AI-enabled LIS ● Specific LIS applications ● Energy efficient solutions
NOMA	[121], [122], [115]	Eavesdropping Power allocation contamination Location exposure Signal space expose	● Frequency hopping ● Physical key generation ● Physical coding	Secrecy rate maximization	● Security for NOMA-VLC, NOMA-THz, NOMA-LIS networks
Holographic radio	[94], [123]	Eavesdropping Location exposure	● Utilize beam alignment ● Randomly power limits ● Access point placement ● Physical key generation ● Physical coding	Secrecy rate maximization	● Optimal radio management ● Joint RF and non-RF hardware ● Holographic radio-LIS integration ● Energy efficient solutions
Terahertz communications	[125], [126], [127]	Eavesdropping Jamming Location exposure	● Frequency hopping ● Randomly power limits ● Access point placement ● Utilize beam alignment ● Injecting artificial noise or friendly jamming ● Physical key generation ● Physical coding	Secrecy rate maximization	● Optimal THz base stations ● Optimal THz-LIS integration ● Optimal beam alignment ● ● AI-based low-complexity anti-jamming solutions ● High-performance coding ● Optimal mmWave-THz links ● Energy efficient solutions
VLC communications	[128], [129], [132]	Eavesdropping Obscured attacks	● Frequency hopping ● Injecting artificial noise or friendly jamming ● Physical key generation ● Physical coding	Secrecy rate maximization	● NOMA-VLC performance ● VLC/LiFi deployment ● Optimal VLC access points
Molecular communications	[86], [93], [135]	Device configuration manipulation, kills the molecules, attacking bio-machines from Internet environment Data leakage	● Biochemical cryptography ● Firewall, IDS to detect attacks from the Internet	Confidentiality & Integrity	● Energy efficient solutions ● Secure Internet access
Physical-aided security	[137], [136], [138]	Sybil attack Physical data tampering Trajectory tracking	● Physical layer authentication	Exploit physical signal attributes to detect special attacks	● AI-based low-complexity solution ● Multi-attribute multi-observation technique

generation has its weakness. First, the key generation process must deal with heavy computation in signal processing and encoding. The key error-correction process in reconciliation requires several extra bits to reconcile bit mismatch that often consumes a significant amount of time and space. Second, due to the limited capacity of wireless channels and reconciliation overhead, physical key generation techniques offer very low key-generation rates. The authors of [143], [147] propose to use group keys to overcome the low-rate problem. The group-key generation model can increase the efficiency of key usages, e.g., all the nodes in a group use an identical key. However, the challenge is to maintain trust in a group. Defining optimal criteria to group the nodes correctly is another open issue.

3) Physical coding for PHY data integrity protection: Physical coding is the fundamental process in communication technology to maximize data transmission rate among legitimate users. However, enhancing physical coding can significantly mitigate attacks on integrity, such as tampering with messages in transit. For now, several structured coding schemes such as Low-Density Parity-check Code (LDPC) coding and polar coding have demonstrated excellent performance in enhancing both integrity and network capacity in a 5G physical layer [103]. For 6G, advanced channel coding will be crucial for achieving super speed (terabits per second), extremely low latency, and reliability. New coding schemes for 6G, such as space-time coding and quasi-cyclic multi-user LDPC are still under development. The preliminary results of the study in [148] indicate that, by controlling the propagation direction and harmonic power distribution simultaneously, the proposed space-time modulated digital coding scheme can significantly improve reliability of data transmission in multi-antenna technologies. The technology can be applied to enhance performance for several 6G technologies such as adaptive beamforming and holographic imaging.

Remaining challenges

Optimal coding requires perfect knowledge of CSI from both the receiver and the sender, including their transmission probabilities and channel gains. However, in practice, estimation errors, feedback quantization errors/delays, or channel mobility are challenges to CSI estimation. Fading influence and partial/imperfect CSI are the prime challenges for achieving secrecy capacity with coding techniques. The authors of [149] list several promising studies on using deep learning models to overcome the challenges as well as improving the error-correction and decoding/encoding process of LDPC and polar code. However, lack of practical implementation is still a major issue.

I. Summary of lessons learned from physical layer security

Table VI summarizes key technologies, security attacks, corresponding solutions and open problems in enhancing physical layer security. Eavesdropping is the most common threat over nearly all the technologies while the favorite defense method is to maximize the secrecy rate for the communication channel. Also, when joint communication and radar become real in 6G, because of the high directionality characteristic in 6G communications, location exposure will be likely the major privacy concern for subscribers. Three lessons learned from the survey for 6G physical layer security are as follows.

1) *Monitoring the surrounding atmospheric conditions and the objects present in the transmitter-receiver path is critical for ensuring reliable and secure 6G physical communications*. Since the harsh environment conditions (rain/fog) or thick obstacles like building can cause a THz/VLC link to scatter signals to surrounding areas, making the link vulnerable to eavesdropping. In this way, an attacker may release gaseous particles or molecules sensitive to the target THz links to cause inference to signals. The attacker can then adjust this physical interference to cause scattering of signals, i.e., signals can get deviated from their trajectories to non-uniform paths after passing through a medium, aiding eavesdropping of the signal. And then, a multi-attribute multi-observation technique to sense the surrounding environment and adjust beamforming and routing strategy can significantly reinforce the security capability for THz/VLC links and mitigate the impact of anti-jamming and eavesdropping.
2) *For AI-aided physical layer security methods, dataset is an Achilles' heel*. Lack of a rigorous public dataset for testing is a major obstacle to a breakthrough in performance detection. Thus, generating/collecting a qualified physical-layer dataset (e.g., benign, attack logs) will be critical and beneficial for 6G-PHY-related research. Also, if the jammers are equipped with intelligent capability, the mentioned conventional approaches likely fail to gain effective defense.
3) *Physical layer security will be a breakthrough for 6G security*. When millions of devices are connected in 6G, securing communications by cryptography alone is somewhat insufficient, given the growing threats of many physical attacks. And then 6G physical layer security will be the key technology to satisfy the requirement, a feature many earlier generations wanted but has achieved little success so far. However, based on our survey, neither 6G enabling physical technologies (THz, VLC, LIS/NOMA) nor any state-of-the-art solution of the seven protection approaches mentioned above, has the capability of resisting all physical attacks, such as jamming and eavesdropping. Further security enhancements for the technologies are *imperative* in the coming years to reach the goal.

VI. Security in the connection layer

The connection layer can be seen as a combination of network and transport layers. Security in this layer addresses a broad range of communication security issues between a UE and its requested services, particularly the network segments of access networks and core networks. The network segments include access networks (radio units, gNB, ground stations), and core networks (endpoint gateways, authentication servers, edge servers). For years, communications in the connection layer have been subject to many notorious attacks. For example, the lack of integrity protection of signalling data traffic between UE and the gNB or AMF can let an attacker compromise and alter data or advance a spoofing attack. Worse, exploiting the paging procedures, an attacker can launch massive signalling DoS attacks from millions of injected mobile UEs [150] to overload core networks (authentication servers) and degrade/block access of legitimate subscribers. The following subsections discuss key security concerns and prospective technologies that enhance 6G connection layer security. Note that network operators are the main stakeholders to take in charge of security protection in this layer.

A. 6G authentication and key management (6G-AKA) for mutual authentication between the subscriber and the network: Network access control

Like the upgrade of 4G EPS-AKA to 5G AKA, 6G AKA will certainly require significant upgrades of 5G AKA in order to satisfy highly personalized services and requirements of novel applications such as holographic telepresence. Since many components of 6G networks have not yet been formalized, it is unclear how the final 6G AKA shape will look. However, based on the open security problems of 5G, 6G AKA expects to solve the following issues.

- Stronger authentication between the serving network (SN) and the subscribers as well as between the SN and the home network (HN) should be seriously considered. For example, as illustrated in Figure 13, AUSF and ARPF of the HN take the main responsibility for authentication on the subscribers. The problem is the subscriber's SUPI and K_{SEAF} only appear together in a one-way response (steps 15, 16). Due to this limitation, if there are two concurrent authentication sessions on the SN and the HN, K_{SEAF} in step 15 can be linked into another SUPI of the concurrent session. Consequently, the SN may associate the session key K_{SEAF} to a wrong SUPI. Exploiting the vulnerability, an attacker can transfer his network bill to someone else for what he used on the SN [74]. Note that SUPI can be tracked by using rogue stations [75]. Although there is no attack recorded on this vulnerability, 6G AKA can prevent the threat by enabling the stronger binding between the HN and the SN.
- Closing the gap for the security capabilities of the network operators and dual authentication model is critical. Like 5G, 6G can be a huge heterogeneous network where many operators with different security capabilities coexist. Some small operators may provide 5G or older generations in the rural areas or sparse populations.

The dual authentication to support both old-generation and new-generation subscribers along with weak security infrastructure of the small operators can double trouble for security protection. The attacker can carry out bidding down attacks [151] to fool the small HN that the subscriber does not have a security capability and select the weaker authentication model (step 4 in Figure 13). Efficient authorization and authentication to protect the subscribers, regardless of the operators' capability, is critical. For supporting a secure united authentication model in 6G space-air-ground-sea networks, non-3GPP authentication protocols for open interfaces can be implemented with quantum-resistant algorithms (present below).

- A new subscriber identifier privacy model (refer more to Section IV-E) can require a new design for 6G AKA. Privacy is still a problem in 5G for now. 3GPP recommends using SUCI to enhance anonymity during the network access (e.g., as step 1 in Figure 13). However, a fake home network injector can track users, similar to IMSI catching [75]. To protect privacy, a better solution is to let the home network's AUSF publish its certificate to registering UEs, which then encrypts the SUPI to prevent it from being identified by the SN. The challenge of this approach is to determine who are trusted partners. Another is a requirement to support lawful interceptions in the case of satisfying data recovery from authorized agencies for crime investigation. If a new identity model (e.g., non-ID) becomes reality, privacy preservation in 6G AKA likely needs a reform of attaching identifier information in authentication requests.

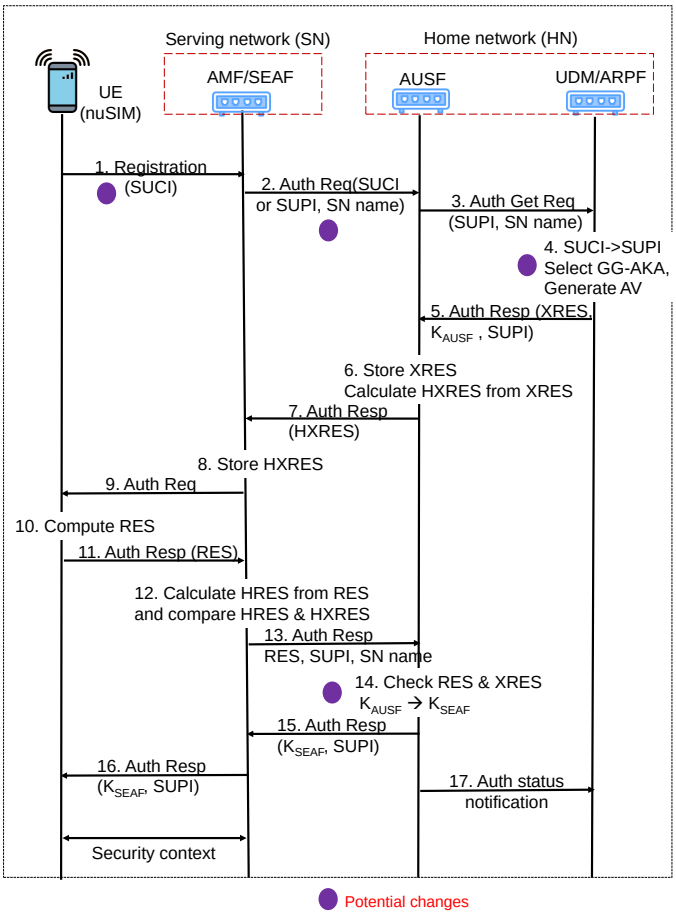

Fig. 13. An illustration of 5G-AKA for reference on the potential changes of 6G AKA. For now, the authentication occurs in the serving network (SN) against the subscribers is weak.

B. Quantum-safe algorithms and quantum communication networks for 6G secure communication

Preventing unauthorized interceptors from accessing communications is an essential requirement of secure data transmission in cellular networks. For example, 3GPP suggests using cipher algorithms such 128-NEA1(SNOW 3G)/128-NEA2(AES-128 CTR)/128-NEA3(128-bit ZUC) to protect the confidentiality of user data [73] and 128-NIA1(SNOW 3G)/128-NIA2(AES-128 CMAC)/128-NIA3(128-bit ZUC) for integrity checking in the 5G networks. However, quantum computing appears to threaten the security status quo pretty soon [152]. With the capability of searching and factoring much faster than a classical computer, a quantum computer can theoretically break any cryptosystem built on top of the mathematical complexities of integer factoring and discrete logarithms by running Shor's algorithms [153]. Accordingly, most public-key cryptography such as RSA and ECC and related security protocols (e.g., SSH, IPSec, TLS) are vulnerable to quantum attacks. By contrast, symmetric key algorithms with a proper key length (e.g., AES-256, SNOW 3G-256) or good hash functions (e.g., SHA-2, SHA-3) are safe from quantum attacks. Although there are no known attacks that successfully break existing public cryptographic schemes [154], many cryptographers are still pursuing futuristic cryptographic schemes to prepare for when such attacks become reality. Adopting quantum-safe cryptographic schemes is also vital for protecting long-lived sensitive information (e.g., finance transactions). This is to prevent an adversary from obtaining the documents and decrying them later when quantum computing is available.

There are two approaches to build quantum-safe algorithms: (1) in the near term, enhancing existing ciphersuites and related protocols to support a certain quantum resistance, and (2) in the long term, using post-quantum algorithms. In the first approach, cryptographic algorithms can extend their key length to enhance the resistance to quantum attacks. However, increasing the key sizes of nearly all public-key ciphers is infeasible to adapt to a constant increase of quantum computing power every year [153]. For the long-term target, a potential enhancement is to use a public-key quantum-resistant algorithm like lattice-based cryptography (e.g., NTRU) to replace RSA/ECC. Another prospective technology to enhance the quantum resistance in the public-key cryptography model is to use quantum key distribution (QKD) (as illustrated in Figure 14). QKD enables security based on fundamental laws in quantum physics (transmitting a string of photons in real time) and quantum information theory (cannot be eavesdropped without detecting). However, applying QKD for long-distance transmission is still a technical challenge due to the difficulty of developing repeater systems for QKD networks [153]. In

the first quarter of 2021, researchers demonstrated the state-of-the-art prototypes of QKD networks to support transmission over 4,600km if use satellites [155] or 511km on the ground if using optical fiber networks [156]. However, due to the high cost, it is unclear how to deploy such a QKD worldwide. Another emerging method is to use the quantum-safe hybrid key exchange mechanisms, which is based on the theory that the cryptosystem will remain secure if one of its key exchange methods remains secure [157]. Following this direction, some researchers propose to combine a classic key exchange method like Elliptic-curve Diffie–Hellman (ECDH) and a quantum-safe key-encapsulation mechanism (KEM), e.g., ECDH with NIST P-256, Kyber512, and SHA-256.

The most feasible plan securing 6G communication is gradual transformation and coexistence of the current ciphersuites. A quantum-safe cryptographic model like QKD will be deployed on the market demands and the progress of standardization. Currently, NIST has been hosting a contest since 2016 [1] to find the optimal quantum-safe cryptographic standard for the U.S., which will likely be applied worldwide. Figure 14 illustrates the coexistence of the ciphersuites among network nodes. The QKD model based on post-quantum algorithms and symmetric cryptography (e.g., QKD-AES) will be applied to enterprise nodes, highly sensitive applications, and key network elements in 6G networks. By contrast, the advanced standard Diffie–Hellman key exchange with AES, or quantum-resistant algorithms (QRA) based on NTRU/AES could be more suitable for legacy networks [45] and regular applications.

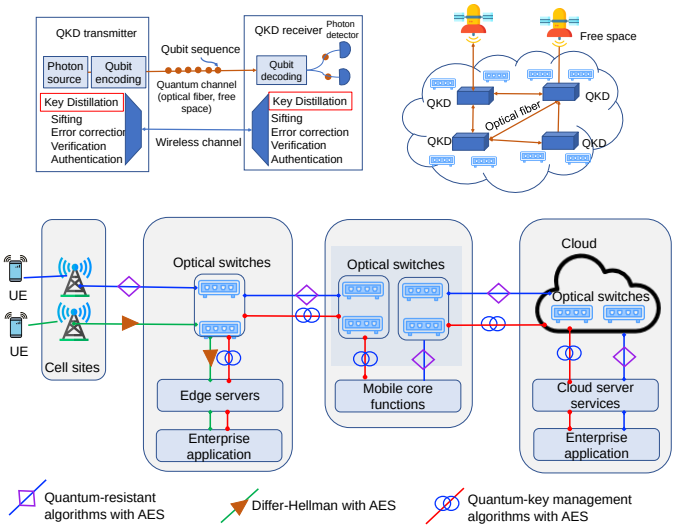

Fig. 14. The illustration of a QKD system and the deployment of using quantum-safe communications for various enterprises. Quantum-resistant algorithms with AES will likely be used for many purposes, while quantum-key models may be applied to high sensitive applications first.

Remaining challenges

Major challenges for 6G communication security are end-to-end encryption and reducing the expense of security (e.g., energy consumption, deployment cost). Since user traffic is booming in recent mobile networks, implementing end-to-end encryption may involve too much overhead for data transmission in 6G. 3GPP and standardization bodies currently prefer the optional use of security measures according to their ability to meet required services. If 6G requires mandatory end-to-end encryption, it is unclear how to satisfy this requirement. Also, upgrading all current security protocols to support quantum-safe standards will be a multi-year effort, given the time consuming of standardization and commercial testings. Finally, the expansion keyspace, if any, also has a significant effect on energy consumption and storage size. According to [158], nearly all encryption algorithms' energy consumption will rapidly soar if increasing their key size or data amount for processing (transaction size), as illustrated in Figure 15. Given the goal of energy efficiency in 6G up to 10-100 times, compared with 5G [1], it is unclear how to satisfy the requirement if all 6G devices are forced to equip quantum-resistant algorithms. Due to the constraints, we believe that many IoT networks may not quickly jump to the end-to-end encryption or fully quantum-resistant goal but use them in context (e.g., in the network segments integrated with dedicated energy). The trade-offs of performance and cost/time-to-market at expense of security can cause some operators to even ignore several mandatory security features of expensive implementation.

[1]https://csrc.nist.gov/projects/post-quantum-cryptography

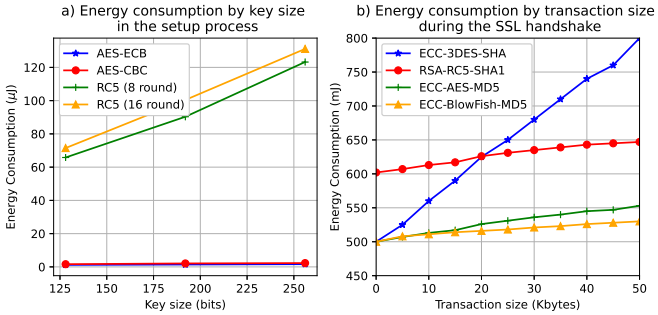

Fig. 15. Energy consumption of the cryptographic algorithms, according to [158]. Energy consumption of AES and related cipher suites is least in all cryptographic algorithms.

C. Enhanced Security Edge Protection Proxy (SEPP) for securing interconnect between 6G networks: Roaming Security

In 5G security architecture model, Security Edge Protection Proxy (SEPP) is the main force to protect interconnections between the home network and serving/visiting networks (as illustrated in Figure 7). SEPPs support end-to-end authentication, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages [8]. If there are no IP exchange (IPX) entities, SEPP will use TLS protocols to protect communications; otherwise, an application layer security protocol over the N32 layer called PRINS shall be used. According to [8], SEPPs use JSON Web Encryption described in IETF RFC 7516 for protecting exchange messages between the home network and serving network (via N32 interface) against eavesdropping and replay attacks. During the transit,

if the IP exchange (IPX) service providers need to carry out modifications (for mediation services), the standard JSON Web Signatures (defined in IETF RFC 7515) will be used to sign for the modifications [159]. In 6G, these TLS-based protocols can be upgraded with potential enhancements on cryptographic algorithms (e.g., support quantum-safe standards) or to support high-performance TCP/IP transmissions on gigabit networks.

Remaining challenges

Due to the wide usage of TLS in many secure communication protocols, finding and addressing potential vulnerabilities of future TLS (e.g., protocol downgrade attacks [160], in which the entities are lured to communicate with previous versions of TLS that are notoriously insecure) will be major challenges.

D. Blockchain and distributed ledger technologies for a vision of 6G trust networks

Trust networks and services are key expectations of 6G [76]. By definition, trust assumes a risk in an interaction [30], and implies the assumption that the communication party of an entity will act consistently and faithfully [161]. Many assume that embedding trust into the 6G networks will include the following key features: (1) maintaining the worth of information sharing while preventing fake/misbehaving sources, (2) guaranteeing that the likelihood of any undesirable events is extremely low, and (3) avoiding the single-point-of-failure. However, satisfying all of these is a challenge. From a design perspective, trust is commonly accomplished by various cryptographic schemes, such as digital signatures and certificates. Other than quantum-safe encryption mentioned above, blockchain and distributed ledger technologies (DLT), which are renowned for being used in cryptocurrency and financial transactions, are possible solutions to evolve to build a trust network in 6G [101]. Theoretically, the peer-reviewed ability of blockchain and DLT will guarantee key security and privacy features such as immutability, transparency, verifiability, anonymity and pseudonymity, data integrity, traceability, authentication, and monitoring. For 6G vision, US Federal Communications Commission (FCC) eyes blockchain to provide a more efficient tool to track and monitor growing wireless spectrums, given the complexity and high cost of the current spectrum auction and administration model [162]. Further, blockchain/distributed ledgers are expected to be used for many other applications such as pay-per-use energy sharing and computing infrastructure sharing [100], as illustrated in Figure 16. The top expectations of blockchain and DLT in 6G are (1) extending to apply blockchain and DLT for enhancing specific applications such as UAV and autonomous driving, (2) enhancing the security of smart contracts and reliability of consensus protocols, and (3) combining with artificial intelligence for enhancing the analytics on computing nodes (e.g., to detect 51% attacks) and then exploiting the blockchain smart contracts to automate the synchronization process.

Remaining challenges

Blockchain and DLT implementation are still at an early stage. Many of their fundamental components are still under active development. The burden on computation and communications are the main concerns of these technologies.

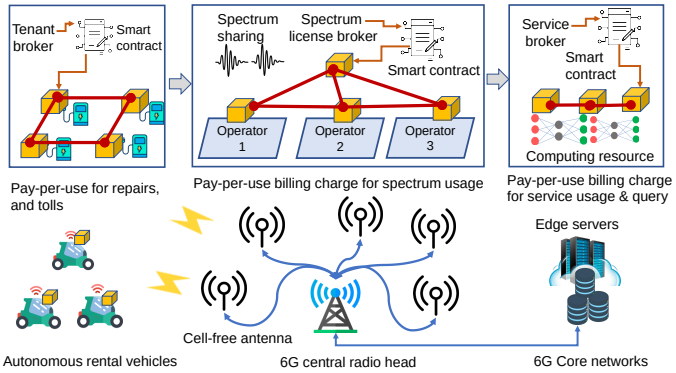

Fig. 16. Illustration of using blockchain technologies for autonomous rental vehicles, spectrum sharing, or dynamic resource allocation in 6G.

Further, lack of clarity on how the technology is governed, uncertainty around regulation, and the energy-intensive nature of the technology, are among many reasons that it will take more years to deploy in practice. Despite many available mitigating solutions [101], security risks such as 51% attacks and transaction privacy leakage are still open issues.

E. SD-WAN security: 6G network management control

SDN is expected to work at full capacity in 6G. Two future versions of SDN are Software-Defined Wide Area Network (SD-WAN) and Software-Defined Local Area Network (SD-LAN) [163], [164]. Like SDN, SD-WAN attempts to enhance network control performance and intelligence by separating the packet forwarding process (data plane) from the routing process (control plane). The largest threats against SDN/SD-WAN are DoS/DDoS attacks and insider adversaries. To protect SDN/SD-WAN, many detection and mitigation methods have been developed, such as using abnormal Intrusion Detection System (IDS) [26] and Moving Target Defense (MTD) [165]. If an anomaly is detected, the detection system can instruct the SDN controller how to reprogram the data plane (programmable switches) in order to mitigate the attack magnitude. There is a growing trend to use ML/DL to enhance detection engines [26], [166]. MTD-based systems protect networks by periodically hiding or changing key properties of networks (e.g., real IPs) to evade DDoS attacks and reconnaissance scanning. Supporting security implementation for SDN architecture, e.g., FlowVisor, FlowChecker, and FlowGuard [26], is another common approach to fixing its design flaw. Secure access service-edge (SASE) architecture, a term introduced by Gartner [167], can be a way of providing cloud-native security service for SD-WAN in mobile networks.

Remaining challenges

Since SD-WAN is still at the early development stage, it is unclear whether many pure SDN protection methods also work with SD-WAN. The convergence of SD-WAN security and cloud security to work as a unified framework also needs more evaluation. SD-WAN security will likely involve IPsec, VPN tunnels, enhanced firewalls, and micro-segmentation of application traffic [168].

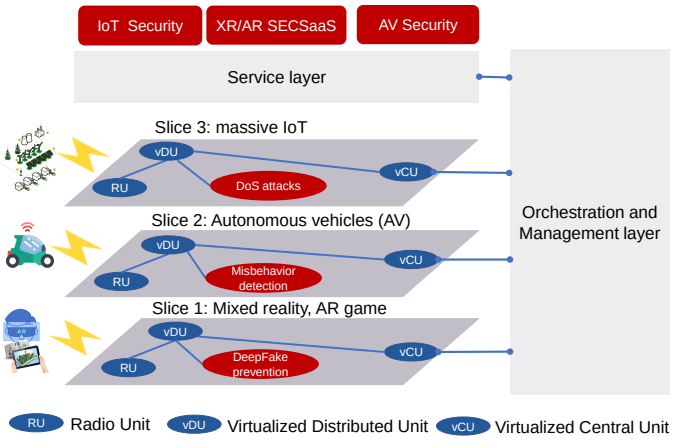

Fig. 17. An illustration of security isolation through full slicing in conjunction with RAN and core network slicing. Implementing slicing at the radio level and guaranteeing stringent Service-Level Agreement (SLA) are challenges for now because of the cost.

F. Deep slicing and Open RAN for 6G network security isolation

1) RAN/Core network slicing: Security enhancement by isolation through network slicing is critical in 5G. In 6G, network slicing promises to be fully utilized at all levels, physical, network and service layers [95], [169], [170]. Figure 17 illustrates how RAN and core network slices logically help to isolate security problems for various 6G applications. Each RAN/Core slice is logically isolated from the others, which are set by specific KPIs [171]–[173]. Since cross-talk between slices is prohibited in network slicing; inter-slice communications must be made through their respective interfaces. Following this model, a potential security interference/breach that occurs in a slice, if any, will not affect the others. Ideally, end-to-end isolation will enhance 6G security significantly.

Remaining challenges

The primary challenge to develop a security-isolation solution via network slicing is to satisfy all KPI requirements per slice while powerfully and independently enforcing the security policies for massive slices. Lack of specifications on how to perform end-to-end slicing and develop a framework for automatic deployment is thus an open issue. Defining isolation attributes for each slice, setting the KPI requirements, and enforcing them play a critical role in network slicing. A network slice manager, such as Network Slice Management Function (NSMF) [173], will be responsible for handling the functions for abstract virtual networks within its administrative domains. This means the NSMF must remain accessible all the time. However, a large-volume DoS attack [174] can make it extremely hard to contain. Despite several existing protection methods such as Slice Management Service Authorization Procedure and mutual authentication [173], real implementation is a challenge, given the stringent requirements of processing and response time.

2) Virtualized RAN, Cloud-RAN, and Open RAN: Virtualized radio access networks (vRAN) and Open RAN are prospective technologies for improving security in 6G [76]. vRAN enables the same functions as conventional RAN but is virtualized – for example, virtualized baseband units – on commodity servers instead of physical parts on vendor-specific hardware. Two more essential advantages of the vRAN and open RAN models for security are improved modularity, and reduced inter-dependencies [175]. The modularity allows more granular security attestation. By contrast, reducing dependencies on unique software makes it less risky for operators to update live networks. These can enable more controls for the operators over their security infrastructure, particularly with the rapid expansion of the threats on the network in the future. Reducing dependencies can also enable operators to select best-of-class vendors – a more robust supply chain– that meet their requirements in security. Note that depending on a single vendor may have massive repercussions. This nightmare occurred in 2018 [176], when expired software certificates on equipment caused a large-scale network outage of O2 and Softbank, two Tier 1 operators in UK and Japan.

Remaining challenges

Most of the drawbacks of vRAN are on the physical signal spectrum management. First, vRAN creates a massive amount of data and complicated computation for beam spaces that require faster baseband processing hardware. As capacity and bandwidth increase, computational requirements will increase. This requirement incidentally will demand high CAPEX investment to virtualize RAN fully. Second, since fade and attenuation of signal processing are more demanding in a high-frequency spectrum, managing the efficiency of data transmission and overheating phenomenon on compact processors is another technical challenge [180]. Finally, the distributed workload environment that vRAN employs through the complete separation of hardware and software can lead to unknown latency between workloads. These challenges forced the industry to coalesce around to virtualize 5G networks in the low-band mmWave spectrum. It is unclear how vRAN will do when 6G is pushed to even higher frequencies, i.e., THz.

Open RAN model and software-driven RAN approaches have their shortcomings. First, publishing open-source code is intended for developers to get constructive feedback from the community. However, suppose the source code is not appropriately designed and inspected intensively by security experts. In that case, it may become vulnerable, and hackers can also easily look for potential vulnerabilities to exploit without reverse engineering. Second, vulnerabilities are frequently propagated if a vulnerable source code is reused (e.g., as a library) for developing other codes.

G. Next-generation firewalls/intrusion detection for 6G network endpoint and multi-access edge security

Endpoints are entities in the borders of the core network (e.g., perimeter routers, IP core network gateways). Core networks are traditionally required to have security gateways to protect against external attacks. A security gateway can inspect bi-directional traffic against the operation policy to prevent unauthorized traffic from core network elements. The types of security gateways include network firewalls, web application firewall (WAF), IDS, service-oriented architecture API protection, antivirus program, VPN, and so on. In 5G

TABLE VII
PROSPECTIVE SOLUTIONS TO ENHANCE 6G CONNECTION LAYER SECURITY

Security domain	Reference	Security & privacy issues	Prospective security solutions 5G	Prospective security solutions 6G	Open challenges
Network access authentication	[151], [75], [74]	Impersonation attacks SUPI/identifier exposure	3GPP: 5G-AKA Non-3GPP: EAP-TLS 5G USIM, SUCI/SUPI	3GPP: 6G-AKA Non-3GPP: Quantume-safe EAP-TLS 6G nuSIM/non-ID	► Many components of 6G remain undefined so no clear relationship among stakeholders. ► System-on-Chip SIM (nuSIM) integration and non-SIM model are still under development
Signalling data encryption	[73], [152], [45]	Man-in-the-middle Eavesdropping Tampering traffic Data leakage	128-NEA1/128-NEA2/128-NEA3 128-NIA1/128-NIA2/128-NIA3	256-NEA1/256-NEA2/256-NEA3 256-NIA1/256-NIA2/256-NIA3 (Quantum-safe support)	► Heavy computation, energy consumption
Transport security protocol	[153], [156], [155]	Man-in-the-middle Data leakage	TLS 1.2/1.3	Quantum-safe TLS (AES-256) Quantum key distribution (QKD)	► Heavy computing if using for user data plane ► Quantum-based technology remains no explicit economical gain for now.
Interconnection security	[8], [177]	Man-in-the-middle Data leakage	SEPP with HTTP/2 and TLS 1.3	SEPP with HTTP/3 and Quantum-safe TLS	► Heavy computing if using for user data plane ► Quantum-based technology remains no explicit economical gain for now.
Trust networks	[29], [101], [30]	Compromised/insider attacks Data leakage	Blockchain/Distributed Ledgers are supported in several applications	Blockchain/Distributed Ledgers are widely used in many applications	► High energy consumption ► High complexity ► Vulnerable to 51% attacks
Network management	[163], [164], [26]	DoS attacks Network topology leakage	SDN security	SD-WAN security	► The risk of centralized SDN control
Network isolation	[174], [171], [173]	DoS attacks	Network slicing	Deep slicing	► Heavy computing to manage massive slices ► High expenditure and energy consumption.
Endpoint/network nodes	[178], [179]	DDos attacks Adversarial attacks Traffic meta profile	Firewall/IDS/MTD	AI-empowered Firewall/IDS/MTD	► Breakthroughs in AI ► High computing Adversarial defense

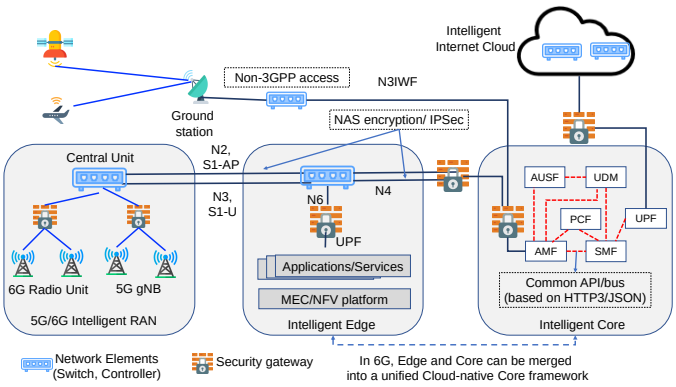

Fig. 18. The illustration of security endpoints located in the RAN/Core mobile networks. The big upgrade of 6G endpoint security is the wide use of AI-driven engines and in-line deep packet inspection (DPI) in firewalls and network intrusion detection systems.

system architecture, a security gateway located at the Access and Mobility Function (AMF) side, normally an Internet Security and Acceleration (ISA) Server, is responsible for inspecting all traffic between RAN and AMF [8], [151]. In 6G, such gateways will need to upgrade their capacity significantly. Many predict that the enhanced capabilities will consist of (1) in-line deep packet inspection (DPI), (2) TLS encrypted traffic inspection, (3) integrated intrusion prevention, (4) inspection for antivirus, and (5) third-party identity management integration (i.e., LDAP). Current AI-driven engines (e.g., using deep learning) will need a significant upgrade in detection capability such as more ability for online traffic training and less impact by the imbalanced datasets as well as robust for protecting heterogeneous networks. A promising solution is to improve the generative learning ability of deep learning models, as the suggestion of artificial general intelligence in [178], [181].

Remaining challenges

The main challenges are that many features of next-generation security gateways are still only concepts. Security automation is likely a mandatory feature to enable efficient protection for 6G ultra-dense networks. However, many of such AI-driven technologies need further enhancements (addressed further in Section VIII).

H. Summary of lessons learned from connection layer security

This section reviews several prospective solutions to protect 6G connection (network) layer such as quantum-safe communications and SD-WAN security. Table VII summarizes our vision on the potential changes of 6G security and privacy in the connection layer, compared with those of 5G. In conclusion, three key lessons learned from 6G connection layer security are as follows.

1) The proposed quantum-safe cryptographic schemes have not yet been standardized or reached a community agreement on the shape. Key generation time, signing time, verification time, encryption time, decryption time, key size, quantum resistance, and well-compatibility with existing security protocols are eight of many important factors to determine the winners. For now, QKD is one of the most prospective candidates for quantum-safe cryptographic schemes. However, the transition from the current non-quantum-safe algorithms (RSA, ECC) to the quantum-safe schemes will be a multi-year process. Accordingly, the transition speed will follow the demands from the market, commercial viability testing, and the readiness of the standards. Meanwhile, exploring the enhancements for the existing cryptographic schemes to mitigate the risk of quantum attacks, such as extending the key length, will still have a shot to maintain many 6G applications, e.g., which cannot afford the high expenditure of post-quantum cryptographic schemes.
2) *Distributed ledgers and blockchain can be the game changers in 6G but their hungry energy consumption can be a trouble for wide usage*. With the help of these two prospective technologies, 6G can be the first generation to be implemented as a grid of trusted networks. However, such a vision will likely be overlooked if distributed ledger technologies' overhead computation and security vulnerabilities are not fixed.

3) *Firewalls, IDS, MTD systems will not lose their roles in 6G, but new capabilities will be required.* These platforms have proven their reputations in protecting the networks against many attacks and network intrusions for years. They are still key players in 6G security. However, these legacy technologies need further upgrades in both automation and predictive capabilities so as to maintain their detection efficiency in a complicated environment with many connection technologies. A potential approach is to equip their core detection engines with AI. However, it is unclear whether AI can achieve a significant improvement, given many existing issues of AI-based models (see details in Section VIII).

VII. Security in the Service Layer

The service layer consists of edge/fog/cloud technologies that aim to provide middleware for serving third-party value-added services. Although upgrading the service layer is supposed to be independent of the timeline of mobile generations, the birth of new applications and hungry KPI requirements in this layer are the main motivations driving the lower layers' evolution. For example, 5G was rushed to deployment because it was challenging to satisfy the low latency of 1ms and gigabit throughput for industrial applications with 4G technologies. Other than active studies to enhance the physical layer, top network providers and the industry recently started to accelerate network transformation towards 6G by equipping the power of AI and the flexibility of cloud-based technologies for the lower layers, such as network/edge intelligence.

In essence, protecting the service layer infrastructure requires a combination of many tasks: authentication, data encryption, application security protocols, firewalls, hardware security, service identity access management, operation/kernel systems reinforcement, data-center network protection, and so on. Protection should be continuous from the host, operation systems, virtual machines, containers, applications to API services. In 6G, the protection systems may have significant changes in functional capabilities, such as intelligence and automation. The following subsections summarize prospective technologies to mitigate attacks in the service layer and envision the remaining challenges for 6G security research.

A. 6G application authentication: Distributed PKI and blockchain-based PKI

The public-key infrastructure (PKI) is a fundamental function to support user and application authentication. Compared with 5G PKI, 6G PKI likely upgrades its core cryptographic algorithms to quantum-safe mode. Another promising upgrade is to decentralize the PKI. Figure 19 illustrates a typical example of decentralized PKI by using blockchain/distributed ledgers [182]. Note that the single point of failure at the Certificate Authority (CA) and CA's supreme role (without any formal oversight) in the centralized PKI architecture has been the concern for years. The centralized CAs are also well-known targets for hackers. By breaching the CAs, hackers can issue many fraudulent certificates to break many applications of public-key cryptography. A blockchain-based PKI model, which leverages the strength of verifiable peer-to-peer networks, can effectively eliminate the risks of trusting the CAs only while enhancing both scalability and reliability for many upcoming 6G applications. Recently, Lin et al. [183] presented a proof-of-concept of PKI based on Ethereum (a public blockchain) to facilitate secure communication in vehicular networks. Another advantage of a blockchain-based PKI is to satisfy high privacy of users (anonymity) and transparency (everyone can know "who did","what", "when" on their record update), which the conventional PKI models do not support. For privacy enhancement, the centralized PKI like X.509 must accomplish through via a complicated model (e.g., using pseudonym certificate generation and Certificate Revocation List (CRL) [184]).

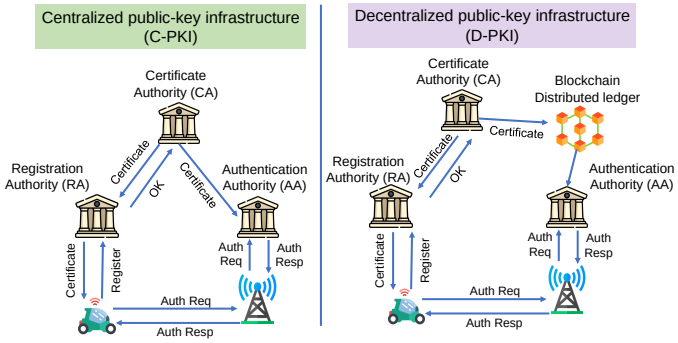

Fig. 19. An illustration of centralized and distributed blockchain-based PKIs for future vehicular networks. Blockchain-based PKIs can eliminate the risks of trusting the CAs only in the centralized PKI model while enhancing both scalability and reliability for many upcoming 6G applications.

Remaining challenges

Expanding the key length in 6G PKI's core cryptographic algorithm will certainly require more computation and energy to run. While end-users may see little impact, service providers may prioritize the upgrade to high-value applications at the vision of potential high expense. Besides, massive processing in blockchain-based PKI verification can also increase significant energy and resource consumption. This constraint, along with remaining security issues of blockchain technology (e.g., 51% attacks), likely limits its application scope. There is still a long way to realize large-scale blockchain-based PKI, let alone finding a suitable application context.

B. Using service access authentication (6G AKA) for application authentication

In prior generations, authentication between a UE and an application server is typically based on credentials such as usernames/passwords and tokens/certificates. In this model, credentials such as session keys will be maintained at both the UE and the application server to protect integrity and confidentiality. A common point of the credential-based authentication approach is to rely on provisioning of pre-shared keys or certificate management. However, managing a large number of pre-shared keys or certificates can be a grave challenge for some application providers against the risks of data breaches. New technology is proposed from 5G is Authentication and

Key Management for Applications (AKMA) [185]. While AKMA is not common in prior generations due to the lack of cooperation between the service providers and network operators, the growth of heterogeneous networks and service-based architecture can open the door for AKMA, e.g., as the form of unified application protocol models to satisfy new business cases (IoT devices). At this point, AKMA exploits the pre-existing cellular authentication and key management procedure to support service authentication instead of managing its own credential management. This approach brings convenience and reduces the complexity of building a new authentication, particularly for small application providers. We believe 6G will further enhance AKMA architecture for reducing delay in edge applications such as XR/AR. Indeed, AKMA can be an alternative solution for single sign-on (SSO) schemes and is particularly suitable for applications located in the network operators' computing infrastructure.

Remaining challenges

Since AKMA is still at the early stage of implementation, the lack of application models and business cases is the most challenging. Unlike conventional authentication, to perform AKMA, close cooperation between the network operators and application providers is critical. However, such a relationship is limited for now, given the competition of OAuth or SSO schemes. The security issues of maintaining AKMA in the interconnection environment (roaming) is also an important issue, but 3GPP has not yet been fully addressed [185].

C. 6G biometric authentication for 6G-enabled IoT and implantable devices

Biometric and behavioral authentication are expanding as prospective technologies for 6G. Biometric authentication systems will directly benefit many 6G applications such as wearable devices and implantable equipment. Biometric authentication can be done without keying complicated codes or memorizing username/passwords, and therefore will benefit many applications and users, including people with disabilities. Besides being applied to the service layer, this approach also has much potential for non-SIM-based access control in 6G core networks. Figure 20 illustrates a case of using biometric authentication for verifying the unique biological characteristics of a user to grant/deny service access. These characteristics have been used in some commercial applications (e.g., traveller/migrant/passenger identification) and in public security (e.g., criminal/suspect identification). However, only recently, this model is supposed to have been implemented for the service access [186].

On the other hand, when 6G THz imaging technologies with penetration depth capability go into operation, they will significantly enhance biometrics security. By identifying superficial skin traits or faces, THz imaging-based scanning can differentiate real from artificial fingers. Biological characteristics in combinations (multimodal biometric [187]) can provide higher accuracy, and more flexibility than a single form [188]. Biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have recently also emerged [189], [190]. It is no longer imagination to identify people from a distance, e.g., 200m, by analyzing their heartbeat. Like a fingerprint, an individual's cardiac signature is unique and cannot be altered or disguised. The futuristic technologies such as brain/heart-signal-based authentication are expected to be much more fraud-resistant than conventional methods like using fingerprints or usernames/passwords.

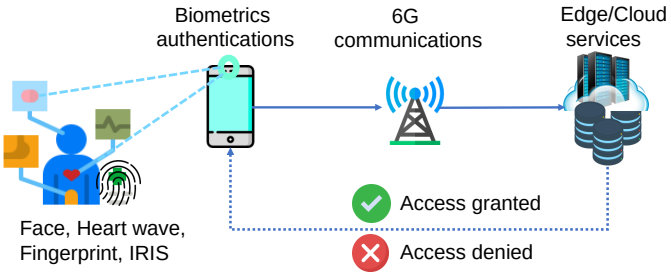

Fig. 20. An illustration of biometric authentication for accessing 6G edge/cloud services. In the future, since the hassles of passwords are expected to be eliminated, biometric authentication will play a key role for 6G service access authentication.

Remaining challenges

Personal information leakage, the safety of technology, and ethical issues are the main concerns of biometric authentication. Despite the many mitigation methods proposed [188], [191], protection against various types of biometric spoofing attacks, e.g., using forged or synthetic face/iris samples, will unlikely be sufficient. It will be a nightmare if highly sensitive information of individuals such as fingerprints becomes massively exposed and then abused for surveillance. Unlike traditional identifiers such as username/password, once a biometric identifier is stolen, there is no way to change and replace it with a newer version. Addressing the challenge, some recent studies propose to use secure enclave equipment, cancellable biometric models, or pseudo-biometric identities [192]. However, such implementation may result in poor performance for objective reasons, such as aging or worn-out fingerprints. The danger to owners of secured items is another great concern. A thief may assault an owner's property to get access to an asset if it is secured with a biometric device. In this case, the irreversible damage to the owner may cost more than just the secured property [193].

D. OAuth 3.0: new authorization protocol for 6G applications and network function services

OAuth 2.0 is a widely used protocol for end-users to authorize an application to access the data in another application without exposing the passwords. OAuth 2.0 appears in nearly all API-enabled applications and many mobile apps. Currently, TLS 1.3 and OAuth 2.0 are also used for authorization of network function service access in 5G service-based architecture [8]. However, complex ecosystems like distributed ledgers and deep slicing in 6G offer a unique means of identification and verification that OAuth 2.0, the version developed in 2012, cannot support. The initiatives to build OAuth 3.0 are in progress with major expectations about new features such as key proofing mechanisms, multi-user delegation, and multi-device processing [194]. We believe that upgrading OAuth

2.0 to OAuth 3.0 is mandatory to support authorization in 6G end-to-end service-based architecture, where spectrum sharing allocation/networking/security can be quickly deployed as a service through on-demand authorization.

Remaining challenges

OAuth 3.0 is still at the stage of concept proposal and feature consideration [194]. The detail of the development progress can be found at https://oauth.net/3

E. Enhanced HTTP/3 over QUIC for secure data exchange in 6G low-latency applications

Hypertext Transfer Protocol Version 3 (HTTP/3) is the upcoming major version of HTTP for exchanging information on Web applications and mobile platforms, alongside HTTP/2 (RFC 7540 in 2015). In 5G, HTTP/2 and TLS 1.3 have also been used to support secure communication on the inter-exchange/roaming links among the serving network and the home network [8]. Unlike HTTP/1.1 and HTTP/2, which use TCP as their transport, as illustrated in Figure 21, HTTP/3 is built on top of Quick UDP Internet Connections (QUIC), a transport layer protocol to handle congestion control over UDP [195]. The switch to QUIC can eliminate a major problem of HTTP/2 called "head-of-line blocking", where a lost or reordered packet can stall all object transactions, even those that are irrelevant to the lost packet. Since QUIC offers per-object error and congestion control over UDP, lost packets only impact the transactions with lost packets. Also, with the support of TLS 1.3 handshake and many fields, including packet flags encrypted in QUIC, HTTP/3 over QUIC can practically prevent pervasive monitoring attacks and protect sensitive data against gathering behavior of protocol artifacts and metadata. In the future, the handshake protocol TLS in QUIC will likely be upgraded along with the development of quantum computing, e.g., support quantum-safe cryptographic algorithms.

With all the enhancements and the advantage of running on the multicast protocol UDP, HTTP/3 can enable faster and more reliable transmission than HTTP/2 does [195]. These features are significant for many 5G/6G low-latency applications, e.g., virtual/extended reality (which often demands fast transmission to render intricate details of a virtual scene), real-time applications (online game streaming services), and broadcasting. Several browsers initially support HTTP/3, although the standard is still officially an Internet-Draft [195] at the time of this work. Given the life cycle of the prior generations, HTTP/3 will continue to be enhanced and eventually dominate in major applications at the time of 6G rolling out. Some new potential implementations are to replace HTTP/2 in carrying roaming messages or support interactive microservices in 6G core networks.

Remaining challenges

The change from TCP to UDP in the transport layer protocol of HTTP/3 can be problematic in security. For example, that the change may negatively impact the filters of many deployed security infrastructure such as load balancers or firewalls to parse and inspect application traffic because UDP traffic may be blocked by default in highly secure networks. HTTP/3 over QUIC is also vulnerable to several attacks, e.g., replay attacks if the server and clients have a mismatch on 0-RTT configuration [195], [196]. Since HTTP/3 promises to be widely used in the coming years, more thorough studies on the potential attacks and defense techniques are needed.

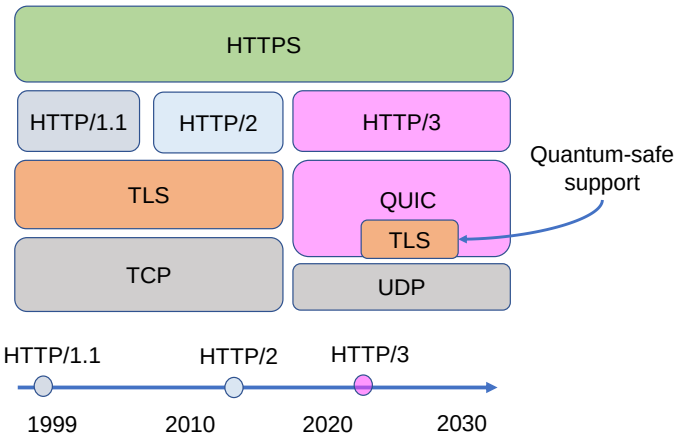

Fig. 21. An illustration of HTTP/3 over QUIC with the support of TLS handshake. HTTP/3 and future enhanced versions will be critical for many 5G/6G low-latency applications, e.g., virtual/extended reality, and interactive microservices in core networks.

F. Quantum homomorphic encryption for secure computation

Secure computation is a fundamental feature for protecting confidentiality and integrity in computing nodes like edge servers. Unlike those in the connection layer, the encryption methods in such service computing nodes may vary and be specified by the providers [197]. For storage information protection in the computing nodes, common approaches include (1) identity-based encryption, (2) attributed-based encryption, and (3) homomorphic encryption [198]. Identity-based encryption denotes a public-key encryption method in which a user's public key is derived from their well-known identity (e.g., email). A trusted authority is required to generate secret keys for every user over a secure channel, but it may be vulnerable to DoS or compromising attacks. Different from identity-based encryption, identity in the attribute-based encryption is replaced by a set of attributes (e.g., living location, age) and only users, whose private keys (related to certain access policies or attributes) match the attributes or access policy of the ciphertext, can access the data. The most prospective technology of the three is homomorphic encryption, which allows to carry out algebraic operations on ciphertext directly without decryption. The model of operations without revealing personal data in homomorphic encryption is a huge step for privacy preservation in the centralized computing nodes. This is extremely meaningful for secure computation and privacy preservation in the 6G era, when outsourcing data storage and computations to the edge servers for low-latency applications become common and encryption in a shared environment is essential. A notable recent upgrade for homomorphic encryption, as presented in the work of [199], is to support quantum-safe standards. We believe the transition to quantum homomorphic encryption will be easy since an operator can

carry out the upgrade on their centralized platforms, reducing security management overhead for individual companies or end-users.

Remaining challenges

Enforcing highly secure encryption standards for every service provider is a challenge. Because of cost constraints, not every provider will implement the strongest protection, let alone satisfy all the security standard recommendations in their platforms. Any fault in the configurations, outdated firmware, employee missteps, or lack of strong encryption can cause risks of data breaches or leave systems open to attacks. Second, with millions of users being served, satisfying both performance and the highest encryption standards, e.g., searching over encrypted data efficiently, is extremely difficult. As the authors in [200], [201] suggested, despite many steps forward, many challenging problems remain, e.g., searchable symmetric encryption, secure multi-keyword semantic search, and even secure range query. More studies are needed on applying suitable quantum-safe encryption to prevent adversaries from using the quantum computing power to run data mining and identify information about the individuals.

G. Liquid software security: a step to 6G platform-agnostic security

The concept of liquid software [202], which allows data and applications to flow from one node to the others, is not new. Currently, many universal apps have partially supported this feature to run on different device types (e.g., tablets, smartphones, wearable devices). In 6G, this platform-agnostic strategy will be enhanced to support computing nodes (e.g., edge servers). However, while applying the strategy for mobile devices in the same provider ecosystem can be carried out easily, due to the coexistence of many ecosystems and multiple network technologies, doing that on the computing nodes of the different network operators is more challenging. A solution to build such platform-agnostic systems is enhancing containerization architecture (e.g., Kubernetes) and cloudization of edge/fog nodes to accommodate multiple applications and enable interactions through API calls. In container-based systems, for security protection, an *extensive security service* such as Docker Trusted Registry will scan container images in advance to detect potential injections and then enforce access policies accordingly. However, according to [203], [204], the imperfection of resource isolation mechanism and shared kernel in multi-tenancy container-based systems can be the potential source of meltdown and spectre attacks that may lead to information leakage of co-resident containers. The authors of [203] introduced ContainerGuard, a non-intrusive variational autoencoders-based method to collect performance events data of processes to detect the attacks.

Remaining challenges

The topics of platform-agnostic security and related attacks, particularly for multiple devices and in combination with hardware solutions such as Trusted Platform Module (TPM) and Hardware Security Module (HSM), are still at the early stage of development and deserve more research efforts.

H. AI-empowered security-as-a-service transition for 6G "Service Everywhere" architecture

In 5G, many forecast that time-sensitive applications such as virtual reality will likely drive network operators and service providers to equip more computing capability near end-users, e.g., edge servers, to reduce the latency. In 6G, the appearance of holographic telepresence, massive IoT applications, and autonomous driving, the trend of allocating computing power will not only occur at the edge but at every hop of 6G communications [2], [3]. The service-based architecture will evolve into the era of end-to-end application or Service Everywhere. The increasing growth of applications will require a better organization from spectrum allocation, memory access to interoperability among the services (e.g., through API interfaces). However, detecting malware/intrusion behaviors and preventing data leakage in such a "Service Everywhere" environment is more challenging. For example, security services need to be able to plugin and detach quickly into a massive amount of microservices in distributed computing nodes. The attacks from many dimensions and different network technologies also require more intelligent defense capability, which traditional IDSs and passive deep learning-based detection models [205] such as CNN does not support. In short, we believe that there will be two major changes to 6G security-as-a-service. One is the expansion and easy deployment of the security-as-a-service (SECaaS) model to the computing nodes. In this model, service tenants or individuals on any network node can outsource anti-virus, anti-malware/spyware, intrusion detection, or penetration testing to the Internet security providers. The other is the upgrade of AI models to support proactive learning and reaction (super-intelligent AI) against multiple threats (see detail in Section VIII), which are hot topics in academia.

Remaining challenges

The most technical challenge for service security is to detect insider attacks. While service providers have clear advantages of providing users with advanced security protection and secure storage, data abuse is possible and then leaked by authorized service provider staff. To tackle these threats, deploying robust distributed backup facilities can be a good strategy. Besides, implementing strong auditing mechanisms on data access with digital time stamping and signatures on data could help to reduce the risks of the abuse of authorized insiders.

I. Summary of lessons learned from service layer security

Table VIII summarizes prospective solutions to enhance 6G service layer security, compared with those of 5G. From the review, application authentication (e.g., 6G PKI, OAuth 3.0), intelligent security-as-a-service, and platform-agnostic security are the primary targets of major upgrades for 6G and the central of ongoing research efforts. In summary, three key lessons learned from the review on security issues and defense methods for 6G service layer are as follows.

1) *Platform-agnostic security with edge/fog intelligence is a key issue to enhance 6G service layer security*. When 6G involves many heterogeneous network technologies

TABLE VIII
PROSPECTIVE SOLUTIONS TO ENHANCE 6G SERVICE LAYER SECURITY

Security domain	Reference	Security & privacy issues	Prospective security solutions		Open challenges
			5G	6G	
Service authentication	[182], [183], [184]	Credential exposure	Public key infrastructure (PKI)	PKI with quantum-safe algorithms PKI with blockchain	Under trials, no standard till now
	[185]	Unauthorized access, personal info leakage	5G AKA for applications	6G AKA for applications	Efficient cooperation between network operators and service providers.
	[187], [188], [190]	Impersonation Biometric data leakage	Face ID, Touch ID	Face ID, Touch ID, IRIS Heart rate, brain signal ID (Biometric authentication)	Biometric data protection
Application protocol	[195], [8]	Man-in-the-middle Fingerprinting a specific client	HTTP/2 over TLS 1.2/1.3 HTTP/3 over QUIC	Enhanced HTTP/3 over QUIC	Update many deployed security infrastructure such as load balancers
Service authorization	[8], [194]	Flawed redirect Access code leakage	OAuth 2.0	OAuth 3.0	The proof-of-concept is still under development
Software security	[202], [203]	API vulnerabilities, Data breach	Container-based security	Platform-agnostic security	Security features can synchronize to support different devices
Secure computation	[198], [199]	Data breach	Homomorphic encryption	Quantum homomorphic encryption	High computation, data mining performance degradation
Security service	[205], [3]	Malware/Virus/spam Deepfake	Cloud security-as-a-service (SECaaS)	Enhanced AI-empowered SECaaS Everywhere	Support interoperability

and ecosystems, the platform-agnostic systems will be an important strategy to simplify the complexity of implementing security solutions and delivering security updates among distributed computing nodes as fast as possible. At this point, softwarization and cloudization-based security solutions are likely the enablers to realize the target.

2) *Supporting open source for security is likely a good approach but not the answer for many enterprise applications*. On the plus side, open-source security can enable network providers to be free from specific vendors. However, the success of open-source platforms in 6G may still need substantial funds from enterprises to attract quality feedback and innovation features. It is otherwise unclear how to maintain security for live business at scale. The best practice would be to develop open standards and encourage competition between multiple vendors.
3) *6G service layer security boosts 6G privacy preservation at best, but more regulations are needed to enable*. Although personal information leakage can occur in the physical and connection layers, the service layer is at greater risk of massive data breaches as a result of its accessibility from the Internet and centralized application data storage. Secure computation and service access control (authentication) in this layer are then vital for enhancing privacy preservation. However, strong or weak implementation to support those features relies on the companies holding the data. Reasonable policing and regulations can encourage these keepers to adopt highly secure standards.

VIII. ARTIFICIAL INTELLIGENCE'S IMPACT ON 6G SECURITY

A key difference between 5G and 6G is intelligence. Artificial Intelligence (AI) creates new opportunities in 6G networks for innovation and business models powered by various machine learning techniques. By definition, machine learning allows a system to learn representations and procedures to perform human tasks in an automatic manner. In other words, machine learning can learn, predict and make improvements all by itself and is a major sub-field of AI. The ability of AI and security in 6G are key success factors in future AI-empowered wireless networks [206]. Due to serving a large number of paid subscribers (e.g., mobile users, enterprise, industry), 6G network operators may have more motivation to enhance their security interest by adopting the state-of-the-art achievements of general AI. Accordingly, the evolution of general AI will then benefit overall 6G-AI-empowered security systems. In the following subsections, we discuss three ways of how AI can change the nature of 6G security in each layer from three aspects: (1) AI as guardians (2) AI as a target, and (3) AI as weapons.

A. AI as a guardian: AI for enhancing 6G security

Defending against security attacks has been the task of many traditional solutions such as firewalls and intrusion detection systems, but AI makes such systems more capable and intelligent. While legacy security mechanisms (e.g., signature-based intrusion detection) have been extensively used, they have limitations in handling complex attacks in a 6G environment. Several studies [4], [207] have surveyed a large number of security applications powered by AI, such as intrusion detection. They found that AI techniques are suitable for 6G security enhancement. Table IX summarizes the AI techniques that aim to improve security for enabling technologies in each layer, along with prospective approaches to enhance the related AI models in the coming years. In the physical layer, open unsecured wireless communication is vulnerable to many attacks such as eavesdropping and jamming attacks. AI can significantly assist security defense by enhancing the performance of the detection engines. For example, the authors of [144] proposed to enhance randomness in physical layer secret key generation by deep reinforcement learning (DRL). The authors of [146], [208] explored to use a CNN/RNN-based channel state estimation to enhance physical layer authentication. Using DRL-based models for anti-jamming is a common approach [209], [210].

AI is also a favored technique for enhancing system performance in many enabling technologies for 6G at the network

TABLE IX
KEY AI SOLUTIONS TO ENHANCE SECURITY TECHNOLOGIES

Layer	Reference	Security & privacy issues	AI-based defense methods	5G	6G (vision)	Open challenges
Physical layer	[149], [211], [212], [144], [208], [146], [213], [214]	● Eavesdropping, jamming ● Location tracking ● Compromised IoT devices	► Channel coding ● Signal detection in PLS ● CSI estimation in PLS ● Beamforming alignment ● Misbehavior detection ● Anti-jamming ● Physical layer authentication	SVM, CNN, LSTM, DNN, RL, DRL, Autoencoder, Deep autoencoder, RNN, RBM	► More generative learning Meta learning Deep RL, Experienced DRL Deep Convolutional GAN Causal Learning ► More large-scale learning Distributed Learning Federated Learning Transfer Learning ► More explainable learning ► Toward end-to-end learning Deep autoencoder ► AI-building AI Security design by AI Machine creativity	► High computing/training cost ► Lack of physical-based datasets ► Energy efficiency ► Realtime processing ► Reliable signal generation
Connection layer	[187], [178], [215] [165],	● Man-in-the-middle ● DoS, DDoS attacks ● IP Spoofing ● SDN controller attacks ● Traffic trace	► Risk-based authentication ● Network intrusion detection ● Deep packet inspection (DPI) ● Protocol vulnerability detection ● Encrypted traffic inspection ● Proactive intrusion prevention	CNN, DNN, RBN, Autoencoder, LSTM, RBN, DBN, RL		► High computing/training cost ► Online learning ► Real-time processing ► High generative learning
Service layer	[186], [187] [216], [165]	● Malware/virus/spam ● NFV and VNF attacks ● Malicious microservices ● Data breach	► Biometric authentication ● Anti-virus/malware detection ● Trusted program verification ● Trusted updates verification ● Edge/Cloud control verification ● Container/Runtime protection	CNN, DNN, LSTM, DNN, DBM, RBM, Autoencoder Deep RL		► High computing/training cost ► Massive surveillance ► Bias learning ► Lightweight model for IoT devices ► Vulnerable to AI-targeted attacks ► High generative learning

Physical layer security (PLS), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long-Short-Term Memory (LSTM), Reinforcement Learning (RL), Autoencoder, Deep autoencoder, Recurrent Neural Network (RNN), Restricted Boltzmann machine (RBM), Deep Neural Network (DNN)

layer. With the advantages of big data analysis and pattern recognition, AI has been applied to several key technologies (but not limited to) as follows:

- Verifying node behavior for detecting insider attacks in maintaining trusted networks (CNN/RBN-based [178])
- Predicting attacks in networks to redirect traffic, make intelligent recommendations for network changes, and isolate suspicious services in SD-WAN/SDN networks (DRL-based [163])
- Optimizing radio and computing control policies in vRAN/Open RAN (Deep autoencoder-based [217])
- Determining prioritization of equipment recovery and isolating failed VNFs (DRL-based [215], [218])
- Inspecting traffic/network access behavior to predict attack events and filter/remove malicious traffic (DNN [165] CNN, LSTM, DBN, RBM [149], Autoencoder [178])

The service layer can be the first place to apply AI as a result of the automation requirement for large-scale data inspection. For example, the authors of [187] proposed to use CNN-based models to check access behavior, device fingerprinting, time, and context usage in risk-based authentication. Since biometric authentication will be futuristic technology for service access networks in 6G, applying AI-based techniques to enhance its performance is an attractive topic [219]. Hwang et al. [216] explored a CNN and LSTM-based model to eliminate the necessity of feature selection and extraction tasks while increasing the robustness and performance of biometric verification systems.

Like general AI, most current studies of AI for security are still at the stage of exploring AI to enhance conventional defense approaches or expand their detection capability. Some prospective approaches for AI security in the coming years, particularly for 6G applications, can be as follows. The first target is to enhance the generative learning capability of the AI-based models, where the intrusion detection engines can auto-learn from the environment and operate correctly on previously unseen inputs. In this direction, DRL, meta-learning, and the combination of DRL and GAN (experienced DRL) will be top approaches [4], [220], [221], given their strength in learning from very large inputs and automatically optimizing the decisions based on continuous feedback from the environment. Generative learning will be an important step forward to the vision of "AI-building AI", causal AI or "security design by AI" in 6G. Besides, since the training cost for AI-based models (computing hardware and energy consumption) and large-scale dataset collection increase substantially, large-scale learning needs a new approach. In this way, distributed learning and federated learning [222], which can coordinate the learning process on millions of distributed devices (local FL models) to improve the quality of the centralized learning model (global FL model), are likely the top candidates for many 6G applications such as misbehavior detection in autonomous driving. According to [223], edge-based applications will be the best places to apply such a learning strategy. To reduce the cost of labelling large-scale datasets, end-to-end unsupervised models like autoencoders [224] can be a promising approach, where their implementation can run directly on the online networks with raw traffic collection. Further, to save training cost, transfer learning is also an emerging approach to enhance service authentication applications (e.g., person re-identification [225]) by exploiting the power of trained models that were often carried out on high-performance computing platforms and related large-scale datasets. Finally, the blackbox of how a deep learning model works under specific conditions has been a concern for applying AI in many applications such as biometric authentication, given the existence of bias and potential flaws of imperfect datasets. To avoid the danger of AI making unjustifiable decisions, e.g., blocking a suspected application or targeting wrong criminals, explainable AI models have been another top target for ongoing efforts in cyber trust. Explainable AI like the studies of [226] and [227] aims to provide an interpretable and faithful manner to predict the results, by proposing the decision trees, rule lists, or Bayesian networks to study the decision of the DL models in the context of live running scenarios.

Remaining challenges

Despite many expectations, there are several challenges to apply AI for enhancing 6G security. First, AI can become the target of adversarial attacks (see details below). If AI-based programs control the key components of network systems, successful attacks can cause devastating damage, creating

chaos in packet forwarding or bypassing specific malicious traffic. Second, online processing in AI is still an open issue. Heavy computation and substantial time for training in AI (training cost) make it less friendly for IDS/IPS in energy-constrained devices, a large class in 6G. Moreover, the current AI has no creativity. Therefore, to gain "security design by AI" and "AI-building AI" in 6G, more breakthroughs are needed. The ethics of AI is also important, given potential biases in AI systems. Finally, AI is probably abused as a weapon when AI expects to be more intelligent in 6G era. With incredible capabilities, AI-empowered attacks would be a nightmare for the vision of safe networks. The best practice is to apply a high standard for developing AI-related solutions.

B. AI as a target: Security attacks against 6G AI-empowered engines and defense approaches

AI is a double-edged sword. Other than the good side of enhancing 6G capabilities, AI may itself become a target of attacks; AI is particularly vulnerable to adversarial attacks. Hackers may conduct a white-box, gray-box or black-box attack depending on how much knowledge they have of a machine learning system. The fundamental configurations are training data, learning algorithms, and hyper-parameters used to control the learning process. Many studies [228], [229] suggested such processes can be exploited to manipulate AI systems, e.g., exploiting the high linearity of AI models. Figure 22 summarizes three main attacks that targets an AI-based system in the literature [207], [221], [228], [229]: (1) *data poisoning* aims to insert wrong labelled data in the datasets or change input objects to mislead machine learning algorithms, (2) *algorithm poisoning* to influence the distributed learning process of an algorithm by uploading manipulated weights in local learning models, and (3) *model poisoning* to replace the deployed model with a malicious one. In three attack types, *data poisoning* is a major challenge since most input objects in the outdoor environment are accessible, and the attacker can easily carry out sophisticated editing. Figure 23 illustrates a case where an attacker uses a UAV to project a manipulated traffic light image on a road banner to mislead AI-based driving control in autonomous vehicles. The attacker can also use data poisoning approaches such as injecting confusing data in transfer learning/federated learning to disrupt AI-based resource allocation systems. AI-based face recognition can also be deceived to accept an attacker's appearance (Bob) as that of a victim (Alice) [228]. In 6G, when major applications rely on AI to operate, e.g., autonomous driving, the risks of the attacks cannot be underestimated.

To defeat adversary models against AI systems, defense strategies can vary. At the time of 6G, several technologies such as high-performance computing and blockchain may assist in addressing the security issues in AI, e.g., enhancing vulnerability assessment speed or protecting the integrity of local data/AI models against adversarial attacks. Another workable vision of 6G for AI protection is that current AI protection methods will be significantly enhanced. Figure 23 summarizes most prospective defense methods from the studies in [207], [221], [229]. In essence, there are three

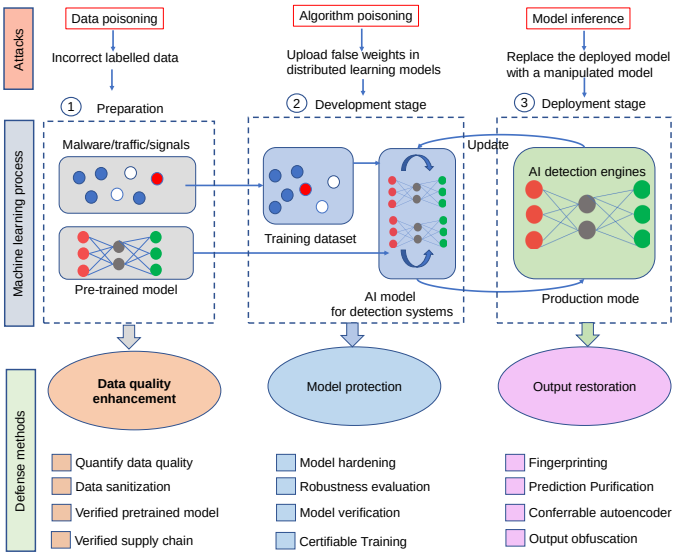

Fig. 22. An illustration of a machine learning-based system, three attack methods against it and potential defense methods. When major 6G applications rely on AI to operate, protecting data supply chain, AI models, and the integrity of output is essential.

approaches: (1) enhance data quality, (2) model protection, and (3) output integrity restoration. For example, the AI designer may modify an ML system with the changes (e.g., reducing noise, altering data features) on adversarial samples or remove contaminated samples from training data (data sanitization) during the training process or ML algorithm. Data collected from verified sources (supply chain) are also preferred, e.g., using blockchain, mutual authentication. For model protection, the AI designer can add a specialized detector in front of an ML system to block any attack in progress or perform multiple evaluations to verify the model.

Figure 24 illustrates a simple defense method against the algorithm poisoning attack from the study [230], where the adversarial model can be detected by comparing the model predictions on the original and squeezed data inputs. If the results of two predictions are substantially different from each other, the original input seems to be contaminated (adversarial samples). To protect output integrity (i.e., in the deployment stage), many methods can be used such as output obfuscation and prediction purification [231]. 6G likely enhances specialized techniques for detecting AI-empowered technologies' weaknesses, e.g., AI model assessment, API for scanning vulnerabilities in AI-empowered services. More detail of adversarial attacks and defenses in deep learning can be found in [229]–[232]. In conclusion, the field of AI security protection keeps capturing the interests of academic and industrial societies. Further research and discussion need to be carried out in the future.

C. AI as a weapon: Ethical AI/Superintelligent AI/AI Regulation

It is widely agreed that AI can be abused as a weapon or tool to evade defense systems. Shen et al. [233] presented FusionRipper to defeat a multi-sensor fusion design and carry

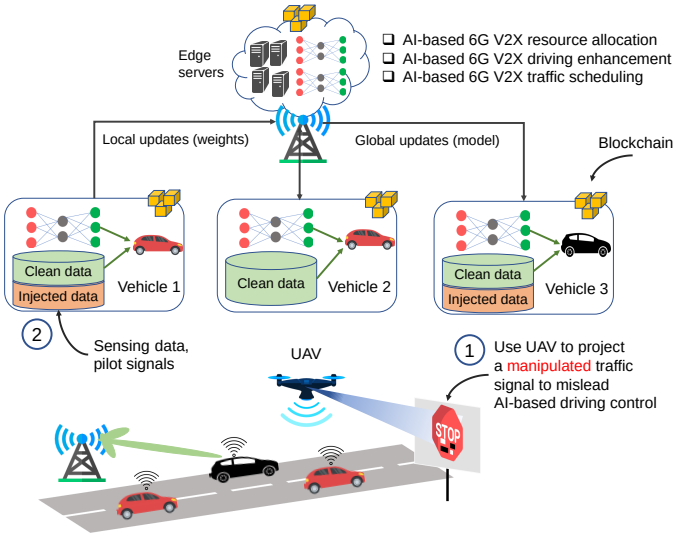

Fig. 23. An illustration of ① the poisoning attacks (physical attacks) by using a UAV to project a manipulated traffic light image on road banner to mislead AI-based driving control in autonomous vehicles and ② algorithm attacks through influencing the global model of AI-based systems at the edge (e.g., for resource allocation, traffic scheduling) with falsification data updates (sensing info, pilot signals). With the expectation of AI popularity in 6G access control (spectrum, resource blocks for transmission) and applications (object detection/tracking in autonomous driving, extended reality), these attacks can pose severe threats.

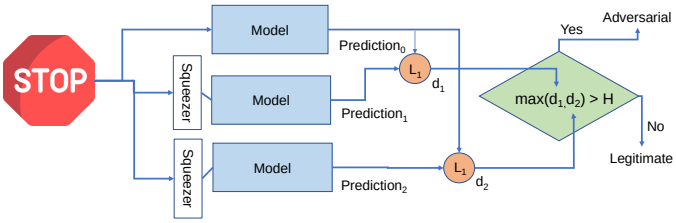

Fig. 24. An illustration of a defense method for AI, where the AI model is trained with multiple types of datasets to find out whether the algorithm is adversarial.

out two autonomous vehicle-specific attack goals, off-road and wrong-way attacks. The FusionRipper attack design consists of (1) vulnerability profiling to predict when vulnerable periods are and (2) aggressive spoofing to exploit the take-over vulnerability with exponential spoofing based on vulnerability profiling scheduling. The lesson learned from FusionRipper is that we face a new challenge, the adversarial use of AI to create sophisticated types of attacks. AI-powered attacks improve the efficacy of conventional attacks; in other words, attackers can use AI to conduct rapid and effective reconnaissance on the target network to learn and prioritize vulnerabilities that can be exploited. DeepLocker, developed by IBM, uses AI techniques to hide malware within a legitimate application (e.g., video conferencing software) and activates the malware when it reaches specific targets [234]. DeepLocker is able to recognize the victim based on facial/voice recognition or geolocation information. Many AI-based attacks can be found in the literature [207], [228], [235]. These authors investigated AI-based attack technology and mitigating strategies, which can help to understand how AI is weaponized for attacks and what mitigating mechanisms can be implemented.

Although AI-based attacks have been extensively studied in network applications, research for such attacks in 6G communications is still in its early stages. Hereby ethics of AI is extremely necessary to avoid potential AI abuse as weapons or harm caused by AI systems. Note that the goal of AI is to make *beneficial machines* to benefit humans, instead of creating terminators that can overwhelm and rule humans. Because of such concerns, many companies and governments recently started to promote global initiatives to build a platform about AI [2] and guidelines for practicing AI technologies at best, including potential legislation and policing.

D. Summary of lessons learned from AI's impact on 6G security

Table IX summarizes the aspects of technologies in all three layers where AI can assist, from physical coding in the physical layer and radio control policy optimization in the connection layer, to access control in the service layer. Such developments provide a basis for further AI studies that will enhance 6G security technologies, regardless of which layer is targeted. AI can help to enhance the technologies from two perspectives: (1) system detection performance, e.g., the accuracy of channel state estimation in physical coding or physical layer authentication) and (2) automation, e.g., auto-learning on abnormal behavior in live traffic. In conclusion, three key lessons learned from AI's impact on 6G security are as follows.

1) *The potential for using AI to enhance 6G security is overwhelming but not a magic wand for every security issue*. First, AI can help to enhance system performance (e.g., accuracy) of many tasks of security systems, regardless of the layers. Because of the complexity and diversity of applications, this feature is vital in 6G. Second, AI enables automation for detecting and filtering malicious traffic as a result of self-learning abilities. However, there are some areas where non-AI innovations still get much support from the industry and are potentially the main driving forces for success of 6G deployment, such as quantum-safe encryption algorithms, secure communication protocols, and network slicing for security isolation.
2) *AI's early achievements in assisting security enhancements have demonstrated that getting to the bottom of what causes attacks or how to fix them is challenging*. For now, the capability of AI is limited at detecting whether there is an attack in a given action/traffic pattern or predicting the probability of a specific attack type. AI cannot help to explain why attacks occur or the causal relationships of discrete events to potential intrusions. In the next decade, AI needs to assist security protection to get the bottom of what causes attacks, predicting such causation, and suggesting how to fix and prevent future exploitation at best (security design by

[2]https://ethicsinaction.ieee.org/

AI). To attain such assistance capability, AI needs huge amounts of available data for its training and significant improvements in learning models. Meta-learning and reinforcement learning are potential candidates which can gain fundamental knowledge of generative learning about the causation of attacks and failed defenses by analyzing invariant criteria across data sets. However, data collection and cleaning for such AI models are laborious tasks. As a result, efficient end-to-end learning and causal learning models will be appealing topics in the coming years.

3) *AI is not always a positive actor*. As we highlighted above, AI can be used to evade detection efforts in an IDS or run effective reconnaissance on a victim's networks. Worsen, AI can be abused to create autonomous weapons to attack a designed target chain (e.g., with face recognition). In the end, AI will be a nightmare if a rigid code of ethics does not constrain wild developments. Legislation and policing for AI are required.

IX. Privacy challenges and preservation approaches

Security and privacy are hand-in-hand technologies. Without security, an attacker can gain access to a victim's networks and steal personal data. By definition, in GDPR Article 4 [236], personal data can be any information directly or indirectly related to an identified or identifiable person, such as a name, an identification number, subscriber's location, and social identity. Figure 25 illustrates three typical personal data types that can be illegally collected or abused for monitoring mobile subscribers. Ensuring *confidentiality*, *integrity*, and *availability* of data in the security design can work as a base for privacy. Privacy preservation is defined as having the ability to protect sensitive information of a specific entity, managed throughout the various stages of data life cycle, such as data in collection, data in processing, and data in use. Different from security, according to [237], three principles specified for privacy preservation are: *linkability*, *identifiability* and *traceability* (LIT). *Linkability* means the feasibility of linking consecutive activities of the same identity in sequence. *Identifiability* denotes the possibility of recognizing the true identity of a party in a system through the collected information. *Traceability* describes the possibility of tracking the activities of a specific identity.

Since collecting and sharing data are essential in today's digital and network economy, any misuse and dissemination of collected data can pose significant threats to users. An adversary can use obtained information to bully or blackmail subscribers. Those risks will increase when 6G networks become more complicated to manage data privacy compliance requirements. To gain public trust, many organizations and companies have recently started to pay serious attention to implementing advanced protection of customer data. The question is, "what are the new challenges and prospective approaches for privacy preservation in 6G, compared to current techniques?". The next section is our vision of data privacy matters in 6G, challenges, and prospective solutions to address those issues.

A. Why data privacy matters in 6G

Data privacy has been a concern for years. Table II in Section III and the summary in the previous sections summarize several potential privacy issues across 6G networks, e.g., location tracking, as illustrated in Figure 25. However, there are many reasons that privacy preservation is more urgent in 6G. First, protecting personal information in an era of supercomputing and smart agents is challenging. With a gigantic network such as 6G that connects things and humans, the demands for AI-enabled smart applications are expected to grow exponentially [6]. These AI-powered applications can dig out more context-related information of a specific individual and his/her environmental context. By using personal or other confidential data, AI can provide more precise and smarter personalized services that users may enjoy, such as recommendations of points of interest, films, and routes. However, having that kind of experience also impacts a users' privacy. Users may not be aware of being targets of massive data collections for unsolicited advertisements; even worse would be stalking and extortion powered by AI. There is a trade-off between two conflicting goals: (1) high privacy preservation for individuals as well as their right to be forgotten, and (2) mining personal data to maximize the accuracy of recommendations/guidelines for users. The border between providing useful information and being abused for monetization is fragile, particularly in a hungry, data-driven industry.

Second, in 6G, more sensitive information of users is expected to be available from key applications such as smart clothes, wearable devices, and implant cyborgs. On the positive side, these applications can help to improve human lives, such as reducing the risk of fatal accidents, enhancing good sleep, or assisting the rehabilitation of people with disabilities. The opposite side is that the physical and medical data for control systems to coordinate these connected applications can be collected illegally and abused. These threats may not be unique but will worsen in 6G. Third, the approach of cloudizing many core components and applications in 6G is also flawed. By migrating workloads to the cloud, a shared infrastructure, customer's personal information faces an increased risk of unauthorized access and exposure, including illegal leakage by unauthorized employees.

Finally, the more accurate localization through telecommunication in dense networks is a critical concern. The idea of THz Access Points following a user's motion to centimeter-level precision for improving link connectivity will raise severe concerns that it can be used for surveillance. Many countries have begun to tighten the rules for protecting users' personal information. Privacy preservation will be no longer an optional feature as it has been but will be required by law. The U.S. Federal Privacy Act (1974) [238] and EU GDPR (2016) [236] was established to provide statutes and fair information practices for preventing potential abuses in using citizens' data. A company can face billions of dollars in fines if a massive amount of its client data is illegally exposed [239]. The high penalty can be the end of a business in such matters, and personnel can also be prosecuted if the damage is qualified. Again, the liability is not new, but record penalties are likely.

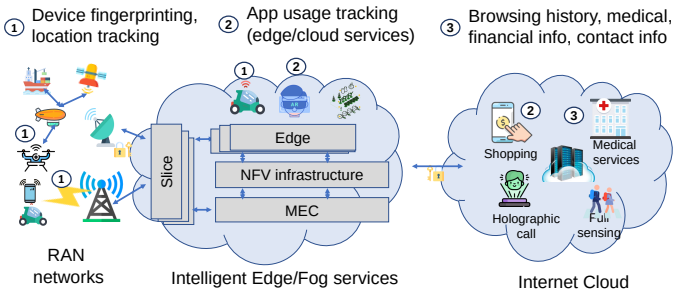

Fig. 25. An illustration of personal data types illegally collected or abused for monitoring mobile subscribers in each layer. As a result of cloudization in data storage and services, large-scale data breaches in the application layer are the most concerns.

B. State-of-the-art privacy preservation techniques and vision for 6G

There have been many surveys into privacy concerns and preservation technologies in different technologies: 6G IoT networks [240], 6G AI-enabled applications [6], autonomous driving [241], big data and cloud [242]. The techniques all meet common goals: (1) reduce identity linkage in data collection; (2) increase secure data storage; and (3) control over data sharing and use. Their goals are consistent with privacy preservation principles in law [236]: privacy by design, privacy policies, and privacy engineering. Several mechanisms, such as Privacy Enhancing Technologies (PET) [243], [244], have recently been proposed to provide the best practices for privacy preservation in collecting, processing , and using data that meet different requirements by laws. PETs specifically employ principles such as minimizing personal data, maximizing data security, and empowering individuals. Although PETs are a general approach for data privacy, many principles should still be considered for enhancing privacy in mobile networks, given the convergence of network infrastructure ecosystems and universal data sharing. Based on PETs, Table X categorizes privacy preservation technologies in the literature as three models: trusted, untrusted, and semi-trusted.

Trusted privacy preservation methods assume that communication parties trust an external entity in data processing. The external entity can be a central authority (CA) which can link and revoke user certificates used in secure communication. The trusted techniques are widely applied in applications of connection and service layers. Access control (authentication), VPN/tunnel encryption (TLS), anonymization, pseudonymization, are typical examples [243]. By definition, access control maintains the functions of restricting subscribers from obtaining data or placing data onto storage devices. In the service layer, access control is implemented via service authentication. Tunnel encryption is also a commonly applied protocol for protecting control and user data in core networks. Because of their critical role in restricting data access for unauthorized users, legacy technologies such as authentication and VPNs will continue to be the cornerstone of protecting data privacy in 6G.

Another important trusted privacy preservation method is pseudonymization. Pseudonymization provides a method of replacing identifiable information fields (e.g., locations or names of individuals) in data records with artificial identifiers, namely pseudonyms [245]. Pseudonymization techniques include scrambling, encryption, masking, tokenization, and so on. The most popular pseudonymization technology in mobile networks is to use IMSI/GUTI/SUCI to hide the real identity of a subscriber. The other futuristic technique for enhancing privacy, which is likely to be key technology in 6G, is to use blockchain networks [25], [101], [246], which are a specific type of distributed ledgers. Blockchain protects user privacy by using a hashing address (wallet) to represent their identity, known as a pseudonymous credential. By using the hashing address to sign and verify all the transactions, users' identities are not revealed. Many 6G applications such as autonomous driving, health care, fintech, and the energy industry are expected to use blockchain technologies.

By contrast, the idea behind untrusted privacy preservation methods is that subscribers trust themselves only. Subscribers take on the role of protecting their own privacy. Secure Multi-Party Computing (SMC), also known as multi-party computation (MPC) or privacy-preserving computation, is a typical example of the untrusted model [243]. According to [243], SMC aims to protect a distributed computation model from the inputs of communication parties while keeping those inputs private. Participants' communications are also encrypted and protected by cryptographic protocols where each participant cannot say that they learn nothing. A state-of-the-art technique, which is likely a prospective technology for many 6G applications, is federated learning. Many scholars have recently started exploring tweaking federated learning-based techniques for SMC, for example, the work in [251], [252]. Federated learning can be solution to enhance privacy and power of distributed learning models in many 6G cooperative applications, e.g., misbehavior behavior for connected vehicles, 6G mixed reality. However, the risks of adversarial attacks, system induced bias in training data from different capabilities of devices, the ability of monitoring /debugging problems in a wide range, or slow convergence learning speed have been open challenges to federated learning. Data perturbation, known as obfuscation techniques, is another typical technique of an untrusted privacy preservation model. Data perturbation secures data exchange by adding "noise" (e.g., false or irrelevant data, scrambling user names) to the data source and then renders this into a form that unauthorized users cannot read or understand. This technique has been used in protecting electronic medical records from prying eyes [242], which can become more common in 6G health applications. The drawback of data perturbation is that it reduces the ability of data mining/DL-based tools to access information since the noise values may not be meaningful but negative for training accurately.

Unlike the above two models, a semi-trusted model uses a distributed trust model where a communication party's trust is maintained through particular protocols [243]. In this model, a data owner does not completely trust other users, including the service provider, but can maintain a level of trust through majority voting. The key assumption is that peer users are honest or consistent in sharing their infor-

TABLE X
KEY SOLUTIONS TO ENHANCE PRIVACY PRESERVATION

Layer	Reference	Feature method	Model	5G	6G (vision)	Open challenges
Physical layer	[186], [188]	Authentication	Untrusted	● Radio fingerprinting	► Physical layer authentication (AI-empowered)	Location exposure Experience degradation
Connection layer	[243]	Communication anonymization	Trusted	● Proxy servers	► Proxy servers	IP exposure at fake proxy
	[25], [101], [246]	Pseudonymization	Trusted	● IMSI/GUTI/SUCI ● Blockchain networks	► SUCI, Non-ID ► Blockchain/Distributed ledger	Complicated management Energy consumption
	[242]	Data anonymization	Trusted	● Randomization ● Generalization	► Enhanced anonymization (AI-empowered)	Complexity to implement for large-volume data
Service layer	[247], [248]	Differential privacy	Semi-trusted	● Laplace mechanism	► Enhanced differential privacy (AI-empowered)	Challenge to detect the changes of particular values
	[249]	Homomorphic encryption	Semi-trusted	● Homomorphic encryption	► Quantum homomorphic encryption	Complexity, high computation
	[243]	Group-based signatures	Semi-trusted	● Attribute-based signatures	► Group-based signatures	Can identify user if few participants
	[169], [243]	Self-destructing data	Semi-trusted	● Self-destructing data	► Enhanced self-destructing data	Only apply for specific applications
	[169], [243]	Data masking	Semi-trusted	● Substitution, Shuffling, Nulling out, Encryption, Character scrambling	► Enhanced data masking (AI-empowered)	Privacy-data utility trade-off, traffic overhead
	[222], [250]	Secure Multi-Party Computing	Untrusted	● Federated learning	► Federated learning ► Distributed learning	All participants need to be present, High vulnerable to collusion attacks
	[243]	Data perturbation	Untrusted	● Probability distribution ● Value distortion	► Enhanced data perturbation (AI-empowered)	Traffic overhead

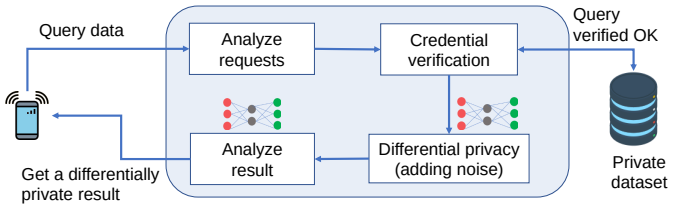

Fig. 26. Illustration of how differential privacy works. Differential privacy will be widely used in 5G/6G for processing private-data-related queries, where all retrieved results will be processed to eliminate the privacy-related data.

mation. Homomorphic encryption, differential privacy, group-based/attribute-based signatures, self-destructing data, and data masking are typical examples. As defined in Section VII, homomorphic encryption allows performing operations, such as search and query, on encrypted data directly without decryption. Subscribers can thus send their data to a third party (e.g., operators, cloud providers) for storage or processing. Homomorphic encryption is expected to be a key technology for protecting data confidentiality and privacy in 6G [169].

Differential privacy is another prospective technology for privacy preservation in coming years [247], [248]. As illustrated in Figure 26, the idea behind differential privacy is to create aggregate information within a dataset (e.g., by group), so that no query to any single individual or private data can be carried out directly without a filter (adding noise, randomness to the result retrieved), thereby providing privacy [6]. However, the weakness of differential privacy is that it is a challenge to distinguish whether a particular value has been changed. Self-destructing data means an entity's encrypted information exists only for a period of time and is valid for decryption if the private key has not expired over that duration, thus protecting privacy. However, this technique's drawback is that data storage is temporary; thus, it may only be applied for some particular applications, such as to secrete instant messages. Finally, another name of data obfuscation, data masking protects personal data by hiding identifiable information with modified content. Some state-the-art studies [249] found that the combination of homomorphic encryption and data masking can be a perfect way to provide a high degree of security against quantum attacks, which are taken to appear in 6G, while still maintain privacy at best.

C. Privacy challenges

Implementing perfect privacy preservation mechanisms, at least to satisfy laws/regulations, is more challenging than just talk. Some factors that may have to be considered are as follows. First, implementation could burden the finances of an organization in order to maintain data privacy. Such cost will come from substantial investments in end-to-end protection equipment for data encryption and anonymization, let alone software customization to fully comply with legal requirements. The challenge is, not many small enterprises have the resources for such investments. In an era of data explosion like 6G, processing massive data may require expensive commodity devices that can overwhelm business expenditure.

Protecting privacy in massive IoT devices with limited resources is another challenge. Wearable devices and low-cost IoT sensors tracking user location and health information are rarely equipped with strong authentication and security mechanisms. Lack of high-end protection can ease the shield for massive data collection from attacks. In 6G, when smart things and humans are supposed to be connected, the challenges of securing networks will increase exponentially.

Mobile users may regrettably accept risks to use services and are unaware of potential threats until real damage occurs. Another common pitfall is that collecting personal information does not matter since many users think data poses no risk or has little value. Worse, many data-driven businesses may not warn or may mislead users about potential consequences following the severity or the range of data collection in all ways. For example, a company may want sensitive data about their employees, arguing it may impact job performance. Social platforms seek information to help them run personalized ads and improve user experience by obtaining relevant information. Many laws [238] have tried to close such loopholes by imposing a high responsibility on data collectors or a limit on the kind of data they can collect. However, the challenge is that the oversight of privacy preservation practices is often limited. Users have little control over what companies can do regarding the kind of data gathered or how much data is collected. Penalties can only be imposed after massive

data breaches have occurred. It is also unclear whether any campaign exploited collected data to target a specific object.

D. Summary of lessons learned from privacy enhancing technologies

Table X summarizes key state-of-the-art solutions and their pros and cons for enhancing privacy preservation in all three layers (physical/connection/service). Privacy preservation in 6G will likely significantly inherit from these key methods. Some prospective privacy enhancing technologies that will impact 6G consist of blockchain, federated learning/distributed learning, quantum homomorphic encryption, and differential privacy. However, to achieve feasible implementation for 6G, many of their flaws and weaknesses need to be addressed, such as the capability to resist insider attacks. Three key lessons learned from the privacy-enhancing technologies are as follows.

1) *6G privacy matters, but preserving it properly needs much input*. Privacy preservation issues are not new and have been researched for years. However, the technologies have achieved little to resolve the realities of massive data breaches, which take place almost every day. Bad practices by data collectors in storing/processing user information and lack of advanced data protection are two of many reasons that contribute to worsening the chance of addressing these issues thoroughly. If policy and laws do not keep up, solving all of these problems may take years, even longer.
2) *A good privacy preservation solution should take care more about conditional anonymity to meet QoS of applications and less cost to implement than perfect anonymity at any price*. History shows that none of the state-of-the-art security and privacy preservation methods such as end-to-end encryption and blockchain can quickly be applied at large if their implementations result in the high complexity and high latency. A reasonable approach would be to link privacy preservation design to the anonymity requirements of applications, deployment/maintenance cost, and, importantly, less to changes in the security architecture. Also, besides enhancing high-performance computing and networking technologies to accelerate processing/transmission capability, security solutions that can balance the anonymity and QoS of applications such as distributed learning may have a greater chance of being implemented in many 6G applications.
3) *Community awareness about the right to privacy and well-organized regulations are important factors for accelerating privacy-enhancing technologies*. While few data-driven companies will voluntarily comply with GDPR and ISO/IEC's privacy principles if not forced to do, individuals may be able to protect themselves by avoiding sharing their personal data to use a service at any cost. The stringent requirements from end-users and high penalties by law are the strongest motivations for businesses to enhance data privacy.

X. Discussion on Future Research Directions and Open Issues

6G is a unique opportunity for significantly improving security and privacy. There are two main approaches to advance this goal. One is to secure high-impact enabling technologies for 6G, and the other is to improve 5G technologies which will likely be carried over to 6G. The summary of some prospective technologies for enhancing 6G security and privacy are illustrated in Fig. 27. These assessments are classified by our vision on the criteria of automation, trustworthiness, privacy, reliability, and openness. For example, before the full quantum-safe TLS protocols operate, a period transition with temporary quantum-resistance ciphersuites can be reasonable. In the other example, the distributed subscription may come after a transition of using nuSIM or non-ID for subscriber identity management. The positions of the technologies can change periodically, depending on the standardization and the market demands.

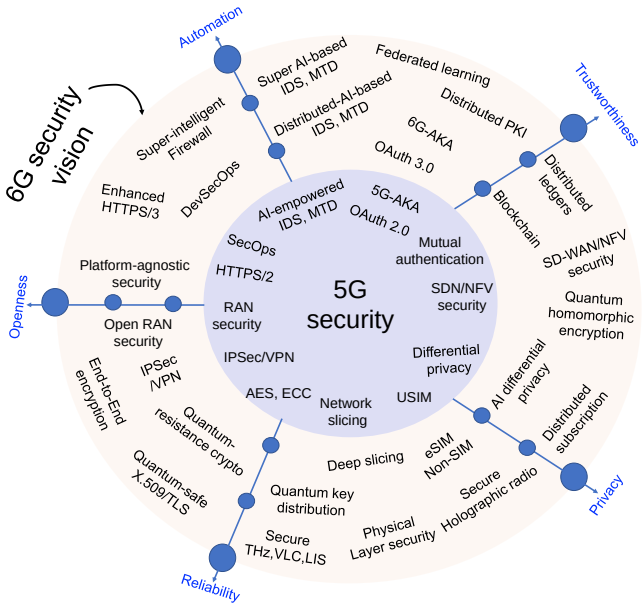

Fig. 27. The illustration of our vision on the evolution path of security technologies in 6G, from 5G. 6G will continue the trajectory of many 5G security technologies with significant upgrades of performance capabilities and models to satisfy new applications.

A. Future research directions for 6G security and privacy

1) Securing high-impact enabling technologies for 6G: AI, THz, quantum computing, ultra-massive MIMO, and more: The biggest upgrade on 6G networks will likely occur in the physical layer. To satisfy requirements such as network speeds greater that 1Tbps, many bet on THz communications and ultra-massive MIMO antenna technologies. Despite impressive initial results, these technologies have proved to be vulnerable to physical layer attacks, such as jamming and pilot contamination attacks [36]. Therefore, enhancing security of THz communications and relevant technologies such as NOMA/LIS/Holographic Radio is an important issue. An emerging solution is to build AI/ML models to improve

secrecy rates and minimize the secrecy outage probabilities in these technologies, particularly with the existence of fading influence of partial or imperfect CSI. Such integration can be applied to improve key physical generation performance, physical layer authentication, radio slicing, and anti-jamming. However, 6G physical layer security will need a breakthrough in implementation; otherwise, the vision of commercial deployment will be unlikely. In the connection layer, quantum-safe encryption and key distribution are expected to be the next-generation standards for communication security, likely to be first applied to 6G. While the winner of the standardization process race is unclear, related studies such as [152] have revealed technical challenges of efficient key exchange that may take years to solve, at least with the current infrastructure. At the service layer, microservices and serverless security will likely dominate the protection models in 6G, in which security will be integrated into functions instead of using firewalls and secure web gateways as is currently done.

2) Enhancing 5G technologies for 6G: SDN, network slicing, vRAN/Open RAN, Edge, and their successors: 6G continues to perfect many of the technologies and features of 5G security. MmWave bands above 300 GHz are likely important forces for 6G-compatible communications (with 5G/5.5G network infrastructure) in the physical layer. Therefore, fixing vulnerabilities of mmWave and massive MIMO technologies is still an important task for maintaining 6G security, given that a complete transition to THz technology may take years. Security challenges in vRAN and cloud paradigms (C-RAN) are further concerns. Given the complexity of vRAN management, more testing on vRAN API control vulnerabilities is required. Any bug or design flaw in the shared infrastructure of vRAN/C-RAN can also compromise entire security isolation functions and result in networks in chaos. It is certainly critical to address these vulnerabilities since vRAN/C-RAN will shortly be deployed.

Although it is only at an early stage of development, there is a high expectation of a breakthrough in SD-WAN security, which will be crucial because 6G, or at least autonomous systems in 6G, will likely be managed by this technology. SD-WAN security will be an important step toward the vision of intent-based networking and network-as-a-service models, the key goal of 6G. In the service layer, enhanced versions of biometric authentication, AI-empowered firewalls/IDS, and open-source security will be the pillars of 6G service security, given the reputation of efficiency of its predecessors, proved by commercial deployment.

3) Enhancing privacy technologies that satisfy GDPR: The complexity of networks and the diversity of applications in 6G will likely complicate data privacy preservation more than ever. As we noted in Section IX, privacy concerns are not unique to 6G, but will probably become worse. Privacy challenges rooted in many factors (e.g., tricks of data-driven business platforms or lack of advanced security protection in low-cost devices) are not easy to fix quickly. However, since big data is critical for AI and knowledge mining, balancing data collection needs for learning in beneficial applications and business is extremely hard. Blockchain, distributed learning, federated learning, homomorphic encryption, and differential privacy are potential technologies that support protecting personal data, complying with GDPR standards, and satisfying the needs for information mining models. With many remaining high complexity and computation challenges, more enhancements and stress tests to verify their feasibility for real network environments will then be needed.

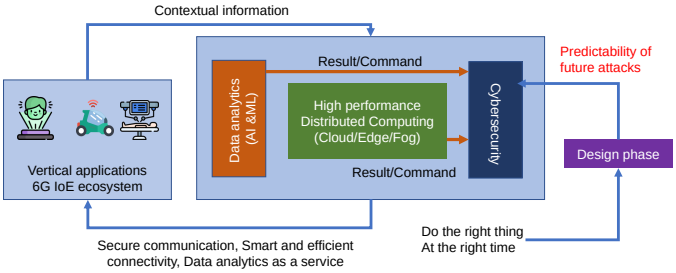

Fig. 28. An illustration of the key role of timely processing and predictability in 6G security to support two other pillars of 6G networks (updated from the "Smart Networks" concept of [3]).

B. Open challenges and issues

1) Real-time adaptive security – challenge for a breakthrough: 6G will deliver ultra-low latency (less than 0.1 milliseconds), which will enable many latency-sensitive applications, such as autonomous vehicles, industrial automation, and telesurgery. These applications must meet their deadlines. Conventional security solutions are designed to defend both IT and corporate networks, but they will likely fail to satisfy such 6G-enabled real-time applications if there are no further breakthroughs. A real-time security system should ensure that these time-critical applications meet their deadlines regardless of malicious activities. There are three design challenges for real-time security described briefly below.

1) Seeking no interference influence in the system to preserve the time constraints of applications. Such interference influences may introduce infinite delays which will impair the predictability and determinism of real-time applications.
2) Employing real-time adaptive responses to security incidents: Adaptive security software must be able to learn network behavior dynamically and respond to security alerts.
3) Implementing rapid and real-time context-aware security for target applications: A security solution is expected to demonstrate its efficiency in intrusion detection in two ways, by performing real-time anomaly detection compatible with 6G "wire" speed or by supporting context-aware security protection with diversified data generated from target applications.

We believe that implementing an adaptive security defense system to respond to attacks in real-time is a challenge, given the difficulty of processing massive data transmission without delay. Advancements of optical networks, superluminal communication, high-performance computing, and intelligent edge technologies may in the future partially address this problem by enabling super-fast processing and one-hop communication. Also, apply AI to support predictability in protection

systems is another promising approach. Fig. 28 illustrates the key role of timely processing and predictability in 6G security, besides availability-integrity-confidentiality principles.

2) Simplifying the security architecture and relevant technologies – a not-easy-at-all target: Simplicity and transparency are the keys to keeping a network system more secure and introducing fewer vulnerabilities because of more oversight of the community. Many hope that 6G security architecture will be simpler or even enable better oversight rights for users on how operators protect their data, which 5G is not supposed to have achieved. Supposing 6G network coverage will be expanded substantially, as well as the diversity of applications and services with different protection requirement goals, achieving these goals will not be a trivial task. Several initiatives such as slicing, open encryption standards, open security orchestration, and open authentication protocols may boost this target.

3) Maintaining backward compatibility is a complicated issue but likely a must-have feature in 6G security: As we noted in Section III-C, selecting a non-stand-alone deployment strategy, which most operators favor, requires the capability of backward compatibility maintenance in network access authentication and mutual authentication between the serving network and the home network. However, the backward compatibility feature can open the door to exposing old vulnerabilities when 6G must request 5G security architecture to authenticate deployed devices. The details of a backward compatibility feature and how to implement it in 6G security architecture may need to be given more thought in the future.

4) Supply chain security – an emerging issue for the development of 6G security: Supply chain digitalization has become unavoidable in modern business processes by making them more flexible and accurate. The shortage of supply chains recently highlighted the vital role of supply assurance. A timeline for enabling many 6G key technologies, such as AI and high-performance computing, will likely significantly impact a supply chain if it is cut off or disrupted on a large scale. Security and privacy issues become an even bigger challenge to overcome when supply-chain management becomes a potential attack target because of the wide attack surfaces and consequences from system breaches. Also, software and hardware from untrusted sources can threaten the trust of networks and be a real danger to business assets.

A recent hearing called "5G Supply Chain Security: Threats and Solutions" held on March 2020 in the US Senate examined the security and integrity of telecommunications supply chains and protecting the network transition to 5G. Further, the ATIS Supply Chain Working Group is working on the development of supply chain standards for public and private sectors. We can expect that stakeholders in 6G technologies and infrastructure will be concerned about supply chain security in terms of hardware, software and communications aspects, and make efforts to develop mechanisms to detect corrupted components before use. For example, hardware supply chain authentication and security are intended as countermeasures to various threats and attacks on networks, and to validate 6G hardware/equipment's authenticity. Three key technologies to ensure supply chain security are based on, (1) blockchain, (2) AI, and (3) physically unclonable functions [253]. In the future, AI can be the key technology for reinforcing security protection for supply chain management platforms and enhance accuracy performance for key processes, such as demand forecasting and secure shipping. From a telecom operator's point of view, attention to security validations and measurements of hardware (e.g., chipsets, semiconductors, and equipment) and software (e.g., inhouse built software, commercial software, and open-source software) could significantly contribute to for supply chain security and effectiveness.

5) Transforming the hardware-driven security platforms into the software-driven security platforms can create new risks: Top network operators are major forces who lobby strongly for the idea of transforming network control functions from a hardware-based model into a software-based platform or platform-agnostic system. The goal is to avoid locking in a specific vendor, increase modularity and diversify supply chains. At first glance, this transition seems a good strategy and will benefit operators with a long-term vision. However, we argue that open software-driven platforms may still have certain drawbacks in security aspects. First, software-based platforms are susceptible to more attack surfaces, such as from conventional techniques like DDoS. Although issuing software patches is undoubtedly faster than going with hardware, these platforms are also at risk of more defections and human errors when managing millions of line codes.

XI. Conclusion

Security and privacy have been the pillars of the success of mobile networks. In 6G, when the right to Internet access is guaranteed to everyone, the networks will become a gigantic connected world, with heterogeneous domains of enterprise and telecom networks, virtual and physical, satellites, terrestrial nodes, and so on. The more complicated the networks are, the more risks we face. Other than traditional security concerns such as virus/malware/DDoS attacks/deepfake, learning-empowered attacks and massive data breaches may occur more commonly in 6G because of the increase in connected devices and novel technologies. This work has provided an overview of security and privacy issues of prospective technologies for the physical, connection, service layers of 6G. Based on the lessons learned from the survey, we have outlined an assessment of the prospective technologies for 6G security and privacy issues, such as physical layer security, QKD, deep slicing, and distributed ledgers. However, satisfying real-time protection requirements and energy efficiency are still major challenges for such technologies. Without these features, many 6G security services likely fall short of their own goals. Finally, we believe that supply chain security – while not a technical issue – will play a central role in keeping the development of 6G security on the right track. The success of several initiatives, such as open RAN and open-source security, will be an essential part of improving supply chain security.

Acknowledgment

This work was supported in part by the Ministry of Education and Training (MOET) of Vietnam and Thai Nguyen University under Grant No B2021-TNA-02.

REFERENCES

[1] N. DOCOMO, "White paper: 5g evolution and 6g," *Technical report*, accessed on 10 August 2021.

[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6g wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

[3] 5GIA, "Strategic research and innovation agenda 2021-27 - smart networks in the context of ngi," *European Technology Platform NetWorld 2020*, Sep 2020.

[4] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6g: State of the art, challenges, and opportunities," *Computer Networks*, vol. 183, 2020.

[5] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6g: Machine-learning approaches," *Proceeding of IEEE*, vol. 108, no. 02, 2020.

[6] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6g: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020.

[7] M. A. Ferrag, L. Maglaras, and A. Derhab, "Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends," *Security and Communication Networks*, 2019.

[8] 3GPP.SA3, "Technical specification group services and system aspects;security architecture and procedures for 5g system," *3GPP TS 33.501 V16.4.0*, 2020.

[9] M. Bartock, J. Cichonski, and M. Souppaya, "5g cybersecurity - preparing a secure evolution to 5g," *National Institute of Standards and Technology*, 2020.

[10] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5g and beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682–3722, 2019.

[11] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6g: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, 2020.

[12] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6g wireless communications: Vision and potential techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, 2019.

[13] Verizon, "Dynamic spectrum sharing," *https://www.fiercewireless.com/operators/verizon-cto-we-re-thrilled-dss-performance*, accessed on 10 August 2021.

[14] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[15] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, "Enabling massive iot toward 6g: A comprehensive survey," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[16] S. A. et al., "6g white paper on machine learning in wireless communication networks," *https://arxiv.org/pdf/2004.13875.pdf*, accessed on 10 August 2021.

[17] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging sdn and nfv security mechanisms for iot systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 812–837, 2019.

[18] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[19] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (v2x) communication platforms," *IEEE Transactions on Intelligent Vehicles*, vol. 5, no. 4, pp. 693–713, 2020.

[20] N. Promwongsa, A. Ebrahimzadeh, D. Naboulsi, S. Kianpisheh, F. Belqasmi, R. Glitho, N. Crespi, and O. Alfandi, "A comprehensive survey of the tactile internet: State-of-the-art and research directions," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 472–523, 2021.

[21] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[22] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3gpp 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[23] Y. Hui, N. Cheng, Z. Su, Y. Huang, P. Zhao, T. H. Luan, and C. Li, "Secure and personalized edge computing services in 6g heterogeneous vehicular networks," *IEEE Internet of Things Journal*, pp. 1–1, 2021.

[24] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, 2021.

[25] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, 2019.

[26] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in sdn: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 159, 2020.

[27] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2021.

[28] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, pp. 281–291, 2020.

[29] M. Ylianttila et al., "6g white paper: Research challenges for trust, security and privacy," *https://arxiv.org/pdf/2004.11665.pdf*, accessed on 10 August 2021.

[30] R. Kantola, "Trust networking for beyond 5g and 6g," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–6, 2020.

[31] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of ai techniques for 6g communication networks," *Comput. Commun.*, vol. 161, pp. 279–303, 2020.

[32] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, "6g: A comprehensive survey on technologies, applications, challenges, and research problems," *Wiley Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, 2021.

[33] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021(early access).

[34] K. W. Huang and H. M. Wang, "Intelligent reflecting surface aided pilot contamination attack and its countermeasure," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 345–359, 2021.

[35] S. Pirandola et al, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[36] W. Xu, C. Yuan, S. Xu, H. Q. Ngo, and W. Xiang, "On pilot spoofing attack in massive mimo systems: Detection and countermeasure," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1396–1409, 2021.

[37] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[38] Ericsson, "5g security - enabling a trustworthy 5g system," *https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security—enabling-a-trustworthy-5g-syste*, accessed on 10 August 2021.

[39] Huawei, "5g security assurance," *https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf?la=en*, accessed on 10 August 2021.

[40] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Pöpper, "On security research towards future mobile network generations," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2518–2542, 2018.

[41] ETSI, "Network functions virtualisation (nfv) security," *ETSI GS NFV-SEC 013 V3.1.1*, 2017.

[42] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5g: Ran, core network and caching solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3098–3130, 2018.

[43] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edge-computing-assisted internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, 2021.

[44] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[45] P. Wright, C. White, R. C. Parker, J. S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. V. Penty, T. P. Spiller, and A. Lord, "5g network slicing with qkd and quantum-safe security," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 13, no. 3, pp. 33–40, 2021.

[46] EMnify, "Global 2g and 3g phase out/ sunset: What do we know so far?," *https://www.emnify.com/en/resources/global-2g-phase-out*, accessed on 10 August 2021.

[47] Wikipedia, "Imsi-catcher," *https://en.wikipedia.org/wiki/IMSI-catcher*, accessed on 10 August 2021.

[48] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "Imsi-catch me if you can: Imsi-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ACSAC '14, (New York, NY, USA), p. 246–255, Association for Computing Machinery, 2014.

[49] G. Cattaneo, G. D. Maio., P. FaruoloUmberto, and F. Petrillo, "A review of security attacks on the gsm standard," *Information and Communication Technology*, pp. 507–512, 2013.

[50] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating imsi catchers," *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

[51] U. Meyer and S. Wetzel, "A man-in-the-middle attack on umts," *ACM Workshop on Wireless Security*, 2004.

[52] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[53] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019.

[54] 3GPP, "3gpp v10.0.0, technical specifications and technical reports for a utran-based 3gpp system," *Technical Specification*, 2009.

[55] GSA, "Lte & 5g market statistics – december 2020," *https://gsacom.com/paper/lte-5g-market-statistics-december-2020/*, accessed on 10 August 2021.

[56] 3GPP, "3gpp ts 33.401, 3gpp system architecture evolution (sae); security architecture," *Technical Specification*, 2015.

[57] M. Paolini, "Wireless security in lte networks," *https://www.f5.com/content/dam/f5/corp/global/pdf/white-papers/SenzaFili_WirelessSecurity_F5_Oct-2012.pdf*, accessed on 10 August 2021.

[58] B. Hong, S. Bae, and Y. Kim, "Guti reallocation demystified: Cellular location tracking with changing temporary identifier," *Network and Distributed System Security (NDSS) Symposium*, 2018.

[59] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "Lteinspector: A systematic approach for adversarial testing of 4g lte," *Network and Distributed Systems Security (NDSS) Symposium*, 2018.

[60] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4g and 5g cellular paging protocols using side channel information," *Network and Distributed Systems Security (NDSS) Symposium*, 2019.

[61] C.-Y. Li, G.-H. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of voice solution volte in lte mobile networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, (New York, NY, USA), p. 316–327, Association for Computing Machinery, 2015.

[62] H. Kim et al., "Breaking and fixing volte: Exploiting hidden data channels and mis-implementations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, (New York, NY, USA), p. 328–339, Association for Computing Machinery, 2015.

[63] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Call me maybe: Eavesdropping encrypted LTE calls with revolte," in *29th USENIX Security Symposium (USENIX Security 20)*, pp. 73–88, USENIX Association, 2020.

[64] P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling dos attacks on 3g wireless networks," in *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pp. 1289–1297, 2007.

[65] N. Golde, K. Redon, and J.-P. Seifert, "Let me answer that for you: Exploiting broadcast information in cellular networks," in *22nd USENIX Security Symposium (USENIX Security 13)*, (Washington, D.C.), pp. 33–48, USENIX Association, 2013.

[66] P. Traynor et al., "On cellular botnets: Measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, (New York, NY, USA), p. 223–234, Association for Computing Machinery, 2009.

[67] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in sms-capable cellular networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 40–53, 2009.

[68] P. Chandra, D. Bensky, T. Bradley, C. Hurley, S. A. Rackley, J. Rittinghouse, J. Ransome, T. Stapko, G. L. Stefanek, F. Thornton, C. Lanthem, and J. Wilson, "Wireless security: Know it all," *Newnes - Book*, 2008.

[69] K. Nohl, "Rooting sim cards," *Blackhat*, 2013.

[70] J. R. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely, "Partitioning attacks: or how to rapidly clone some gsm cards," in *Proceedings 2002 IEEE Symposium on Security and Privacy*, pp. 31–41, 2002.

[71] D. Rupprecht, K. Kohls, T. Holz, and C. Popper, "Imp4gt: Impersonation attacks in 4g networks," *Network and Distributed Systems Security (NDSS) Symposium*, 2020.

[72] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," *Network and Distributed Systems Security (NDSS) Symposium*, 2017.

[73] Verizon, "5g privacy preservation," *https://www.verizon.com/about/sites/default/files/2020-09/200574_Schulz_07242020.pdf*, accessed on 10 August 2021.

[74] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[75] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5g specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

[76] M. Juntti, R. Kantola, P. Kyösti, S. LaValle, C. M. de Lima, M. Matinmikko-Blue, T. Ojala, A. Pouttu, A. Pärssinen, and S. Yrjölä, "Key drivers and research challenges for 6g ubiquitous wireless intelligence," *6G First Sumit*, 2019.

[77] N. H. Mahmood et al., "White paper on critical and massive machine type communication towards 6g," *https://arxiv.org/abs/2004.14146*, accessed on 10 August 2021.

[78] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hätönen, "6g architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173508–173520, 2020.

[79] N. Rajatheva et al., "White paper on broadband connectivity in 6g," *http://jultika.oulu.fi/files/isbn9789526226798.pdf*, accessed on 10 August 2021.

[80] T. Taleb et al., "White paper on 6g networking," *http://jultika.oulu.fi/files/isbn97895262268842.pdf*, accessed on 10 August 2021.

[81] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, S. Mandal, A. Madanayak, A. Alkhateed, and G. C. Tripchopoulos, "Wireless communications and applications above 100 ghz: Opportunities and challenges for 6g and beyond," *IEEE Access*, vol. 7, pp. 78729–78757, 2019.

[82] M. Prytz, "Towards 6g - ericsson research," *2nd 6G Summit*, 2020.

[83] M. Matthaiou, O. Yurduseven, H. Q. Ngo, D. Morales-Jimenez, S. L. Cotton, and V. F. Fusco, "The road to 6g: Ten physical layer challenges for communications engineers," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 64–69, 2021.

[84] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjolan, and F. Tufvesson, "6g wireless systems: Vision, requirements, challenges, insights, and opportunities," *https://arxiv.org/abs/2008.03213*, accessed on 10 August 2021.

[85] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6g: Ai empowered wireless networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[86] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[87] H. Saarnisaari, S. Dixit, M.-S. Alouini, A. Chaoub, M. Giordani, A. Kliks, M. Matinmikko-Blue, and N. Zhang, "6g white paper on connectivity for remote areas," 2020.

[88] T. Wei, W. Feng, Y. Chen, C.-X. Wang, N. Ge, and J. Lu, "Hybrid satellite-terrestrial communication networks for the maritime internet of things: Key technologies, opportunities, and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8910–8934, 2021.

[89] Y. Wang, W. Feng, J. Wanga, and T. Q. S. Quek, "Hybrid satellite-uav-terrestrial networks for 6g ubiquitous coverage: A maritime communications perspective," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2021.

[90] J. Happa, M. Glencross, and A. Steed, "Cyber security threats and challenges in collaborative mixed-reality," *Frontiers in ICT*, vol. 6, p. 5, 2019.

[91] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, 2020.

[92] T. H. Szymanski, "Securing the industrial-tactile internet of things with deterministic silicon photonics switches," *IEEE Access*, vol. 4, pp. 8236–8249, 2016.

[93] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks*, vol. 3, no. 3, pp. 151–160, 2012.

[94] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. D. Renzo, and M. Debbah, "Holographic mimo surfaces for 6g wireless networks: Opportunities, challenges, and trends," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 118–125, 2020.

[95] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6g technologies: Key drivers, core requirements, system architectures, and enabling technologies," *IEEE Vehicular Technology Magazine*, vol. 18, no. 3, pp. 18–27, 2019.

[96] J. Hoffstein, J. Pipher, and J. H. Silverman, "Ntru: A ring-based public key cryptosystem," *Algorithmic Number Theory*, pp. 267–288, 1998.

[97] T. V. de Velde, "Building mutual trust in 6g," *Post*, 2020.

[98] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2714–2741, 2018.

[99] S. Yao, J. Guan, Y. Wu, K. Xu, and M. Xu, "Toward secure and lightweight access authentication in sagins," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 75–81, 2020.

[100] T. Maksymyuka, J. Gazda, M. Vološin, G. Bugár, D. Horváth, M. Klymash, and M. Dohler, "Blockchain-empowered framework for decentralized network management in 6g," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 86–92, 2020.

[101] T. N. N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: Challenges and opportunities," *2nd 6G Wireless Summit (6G SUMMIT)*, 2020.

[102] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5g mmwave grant-free iot networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 658–670, 2021.

[103] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[104] J. K. Tugnait, "Pilot spoofing attack detection and countermeasure," *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 2093–2106, 2018.

[105] W. Zhang, H. Lin, and R. Zhang, "Detection of pilot contamination attack based on uncoordinated frequency shifts," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2658–2670, 2018.

[106] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in iot network: From awgn channel to thz band," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3378–3388, 2020.

[107] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure mimo wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851–7866, 2020.

[108] J. Tang, L. Jiao, K. Zeng, H. Wen, and K. Y. Qin, "Physical layer secure mimo communications against eavesdroppers with arbitrary number of antennas," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 466–481, 2021.

[109] Y. Arjoune and S. Faruque, "Smart jamming attacks in 5g new radio: A review," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1010–1015, 2020.

[110] M. Lichtman, R. M. Rao, V. Marojevic, J. H. Reed, and R. P. Jover, "5g nr jamming, spoofing, and sniffing: Threat assessment and mitigation," *https://arxiv.org/abs/1803.03845*, 2018.

[111] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2734–2771, 2019.

[112] J. Si, Z. Cheng, Z. Li, J. Cheng, H.-M. Wang, and N. Al-Dhahir, "Cooperative jamming for secure transmission with both active and passive eavesdroppers," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5764–5777, 2020.

[113] Z. Li, M. Xia, M. Wen, and Y. C. Wu, "Massive access in secure noma under imperfect csi: Securit guaranteed sum-rate maximization with first-order algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 4, pp. 998–1014, 2021.

[114] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1656–1672, 2017.

[115] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security for noma: Requirements, merits, challenges, and recommendations," 2020.

[116] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys Tutorials*, vol. 9, no. 3, pp. 44–57, 2007.

[117] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 3313–3351, 2021.

[118] M. Wijewardena, T. Samarasinghe, K. T. Hemachandra, S. Atapattu, and J. S. Evans, "Physical layer security for intelligent reflecting surface assisted two–way communications," *IEEE Communications Letters*, pp. 1–1, 2021.

[119] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, "Secure multiple-users transmission using multi-path directional modulation," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1–5, 2016.

[120] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-domain non-orthogonal multiple access (noma) in 5g systems: Potentials and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 721–742, 2017.

[121] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity and confidentiality," *https://arxiv.org/pdf/2001.07153.pdf*, accessed on 10 August 2021.

[122] H. Peng, Z. Wang, S. Han, and Y. Jiang, "Physical layer security for miso noma vlc system under eavesdropper collusion," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2021.

[123] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 162–169, 2018.

[124] K.-c. Huang and Z. Wang, "Terahertz terabit wireless communication," *IEEE Microwave Magazine*, vol. 12, no. 4, pp. 108–116, 2011.

[125] R. Singh and D. Sicker, "Thz communications - a boon and/or bane for security, privacy, and national security," in *TPRC48: The 48th Research Conference on Communication, Information and Internet Policy*, 2020.

[126] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89–93, 2018.

[127] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmwave and terahertz systems," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1743–1747, 2020.

[128] N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6g: Advances, challenges, and prospects," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 93–102, 2020.

[129] X. Wu, M. D. Soltani, L. Zhou, M. Safari, and H. Haas, "Hybrid lifi and wifi networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 23, no. 2, pp. 1398–1420, 2021.

[130] A. Mostafa and L. Lampe, "Physical-layer security for miso visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, 2015.

[131] A. Yesilkaya, T. Cogalan, S. Erkucuk, Y. Sadi, E. Panayirci, H. Haas, and H. V. Poor, "Physical-layer security in visible light communications," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[132] E. Panayirci, A. Yesilkaya, T. Cogalan, H. V. Poor, and H. Haas, "Physical-layer security with optical generalized space shift keying," *IEEE Transactions on Communications*, vol. 68, no. 5, pp. 3042–3056, 2020.

[133] Y. Moritani, S. Hiyama, and T. Suda, "A molecular communication system," in *Natural Computing*, pp. 82–89, 2010.

[134] W. Guo, M. Abbaszadeh, L. Lin, J. Charmet, P. Thomas, Z. Wei, B. Li, and C. Zhao, "Molecular physical layer for 6g in wave-denied environments," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 33–39, 2021.

[135] V. Loscrí, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE Transactions on NanoBioscience*, vol. 13, no. 3, pp. 198–207, 2014.

[136] V. L. Nguyen, P. C. Lin, and R. H. Hwang, "Enhancing misbehavior detection in 5g vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9417–9430, 2020.

[137] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, "Deep learning for rf fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020.

[138] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1506–1521, 2021.

[139] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[140] N. Xie, S. Zhang, and A. X. Liu, "Physical-layer authentication in non-orthogonal multiple access systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1144–1157, 2020.

[141] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2260–2273, 2019.

[142] X. Lu, J. Lei, Y. Shi, and W. Li, "Intelligent reflecting surface assisted secret key generation," *IEEE Signal Processing Letters*, pp. 1–1, 2021.

[143] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, 2014.

[144] N. Ebrahimi, H. S. Kim, and D. Blaauw, "Physical layer secret key generation using joint interference and phase shift keying modulation," *IEEE Transactions on Microwave Theory and Techniques*, pp. 1–1, 2021 (early access).

[145] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020.

[146] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Artificial noise-aided mimo physical layer authentication with imperfect csi," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[147] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, 2016.

[148] L. Zhang et al., "Space-time-coding digital metasurfaces," *Nature*, vol. 9, 2018.

[149] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2595–2621, 2018.

[150] B. Hussain, Q. Du, B. Sun, and Z. Han, "Deep learning-based ddos-attack detection for cyber–physical system over 5g network," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 860–870, 2021.

[151] ETSI, "Etsi ts 133.501 v15.2.0, security architecture and procedures for 5g system," *Technical Specification Group Services and System Aspects*, 2018.

[152] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[153] ETSI, "Quantum safe cryptography and security," *White Paper No. 8*, 2015.

[154] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 9, pp. 188–194, 2017.

[155] Y.-A. Chen, Q. Zhang, and T.-Y. C. et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, p. 214–219, 2021.

[156] J.-P. Chen, C. Zhang, and Y. L. et al., "Twin-field quantum key distribution over a 511km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 68, 2021.

[157] ETSI, "Etsi ts 103 744 v1.1.1, quantum-safe hybrid key exchanges," *Technical Specification Group Services and System Aspects*, 2020.

[158] N. Potlapally, S. Ravi, A. Raghunathan, and N. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128–143, 2006.

[159] G. Milenkovic and M. Dekker, "Security in 5g specifications," *European Union Agency for Cybersecurity*, 2021.

[160] Wikipedia, "Transportation layer security," *https://en.wikipedia.org/wiki/Transport_Layer_Security*, Accessed on 10 August 2021.

[161] ITU-Y.3052, "Y.3052: Overview of trust provisioning for information and communication technology infrastructures and services," *Technical specification, https://www.itu.int/rec/T-REC-Y.3052/en*, 2017.

[162] Federal Communications Commission, "Fcc's rosenworcel talks up 6g," *https://docs.fcc.gov/public/attachments/DOC-354091A1.pdf*, accessed on 10 August 2021.

[163] S. Troia, F. Sapienza, L. Varé, and G. Maier, "On deep reinforcement learning for traffic engineering in sd-wan," *IEEE Journal on Selected Areas in Communications*, pp. 1–1, 2021 (early access).

[164] Z. Duliński, R. Stankiewicz, G. Rzym, and P. Wydrych, "Dynamic traffic management for sd-wan inter-cloud communication," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1335–1351, 2020.

[165] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020.

[166] A. Abdou, P. C. van Oorschot, and T. Wan, "Comparative analysis of control plane security of sdn and conventional networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3542–3559, 2018.

[167] M. Wood, "How sase is defining the future of network security," *Network Security*, vol. 2020, no. 12, pp. 6–8, 2020.

[168] C. Craven, "What is sd-wan security," *https://www.sdxcentral.com/networking/sd-wan/definitions/what-is-sd-wan-security*, accessed on 10 August 2021.

[169] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent advances, taxonomy, requirements, and open research challenges," *IEEE Access*, vol. 8, pp. 36009–36028, 2020.

[170] Q. Bi, "Ten trends in the cellular industry and an outlook on 6g," *IEEE Communications Magazine*, vol. 57, no. 12, pp. 31–36, 2019.

[171] M. Chahbar, G. Diaz, A. Dandoush, C. Cérin, and K. Ghoumid, "A comprehensive survey on the e2e 5g network slicing model," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2020.

[172] H. Zhang and V. W. S. Wong, "A two-timescale approach for network slicing in c-ran," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6656–6669, 2020.

[173] 3GPP.SA3, "Study on security aspects of 5g network slicing management," *3GPP TR 33.811 V15.0.0*, 2018.

[174] S. Lal, T. Taleb, and A. Dutta, "Nfv: Security threats and best practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[175] E. Hanselman, "Security benefits of open virtualized ran," *https://www.redhat.com/cms/managed-files/ve-451-research-telco-vran-security-analyst-material-f23695-en.pdf*, accessed on 10 August 2021.

[176] C. Reichert, "Ericsson: Expired certificate caused o2 and softbank outages," *https://www.zdnet.com/*, accessed on 10 August 2021.

[177] C. Skouloudi, A. Malatras, and R. Naydenov, "Guidelines for securing the internet of things," *European Union Agency for Cybersecurity*, 2020.

[178] A. Aldweesh, A. Derhab, and A. Z.Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, p. 105124, 2020.

[179] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[180] C. Sexton, N. J. Kaminski, J. M. Marquez-Barja, N. Marchetti, and L. A. DaSilva, "5g: Adaptable networks enabled by versatile radio access technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 688–720, 2017.

[181] D. Silver, S. Singh, D. Precup, and R. S. Sutton, "Reward is enough," *Artificial Intelligence*, vol. 299, p. 103535, 2021.

[182] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Network*, vol. 34, no. 6, pp. 133–139, 2020.

[183] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "Bcppa: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, June 2020.

[184] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." RFC 5280, 2008.

[185] 3GPP, "Authentication and key management for applications (akma) based on 3gpp credentials in the 5g system (5gs)," *Technical Specification*, 2021.

[186] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "Cloudid: Trustworthy cloud-based and cross-enterprise biometric identification," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7905–7916, 2015.

[187] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Deep hashing for secure multimodal biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1306–1321, 2021.

[188] C. Yuan, S. Jiao, X. Sun, and Q. M. J. Wu, "Mfffld: A multi-modal feature fusion based fingerprint liveness detection," *IEEE Transactions on Cognitive and Developmental Systems*, pp. 1–1, 2021 (early access).

[189] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "Ecg authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2016.

[190] P. Arnau-González, S. Katsigiannis, M. Arevalillo-Herráez, and N. Ramzan, "Bed: A new dataset for eeg-based biometrics," *IEEE Internet of Things Journal*, pp. 1–1, 2021 (early access).

[191] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[192] F. Lin, K. W. Cho, C. Song, Z. Jin, and W. Xu, "Exploring a brain-based cancelable biometrics for smart headwear: Concept, implementation, and evaluation," *IEEE Transactions on Mobile Computing*, vol. 19, no. 12, pp. 2774–2792, 2020.

[193] Wikiperdia, "Biometric," *https://en.wikipedia.org/wiki/Biometrics*, accessed on 10 August 2021.

[194] J. Richer, A. Parecki, and F. Imbault, "Grant Negotiation and Authorization Protocol," Internet-Draft draft-ietf-gnap-core-protocol-06, Internet Engineering Task Force, 2021. Work in Progress.

[195] M. Bishop, "Hypertext Transfer Protocol Version 3 (HTTP/3)," Internet-Draft draft-ietf-quic-http-34, Internet Engineering Task Force, 2021.

[196] R. Lychev, S. Jero, A. Boldyreva, and C. Nita-Rotaru, "How secure and quick is quic? provable security and performance analyses," in *2015 IEEE Symposium on Security and Privacy*, pp. 214–231, 2015.

[197] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[198] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020.

[199] J. Zeuner, I. Pitsios, S.-H. Tan, A. N. Sharma, J. F. Fitzsimons, R. Osellame, and P. Walther, "Experimental quantum homomorphic encryption," *npj Quantum Information*, vol. 1, no. 1, pp. 38–45, 2021.

[200] Z. Fu, L. Xia, X. Sun, A. X. Liu, and G. Xie, "Semantic-aware searching over encrypted data for cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2359–2371, 2018.

[201] X. Ge, J. Yu, H. Zhang, C. Hu, Z. Li, Z. Qin, and R. Hao, "Towards achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 490–504, 2021.

[202] E. Peltonen et al., "6g white paper on edge intelligence," *CoRR*, vol. abs/2004.14850, 2020.

[203] Y. Wang, Q. Wang, X. Chen, D. Chen, X. Fang, M. Yin, and N. Zhang, "Containerguard: A real-time attack detection system in container-based big data platform," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2020.

[204] X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis, and H. Wang, "A study on the security implications of information leakages in container clouds," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 174–191, 2021.

[205] S. Iqbal, M. L. Mat Kiah, B. Dhaghighi, and Muzammil, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *Journal of Network and Computer Applications*, vol. 74, pp. 98–120, 2016.

[206] U. Challita, H. Rydén, and H. Tullberg, "When machine learning meets wireless cellular networks: Deployment, challenges, and applications," *IEEE Communications Magazine*, vol. 58, pp. 12–18, 2020.

[207] N. Kaloudi and J. Li, "The AI-based cyber threat landscape," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–34, 2020.

[208] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[209] C. Han, L. Huo, X. Tong, H. Wang, and X. Liu, "Spatial anti-jamming scheme for internet of satellites based on the deep reinforcement learning and stackelberg game," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5331–5342, 2020.

[210] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, pp. 2–14, 2019.

[211] N. Ye, X. Li, H. Yu, A. Wang, W. Liu, and X. Hou, "Deep learning aided grant-free noma toward reliable low-latency access in tactile internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2995–3005, 2019.

[212] W. Kim, Y. Ahn, and B. Shim, "Deep neural network-based active user detection for grant-free noma systems," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2143–2155, 2020.

[213] M. Yan, G. Feng, J. Zhou, Y. Sun, and Y. C. Liang, "Intelligent resource scheduling for 5g radio access network slicing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 8, pp. 7691–7703, 2019.

[214] Y. J. Liu, G. Feng, Y. Sun, S. Qin, and Y. C. Liang, "Device association for ran slicing based on hybrid federated deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15731–15745, 2020.

[215] J. Chen, J. Chen, and H. Zhang, "Drl-qor: Deep reinforcement learning based qos/qoe-aware adaptive online orchestration in nfv-enabled networks," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2021 (early access).

[216] D. Y. Hwang, B. Taha, D. S. Lee, and D. Hatzinakos, "Evaluation of the time stability and uniqueness in ppg-based biometric system," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 116–130, 2021.

[217] J. A. Ayala-Romero, A. Garcia-Saavedra, M. Gramaglia, X. Costa-Pérez, A. Banchs, and J. J. Alcaraz, "Vrain: A deep learning approach tailoring computing and radio resources in virtualized rans," in *The 25th Annual International Conference on Mobile Computing and Networking*, MobiCom '19, (New York, NY, USA), Association for Computing Machinery, 2019.

[218] G. Ishigaki, S. Devic, R. Gour, and J. P. Jue, "Deeppr: Progressive recovery for interdependent vnfs with deep reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 10, pp. 2386–2399, 2020.

[219] T. Edwards and M. S. Hossain, "Effectiveness of deep learning on serial fusion based biometric systems," *IEEE Transactions on Artificial Intelligence*, pp. 1–1, 2021 (early access).

[220] H. Yang, A. Alphones, Z. Xiong, D. Niyato, J. Zhao, and K. Wu, "Artificial-intelligence-enabled intelligent 6g networks," *IEEE Network*, vol. 34, pp. 272–280, 2020.

[221] B. Caroline et al., "Artificial intelligence cybersecurity challenges, threat landscape for artificial intelligence," *Technical report*, 2020.

[222] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6g communications: Challenges, methods, and future directions," *China Communications*, vol. 17, pp. 105–118, 2020.

[223] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[224] G. Muhammad, M. S. Hossain, and S. Garg, "Stacked autoencoder-based intrusion detection system to combat financial fraudulent," *IEEE Internet of Things Journal*, pp. 1–1, 2020 (early access).

[225] P. Peng, T. Xiang, Y. Wang, M. Pontil, S. Gong, T. Huang, and Y. Tian, "Unsupervised cross-dataset transfer learning for person re-identification," in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1306–1315, 2016.

[226] M. Ribeiro, S. Singh, and C. Guestrin, ""why should I trust you?": Explaining the predictions of any classifier," in *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Demonstrations*, (San Diego, California), pp. 97–101, Association for Computational Linguistics, June 2016.

[227] T. Vidal and M. Schiffer, "Born-again tree ensembles," in *Proceedings of the 37th International Conference on Machine Learning* (H. D. III and A. Singh, eds.), vol. 119 of *Proceedings of Machine Learning Research*, pp. 9743–9753, PMLR, 13–18 Jul 2020.

[228] M. Comiter, "Attacking artificial intelligence: Ai's security vulnerability and what policymakers can do about it," *https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf*, accessed on 10 August 2021.

[229] K. Sadeghi, A. Banerjee, and S. Gupta, "A system-driven taxonomy of attacks and defenses in adversarial machine learning," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, pp. 450–467, 2020.

[230] K. Ren, T. Zheng, Z. Qin, and X. Liu, "Adversarial attacks and defenses in deep learning," *Engineering*, vol. 6, no. 3, pp. 346–360, 2020.

[231] ETSI, "Etsi gr sai 005 v1.1.1, securing artificial intelligence (sai); mitigation strategy report," *Technical Specification Group Services and System Aspects*, 2021.

[232] A. Bar, J. Lohdefink, N. Kapoor, S. J. Varghese, F. Huger, P. Schlicht, and T. Fingscheidt, "The vulnerability of semantic segmentation networks to adversarial attacks in autonomous driving: Enhancing extensive environment sensing," *IEEE Signal Processing Magazine*, vol. 38, pp. 42–52, 2021.

[233] J. Shen, J. Won, Z. Chen, and Q. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under gps spoofing (extended version)," *https://arxiv.org/abs/2006.10318*, accessed on 10 August 2021.

[234] M. P. Stoecklin, "Deeplocker: How ai can power a stealthy new breed of malware," *Security Intelligence*, vol. 8, 2018.

[235] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized ai for cyber attacks," *J. Inf. Secur. Appl.*, vol. 57, p. 102722, 2021.

[236] European-Union, "General data protection regulation," *European Union - Regulation 2016/679*, 2016.

[237] P. Pleva, "A revised classification of anonymity," *http://arxiv.org/abs/1211.5613*, accessed on 10 August 2021.

[238] US.Congress, "The privacy act of 1974," *U.S. Department of Justice*, 2016.

[239] I. Sherr, "Facebook, cambridge analytica and data mining: What you need to know," *https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/*, accessed on 10 August 2021.

[240] J. C. W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy-preserving multiobjective sanitization model in 6g iot environments," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5340–5349, 2021.

[241] Y. Wu, Y. Ma, H.-N. Dai, and H. Wang, "Deep learning for privacy preservation in autonomous moving platforms enhanced 5g heterogeneous networks," *Computer Networks*, vol. 185, p. 107743, 2021.

[242] P. Silva, E. Monteiro, and P. Simões, "Privacy in the cloud: A survey of existing solutions and research challenges," *IEEE Access*, vol. 9, pp. 10473–10497, 2021.

[243] N. Kaaniche, M. Laurent, and S. Belguith, "Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey," *Journal of Network and Computer Applications*, vol. 171, p. 102807, 2020.

[244] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, "Privacy enhancing technologies in the internet of things: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2159–2187, 2019.

[245] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[246] H. Xu, P. V. Klaine, O. Onireti, B. Cao, and M. Imrana, "Blockchain-enabled resource management and sharing for 6g communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, 2020.

[247] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for industrial internet of things: Opportunities, applications and challenges," *IEEE Internet of Things Journal*, pp. 1–1, 2021 (early access).

[248] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2020.

[249] Y. Rahulamathavan, S. Dogan, X. Shi, R. Lu, M. Rajarajan, and A. Kondoz, "Scalar product lattice computation for efficient privacy-preserving systems," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1417–1427, 2021.

[250] Y. Xiao, G. Shi, and M. Krunz, "Towards ubiquitous ai in 6g with federated learning," *https://arxiv.org/pdf/2004.13563.pdf*, 2020.

[251] Q. Zhang, C. Xin, and H. Wu, "Privacy preserving deep learning based on multi-party secure computation: A survey," *IEEE Internet of Things Journal*, pp. 1–1, 2021 (early access).

[252] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, and X. Zheng, "Privacy-preserving federated learning framework based on chained secure multiparty computing," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6178–6186, 2021.

[253] V. Hassija, V. Chamola, V. Gupta, S. Jain, and N. Guizani, "A survey on supply chain security: Application areas, security threats, and solution architectures," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6222–6246, 2021.

Van-Linh Nguyen is an assistant professor of the Department of Information Technology, Thai Nguyen University of Information and Communication Technology (ICTU), Vietnam. He received his Ph.D. degree in computer science and information engineering from National Chung Cheng University (CCU), Taiwan, in 2019. His current research interests include cybersecurity, network/edge intelligence, autonomous driving, and vehicular networks.

Po-Ching Lin received his Ph.D. degree in computer science from National Chiao Tung University, Hsinchu, Taiwan, in 2008. He joined the faculty of the Department of Computer Science and Information Engineering, CCU, in August 2009. He is currently a professor. His research interests include network security, network traffic analysis, and performance evaluation of network systems.

Bo-Chao Cheng is a Professor of Department of Communications Engineering at National Chung-Cheng University. Cheng received a PhD degree in CIS from New Jersey Institute of Technology in 1996. After graduations, he also worked for Transtech Network (2000-2002), Bellcore (1998–2000) and Racal DataCom (1996-1998) respectively. His broad interests include network security, network management and real-time embedded system design.

Ren-Hung Hwang received his Ph.D. degree in computer science from the University of Massachusetts, Amherst. He joined the Department of Computer Science and Information Engineering, National Chung Cheng University in 1993, where he is now a distinguished professor and the chief information technology officer. He has published more than 250 international journal and conference papers. He served as the Dean of the College of Engineering during 2014–2017. He received the IEEE Best Paper Award from IoV 2019, IEEE Ubi-Media 2018, IEEE SC2 2017, and IEEE IUCC 2014. His current research interests include Internet of Things, network security, cloud/edge/fog computing, and 5G V2X networks.

Ying-Dar Lin is a Chair Professor of computer science at National Yang Ming Chiao Tung University, Taiwan. He received his Ph.D. in computer science from the University of California at Los Angeles (UCLA) in 1993. He was a visiting scholar at Cisco Systems in San Jose during 2007–2008, CEO at Telecom Technology Center, Taiwan, during 2010–2011, and Vice President of National Applied Research Labs (NARLabs), Taiwan, during 2017-2018. He was the founder and director of Network Benchmarking Lab (NBL) in 2002–2018, which reviewed network products with real traffic and automated tools, and has been an approved test lab of the Open Networking Foundation (ONF). He also cofounded L7 Networks Inc. in 2002, later acquired by D-Link Corp, and O'Prueba Inc. a spin-off from NBL, in 2018. His research interests include network security, wireless communications, network softwarization, and machine learning for communications. His work on multi-hop cellular was the first along this line, and has been cited over 1000 times and standardized into IEEE 802.11s, IEEE 802.15.5, IEEE 802.16j, and 3GPP LTE-Advanced. He is an IEEE Fellow (class of 2013), IEEE Distinguished Lecturer (2014–2017), ONF Research Associate (2014-2018), and received in 2017 Research Excellence Award and K. T. Li Breakthrough Award. He has served or is serving on the editorial boards of several IEEE journals and magazines, including Editor-in-Chief of IEEE Communications Surveys and Tutorials (COMST, 1/2017–12/2020). He published a textbook, Computer Networks: An Open Source Approach, with Ren-Hung Hwang and Fred Baker (McGraw-Hill, 2011).